



CENTRALISED DECENTRALISATION:

**Investigating the Regulatory Challenges and Mitigations of a
Cryptocurrency Solution for Cross-Border Transfers in South Africa**

25 May 2026

**Research Dissertation in fulfilment of the requirements for the degree of
Master of Arts in Interdisciplinary Digital Knowledge Economy Studies**

Craig Meyer

Student Number: 1342655

Supervisor: Dr Lucienne Abrahams

Co-Supervisor: Dr Kiru Pillay

LINK Centre, University of the Witwatersrand

ABSTRACT

The emergence of cryptocurrency and blockchain technology presents significant opportunities to transform cross-border financial transfers by improving transaction speed, transparency, and cost efficiency. However, integrating these decentralised technologies into highly regulated financial systems remains challenging, particularly in jurisdictions such as South Africa where regulatory frameworks were designed for traditional fiat-based financial infrastructures. This study, titled *Centralised Decentralisation: Investigating the Regulatory Challenges and Mitigations of a Cryptocurrency Solution for Cross-Border Transfers in South Africa*, investigates the regulatory, institutional, and technological barriers that influence the adoption of cryptocurrency-enabled cross-border payment solutions.

A qualitative research approach was employed, drawing on semi-structured interviews with professionals from regulatory bodies, financial institutions, and the broader fintech ecosystem. The research analyses the interaction between decentralised cryptocurrency systems and centralised financial regulation, focusing on compliance requirements such as anti-money laundering (AML), know-your-customer (KYC) obligations, exchange control policies, and financial stability considerations. The findings reveal a fragmented and evolving regulatory environment characterised by definitional ambiguity around crypto-assets, limited interoperability between blockchain systems and traditional payment infrastructure, and institutional coordination challenges among regulatory authorities.

Building on these findings, the study develops a Design Science Research (DSR) knowledge model in Chapter 6 to address regulatory gaps affecting cryptocurrency-enabled cross-border transfers. The proposed model organises reforms into interconnected regulatory and technological echelons that integrate policy alignment, institutional coordination, risk-based compliance mechanisms, and technological interoperability. This hybrid framework combines the decentralised efficiencies of blockchain with appropriate centralised oversight, enabling innovation while preserving regulatory integrity.

The conclusions highlight that while regulatory uncertainty remains a significant barrier, cryptocurrency-based systems hold considerable potential to improve cross-border payments, particularly in remittances and trade settlement. The study demonstrates that a balanced, adaptive regulatory approach, one supported by coordinated governance, regulatory sandboxes, and clear crypto-asset classifications. It can enable South Africa to harness blockchain innovation while maintaining financial stability and compliance. This research contributes to a growing body of knowledge on the intersection of cryptocurrency and financial regulation, offering insights into how South Africa can effectively adopt blockchain for cross-border transfers. It demonstrates that while regulatory challenges are significant, they are not insurmountable, and with the right mitigations, cryptocurrency technology can offer a viable and secure solution for transforming cross-border financial transfers in South Africa.

KEYWORDS

Cryptocurrency, Blockchain, Cross-border transfers, Decentralisation, Financial regulation, Anti-money laundering (AML), Know Your Customer (KYC), Counter-terrorism financing (CFT), Protection of Personal Information Act (POPIA), DeFi (Decentralised Finance), Regulatory Compliance, Regulatory sandbox, Distributed ledger technology (DLT), Regulatory Technology (RegTech)

GLOSSARY

TERM / ACRONYM	DEFINITION
Actor-Network Theory (<i>ANT</i>)	A socio-technical framework, drawn on in this study, that treats technological artefacts, institutions, and human actors as equally significant nodes in a network. Applied here to explain how blockchain protocols, CASP platforms, regulatory bodies, and end-users co-constitute South Africa's cryptocurrency ecosystem.
Algorithm / Consensus Mechanism	The set of rules by which nodes in a blockchain network agree on the validity of transactions and the state of the shared ledger. Common mechanisms include Proof of Work (PoW) and Proof of Stake (PoS), each with different implications for energy consumption, security, and governance.
Asset-Referenced Token (<i>ART</i>)	A type of crypto-asset whose value is pegged to a basket of assets (currencies, commodities, or other crypto-assets). Regulated under the EU's MiCA framework with stricter reserve and disclosure requirements than general crypto-assets.
Blockchain	A distributed ledger technology (DLT) in which validated transactions are grouped into blocks and cryptographically linked in a chronological chain, making the record tamper-resistant and transparent. Blockchain is the underlying infrastructure for cryptocurrency but is not itself the object of financial regulation; regulation applies to the crypto-assets and service providers that operate on it.
Central Bank Digital Currency (<i>CBDC</i>)	A digital form of a country's fiat currency issued and backed by the central bank. Differs from cryptocurrency in that it is centralised, legal tender, and subject to monetary policy. South Africa's SARB has explored a wholesale CBDC through Project Khokha and Project Khokha II.
Crypto-Asset Service Provider (<i>CASP</i>)	An entity that provides services involving crypto-assets, including exchange, custody, transfer, or advice. CASPs are the principal compliance actors under South Africa's regulatory framework and FATF's virtual asset standards; regulation is applied at the CASP level rather than at the blockchain protocol level.
Cryptocurrency	A subset of crypto-assets that function primarily as a medium of exchange or store of value, operating on distributed ledger infrastructure. Examples include Bitcoin, Ethereum-based stablecoins, and other tokenised digital assets. Distinct from blockchain, which is the infrastructure on which cryptocurrency operates.
Decentralised Autonomous Organisation (<i>DAO</i>)	An entity governed by smart contracts and token-holder voting rather than by a traditional legal or corporate structure. DAOs present significant regulatory challenges because they have no identifiable legal person to hold accountable under AML/KYC or consumer protection frameworks.
Decentralised Finance (<i>DeFi</i>)	A category of financial services built on public blockchain networks that operate without traditional centralised intermediaries such as banks or

TERM / ACRONYM	DEFINITION
	exchanges. DeFi protocols present particular regulatory challenges because there may be no identifiable CASP to regulate, complicating AML/CFT enforcement.
Distributed Ledger Technology (DLT)	An umbrella term for technologies that enable a shared, synchronised record of transactions across multiple nodes without a central administrator. Blockchain is the most prominent form of DLT. The term is used in this study primarily to distinguish infrastructure (DLT/blockchain) from the financial instruments (crypto-assets) that operate on it.
Immutability	The property of blockchain records that makes them practically irreversible once confirmed, data written to the chain cannot be altered without redoing all subsequent computational work. Immutability underpins blockchain's value as an audit trail but also creates challenges for data correction, consumer redress, and POPIA compliance.
Non-Fungible Token (NFT)	A unique, non-interchangeable cryptographic token recorded on a blockchain that represents ownership of a specific asset, whether digital or physical. In this study, NFTs are discussed as a potential mechanism for digital identity verification, enabling tamper-proof, portable KYC credentials.
Proof of Concept (PoC)	A preliminary test or demonstration of a technology's feasibility in a controlled environment. South Africa's Project Khokha (2018) was a PoC for blockchain-based wholesale interbank settlement, demonstrating the technical feasibility of DLT in the South African payment context.
Pseudonymity	The condition in which cryptocurrency transactions are associated with cryptographic addresses rather than verified real-world identities. Pseudonymity is distinct from anonymity: transactions are publicly visible on the ledger, but linking addresses to identities requires additional analytical tools or KYC enforcement at the CASP level.
Self-Sovereign Identity (SSI)	A model of digital identity in which individuals control and share their own verified credentials without depending on a central authority. SSI systems are discussed in this study as a mechanism for enabling KYC compliance while preserving user privacy and supporting financial inclusion for populations lacking traditional identity documents.
Smart Contract	A self-executing programme stored on a blockchain that automatically enforces the terms of an agreement when predefined conditions are met. Smart contracts are central to this study's embedded compliance argument: they can automate KYC/AML checks, tax withholding, exchange control reporting, and transaction threshold enforcement without human intervention.
Stablecoin	A crypto-asset designed to maintain a stable value, typically by pegging to a fiat currency (e.g., USD) or a basket of assets. Stablecoins are particularly relevant to the remittance use case because their price stability makes them more practical for value transfer than volatile cryptocurrencies such as Bitcoin.

TERM / ACRONYM	DEFINITION
Tokenisation	The process of representing a real-world asset or right as a digital token on a blockchain. A tokenised digital asset is a digital representation of a real-world asset recorded on a distributed ledger. Tokenisation is discussed in this study in the context of wholesale settlement and stablecoin-based cross-border transfers.
Virtual Asset Service Provider (VASP)	The FATF's equivalent of South Africa's CASP — an entity that provides exchange, transfer, custody, or other services relating to virtual assets. FATF Recommendation 15 requires jurisdictions to regulate and supervise VASPs for AML/CFT purposes, which South Africa has operationalised through FICA amendments designating CASPs as accountable institutions.
Wallet	A software or hardware tool that stores the cryptographic keys needed to access and transact with cryptocurrency. Wallets may be custodial (managed by a CASP, who holds the private keys) or non-custodial / self-hosted (managed by the user). Non-custodial wallets create regulatory blind spots because transactions may occur outside CASP-level AML/KYC oversight.
Zero-Knowledge Proof (ZKP)	A cryptographic technique that allows one party to prove to another that a statement is true without revealing any information beyond the truth of the statement. ZKPs are discussed in this study as a privacy-preserving compliance tool, enabling a user to demonstrate AML/KYC compliance without exposing personal data, and as a tension point between FATF Travel Rule requirements and POPIA privacy obligations.

DECLARATION OF ORIGINALITY

I declare that this report is my own, unaided work. It is submitted in fulfilment of the requirements of the degree of Master of Arts in the field of Interdisciplinary Digital Knowledge Economy Studies at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination at any other University.

Craig Rolando Meyer

A handwritten signature in black ink, appearing to read 'Craig Rolando Meyer', enclosed within a large, loopy, handwritten oval or loop.

Signature

Date: 16 March 2026

ACKNOWLEDGEMENTS

The completion of this dissertation was not a solitary intellectual exercise, but a deeply human journey, marked by perseverance, vulnerability, growth, and an unwavering belief in the transformative power of knowledge. What began as an academic inquiry became, over time, a personal testament to resilience.

I extend my profound gratitude to Dr Lucienne Abrahams and Dr Kiru Pillay, who served not merely as supervisors, but as steady intellectual anchors during one of the most trying periods of this journey. Your guidance was rigorous yet compassionate; your expectations, demanding yet affirming. At moments when the weight of scholarship felt overwhelming, you reminded me that difficulty is often the crucible of clarity. Your mentorship sharpened my thinking, strengthened my resolve, and restored my confidence when it faltered. I remain deeply indebted to you both.

To my partner, Leena Singh, your support was unwavering and absolute. You carried more than your share of the emotional burden so that I could continue to write, analyse, and reflect. You believed in the work even when I doubted it. Your patience in the long evenings, your encouragement in moments of fatigue, and your quiet strength in the background of every chapter made this achievement possible. This dissertation is as much yours as it is mine.

To my children, thank you for your encouragement, your pride, and your understanding when time and attention were unevenly distributed. You reminded me, often without knowing it, why perseverance matters. Your belief in me became a responsibility I was determined to honour. May this work stand as a demonstration that sustained effort, even through adversity, yields meaning and that higher power always guides us.

This dissertation represents more than research. It represents forward motion. It affirms that innovation is not merely technological but human, built on relationships, courage, and the refusal to stand still.

Sic Parvis Magna.

Table of Contents

ABSTRACT.....	2
GLOSSARY	4
DECLARATION OF ORIGINALITY	7
ACKNOWLEDGEMENTS	8
LIST OF FIGURES.....	16
LIST OF TABLES	18
CHAPTER 1.....	16
1.1 Chapter Overview.....	19
1.2 Cross-border and remittance transfer fees	21
1.3 Cryptocurrency as an alternative cross-border payment rails.....	22
1.4 South African regulatory environment for cryptocurrency	23
1.5 The Nature of Blockchain Technology	24
1.6 Classification of Cryptocurrency in South Africa	25
1.7 Research Problem Statement	27
1.8 The 3 Dimensions	27
1.8.1 Gap and need for regulations	31
1.8.2 Problem.....	34
1.8.3 Objective	34
1.9 Research Purpose Statement.....	35
1.10 Research Questions	35
1.11 Background	36
1.12 Key characteristics of the cross-border transfer (remittance) process.....	39
1.13 Key issues in legislation and regulation: Legislative compliance	39
1.14 Delimitations.....	42
1.15 Dissertation Structure and Chapter Outline.....	41
CHAPTER 2	46
2.1 Chapter Overview.....	46
2.2 Blockchain, Crypto-Assets, Cryptocurrency Networks	47

2.3	Systematic Literature Review Methodology.....	49
2.4	Regulatory Theory and Frameworks for Crypto-Asset Governance.....	55
2.4.1	Foundational Theories of Financial Regulation: Public Interest Theory.....	55
2.4.2	Responsive Regulation Theory.....	56
2.4.3	Principles-Based Versus Rules-Based Regulatory Approaches.....	58
2.4.4	Risk-Based Regulatory Approaches.....	59
2.4.5	International Regulatory Coordination.....	60
2.4.6	Institutional Economics and Regulatory Path Dependence.....	61
2.4.7	Technological Neutrality and Activity-Based Regulation.....	62
2.4.8	Critical Synthesis: Regulatory Theory.....	63
2.4.9	Caveat emptor on cryptocurrency.....	65
2.5	Application of innovation theory.....	67
2.6	Application of socio-technical theory to digital solutions.....	71
2.7	Benefits of Blockchain in cross-border transfer fee reduction.....	74
2.8	Gaps in existing literature and contribution of study.....	77
CHAPTER 3		80
3.1	Philosophical assumptions underpinning the study.....	80
3.2	Research Approach.....	82
3.3	Research Design.....	83
3.3.1	Reserach methods.....	83
3.3.2	Data Collection Method.....	84
3.3.3	Population and Sample.....	85
3.4	Interview protocol, guides the semi-structured interviews.....	86
3.5	Data Collection.....	87
3.6	Ethical Considerations.....	87
3.7	Research Data Analysis.....	88
3.8	Researcher Positionality and Reflexivity.....	89
3.9	Limitations and challenges of the study.....	90
3.9.1	Limited Scope of the Study.....	90
3.9.2	Qualitative Methodology and Subjectivity.....	90
3.9.3	Limited Number of Interview Respondents.....	91
3.9.4	Evolving Nature of Cryptocurrency Technology and Regulation.....	91

3.9.5	Lack of Quantitative Data.....	91
3.9.6	Complexity of Cross-Border Payment Systems	92
3.9.7	Technological and Regulatory Lag.....	92
3.9.8	Ethical and Privacy Concerns	92
3.9.9	Lack of Comparison with Traditional Systems	93
3.9.10	Technological Rapid Evolution.....	93
3.10	Quality Assurance	93
3.10.1	Credibility	93
3.10.2	Transferability	94
3.10.3	Dependability	94
3.10.4	Confirmability	94
3.10.5	Researcher Bias.....	94
4.1	Chapter Overview	97
4.2	Classification of Cryptocurrency in South Africa	99
4.3	Primary Legislative Framework.....	106
4.4	Exchange Control Regulations	108
4.5	National Payment System Act	110
4.6	Financial Intelligence Centre Act.....	111
4.7	Financial Sector Regulation Act	114
4.8	Currency and Exchanges Manual for Authorised Dealers	116
4.9	Supporting Guidelines Relevant to Cross-Border Transfers	118
4.9.1	Currency and Exchanges Manual for ADLA.....	118
4.9.2	SARB Position Paper on Virtual Currencies.....	120
4.9.3	IFWG Position Paper on Crypto Assets	122
4.9.4	Draft Directive in Respect of Specific Payment Activities.....	124
4.9.5	Guidance Note 104A on International Funds Transfer Reports (Draft, FIC).....	128
4.9.6	SARS Crypto Assets & Tax Guidance.....	130
4.10	Regulations Specific to Blockchain and Crypto Assets	132
4.10.1	Financial Sector Regulation Act, 2017 (Act No. 9 of 2017).....	132
4.10.2	Amendments to FICA Schedules (2022)	134
4.10.3	Visual Mapping of Regulatory Framework.....	136
4.11	Key Observations and Regulatory Gaps	139
4.11.1	Cross-Border Transfers and Remittances	139

4.11.2	Blockchain and Crypto Assets	140
4.11.3	Regulatory Challenges.....	140
4.11.4	Future Developments	140
4.12	Empirical Research Findings: Industry Perspectives on Cryptocurrency	142
4.13	Dimension 1: Regulatory and Compliance Framework Analysis.....	148
4.13.1	Current Regulatory Inadequacy and Institutional Resistance.....	148
4.13.2	Real-Time Compliance Enhancement Opportunities.....	149
4.13.3	Anti-Money Laundering and Know Your Customer Enhancement	150
4.13.4	Digital Identity Solutions and Smart Contract Implementation	150
4.13.5	Integration Challenges and System Incompatibility.....	151
4.13.6	Implications and Reform Requirements	152
4.14	Dimension 2: Technological and Compliance Enhancements.....	153
4.14.1	Enhanced Transaction Monitoring and Auditability	153
4.14.2	Combating Financial Crime Through Blockchain Transparency	154
4.14.3	Self-Sovereign Identities and NFT-Based Verification.....	155
4.14.4	Smart Contracts and Automated Regulatory Enforcement.....	155
4.14.5	Managing Blockchain-Specific Compliance Risks.....	156
4.15	Dimension 3: Socio-Economic and Global Implications	157
4.15.1	Financial Inclusion Through Cost Reduction	157
4.15.2	Digital Identity Innovation and Self-Sovereign Solutions.....	158
4.15.3	Cross-Border Collaboration and Regulatory Harmonisation.....	159
4.15.4	Learning from Global Best Practices	160
4.15.5	Future Outlook and Continental Leadership.....	160
4.15.6	Balancing Innovation with Security and Regulatory Integrity	161
4.16	Summary	162
CHAPTER 5		165
5.1	Regulatory Architecture Gaps	168
5.2	Definitional and Classification Inconsistencies.....	169
5.3	Cross-Border Transaction Oversight Gaps.....	171
5.4	Exchange Control Enforcement Limitations.....	175
5.5	Anti-Money Laundering and Know Your Customer Compliance Gaps	176
5.6	Identity Verification and Transaction Monitoring Gaps.....	178
5.7	Innovation and Implementation Gaps	179

5.8	Institutional Readiness Gap.....	181
5.9	Technical Integration and Standards Gaps.....	182
5.10	Real-Time Monitoring and Compliance Integration	183
5.11	International Coordination and Harmonisation Gaps	184
5.12	Jurisdictional Arbitrage Prevention.....	185
5.13	Consumer Protection and Education Gaps	186
5.14	Recommendations for Addressing Identified Gaps	188
5.15	Medium-Term Structural Changes	188
5.16	Long-Term Transformation.....	189
5.17	Synthesis of Regulatory Framework and Research Findings.....	190
5.17.1	Alignment Between Regulatory Intent and Industry Needs.....	190
5.17.2	Critical Gaps and Reform Priorities	191
5.17.3	Recommendations for Regulatory Reform.....	192
5.17.4	Strategic Imperatives for South Africa	194
CHAPTER 6		200
6.1	Introduction.....	202
6.2	Theoretical Foundations.....	202
6.3	Design Science Research Methodology	203
6.4	The 5-Echelon Knowledge Model.....	205
6.4.1	Model Architecture and Hierarchical Structure.....	205
6.5	Echelon 1: Foundational Policy & Legislative Clarity	207
6.5.1	Purpose and Strategic Importance	207
6.5.2	Gaps Addressed.....	208
6.5.3	Key Components and Implementation Strategies.....	209
6.5.4	Root Causes and Impact Mitigation	210
6.5.5	Actionable Steps and Implementation Timeline	212
6.5.6	International Alignment and Comparative Analysis	213
6.6	Echelon 2: Oversight & Compliance Mechanisms.....	215
6.6.1	Purpose and Strategic Importance.....	215
6.6.2	Gaps Addressed.....	216
6.6.3	Key Components and Implementation Strategies	217
6.6.4	Root Causes and Structural Adaptations	219

6.6.6	Actionable Steps and Implementation Timeline	221
6.6.7	International Coordination and FATF Compliance.....	222
6.7.8	Theoretical Foundations.....	223
6.8	Echelon 3: Technical & Operational Integration.....	224
6.8.1	Purpose and Strategic Importance.....	224
6.8.2	Gaps Addressed.....	225
6.8.3	Key Components and Implementation Strategies	226
	Implications for South Africa	231
6.8.4	Root Causes and Technical Solutions	232
6.8.5	Impacts and Benefits of Technical Integration.....	234
6.8.6	Actionable Steps and Implementation Timeline	235
6.8.7	Regulatory Sandboxes and Controlled Innovation Testing	239
6.8.8	Addressing the Digital Divide and Capacity Building	241
6.8.9	Theoretical Foundations of Technical Integration.....	242
6.9	Echelon 4: Coordination & Collaboration	243
6.9.1	Purpose and Strategic Importance.....	243
6.9.2	Gaps Addressed.....	244
6.9.3	Key Components and Implementation Strategies.....	246
6.9.4	Collaboration with Fintechs and Traditional Institutions.....	249
6.9.5	Fostering Mindset Shifts from Gatekeeping to Facilitation	250
6.9.6	Addressing Global Standards Misalignment.....	251
6.9.7	Case Study: EU MiCA and the Challenges of Unilateral Comprehensive Regulation .	252
6.9.8	Actionable Steps and Implementation Timeline	254
6.9.9	Theoretical Foundations of Coordination and Collaboration	254
6.10	Echelon 5: Adaptive & User-Centric Mechanisms.....	256
6.10.1	Purpose and Strategic Importance.....	256
6.10.2	Gaps Addressed.....	257
6.10.3	Key Components and Implementation Strategies	259
6.10.4	Case Studies: Singapore's and EU's User-Centric Approaches	264
6.10.5	Consumer Protection Mechanisms and Dispute Resolution.....	267
6.10.6	Promoting Financial Inclusion through Blockchain	270
6.10.7	Actionable Steps and Implementation Timeline.....	274
6.10.8	Reducing Information Asymmetry and Adoption Barriers	275
6.10.9	Long-term Sustainability and Regulatory Evolution.....	276
6.11	Summary: Toward a Balanced, Adaptive, and Inclusive	277
6.12	Theoretical Contributions and Scholarly Significance	280

6.16	Future Research Agenda.....	292
6.17	Concluding Reflections: Toward Responsible Innovation in the Digital Age	294
CHAPTER 7		298
CONCLUSION		298
7.1	Key Findings: Insights from the Regulatory Environment	298
7.1.1	Regulatory Uncertainty and Fragmentation	298
7.1.2	Blockchain's Potential for Innovation and Transformation	300
7.1.3	Regulatory Concerns: AML, KYC, and Consumer Protection	301
7.1.4	Need for International Collaboration	303
7.1.5	Mitigations for Regulatory Challenges	303
7.1.6	Establishment of Regulatory Sandboxes	304
7.1.7	Clearer Guidelines and Policy Frameworks.....	304
7.1.8	Public-Private Partnerships	305
7.1.9	Harmonisation of International Regulations.....	305
7.1.10	Contribution to the Field	306
7.1.11	Conclusion and Recommendations for Future Research.....	306
7.2	CONSOLIDATED RESPONSES TO THE RESEARCH SUB-QUESTIONS.....	311
7.2.1	Sub-Question 1: Balancing Innovation with Compliance	311
7.2.2	Sub-Question 2: Financial Inclusion.....	313
7.2.3	Sub-Question 3: Technically Embedding KYC/AML Compliance	314
7.3	LIMITATIONS OF THE STUDY	316
7.4	DIFFERENTIATED RECOMMENDATIONS BY STAKEHOLDER GROUP	318
7.4.1	Recommendations for Policymakers and the National Treasury	318
7.4.2	Recommendations for the SARB and the FSCA.....	319
7.4.3	Recommendations for the Crypto-Asset Industry and CASPs	319
7.4.4	Recommendations for Future Researchers	320
7.5	CONCLUDING REMARKS.....	321
REFERENCES.....		323
APPENDIX A.....		344
APPENDIX B.....		346
APPENDIX C.....		348
APPENDIX D.....		349

LIST OF FIGURES

FIGURE 1. 3 DIMENSIONS OF CRYPTOCURRENCY REGULATION (RESEARCHER)	31
FIGURE 2. BANCO BILBAO VIZCAYA ARGENTARIA RESEARCH (SOURCE).....	33
FIGURE 3. FLOWCHART DEPICTING SOCIO-TECHNICAL ANALYSIS OF CROSS-BORDER TRANSFERS	34
FIGURE 4. KEY CHARACTERISTICS OF THE GLOBAL REMITTANCE PROCESS WORLD BANK (2007)	39
FIGURE 5. THE DISRUPTIVE FEATURES OF BLOCKCHAIN BBVA RESEARCH (SOURCE).....	48
FIGURE 6. THE SPIDER RESEARCH TOOL, COOK ET AL 2012	50
FIGURE 7. THE MULTITUDE OF REGULATORY THEORIES GOVERNING FINTECH IN SOUTH AFRICA	64
FIGURE 8. DIAGRAM DEPICTING THE INTERLINKING ASPECTS OF SOCIO-TECHNICAL THEORY.....	72
FIGURE 9. CHARACTERISTICS OF QUALITATIVE RESEARCH BY BUNMI MALAU-ADULI AND FAITH ALELE	83
FIGURE 10. GRAPHIC INDICATING THE LINKAGE BETWEEN THE CURRENCY AND EXCHANGES ACT.....	107
FIGURE 11. GRAPHIC INDICATING THE LINKAGE BETWEEN THE EXCHANGE CONTROL REGULATIONS	109
FIGURE 12. GRAPHIC INDICATING THE LINKAGE BETWEEN THE NATIONAL PAYMENT SYSTEM ACT	110
FIGURE 13. GRAPHIC INDICATING THE LINKAGE BETWEEN THE FINANCIAL INTELLIGENCE CENTRE ACT	113
FIGURE 14. GRAPHIC INDICATING THE LINKAGE BETWEEN FINANCIAL SECTOR REGULATION ACT, 2017.....	115
FIGURE 15. GRAPHIC INDICATING THE IMPACT OF THE CURRENCY AND EXCHANGES MANUAL	118
FIGURE 16. GRAPHIC INDICATING THE LINKAGE BETWEEN CURRENCY AND EXCHANGES MANUAL	119
FIGURE 17. GRAPHIC INDICATING THE LINKAGE BETWEEN SARB POSITION PAPER.....	121
FIGURE 18. GRAPHIC INDICATING THE PHASED APPROACH OF THE IFWG POSITION PAPER	123
FIGURE 19. GRAPHIC INDICATING THE PHASED APPROACH OF THE IMPACT	126
FIGURE 20. GRAPHIC INDICATING THE LINKAGE BETWEEN THE GUIDANCE NOTE 104A	129
FIGURE 21. GRAPHIC INDICATING THE IMPACT OF THE SARS CRYPTO ASSETS & TAX GUIDANCE	132
FIGURE 22. GRAPHIC INDICATING THE LINKAGE BETWEEN THE FINANCIAL SECTOR REGULATION ACT	134
FIGURE 23. GRAPHIC INDICATING THE LINKAGE BETWEEN THE AMENDMENTS TO FICA SCHEDULES.....	136
FIGURE 24. (LEGISLATION): DEMONSTRATES STATUTORY FOUNDATIONS.....	136
FIGURE 25. (SUPPORTING GUIDELINES): HIGHLIGHTS OPERATIONAL GUIDANCE	137
FIGURE 26. REGULATION): MAPS ENFORCEMENT INSTRUMENTS, INCLUDING EXCHANGE CONTROL.	138
FIGURE 27. THIS DIAGRAM HIGHLIGHTS THE 3 DIMENSIONS OF INQUIRY (RESEARCHER)	143
FIGURE 28. ATLAS.TI WORD CLOUD DERIVED FROM INTERVIEWS	144
FIGURE 29. THEMATIC ANALYSIS PROCESS (RESEARCHER)	144
FIGURE 30. ATLAS.TI GRAPHIC REPRESENTATION OF CODE GROUPS AND FREQUENCY	145
FIGURE 31. ATLAS.TI GRAPHIC REPRESENTATION OF KEY CODES AND FREQUENCY	146
FIGURE 32. ATLAS.TI GRAPHIC REPRESENTATION OF KEY CONCEPTS AND FREQUENCY USE IN INTERVIEWS ..	147
FIGURE 33. GRAPHIC OUTLINING LINKAGE MAPPING BETWEEN CHAPTER 4 GAP TYPES	165
FIGURE 34. TABULAR REPRESENTATION OF SOUTH AFRICAN GAP ANALYSIS FRAMEWORK (RESEARCHER)..	167
FIGURE 35. GRAPHIC OF THE REGULATORY ARCHITECTURE GAPS (RESEARCHER)	169
FIGURE 36. GRAPHIC OF THE DEFINITIONAL AND CLASSIFICATION INCONSISTENCIES GAPS (RESEARCHER).	170
FIGURE 37. GRAPHIC OF THE THRESHOLD AND REPORTING MECHANISM INADEQUACIES GAPS.....	175

FIGURE 38. GRAPHIC OF THE EXCHANGE CONTROL ENFORCEMENT LIMITATIONS (RESEARCHER).....	176
FIGURE 39. GRAPHIC OF THE AML FRAMEWORK STRUCTURAL LIMITATIONS (RESEARCHER).....	178
FIGURE 40. GRAPHIC OF THE IDENTITY VERIFICATION AND TRANSACTION MONITORING GAPS.....	179
FIGURE 41. GRAPHIC OF THE INNOVATION AND IMPLEMENTATION GAPS (RESEARCHER).....	180
FIGURE 42. GRAPHIC OF THE INSTITUTIONAL READINESS GAP (RESEARCHER)	182
FIGURE 43. GRAPHIC OF THE TECHNICAL INTEGRATION AND STANDARDS GAPS (RESEARCHER).....	183
FIGURE 44. GRAPHIC OF THE REAL-TIME MONITORING AND COMPLIANCE INTEGRATION GAPS.....	184
FIGURE 45. GRAPHIC OF THE INTERNATIONAL COORDINATION AND HARMONISATION GAPS (RESEARCHER) .	185
FIGURE 46. GRAPHIC OF THE JURISDICTIONAL ARBITRAGE PREVENTION (RESEARCHER).....	186
FIGURE 47. GRAPHIC OF THE CONSUMER PROTECTION AND EDUCATION GAPS (RESEARCHER).....	187
FIGURE 48. GRAPHIC OUTLINING RECOMMENDATIONS TO ADDRESS IDENTIFIED GAPS (RESEARCHER).....	189
FIGURE 49. GRAPHIC OUTLINING CRITICAL GAPS AND REFORM PRIORITIES (RESEARCHER)	192
FIGURE 50. GRAPHIC OUTLINING RECOMMENDATIONS FOR REGULATORY REFORM (RESEARCHER)	195
FIGURE 51. GRAPHIC OUTLINING RECOMMENDATIONS TO BRIDGE GAPS IN CRYPTOCURRENCY	196
FIGURE 52. GRAPHIC OUTLINING THE GAP ANALYSIS THROUGH THE LENS OF THE 3 DIMENSIONS	198
FIGURE 53. GRAPHIC OUTLINING LINKAGE MAPPING BETWEEN KNOWLEDGE MODEL AND GAPS IDENTIFIED ..	201
FIGURE 54. GRAPHIC OUTLINING THE PYRAMID OF ECHELONS (RESEARCHER).....	206
FIGURE 55. GRAPHIC OUTLINING ECHELON 1 (RESEARCHER).....	207
FIGURE 56. GRAPHIC OUTLINING ECHELON 2 (RESEARCHER).....	215
FIGURE 57. GRAPHIC OUTLINING ECHELON 3 (RESEARCHER).....	224
FIGURE 58. GRAPHIC OUTLINING COMPARISONS BETWEEN SINGAPORE (PROJECT UBIN)	231
FIGURE 59. GRAPHIC OUTLINING COMPARISONS BETWEEN EU (MiCA) AND SOUTH AFRICA	239
FIGURE 60. GRAPHIC OUTLINING ECHELON 4 (RESEARCHER).....	243
FIGURE 61. GRAPHIC OUTLINING ECHELON 5 (RESEARCHER).....	256
FIGURE 62. GRAPHIC OUTLINING CURRENT ARENA REGARDING BLOCKCHAIN REMITTANCES	272
FIGURE 63. GRAPHIC OUTLINING THE 5-ECHELON KNOWLEDGE MODEL	296
FIGURE 64. GRAPHIC INDICATING CRYPTOCURRENCY REGULATORY UNCERTAINTY IN SOUTH AFRICA.....	299
FIGURE 65. GRAPHIC OUTLINING MITIGATIONS FOR REGULATORY CHALLENGES (RESEARCHER)	303
FIGURE 66. GRAPHIC OUTLINING THE WAY FORWARD FOR CRYPTOCURRENCY (RESEARCHER).....	307
FIGURE 67. GRAPHIC OUTLINING THE KEY FINDINGS AND MITIGATION STRATEGIES	310

LIST OF TABLES

TABLE 1. LIST OF REGULATIONS AND POLICIES RELATING TO FISCAL TRANSFERS	106
TABLE 2. THIS TABLE SUMMARISES THE POTENTIAL DRIVERS AND BARRIERS TO CRYPTOCURRENCY.	142
TABLE 3. TABULAR REPRESENTATION OF THE KEY CODES AND THEIR FREQUENCY	148
TABLE 4. CONSOLIDATED GAP TABLE	188

CHAPTER 1

BETWEEN DISRUPTION AND COMPLIANCE: FRAMING SOUTH AFRICA'S CRYPTOCURRENCY CHALLENGE

Dissertation Overview

This dissertation investigates the regulatory challenges and opportunities associated with cryptocurrency-driven cross-border transfers in South Africa. Cryptocurrency has emerged as a disruptive force in global finance, offering the potential to reduce remittance costs, accelerate transaction speeds, and enhance financial inclusion. These benefits are especially relevant in developing economies, where traditional cross-border payment systems remain constrained by high fees, lengthy processing times and complex intermediary networks. However, the adoption of cryptocurrency introduces significant regulatory concerns, including compliance with Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements, consumer protection, and systemic stability.

This study emphasises the need for a balanced regulatory framework that fosters innovation while reducing the risks associated with illegal financial transactions and market volatility. It explores the feasibility of a hybrid model that combines the decentralised efficiencies of cryptocurrency with centralised oversight mechanisms, ensuring both operational resilience and regulatory compliance. By analysing existing financial policies, institutional roles, and global best practices, this research aims to demonstrate how adaptive regulation can unlock cryptocurrency's potential for cost-effective remittances and inclusive financial systems.

By drawing on academic literature and industry reports, the dissertation argues that well-designed regulatory frameworks are essential to harness the transformative capabilities of cryptocurrency. This analysis contributes to ongoing debates on digital finance governance and positions South Africa within the broader global discourse on cryptocurrency regulation and cross-border payment innovation. Although blockchain technology underpins cryptocurrency, this study does not seek to regulate blockchain as a technology. Technologies themselves are not subject to financial legislation; rather, it is the financial instruments, services, and intermediaries built upon such technologies

that fall within regulatory mandates (Zetzsche et al. 2018). Therefore, the analytical focus of this dissertation shifts from blockchain infrastructure to cryptocurrency and crypto-asset service providers (CASPs) as the legally governable units of cross-border financial activity. This distinction aligns with contemporary regulatory approaches adopted by the Financial Action Task Force (FATF), the Financial Stability Board (FSB), and South Africa's Financial Sector Conduct Authority (FSCA), all of which regulate crypto-assets, not blockchain protocols.

1.1 Chapter Overview

The exorbitant cost of cross-border transfer fees in Africa continues to burden individuals and families who rely on these funds for their livelihoods. Despite the significant contributions these financial transfers make to local economies, the high fees imposed by financial institutions and money transfer operators have become a major obstacle. These fees can range from 8% to 11% of the principal amount being transferred or even more, resulting in a substantial reduction in the actual amount received by recipients (World Bank, 2021). This places an undue burden on the already limited resources of individuals who depend on these financial transfers for basic needs such as education, healthcare, and daily expenses. Financial regulations implemented by banks and money transfer organisations play a role in perpetuating these inordinately high fees, as they profit from the cross-border transfer process. The lack of competition, limited transparency, and complex regulatory frameworks contribute to this issue, leaving many Africans paying a significant portion of their hard-earned money in fees, hindering economic growth and development. Addressing this challenge requires collaborative efforts between governments, financial institutions, and fintech innovators to create more accessible and affordable cross-border transfer channels, fostering greater financial inclusion and empowering individuals and families across the continent (World Bank, 2021). Previously constrained by low banking penetration, Africa is now redefining financial inclusion, through the growth of mobile money and fintech innovation. This shift is further propelled by the increased internet and mobile phone penetration, the rise of e-commerce platforms and youthful tech-savvy population (Sabilinka, 2025).

A cross-border transfer is a broad term that encompasses any financial transaction that involves moving money from one country to another, including business transactions,

investments, or personal transfers. It does not specify the purpose or the sender and recipient. A remittance is a specific type of cross-border transfer. Remittances refer to the transfer of money by foreign workers, often immigrants, to their home country to support their families or for other personal purposes. Remittances are usually characterised by the sender's intention to provide financial support to relatives or loved ones in their home country. While remittances fall under the category of cross-border transfers, not all cross-border transfers are remittances. Money sent home by migrants competes with international aid as one of the largest financial inflows to developing countries, and is estimated at \$600 billion annually (World Bank Group, 2019) with \$40 billion being transferred to Sub-Saharan African countries in 2018. A recent World Bank report estimated the Africa received \$95 billion in 2024. Remittances increase disposable income for households and have potential multiplier effects. In addition to being an important income source for the households, remittances spent on consumption may also contribute to development and growth by increasing the demand for goods and services, while stimulating production and employment (Durand et al., 1996). Since 2010, the international migrant population numbers from Africa have grown significantly. Eight in ten of the fastest-growing migrant populations are from sub-Saharan African nations, according to a Pew Research Centre analysis of the latest United Nations data on the number of emigrants, or people living outside their country of birth (Adegoke, 2018).

It is crucial to remember that remittances are a vital lifeline for many families and communities in Africa, providing crucial financial support for education, healthcare, and basic needs. However, the cost of sending money to Africa remains disproportionately high compared to other regions. This is partly due to the complex web of regulations and compliance requirements imposed by financial institutions to mitigate risks associated with money laundering, terrorism financing, and fraud. These regulations serve an important purpose in safeguarding the financial system. However, they often result in increased costs for cross-border money transfer providers, who pass on these expenses to consumers in the form of higher fees. Banks, in particular, face rigorous compliance obligations that necessitate extensive due diligence, transaction monitoring, and reporting, all of which add significant operational costs. Consequently, these expenses are transferred to individuals sending money to Africa, disproportionately affecting the most vulnerable populations who heavily rely on remittances.

In addition to regulatory compliance costs, the dominance of a few major players in the cross-border transfer market further contributes to these persistently high fees. These companies have established extensive networks and infrastructure, which allows them to charge significant fees for their services. Due to the market dominance held by these financial services providers, consumers often have limited alternatives and are forced to pay these inordinately high fees. Financial regulations which were intended to maintain stability and combat illicit financial activities have inadvertently contributed to the steep cost of cross-border transfer fees. Banks and money transfer organisations are required to comply with stringent anti-money laundering and know-your-customer regulations. While these regulations serve important purposes, their implementation often adds operational costs that are ultimately passed on to remittance senders and recipients. The lack of competition and transparency within the cross-border payments industry exacerbates the issue. Many African countries suffer from limited access to affordable and efficient financial services, creating a captive market where consumers have limited options for sending and receiving money. This lack of competition reduces the incentive for remittance providers to lower their fees, leading to a perpetuation of the status quo.

1.2 Cross-border and remittance transfer fees

The global economy increasingly relies on efficient cross-border payment systems to facilitate international trade, remittances, and financial services. However, the current infrastructure for international money transfers remains fragmented, costly, and inefficient, creating barriers to economic participation and growth (World Bank, 2022). Traditional cross-border payment systems, built on decades-old correspondent banking networks, involve multiple intermediaries, lengthy settlement periods, and substantial costs that disproportionately affect developing economies and individual consumers (Pazarbasioglu et al., 2020).

Africans across the world are charged excessive fees to transfer remittances to their home countries, with a World Bank report (2019) showing that the cost of sending remittances to Sub-Saharan Africa continues to be far higher than any other region in the world. On average, transferring \$200 to and from a country in the region cost almost \$19 in the first quarter of 2018 (World Bank Group, 2019). The people in most need in

sub-Saharan Africa is deprived of much-needed financial aid because of the exorbitantly high remittance fees levied on the African diaspora. (World Bank Group, 2019). The inordinately high fees charged on the African diaspora reduce recipient households from increased spending on essential goods and services, investing in healthcare and education, as well as curtailing opportunities for recipients to build financial asset bases and limit access to financial services and investment opportunities. This inevitably leads to a vicious circle of financial exclusion exacerbated by rampant remittance fees which diminish the financial and socio-economic impact remittances could have on recipients (World Bank Group, 2019).

1.3 Cryptocurrency as an alternative cross-border payment rails

Although blockchain provides the foundation upon which distributed ledger infrastructure enables cryptocurrency, it is crypto-assets and their associated service ecosystems that function as payment and settlement mechanisms in cross-border transfers. Cryptocurrency such as Bitcoin, Ethereum-based stablecoins, and other tokenised digital assets operate as value transfer systems. A tokenized digital asset is a digital representation of a real-world asset (like real estate, stocks, or art) or a digital-native asset recorded on a blockchain (Chainalysis, 2024). This reduces reliance on correspondent banking chains. This is achieved by enabling peer-to-peer or wallet-based settlement. The potential to reduce remittance costs therefore does not reside in blockchain as an abstract infrastructural concept, but in the concrete transaction models through which crypto-assets operate, such as stablecoin-based settlement, exchange-based liquidity pools, and direct wallet-to-wallet transfers.

A report by Santander InnoVentures, a fintech investor, estimates that crypto-asset payment rails could reduce intermediation layers and potentially could save banks up to \$20 billion a year in cross-border settlement costs (Santander InnoVentures, Oliver Wyman & Anthemis Group. 2015). The efficiency of blockchain technology allows for faster settlement of cross-border transfers. This speed can reduce costs associated with delayed transfers, including liquidity costs. According to a report by Accenture, blockchain could reduce banks' infrastructure costs for cross-border payments by 30% (Accenture Report). The elimination of intermediaries and automation of processes can reduce transaction fees. Cryptocurrency cross-border transfers can bypass costly

correspondent banking networks, resulting in lower fees for both businesses and individuals (Accenture & McLagan, 2017). A case study involving IBM and Stellar indicates that blockchain-based cross-border payment systems can significantly reduce transaction costs, potentially by up to 40%, by removing intermediaries and enabling near-instant settlement.

The transparency and immutability of blockchain ledgers can significantly reduce reconciliation costs and the need for manual intervention in the event of disputes or errors. This reduction in reconciliation expenses can lead to cost savings. Blockchain enables the use of smart contracts, which can automate various aspects of cross-border transactions. Automation can reduce operational costs by eliminating the need for manual intervention and associated labour costs. The security features of blockchain technology can potentially reduce the risk of fraud and cyberattacks, thereby cutting down costs related to security measures, investigations, and fraud prevention. While these potential cost-saving benefits are promising, it's essential to consider that the actual cost reductions can vary depending on the specific blockchain solution, regulatory compliance, and the scale of adoption. As a result, blockchain solutions have gained attention as a viable alternative to traditional cross-border financial transfers due to their potential to reduce costs significantly.

Blockchain solutions address inefficiencies, reduce the number of intermediaries, provide transparency, and streamline the settlement process. While there are challenges to overcome and regulatory considerations, the cost-saving potential is a compelling reason for the growing interest and adoption of these technologies in the cross-border financial transfer sector. The blockchain industry continues to evolve, and more data is needed to assess the long-term impact on cross-border transfer costs accurately. It is important to note that blockchain is a general-purpose infrastructure technology, whereas cryptocurrency constitute economically transactable digital assets that fall within the regulatory and legal domain of financial governance.

1.4 South African regulatory environment for cryptocurrency

Blockchain and cryptocurrency technologies represent a transformative shift in global financial systems. Cryptocurrency, defined as digital or virtual forms of currency

secured by cryptographic algorithms, are decentralised and operate on blockchain technology. Blockchain is a distributed ledger system that records transactions across a peer-to-peer network of computers. This system provides decentralised security, transparency, and immutability, thereby challenging traditional financial infrastructures (Nakamoto, 2008; Tapscott & Tapscott, 2016). In the South African context, regulators have increasingly turned their attention to cryptocurrency and blockchain-based innovations due to their rapid proliferation and implications for financial stability, monetary policy, and consumer protection. South Africa's approach to blockchain and cryptocurrency regulation is evolving, reflecting broader global trends while addressing local policy and infrastructural concerns (Botha, 2020). This technology also promises enhanced transparency, immutability, and decentralisation, characteristics that challenge the paradigms of traditional centralised financial infrastructures (Tapscott & Tapscott, 2016). As global interest in blockchain and crypto-assets continue to grow, regulatory frameworks worldwide have struggled to adapt, often caught between promoting innovation and protecting financial integrity.

In South Africa, the regulatory discourse surrounding cryptocurrency and blockchain innovations has evolved significantly over the past decade. With increasing use of digital assets for investment, remittances, and payment solutions, South African regulators have been compelled to establish a more formal framework for governance. This research paper explores the regulatory landscape governing cryptocurrency in South Africa, evaluating existing classifications, institutional roles, regulatory objectives, implementation challenges, and emerging trends such as central bank digital currencies (CBDCs). South Africa's regulatory stance not only reflects local policy imperatives but is also increasingly aligned with global best practices.

1.5 The Nature of Blockchain Technology

At its core, blockchain is a decentralised, peer-to-peer network that maintains a digital ledger of transactions. Each transaction is bundled into a block, and these blocks are sequentially linked (hence "block-chain") through cryptographic hashes, making any attempt to alter historical data computationally infeasible without consensus across the network (Pilkington, 2016). Blockchain technology typically uses consensus mechanisms such as proof-of-work (PoW), proof-of-stake (PoS), or delegated proof-of-stake (DPoS) to validate transactions. The potential applications of blockchain extend

far beyond cryptocurrency, including supply chain management, identity verification, healthcare record systems, property registries, and smart contracts. However, cryptocurrency remain its most prominent use case, with Bitcoin, Ethereum, and stablecoins like USDT dominating global markets (Catalini & Gans, 2016; Zohar, 2015).

1.6 Classification of Cryptocurrency in South Africa

In a watershed moment for crypto regulation in South Africa, the Financial Sector Conduct Authority (FSCA) announced in 2021 that cryptocurrency would be classified as financial products under the Financial Advisory and Intermediary Services Act (FAIS). This classification compels crypto-asset service providers (CASPs), such as exchanges, brokers, and wallet providers, to register with the FSCA and comply with regulatory requirements (FSCA, 2021). According to the FSCA, crypto assets are defined as a "digital representation of value that is not issued by a central bank but is capable of being traded, transferred, or stored electronically by natural and legal persons for the purpose of payment, investment, and other forms of utility" (FSCA, 2021). This definition echoes the Financial Action Task Force (FATF) guidance on virtual assets, aimed at mitigating risks related to money laundering and terrorist financing (FATF, 2021).

The classification under FAIS also ensures that service providers offering advice or intermediary services regarding cryptocurrency must comply with standards on licensing, disclosure, and conflict of interest mitigation, principles traditionally reserved for mainstream financial instruments. In addition to the South African Reserve Bank's (SARB) oversight role within the national payment system, the Prudential Authority (PA), established under the Financial Sector Regulation Act and operating within the SARB, plays a distinct but complementary regulatory role in the cryptocurrency ecosystem. While the SARB focuses primarily on monetary stability, payment system integrity, exchange control, and broader systemic risk implications associated with crypto-assets, the Prudential Authority is specifically responsible for promoting the safety and soundness of banks, insurers, and other regulated financial institutions. In the context of cryptocurrency, the Prudential Authority's role becomes particularly relevant where banks and financial institutions engage with crypto-asset service providers (CASPs), provide custody services, maintain exposure to crypto-assets, or facilitate cryptocurrency-related financial activities. The Prudential Authority therefore

evaluates prudential risks such as capital adequacy, liquidity exposure, operational risk, cyber-security vulnerabilities, and governance concerns arising from crypto-asset participation. This distinction illustrates South Africa's evolving twin-peaks regulatory model, where the SARB oversees systemic and payment-related dimensions of cryptocurrency activity, while the Prudential Authority focuses on institutional resilience and financial sector stability. Together, the SARB and the Prudential Authority form part of South Africa's broader multi-agency approach to cryptocurrency governance, alongside institutions such as the Financial Sector Conduct Authority (FSCA) and the Financial Intelligence Centre (FIC).

Regulatory Objectives and Rationale

South Africa's regulatory posture towards cryptocurrency is shaped by a set of policy objectives grounded in the protection of consumers, market integrity, and financial system stability:

1. **Consumer Protection:** The unregulated crypto market in South Africa has witnessed widespread scams, fraudulent investment schemes, and the proliferation of pyramid schemes. Without formal oversight, consumers are vulnerable to significant financial losses due to market volatility, lack of information, and misinformation. Regulation seeks to ensure that crypto service providers operate transparently, honestly, and in a manner that mitigates the risk of consumer exploitation (Zamani & Giaglis, 2018).
2. **Market Integrity and Financial Stability:** As crypto-assets grow in prominence, they may introduce systemic risk to the broader financial system, particularly if financial institutions gain exposure without appropriate safeguards. Regulation allows authorities to monitor developments and intervene where necessary to preserve market stability (Arner et al., 2017).
3. **Prevention of Illicit Activity:** The pseudonymous and borderless nature of cryptocurrency renders them susceptible to abuse for money laundering, terrorist financing, and tax evasion. Through AML/KYC requirements, South African regulators aim to curtail these risks while integrating crypto-assets into a controlled financial ecosystem (Houben & Snyers, 2018).

Monetary Policy Control: A growing dependence on privately-issued digital currencies could erode the South African Reserve Bank's (SARB) ability to influence liquidity, inflation, and interest rates. Regulation helps reassert central authority over monetary policy mechanisms (Reuters, 2022).

1.7 Research Problem Statement

Despite rapid technological advances in digital payments, cross-border transfers remain costly, slow, and opaque. While cryptocurrency offers alternative settlement pathways, there is insufficient academic and policy clarity on how financial regulation can govern crypto-asset-based remittance channels without undermining innovation or financial inclusion (Rühmann et al., 2020). The core research problem is therefore not technological feasibility, but regulatory integration of cryptocurrency into South Africa's cross-border financial system.

1.8 The 3 Dimensions

This research examines three interrelated dimensions that shape the regulatory framework for cryptocurrency-based cross-border transfers in South Africa. Rather than focusing on blockchain infrastructure, the study evaluates how crypto-assets, service providers, and transaction ecosystems interact with financial regulation.

Dimension 1: Regulatory challenges

The first dimension reflects the tension between decentralised crypto-asset networks and centralised financial regulatory systems. Unlike traditional bank-mediated transfers, cryptocurrency transactions may occur via exchanges, wallets, DeFi platforms, or peer-to-peer mechanisms, complicating the application of AML, KYC, exchange control, and consumer protection laws. Regulatory challenges therefore arise at the asset, intermediary, and service-provider levels, rather than at the level of blockchain protocol design.

Interviews conducted for this study reveal three primary barriers to effective regulation: (1) the absence of clear and comprehensive legal guidelines governing cryptocurrency use, (2) the lack of harmonised global standards, which creates

inconsistencies and opportunities for regulatory arbitrage, and (3) the cautious stance adopted by South African financial institutions, driven by uncertainty and perceived risks. These challenges are compounded by the rapid evolution of cryptocurrency technologies and the slow pace of regulatory adaptation, which often lags behind innovation. This regulatory stagnation fosters an environment of uncertainty that discourages experimentation and limits progress in critical areas such as retail remittances.

Furthermore, the decentralised nature of cryptocurrency introduces unique financial compliance risks. For example, pseudonymity (the state of using a false name) in transactions complicates AML enforcement, while the absence of intermediaries undermines usual mechanisms for dispute resolution and consumer protection. These issues are not unique to South Africa, but reflect global regulatory struggles, as jurisdictions worldwide attempt to balance innovation with systemic stability. The result is a fragmented regulatory landscape that impedes the scalability of cryptocurrency-based solutions for cross-border payments. Addressing these challenges requires a coordinated approach that combines adaptive regulation, technological solutions for compliance, and international cooperation to establish consistent standards.

Dimension 2: Regulatory mitigation approaches

The second dimension, regulatory mitigation approaches, focuses on strategies that aim to reduce regulatory barriers while enabling innovation in cryptocurrency-based financial services. These strategies encompass institutional, legal, and policy interventions designed to create a more flexible regulatory environment. One important approach is the use of regulatory sandboxes, such as those implemented by the Intergovernmental Fintech Working Group (IFWG) in South Africa. These sandboxes provide a controlled environment where innovators can test cryptocurrency solutions under the supervision of regulators, ensuring compliance with existing laws while allowing flexibility for experimentation.

Experts interviewed for this study emphasised the importance of risk-based compliance models which are adaptive. These modify regulatory investigations to the level of risk associated with specific transactions or actors. This approach allows regulators to allocate resources efficiently while reducing unnecessary burdens on low-risk activities. At the international level, frameworks such as the Financial Action

Task Force (FATF) Travel Rule have influenced global efforts to harmonise standards for cryptocurrency transactions, particularly in relation to AML and KYC requirements. These global initiatives are critical for addressing cross-border regulatory inconsistencies and preventing regulatory arbitrage.

However, mitigation strategies extend beyond technical compliance. Interviewees highlighted the need for enhanced collaboration between regulators across international jurisdictions and a more proactive stance from South African authorities in engaging with industry stakeholders. Such collaboration is essential for developing clear industry standards, fostering trust, and ensuring that regulatory frameworks evolve in step with technological innovation. Without these measures, regulatory uncertainty will continue to hinder adoption and limit the potential benefits of cryptocurrency for reducing remittance costs and improving financial inclusion.

Ultimately, regulatory mitigation approaches must strike a balance between safeguarding financial integrity and promoting innovation. This requires a coordinated effort that combines policy flexibility, technological solutions for compliance, and international cooperation to create a regulatory environment conducive to sustainable growth in cryptocurrency-based cross-border payments.

Dimension 3: Embedding regulation in cryptocurrency design

The third dimension explores how regulatory compliance can be embedded within crypto-asset ecosystems, including exchanges, wallet providers, stablecoin issuers, and identity-verification layers. Rather than regulating code at the protocol level, regulators increasingly rely on RegTech (regulatory technology) integration at the service-provider interface, such as Travel Rule compliance, transaction monitoring, and blockchain analytics. RegTech refers to the use of technology, particularly information technology, to help businesses comply with regulations more efficiently and effectively. Interviewees for this study highlighted the potential of self-sovereign identity frameworks, built on blockchain technology, to enable user-centric identification systems that comply with regulatory standards while preserving privacy. Such frameworks allow individuals to control their identity credentials while granting regulators verifiable access when required. Additionally, immutable, real-time ledgers can potentially provide regulators with transparent data streams, improving accountability and auditability without introducing excessive surveillance concerns.

(Hossain et al., 2025). This capability addresses one of the most pressing challenges in cryptocurrency regulation, ensuring compliance without undermining decentralisation or user autonomy.

This perspective marks a significant shift in how technology is perceived: from being a tool to evade regulation to becoming an enabler of compliance. By embedding compliance features within cryptocurrency ecosystems, regulators and innovators can create systems that support financial integrity while maintaining efficiency and innovation. Globally, similar approaches are gaining traction, with initiatives exploring regulatory technology solutions, automated reporting, and interoperability standards to align compliance across jurisdictions.

Together, these three dimensions: regulatory challenges, mitigation strategies, and embedded compliance form the foundation of this study's analysis of how South Africa can develop a regulatory framework that promotes innovation while safeguarding systemic stability. Achieving this balance requires not only legislative reform but also a cultural shift within regulatory institutions, from restrictive gatekeeping to collaborative engagement with industry stakeholders. Such a transformation is essential for unlocking the full potential of cryptocurrency in reducing remittance costs and advancing financial inclusion.

The Three Dimensions of Cryptocurrency Regulation

A framework for analysing regulatory challenges, mitigation strategies, and embedded compliance in South Africa's crypto-asset cross-border payment ecosystem



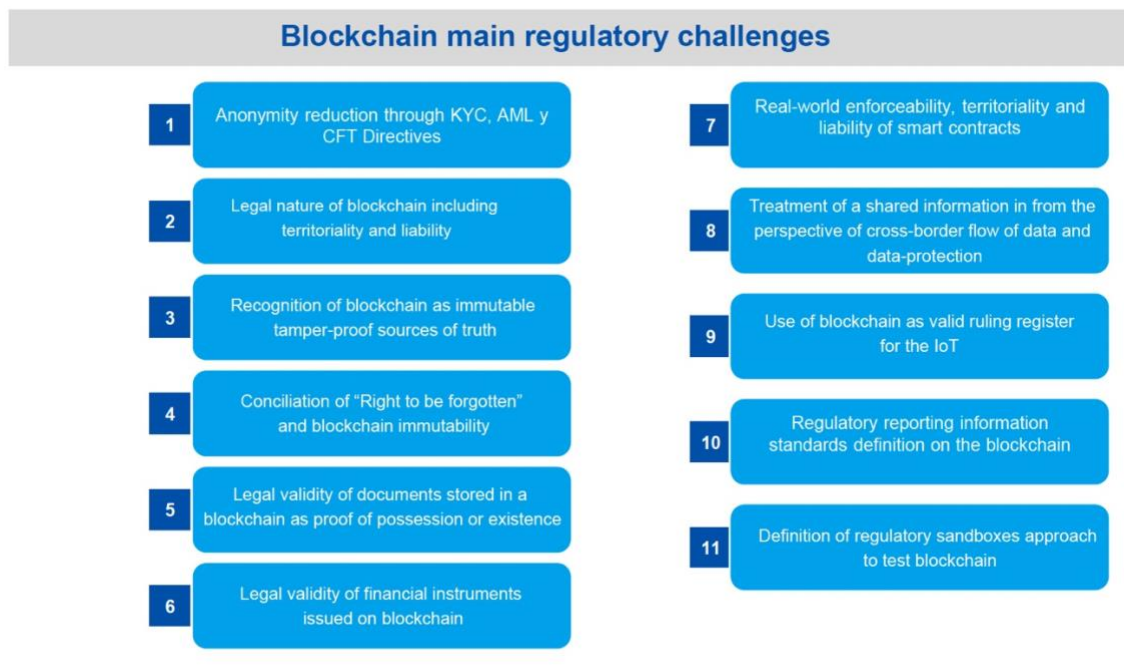
Figure 1. 3 Dimensions of Cryptocurrency Regulation (Researcher)

1.8.1 Gap and need for regulations

Blockchain technology and by definition, cryptocurrency, have the capacity to revolutionise the conventional cash transfer system by eliminating intermediaries and enabling direct transactions between peers. Utilising blockchain technology, transactions can be settled instantly, reducing the capital costs associated with the existing settlement system. This innovative technology aims to tackle the limitations of traditional payment systems, including slow transaction speeds, restricted access,

lack of transparency, and high transaction costs (Rühmann et al, 2020). However, current literature identifies several limitations, including *inter alia* data privacy risks, regulatory uncertainty and last-mile delivery, in deploying the blockchain as a solution to reduce the cost of cross-border transfers in South Africa. There is also a lack of uniformity in blockchain and cryptocurrency regulations globally. Different countries have developed varying regulatory approaches, from embracing blockchain technology to imposing strict restrictions or bans. This lack of harmonisation creates uncertainty for businesses and users, hindering the adoption of blockchain for cross-border transfers.

Regulatory authorities struggle to classify cryptocurrency and tokens properly. Is a particular cryptocurrency a security, commodity, currency, or something else entirely? The classification significantly affects how it is regulated. This lack of clarity can lead to confusion and inconsistent enforcement. Cross-border blockchain transactions involve multiple jurisdictions, each with its own regulations. This complexity makes it challenging to navigate regulatory requirements, leading to potential compliance issues. Furthermore, regulatory gaps exist concerning the coordination of international efforts to regulate cross-border blockchain transactions effectively. Recently, regulators and practitioners have studied the capabilities of blockchain technologies to streamline and, potentially, replace the infrastructure underpinning cross-border payments and remittances (Rella, 2019). Addressing these regulatory gaps and creating a more comprehensive, coherent, and adaptable regulatory framework for blockchain, especially in relation to cross-border transfers, is essential for the technology's responsible and effective integration into the South African financial system.



Source: BBVA Research

Figure 2. Banco Bilbao Vizcaya Argentaria Research (Source)

In June 2018, the South African Reserve Bank successfully completed Project Khokha, a PoC (Proof of Concept) designed to simulate a ‘real-world’ trial of a blockchain-based wholesale payment system (Govchain 2020). The project focused on providing respondents practical experience on aspects of using blockchain in a realistic test environment where different deployment models were utilised. The objectives of Project Khokha were to build on the initiatives previously undertaken by global peers and to gain further insights on blockchain developments in a South African wholesale payments context. The Project provides a better understanding of how South African Multiple Option Settlement (SAMOS) system would integrate with a blockchain system (Govchain 2020).

Currently, the technology powering blockchain and its associated cryptocurrency is relatively new and not fully developed. Ongoing pilot projects and small-scale initiatives underscore the importance of conducting additional research in collaboration with regulators and policymakers. It is crucial for policymakers to play a proactive role in creating a supportive environment for the adoption of blockchain technology. This can be achieved by endorsing pilot programs, establishing innovation hubs and regulatory sandboxes, and defining regulatory frameworks that can be implemented on a national level (Rühmann et al., 2020).

1.8.2 Problem

The current body of literature does not adequately address the critical gap in knowledge regarding the effects of the utilisation of blockchain and cryptocurrency technology in the reduction of cross-border transfer fees in South Africa. The underlying blockchain technology with its distributed and immutable characteristics offers new ways of making cross-border payment systems faster, more cost-effective, efficient and secure. This study explores the opportunities and challenges of employing blockchain technology to reduce the cost of cross-border payments.

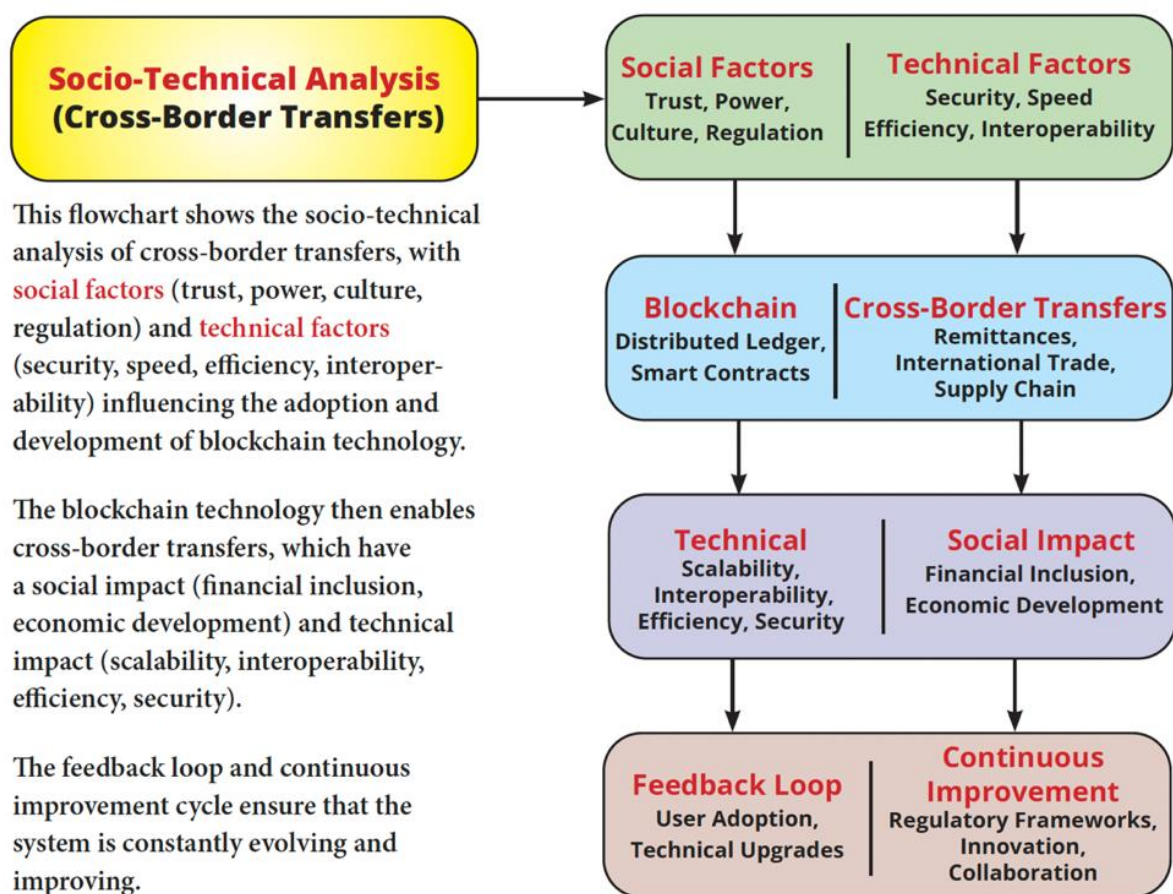


Figure 3. Flowchart depicting socio-technical analysis of cross-border transfers (Researcher)

1.8.3 Objective

This study aims to fill the research gap by exploring the South Africa's financial regulatory systems and to develop a deeper understanding on the regulatory

imperatives that will support blockchain technology to facilitate the reduction of cross-border transfers.

1.9 Research Purpose Statement

The objective of this research is to investigate the regulatory challenges and mitigations of cryptocurrency and crypto-asset systems in cross-border payments and its impact on the South African financial regulatory system. In order to do this, the researcher engaged with government and corporate fintech experts with blockchain expertise who work in the financial regulatory space. In addition, the researcher conducted a review of current legislation and regulation relevant to processing of cross-border payments in the South African context.

1.10 Research Questions

Main research question

How might regulatory challenges and potential mitigation strategies inform the future design of a cryptocurrency solution for cross-border payments in the context of the South African regulatory system?

Research sub-questions

Sub-question 1: *How can South Africa develop an effective regulatory framework that balances blockchain innovation in cross-border transfers with compliance requirements, while addressing institutional resistance and technical integration challenges?*

Sub-question 2: *How can South Africa develop a cryptocurrency implementation approach for cross-border transfers that balances regulatory innovation with financial inclusion while addressing the cultural shift required for institutional stakeholders to transition from gatekeepers to facilitators?*

Sub-question 3: *How can regulatory compliance (e.g., KYC, AML) be technically embedded into blockchain-based cross-border solutions?*

1.11 Background

Maloumby-Baka and Kingombe (2016) state that cross-border payments are considered to be one of the tools which can reduce poverty, as they provide recipient households with extra incomes, which, in turn, increase the aggregate demand, and they are an income stream to locales where credit and labour markets are often non-existent. High cross-border transfer costs reduces the amounts beneficiaries actually receive. Maloumby-Baka and Kingombe (2016) posit that the high charges undermine the impact of remittances on inclusive growth and structural transformation. Karikari et al. (2016) supports the positive relationship between cross-border transfers and financial intermediation by arguing that migrant transfers in excess of consumption expenditures are likely to be placed in savings, thus introducing recipient individuals to financial products and services, which could lead to enhanced financial development.

1.11.1 Causes of high cross-border transfer fees

The existing cross-border payment infrastructure relies heavily on the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network and correspondent banking relationships. This system, established in the 1970s, requires financial institutions to maintain relationships with banks in different jurisdictions to facilitate international transfers (SWIFT, 2021). Each transaction typically involves multiple intermediaries, including originating banks, correspondent banks, clearinghouses, and receiving banks, creating a complex web of relationships and dependencies. The multi-layered nature of traditional cross-border payments results in significant cost burdens for end users. According to the World Bank's Remittance Prices Worldwide database, the global average cost of sending remittances was 6.3% in 2022, more than double the United Nations Sustainable Development Goal target of 3% (World Bank, 2022). These costs are particularly pronounced in developing markets, where limited banking infrastructure and regulatory complexities exacerbate transaction expenses. The high costs stem from several factors: correspondent banking fees, foreign exchange margins, regulatory compliance costs, operational overhead, and liquidity management expenses (McKinsey & Company, 2022). Additionally, the time-intensive nature of traditional settlements, which can take 3-5 business days for completion, creates opportunity costs and liquidity constraints for both financial institutions and their customers (Bank for International Settlements, 2021).

Maloumby-Baka and Kingombe (2016) argue that underdeveloped financial and payment infrastructures, especially in rural areas, contribute to keeping cross-border financial transfer prices high, since money sent and received may not circulate easily and that makes inefficient remittance services. This inefficient cross-border transfer services result in social costs for remittance senders and receivers, as the former may not have easy access to remittance service providers (RSPs) and the latter may not be able to collect the funds transferred in a timely manner. This relates to the underdeveloped financial system in Africa, as witnessed by its low level of access and use of formal banking services. The consequence of this is the limited use of the financial services, which contributes to increasing remittance prices (Ratha et al., 2011). Maloumby-Baka and Kingombe (2016) state that such an underuse of the existing formal financial infrastructures result's in a lack of transparency in the market and in a lack of competition among RSPs.

The authors further state that lack of competition means that major money transfer operators (MTOs) in a region, namely Western Union and MoneyGram that in SSA control two-thirds of the market, are unchallenged and free to impose their own, usually high, prices (ODI, 2014; UNCTAD, 2012). Orozco, (2017) states that the largest money transfer companies such as MoneyGram and Western Union demand that agents sign exclusivity agreements. These agreements effectively 'lock' more than half of all available pay-out locations. Because they apply to all agents, banks, foreign exchange bureaus and post offices, among others, an effective control of 65% of the authorised pay-out market results. Entities wishing to partner with these companies have to sign exclusivity agreements.

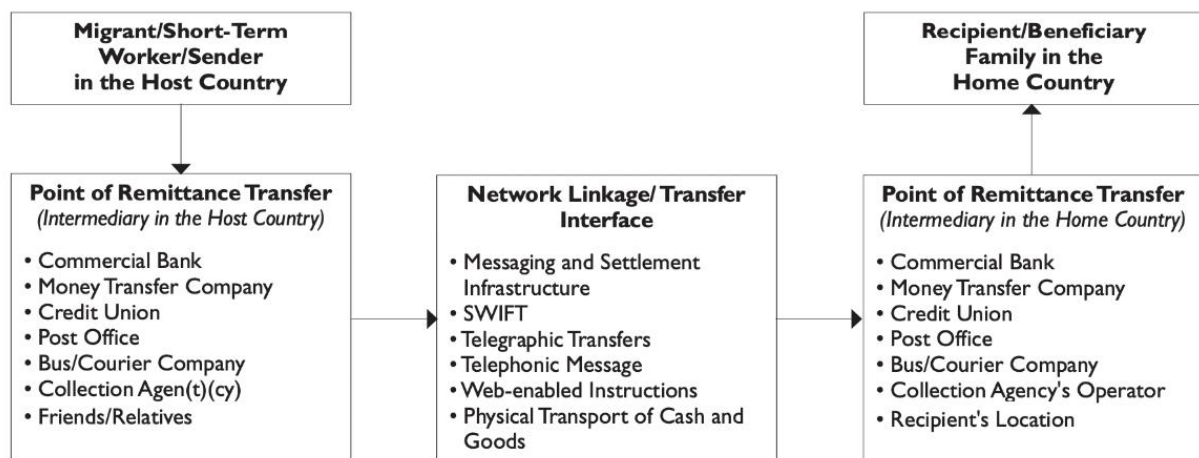
The charges levied against cross-border transfers depends on the channel through which remitters decide to send money, i.e. cash, bank account, card, etc. Thus, the average cost of sending money to and within Africa should be looked at with this in mind (World Bank, 2014b). For example, financial institutions tend to have higher overhead costs than money transfer organisations (MTO) due to the high fixed costs related to their network of branches, automated teller machines (ATMs) and regulatory compliance requirements. Those items feed into higher remittance fees (UNCTAD, 2012). As for the methods of sending money, bank accounts were the most expensive way, with an average total cost of 15.07% of the funds transferred, while the cheapest

method was the mobile phone, with an average total cost of 6.15% (African Institute for Remittances, 2015). As a result, the market of remittances is increasingly diversifying in terms of innovative financial products. In particular, the emergence and growth of 'mobile-banking', a "form of branchless banking based exclusively on the use of mobile phones and the capacity of telecommunications operators to provide payments and assets storage (i.e. electronic wallet)", are beneficial to remitters and recipients (Épargne sans frontières, 2014, p.14).

An emerging digital instrument is increasingly being referred to as even cheaper than cell phones, that is the cryptocurrency Bitcoin (payment system) made possible by the internet. (Ratha, et al, 2011) state that M-Pesa in Kenya is a striking example of the ability of African countries to "leapfrog" even developed countries in the use of innovative mobile money services. Maloumby-Baka and Kingombe (2016) state that Bitcoin is believed to be able to revolutionize the cross-border transfer market worldwide, in terms of reducing remittance transaction costs drastically. The authors assert that because transactions are performed amongst users directly, that is, without the need of banks or any other financial intermediary in an entirely decentralised way, transfer fees will be significantly lower. This is due to the fact that users and volunteer developers keep track of transactions (i.e. transfers of value between Bitcoin wallets) and update the records of transactions in real time.

1.12 Key characteristics of the cross-border transfer (remittance) process

Remittance Channels



Note: Not all funds transferred through these channels are remittances.

Figure 4. Key characteristics of the global remittance process World Bank (2007)

When executing a cross-border money transfer, funds of the remittance amount must be present in the sender's bank account. After the transaction has been issued, the funds are transmitted to the recipient's bank for processing. Once the money is at the bank, a foreign exchange rate and banking fee are applied. The funds are now available as local currency, minus the fees, for the recipient to access. Remittance services can be more or less complex, and of varying speed. However, in all cases it is necessary to have some kind of "network" - ie access points, where consumers of remittance services pay and receive funds. Also needed are procedures to link those access points to enable messaging (the transfer of information about the remittance) and settlement (the transfer of the funds themselves) (World Bank, 2007). Some Remittance Service Providers (RSPs), such as global banks, may have branch networks they can use for this purpose ("unilateral service").

1.13 Key issues in legislation and regulation: Legislative compliance

South Africa's fiscal and financial regulatory environment is governed by a complex but evolving framework designed to uphold financial system integrity, ensure consumer protection, and maintain alignment with global AML and counter-terrorism financing

(CTF) norms. The core regulatory bodies include the South African Reserve Bank (SARB), which is responsible for monetary policy and financial system oversight; the Financial Sector Conduct Authority (FSCA), tasked with market conduct regulation; and the South African Revenue Service (SARS), which oversees taxation and compliance. While this tripartite structure has traditionally supported financial stability, it faces growing pressure to adapt to the emergence of blockchain and digital financial technologies, particularly for use cases such as cross-border payments. The current legal and regulatory framework was not originally designed with decentralised technologies in mind, leading to a state of “regulatory lag” (Zetzsche et al., 2018), where innovation in the market outpaces the ability of legislation and policy to respond. As such, regulatory uncertainty concerning licensing, compliance obligations, data privacy, and exchange control requirements continues to hamper the deployment of blockchain-based payment infrastructure.

In recent years, the SARB has demonstrated cautious openness to exploring distributed ledger technologies (DLTs) as part of its modernisation agenda. Through strategic pilots like Project Khokha (2018) and Project Khokha 2 (2021), SARB assessed the feasibility of using blockchain for interbank settlements and tokenized asset transactions. These pilots revealed potential efficiency gains, reduced transaction costs, and increased transparency in wholesale financial markets. However, the SARB has remained clear that any blockchain-enabled system, particularly those facilitating cross-border transactions, must comply with South Africa’s strict exchange control regulations under the Currency and Exchanges Act, 1933 (as amended). This includes the requirement for authorised dealers and prior SARB approval for most outbound flows of capital, a measure aimed at safeguarding the country’s balance of payments and macroeconomic sovereignty. Consequently, blockchain’s borderless nature and decentralised architecture are at odds with these entrenched capital control mechanisms, creating tension between innovation and regulation (SARB, 2021). Furthermore, SARB has expressed concerns around the use of crypto-assets to circumvent AML/CTF laws and capital outflow reporting, reinforcing the institution’s emphasis on regulatory prudence over rapid innovation.

Complementing SARB’s prudential oversight, the FSCA has taken decisive steps to bring blockchain-based financial products and services into the formal regulatory

perimeter. In 2022, the FSCA formally declared crypto assets as “financial products” under the Financial Advisory and Intermediary Services (FAIS) Act, thereby subjecting crypto asset service providers (CASPs) to licensing, fit-and-proper requirements, and oversight mechanisms (FSCA, 2022). This declaration marked a significant regulatory milestone in establishing legal accountability within the digital asset ecosystem. However, it also introduced new compliance burdens for fintech firms and institutional players seeking to operationalize blockchain applications for international payments. At the same time, SARS has issued interpretative guidance confirming that income from crypto asset transactions is subject to taxation under normal income tax principles. Yet, there is a notable absence of comprehensive tax regulation for decentralised applications, tokenized asset classes, and smart contract-based transactions, particularly when it comes to the nuances of cross-border reporting obligations, double taxation risks, and valuation of intangible digital assets (SARS, 2021). These ambiguities contribute to legal uncertainty, making it difficult for market participants to structure compliant cross-border blockchain payment solutions.

To address the regulatory fragmentation and foster an environment conducive to responsible innovation, South Africa has established the Intergovernmental Fintech Working Group (IFWG), a collaborative body comprising SARB, FSCA, SARS, National Treasury, and the Financial Intelligence Centre (FIC). The IFWG has served as a critical platform for policy coordination, stakeholder engagement, and regulatory experimentation. Its 2021 Crypto Assets Regulatory Position Paper laid the groundwork for a phased approach to regulating crypto assets, emphasising AML/CTF compliance, consumer protection, and systemic risk mitigation (IFWG, 2021). Additionally, the IFWG launched a regulatory sandbox and an Innovation Hub to allow fintechs and blockchain startups to test novel solutions in a controlled environment, under close regulatory supervision.

These mechanisms are designed to reduce compliance uncertainty, accelerate regulatory learning, and support the safe scaling of financial innovation. However, the broader context has become more complex following South Africa’s grey-listing by the Financial Action Task Force (FATF) in February 2023. The FATF cited deficiencies in South Africa’s AML/CTF framework, leading to heightened scrutiny on cross-border financial flows. As a result, regulators may be less willing to approve or endorse

blockchain-based cross-border payment systems that are not fully aligned with international standards on due diligence, KYC, and transaction monitoring (FATF, 2023).

In summary, South Africa's fiscal regulatory environment reflects a delicate balancing act: it aims to encourage technological innovation while maintaining financial stability, exchange control sovereignty, and international compliance. Although significant strides have been made through the efforts of SARB, FSCA, and the IFWG, key challenges remain, most notably regulatory uncertainty, fragmented governance, and conflicting policy priorities. The successful implementation of blockchain for cross-border payments in South Africa therefore requires not only robust technical design and market fit, but also a proactive engagement strategy with regulators, adaptive compliance mechanisms, and alignment with both domestic and international regulatory standards.

1.14 Delimitations

The study is restricted to South Africa's policy, legal, and regulatory jurisdiction. While cross-border transfers inherently involve multiple national jurisdictions, this research focuses specifically on how South Africa's regulatory framework governs and responds to cryptocurrency-enabled cross-border transfers, rather than conducting a comparative analysis of international regulatory systems.

1.15 Dissertation Structure and Chapter Outline

This dissertation is structured into seven chapters, each designed to address specific aspects of the research problem and contribute toward answering the main research question concerning the regulatory challenges and mitigations associated with cryptocurrency-enabled cross-border transfers in South Africa.

Chapter 1: Between Disruption and Compliance: Framing South Africa's Cryptocurrency Challenge

Chapter 1 introduces the study by contextualising the problem of high cross-border transfer and remittance fees, particularly within the African and South African context.

The chapter outlines the emergence of cryptocurrency as an alternative payment mechanism and examines the evolving South African regulatory environment. It presents the research problem, research objectives, research questions, and the three analytical dimensions underpinning the study. The chapter establishes the conceptual foundation for the dissertation and defines the scope and delimitations of the research.

Research objective addressed:

To establish the regulatory and socio-economic context surrounding cryptocurrency-enabled cross-border transfers in South Africa and to define the research problem and analytical framework guiding the study.

Chapter 2: Literature Review and Theoretical Frameworks

Chapter 2 critically reviews existing literature on blockchain technology, cryptocurrency, crypto-assets, and cross-border payment systems. It evaluates regulatory theories relevant to fintech governance, including public interest theory, responsive regulation, risk-based regulation, and socio-technical theory. The chapter also analyses existing scholarly debates on financial inclusion, regulatory harmonisation, and innovation governance, while identifying key gaps in current literature.

Research objective addressed:

To analyse existing academic and policy literature relating to cryptocurrency regulation, blockchain-enabled cross-border transfers, and innovation governance, while identifying theoretical and empirical gaps addressed by this study.

Chapter 3: Research Methodology

Chapter 3 outlines the philosophical assumptions, qualitative research approach, and methodological design employed in the study. It explains the use of semi-structured interviews with regulatory and fintech experts, data collection procedures, thematic analysis techniques, ethical considerations, and limitations of the research. The chapter also discusses researcher positionality and quality assurance measures used to ensure credibility and trustworthiness.

Research objective addressed:

To develop and justify a qualitative research methodology capable of exploring the

regulatory challenges and mitigation strategies associated with cryptocurrency-enabled cross-border transfers.

Chapter 4: Regulatory Analysis and Empirical Findings

Chapter 4 provides a detailed analysis of South Africa's legislative and regulatory framework governing cryptocurrency and cross-border financial transfers. The chapter examines legislation, regulatory directives, and institutional frameworks relevant to crypto-assets, including AML/KYC requirements and exchange control regulations. It further presents the empirical findings derived from interviews with industry and regulatory stakeholders, organised according to the study's three analytical dimensions.

Research objective addressed:

To evaluate the current South African regulatory framework governing cryptocurrency and to identify the practical regulatory, technological, and institutional challenges affecting cryptocurrency-based cross-border transfers.

Chapter 5: Gap Analysis and Regulatory Reform Imperatives

Chapter 5 synthesises the empirical findings and regulatory analysis to identify key gaps within South Africa's current cryptocurrency governance framework. These include regulatory architecture gaps, compliance limitations, institutional readiness deficiencies, interoperability challenges, and international coordination shortcomings. The chapter further proposes strategic recommendations and reform priorities required to address these deficiencies.

Research objective addressed:

To identify and analyse the critical regulatory and institutional gaps limiting the effective adoption of cryptocurrency-enabled cross-border payment systems in South Africa.

Chapter 6: Design Science Research Knowledge Model

Chapter 6 develops the study's proposed Design Science Research (DSR) knowledge model, structured as a five-echelon framework for cryptocurrency regulation and implementation. The model integrates legislative reform, compliance mechanisms, technical interoperability, institutional collaboration, and adaptive user-centric

governance approaches. The chapter demonstrates how regulatory integrity and innovation can coexist through a hybrid governance approach.

Research objective addressed:

To develop a practical and theoretically informed regulatory knowledge model capable of supporting cryptocurrency-enabled cross-border transfers while balancing innovation, compliance, and financial stability.

Chapter 7: Conclusion and Recommendations

Chapter 7 concludes the dissertation by consolidating the key findings and addressing the main research question and sub-questions. The chapter reflects on the broader implications of the study for financial regulation, digital innovation, and financial inclusion in South Africa. It also provides differentiated recommendations for policymakers, regulators, industry stakeholders, and future researchers, while identifying areas for further investigation.

Research objective addressed:

To consolidate the study's findings and provide actionable recommendations for the future development of cryptocurrency regulation and cross-border payment innovation in South Africa.

CHAPTER 2

CROSSING KNOWLEDGE BORDERS: MAPPING LITERATURE ON THE REGULATION OF CRYPTOCURRENCY AND CRYPTO-ASSET ECOSYSTEMS IN CROSS-BORDER PAYMENTS

This chapter reviews the interdisciplinary literature on the regulation of cryptocurrency and crypto-asset ecosystems within the framework of cross-border financial transfers. While blockchain technology underpins these systems, blockchain itself is a general-purpose infrastructure and not the object of financial regulation. Regulatory frameworks instead govern crypto-assets as financial instruments, the service providers that facilitate their use, and the financial activities performed through them (FATF, 2021; FSB, 2023; Arner et al., 2017).

This chapter therefore shifts the methodological focus from distributed ledger technology to crypto-asset payment rails, examining how these systems intersect with financial regulation, innovation diffusion, socio-technical systems, and institutional economics. Particular attention is given to how cryptocurrency are positioned as alternative cross-border settlement mechanisms capable of reducing remittance costs while introducing regulatory, monetary, and systemic risk concerns. It is important, however to make a clear distinction between blockchain and cryptocurrency.

2.1 Chapter Overview

This section aims to provide a review of relevant literature on financial regulation in relation to the importance of cryptocurrency in the reduction of cross-border transfer fees to destination countries and the ways in which implementation could support the reduction in fees associated with remittances to South Africa. Two key concepts upon which this literature review is built on is that of innovation theory and socio-technical theory. Systematic reviews and meta-analyses are the “gold standard” of research reviews (Clarke & Stewart, 1994). Systematic review methods can be applied to almost any study type and aim to be systematic, explicit, and reproducible (Tricco, Tetzlaff & Moher, 2010).

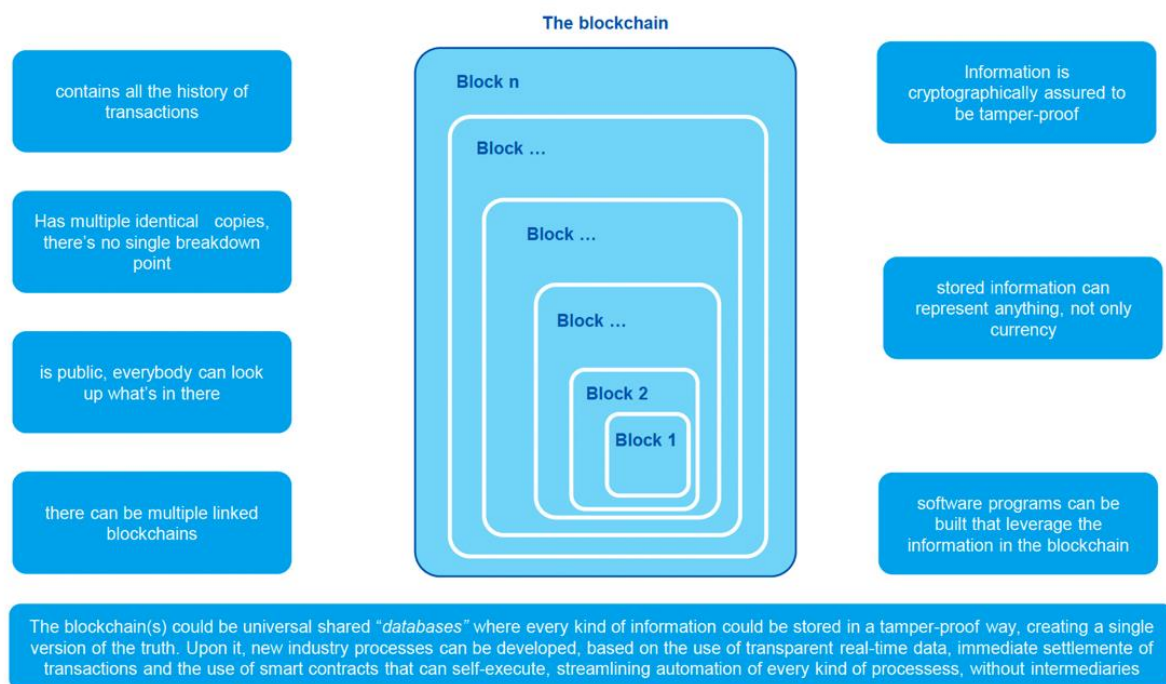
2.2 Blockchain, Crypto-Assets, Cryptocurrency Networks and Digital Settlement Systems

Cryptocurrency is a digital representation of value that operates on distributed ledger infrastructure but function economically as transferable financial assets rather than as technological protocols (FSB, 2023; IMF, 2022). Unlike blockchain infrastructure, cryptocurrency enter the regulatory domain because they perform monetary, payment, investment, and store-of-value functions. Its important to note that blockchain is infrastructure and cryptocurrency are financial instruments. Regulation governs the latter.

The FATF defines virtual assets as “digital representations of value that can be digitally traded or transferred and can be used for payment or investment purposes” (FATF, 2021). This definition forms the regulatory basis for global oversight of crypto-asset service providers (CASPs), exchanges, custodians, and wallet providers. Consequently, academic discourse has shifted from blockchain governance toward financial regulation of crypto-asset ecosystems.

Tapscott and Tapscott (2016) explain that the difference between cryptocurrency and blockchain, is that blockchain is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way." The distributed ledger in blockchain refers to the decentralised network of nodes that collectively maintain and validate the integrity of the ledger. Each participant in the blockchain network has a copy of the entire ledger, and transactions are verified and added to the ledger through consensus mechanisms, such as proof-of-work or proof-of-stake.

The disruptive features of the blockchain



Source: BBVA Research

Figure 5. The disruptive features of blockchain BBVA Research (Source)

This decentralised nature of blockchain eliminates the need for a central authority or intermediary to validate and authorise transactions. As Antonopoulos (2017) states, "Blockchains provide a way for multiple parties who do not necessarily trust each other to agree on a common state of a database, without relying on a central authority." A distributed ledger is therefore a broader concept that encompasses various decentralised systems for recording and sharing data. Blockchain is a specific implementation of a distributed ledger, utilising cryptographic techniques and consensus mechanisms to create an immutable chain of blocks containing verified transactions or data. According to the World Economic Forum (WEF), blockchain is one of the most promising technologies of the fourth industrial revolution. This is because, regardless of the size of the logistics actor or its position within the value chain, there is a good chance that its processes or the data generated will soon use this technology either directly or through applications that incorporate blockchain technology (WEF, 2019).

Blockchain technology operates on a fundamental principle that pertains to the regulation of activities conducted through it rather than the technology itself. In the

scope of blockchain, the absence of established regulations for activities within the financial services industry is primarily due to the relative immaturity of initiatives and the ongoing pilot phases of identified use cases (Cermeño 2016). It is worth noting that the regulatory framework for activities on the Blockchain depends on the specific nature of those activities. Consequently, it is challenging to make broad regulatory assertions within the industry, except for appeals to regulatory authorities to ensure fair competition between traditional incumbents and emerging Blockchain start-ups. There is also the suggestion of creating "regulatory sandboxes" to pilot potential technology-driven activities while avoiding conflicts with existing regulations (Cermeño, 2016). It is, nonetheless, essential to acknowledge that certain existing regulations are applicable to services facilitated by Blockchain technology. Furthermore, the application of regulations depends on the type of financial services being offered through Blockchain, such as payment processing, lending, and investment, among others.

This encompasses the need to comply with regulations related to KYC and AML, capital markets, lending practices, etc. It is imperative to establish close collaboration with regulatory bodies and supervisory authorities right from the inception of Blockchain initiatives. This collaborative effort is crucial to adapt to the evolving landscape and to develop a coherent and comprehensive regulatory framework tailored to the unique characteristics and challenges posed by Blockchain technologies (Cermeño, 2016).

2.3 Systematic Literature Review Methodology

A systematic literature review was conducted utilising the SPIDER method against available and grey literature concerning remittance fees in relation to the utilisation of blockchain and cryptocurrency. The SPIDER tool offers a systematic strategy for searching for qualitative and mixed-methods research studies which facilitates rigour in research by defining key elements of non-quantitative research questions. Evans (2002) suggested that confidence in finding all articles related to a specific topic by searching relevant databases is difficult because the searcher cannot know the full quota of relevant articles. Retrieval of the entire population of relevant studies would be possible only if a hand search of all relevant journals were undertaken. Evans (2002)

posited that the SPIDER tool is a good basis for a search strategy tool that can be used more efficiently with qualitative and mixed-methods research questions.

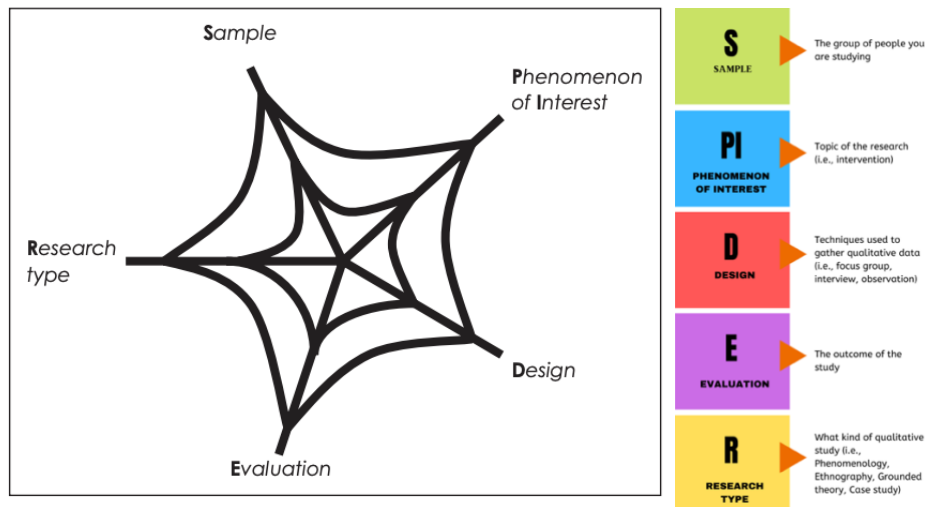


Figure 6. The SPIDER research tool, Cook et al 2012

Steps for Using Method/Tool

The SPIDER tool is adapted from the PICO tool:

(S) Sample size

(PI) Phenomenon of Interest

(D) Study Design

(E) Evaluation

(R) Research type

The application of the SPIDER framework in this study was operationalised through a structured and transparent literature search process, the steps of which are detailed below. This documentation is provided in accordance with best-practice reporting standards for systematic and structured literature reviews in qualitative research contexts (Booth et al., 2016; Liberati et al., 2009).

Search Databases and Sources

The systematic literature search was conducted across the following academic databases and grey literature repositories: (1) Scopus; (2) Web of Science; (3) Google Scholar; (4) SSRN (Social Science Research Network); (5) the South African Reserve

Bank (SARB) publications portal; (6) the Financial Action Task Force (FATF) document repository; (7) the Bank for International Settlements (BIS) working papers archive; and (8) the Intergovernmental Fintech Working Group (IFWG) publications repository. The inclusion of grey literature repositories, particularly regulatory guidance documents from the SARB, FATF, and the IFWG was deliberate, given that the regulatory landscape governing cryptocurrency in South Africa is substantially documented in policy and guidance documents rather than in peer-reviewed journal literature alone (Tricco et al., 2018).

Search Terms and Boolean Strategy

Search strings were constructed using Boolean operators to maximise retrieval precision and recall. The primary search string applied across academic databases was as follows: ("cryptocurrency" OR "crypto-asset" OR "digital asset" OR "blockchain") AND ("cross-border transfer" OR "remittance" OR "international payment") AND ("regulation" OR "regulatory framework" OR "compliance" OR "AML" OR "KYC") AND ("South Africa" OR "sub-Saharan Africa" OR "emerging markets"). Secondary search strings were developed to capture literature on specific regulatory frameworks, including: ("CASP" OR "crypto asset service provider") AND ("FATF" OR "Travel Rule" OR "Financial Action Task Force"); and ("blockchain" OR "distributed ledger technology" OR "DLT") AND ("financial regulation" OR "payment system" OR "exchange control"). Date parameters were not applied as a blanket restriction. However, given the nascent nature of cryptocurrency regulation, literature published between 2009 and 2025 formed the primary corpus, with seminal regulatory theory works included regardless of publication date.

Inclusion and Exclusion Criteria

The following inclusion criteria were applied to determine the relevance of retrieved literature: (1) studies addressing cryptocurrency, blockchain, or distributed ledger technology in the context of payments, remittances, or cross-border transfers; (2) studies examining regulatory frameworks, compliance requirements, or governance challenges for crypto-asset ecosystems; (3) policy documents, position papers, and guidance notes from regulatory authorities directly relevant to the South African or comparative international context; (4) empirical studies, conceptual frameworks, and theoretical analyses published in peer-reviewed journals, working papers, or credible

grey literature sources; and (5) literature addressing financial regulation theory, including public interest theory, responsive regulation, and risk-based approaches, insofar as these frameworks are applied to financial services or technology governance.

The following exclusion criteria were applied: (1) literature focused exclusively on cryptocurrency as a speculative investment asset without reference to payment systems, regulation, or financial infrastructure; (2) highly technical cryptographic or computer science literature that does not engage with regulatory, governance, or socio-economic dimensions; (3) newspaper articles and non-peer-reviewed commentary without substantive analytical content; and (4) studies focused exclusively on jurisdictions with no comparative relevance to South Africa's regulatory context.

Screening Process

Initial database searches yielded approximately 1,840 unique records after the removal of duplicates. Titles and abstracts were screened against the inclusion and exclusion criteria described above, yielding 312 potentially relevant sources for full-text review. Following full-text assessment, 187 sources were retained for use in the thesis, comprising peer-reviewed journal articles (n=94), working papers and reports from international organisations (n=51), regulatory guidance documents and position papers (n=28), and book chapters or monographs (n=14). Where multiple editions or versions of a document existed (for example, successive FATF guidance notes on virtual assets), the most recent version was cited as the primary reference, with earlier iterations referenced where relevant to trace the evolution of regulatory thought.

Quality Assessment

Given the qualitative and interpretive character of this study, formal quality appraisal scoring instruments (such as CASP checklists) were not applied as gatekeeping mechanisms. Rather, source credibility was assessed on the basis of: (1) the reputation and mandate of the publishing institution (in the case of regulatory and grey literature); (2) citation frequency and academic recognition (in the case of journal literature); and (3) methodological transparency and clarity of argumentation. This approach aligns with recognised practice in systematic reviews of qualitative and mixed-methods research literature (Dixon-Woods et al., 2006; Booth et al., 2016). The SPIDER tool's emphasis on the "Evaluation" component ie: the outcome of interest, provided an additional organising criterion, ensuring that retained literature directly addressed the study's core

research questions concerning regulatory challenges and mitigations for cryptocurrency-enabled cross-border payments in South Africa.

Synthesis Approach

The retained literature was synthesised using a narrative and thematic approach consistent with the inductive qualitative methodology of the broader study. Thematic categories were developed iteratively, informed by the research questions and the theoretical frameworks elaborated in Section 2.4. These categories, which include regulatory theory, AML/KYC compliance architecture, exchange control, technological infrastructure, and comparative regulatory models structured the organisation of Chapter 2 and provided the analytical scaffolding against which the primary interview findings in Chapter 5 were subsequently interpreted.

The sample size was 8 recognised government and corporate experts in the fintech and cryptocurrency regulatory arena. The phenomenon of interest was: What are the regulatory challenges and mitigations of a cryptocurrency solution on cross-border payments and its impact on the South African financial regulatory? The design technique used was the conducting of interviews with fintech regulatory experts and the development of a questionnaire which was used in the interviews. The outcome of the study that the researcher conducted is evidence regarding the efficacy of cryptocurrency and its use in the reduction of cross-border transfer fees on remittances to South Africa. The research type was be qualitative.

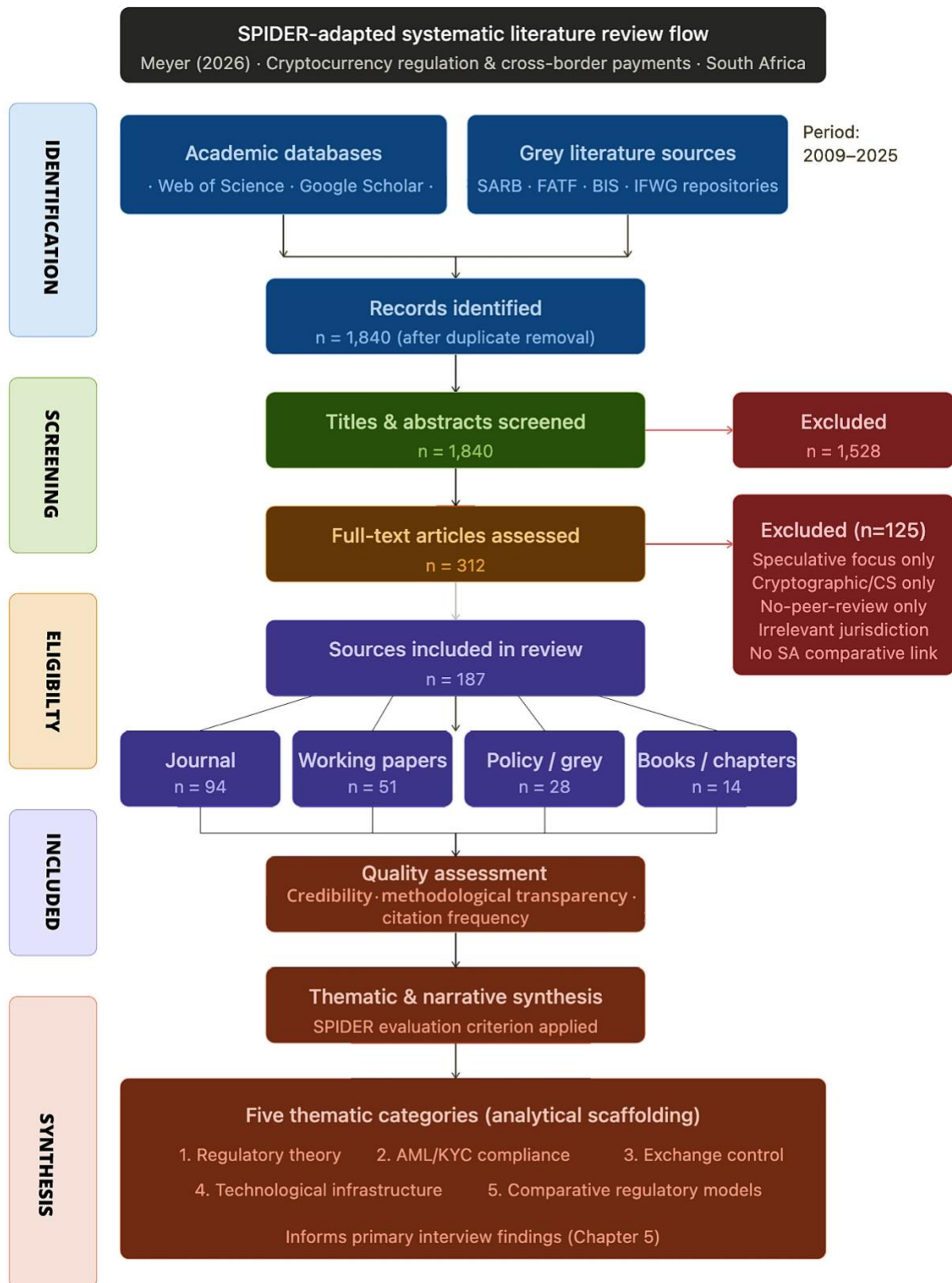


Figure 7. Diagram depicting the Systemic Literature Review Flowchart (Researcher)

2.4 Regulatory Theory and Frameworks for Crypto-Asset Governance

Effective regulation of cryptocurrency and crypto-asset ecosystems for cross-border payments requires more than an analysis of specific laws or directives; it demands a robust theoretical foundation that explains why regulatory systems emerge, how they function, and under what conditions they succeed or fail. This section critically reviews the dominant regulatory theories and frameworks most relevant to the challenges that this study investigates. The theoretical landscape surveyed here, spanning public interest theory, capture theory, responsive regulation, principles-based regulation, regulatory sandboxes, and risk-based approaches, collectively provides the conceptual architecture through which South Africa's regulatory response to cryptocurrency-enabled remittances can be understood, evaluated, and reformulated.

2.4.1 Foundational Theories of Financial Regulation: Public Interest Theory

The public interest theory of regulation, originating with Pigou (1932) and systematised in contemporary regulatory scholarship, holds that regulation exists to correct market failures, protect consumers, and serve the broader societal good. In the financial sector, this justification is operationalised through prudential oversight, AML regimes, consumer protection mandates, and systemic risk management. Posner (1974) subjected this theory to early critique, arguing that it fails to account for regulatory behaviour that diverges from public welfare maximisation, but its normative prescriptions remain foundational to financial regulatory design globally.

Applied to cryptocurrency governance, public interest theory supports the regulation of crypto-asset service providers (CASPs) on grounds that unregulated markets in digital assets expose consumers to volatility, fraud, and financial exclusion (Zetsche et al., 2020). The Financial Stability Board (FSB, 2023) has explicitly grounded its global crypto-asset regulatory recommendations in public interest rationales, arguing that unchecked crypto-asset markets generate systemic risk and undermine monetary policy transmission. However, critics such as Omarova (2021) argue that in emerging markets like South Africa, where financial inclusion is a pressing public interest concern, overly prescriptive regulatory responses anchored in stability concerns may

paradoxically deepen exclusion by foreclosing low-cost crypto-based remittance channels.

Capture Theory and Regulatory Rent-Seeking

Stigler's (1971) seminal theory of economic regulation challenges the public interest paradigm by arguing that regulation is typically acquired by the industry and operated primarily for its industry's benefit. Peltzman (1976) extended this analysis, showing that regulators respond to organised interest groups capable of delivering political support, at the expense of diffuse consumer interests. In relation to financial services, capture theory has been extensively applied to explain the persistence of incumbent bank advantages in payment systems (Avgouleas, 2012).

For cross-border remittances in South Africa, the capture thesis carries particular analytical force. The high fees charged by incumbent money transfer operators (MTOs) in the South African remittance corridor, averaging 8-11% of transaction value, well above the G20's 5% target (World Bank, 2023), may be sustained in part by regulatory frameworks that create barriers to entry for cryptocurrency-based competitors. Rauchs et al. (2018) argue that incumbent financial institutions have actively shaped AML/KYC compliance requirements in ways that are disproportionately onerous for crypto-asset entrants. This regulatory asymmetry, whether the result of deliberate capture or institutional inertia, has material consequences for the cost and accessibility of remittances for South African migrant workers.

2.4.2 *Responsive Regulation Theory*

Ayres and Braithwaite's (1992) responsive regulation theory represents a foundational shift away from both command-and-control and pure market-liberal approaches. The theory proposes a regulatory pyramid in which enforcement responses escalate from persuasion and education at the base, through warnings and civil penalties in the middle, to license revocation and criminal prosecution at the apex. Critically, responsive regulation emphasises that regulatory strategy must respond to the motivational posture of the regulated entity: cooperative actors receive facilitative treatment, while recalcitrant actors face escalating coercive responses.

Braithwaite (2011) subsequently developed the concept of 'meta-regulation', wherein regulators oversee and audit firms' own self-regulatory systems rather than directly prescribing conduct. This framework has been applied extensively to financial regulation in the post-GFC reform era (Black, 2012). For South Africa's crypto-asset regulatory trajectory, responsive regulation offers a constructive template: the IFWG, and the FSCA have increasingly employed responsive approaches, engaging CASPs in dialogue before mandating compliance, and deploying the Regulatory Sandbox as a facilitative mechanism for novel entrants. However, Van der Berg and Roos (2022) caution that responsive regulation's effectiveness depends critically on regulators possessing the technical capacity to assess crypto-asset risks accurately, a capacity gap that remains significant in many emerging market jurisdictions.

Regulatory Sandbox Frameworks

The regulatory sandbox, a controlled environment in which innovative financial products or services are tested under regulatory supervision with relaxed obligations, has become a pivotal instrument of adaptive regulation globally. First introduced by the UK's Financial Conduct Authority in 2015, sandboxes have since been adopted by over 50 jurisdictions (World Bank, 2020). Theoretically, sandboxes operationalise the 'safe harbour' concept identified in innovation policy scholarship, reducing regulatory risk for first-movers while generating evidence that informs subsequent rule-making (Bromberg et al., 2017).

In South Africa, the IFWG's Regulatory Sandbox has provided a structured mechanism for testing crypto-asset remittance applications, including stablecoin settlement trials and blockchain-based payment rails (IFWG, 2021). Zetzsche et al. (2020) offer a critical assessment of sandbox frameworks, however, noting that they may create regulatory arbitrage opportunities, generate false confidence in untested business models, and delay the development of permanent regulatory clarity that markets require for investment certainty. For the cross-border transfer use case examined in this study, the absence of a post-sandbox regulatory pathway in South Africa represents a significant gap: firms that successfully complete sandbox trials face an uncertain regulatory environment upon exit, inhibiting scale-up and consumer adoption.

2.4.3 *Principles-Based Versus Rules-Based Regulatory Approaches*

The tension between principles-based regulation (PBR) and rules-based regulation (RBR) is central to contemporary regulatory design debates, particularly in the context of rapidly evolving fintech markets. RBR prescribes specific conduct requirements, minimum capital ratios, transaction limits, and reporting frequencies that are certain, predictable, and amenable to straightforward compliance auditing. PBR, by contrast, articulates high-level standards, 'treat customers fairly', 'maintain adequate risk management', and holds regulated entities responsible for achieving those outcomes through means of their own devising (Black, 2008).

Black (2008) argues that PBR's advantages, flexibility, adaptability to novel circumstances, and avoidance of regulatory arbitrage through technical compliance, make it particularly well-suited to financial innovation contexts. However, the author also identifies PBR's critical vulnerabilities: it demands sophisticated regulatory capacity to evaluate compliance with open-textured standards, and it may create uncertainty that disproportionately burdens smaller, less legally resourced entrants. The Financial Stability Board (FSB, 2023) and the Basel Committee on Banking Supervision (BCBS, 2022) have navigated this tension in their crypto-asset frameworks by adopting a hybrid approach: technology-neutral principles at the apex of the regulatory hierarchy, combined with specific rules for identified risk categories such as stable-coin reserve requirements and CASP capital adequacy.

South Africa's crypto-asset regulatory framework, as evidenced by the FSCA's Declaration of Crypto Assets as Financial Products under the Financial Advisory and Intermediary Services Act (FAIS) in 2022 and subsequent draft conduct standards, reflects a predominantly rules-based approach adapted to an inherited legislative architecture designed for traditional financial instruments. Kruger (2023) argues that this creates a category mismatch: rules designed for securities and collective investment schemes cannot map cleanly onto the technical attributes of crypto-assets, producing compliance ambiguity without the adaptive capacity of PBR. For the regulatory design implications of this study, this suggests a need for a hybrid framework that articulates clear, technology-specific rules for high-risk activities (AML/CFT

compliance, consumer disclosures) while preserving principles-based flexibility for emerging use cases in cross-border payments.

2.4.4 Risk-Based Regulatory Approaches

Risk-based regulation (RBR) has become the dominant paradigm of contemporary financial supervision, directing regulatory resources toward those entities and activities that pose the greatest risks to regulatory objectives (Black & Baldwin, 2010). Black and Baldwin's foundational framework identifies five key dimensions of regulatory risk assessment: the probability of harm, the magnitude of harm, the breadth of harm, the vulnerability of those affected, and the responsiveness of regulated entities. This framework has been operationalised by the FATF in its risk-based approach to AML/CFT, which requires jurisdictions and financial institutions to identify, assess, and mitigate the money laundering and terrorist financing risks associated with virtual assets and their service providers (FATF, 2021).

The FATF's 2021 updated guidance on virtual assets is theoretically grounded in risk-based principles: it requires CASPs to conduct risk assessments calibrated to their specific service offerings, customer profiles, and geographic exposures, rather than applying a uniform compliance template. The 'Travel Rule', requiring CASPs to obtain, hold, and transmit originator and beneficiary information for virtual asset transfers above threshold amounts, exemplifies risk-based thinking applied to crypto-asset oversight (FATF, 2021). South Africa's Financial Intelligence Centre (FIC) has incorporated these FATF requirements into its AML/CFT framework, but implementation for CASPs remains nascent, creating a regulatory gap that this study's empirical data illuminates.

A critical limitation of risk-based regulation in the crypto-asset context is what Ringe and Ruof (2020) term 'regulatory volatility': the instability of risk assessments in a technologically dynamic environment creates compliance uncertainty for regulated entities and may discourage investment in innovative remittance solutions. Moreover, Zetsche et al. (2020) argue that risk-based approaches in crypto-asset regulation have exhibited systematic bias toward treating all crypto-assets as high-risk instruments irrespective of their actual risk profiles, thereby over-regulating low-risk stablecoins and

exchange-traded cryptocurrency instruments alongside genuinely high-risk speculative tokens.

2.4.5 *International Regulatory Coordination and Jurisdictional Arbitrage*

The cross-border nature of cryptocurrency transactions renders unilateral national regulation inherently limited in effectiveness, generating substantial scholarly attention to international regulatory coordination mechanisms. Zetsche et al. (2019) develop the concept of the 'Global Financial Regulatory Ecosystem', arguing that effective crypto-asset governance requires coordinated standards across jurisdictions to prevent regulatory arbitrage, the strategic relocation of crypto-asset activities to permissive jurisdictions to evade regulatory requirements. The authors identify three coordination modalities: harmonisation (adoption of common rules), mutual recognition (acceptance of foreign regulatory equivalence), and information sharing (cross-border supervisory cooperation).

The FSB's (2023) high-level recommendations for the regulation of crypto-asset activities and global stablecoin arrangements represent the most significant contemporary attempt at international regulatory harmonisation. By articulating the principle that 'same activity, same risk, same regulation' should govern crypto-assets alongside traditional financial instruments, the FSB recommendations aim to reduce jurisdictional arbitrage while preserving regulatory proportionality. However, Avgouleas and Kiayias (2019) critique this approach as insufficiently attentive to the developmental contexts of emerging economies: applying regulatory standards designed for mature financial systems in jurisdictions like South Africa may disproportionately burden domestic CASPs and obstruct the development of cost-effective remittance infrastructure.

For South Africa specifically, the SARB's participation in the Project Khokha wholesale CBDC experiments and SADC-level discussions on cross-border payment harmonisation indicate an emerging recognition that effective crypto-asset regulation for remittances requires both domestic coherence and regional coordination. Allen et al. (2020) argue that the potential for cryptocurrency-based remittances to reduce the cost of intra-African transfers is contingent on regulatory frameworks that recognise the

multi-jurisdictional character of remittance corridors and develop proportionate, corridor-specific compliance arrangements.

2.4.6 *Institutional Economics and Regulatory Path Dependence*

North's (1990) institutional economics framework, which conceptualises institutions as 'the rules of the game' governing economic interaction, provides a powerful lens through which to analyse the persistence of regulatory arrangements that impose high costs on cross-border remittances. North argues that institutions exhibit path dependence: once established, regulatory frameworks generate constituencies with interests in their perpetuation, creating lock-in effects that resist change even when the original rationale for the rules has eroded.

Applied to South Africa's exchange control framework, institutionalist analysis illuminates why the Currency and Exchanges Act (1933) and its associated regulations, designed to manage capital flows in a post-war, Bretton Woods monetary context, continue to shape cryptocurrency regulation nearly a century later. Acemoglu and Robinson (2012) extend this analysis, arguing that extractive economic institutions persist because they serve the interests of politically powerful incumbents. While South Africa's regulatory modernisation agenda reflects a genuine commitment to institutional reform, the persistence of exchange control restrictions that impede cryptocurrency-based remittances is consistent with institutionalist predictions about the durability of path-dependent regulatory regimes.

Mayer Brown (2019) and Allen et al. (2020) both document the extent to which South Africa's inherited regulatory architecture creates structural barriers to cryptocurrency adoption in remittances. The theoretical contribution of institutionalist analysis here is to explain why technically superior solutions: lower-cost, faster, more transparent, do not automatically displace incumbent systems. Institutional factors, including regulatory frameworks, industry standards, and supervisory expectations, mediate the relationship between technological capability and market adoption.

2.4.7 *Technological Neutrality and Activity-Based Regulation*

A central debate in contemporary financial regulatory theory concerns whether regulation should target technologies (technology-specific regulation) or the activities and risks those technologies enable (activity-based regulation). The principle of technological neutrality, that regulation should not discriminate between technologies performing equivalent economic functions, has been endorsed by the FSB (2023), the IMF (2022), and the BIS Committee on Payments and Market Infrastructures (BIS/CPMI, 2022). Theoretically, technological neutrality prevents regulatory frameworks from becoming obsolete as technologies evolve and avoids creating distortions that advantage or disadvantage specific technological approaches to equivalent financial activities.

Arner, Barberis, and Buckley (2017) argue that the reconceptualisation of financial regulation suggests that the dominant challenge for regulators is not to regulate specific technologies but to regulate the financial activities those technologies enable, irrespective of the technological medium. Their TechFin/FinTech typology, distinguishing between technology companies entering financial services (TechFin) and financial services firms using technology (FinTech), has been adopted by the FSB and multiple national regulators as a framework for activity-based risk assessment. For South Africa's crypto-asset regulatory framework, the shift toward activity-based regulation is evident in the FSCA's 2022 declaration, which subjects crypto-asset service activities to FAIS obligations without prescribing the underlying technology.

Ringe and Ruof (2020) offer a critical perspective on activity-based regulation in the crypto-asset context, arguing that the granularity of activity classifications required to operationalise technological neutrality may generate excessive compliance complexity for novel business models that combine activities traditionally regulated by separate regimes — payments, investment services, and custody, for example. This observation is directly pertinent to cryptocurrency-based remittance providers, whose services may simultaneously engage payment system regulation, foreign exchange controls, CASP authorisation requirements, and AML/CFT obligations, creating a multi-regulator compliance burden that imposes costs disproportionate to the risks involved.

2.4.8 *Critical Synthesis: Regulatory Theory and South Africa's Crypto-Asset Services*

The regulatory theories reviewed in this section collectively illuminate the complex institutional ecology within which cryptocurrency-based cross-border transfer services operate in South Africa. Public interest theory provides the normative justification for regulation but must be calibrated to South Africa's specific public interest priorities, which include financial inclusion and remittance cost reduction alongside systemic stability and AML/CFT compliance. Capture theory alerts researchers and policymakers to the risk that incumbent financial institutions may shape regulatory frameworks in ways that protect their market positions rather than serve the public interest, and the empirical data in this study is analysed with this possibility in mind.

Responsive regulation and sandbox frameworks offer constructive models for engaging with innovative remittance technologies without foreclosing their developmental potential, but their effectiveness is contingent on regulatory capacity and a clear post-sandbox pathway that South Africa's framework has yet to fully articulate. The PBR/RBR debate advises a hybrid approach that provides certainty for compliance-critical activities while preserving flexibility for technological innovation. Risk-based regulation, as embodied in the FATF's virtual asset framework, provides the international standard against which South Africa's AML/CFT architecture for CASPs is measured, revealing significant implementation gaps.

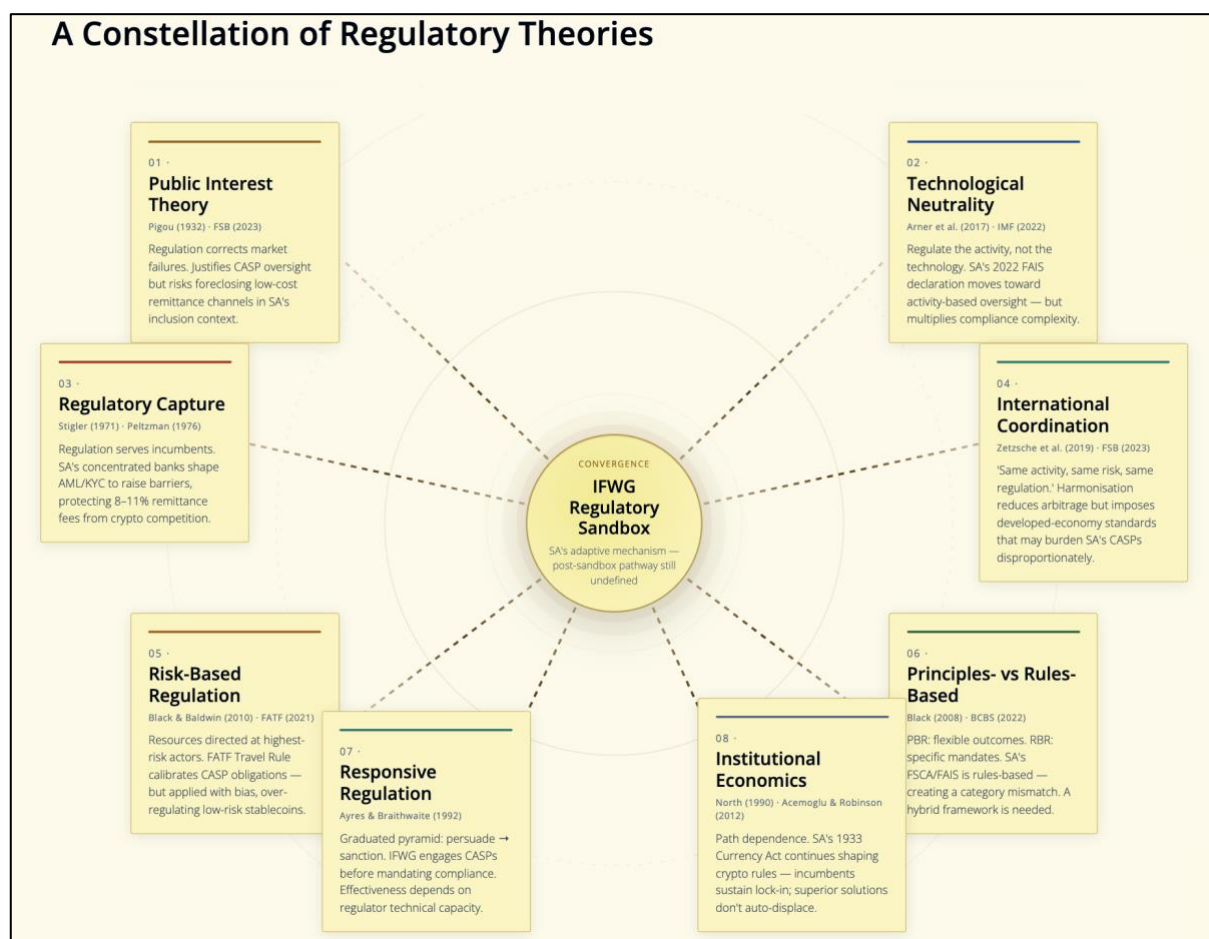


Figure 8. The multitude of regulatory theories governing fintech in South Africa (Researcher diagram)

International coordination and institutional economics perspectives together explain both the drivers of regulatory change and the forces of institutional inertia that resist it, framing the empirical analysis of regulatory challenges and mitigations that forms the core of this study. Finally, activity-based, technologically neutral regulation represents the theoretical gold standard toward which South Africa's evolving crypto-asset framework is moving, even as implementation lags behind the pace of technological and market development.

This theoretical synthesis provides the foundation for the data collection instrument, analytical categories, and knowledge model developed in subsequent chapters. The regulatory challenges identified by interview respondents in Chapter 4 and the knowledge model constructed in Chapter 5 are grounded in and interpreted through this regulatory theory framework, ensuring that the study's empirical contributions are theoretically coherent and capable of informing both policy and practice.

2.4.9 *Caveat emptor on cryptocurrency*

The principle of caveat emptor, which means 'let the buyer beware', is a strong warning that should be considered when evaluating the claims and risks associated with cryptocurrency, especially as it moves from being a new cryptographic concept to a widely used economic system. Many risks attributed to “blockchain” in popular discourse are, in practice, market structure, governance, and regulatory perimeter issues relating to crypto-asset ecosystems, including exchange failures, stable-coin reserve opacity, and decentralised finance (DeFi) protocol vulnerabilities. Although blockchain and cryptocurrency is often praised for its potential to transform digital trust, decentralise power, and enhance transparency in transactions, this excitement tends to overshadow significant legal, technical, economic, and ethical weaknesses. These shortcomings, when not fully understood or managed, may result in substantial risks for end users, regulators, and even entire financial systems. One of the main problems is the uncertainty surrounding the regulations for blockchain projects, particularly those related to cryptocurrency, smart contracts, and Defi. According to Zetsche et al. (2018), blockchain operates in a legal grey area where technological advancements have surpassed regulatory capacities, leading to opportunities for fraudulent activities, market manipulation, and investor exploitation.

The delay in implementing regulations is most noticeable in initial coin offerings (ICOS), which raised billions of dollars between 2016 and 2018 with minimal disclosure requirements and limited investor protection. Numerous of these ICOS eventually collapsed or were exposed as fraudulent, highlighting the risks associated with unregulated financial innovation in blockchain ecosystems. The technical architecture of blockchain further complicates the caveat emptor landscape. Its decentralised and immutable nature, though heralded as a breakthrough in eliminating reliance on intermediaries, paradoxically introduces a lack of recourse when things go wrong. Smart contracts, automated agreements stored on blockchain platforms, represent this dual-edged sword. The automaticity of the system eliminates the need for court intervention or intermediaries to enforce coding rules, but it also means that any coding errors or unintended execution logic can have permanent and irreversible effects. Raskin and Yermack (2016) argue that smart contracts' 'lack of interpretive flexibility

and judicial review' may result in rigid enforcement of unjust outcomes, especially in cases involving asymmetric information or complex contingencies.

A prime example is the 2016 hack of the DAO (decentralised autonomous organisation), which exploited a recursive call vulnerability in a smart contract, resulting in the theft of approximately \$60 million worth of ether, a cryptocurrency. The incident caused a divisive split in the Ethereum blockchain, leading to a reversal of the effects, which challenged the core principles of immutability and decentralisation that blockchain is known for. Furthermore, the concept of decentralisation is frequently deceptive. Numerous blockchain systems display characteristics of oligopoly in governance and control, where a limited group of miners, developers, or platform founders possess significant influence over system regulations and decision-making processes. Walch (2019) observes that 'despite rhetoric of decentralisation, real-world blockchain governance frequently reflects unaccountable and opaque power structures.'

This misalignment between ideology and implementation exacerbates the risks for ordinary users, who may be unaware that the platforms they interact with are effectively governed by centralised actors without democratic oversight. Similarly, end users often lack the technical literacy to audit smart contracts or understand consensus mechanisms, creating conditions of information asymmetry ripe for exploitation by technologically sophisticated actors.

Atzori (2015) cautions that 'technical knowledge barriers and the lack of institutional mediation increase the risk of user disempowerment, rather than empowerment,' challenging the belief that blockchain technology can bring about a utopian society. Environmental issues also emphasise the necessity for prudence. The energy-intensive proof-of-work consensus mechanisms used by bitcoin have raised concerns about their environmental impact, as they require significant electricity consumption and contribute to carbon emissions. According to Truby (2018), the environmental impact of blockchain technology poses a significant threat to its long-term sustainability and conflicts with global climate goals.

As global institutions push toward greener digital economies, the high energy cost of blockchain could become a significant liability, especially for governments or organisations seeking to align digital transformation with sustainable development goals. These environmental costs are often externalised and borne by communities far

removed from the benefits of the technology, adding a layer of environmental injustice to the blockchain debate. Cross-border applications of blockchain, such as in international remittances or supply chain management, further expose legal and regulatory tensions. In the absence of harmonised international legal standards, blockchain can enable regulatory arbitrage, facilitate illicit capital flows, and frustrate AML efforts. Arner, Barberis, and Buckley (2017) highlight that 'without coordinated global oversight, blockchain may erode national regulatory sovereignty and financial stability.' in jurisdictions like South Africa, where exchange control regulations and consumer protection laws are tightly governed, the proliferation of blockchain-based financial products may pose challenges to financial regulators and courts unprepared for decentralised disputes that transcend national boundaries. These risks are not merely hypothetical. Real-world cases have already emerged involving tax evasion, sanction evasion, and cross-border fraud enabled by blockchain anonymity and irreversibility.

Consequently, although blockchain technology has the potential to improve efficiency, transparency, and innovation in various fields, a careful evaluation indicates that its advantages are not guaranteed, and its drawbacks are not evenly distributed. It is crucial for policymakers, investors, developers, and users to approach blockchain with a critical mindset, backed by strong legal protections, comprehensive regulations, and thorough technical assessments. The lack of these structures encourages the very issues blockchain aims to address, opacity, inequality, and systemic risk. Therefore, caveat emptor is not just a cautionary message for individual blockchain users, but a broader warning to societies that embrace technological solutions without thoroughly examining their long-term consequences or establishing the necessary governance structures to ensure accountability, justice, and sustainability.

2.5 Application of innovation theory

Diffusion of Innovation (DOI) Theory (Rogers, 1962) is one of the oldest social science theories and in this dissertation applies to the adoption of cryptocurrency-based financial services by institutions, regulators, and users. Adoption barriers are not primarily technological, but regulatory legitimacy, risk perception, and institutional

compatibility (Rogers, 1962; Arner et al., 2017). The innovation under diffusion is therefore the financial use of crypto-assets, not blockchain infrastructure.

This theory originated in communication to explain how, over time, an idea or product gains momentum and diffuses (or spreads) through a specific population or social system. The end result of this diffusion is that people, as part of a social system, adopt a new idea, behaviour, or product. Adoption means that a person does something differently than what they had previously (i.e., purchase or use a new product, acquire and perform a new behaviour, etc.). The key to adoption is that the person must perceive the idea, behaviour, or product as new or innovative. It is through this that diffusion is possible (Boston University School of Public Health, 2019). The ability to enhance socio-economic development through information communication technology (ICT's) is incrementally diminished by the inability of citizens access to affordable information and communication technologies.

Affordable ICT's are a necessity not only for communication, but also for commerce across the world-wide web. The Diffusion of Innovation (DOI) Theory explains how new technologies spread through societies, influenced by factors such as relative advantage, compatibility, complexity, trialability, and observability. Regarding blockchain adoption for South African cross-border transfers, DOI theory helps analyse why financial institutions and regulators may be slow to embrace blockchain solutions. Factors like regulatory uncertainty, the complexity of integration with existing financial systems, and concerns about compliance with anti-money laundering (AML) laws can hinder adoption. However, addressing these regulatory challenges, through clear guidelines, regulatory sandboxes, and phased implementation, can enhance blockchain's perceived advantages, improve its compatibility with existing frameworks, and accelerate its diffusion in South Africa's financial ecosystem.

Unfortunately, the global digital divide has deepened to include limits on access to mobile broadband services which exacerbates digital and financial exclusion. Frugal innovation is a design innovation process which flows from Innovation theory in which the needs and context of citizens in the developing world are put first in order to develop appropriate, adaptable, affordable, and accessible services and products for emerging markets" Basu et al. (2013). Frugal innovation, often exemplified by the concept of *jugaad*, a Hindi term referring to improvised, resourceful problem-solving, has garnered significant scholarly interest as a means of addressing development challenges in

resource-constrained environments. It embodies a mindset of “doing more with less,” aiming to deliver value through flexible, low-cost, and adaptive solutions tailored to the socio-economic contexts of emerging markets (Radjou et al., 2012). Jugaad innovation is defined as “an innovative fix; an improvised solution born from ingenuity and cleverness” (Radjou et al, 2013).

The six principles of *jugaad* include frugality, flexibility, keep it simple, intuition, opportunity in adversity and include the margin. In general, though, it is described as an unstructured process or mind-set that embodies ‘making do’ in order to come up with an innovative fix. Simply put, frugal innovation corresponds to the formula that “Learning to do more with less for more people should be the innovator’s dream” (Prahalad, Mashelkar, 2010). In this regard, blockchain technology presents a compelling convergence with frugal innovation principles. Although blockchain is often associated with high-tech financial markets, its decentralised, transparent, and secure architecture can be deployed frugally to transform socio-economic systems in the Global South, particularly when coupled with grassroots innovation. Both *jugaad* and blockchain share a common philosophical underpinning: the decentralisation of power and the democratization of access. While *jugaad* seeks to bypass rigid institutional frameworks through ingenuity, blockchain disrupts centralised control by creating peer-to-peer trust networks without reliance on intermediaries (Tapscott & Tapscott, 2016). This synergy enables low-cost, high-trust systems that can operate in environments plagued by institutional inefficiencies, corruption, or infrastructural deficits.

An example of this is blockchain-based land registries in India and Kenya illustrate the fusion of frugal innovation and blockchain. These initiatives enable transparent, tamper-proof record-keeping without requiring expensive proprietary infrastructure (Tenorio, 2021). Similarly, in the realm of financial inclusion, blockchain can facilitate micro-payments, remittances, and identity verification for unbanked populations through low-bandwidth mobile platforms, aligning with the *jugaad* philosophy of leveraging existing resources to meet urgent needs (Narula, 2020). Furthermore, smart contracts, self-executing agreements coded onto the blockchain, can enforce accountability in development aid disbursement, thus minimizing administrative overheads and leakages (Gupta, 2021). Such applications underscore how blockchain, when designed with frugality and contextual relevance in mind, can enhance the resilience and agility of innovation ecosystems in the Global South.

However, the integration of blockchain with *jugaad*-style innovation is not without its challenges. The paradox lies in adapting a relatively complex digital infrastructure to communities that may lack digital literacy, stable electricity, or internet connectivity. Here, frugal innovation offers a pathway: modular, scalable blockchain platforms can be built using open-source protocols and local developer talent to ensure sustainability and adaptability (Chesbrough et al., 2014). Moreover, the co-creation of solutions with local communities ensures that blockchain does not become an imported technological imposition but rather a participatory tool of empowerment.

In conclusion, the convergence of frugal innovation and blockchain heralds a transformative paradigm in technological development, one that resists both the high-cost formalism of traditional innovation systems and the exclusive nature of high-tech globalisation. Rooted in the ethos of *jugaad*, blockchain's implementation in the Global South must prioritise adaptability, inclusivity, and minimalism. Therefore, by harmonising grassroots ingenuity with decentralised digital architecture, policymakers and innovators can unlock new frontiers for equitable and sustainable development.

This concept therefore, underpins blockchain as an innovation which could drive down the costs of cross-border transfer fees. Blockchain is, by its nature, the definition of frugal design. Although it is a very complex system, blockchain is a foundational technology: It has the potential to create new foundations for our economic and social systems. The impact will be enormous, but it will take decades for blockchain to seep into the economic and social infrastructure. The process of adoption will be gradual and steady, not sudden, as waves of technological and institutional change gain momentum (Iansiti, Lakhani, 2017). Blockchain was introduced in October 2008 as part of a proposal for Bitcoin, a virtual currency system that eschewed a central authority for issuing currency, transferring ownership, and confirming transactions (Iansiti, Lakhani, 2017). Jugaad innovation theory is usually discussed in the context of product design. It is the observation that resource-constrained environments produce leaner, more adaptive solutions than well-resourced ones do. Its connection to this study's regulatory argument is less obvious but more important. South Africa does not have the luxury of designing its cryptocurrency regulatory framework from scratch, with unlimited institutional capacity, a clean legislative slate, and years of consultation time. It has the Currency and Exchanges Act of 1933 (amended), a multi-regulator architecture that coordinates imperfectly, a technical skills gap in the agencies that would need to

supervise blockchain markets, and a technology that is changing faster than any legislative process can track.

These are constraints, but jugaad theory reframes them. Constrained environments do not just limit what is possible, they force a kind of clarity about what actually matters. What South Africa needs is not a comprehensive regulatory framework modelled on MiCA, which took years and enormous institutional resources to produce and still does not fully fit an emerging market context. It needs a framework that identifies the minimum foundations. Legal clarity on what a crypto-asset is, proportionate compliance obligations on service providers, enforceable AML and KYC requirements at transaction entry and exit points and builds upward from those, treating each stage as a learning opportunity rather than a final answer. This is exactly what the five-echelon model is designed to do. Jugaad, understood this way, is not just a theory about how blockchain spreads in the Global South. It is a theory about how regulators in the Global South can govern it, adaptively, iteratively, and without pretending that the conditions for perfect regulation will ever exist.

2.6 Application of socio-technical theory to digital solutions for cross-border transfers

The socio-technical theory has at its core the idea that the design and performance of any organisational system can only be understood and improved if both ‘social’ and ‘technical’ aspects are brought together and treated as interdependent parts of a complex system (Leeds University, 2012). Socio-technical systems bring communities of humans together with technology, and some of the most well-known examples of these are large technology companies and platforms. Social media companies such as Facebook, Twitter, and LinkedIn are examples as well as other technology companies such as Apple and Microsoft.

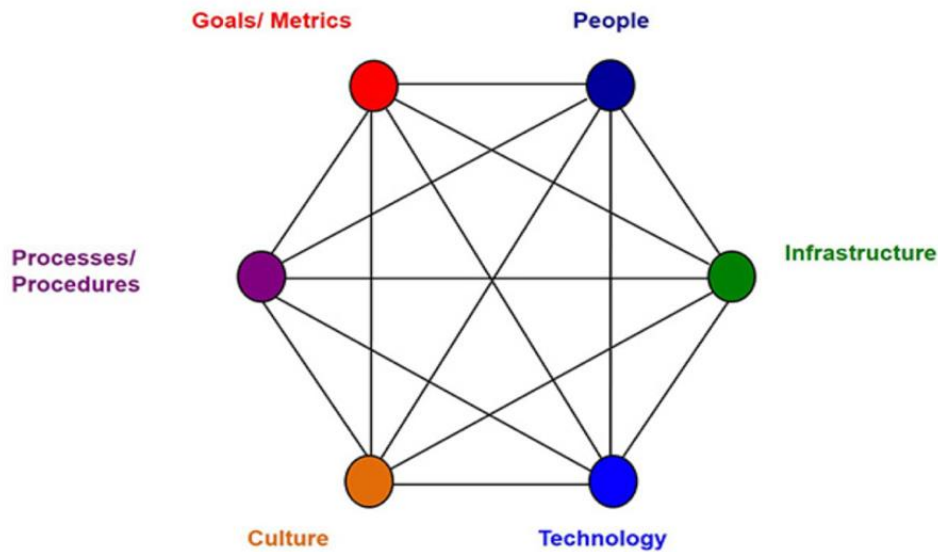


Figure 7. Diagram depicting the interlinking aspects of socio-technical theory

The implementation of blockchain technology can be meaningfully understood through the lens of socio-economic theory, particularly institutional economics and the theory of transaction costs. Blockchain's core proposition, distributed, immutable ledgers, disrupts traditional socio-economic structures by reducing dependency on centralised institutions and intermediaries. From a transaction cost economics perspective, as articulated by Coase (1937) and later expanded by Williamson (1985), institutions exist to minimise the costs associated with economic exchanges, such as search, coordination, and enforcement costs. Blockchain, by enabling peer-to-peer transactions and automated trust through smart contracts, directly lowers these costs, thereby altering the economic rationale for centralised institutions. This decentralisation reshapes the socio-economic power dynamics, reducing asymmetries in information and control and potentially democratizing access to economic participation (Davidson, De Filippi & Potts, 2018).

Furthermore, socio-economic theory's emphasis on the embeddedness of economic activity within social systems (Granovetter, 1985) provides critical insight into blockchain's adoption and utility. The success of blockchain is not merely technological but also hinges on socio-institutional factors such as trust, legitimacy, and governance frameworks. While blockchain is often lauded for its potential to create 'trustless' systems, in reality, its adoption still depends on social constructs of legitimacy and

collective norms (Zohar, 2015). For example, the implementation of blockchain in cross-border financial transfers intersects with national regulatory regimes, monetary sovereignty, and socio-political agendas, which reflects Polanyi's (1944) argument that economic systems are always embedded in broader social and institutional frameworks.

Blockchain also introduces a new form of institutional innovation, what Davidson et al. (2016) refer to as "institutional crypto-economics", where economic coordination is achieved through code rather than legal or bureaucratic processes. This has profound implications for socio-economic development in contexts characterised by institutional voids or inefficiencies, such as in many developing economies. For instance, in sub-Saharan Africa, blockchain has been piloted for land titling and remittance systems, offering alternatives to weak state institutions and high remittance fees (Tapscott & Tapscott, 2016). However, the transformative potential of blockchain must be critically evaluated against existing socio-economic inequalities and digital divides, which may limit its inclusivity and scalability (Atzori, 2015). Therefore the intersection of socio-economic theory and blockchain implementation reveals a complex dynamic where technology reconfigures institutional structures, yet remains shaped by social, political, and economic contexts. A nuanced socio-economic understanding is essential to harness blockchain's potential for inclusive and sustainable development.

It is within these parameters of social-technical theory that the researcher analysed the regulatory challenges and mitigations of blockchain technology on cross-border payments and its impact on the South African financial regulatory system. The implication is that understanding and improvement requires the input of all key stakeholders, including those who work within different parts of the system. 'User participation' thereby is a pre-requisite for systemic understanding and change and, in this perspective, the term 'user' is broadly defined to include all key stakeholders. Socio-technical theory offers insights into the interplay between technical and social factors in implementing a blockchain solution for cross-border transfers in South Africa. This perspective underscores the significance of balancing technical elements (like blockchain technology itself) with social elements (such as regulatory frameworks and stakeholder engagement) for successful implementation and adoption.

Socio-technical systems perspective: From a socio-technical systems perspective, cryptocurrency payment ecosystems represent the interaction of technological

infrastructure with financial institutions, regulatory bodies, market actors, and users. Regulatory integration occurs at the service-provider and transaction layer, not at the protocol layer. This distinction is central to understanding the limits of regulatory reach and the emergence of RegTech, Travel Rule compliance, and blockchain analytics as supervisory tools (BIS, 2023; Zetzsche et al., 2018).

Regulatory frameworks as social components: Existing regulations governing cross-border transfers play a vital role in shaping the environment for cryptocurrency solutions. They influence the design, implementation, and adoption of such solutions.

Stakeholder engagement and alignment: Involving and aligning stakeholders, including regulators, financial institutions, and end-users, is essential for addressing regulatory challenges and ensuring successful adoption.

Organizational and cultural factors: Implementing a cryptocurrency solution may necessitate changes in organisational structures and cultural norms within regulatory bodies and financial institutions. Considering these factors facilitates smooth integration with existing social systems.

User adoption and acceptance: The success of a blockchain solution hinges on user adoption, influenced by factors like usability and perceived benefits. Addressing these social factors is crucial for ensuring acceptance and utilization.

Continuous adaptation and feedback loops: Socio-technical theory underscores the need for ongoing adaptation and feedback between technical and social components. As regulations evolve and stakeholder needs change, the blockchain solution must adapt accordingly. By adopting a socio-technical perspective, the researcher can better understand and tackle the regulatory challenges associated with implementing blockchain solutions for cross-border transfers. This approach acknowledges the interconnectedness of technical and social elements, enabling a more comprehensive and effective strategy for leveraging blockchain technology's potential.

2.7 Benefits of Blockchain in cross-border transfer fee reduction

Blockchain technology has gained significant attention in recent years due to its potential to revolutionise various industries, including finance and remittances. This comprehensive literature review aims to provide an in-depth analysis of existing research and scholarly works on blockchain technology and its application in reducing remittance fees. The review explores the benefits, challenges, regulatory

considerations, and potential future developments in utilising blockchain for cost-effective remittance transactions. Several studies highlight the potential benefits of blockchain technology in reducing remittance fees. According to Yao et al. (2019), blockchain-based remittance systems can provide faster, cheaper, and more secure cross-border transactions. By eliminating intermediaries and utilising smart contracts, blockchain enables direct peer-to-peer transfers, resulting in reduced fees and enhanced transactional efficiency.

Transparency and Trust: Blockchain technology offers transparency and immutability, which are key factors in reducing remittance costs and improving trust among respondents. Bhagat et al. (2020) emphasise that blockchain provides a decentralised ledger that records all transactions in a transparent and tamper-resistant manner. This transparency fosters trust and reduces the risk of fraud or unauthorised alterations to transaction records.

Cost Reduction: The potential for cost reduction is a significant advantage of cryptocurrency blockchain-based remittance systems. The elimination of intermediaries and the use of smart contracts can significantly reduce transaction fees. The World Bank (2018) suggests that blockchain technology can eliminate intermediary fees, resulting in reduced costs for remittance senders and recipients. Mallick et al. (2020) further highlight that blockchain-enabled remittance systems could potentially lower costs by up to 90%.

Speed and Efficiency: Blockchain technology enables real-time transaction verification and settlement, leading to faster remittance processes compared to traditional methods. Ali et al. (2019) state that blockchain-based remittance systems can expedite cross-border transactions by eliminating time-consuming intermediaries and manual processes. This increased efficiency can provide faster access to funds for recipients, particularly in regions where traditional remittance channels may be slow or unreliable.

Security and Fraud Prevention: Blockchain technology offers enhanced security measures that can mitigate the risk of fraud and unauthorized activities in remittance transactions. Bano et al. (2019) emphasise that blockchain's cryptographic techniques and consensus mechanisms ensure the integrity and immutability of transaction records. Additionally, the decentralised nature of blockchain reduces the vulnerability to single points of failure, enhancing the overall security of remittance processes.

Challenges and Limitations: While blockchain technology offers potential benefits, several challenges and limitations need to be addressed. Scalability remains a primary concern, as the current blockchain infrastructure may struggle to handle the high transaction volumes required for remittances (Zavolokina et al., 2019). Regulatory frameworks and legal considerations also present challenges for the widespread adoption of blockchain-based remittance systems. Ali et al. (2019) highlight the need for regulatory clarity and the development of appropriate frameworks to address issues related to identity verification, consumer protection, and AML/KYC compliance.

Regulatory Considerations: The adoption of blockchain technology in remittance systems requires a supportive regulatory environment. Governments and regulatory bodies are actively exploring the integration of blockchain and digital currencies. Biswas et al. (2020) suggest that the collaboration between regulators, financial institutions, and technology providers is crucial to establishing regulatory frameworks that ensure compliance, consumer protection, and interoperability.

Future Directions: Future research and development efforts should focus on addressing the challenges and maximizing the potential of blockchain technology in reducing remittance fees. Scalability solutions, such as layer-two protocols and off-chain scaling techniques, should be explored to improve transaction processing capabilities (Zavolokina et al., 2019). Furthermore, the integration of blockchain with emerging technologies, such as central bank digital currencies (CBDCs) and stablecoins, holds promise for revolutionising remittance processes and further reducing costs.

The literature review demonstrates that crypto-asset transaction models reduce intermediary layers and settlement latency through:

- Stablecoin settlement
- Exchange liquidity pools
- Wallet-to-wallet transfers
- Automated clearing

by enabling cost-effective, secure, and efficient cross-border transactions IMF (2022), BIS (2023), FSB (2023). The benefits of transparency, trust, cost reduction, speed, and security have been extensively studied. However, challenges related to scalability,

regulatory frameworks, and legal considerations require further attention. Future research should focus on addressing these challenges, developing scalable solutions, and fostering collaborations among industry stakeholders, policymakers, and regulators to unlock the full potential of blockchain in reducing remittance fees.

2.8 Gaps in existing literature and contribution of study

As blockchain and cryptocurrency technology gains attention as a potential solution for reducing cross-border transfer fees, it is important to identify the literature gaps that exist in this field. Several key areas require further exploration and research:

Scalability and Performance: Blockchain networks face scalability challenges in terms of transaction speed and volume. Studies should investigate the scalability of blockchain platforms and propose solutions to handle the large-scale transaction volumes required for remittances (Zheng et al., 2018).

Cost-effectiveness and Efficiency: While blockchain has the potential to reduce cross-border transfer fees, it is essential to conduct empirical studies to assess the cost-effectiveness of implementing blockchain-based remittance systems. This includes evaluating transaction costs, network fees, and the overall economic impact of adopting blockchain technology for remittances (Barber et al., 2012; World Bank, 2021).

User Experience and Adoption: Understanding the user experience and factors influencing the adoption of blockchain-based cross-border transfer platforms is critical. Research should investigate user preferences, usability challenges, and design interfaces that promote user-friendly experiences to facilitate widespread adoption (Shin, 2018; Fan et al., 2021).

Regulatory and Legal Frameworks: The regulatory landscape for cryptocurrency is evolving rapidly. Further research is needed to analyse the regulatory implications, compliance requirements, and legal frameworks governing cryptocurrency-based cross-border transfer. This includes exploring issues related to AML and KYC regulations, consumer protection, and jurisdictional considerations (Chiu et al., 2018; Liu et al., 2019).

Privacy and Security: As blockchain transactions are transparent and traceable, privacy and security are important considerations. Researchers should investigate privacy-enhancing techniques, cryptographic protocols, and data protection

mechanisms to ensure secure remittance transactions while maintaining privacy (Zyskind et al., 2015; Suiche, 2018).

Interoperability and Standardisation: Blockchain interoperability and the establishment of industry-wide standards are vital for seamless integration and collaboration among different blockchain platforms. Research should focus on developing interoperability protocols, consensus mechanisms, and standardised approaches to enable cross-border remittances (Conoscenti et al., 2016; Saberi et al., 2019). The literature reviewed includes diverse arguments linking remittances to financial development, although most lean toward their potential to enhance financial inclusion, especially for the unbanked, lowest-income earners in developing countries (Misati et al. 2019). One theory linking cross-border transfers and financial development is anchored in the financial literacy hypothesis. Proponents of this hypothesis argue that both remittance senders and recipients create a demand for the financial systems involved in international remittances, which can incentivise either or both parties to seek and interact with the financial institutions involved in other financial products beyond remittances (Misati et al. 2019). This literature review assesses various views of authors regarding South African financial regulations regarding remittances and the possible effects the introduction of blockchain technology will have. There are several gaps in the existing literature regarding the use of blockchain for remittances. While there have been a number of studies and reports on the potential benefits of blockchain for remittances, there is a lack of empirical research on the actual usage and adoption of the technology. This makes it difficult to understand the real-world impact of blockchain on the remittance industry. There is limited research on the specific legal and regulatory frameworks that are needed to support the use of blockchain for remittances in South Africa. Furthermore, with the emerging and changing regulatory environment, it is difficult to keep track of the current state of regulations globally.

There is a need for more research on the scalability and interoperability of blockchain-based remittance systems. As the number of users and transactions increase, it is unclear how well these systems will be able to handle the volume, and if they will be able to connect with other remittance systems and financial institutions. Despite the hype, there is still a lack of conclusive evidence and research on the extent to which blockchain-based remittances can actually reduce costs. While a lot of attention has been focused on the technical aspects of blockchain-based cross-border payments,

there is limited research on how easy these systems are to use and how they compare to traditional cross-border payments methods in terms of user experience.

In summation, there is a clear need for more research to fully understand the potential of blockchain for cross-border transfers, as well as how to best design and implement these systems in order to provide benefits for all stakeholders. As there is no clear evidence to substantiate the promises of blockchain technology, this dissertation aims to fill the research gap by further exploring South Africa's regulatory environment and the likely impact blockchain will have and provide an overview to develop a clearer understanding of what blockchain and cryptocurrency offers. This body of knowledge links cross-border transfers, blockchain technology and cryptocurrency in South Africa's fiscal regulatory space and the potential effect the three exert on each other in terms of the reduction of remittance fees in South Africa.

CHAPTER 3

RESEARCH METHODOLOGY

Chapter Overview

This chapter outlines the research philosophy, methodology, and methods employed in this study. It establishes the qualitative research approach adopted to investigate the regulatory challenges and mitigations associated with cryptocurrency and crypto-asset systems used in cross-border financial transfers in South Africa. While blockchain technology provides the underlying infrastructure for cryptocurrency, it is not itself the object of financial regulation. Regulatory frameworks apply to crypto-assets, financial activities, and service providers, rather than to distributed ledger technology as a neutral infrastructure (FATF, 2021; FSB, 2023).

The chapter details the study's ontological and epistemological foundations, justifies the selection of purposive sampling, and explains the use of inductive thematic analysis. Ethical considerations and quality assurance procedures are also described to demonstrate the rigour of the study.

3.1 Philosophical assumptions underpinning the study

Ontology

Ontology concerns the nature of reality and what exists in the social world (Marsh & Furlong, 2002; Mouton, 1996). In regulatory and financial research, ontological assumptions relate to how financial systems, institutions, and technologies are understood as social constructs embedded within legal and economic structures.

This study adopts a constructivist ontological position, recognising that financial regulatory systems, technological innovation, and market practices co-evolve through institutional and policy interactions. Cryptocurrency is therefore not treated merely as a technical artefact, but as socio-economic instruments whose meaning, risks, and legitimacy are shaped through regulatory discourse and financial governance structures.

The ontological foundation of using cryptocurrency in cross-border transfers rests on several assumptions:

1. Disintermediation of financial value transfer – cryptocurrency networks enable peer-to-peer or wallet-based settlement, reducing reliance on correspondent banking chains (Nakamoto, 2008; Swan, 2015).
2. Programmable financial architecture – smart contracts and tokenised settlement introduce new forms of financial automation.
3. Transparency and traceability – public ledgers allow transaction monitoring through blockchain analytics, which regulators increasingly use for AML/CFT compliance (BIS, 2023).
4. Financial inclusion potential – crypto-asset systems may offer access to digital financial services in contexts where banking penetration is limited (World Bank, 2018; IMF, 2022).

Thus, the reality under investigation is not “cryptocurrency regulation,” but the interaction between crypto-asset ecosystems and existing financial regulatory systems.

Epistemology

Epistemology addresses how knowledge about this reality is generated (Crotty, 1998; Carson et al., 2001). This study adopts an interpretivist epistemology, recognising that regulatory practices, risk perceptions, and policy decisions are socially constructed and best understood through expert interpretation.

Knowledge is therefore derived from expert experience within the financial regulatory and fintech sectors. Respondents are viewed as holders of situated knowledge regarding:

- Crypto-asset regulatory compliance
- Exchange control implications
- AML/CFT supervision
- Payment system governance

Their insights provide interpretive understanding rather than statistical generalisation.

3.2 Research Approach

This study adopts a qualitative research design to explore the experiences and perspectives of government officials and financial industry experts regarding the integration of cryptocurrency technology into fiscal regulatory frameworks. Qualitative research is particularly suited to inquiries that seek to understand the meaning and experiential dimensions of social phenomena, emphasising participants' subjective interpretations, actions, and contexts (Fossey et al., 2002). By employing this approach, the research aims to generate rich, detailed insights into the motivations, challenges, and decision-making processes associated with blockchain adoption in regulatory environments. Such depth of understanding is critical for informing policy development and implementation strategies that are both context-sensitive and practically viable.

Unlike quantitative methods, which focus primarily on numerical patterns, qualitative inquiry enables a holistic and nuanced examination of complex issues, uncovering underlying drivers and barriers that may not be evident through statistical analysis alone (Fossey et al., 2002). This study therefore prioritises in-depth interviews with South African experts from both public and private sectors, including those involved in blockchain-based remittance and compliance initiatives. These interviews illuminated diverse viewpoints and provide a comprehensive understanding of the opportunities and constraints shaping blockchain's role in fiscal regulation. Ultimately, the qualitative approach facilitates the identification of emergent trends and patterns, offering actionable recommendations for effective and sustainable implementation of cryptocurrency technology in the regulatory domain.

This study researches the regulatory challenges and mitigations of a cryptocurrency solution on cross-border payments and its impact on the South African financial regulatory system and whether a cryptocurrency solution could offer a reduction in remittance fees and its impact on the South African financial regulatory system. This problem-statement requires analysis from a multiple stakeholder perspective in order to understand the history, the current state, and where or how in the future the blockchain technology could disrupt or support the cross-border transfer industry.

Characteristics of Qualitative Research



Figure 8. Characteristics of Qualitative Research by Bunmi Malau-Aduli and Faith Alele

3.3 Research Design

Research design refers to the overall structure and plan that guides the process of conducting a research study. It encompasses the methodology, data collection methods, and analytical techniques used to address research questions and objectives. A well-designed research study ensures that the research process is systematic, rigorous, and capable of producing valid and reliable results. According to Creswell (2014), research design is the "plan, structure, and strategy of investigation used to obtain evidence to answer a research question." It involves making decisions about the research approach, data collection methods, sampling strategy, and data analysis techniques. Various research paradigms and methodologies influence research design. For example, quantitative research designs focus on collecting and analysing numerical data to establish patterns and relationships, while qualitative research designs emphasise in-depth exploration of meanings, experiences, and perceptions (Creswell, 2014).

3.3.1 Research methods

According to Creswell (2014), there are five main types of research methods:

qualitative, quantitative, mixed-methods, arts-based, and action research. Each method has its own unique features and is suited to different types of research questions. An example would be that qualitative research is often used to explore and understand people's experiences, perspectives, and behaviours, while quantitative research is used to test hypotheses and measure relationships between variables. A researcher should carefully consider the research question and the goals of the study when choosing the most appropriate research method.

Additionally, they should also ensure that the research design is well-planned and executed to ensure the reliability and validity of the results. The strength of qualitative research is its ability to provide complex textual descriptions of how people experience a given research issue. It provides information about the “human” side of an issue such as the often contradictory behaviours, beliefs, opinions, emotions, and relationships of individuals. Qualitative methods are also effective in identifying intangible factors, such as social norms, socioeconomic status, gender roles, ethnicity, and religion, whose role in the research (Mack et al 2002).

3.3.2 *Data Collection Method*

Semi-structured interviews are employed in this study because this method has a pre-planned set of core questions for consistency among respondents, and also allows respondents to further elaborate or provide more relevant information as the interview progresses (Yohannan, 2010). Semi-structured interviews are commonly used in qualitative research as they allow the researcher to explore a topic in-depth and understand the participant's perspective on the issue (Bryman, 2012). Semi-structured interviews play a crucial role in qualitative research, offering a level of flexibility that allows for deeper exploration of topics. Unlike rigidly structured interviews, they encourage open-ended discussions where participants can share their thoughts more freely, leading to richer, more detailed insights. This format helps researchers uncover perspectives that might otherwise be missed, making it easier to understand participants' experiences in a meaningful way. Another major advantage is the ability to build a natural rapport with interviewees. Since the conversation flows more organically, participants often feel more comfortable opening up, which can lead to more honest and in-depth responses. This approach is especially useful in exploratory research, where the goal is not just to collect answers but to uncover new ideas and patterns. In addition, semi-structured interviews work well alongside other research methods. They can help

clarify findings from surveys or experiments, offer deeper context to quantitative data, and provide a well-rounded understanding of a subject. By combining structure with flexibility, this method remains one of the most effective tools for capturing the complexity of human experiences in research. Semi-structured interviews are also useful in situations where the researcher is looking to gather rich, detailed data about a specific topic or issue (Saldaña, 2015). The flexible nature of the interview process allows the researcher to adapt to the participant's responses and explore relevant topics as they arise. Another advantage of interviews is that the rate of non-responses is low and it can obtain in-depth information (Kothari, 2004).

3.3.3 *Population and Sample*

This research paper incorporates semi-structured interviews with experts in the public and commercial financial regulatory space, blockchain technology and cryptocurrency. This allowed for detailed data collection processes and produced a holistic view of the fintech regulatory and blockchain ecosystem.

Blockchain has been the focus of very few academic papers, and their study is an essential part of research and the theory-building process in this field, in order to fill the gaps between theory and practice, which are especially relevant given that the blockchain and cryptocurrency is an industry in its nascent inception. It is for this reason that the qualitative approach is the most relevant to this research paper.

Purposive sampling is a type of sampling method that is used when researchers have a specific purpose or research question in mind and want to study a specific group of people or cases in depth. This type of sampling is often used in qualitative research and is chosen because it allows the researcher to study a particular group of people or cases that are particularly relevant to their research question (Creswell, J. W. 2018). One of the main advantages of purposive sampling is that it allows researchers to study a specific group of people or cases in depth, which can provide a more nuanced and detailed understanding of the research topic. Additionally, purposive sampling is often used when the population of interest is small or hard to access, as it allows researchers to focus on a specific group of people or cases that are easier to study (Creswell, J. W. 2018).

The choice of purposive sampling in this study is informed by the sample size which is small and by the common characteristics that the respondents have. Respondents who

were interviewed are people who are knowledgeable about the topic of interest and experts from government institutions and financial corporate institutions. Furthermore, data was collected using qualitative data sources, namely in depth interviews, which provided primary data for the study.

3.4 Interview protocol, guides the semi-structured interviews

The interview protocol details the specific guidelines and procedures that were followed during an interview as part of this research study. A well-defined protocol ensures the reliability and validity of the data being collected. De Vaus (2002) states that an effective interview protocol should include the following elements:

1. A clear set of objectives: The purpose of the interview should be clearly defined in advance, and the questions should be designed to elicit the information needed to achieve these objectives.
2. A structured interview guide: The interviewer should have a list of predetermined questions to ask the participant, as well as a plan for probing for more information if necessary.
3. Standardised procedures: The interviewer should follow a consistent approach when conducting the interviews, including using the same tone of voice and body language.
4. Training for the interviewer: The interviewer should be well-trained in the specific research topic and should have a thorough understanding of the interview protocol.
5. Ethical considerations: The interviewer should ensure that the participant's rights are protected, including obtaining informed consent and maintaining confidentiality.

A well-defined interview protocol is therefore crucial for ensuring the reliability and validity of the data being collected in research. It helps to ensure that the interviews are conducted in a consistent and standardised manner, allowing for more accurate and meaningful results.

3.5 Data Collection

Respondents in this study were given a participant information sheet which outlines what is being done, the aim of the study, what is it that is required from them, explanation of the data collection method and details of the researcher and their supervisor (Yohannan, 2010). The participant information sheet also informed the respondents that their identities and personal identifying information would not be revealed and that the data collection and analysis methods maintained the participant's confidentiality. Additionally, the participant information sheet assured the respondents that data collected from the study is kept in a safe place. Respondents were required to sign a consent form where they agree to participate in the study and also to indicate where they choose to agree or disagree to their participation remaining anonymous as well as choosing to agree or disagree to their information being used anonymously for other academic research projects subject to ethics clearance being obtained by those researchers. The interviews with the respondents who agreed to participate in this research was conducted between July and December 2024.

The 8 interviews were conducted in English and lasted between 45 and 90 minutes. Interviews was conducted online due to differences in geographic location. Online communication tools such as Zoom, Jitsi.Meet and Microsoft Teams was used to conduct the interviews. To ensure the quality and accuracy of the data, the interviews was recorded using an internal recording feature from online communication tools. Subsequently, the audio file was saved and transcribed with the guidance of the transcription application Zamzar and Turboscribe for those conducted in English via Zoom, and those conducted via Microsoft Teams were automatically transcribed by the transcription's native feature.

3.6 Ethical Considerations

Ethical considerations were carefully adhered to during this qualitative study. As outlined by (Bryman, 2012), ethical risks to respondents include lack of informed consent, invasion of privacy, and deception. To mitigate these risks, all respondents provided informed consent prior to the start of the study, agreeing to participate voluntarily. Their privacy and the confidentiality of the data collected were fully protected throughout the process. Additionally, to ensure the integrity and objectivity

of the research, the interviewer remained neutral and avoided any bias during the interviews, with no prior relationships to any of the respondents. In line with Bryman's principles, respondents were informed about their rights, including the voluntary nature of their involvement, the confidentiality and anonymity of their data, and the purpose of the study. The consent form provided clear information on how the data would be used and the respondents' rights before, during, and after the interviews. To uphold the anonymity and confidentiality of the respondents, each individual was assigned a distinct identifier (e.g., Respondent R1, R2, R3). This measure was designed to protect the privacy of respondents and prevent the disclosure of their identities in the final research report. In accordance with the university's research guidelines, respondents completed and signed the required permission letters. This formalised process underscored their consent to contribute to the study and their support for academic research endeavours. Additionally, to safeguard the confidentiality of the organisations involved, institutional names were not disclosed in the final report. Generic descriptors were used to reference the organisations, ensuring their identities remained protected.

3.7 Research Data Analysis

Qualitative data generated from interviews was analysed using the inductive data analysis method, where specifically collected data is analysed to form general concepts. Inductive data analysis is a method of analysing research data that involves starting with specific observations and working towards more general theories and explanations (Creswell, J. W. 2018). This method is often used in qualitative research, where the goal is to understand and interpret complex social phenomena. To use the inductive data analysis method, researchers first gather and collect data through methods such as in-depth interviews, focus groups, or observations. This data is then carefully reviewed and coded, with the researcher identifying patterns, themes, and relationships within the data. These patterns and themes are used to generate hypotheses and theories about the phenomenon being studied. One of the key features of inductive data analysis is that it is an iterative process, with researchers continually reviewing and revising their theories and explanations as they gather and analyse more data (Bryman, 2012). This allows researchers to build a more complete and nuanced understanding of the phenomenon being studied. Overall, the inductive data analysis method is a useful tool for researchers looking to understand and interpret complex social

phenomena. By starting with specific observations and working towards more general theories and explanations, researchers can build a rich and detailed understanding of the experiences, perspectives, and meanings of those being studied (Bryman, 2012). In this study, thematic analysis was used to analyse the collected data following Creswell's six-step process [40]: organising and preparing the data, initial reflection, coding, identifying themes and descriptions, linking themes and descriptions, and making final interpretations. The raw interview data were first organised and transcribed, with the transcripts reviewed multiple times to ensure accuracy and comprehension. The audio recordings were replayed to verify the accuracy of the auto-transcriptions from Zamzar and Turboscribe. Atlas.ti was utilised as the qualitative analysis tool, and a word frequency query was employed to gain a visual representation of the data. The transcribed data were then coded, broken into similar segments, and categorised. Unnecessary information within the identified categories was also reviewed and removed.

In line with Bryman's approach, the analysis focused on recurring topics across multiple interviews, identifying both similarities and differences between them to develop themes. Table A1 illustrates the identified themes and coding structure. Respondents' answers were analysed, and keywords were used to find commonalities between responses. These keywords were highlighted to aid in identifying themes, which were then used to categorise the responses accordingly.

3.8 Researcher Positionality and Reflexivity

This study adopts a qualitative design based on elite interviews with financial regulatory professionals operating within South Africa's fintech and financial services ecosystem. In line with established qualitative research practice, reflexivity requires the researcher to critically examine how their professional background, institutional location, and prior assumptions may shape the research process (Creswell & Creswell, 2018).

The researcher occupies a professional position adjacent to the fintech and digital innovation environment within South Africa. This proximity facilitated access to high-level participants, including regulatory officials and industry experts, who may otherwise have been difficult to recruit. Existing professional networks likely enhanced trust and reduced gatekeeping barriers, enabling candid engagement during interviews.

However, this positionality also introduced potential risks: participants may have assumed shared knowledge, moderated criticism of regulatory institutions, or framed responses strategically based on perceived alignment. Furthermore, the researcher's familiarity with regulatory discourse and fintech innovation could predispose interpretation toward reform-oriented or innovation-supportive conclusions.

To mitigate these risks, several safeguards were implemented. First, interview questions were structured to remain open-ended and neutral, avoiding leading language that presupposed regulatory inadequacy or technological superiority. Second, reflexive memoing was employed throughout the data collection and analysis phases to document emerging assumptions and bracket preconceptions. Third, thematic coding was conducted iteratively, with deliberate attention to disconfirming evidence and contradictory perspectives. The analysis therefore prioritised participant voice over prior professional experience.

By explicitly acknowledging positionality and implementing methodological safeguards, the study aligns with Creswell and Creswell's (2018) guidance that qualitative researchers must situate themselves transparently within the research context while demonstrating systematic efforts to preserve analytical integrity.

3.9 Limitations and challenges of the study

3.9.1 *Limited Scope of the Study*

The research focuses specifically on the regulatory challenges and mitigations of cryptocurrency technology for cross-border payments in South Africa. While this geographic focus allows for in-depth analysis, it limits the generalisability of the findings to other countries or regions with different regulatory frameworks. Cryptocurrency regulation is highly dependent on national legal systems, so conclusions drawn for South Africa may not apply to jurisdictions with more developed or less stringent regulatory environments.

3.9.2 *Qualitative Methodology and Subjectivity*

The study primarily relies on a qualitative research approach, which includes interviews with stakeholders in the blockchain and financial sectors. While this provides rich

insights, it may also introduce subjectivity and bias. Respondents' views could be shaped by personal or organisational interests, which may not reflect the broader industry consensus. Furthermore, the interpretation of interview data, especially in thematic analysis, relies heavily on the researcher's understanding, potentially introducing interpretive bias.

3.9.3 *Limited Number of Interview Respondents*

The number of interview respondents could be a limitation, especially if the sample size is small. A limited number of interviewees may not fully capture the diversity of views in the blockchain and financial sectors. As a result, the study may miss important perspectives from other industry players, regulators, or global stakeholders, which could impact the comprehensiveness of the conclusions drawn.

3.9.4 *Evolving Nature of Cryptocurrency Technology and Regulation*

Cryptocurrency technology and its regulatory frameworks are rapidly evolving. The conclusions of the dissertation may become outdated as new regulations are implemented or as the technology itself undergoes advancements. Cryptocurrency is a dynamic field, and regulatory responses are continually being updated, particularly as countries learn from one another's experiences. This evolving landscape could limit the long-term relevance of the findings.

3.9.5 *Lack of Quantitative Data*

The absence of a quantitative component limits the study's ability to provide empirical evidence supporting the interview findings. For example, statistical data on the number of cryptocurrency-based cross-border transactions, or quantitative measures of the costs and efficiency of these transactions compared to traditional methods, could enhance the rigour of the conclusions. Without such data, the study remains primarily

qualitative, which may limit its appeal to policymakers or practitioners who prefer data-driven insights.

3.9.6 *Complexity of Cross-Border Payment Systems*

Cross-border transfers are inherently complex, involving multiple stakeholders, including governments, central banks, private financial institutions, and international organisations. The study's focus on blockchain may not account for the full scope of these complexities, particularly the roles of intermediaries like correspondent banks or the challenges posed by currency exchange fluctuations. These external factors could limit the study's ability to provide a holistic solution for cross-border payments, beyond blockchain-specific mitigations.

3.9.7 *Technological and Regulatory Lag*

This dissertation explores the regulatory environment for cryptocurrency, but it is possible that the technology will advance more quickly than the regulatory frameworks can adapt. This technological-regulatory lag may mean that some of the regulatory challenges discussed in the dissertation will become outdated or irrelevant as new cryptocurrency innovations emerge, potentially limiting the study's foresight into future developments.

3.9.8 *Ethical and Privacy Concerns*

Blockchain's inherent transparency and immutability may raise ethical and privacy issues, particularly regarding compliance with South Africa's Protection of Personal Information Act (POPIA). While the study discusses regulatory mitigations, it may not fully address the long-term privacy risks associated with cryptocurrency adoption. The evolving intersection between privacy, data security, and cryptocurrency technology could present limitations in understanding how these factors will be managed within South Africa's regulatory landscape.

3.9.9 *Lack of Comparison with Traditional Systems*

The study focuses on cryptocurrency as a solution for cross-border payments, but it may lack a comparative analysis with traditional payment systems. Understanding the strengths and weaknesses of blockchain versus conventional systems, such as SWIFT or correspondent banking, could provide more pertinent insights.

3.9.10 *Technological Rapid Evolution*

The fast-paced nature of cryptocurrency technology means that findings may quickly become outdated as new developments emerge. The dissertation may not account for future innovations or adaptations in cryptocurrency technology that could address existing regulatory challenges. Additionally, evolving best practices and standards in the cryptocurrency industry could influence regulatory approaches, which may not be captured within the scope of this research.

3.10 Quality Assurance

Quality assurance is a cornerstone of qualitative research, ensuring that findings from the study on cryptocurrency solutions for South African cross-border transfers are credible, transferable, dependable, confirmable, and ethically sound. By addressing the following quality assurance issues, the researcher can produce reliable insights that contribute significantly to understanding regulatory challenges and the potential mitigations in this emerging field.

3.10.1 *Credibility*

Credibility is crucial for establishing the truthfulness of the findings. In this study, credibility can be enhanced through methods such as member checking, where respondents validate the findings, and prolonged engagement with respondents to foster trust. “Credibility can be enhanced through member checking and prolonged engagement, allowing researchers to establish rapport and deeper insights” (Creswell, 2013).

3.10.2

Transferability

Transferability refers to the applicability of findings to other contexts. By providing rich descriptions of the South African financial landscape and the specific challenges of cryptocurrency adoption, the researchers enable readers to determine the relevance of the findings to their contexts. “Providing thick descriptions allows readers to assess the transferability of findings to other settings” (Lincoln & Guba, 1985).

3.10.3

Dependability

Dependability concerns the consistency of data over time. In this study, maintaining an audit trail, documenting all research decisions, and the iterative process of data collection and analysis can ensure dependability “An audit trail contributes to the dependability of qualitative research, allowing for an external review of the research process” (Creswell, 2013).

3.10.4

Confirmability

Confirmability involves ensuring that findings are shaped by respondents rather than researcher bias. Researchers should engage in reflexive practices, such as keeping journals, to track their thoughts and potential biases throughout the study “Reflexivity is critical in qualitative research to minimise researcher bias and enhance the confirmability of findings” (Finlay, 2002).

3.10.5

Researcher Bias

The potential for researcher bias necessitates awareness of how the researchers' values and experiences may influence the study. Acknowledging positionality helps in recognising and addressing these biases. “Researchers should acknowledge their positionality and how it might influence their interpretations” (Schwartz-Shea & Yanow, 2012). The methodological choices in this chapter are directly aligned with the three-dimensional analytical framework introduced in Chapter 1, which examines regulatory challenges, mitigation approaches, and embedded compliance in relation to

cryptocurrency-based cross-border transfers in South Africa. Because these dimensions concern institutional tensions, interpretive ambiguity, and the gap between written regulation and practical implementation, a qualitative design, particularly semi-structured interviews with purposively selected regulators and financial sector experts, is best suited to capture the lived experiences and nuanced insights that quantitative methods cannot reveal. This approach enables a deeper understanding of barriers such as absent legal guidelines, lack of harmonised global standards, and institutional caution, all of which emerge within the complex interplay between decentralised crypto-asset systems and centralised regulatory frameworks.

Chapter 1 identified regulatory sandboxes, risk-based compliance models, and the FATF Travel Rule as the primary mitigation mechanisms available to South African regulators, but whether those instruments are operationally viable, whether they are perceived as adequate by practitioners, and what conditions would be necessary for them to succeed are questions that cannot be answered from legislation alone. The inductive thematic analysis employed in this study is grounded in the systematic coding of interview transcripts using Atlas.ti, enables the researcher to move from the specific experiences of respondents toward the broader patterns that characterise the mitigation landscape, identifying what works, what falls short, and why.

This approach is consistent with the epistemological position established at the outset of this chapter: knowledge in this domain is generated through systematic engagement with informed practitioners, and it must be validated through the rigour of credibility, transferability, dependability, and confirmability rather than statistical generalisation. The third dimension, embedding regulation within cryptocurrency design, introduces a technological and forward-looking dimension that the qualitative approach handles through its openness to emergent themes.

Chapter 1 described this dimension as a shift in how technology is perceived, from a regulatory evasion mechanism to a compliance enabler, encompassing RegTech integration, self-sovereign identity frameworks, and real-time immutable ledgers. Whether South African industry actors and regulators share that reoriented understanding, what institutional and cultural barriers impede its adoption, and what practical conditions would be required to embed compliance within crypto-asset ecosystems at the service-provider level are precisely the kinds of questions that

emerge organically from open-ended interview dialogue and are captured through iterative inductive coding.

The flexibility inherent in semi-structured interviewing, its capacity to follow respondents into unexpected territory while maintaining thematic coherence, makes it the appropriate instrument for mapping a dimension that is as much about evolving perceptions and institutional readiness as it is about technical capability. In sum, the methodology presented in this chapter is not a neutral procedural choice but a theoretically grounded response to the epistemological demands of the three dimensions that structure this study. The qualitative design, purposive sampling, semi-structured interviews and inductive thematic analysis together constitute the methodological infrastructure through which the three dimensions of Chapter 1 are translated into researchable, empirically grounded questions, and through which the findings of subsequent chapters are made analytically credible.

CHAPTER 4

CROSS-BORDER MONEY TRANSFERS AND CRYPTOCURRENCY: SOUTH AFRICA'S REGULATORY LANDSCAPE

4.1 Chapter Overview

Cross-border transfers and remittances represent a cornerstone of South Africa's economic and social fabric. They facilitate trade, investment, and financial inclusion, especially for migrant communities supporting families across borders. The regulatory architecture underpinning these flows must balance financial integrity, compliance with global standards, and enable access to financial services. The emergence of cryptocurrency-based solutions introduces new opportunities and risks that demand careful examination from both regulatory and practical implementation perspectives. This chapter presents and analyses findings derived from expert interviews regarding regulatory challenges and mitigation strategies associated with cryptocurrency and crypto-asset systems used in cross-border financial transfers in South Africa. While participants occasionally referenced “blockchain,” analysis in this chapter recognises that financial regulation applies to crypto-assets, financial activities, and crypto-asset service providers (CASPs) rather than to distributed ledger technology as infrastructure (FATF, 2021; FSB, 2023).

The findings are organised thematically and interpreted through global regulatory frameworks governing crypto-asset markets, AML/CFT standards, and financial supervisory models.

4.1.1 *Blockchain-Enabled Solutions in the SADC and Wider African Region*

Within the SADC and broader African context, several blockchain-based and crypto-enabled platforms have emerged as important case studies for understanding the operational, regulatory, and developmental implications of distributed ledger technologies for cross-border financial transfers. These platforms illustrate both the potential efficiencies and the complex regulatory challenges associated with blockchain adoption in emerging market financial systems.

SwyChR (Southern Africa)

SwyChR represents a regionally focused blockchain-driven remittance and settlement platform designed specifically for SADC cross-border payments. The system leverages distributed ledger technology to improve transaction transparency, facilitate near-real-time settlement, and reduce the high intermediary costs that typically characterise cross-border transfers within the region.

Regulatory implications: SwyChR operates in a regulatory environment still largely shaped by exchange control rules, AML requirements, and the need for interoperability with centralised financial messaging systems. Its model highlights the regulatory tension between enabling innovation and maintaining compliance with South Africa's prudential authorities, particularly the SARB and the Financial Intelligence Centre (FIC).

BitPesa (AZA Finance)

Initially launched as one of Africa's earliest blockchain-based payments platforms, BitPesa used cryptocurrency rails to facilitate low-cost, rapid B2B foreign-exchange payments across East, West, and Southern Africa. Although the company has since evolved into AZA Finance, its early adoption of blockchain infrastructure demonstrated how decentralised payment channels can bypass costly correspondent banking arrangements and improve liquidity in frontier markets.

Regulatory implications: BitPesa's trajectory underscores the challenges associated with regulatory recognition of crypto-driven FX services. Early operations required extensive engagement with central banks, including obtaining licensing under money transfer, payments service provider, or FX dealer regulations—demonstrating how blockchain firms must negotiate fragmented regulatory classifications across jurisdictions.

Yellow Card (Pan-African)

Yellow Card is one of the continent's most widely used cryptocurrency exchanges and payments ecosystems, with active operations across several SADC countries. Its platform enables users to buy, sell, hold, and transfer crypto-assets, which are often repurposed by users for remittances, hedging against inflation, or circumventing high transaction fees associated with traditional remittance channels.

Regulatory implications: Yellow Card's multi-jurisdictional footprint highlights the absence of harmonised crypto regulations across Africa. The platform must navigate divergent legal treatment of crypto-assets, ranging from acceptance under VASP (Virtual Asset Service Provider) frameworks in some countries to restrictive or ambiguous environments in others. This fragmentation underscores the need for regional regulatory coordination, an important theme in SADC financial integration discourse.

Together, these platforms demonstrate the growing relevance of blockchain-enabled solutions for the African cross-border payments landscape. They highlight a dual reality: blockchain can materially lower transaction costs and settlement times, yet regulatory frameworks in the region remain fragmented, reactive, and slow to adapt. These cases provide empirical grounding for analysing the regulatory barriers and transitional frameworks required for South Africa, and SADC more broadly, to support innovation while safeguarding financial stability and compliance.

Regulators must respond to innovations such as cryptocurrency, stablecoins, and blockchain-based remittance systems while preserving South Africa's compliance with FATF standards and maintaining macro-financial stability. This chapter maps the relevant South African legislative, regulatory, and policy instruments, critically analysing their applicability to cross-border financial flows and blockchain-related innovations. Subsequently, it presents empirical findings from semi-structured interviews with eight industry experts, regulatory bodies, and stakeholders to assess the practical implications of implementing blockchain solutions within this regulatory framework.

4.2 Classification of Cryptocurrency in South Africa

In a watershed moment for crypto regulation in South Africa, the FSCA announced in 2021 that cryptocurrency would be classified as financial products under the Financial Advisory and Intermediary Services Act (FAIS). This classification compels CASPs, such as exchanges, brokers, and wallet providers, to register with the FSCA and comply with regulatory requirements (FSCA, 2021). According to the FSCA, crypto assets are defined as a "digital representation of value that is not issued by a central bank but is capable of being traded, transferred, or stored electronically by natural and legal persons for the purpose of payment, investment, and other forms of utility" (FSCA,

2021). This definition echoes the FATF guidance on virtual assets, aimed at mitigating risks related to money laundering and terrorist financing (FATF, 2021).

The classification under FAIS also ensures that service providers offering advice or intermediary services regarding cryptocurrency must comply with standards on licensing, disclosure, and conflict of interest mitigation, principles traditionally reserved for mainstream financial instruments.

Regulatory Objectives and Rationale

South Africa's regulatory posture towards cryptocurrency is shaped by a set of policy objectives grounded in the protection of consumers, market integrity, and financial system stability:

4. **Consumer Protection:** The unregulated crypto market in South Africa has witnessed widespread scams, fraudulent investment schemes, and the proliferation of pyramid schemes. Without formal oversight, consumers are vulnerable to significant financial losses due to market volatility, lack of information, and misinformation. Regulation seeks to ensure that crypto service providers operate transparently, honestly, and in a manner that mitigates the risk of consumer exploitation (Zamani & Giaglis, 2018).
5. **Market Integrity and Financial Stability:** As crypto-assets grow in prominence, they may introduce systemic risk to the broader financial system, particularly if financial institutions gain exposure without appropriate safeguards. Regulation allows authorities to monitor developments and intervene where necessary to preserve market stability (Arner et al., 2017).
6. **Prevention of Illicit Activity:** The pseudonymous and borderless nature of cryptocurrency renders them susceptible to abuse for money laundering, terrorist financing, and tax evasion. Through AML/KYC requirements, South African regulators aim to curtail these risks while integrating crypto-assets into a controlled financial ecosystem (Houben & Snyers, 2018).
7. **Monetary Policy Control:** A growing dependence on privately-issued digital currencies could erode the South African Reserve Bank's (SARB) ability to influence liquidity, inflation, and interest rates. Regulation helps reassert central authority over monetary policy mechanisms (Reuters, 2022).

Role of the South African Reserve Bank (SARB)

As the custodian of monetary policy and financial stability in South Africa, the SARB has adopted a measured and consultative approach to regulating crypto-assets. In coordination with the FSCA, National Treasury, and other stakeholders, the SARB has acknowledged the need to strike a balance between innovation and risk mitigation (SARB, 2021).

One of the SARB's principal concerns is the potential disintermediation of the traditional banking sector. DeFi applications built on public blockchains can allow users to bypass commercial banks, thereby threatening the conventional financial intermediation model. Additionally, the SARB has expressed caution about the risks posed by stablecoins, which, despite being pegged to fiat currencies, may not be subject to the same regulatory scrutiny. To mitigate systemic risk, the SARB supports inter-agency cooperation through the IFWG, which helps coordinate fintech and crypto regulation across departments.

Proposed Regulatory Framework

The emerging regulatory framework in South Africa adopts a multi-pronged approach:

- **Licensing of CASPs:** Under the FSCA mandate, CASPs must register and comply with conduct and disclosure requirements in line with the FAIS Act.
- **AML and KYC Compliance:** The Financial Intelligence Centre (FIC) enforces AML protocols, mandating that CASPs conduct customer due diligence, report suspicious transactions, and maintain audit trails (FIC, 2022).
- **Exchange Control Regulations:** Cross-border crypto transactions are subject to SARB exchange control rules. Crypto is not recognised as legal tender, but transfers involving crypto must still comply with foreign exchange limitations.
- **Taxation:** The South African Revenue Service (SARS) treats crypto as an asset subject to capital gains tax. Any earnings, whether from mining, trading, or staking, must be declared for tax purposes.
- **Regulatory Sandbox and Innovation:** The IFWG has launched a regulatory sandbox allowing startups to test cryptocurrency applications under controlled conditions.

Global Context and Comparative Approaches

Globally, countries have adopted varying approaches to blockchain and crypto regulation, from prohibition to proactive support.

- **European Union (EU):** The Markets in Crypto-Assets Regulation (MiCA) introduces a harmonised EU framework for crypto-asset issuance, CASP authorisation, and transparency obligations (European Commission, 2020).
- **United States:** The regulatory environment is fragmented. The SEC views some crypto-assets as securities, while the CFTC considers others as commodities. Both agencies impose compliance requirements for disclosure and anti-fraud measures (Goforth, 2021).
- **Singapore and Switzerland:** These jurisdictions offer progressive models. Singapore's Monetary Authority encourages innovation via regulatory sandboxes, while Switzerland's FINMA provides clear categorisation and licensing pathways (Zetsche et al., 2018).

South Africa can draw from these examples to craft a balanced regulatory framework that enables innovation while safeguarding market and consumer interests.

Challenges in Implementation

While the regulatory intent is clear, practical challenges remain:

1. **Technological Complexity:** Cryptocurrency systems operate on complex, evolving technologies that require regulators to build capacity and expertise. Understanding technical protocols and ensuring compliance is a steep learning curve (Walch, 2019).
2. **Jurisdictional Arbitrage:** Crypto businesses can easily relocate to less stringent jurisdictions, making enforcement difficult unless international coordination is achieved. A harmonised global regulatory framework is necessary to avoid regulatory arbitrage (FATF, 2021).
3. **Evolving Nature of Assets:** The definition of cryptocurrency and crypto-assets continues to evolve, requiring adaptive regulatory frameworks that can respond to innovation. Regulators must remain agile to avoid stifling beneficial innovation (De Filippi & Wright, 2018).

4. **Public Awareness and Education:** Many consumers lack a comprehensive understanding of crypto risks. Public awareness campaigns and investor education are critical to supplement regulatory efforts (OECD, 2020).

Central Bank Digital Currency Initiatives

To modernise the national payment infrastructure and retain monetary sovereignty, the SARB is actively exploring the feasibility of a central bank digital currency (CBDC). Project Khokha II tested the issuance and settlement of a wholesale CBDC using DLT. The pilot involved tokenised fiat settlement and demonstrated real-time gross settlement functionality in a multi-party environment (SARB, 2022). A CBDC could offer benefits such as improved payment efficiency, enhanced financial inclusion, and reduced transaction costs. However, its implementation also poses legal, privacy, and cybersecurity considerations.

The South African regulatory environment for cryptocurrency reflects an evolving ecosystem that balances innovation with financial stability. By recognising cryptocurrency as financial products, implementing licensing regimes for CASPs, and mandating AML compliance, the country has laid the groundwork for a regulated digital finance sector. However, the road ahead presents significant challenges, including rapid technological change, jurisdictional arbitrage, capacity-building among regulators, and public education. As the nature of crypto-assets evolves, so too must the regulatory tools that govern them. A flexible, principles-based, and collaborative regulatory approach, grounded in interagency coordination and informed by global best practices, is imperative for South Africa to thrive in the digital economy.

The development of CBDCs and the adoption of blockchain and cryptocurrency in public administration mark important milestones in the country's digital transformation journey. South Africa's commitment to regulation that is innovation-friendly, risk-aware, and inclusive will determine its success in integrating blockchain technologies into a sustainable financial future.

Year	Regulation/Policy	Description	Source
1933	Currency and Exchanges Act, 1933 (as amended), 1933 (Act No. 9 of 1933) (Currency and Exchanges Act 9 of 1933)	Governs cross-border transactions and remittances, administered by SARB's Financial Surveillance Department. Prohibits capital exports without National Treasury approval, including crypto asset purchases.	South African Reserve Bank (SARB)
1961	Exchange Control Regulations	Constitutes the central mechanism for governing cross-border financial transactions. It prescribes restrictions and conditions on the purchase and sale of foreign exchange, the export of capital, and payments to and from non-residents. Authorised Dealers (ADs), typically commercial banks, serve as the operational gatekeepers for executing cross-border payments under these regulations.	South African Reserve Bank (SARB)
1998	National Payment System Act, 1998 (Act No. 78 of 1998)	Regulates South Africa's payment systems, including cross-border electronic funds transfers. Supports SADC real-time gross settlement and CLS systems. Crypto assets are not recognized as payment instruments.	South African Reserve Bank (SARB)
2001	Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001, as amended)	Combats money laundering and terrorist financing. Requires reporting of international funds transfers above R19,999.99. 2022 amendments extended obligations to Crypto Asset Service Providers (CASPs).	Financial Intelligence Centre (FIC)
2014	SARB Position Paper on Virtual Currencies	Clarifies that crypto assets are not legal tender and are unregulated by SARB. Transactions are at the user's risk.	South African Reserve Bank (SARB)

Year	Regulation/Policy	Description	Source
		Signals a “wait and see” approach to future regulation.	
2017	Financial Sector Regulation Act, 2017 (Act No. 9 of 2017)	Establishes FSCA and Prudential Authority. Crypto assets are not currently financial products but are being integrated into the regulatory framework per IFWG recommendations.	Financial Sector Conduct Authority (FSCA)
2021	IFWG Position Paper on Crypto Assets	Outlines a phased approach to regulate crypto assets, defining them as digital representations of value. CASPs are subject to FICA for AML/CTF compliance.	Intergovernmental Fintech Working Group (IFWG) via SARB
2022	Amendments to FICA Schedules	Adds CASPs as accountable institutions under FICA, requiring AML/CTF compliance for blockchain-based transactions, including cross-border transfers.	Financial Intelligence Centre (FIC)
Ongoing (Updated Regularly)	Currency and Exchanges Manual for Authorised Dealers	Specifies conditions for cross-border transactions, including the R1 million single discretionary allowance and R10 million foreign investment allowance. Prohibits crypto asset purchases abroad.	South African Reserve Bank (SARB)
Ongoing (Updated Regularly)	Currency and Exchanges Manual for Authorised Dealers in Foreign Exchange with Limited Authority (ADLA)	Governs ADLAs (e.g., bureaux de change, money transfer operators) for remittances within specified limits. Includes capital requirements for operators.	South African Reserve Bank (SARB)
Ongoing	SARS Crypto Assets & Tax Guidance	Treats crypto assets as property for tax purposes. Cross-border crypto transactions must comply with SARB	South African Revenue Service (SARS)

Year	Regulation/Policy	Description	Source
		exchange controls. Addresses tax evasion risks.	
2025 (Draft, Comments due April 16, 2025)	Draft Directive in Respect of Specific Payment Activities (Authorisation Framework)	Proposes an authorisation framework for payment activities, including cross-border transfers. Addresses cybersecurity and AML for blockchain-based transfers.	South African Reserve Bank (SARB)
Ongoing (Draft)	Guidance Note 104A on International Funds Transfer Reports	Provides instructions for FICA Section 31 compliance, requiring reporting of international funds transfers above R19,999.99 within three days. Applies to CASPs.	Financial Intelligence Centre (FIC)Th

Table 1. List of regulations and policies relating to Fiscal Transfers and Cryptocurrency in South Africa

4.3 Primary Legislative Framework

Respondents emphasised that South Africa's exchange control regime was designed for bank-mediated transfers. Cryptocurrency transactions, particularly peer-to-peer or wallet-based transfers, may occur outside authorised dealer channels. This creates supervisory gaps not because blockchain is unregulatable, but because crypto-asset settlement pathways operate through non-bank intermediaries. The issue, therefore, concerns financial reporting and capital flow monitoring, not technological architecture (IMF, 2022).

4.3.1 Currency and Exchanges Act, 1933 (as amended)

This Act, as amended, empowers the competent authority to make regulations relating to currency, banking and exchanges, forming the enabling basis for South Africa's exchange control framework (Currency and Exchanges Act 9 of 1933). Exchange control is operationalised through the Exchange Control Regulations, 1961 issued under section 9, and administered in practice via National Treasury delegations to the South African Reserve Bank (SARB) (Orders and Rules under the Exchange Control Regulations, 1961, Order 2). Accordingly, cross-border transactions that externalise

value may require Treasury permission where they amount to the export of capital or rights to capital (Exchange Control Regulations, 1961, reg 10(1)(c)).



Figure 9. Graphic indicating the linkage between the Currency and Exchanges Act

Key Provisions:

The exchange control regime is implemented through authorised channels and operating rules. Transactions involving cross-border transfers must be effected through authorised dealers (ADs) and authorised dealers with limited authority (ADLAs) operating under Treasury delegation (Orders and Rules under the Exchange Control Regulations, 1961, Orders 2–3). In addition, outward transfers of funds are subject to the general prohibition on exporting capital or rights to capital without permission (Exchange Control Regulations, 1961, reg 10(1)(c)). Operationally, these permissions and prohibitions are applied through the SARB Financial Surveillance Department's Currency and Exchanges Manuals (SARB, Currency and Exchanges Manual for Authorised Dealers, 2025, relevant sections).

Third, the Financial Intelligence Centre Act (FICA) creates a mandatory reporting obligation for international electronic transfers of money. Section 31 requires accountable institutions to file an international funds transfer report (IFTR) for cross-border electronic transfers above a prescribed amount (Financial Intelligence Centre Act 38 of 2001, s 31). The prescribed threshold is R19 999,99 (Money

Laundering and Terrorist Financing Control Regulations, reg 23D, inserted by GN 2943 in GG 47883 of 20 January 2023). The prescribed information is set out in regulation 23E and the report must be submitted within three days (Money Laundering and Terrorist Financing Control Regulations, regs 23E and 24(5)).

Impact of the Currency and Exchanges Act, 1933 (as amended), 1933 on Cryptocurrency Adoption

The Currency and Exchanges Act, 1933 (as amended), 1933 (as amended) was enacted to regulate foreign exchange and currency transactions within South Africa. However, its definitions of “currency” and “exchange” do not explicitly encompass cryptocurrency, which are generally treated as assets rather than legal tender. This exclusion has created a regulatory gap, resulting in significant uncertainty for financial institutions and investors. While the absence of direct restrictions has allowed retail and fintech players to experiment with crypto solutions, banks and large institutions remain cautious due to compliance risks and the potential for future legislative amendments. Consequently, the Act (1996) indirectly inhibits widespread cryptocurrency adoption by maintaining ambiguity rather than providing a clear regulatory framework. (Currency and Exchanges Act 9 of 1933, s 9)

4.4 Exchange Control Regulations, 1961

These regulations, issued under the 1933 Act (as amended), constitute the central mechanism for governing cross-border financial transactions. They prescribe restrictions and conditions on (i) the purchase, sale and lending of foreign currency and gold (Exchange Control Regulations, 1961, reg 2), (ii) the export of currency, securities and related instruments (Exchange Control Regulations, 1961, reg 3), and (iii) the export of capital or rights to capital (Exchange Control Regulations, 1961, reg 10(1)(c)). Authorised dealers (ADs) and authorised dealers with limited authority (ADLAs) act as the operational gatekeepers under Treasury delegation (Orders and Rules under the Exchange Control Regulations, 1961, Orders 2–3). AML/CFT risks emerged as a major concern. Participants highlighted difficulties in tracing transactions involving self-hosted wallets and decentralised platforms.

However, global practice demonstrates that compliance is embedded at the service-provider level through Travel Rule implementation, customer due diligence, and

blockchain analytics (BIS, 2023). FATF Recommendation 15 explicitly regulates VASPs rather than protocols, confirming that governance focuses on entities and transactions, not blockchain technology.

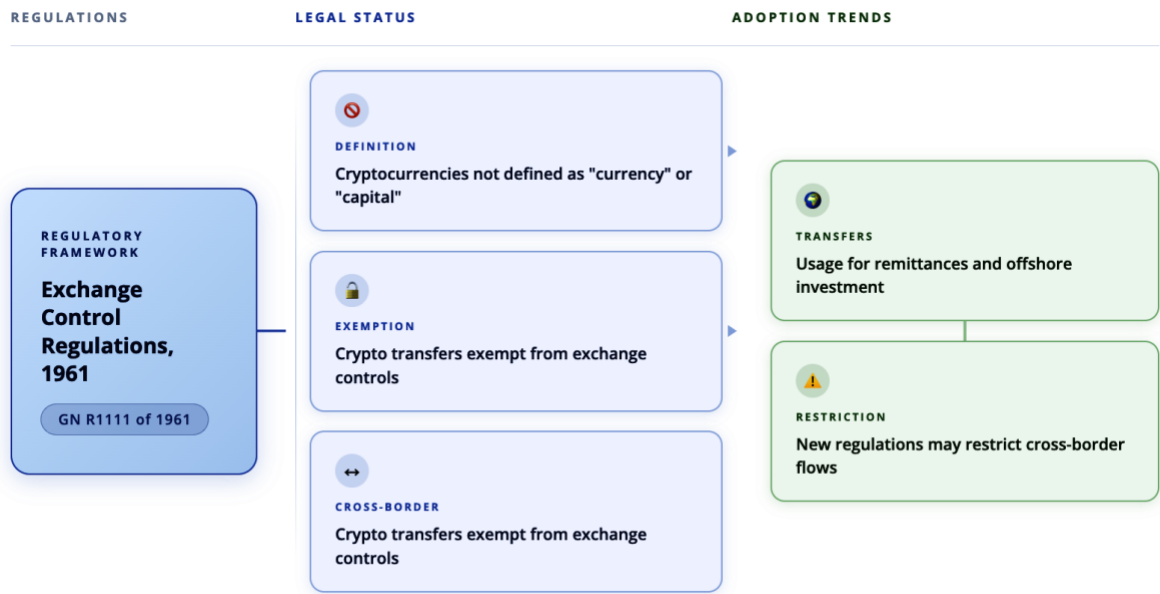


Figure 10. Graphic indicating the linkage between the Exchange Control Regulations, 1961 Act, its Legal Status and its Adoption trend (Researcher)

Key Provisions:

The Exchange Control Regulations derive their legal authority from section 9 of the Currency and Exchanges Act of 1933 (Currency and Exchanges Act 9 of 1933). The regulations operationalise exchange control by imposing conditions on foreign exchange dealings (Exchange Control Regulations, 1961, reg 2) and by restricting the export of capital without Treasury permission (Exchange Control Regulations, 1961, reg 10(1)(c)). A critical component of the regulatory architecture involves the oversight of non-resident transactions, with prescribed conditions governing payments to and from non-residents, including remittances, trade settlements, and foreign investment flows. The operational implementation of these controls is delegated to Authorised Dealers (ADs), typically commercial banks, which are formally designated to implement and monitor compliance with exchange control provisions. These institutions function as regulatory gatekeepers, executing and validating cross-border payment transactions in accordance with prescribed regulatory standards. (Orders and Rules under the Exchange Control Regulations, 1961, Orders 2–3)

Impact of Exchange Control Regulations, 1961 on Cryptocurrency Adoption

The Exchange Control Regulations of 1961 were enacted to govern the movement of currency and capital across South African borders. However, recent judicial interpretations have clarified that cryptocurrency do not fall within the definitions of “currency” or “capital” under these regulations. This exclusion has created a regulatory vacuum, allowing crypto transactions to occur without violating exchange control laws. While this has encouraged short-term adoption, it has also introduced significant legal uncertainty and enforcement challenges, as regulators lack explicit authority to govern cross-border crypto flows. Consequently, institutional participation remains limited, and the risk of abrupt legislative changes continues to shape market behaviour.

4.5 National Payment System Act, 1998 (Act No. 78 of 1998)

Description: This act regulates South Africa's national payment system (NPS), including cross-border electronic funds transfers and remittances. It empowers the SARB to issue directives on payment systems, including low-value cross-border electronic funds transfers within the Common Monetary Area (CMA) and the Southern African Development Community (SADC) real-time gross settlement system.

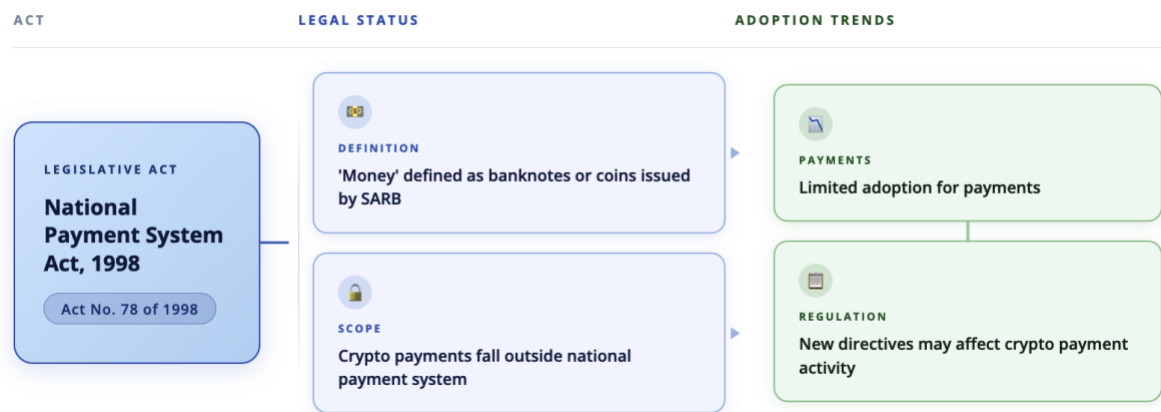


Figure 11. Graphic indicating the linkage between the National Payment System Act, 1998 (Act No. 78 of 1998), its Legal Status and its Adoption trend (Researcher)

Key Provisions:

Recent regulatory developments have sought to modernise cross-border payment infrastructure within the Common Monetary Area (CMA). Specifically, Directive No. 1 of 2025 provides regulatory guidance concerning low-value cross-border electronic funds transfers conducted within the CMA framework. This directive reflects efforts to facilitate

regional financial integration while maintaining appropriate oversight mechanisms. The National Payment System Act advances the integration of sophisticated cross-border payment infrastructure by supporting participation in regional and global settlement systems, including the Southern African Development Community (SADC) Real-Time Gross Settlement (RTGS) system and the Continuous Linked Settlement (CLS) system for foreign exchange transactions. These systems enhance settlement efficiency and reduce systemic risk in cross-border financial transactions. However, the current National Payment System (NPS) regulatory framework does not recognise cryptocurrency assets as legitimate payment instruments. This regulatory position reflects ongoing policy deliberations regarding the appropriate classification and oversight of digital assets within the formal payment system architecture.

Impact of the National Payment System Act, 1998 on Cryptocurrency Adoption

The National Payment System Act, 1998 was introduced to regulate payment systems in South Africa, ensuring safety, efficiency, and oversight of clearing and settlement processes. However, cryptocurrency and blockchain-based payment platforms fall outside the scope of this Act, as they do not operate within the licensed and regulated payment infrastructure overseen by the South African Reserve Bank. While the Act does not explicitly prohibit crypto transactions, its exclusion from the formal payment system limits interoperability with mainstream financial services and prevents integration into official platforms such as SAMOS or PayShap. This regulatory gap has allowed decentralised payment innovation but has simultaneously constrained institutional adoption and consumer trust, creating a barrier to widespread cryptocurrency use in the national payment ecosystem (National Payment System Act 78 of 1998, s 2). Banks remain cautious toward crypto-asset businesses, perceiving heightened compliance risk. This “de-risking” reflects uncertainty rather than inherent incompatibility. Literature shows that regulatory clarity reduces institutional resistance and promotes supervised innovation (Catalini & Gans, 2019).

4.6 Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001, as amended)

FICA establishes the statutory framework for combating money laundering and terrorist financing in South Africa. It applies to cross-border money transfers and remittances by

requiring accountable institutions to submit international funds transfer reports for international electronic transfers of money above the prescribed threshold (Financial Intelligence Centre Act 38 of 2001, s 31; Money Laundering and Terrorist Financing Control Regulations, reg 23D). The information content and reporting window are prescribed in the regulations (Money Laundering and Terrorist Financing Control Regulations, regs 23E and 24(5)). Amendments to Schedule 1 further designated crypto asset service providers (CASPs) as accountable institutions (Financial Intelligence Centre Act 38 of 2001, Sch 1 item 22, as inserted by GN 2800 in GG 47596 of 29 November 2022, effective 19 December 2022).

Key Provisions:

The Financial Intelligence Centre Act establishes comprehensive reporting obligations for cross-border financial transactions. Section 31 of the Act imposes a mandatory reporting requirement on accountable institutions to submit reports concerning international funds transfers that exceed the prescribed threshold, with such reports required to be lodged within a three-day period from the date of the transaction. This temporal requirement ensures timely intelligence gathering for anti-money laundering and counter-terrorist financing purposes. The substantive content requirements for international funds transfer reports are delineated in Regulation 23E, which specifies the precise information that must be captured and transmitted to the Financial Intelligence Centre. These prescribed information elements facilitate the creation of comprehensive audit trails for cross-border payment flows. (Money Laundering and Terrorist Financing Control Regulations, reg 23D) (Money Laundering and Terrorist Financing Control Regulations, reg 24(5))



Figure 12. Graphic indicating the linkage between the Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001, as amended) (FICA), its Legal Status and its Adoption trend (Researcher)

Significantly, amendments promulgated in 2022 expanded the scope of entities subject to FICA obligations by designating Crypto Asset Service Providers (CASPs) as accountable institutions. This regulatory extension represents a legislative response to emerging money laundering vulnerabilities associated with cryptocurrency transactions and reflects international best practices in virtual asset regulation. (Financial Intelligence Centre Act 38 of 2001, Sch 1 item 22, as inserted by GN 2800 in GG 47596 of 29 November 2022, effective 19 December 2022)

Impact of the Financial Intelligence Centre Act, 2001 (FICA) on Cryptocurrency Adoption

The Financial Intelligence Centre Act (FICA) was enacted to combat money laundering and terrorist financing by imposing compliance obligations on accountable institutions. Recent amendments have explicitly included Crypto Asset Service Providers (CASPs) within its scope, requiring them to register with the Financial Intelligence Centre and adhere to stringent AML/KYC requirements. This regulatory inclusion enhances legitimacy and investor confidence in the cryptocurrency market by aligning it with global anti-money laundering standards. However, it also introduces significant compliance costs and operational burdens, particularly for smaller exchanges and startups, which can slow innovation and limit rapid adoption. Overall, FICA strengthens oversight and consumer protection but creates a challenging environment for emerging

players in the crypto ecosystem. (Financial Intelligence Centre Act 38 of 2001, Sch 1 item 22, as inserted by GN 2800 in GG 47596 of 29 November 2022, effective 19 December 2022). Despite risks, respondents highlighted significant benefits:

- Faster settlement
- Reduced remittance costs
- Improved financial inclusion
- Programmable financial infrastructure

These advantages derive from crypto-asset transaction models, including stablecoins and tokenised settlement, rather than blockchain in isolation (World Bank, 2018).

4.7 Financial Sector Regulation Act, 2017 (FSR Act)

The FSR Act established the "Twin Peaks" model of financial regulation, creating the Prudential Authority under the SARB and the Financial Sector Conduct Authority (FSCA). This legislation lays the foundation for systemic stability and market conduct oversight, ensuring that both prudential and conduct risks in cross-border remittances and blockchain-based financial products are addressed. (Financial Sector Regulation Act 9 of 2017) (Financial Sector Regulation Act 9 of 2017). Participants noted that regulatory frameworks lag behind innovation. This mismatch arises because financial regulation is institution-centric, whereas crypto-asset ecosystems introduce new intermediaries (exchanges, custodians, wallet providers). The challenge is therefore institutional adaptation, not technological control.

Key Provisions:

The Financial Sector Regulation Act represents a fundamental restructuring of South Africa's financial regulatory architecture through the establishment of the Twin Peaks regulatory model. This framework marks a departure from the previous institutional-based regulatory approach toward an objectives-based model that separates prudential and conduct regulation.



Figure 13. Graphic indicating the linkage between Financial Sector Regulation Act, 2017 (FSR Act), its Legal Status and its Adoption trend (Researcher)

The Act established two distinct regulatory authorities with complementary mandates. The Prudential Authority (PA) was created as a juristic person within the South African Reserve Bank (SARB), vested with responsibility for maintaining systemic stability and enforcing prudential regulation across the financial sector. The PA's institutional placement within the central bank reflects international best practices in macroprudential oversight and enables coordination between monetary policy and financial stability objectives.

Concurrently, the Financial Sector Conduct Authority (FSCA) was established as an independent regulatory entity responsible for overseeing market conduct regulation and protecting financial customers. The FSCA's mandate encompasses ensuring fair treatment of consumers, promoting financial market integrity, and preventing market abuse. This bifurcated regulatory structure reflects the twin objectives of financial regulation: ensuring institutional safety and soundness while simultaneously protecting consumer interests.

Regulatory Objectives:

- To ensure systemic stability in the financial sector
- To safeguard market integrity and fair conduct

Application to Emerging Sectors:

- The framework explicitly extends to risks in cross-border remittances
- It also addresses conduct and prudential concerns in blockchain-based financial products.

Impact of the Financial Sector Regulation Act, 2017 (FSR Act) on Cryptocurrency Adoption

The Financial Sector Regulation Act (FSR Act) introduced South Africa's Twin Peaks regulatory model, establishing the Prudential Authority for financial stability and the Financial Sector Conduct Authority (FSCA) for market conduct. Under this framework, the FSCA classified crypto assets as financial products in 2022, bringing them under its jurisdiction for licensing and conduct regulation. This development provides a formal regulatory pathway for crypto service providers, enhancing consumer protection and market integrity while improving investor confidence. However, the Act also imposes licensing requirements and compliance obligations that increase operational costs, creating barriers for startups and decentralised platforms. Overall, the FSR Act legitimises cryptocurrency within the financial sector but slows rapid adoption due to regulatory burdens. (Financial Sector Regulation Act 9 of 2017, ss 32–33, 56; FSCA General Notice 1350 of 2022, GG 47334 of 19 October 2022) (Financial Sector Regulation Act 9 of 2017)

4.8 Currency and Exchanges Manual for Authorised Dealers

This manual, issued by the SARB's FinSurv Department, outlines permissions and restrictions for cross-border transactions, including remittances. It specifies conditions for Authorised Dealers (commercial banks) and ADLAs to facilitate cross-border transfers, such as the single discretionary allowance (R1 million per year) and foreign investment allowance (R10 million per year, subject to tax clearance). (Orders and Rules under the Exchange Control Regulations, 1961, Orders 2–3)

Key Provisions:

- Section H(A) restricts instruments offering exposure to foreign assets in Rand terms to those listed on a South African exchange

- Cross-border transfers for purchasing crypto assets are not permitted under the single discretionary allowance or foreign capital allowance
- Non-residents selling crypto assets in South Africa cannot transfer the proceeds abroad without SARB approval

Impact of the Currency and Exchanges Manual for Authorised Dealers on Cryptocurrency Adoption

The Currency and Exchanges Manual for Authorised Dealers provides guidance on foreign exchange transactions under South Africa's exchange control framework. While the manual does not explicitly prohibit cryptocurrency, it restricts cross-border transfers for the purpose of purchasing crypto assets, as the Financial Surveillance Department does not approve such transactions. Individuals may use their Single Discretionary Allowance (up to R1 million annually) or Foreign Investment Allowance (up to R10 million) to acquire crypto assets, but corporate entities face stricter limitations, and foreign direct investment dispensations exclude crypto. This creates a narrow legal pathway for personal investment while limiting institutional participation and large-scale cross-border crypto transactions. Overall, the manual enforces exchange control principles, constraining widespread cryptocurrency adoption and innovation within the regulated financial system. (Orders and Rules under the Exchange Control Regulations, 1961, Orders 2–3). Respondents proposed:

- Regulatory sandboxes
- CASP licensing frameworks
- Integration of blockchain analytics
- Public-private dialogue
- International coordination

These align with global regulatory practice (FSB, 2023).



Figure 14. Graphic indicating the Impact of the Currency and Exchanges Manual for Authorised Dealers on Cryptocurrency Adoption (Researcher)

4.9. Supporting Guidelines Relevant to Cross-Border Transfers

4.9.1 Currency and Exchanges Manual for Authorised Dealers in Foreign Exchange with Limited Authority (ADLA)

This manual governs ADLAs, which include bureaux de change and money transfer operators (e.g., Western Union, MoneyGram). It outlines their authority to facilitate remittances and cross-border transfers within specific limits, such as the R1 million single discretionary allowance. (Orders and Rules under the Exchange Control Regulations, 1961, Orders 2–3)

Key Provisions:

The South African Reserve Bank's regulatory architecture for Authorised Dealers with Limited Authority (ADLAs) employs a tiered categorisation system that delineates operational permissions and capital adequacy requirements according to institutional capacity and business model complexity. (Orders and Rules under the Exchange Control Regulations, 1961, Orders 2–3)

Category Two ADLAs are granted authorisation to facilitate cross-border remittance transactions through collaborative arrangements with external money transfer operators, functioning as agent locations or service points for established international remittance networks. This agency model enables participation in the remittance market while limiting direct exposure to foreign exchange risk and operational complexity.

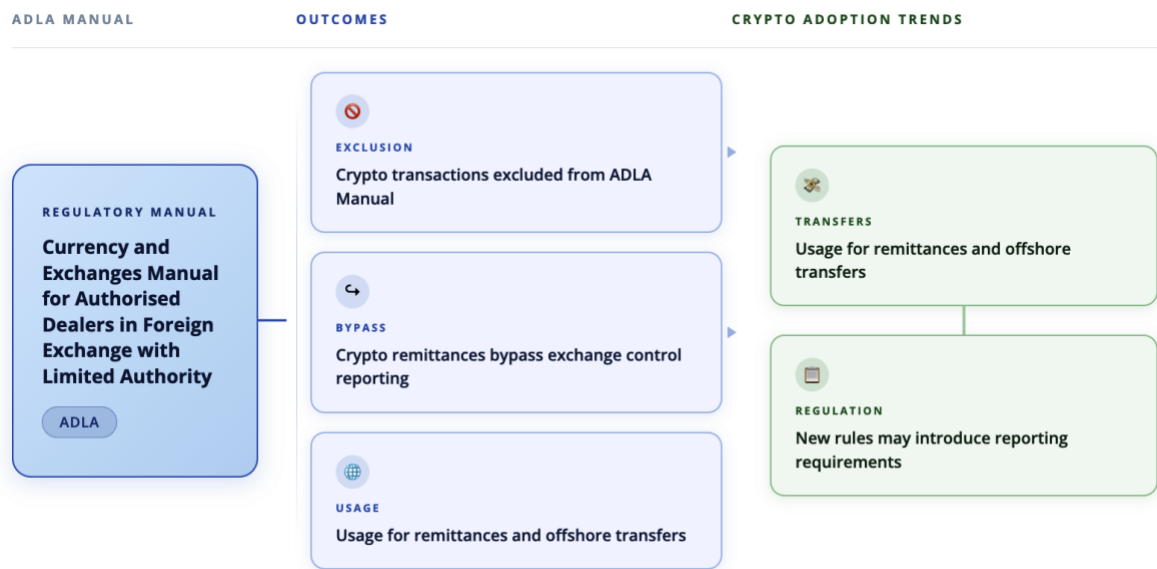


Figure 15. Graphic indicating the linkage between Currency and Exchanges Manual for Authorised Dealers in Foreign Exchange with Limited Authority (ADLA), its Legal Status and its Adoption trend (Researcher)

In contrast, Category Three ADLAs possess broader operational authority, permitting these entities to function as independent money transfer operators or value transfer service providers capable of establishing proprietary remittance channels and correspondent banking relationships. This enhanced operational scope necessitates more sophisticated risk management capabilities and regulatory compliance infrastructure. (Orders and Rules under the Exchange Control Regulations, 1961, Orders 2–3)

The regulatory framework prescribes differentiated minimum capital requirements calibrated to the authorisation category and associated risk profile. Category Two ADLAs must maintain minimum capital of R3 million, while Category Three ADLAs are subject to a higher threshold of R5 million in recognition of their expanded operational scope and attendant risk exposures. These capital requirements serve both prudential objectives, ensuring financial resilience, and consumer protection functions by providing

a buffer against operational losses. (Orders and Rules under the Exchange Control Regulations, 1961, Orders 2–3)

Impact of the Currency and Exchanges Manual for Authorised Dealers in Foreign Exchange with Limited Authority (ADLA) on Cryptocurrency Adoption

The Currency and Exchanges Manual for Authorised Dealers in Foreign Exchange with Limited Authority (ADLA) governs small-scale foreign exchange transactions, such as travel allowances and remittances, under South Africa's exchange control framework. ADLAs are explicitly prohibited from facilitating transactions for the purchase or transfer of cryptocurrency assets, as their authority is limited to approved forex activities overseen by the South African Reserve Bank. This restriction prevents ADLAs from serving as low-cost channels for retail crypto adoption and cross-border remittances, thereby reducing accessibility for individuals who rely on these services. Overall, the manual enforces strict separation between regulated forex services and crypto transactions, hindering widespread cryptocurrency adoption and innovation within the financial ecosystem. (Orders and Rules under the Exchange Control Regulations, 1961, Orders 2–3)

4.9.2 SARB Position Paper on Virtual Currencies (2014)

This position paper clarifies that crypto assets (referred to as virtual currencies at the time) are not legal tender in South Africa and are not regulated by the SARB. Transactions involving crypto assets are at the user's own risk, with no legal recourse to the SARB. The paper highlights the SARB's "wait and see" approach to regulating cryptocurrency.



Figure 16. Graphic indicating the linkage between SARB Position Paper on Virtual Currencies (2014), its Legal Status and its Adoption trend (Researcher)

Key Provisions:

The South African Reserve Bank's position paper on virtual currencies definitively established that cryptocurrency assets do not fulfill the statutory requirements for classification as legal tender under the South African Reserve Bank Act. Legal tender status confers specific juridical attributes, including the mandatory acceptance obligation in discharge of debts and the designation as official means of payment within a jurisdiction. The exclusion of crypto assets from this classification has material implications for their enforceability in contractual obligations and their treatment within the formal monetary system.

The position paper further clarified that cryptocurrency networks and associated transactional infrastructure fall beyond the jurisdictional ambit of the SARB's supervisory and oversight functions. Contemporaneously with this jurisdictional determination, the SARB conducted a preliminary risk assessment that concluded cryptocurrency markets did not, at that juncture, constitute a material threat to systemic financial stability within the South African financial system. This assessment was predicated upon the relatively nascent state of crypto asset adoption and the limited integration between cryptocurrency markets and traditional financial institutions during the period under review.

Notwithstanding the absence of immediate regulatory intervention, the position paper articulated the SARB's commitment to maintaining continuous surveillance of cryptocurrency market evolution and emerging risk profiles, with the explicit reservation of authority to implement regulatory measures should future developments warrant supervisory action. This "watchful waiting" regulatory posture reflects a prudential approach adopted by numerous central banking authorities during the formative stages of cryptocurrency market development, balancing the imperatives of financial innovation with stability concerns.

Impact of the SARB Position Paper on Virtual Currencies (2014) on Cryptocurrency Adoption

The South African Reserve Bank's Position Paper on Virtual Currencies (2014) clarified its stance on cryptocurrency, defining them as digital representations of value without legal tender status. SARB stated that virtual currencies would not be regulated or supervised at that time and would not form part of the National Payment System. This hands-off approach allowed early experimentation and retail adoption but created significant uncertainty for institutional players due to the absence of consumer protection and regulatory oversight. While the position paper encouraged innovation in the short term, it delayed formal integration of cryptocurrency into the regulated financial system, limiting mainstream adoption and trust.

4.9.3 IFWG Position Paper on Crypto Assets (2021)

Published by the Intergovernmental IFWG through the Crypto Assets Regulatory Working Group (CAR WG), this dissertation outlines a phased approach to bringing crypto assets into South Africa's regulatory framework. It addresses risks such as money laundering, terrorist financing, and cross-border illicit flows while promoting innovation.



Figure 17. Graphic indicating the phased approach of the IFWG Position Paper on Crypto Assets (2021) (Researcher)

Key Provisions:

The Intergovernmental Fintech Working Group's position paper established a comprehensive definitional framework for cryptocurrency assets within the South African regulatory context. Crypto assets are formally defined as digital representations of value that are not issued or guaranteed by any central bank or public authority, and which may be utilised for payment purposes, investment activities, or the provision of utility functions, with such assets characteristically relying on distributed ledger technology, particularly blockchain infrastructure. This definition aligns substantially with international regulatory standards articulated by bodies such as the Financial Action Task Force.

The position paper mandates that CASPs, defined as entities facilitating the exchange, custody, or transfer of crypto assets, be subjected to obligations under the Financial Intelligence Centre Act to mitigate money laundering and terrorist financing risks associated with virtual asset transactions. This regulatory designation reflects growing international consensus regarding the vulnerability of cryptocurrency platforms to illicit financial flows.

Importantly, the Working Group adopted a principles-based regulatory philosophy, recommending the integration of crypto assets within existing financial regulatory

frameworks rather than pursuing the development of bespoke legislation. This approach of "same activity, same risk, same regulation" seeks to ensure regulatory consistency while avoiding fragmentation of the supervisory architecture. The integration strategy recognises that crypto assets exhibit characteristics analogous to existing financial instruments and therefore warrant classification within established regulatory categories.

Impact of the IFWG Position Paper on Crypto Assets (2021) on Cryptocurrency Adoption

The Intergovernmental Fintech Working Group (IFWG) Position Paper on Crypto Assets (2021) marked a significant shift in South Africa's regulatory approach to cryptocurrency. The paper recognised crypto assets as part of the financial ecosystem and proposed a structured regulatory framework to mitigate risks. Key recommendations included requiring Crypto Asset Service Providers (CASPs) to register and comply with AML/CFT obligations under FICA, and classifying crypto assets as financial products under FSCA oversight for licensing and conduct regulation. This clarity improved investor confidence and enabled institutional participation, legitimizing the crypto market. However, compliance costs and licensing requirements introduced operational challenges for smaller players and decentralised platforms. Overall, the IFWG paper balanced innovation with consumer protection, fostering regulated growth while slowing rapid adoption. (FSCA General Notice 1350 of 2022, GG 47334 of 19 October 2022)

4.9.4 Draft Directive in Respect of Specific Payment Activities (Authorisation Framework)

This draft directive, issued by the SARB, proposes an authorisation framework for specific payment activities, including cross-border electronic funds transfers. It aims to enhance oversight of payment service providers, including those using blockchain technology, to ensure compliance with anti-money laundering and cybersecurity standards.

Key Provisions:

The National Payment System Act establishes comprehensive regulatory requirements governing payment service providers, including entities that facilitate cross-border remittance services. These requirements encompass authorisation procedures, operational standards, and ongoing compliance obligations designed to ensure the safety and efficiency of payment systems. The regulatory framework applies to both traditional payment intermediaries and emerging financial technology providers operating within the remittance corridor.

A critical dimension of the regulatory framework addresses cybersecurity and cyber-resilience within the National Payment System, provisions that carry particular relevance for blockchain-based transfer mechanisms and distributed ledger technology applications. These requirements mandate that payment system operators implement robust information security controls, business continuity arrangements, and incident response capabilities to mitigate technological and operational risks.

Furthermore, the regulatory framework demonstrates alignment with international standards, specifically the Financial Action Task Force (FATF) Recommendation 16, which establishes requirements for wire transfers and the transmission of originator and beneficiary information in cross-border electronic funds transfers. This harmonisation ensures that South African payment systems operate in conformity with global anti-money laundering and counter-terrorist financing standards, facilitating international regulatory cooperation and reducing compliance fragmentation.

Impact of the Draft Directive in Respect of Specific Payment Activities (Authorisation Framework) on Cryptocurrency Adoption

The Draft Directive in Respect of Specific Payment Activities (Authorisation Framework) represents the South African Reserve Bank's effort to regulate entities involved in payment services, including those operating outside traditional banking structures. Under this proposed framework, any entity facilitating payment activities, such as crypto-based payment platforms, must obtain authorisation from SARB and comply with operational, risk management, and consumer protection standards. This directive provides a clear legal pathway for crypto payment service providers to integrate into the

regulated financial ecosystem, enhancing trust and legitimacy. However, the associated licensing and compliance obligations introduce high costs and complexity, which may discourage smaller players and slow innovation. Overall, the draft directive signals a move toward formal oversight of crypto-related payment activities, balancing regulatory control with the potential for broader adoption.



Figure 18. Graphic indicating the phased approach of the impact of the Draft Directive in Respect of Specific Payment Activities) (Researcher)

Cyber-Risk in Conventional Banking

Any assessment of the relative cybersecurity merits and risks of blockchain-based payment systems must be grounded in a clear-eyed appreciation of the cyber-risk profile of the incumbent conventional banking infrastructure against which cryptocurrency solutions are being compared. The premise that centralised banking systems are inherently more secure than distributed ledger alternatives is not empirically supported. The two architectures present categorically different risk surfaces that require distinct regulatory and technical governance responses.

The conventional banking system is characterised by centralised data architectures in which critical financial data such as account records, transaction histories, customer identity information, and settlement balances is concentrated in databases managed by

individual institutions or infrastructure operators. This centralisation creates single points of failure that are systematically attractive targets for cyberattacks. The Basel Committee on Banking Supervision (BCBS, 2021) has identified operational risk, of which cyber-risk is a primary component, as one of the three foundational risk categories in the Basel III regulatory framework. The Committee's Principles for Operational Resilience (BCBS, 2021) explicitly acknowledge that increasing digitalisation and interconnectedness have materially elevated the cyber-risk exposure of the global banking system.

The empirical record confirms this exposure. The Bank for International Settlements' Cyber Security Advisory Group documented that financial services institutions experienced a 238% increase in cyberattack frequency between 2019 and 2022 (BIS, 2022). South African banks have not been insulated from this trend. The South African Banking Risk Information Centre (SABRIC, 2023) reported that South African financial institutions incurred losses attributable to cybercrime exceeding R2.2 billion in 2022, encompassing phishing, business email compromise, social engineering, and data breaches. Standard Bank, Absa, and Nedbank have each disclosed significant cyber incidents in recent years, underscoring that the regulatory and operational frameworks governing the conventional banking system, while robust in many respects, have not eliminated the systemic cyber-risk inherent in centralised architectures.

The SARB's Guidance Note 3/2017 on Cyber Resilience Requirements for Financial Institutions mandates that banks implement information security frameworks aligned with internationally recognised standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework. However, compliance with these standards does not eliminate residual cyber-risk; it establishes a minimum threshold of organisational and technical controls designed to reduce the probability and impact of incidents. The systemic interconnectedness of South Africa's banking system, particularly through the South African Multiple Option Settlement (SAMOS) system and the Payment Association of South Africa (PASA) infrastructure, means that a successful cyberattack on a systemically important financial institution or on shared payment infrastructure could generate cascading systemic risk, a concern explicitly recognised in the SARB's Financial Stability Review (SARB, 2023).

In the cross-border remittance context specifically, the SWIFT network, which underpins a significant proportion of international correspondent banking transfers, has itself been the subject of sophisticated state-sponsored cyberattacks, most notably the 2016 Bangladesh Bank heist in which attackers exploited SWIFT's messaging infrastructure to fraudulently transfer approximately USD 81 million (Bouveret, 2018). This incident illustrates that even the most extensively governed and technically sophisticated components of the conventional financial system carry material cyber-risk, and that this risk is systemic rather than merely operational.

This baseline assessment does not imply that conventional banking systems are insecure. They are, in the aggregate, highly resilient. Rather, it contextualises the comparative analysis that the case for or against blockchain-based payment solutions on cybersecurity grounds cannot be premised on a binary opposition between a purportedly secure legacy system and a purportedly risky distributed one. Both architectures present distinct and manageable cyber-risk profiles that demand commensurate regulatory responses.

4.9.5 Guidance Note 104A on International Funds Transfer Reports (Draft, FIC)

Issued by the FIC, this guidance note provides accountable institutions with instructions on complying with Section 31 of FICA for reporting international funds transfers. It details reporting timelines, electronic reporting mechanisms, and required information relevant to both traditional and blockchain-based transfers. (Money Laundering and Terrorist Financing Control Regulations, reg 23D) (Money Laundering and Terrorist Financing Control Regulations, reg 23E) (Money Laundering and Terrorist Financing Control Regulations, reg 24(5))



Figure 19. Graphic indicating the linkage between the Guidance Note 104A on International Funds Transfer Reports), its Legal Status and its Crypto Adoption trend (Researcher)

Key Provisions:

The Financial Intelligence Centre Act and its regulations establish specific temporal parameters for international funds transfer reporting obligations. An accountable institution must submit an IFTR when an international electronic transfer exceeds the prescribed amount (Financial Intelligence Centre Act 38 of 2001, s 31; Money Laundering and Terrorist Financing Control Regulations, reg 23D). The report must include the prescribed particulars (Money Laundering and Terrorist Financing Control Regulations, reg 23E) and must be sent to the Centre within three days (Money Laundering and Terrorist Financing Control Regulations, reg 24(5)).

The institutional scope of these reporting obligations encompasses multiple categories of accountable institutions. Traditional banking institutions and money remittance service providers are explicitly subject to these requirements under the Act's definitional provisions. Following amendments to the regulatory framework in 2022, Crypto Asset Service Providers (CASPs) facilitating cross-border cryptocurrency transactions are potentially subject to analogous reporting obligations, contingent upon the characterisation of such transactions as constituting "international funds transfers" within the statutory meaning. This extension reflects regulatory efforts to address emerging money laundering typologies associated with virtual asset transfers across jurisdictional boundaries. (Financial Intelligence Centre Act 38 of 2001, Sch 1 item 22, as inserted by GN 2800 in GG 47596 of 29 November 2022)

Impact of Guidance Note 104A on International Funds Transfer Reports (Draft, FIC) on Cryptocurrency Adoption

The Draft Guidance Note 104A issued by the Financial Intelligence Centre (FIC) clarifies reporting obligations for international electronic funds transfers under Section 31 of the Financial Intelligence Centre Act. It requires accountable institutions to report cross-border transfers above a prescribed threshold within three days. While primarily aimed at traditional financial institutions, these obligations extend to Crypto Asset Service Providers (CASPs) involved in fiat-to-crypto or crypto-to-fiat transactions across borders. This measure enhances transparency and aligns South Africa with global AML/CFT standards, improving trust in the crypto ecosystem. However, it also introduces additional compliance burdens and operational costs for crypto platforms, particularly those handling international transfers. Overall, the guidance strengthens regulatory oversight but may slow adoption by increasing complexity for cross-border crypto activities. (Financial Intelligence Centre Act 38 of 2001, Sch 1 item 22, as inserted by GN 2800 in GG 47596 of 29 November 2022)

4.9.6 SARS Crypto Assets & Tax Guidance

The South African Revenue Service (SARS) treats crypto assets as property for tax purposes, similar to the U.S. IRS approach. This guidance addresses the tax implications of crypto asset transactions, including cross-border transfers, and emphasises compliance with exchange control regulations.

Key Provisions:

The South African Revenue Service has established that cryptocurrency assets are subject to general taxation principles applicable to property, thereby rendering such assets susceptible to both capital gains tax and income tax depending on the nature and circumstances of the transaction. Under this framework, gains arising from the disposal of crypto assets held as capital assets are taxable under the capital gains tax provisions of the Income Tax Act, while crypto assets held as trading stock or received as compensation are subject to income tax in accordance with ordinary revenue principles. This classification approach reflects the tax authority's position that

cryptocurrency should be treated consistently with other forms of intangible property rather than as currency or legal tender.

Cross-border cryptocurrency transactions remain subject to the exchange control regulatory framework administered by the South African Reserve Bank, with specific restrictions imposed on capital transfers. Notably, cross-border transfers undertaken for the purpose of acquiring cryptocurrency assets in foreign jurisdictions are subject to stringent limitations and require authorisation from designated regulatory authorities. These restrictions reflect policy concerns regarding capital flight facilitated through digital asset channels and the circumvention of exchange control mechanisms.

In recognition of emerging tax evasion vulnerabilities, the South African Revenue Service has indicated that it is actively examining tax policy implications associated with cryptocurrency transactions, with particular emphasis on addressing compliance gaps and evasion risks inherent in the pseudonymous nature of blockchain-based transfers. This policy review aligns with international efforts by organisations such as the Organisation for Economic Co-operation and Development to enhance tax transparency in the crypto asset ecosystem. (Exchange Control Regulations, 1961, reg 10(1)(c))

Impact of SARS Crypto Assets and Tax Guidance on Cryptocurrency Adoption

The South African Revenue Service (SARS) Crypto Assets & Tax Guidance clarifies that crypto assets are treated as intangible assets and are subject to normal income tax rules. Gains or losses from cryptocurrency transactions must be declared, with capital gains tax applying to investment holdings and income tax applying to frequent trading, mining, or payments for goods and services. SARS requires detailed record-keeping and reporting, supported by enhanced monitoring measures such as exchange data sharing and blockchain analysis. This guidance improves legitimacy and aligns South Africa with global tax standards, fostering transparency and institutional trust. However, it also introduces administrative burdens and compliance costs, which may discourage informal or small-scale participation. Overall, the tax framework normalises crypto within the financial system but slows rapid adoption due to complexity and fear of penalties for non-compliance. Across all themes, a consistent pattern emerged:

Regulatory tension arises from integrating cryptocurrency as financial instruments into existing governance structures, not from blockchain technology itself.



Figure 20. Graphic indicating the impact of the SARS Crypto Assets & Tax Guidance on cryptocurrency (Researcher)

4.10 Regulations Specific to Blockchain and Crypto Assets

4.10.1 Financial Sector Regulation Act, 2017 (Act No. 9 of 2017)

This act establishes the Financial Sector Conduct Authority (FSCA) and Prudential Authority, which oversee financial institutions but currently do not regulate crypto assets as financial products. However, the FSCA has indicated that crypto assets will be brought into the regulatory purview in a phased manner, as outlined in the IFWG Position Paper. (FSCA General Notice 1350 of 2022, GG 47334 of 19 October 2022)

Key Provisions:

Under the existing regulatory framework established by the Financial Advisory and Intermediary Services Act and the Financial Markets Act, cryptocurrency assets do not satisfy the definitional criteria for "financial products" as currently prescribed within South African financial services legislation. This taxonomical exclusion creates a regulatory lacuna whereby the Financial Sector Conduct Authority's (FSCA) statutory

mandate and supervisory powers do not extend to crypto asset activities conducted outside the purview of explicitly regulated financial products. This jurisdictional limitation has been acknowledged as presenting potential investor protection and market integrity concerns.

In response to this regulatory gap, the FSCA has engaged in collaborative regulatory development through its participation in the IFWG, a multi-stakeholder forum comprising representatives from the National Treasury, the South African Reserve Bank, and relevant regulatory authorities. This collaborative architecture facilitates the development of comprehensive regulatory standards for Crypto Asset Service Providers, with particular emphasis on establishing frameworks governing cross-border cryptocurrency transactions. This cooperative regulatory approach reflects contemporary governance models that emphasise inter-agency coordination in addressing complex, cross-cutting financial innovation challenges.

Impact of the Financial Sector Regulation Act, 2017 (FSRA)

The **Financial Sector Regulation Act, 2017 (FSRA)** introduced South Africa's *Twin Peaks* model, granting the FSCA authority over market conduct and enabling coordinated oversight across financial institutions. Although the Act does not explicitly regulate cryptocurrency, its framework allowed the FSCA to classify crypto assets as "financial products" under FAIS and extend AML/CTF obligations through FICA. These provisions improved consumer trust and market confidence, driving adoption through regulated entities while discouraging illicit activity. However, compliance costs created barriers for smaller entrants, and crypto remains outside legal tender status, limiting its use for everyday payments. Overall, FSRA accelerated formalisation of the crypto sector, shifting adoption toward investment and remittance channels under a regulated environment. (Financial Sector Regulation Act 9 of 2017, s 56)



Figure 21. Graphic indicating the linkage between the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017), its Legal Status and its Crypto Adoption trend (Researcher)

4.10.2 Amendments to FICA Schedules (2022)

Amendments to the FICA schedules added Crypto Asset Service Providers (CASPs) as accountable institutions, requiring them to comply with anti-money laundering (AML) and counter-terrorist financing (CTF) obligations. This is critical for blockchain-based cross-border transfers. (Financial Intelligence Centre Act 38 of 2001, Sch 1 item 22, as inserted by GN 2800 in GG 47596 of 29 November 2022, effective 19 December 2022)

Key Provisions:

The regulatory amendments to the Financial Intelligence Centre Act impose comprehensive anti-money laundering and counter-terrorist financing (AML/CTF) obligations upon Crypto Asset Service Providers (CASPs). These entities are required to register with the Financial Intelligence Centre as accountable institutions and implement a risk-based framework of preventive measures. The prescribed AML/CTF measures encompass customer due diligence procedures, including the identification and verification of clients, beneficial ownership determination, and ongoing monitoring of business relationships. Additionally, CASPs must establish and maintain transaction monitoring systems capable of detecting suspicious or unusual patterns indicative of money laundering, terrorist financing, or other illicit financial activities.

The institutional scope of these regulatory obligations extends to all entities engaged in the trading, conversion, or transfer of crypto assets on behalf of clients or as a principal activity. This definitional framework explicitly encompasses cross-border cryptocurrency transactions, thereby ensuring that virtual asset flows across jurisdictional boundaries are subject to equivalent regulatory scrutiny as domestic transactions. This comprehensive approach aligns with the Financial Action Task Force's revised standards for virtual asset service providers, which emphasise the necessity of applying AML/CTF controls regardless of the geographic nature of the transaction. (Financial Intelligence Centre Act 38 of 2001, Sch 1 item 22, as inserted by GN 2800 in GG 47596 of 29 November 2022, effective 19 December 2022)

Impact of the Financial Intelligence Centre Act (FICA)

The 2022 amendments to the Financial Intelligence Centre Act (FICA) schedules marked a pivotal shift in South Africa's cryptocurrency regulatory landscape by designating Crypto Asset Service Providers (CASPs) as *accountable institutions*. This inclusion subjected CASPs to stringent anti-money laundering (AML) and counter-terrorist financing (CTF) obligations, including customer due diligence, transaction monitoring, and suspicious activity reporting. These measures enhanced consumer protection and aligned South Africa with global FATF standards, mitigating systemic risks and reducing illicit activity. However, compliance requirements significantly increased operational costs, creating barriers for smaller entrants and consolidating market activity among larger, regulated platforms. Consequently, while informal participation declined, overall adoption continued to grow through licensed entities, reinforcing the formalisation of crypto markets within the financial system. (Financial Intelligence Centre Act 38 of 2001, Sch 1 item 22, as inserted by GN 2800 in GG 47596 of 29 November 2022)



Figure 22. Graphic indicating the linkage between the Amendments to FICA Schedules (2022)), its Legal Status and its Crypto Adoption trend (Researcher)

4.10.3 Visual Mapping of Regulatory Framework

The regulatory framework can be visualised through three key dimensions that illustrate the alignment of regulatory instruments with critical operational areas:

Regulation (Operational/Enforcement) Coverage across Study Dimensions

Regulation	Primary coverage Indirect/partial coverage No/limited coverage							
	Cross-border transfers & remittances	Exchange control & capital flows	Payment systems & cross-border EFT (CMA/SADC/CLS)	AML/CFT & IFTR reporting (FICA)	Crypto-assets & CASPs	Consumer protection / market conduct	Prudential / systemic stability	Tax treatment & compliance
Exchange Control Regulations, 1961 (1961)	Primary coverage	Primary coverage	Primary coverage	No/limited coverage	No/limited coverage	Primary coverage	No/limited coverage	No/limited coverage
FICA Schedules Amendments (2022) CASPs added	Primary coverage	Indirect/partial coverage	No/limited coverage	Primary coverage	Primary coverage	Indirect/partial coverage	No/limited coverage	No/limited coverage
SARB Draft Directive: Specific Payment Activities (2025)	Primary coverage	No/limited coverage	Primary coverage	Primary coverage	Indirect/partial coverage	Indirect/partial coverage	Indirect/partial coverage	No/limited coverage
SARB Directive No. 1 (2025) Low-value cross-border EFT (CMA)	Primary coverage	No/limited coverage	Primary coverage	Primary coverage	No/limited coverage	No/limited coverage	No/limited coverage	No/limited coverage

Figure 23. (Legislation): Demonstrates statutory foundations, including the Currency and Exchanges Act (1933), National Payment System Act (1998), Financial Intelligence Centre Act (2001), and Financial Sector Regulation Act (2017).

Supporting Guidelines Coverage across Study Dimensions

Primary coverage Indirect/partial coverage No/limited coverage								
Guideline / Position Paper	Cross-border transfers & remittances	Exchange control & capital flows	Payment systems & cross-border EFT (CMA/SADC/CLS)	AML/CFT & IFTR reporting (FICA)	Crypto-assets & CASPs	Consumer protection / market conduct	Prudential / systemic stability	Tax treatment & compliance
Currency & Exchanges Manual for Authorised Dealers FinSurv								
ADLA Manual Authorised Dealers with Limited Authority								
SARB Position Paper on Virtual Currencies (2014)								
IFWG Position Paper on Crypto Assets (2021)								
FIC Guidance Note 104A (Draft) on IFTR Financial Intelligence Centre								
SARS Crypto Assets & Tax Guidance South African Revenue Service								

Figure 24. (Supporting Guidelines): Highlights operational guidance such as the FinSurv Authorised Dealers Manual, ADLA Manual, SARB and IFWG position papers, FIC Guidance Note 104A, and SARS tax guidance. These documents operationalise compliance and clarify th

Legislation Coverage across Study Dimensions

Primary coverage Indirect/partial coverage No/limited coverage								
Legislation	Cross-border transfers & remittances	Exchange control & capital flows	Payment systems & cross-border EFT (CMA/SADC/CLS)	AML/CFT & IFTR reporting (FICA)	Crypto-assets & CASPs	Consumer protection / market conduct	Prudential / systemic stability	Tax treatment & compliance
Currency and Exchanges Act (1933)								
National Payment System Act (1998)								
				Financial Intelligence Centre Act (FICA, 2001)				
								Financial Sector Regulation Act (2017)

Key Observation: Legislative Gap in Cryptocurrency Coverage

Notice that **none of the four primary legislative Acts have primary coverage for crypto-assets & CASPs**. This represents a significant legislative gap, as regulation of cryptocurrencies currently relies on:

- **Indirect application** through FICA amendments (2022) adding CASPs to schedules
- **Regulatory directives and guidelines** rather than primary legislation
- **Interpretation and extension** of existing laws to cover novel digital assets

This gap highlights the need for dedicated cryptocurrency legislation or substantial amendment of existing Acts to provide clear legal foundation for comprehensive crypto-asset regulation in South Africa.

Figure 25. Regulation): Maps enforcement instruments, including Exchange Control Regulations (1961), FICA schedule amendments (2022) adding CASPs, and SARB directives on cross-border EFTs. These instruments ensure practical implementation and oversight.

Purpose of Diagrams

The three diagrams illustrate the alignment of regulatory instruments with eight critical dimensions: cross-border transfers and remittances; exchange control and capital flows; payment systems; AML/CFT and IFTR reporting; crypto-assets and CASPs; consumer protection; prudential/systemic stability; and tax compliance.

Integrative Discussion

The visual mapping confirms that South Africa's framework is robust in traditional exchange control and AML/CFT compliance, while coverage of crypto-assets remains emergent and policy-driven. The diagrams provide clarity on institutional roles and regulatory layering, supporting a more coherent narrative and informing subsequent analysis on regulatory gaps and reform pathways. The diagrammatic representations contribute substantially to analytical clarity by rendering visible the complex architecture of institutional roles, jurisdictional boundaries, and regulatory layering that characterise South Africa's financial governance system. These visual analytical tools facilitate identification of primary regulators (SARB for monetary policy and prudential oversight; FSCA for market conduct; FIC for financial intelligence), recognition of functional overlaps and coordination mechanisms, and understanding of how regulatory authority cascades from constitutional provisions through enabling legislation to operational guidelines and supervisory practices.

The enhanced clarity afforded by visual mapping methodologies strengthens the overall analytical narrative by providing empirical substantiation for claims regarding regulatory maturity, identifying structural relationships that might otherwise remain obscured in purely textual analysis, and establishing a foundation for evidence-based policy recommendations. Visual representation of complex regulatory structures enables

more precise characterisation of regulatory gaps, not merely as absences, but as specific lacunae within particular institutional domains, functional areas, or enforcement pathways.

This visual-analytical integration proves particularly valuable in informing subsequent examination of regulatory gaps and reform trajectories. By establishing baseline understanding of existing institutional configurations and regulatory coverage, the mapping exercises enable systematic gap analysis that can distinguish between: (1) regulatory voids (areas entirely outside current legal frameworks); (2) regulatory ambiguities (areas subject to interpretive uncertainty due to technological novelty or definitional challenges); (3) enforcement deficits (areas with nominal coverage but insufficient implementation capacity, resources, or expertise); and (4) coordination failures (areas where institutional mandates overlap without effective collaboration mechanisms). The findings demonstrate that South Africa's regulatory challenge is one of financial system integration, not technological prohibition. Cryptocurrency intersect with exchange control, AML/CFT, and payment system oversight, requiring adaptive governance of CASPs and crypto-asset transactions.

4.11 Key Observations and Regulatory Gaps

4.11.1 *Cross-Border Transfers and Remittances*

South Africa has a robust framework for regulating traditional cross-border transfers and remittances through the exchange control regime, AML/CFT reporting rules, and payment-system oversight. Exchange control is enabled by section 9 of the Currency and Exchanges Act (Currency and Exchanges Act 9 of 1933) and operationalised through the Exchange Control Regulations, including the restriction on the export of capital (Exchange Control Regulations, 1961, reg 10(1)(c)). Authorised Dealers and ADLAs are appointed to implement these controls under Treasury delegation (Orders and Rules under the Exchange Control Regulations, 1961, Orders 2–3). In addition, accountable institutions must file IFTRs for international transfers above the prescribed threshold and within the prescribed period (Financial Intelligence Centre Act 38 of 2001, s 31; Money Laundering and Terrorist Financing Control Regulations, regs 23D, 23E and 24(5)).

4.11.2 *Blockchain and Crypto Assets*

South Africa adopts a cautious approach to blockchain and crypto assets. Crypto assets are not legal tender, and cross-border transfers involving crypto are restricted under exchange control regulations. The IFWG's phased approach aims to regulate CASPs under FICA, but comprehensive legislation specific to blockchain is lacking. The "wait and see" approach has been criticised for not proactively addressing money laundering risks.

4.11.3 *Regulatory Challenges*

The decentralised nature of blockchain complicates AML enforcement, as there is no central authority to impose obligations. Current AML frameworks assume a centralised entity, making them less effective for crypto transactions. Additionally, the regulatory framework exhibits several specific challenges:

- Outdated regulations that fail to accommodate blockchain's unique characteristics
- Exchange control restrictions that limit legitimate blockchain innovation
- Institutional resistance from traditional banking institutions
- Knowledge gaps among regulators and policymakers regarding blockchain capabilities
- Integration challenges between blockchain systems and legacy financial infrastructure

4.11.4 *Future Developments*

Ongoing consultations (e.g., Draft Directive on Specific Payment Activities, comments due April 16, 2025) and SARB's exploration of central bank digital currencies (CBDCs) indicate a move toward integrating blockchain into the regulatory framework. However, the pace of regulatory adaptation remains a concern for industry stakeholders seeking clarity and enabling frameworks for innovation.

Comparative Table: Pros and Cons of Cryptocurrency Adoption under SARS Guidance

Impact Area	Pros (Drivers of Adoption)	Cons (Barriers to Adoption)	Key Sources
Regulatory clarity and recognition	Clear classification of 'crypto assets' and application of normal tax principles reduce uncertainty for investors and businesses; crypto is recognized within the tax system (not legal tender, but taxable asset).	Recognition without legal-tender status can limit use cases; taxpayers must determine revenue vs capital intent, which can be complex.	SARS guidance; IFWG position context
Institutional participation	Predictable tax treatment and the move toward global reporting standards (CARF) signal maturity, encourages institutions, exchanges, and service providers to operate in SA.	Institutions face new data, due-diligence and reporting obligations; higher compliance costs may reduce product breadth or raise fees.	KPMG summary of CARF adoption; SARS overview
Compliance and enforcement posture	Strong enforcement (exchange data sharing, blockchain analytics) promotes a level playing field and consumer protection; deters fraud.	Reduced privacy/anonymity, greater audit risk, and stricter monitoring can deter some users, especially casual or privacy-focused participants.	Taxify 2025 compliance/enforcement; SARS history and FAQs
Record-keeping and reporting	Clear expectations (declare gains/losses; maintain detailed records) help compliant users avoid penalties and integrate crypto into formal finance.	Burdensome tracking, especially for high-frequency trading, DeFi, or crypto-to-crypto disposals; proposed thresholds (e.g., >R50,000 reporting) add friction.	Taxify 2025 guide; SARS 'Do I need to pay tax on crypto assets?'
Cross-border use	Ongoing SARB work on rules suggests potential future channels for lawful international transfers, could unlock	Until SARB finalizes, crypto transfers abroad are illegal, curbing cross-border utility and enterprise adoption for payments.	SARS page (SARB note); IFWG/SARB references

	remittances/FX use cases.		
Global alignment and transparency	CARF + revised CRS (from 1 March 2026) integrate crypto into automatic information exchange, boosts SA's international standing and reduces regulatory arbitrage.	CASPs must implement new systems, suspend/terminate services for non-compliant self-certifications, possible service disruption during transition.	KPMG CARF/CRS briefing (Sep 25, 2025)
Investor protection and market integrity	Standard tax treatment of gains, income (staking/mining), and disposals helps normalize risk disclosure and investor behaviour.	Ambiguity remains for certain DeFi mechanics; misclassification (capital vs revenue) can lead to disputes and retroactive assessments.	VAT about legal/tax analysis; Taxify updates on DeFi guidance
Cost of participation	Compliance provides long-term stability and access to regulated services; clearer paths to mainstream adoption.	Administrative time, software/tools, and professional advice raise the effective cost of using crypto, may slow retail adoption.	Taxify 2025; SARS FAQs & guidance

Table 2. This table summarises the potential drivers and barriers to cryptocurrency adoption under SARS's Crypto Assets & Tax Guidance. Sources include SARS official guidance, KPMG CARF briefings, and Taxify compliance updates.

4.12 Empirical Research Findings: Industry Perspectives on Cryptocurrency Implementation

4.12.1 Research Methodology and Respondent Background

This section presents findings derived from semi-structured interviews conducted with industry experts, regulatory bodies, and stakeholders involved in the cryptocurrency landscape in South Africa. Eight respondents were selected through purposive sampling, holding positions as middle, senior and executive managers within financial and cryptocurrency companies. Respondents were chosen based on their ability to provide substantive responses to the research questions and their direct involvement with blockchain technology, cross-border payments, or financial regulation. The interview data is less explicit than the data from document review but it does offer

confirmation of the findings from the document review and encourages the researcher to build a knowledge model.

Due to agreed confidentiality prescripts, respondents are assigned unique numerical codes from Respondent 1 through Respondent 8. The interviews were conducted using a semi-structured format that allowed for in-depth exploration of three key research dimensions:

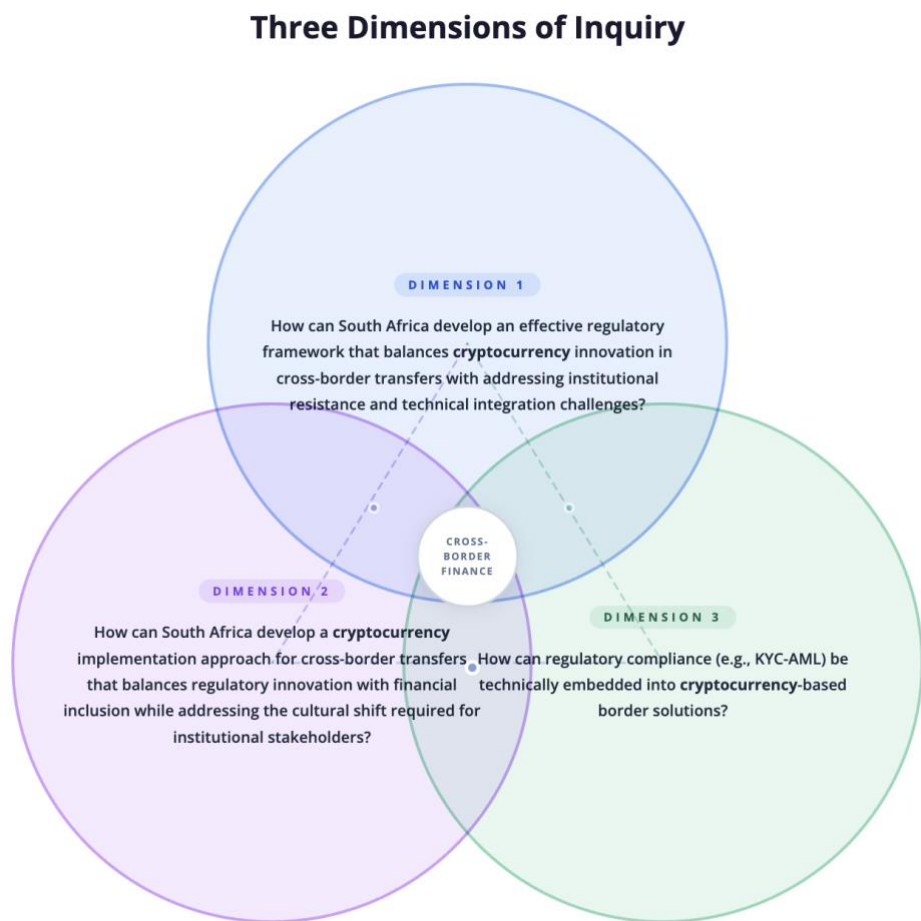


Figure 26. This diagram highlights the 3 dimensions of inquiry (Researcher)

The data analysis employed thematic analysis following established qualitative research methodologies, utilising Atlas.ti software for coding and identifying recurring themes. The analysis was structured to provide a comprehensive understanding of regulatory challenges and potential mitigations associated with implementing blockchain solutions for cross-border payments.

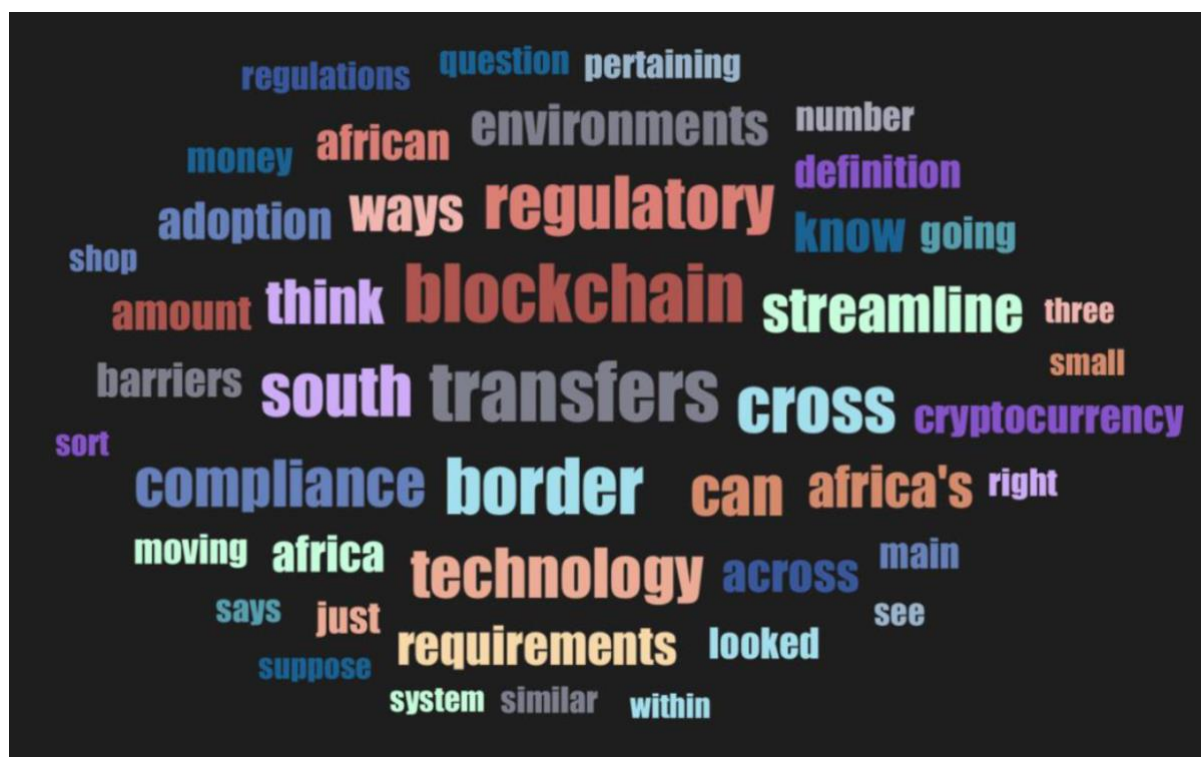


Figure 27. Atlas.ti Word cloud derived from interviews

Overall Approach to Data Analysis

The overall approach taken to analyse the data was primarily qualitative and involved several key steps:

- a) *Thematic Analysis*: The data collected from interviews were analysed using a thematic analysis approach, following Creswell's six steps: organising and preparing data, initial reflection, coding the data, identifying themes and descriptions, connecting themes, and making final interpretations. This systematic process allowed for the identification of key themes and patterns related to regulatory challenges and mitigations.

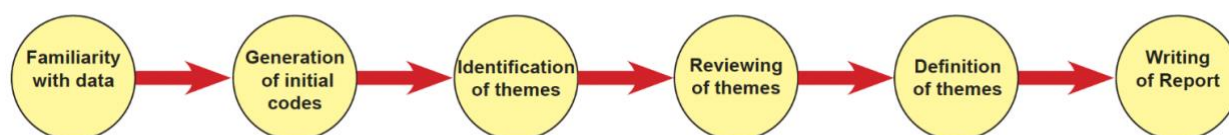


Figure 28. Thematic analysis process (Researcher)

- b) *Coding Process*: The transcribed interviews were coded using Atlas.ti software, which facilitated the organisation of qualitative data and the identification of recurring themes. The coding process involved breaking down the data into segments, categorising similar responses, and identifying overarching themes related to regulatory uncertainty and its implications.

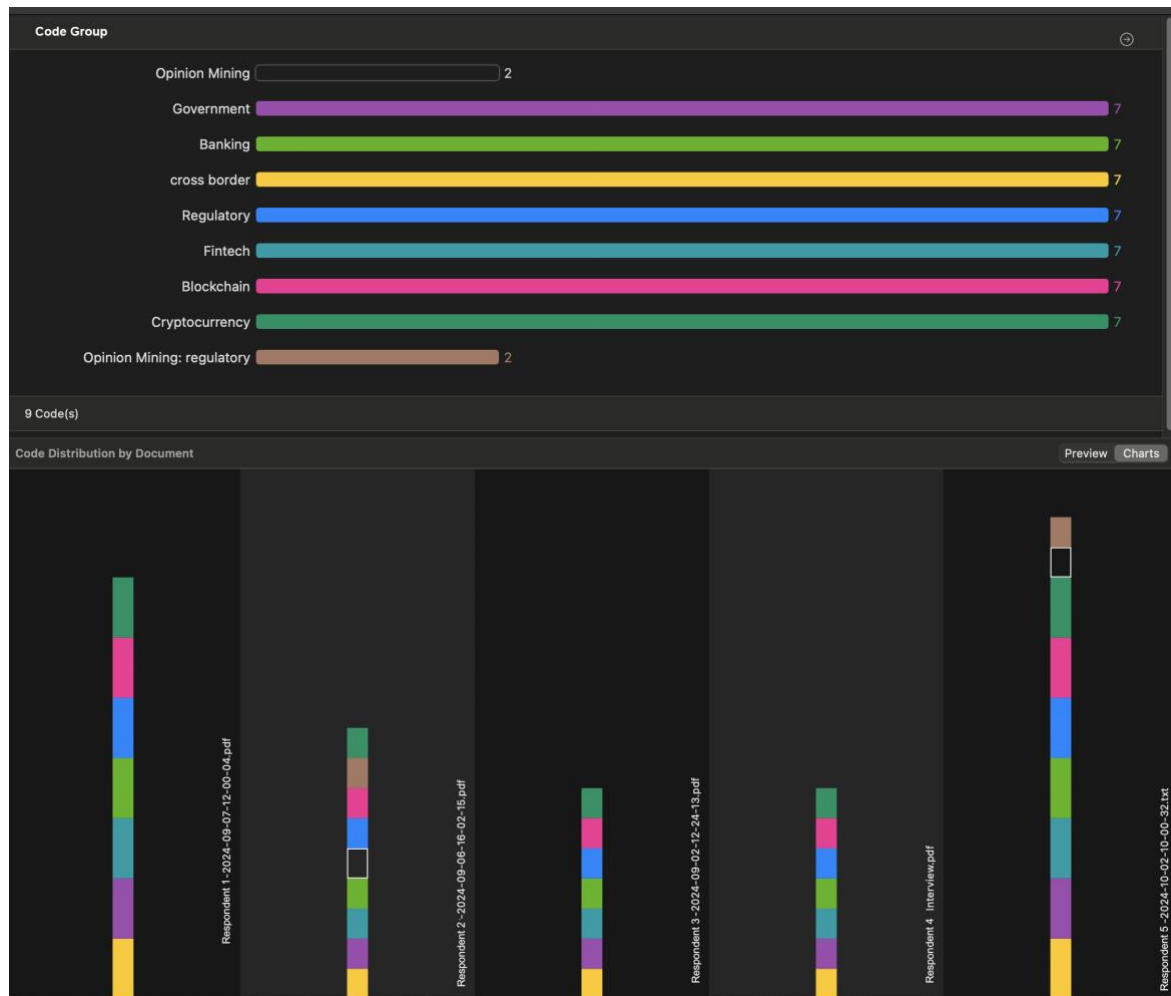


Figure 29. Atlas.ti graphic representation of code groups and frequency of mentions in interviews

- **Triangulation**: To enhance the credibility and validity of the findings, a triangulation approach was employed. This involved cross-referencing insights from interviews with the findings from the literature and interrogation of the theoretical frameworks. By corroborating evidence from multiple sources, the analysis aimed to provide a comprehensive understanding of the regulatory landscape for blockchain technology in South Africa.

• **Visual Representation:** Data visualisation techniques, such as word frequency queries and thematic maps, were utilised to present the findings in a clear and accessible manner. These visual representations helped to illustrate key themes and the relationships between various regulatory challenges and stakeholder sentiments.

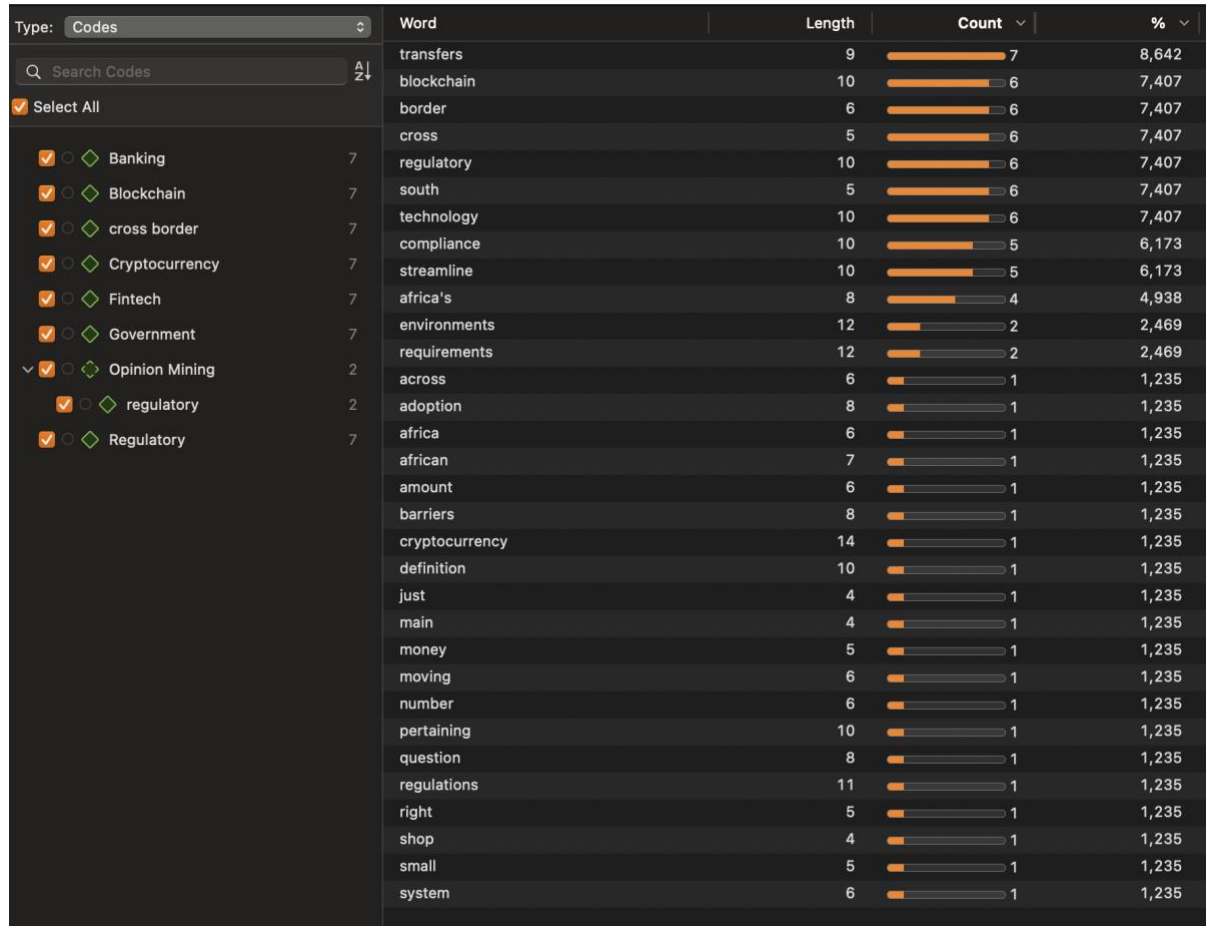


Figure 30. Atlas.ti graphic representation of key codes and frequency of word use in interviews

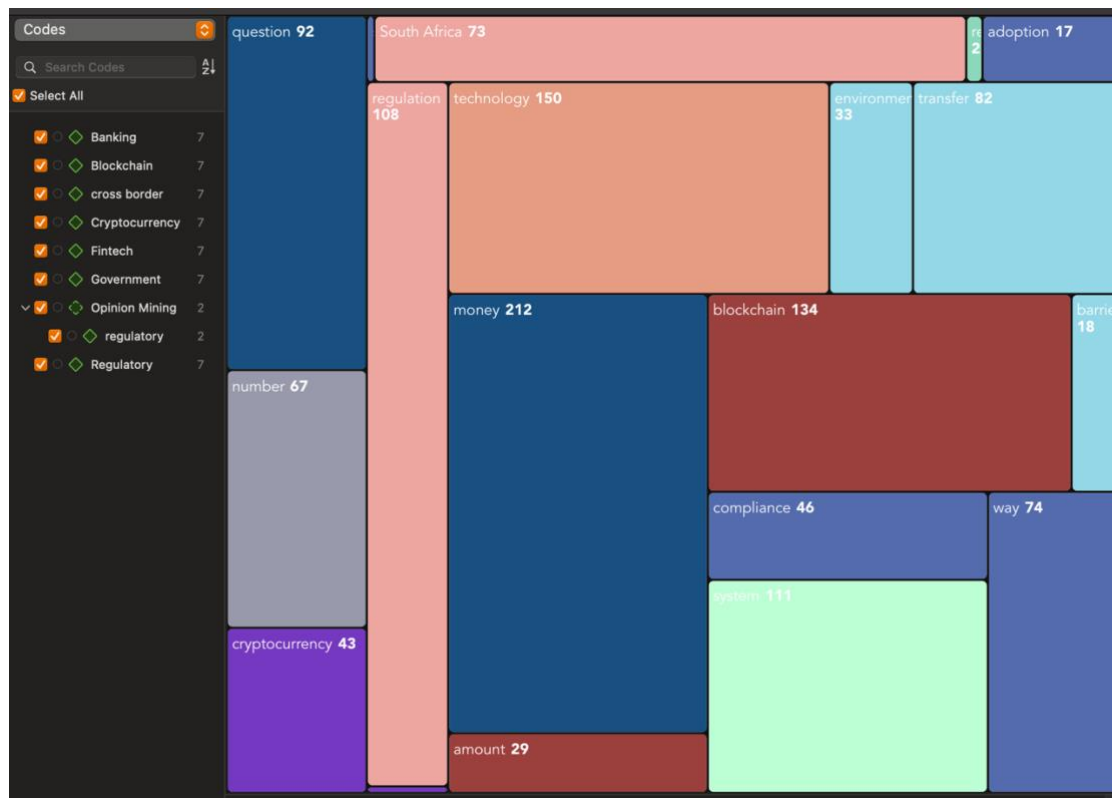


Figure 31. Atlas.ti graphic representation of key concepts and frequency use in interviews

By employing a combination of qualitative methods and data sources, the analysis aimed to provide a rich and nuanced understanding of the regulatory challenges and mitigations of blockchain solutions in relation to South African cross-border payments.

Theme	Key Code	Frequency of Mention
Regulatory Challenges	Outdated Regulations	8
	Exchange Controls	7
	Bank Resistance	9
	Slow Adoption	6
Compliance and Transparency	AML/KYC Benefits	7
	Smart Contract Compliance	6

Theme	Key Code	Frequency of Mention
	Regulatory Oversight	5
Financial Inclusion	Lower Remittance Costs	8
	Digital Identity Solutions	7
	Unbanked Access	6
Blockchain Risks	Regulatory Uncertainty	5
	Taxation Issues	6
	Loss of Financial Oversight	5
Future of Blockchain	CBDCs vs Crypto	7
	Private Sector Innovation	9
	Global Regulatory Trends	8

Table 3. Tabular representation of the key codes and their frequency of mention across interviews

4.13 Dimension 1: Regulatory and Compliance Framework Analysis

4.13.1 Current Regulatory Inadequacy and Institutional Resistance

The research reveals a regulatory environment that respondents characterise as fundamentally inadequate for addressing cryptocurrency technology's unique characteristics. Multiple respondents (2024) interviewed described the current framework as "totally inadequate," with blockchain technology being "frowned upon" by authorities. This regulatory inadequacy creates critical gaps between technological capabilities and regulatory frameworks, potentially limiting South Africa's ability to leverage blockchain's benefits for financial inclusion and economic development.

The inadequacy extends beyond mere absence of specific cryptocurrency regulations to encompass institutional attitudes that impede innovation. Respondent 5 (2024) warned that the current "wait-and-see approach will leave South Africa behind" international trends, while Respondent 3 (2024) described blockchain as offering "a paradigm shift in compliance efficiency" that regulators have yet to embrace fully. Traditional financial institutions maintain what respondents describe as a "fortress mentality," viewing blockchain as a threat rather than an opportunity. Banks derive substantial income from SWIFT transaction fees, currency conversion charges, and other services that blockchain technology could potentially disrupt. This creates entrenched economic interests in maintaining current systems. Respondent 2 (2024) noted that many financial leaders and policymakers come from an "analogue era" of finance, lacking the digital fluency necessary to understand blockchain's potential benefits.

4.13.2 *Real-Time Compliance Enhancement Opportunities*

Despite regulatory resistance, the research reveals that blockchain technology offers unprecedented opportunities for enhancing regulatory compliance through real-time monitoring capabilities. Respondents 4 and 6 (2024) emphasised that blockchain's distributed ledger technology "records transactions instantaneously and irrevocably," enabling regulators to trace the origin, destination, and ownership of funds with what experts describe as "mathematical certainty." This capability represents a fundamental improvement over current systems that depend on batch processing and manual reporting. Respondent 5 (2024) highlighted that blockchain enables "suspicious activity to be flagged in real time rather than after the fact," representing a significant advancement over systems such as SWIFT that rely on intermediary-based validation and end-of-day settlement reconciliations.

The immutable nature of blockchain ledgers provides regulators with unprecedented visibility into financial transactions. Respondent 7 (2024) stated that blockchain technology can "trace payment histories with mathematical certainty," providing capabilities that "map the entire lifecycle of transactions within the blockchain ecosystem." This level of traceability far exceeds traditional financial systems, where transaction histories become opaque once funds enter the broader banking network.

4.13.3 *Anti-Money Laundering and Know Your Customer Enhancement*

Blockchain technology demonstrates particular strength in addressing AML and KYC regulatory requirements. Six respondents (Respondents 1, 2, 4, 5, 7, and 8) (2024) stated that blockchain "eliminates a lot of AML activities" by ensuring "every transaction can be traced to its origin, down to the exact source of funds, which is in stark contrast to the opacity of fiat-based transactions."

The pseudonymous nature of blockchain transactions, often cited as a compliance concern, actually enhances regulatory oversight when properly implemented. Respondents 2, 6 and 8 (2024) emphasised that blockchain "actually enhances compliance with AML and KYC regulations because of its inherent transparency," challenging "prevailing regulatory scepticism regarding anonymity risks." Every transaction is recorded on public ledgers, and with appropriate regulatory tools and identity protocols, blockchain can surpass traditional systems in providing clear audit trails for financial regulators.

Traditional AML and KYC processes suffer from significant inefficiencies that blockchain technology could address. FICA currently requires "repeated documentation submissions across multiple institutions, creating redundancy and inefficiency," according to Respondents 5 and 6 (2024). A blockchain-based digital identity system could fundamentally streamline this process by creating a centralised, secure repository for verified KYC information that multiple institutions could access while maintaining compliance and privacy standards.

4.13.4 *Digital Identity Solutions and Smart Contract Implementation*

The research identified substantial potential for blockchain-based digital identity systems to streamline compliance processes while enhancing security and privacy protections. Self-sovereign identity (SSI) systems represent a transformative approach to digital credentialing that could address persistent compliance challenges. These systems "allow individuals to control and share their identity data directly with third

parties, ensuring consent-driven data sharing while maintaining compliance with legal requirements". Respondents 1, 4, 8 (2024).

The application of Non-Fungible Tokens (NFTs) for identity verification represents an innovative approach that could significantly impact financial inclusion. Respondent 6 (2024) suggested that "NFTs could create secure, non-replicable digital IDs," making them "ideal for linking verified identity with blockchain wallets." This technology could be particularly impactful for financial inclusion, allowing individuals without traditional identity documents to access financial services through cryptographically secured, tamper-proof identification mechanisms. Smart contracts emerge as particularly promising technological components for regulatory enforcement, offering potential to automate compliance processes and reduce human error. Respondent 4 and 7 (2024) explained that these "self-executing contracts, embedded with legal and regulatory conditions, can automate transaction approvals, flag suspicious activity, and enforce KYC or AML requirements in real time."

The potential applications of smart contracts in South African regulatory frameworks are extensive. Smart contracts could be designed to "prohibit transactions above a certain threshold unless KYC verification is complete and regulatory checks are satisfied," according to Respondent 5, 6 and 7 (2024). Such automated enforcement mechanisms could reinforce Financial Sector Conduct Authority (FSCA) frameworks by creating conditions where "compliance rules are enforced automatically," thereby reducing both human error and intentional circumvention of regulatory requirements.

4.13.5 Integration Challenges and System Incompatibility

Despite blockchain's compliance advantages, integration with South Africa's existing financial infrastructure presents substantial technical and operational challenges. The current financial ecosystem relies heavily on "centralised messaging protocols such as SWIFT and systems designed for batch processing and end-of-day reconciliation," according to Respondent 5 (2024). These systems are "inherently incompatible with the real-time, peer-to-peer architecture of blockchain networks." The fundamental incompatibility represents more than a technical challenge; it constitutes a conceptual mismatch between different paradigms of value transfer. Respondents 1, 2,

and 7 (2024) articulated that "SWIFT messages and ISO 20022 are built for a structured world; blockchain is more like the internet: fluid, immediate, and decentralised." This paradigmatic difference necessitates comprehensive architectural changes rather than simple system additions.

Technical barriers extend beyond system architecture to include practical implementation challenges. Key issues include "a lack of standardised application programming interfaces (APIs) that allow blockchain platforms to interface with traditional core banking software," according to Respondent 4 (2024). Additionally, the on/off-ramping process, where users convert between crypto assets and fiat currency, faces complications from "inconsistent banking support and regulatory uncertainty." The unpredictability of banking support creates significant compliance risks. Respondents 3, 5, and 8 (2024) revealed that major South African banks have "summarily cut ties with crypto platforms due to risk committee decisions, pushing users toward unregulated alternatives." This institutional volatility forces users to seek alternative, potentially unregulated channels for blockchain-based financial services, undermining regulatory objectives.

All respondents identified a critical barrier: the shortage of qualified professionals who understand both blockchain technologies and legacy financial systems. This talent gap was described by multiple respondents as "the biggest bottleneck to integration." The scarcity of professionals capable of bridging the technological divide between traditional banking and blockchain systems significantly impedes implementation efforts.

4.13.6 *Implications and Reform Requirements*

The findings suggest that South Africa requires a comprehensive regulatory transformation to effectively leverage blockchain technology for cross-border transfers. The current framework's inadequacy necessitates fundamental shifts in regulatory approach from restrictive gatekeeping to collaborative facilitation of innovation. This transformation requires more than technical adjustments; it demands "a cultural shift in how regulators view their role," according to Respondents 2, 5 and 8 (2024).

The implications extend to regulatory capacity building, with experts emphasising the need for "secondments, training, and public-private working groups" to address the current skills gap. The regulatory transformation must encompass multiple dimensions of institutional change, including policy development, enforcement mechanisms, and international cooperation frameworks. Economic implications are equally significant. Current cross-border transfer systems impose costs reaching 8-11% of transfer amounts, what Respondent 1 (2024) described as "daylight robbery." Blockchain implementation within appropriate regulatory frameworks could dramatically reduce these costs, potentially improving South Africa's economic competitiveness and enhancing financial inclusion for millions of citizens.

4.14 Dimension 2: Technological and Compliance Enhancements

4.14.1 *Enhanced Transaction Monitoring and Auditability*

Blockchain technology introduces a paradigm shift in compliance efficiency by offering immutable, transparent ledgers that enable real-time transaction monitoring with unprecedented accuracy and reliability. Unlike traditional systems that depend on batch processing, manual reporting, and end-of-day reconciliation, blockchain's distributed ledger technology records transactions instantaneously and irrevocably.

Respondents 3, 5, 7 and 8 (2024) emphasised that blockchain enables tracing of payment histories with "mathematical certainty," offering regulators an immutable audit trail that surpasses traditional banking systems in both accuracy and comprehensiveness. This capability directly addresses one of the most persistent challenges in cross-border compliance: the difficulty of tracking funds across multiple jurisdictions, intermediaries, and currency conversions.

Current SWIFT-based cross-border transfers rely on complex networks of correspondent banks, each maintaining separate records and performing independent reconciliation processes. This architecture creates temporal gaps and information asymmetries where suspicious activities may go undetected until well after transactions are completed. Blockchain's real-time settlement capability eliminates these blind spots, enabling what experts describe as "real-time compliance," where regulatory adherence is verified instantaneously rather than through time-delayed post-transaction audits.

4.14.2 *Combating Financial Crime Through Blockchain Transparency*

Respondents 1, 3, 5, 5, 6, and 7 (2024) emphasised that blockchain is "a much better technology to actually police and enforce AML regulations compared to traditional fiat currency systems." This superiority stems from blockchain's inherent transparency, where every transaction is recorded on a public ledger, creating an immutable trail that can be traced back to the genesis of the blockchain network. This transparency advantage becomes particularly evident when compared to traditional cash-based or conventional banking systems. In traditional systems, once cash is withdrawn from the banking system, its movement becomes virtually untraceable. Blockchain eliminates these limitations by maintaining a complete, immutable record of every transaction from creation to current ownership.

Respondents 2, 3, 4, and 7 (2024) observed that "with digital currency, every transaction is traceable from inception," contrasting sharply with traditional fiat currency that "loses traceability after withdrawal." The implications for financial crime prevention are substantial. Money laundering schemes typically depend on obscuring the trail of illicit funds through complex transaction chains, multiple jurisdictions, and conversion between different financial instruments. Blockchain's complete transaction history makes these obfuscation strategies significantly more difficult to execute successfully.

A critical aspect of blockchain's compliance enhancement lies in addressing widespread regulatory concerns about transaction anonymity. Expert analysis reveals a fundamental misunderstanding in regulatory discourse: blockchain is not inherently anonymous but pseudonymous, with every wallet transaction visible on open blockchains. Respondent 2, 3,5 and 6 (2024) argued that the perceived anonymity problem stems from "a lack of understanding" among regulators and policymakers about blockchain's actual transparency characteristics.

4.14.3 Self-Sovereign Identities and NFT-Based Verification

The integration of Non-Fungible Tokens (NFTs) into identity verification represents a significant technological advancement for KYC compliance. Respondent 3, and 6 (2024) stated that NFTs can create "secure, non-replicable digital IDs" that provide immutable proof of identity verification, particularly beneficial for populations without traditional documentation or formal banking relationships.

This capability is especially relevant in South Africa's context, where significant portions of the population lack conventional banking documentation required for traditional KYC processes, creating barriers to financial inclusion. NFT-based identity systems address multiple compliance challenges through a single technological solution. They provide cryptographically secured proof of identity verification that cannot be duplicated, falsified, or manipulated, while enabling instant verification across multiple institutions without requiring repeated documentation submission. Self-sovereign identity (SSI) systems represent a fundamental paradigm shift in how identity verification and compliance are managed in financial services, moving from institution-controlled identity management to user-controlled, consent-driven identity sharing. Respondent 4 explained that these systems allow individuals to control and share their identity data directly with third parties while ensuring consent-driven data sharing that maintains compliance with legal requirements and privacy regulations.

The implementation of SSI systems could dramatically reduce both compliance costs and consumer friction while actually improving regulatory visibility and oversight capabilities. Instead of the current system requiring repeated documentation submission and verification across multiple institutions, a blockchain-based SSI system would enable instant verification while maintaining comprehensive audit trails that enhance rather than compromise regulatory compliance.

4.14.4 Smart Contracts and Automated Regulatory Enforcement

Smart contracts represent perhaps the most revolutionary aspect of blockchain's compliance enhancement capabilities, enabling the direct embedding of legal and regulatory conditions into transaction logic through programmable, self-executing

contracts. These contracts can automatically enforce compliance requirements in real-time, eliminating the delays, errors, and opportunities for circumvention that characterise traditional compliance monitoring systems. Expert analysis suggests that smart contracts could be designed to reinforce Financial Sector Conduct Authority (FSCA) frameworks by creating conditions where "compliance rules are enforced automatically," reducing both human error and intentional circumvention while providing regulators with unprecedented visibility into system-wide compliance status.

The practical applications of smart contract-based compliance automation are extensive and transformative. Smart contracts could automatically:

- Prohibit transactions above certain thresholds unless KYC verification is complete and current
- Flag suspicious patterns for immediate regulatory review
- Ensure that cross-border transfers comply with exchange control limits
- Automatically generate required regulatory reports

This automation creates what experts describe as "programmable compliance" where regulatory requirements are embedded in the transaction infrastructure itself rather than monitored and enforced after the fact. The integration of smart contracts with regulatory reporting systems could fundamentally transform how financial institutions interact with regulators. Rather than relying on periodic batch reports that may be incomplete, delayed, or inaccurate, smart contract-enabled systems could provide continuous, real-time reporting of relevant transactions and compliance metrics.

4.14.5 Managing Blockchain-Specific Compliance Risks

While blockchain offers superior capabilities for compliance and transparency, its implementation requires careful attention to blockchain-specific risks that must be addressed through appropriate regulatory frameworks and technical standards. Anonymity concerns, while often overstated, represent legitimate regulatory considerations that require sophisticated identity protocols and off-chain data verification to ensure compliance without undermining privacy rights.

The key insight is that blockchain's transparency can actually enhance rather than hinder regulatory oversight when properly implemented with appropriate identity protocols. With suitable technical architecture, blockchain systems can provide better visibility into transaction flows than traditional banking systems while maintaining necessary privacy protections for legitimate users and compliance with data protection regulations. Cybersecurity risks represent another critical consideration, particularly regarding smart contract vulnerabilities that could be exploited by malicious actors. Respondent 8 (2024) noted that smart contracts are vulnerable to coding errors and exploitation, requiring minimum security and auditing standards as well as clear legal remedies for unintended outcomes. Regulatory frameworks must anticipate these risks without stifling innovation, requiring technical expertise within regulatory bodies and clear standards for smart contract development, testing, and deployment in financial services applications.

Respondents 2, 5, 6 and 7 (2024) referenced the Nigerian experience with cryptocurrency adoption, providing important lessons about avoiding "forced innovation" failures where cryptocurrency technology is implemented without aligned regulatory frameworks, resulting in chaos and loss of public trust. South Africa's approach must balance innovation promotion with careful preparation, ensuring that regulatory frameworks are adapted before large-scale blockchain implementation.

4.15 Dimension 3: Socio-Economic and Global Implications

4.15.1 Financial Inclusion Through Cost Reduction

South Africa's cross-border financial system currently imposes what experts characterise as "prohibitive costs, ranging from 12% to 17% per transaction, on migrant workers and low-income users who rely on cross-border transfers for family support," according to Respondent 3 (2024). This cost structure creates a system of financial exclusion where access to cross-border financial services is determined by economic status rather than need.

Respondent 1 (2024) described current remittance fees as "daylight robbery," emphasising that these charges constitute an unfair burden that disproportionately

affects those least able to bear it. This assessment is supported by multiple respondents who emphasised that current transaction costs of 8-11% make traditional remittance systems fundamentally inaccessible to low-income users. Blockchain technology offers a direct solution to the cost crisis through the elimination of intermediaries. Traditional cross-border transactions require multiple intermediaries, each extracting fees while adding processing time and complexity. Respondent 8 stated that "these costs are not simply a function of profit-maximisation but stem from complex layers of intermediaries, compliance structures, and currency conversion regulations."

The transformative potential of blockchain lies in its ability to enable "direct, peer-to-peer value transfers, reducing fees to negligible levels while increasing speed and reliability," according to Respondent 4 (2024). This technological capability could fundamentally alter the economics of cross-border transactions, making them accessible to populations currently excluded from formal financial services.

4.15.2 Digital Identity Innovation and Self-Sovereign Solutions

Beyond cost reduction, blockchain addresses the fundamental barrier of identity verification that excludes millions from formal financial services. The current system requires "government-issued identification or proof of residence" that many South Africans and cross-border migrants cannot provide, according to Respondent 6. This creates a circular exclusion where those most in need of financial services are systematically denied access. Blockchain-based digital identity systems, particularly "self-sovereign identity (SSI) models and NFT-based credentials," offer a revolutionary alternative that could "securely verify identity through biometric data, mobile credentials, or verified attestations from trusted entities, without requiring state-issued documents," according to Respondent 5 (2024).

Respondents 2 and 8 (2024) supported this potential, arguing that blockchain-based identity solutions "cannot be stopped" and "work better for inclusion than any banking solution we've seen." Respondent 4 (2024) specifically highlighted how NFTs could create "secure, non-replicable digital IDs" that could help unbanked individuals without traditional documentation access financial services. The convergence of cost reduction and identity innovation through blockchain technology could generate profound socio-

economic benefits. Respondent 7 (2024) noted that "lowering remittance costs and removing identification barriers would enhance disposable income for millions, reduce dependency on informal money transfer systems, and improve economic participation among the underserved."

This transformation is particularly significant in South Africa's post-pandemic economic context, where economic inequality and unemployment remain at crisis levels. Blockchain technology offers the potential for what Respondent 6 (2024) described as a "leapfrogging effect, circumventing inefficient legacy systems and directly establishing inclusive, secure, and accessible financial infrastructure."

4.15.3 Cross-Border Collaboration and Regulatory Harmonisation

The global nature of cross-border transactions necessitates international cooperation for cryptocurrency adoption to achieve its full potential. Respondent 4 and 6 (2024) stated that "current cross-border systems are fragmented, with regulatory inconsistency and jurisdictional silos that inhibit seamless international blockchain operations." The challenge is particularly acute because cross-border transfers inherently involve multiple regulatory regimes, requiring "harmonisation of digital currency, identity verification, and AML/KYC frameworks," according to Respondent 8 (2024). Without coordinated international approaches, blockchain implementation risks creating new forms of regulatory arbitrage that could undermine financial stability and security.

South Africa's participation in BRICS (Brazil, Russia, India, China, and South Africa) presents a unique opportunity for coordinated blockchain adoption. Respondent 1 identified "Central Bank Digital Currencies (CBDCs) for wholesale or retail use among BRICS nations" as a promising development path that could "enable instant settlement across national borders, bypassing the dollar-dominated SWIFT system and reducing currency conversion risks."

Multiple respondents supported this direction, noting that BRICS countries are increasingly saying, "when we do transactions between ourselves, let's not use the dollar, let's use our own digital currency." This represents a significant geopolitical shift that could enhance monetary sovereignty while improving transaction efficiency.

The technical feasibility of such cooperation is demonstrated by successful international implementations. Respondent 7 (2024) referenced involvement in an Asian Development Bank project that "brought all the banks in Asia together" and proved that "not only can we do remittances cross-border using this technology, we proved that we can do delivery versus payment, meaning connecting the stock exchanges to the central banks, real-time, cross-border, using internet-type blockchain technology."

4.15.4 *Learning from Global Best Practices*

The interviews reveal significant awareness of international best practices that South Africa could emulate. Respondent 6 (2024) emphasised that policymakers should include private sector experts and learn from successful countries, specifically mentioning "Sweden, Dubai, Japan, Thailand, Singapore" and noting that "first-world countries developing central bank digital currencies" have shown willingness to support developing nations. However, the research reveals significant limitations in South Africa's current approach. Respondents 1, 2, and 5 (2024) noted that "South Africa's current posture on international cooperation remains limited and reactive" with "the exclusion of start-ups and private sector innovators from regulatory dialogues" and "the lack of South African presence in international blockchain working groups."

This reactive stance contrasts unfavourably with countries that are "actively aligning blockchain policy across jurisdictions, ensuring that remittances, investments, and data exchanges are recognised and streamlined across borders." Respondent 5 (2024) specifically criticised how the "South African government is on the side-lines of international discussions" while "private South African companies are working with international entities" but "domestic working groups exclude third parties and start-ups."

4.15.5 *Future Outlook and Continental Leadership*

The future potential of blockchain adoption in South Africa extends significantly beyond cross-border payments to encompass broader transformation of the country's institutional and governance systems. Multiple respondents suggested that blockchain could drive "a comprehensive transformation of the country's financial, legal, and

governance ecosystems, driven by blockchain's capacity to embed trust, automate regulation, and ensure real-time oversight".

This transformation potential includes applications in "land registries, social grants, and procurement systems" that could be "placed on-chain, creating transparent and tamper-proof governance mechanisms." Such applications are particularly significant in South Africa's context, where state capture and corruption have eroded public trust, according to Respondent 4 (2024). South Africa's technological maturity and geopolitical positioning create opportunities for continental leadership in blockchain adoption. Respondents suggest that South Africa could serve as "the anchor of an 'African Union blockchain currency' or as a central node in a pan-African digital identity network." These initiatives could have transformative effects on intra-African trade and economic integration.

Respondent 3 (2024) specifically discussed the potential for blockchain to support "an African Union similar to the EU's digital currency" and create opportunities for "wholesale CBDC as a trading token between African countries" that could generate "an African Union coin backed by national currencies." Such developments could reduce capital flight and build economic resilience across the continent. The successful implementation of blockchain technology could provide South Africa with significant soft power advantages in the global economy. Respondent 1 (2024) suggested that "by developing exportable regulatory models, South Africa could become a reference point for other African and Global South nations navigating the blockchain transition."

4.15.6 *Balancing Innovation with Security and Regulatory Integrity*

While blockchain technology offers transformative potential, expert analysis emphasises that "innovation must not come at the expense of regulatory integrity, financial security, or social protection," according to Respondent 2 (2024). The risks associated with blockchain implementation, including anonymity concerns, regulatory arbitrage, cyber vulnerabilities, and integration complexity, require proactive, principle-based governance. Expert testimony reveals that the primary challenges are institutional rather than technological. Several respondents (2024) observed that "the main risks aren't technological, they're institutional," with "resistance from banks, legal

uncertainty, and policymaker unfamiliarity" continuing to "slow down progress, reinforcing inequality in digital access and innovation outcomes." To address these challenges, respondents recommend transitioning "from a compliance-first model to a trust-and-verify approach rooted in digital transparency." This approach would involve "regulatory frameworks that allow phased implementation of blockchain solutions with built-in oversight mechanisms."

All Respondents strongly support the use of regulatory sandboxes for blockchain innovation. The analysis recommends that "regulatory sandboxes should be scaled and made permanent, allowing for iterative policy development based on real-world use cases." Respondent 8 (2024) specifically suggested creating "a 'regulatory sandbox' with temporary regulations to kickstart innovation." However, respondents consistently warned against the risks of excessive regulation that could stifle innovation. Respondent 5 (2024) specifically argued that additional regulation would be "counterproductive due to costs and complexity" and that more regulation would make "the transaction chain longer and more difficult to understand." This perspective suggests that regulators should adopt a facilitative posture, setting guardrails while enabling experimentation.

4.16 Summary

This chapter has provided a comprehensive examination of South Africa's regulatory framework for cross-border money transfers and cryptocurrency technology, integrating detailed analysis of legislative instruments with empirical research findings from industry experts. The analysis reveals a sophisticated but incomplete regulatory architecture that excels in traditional financial oversight but struggles to accommodate cryptocurrency innovation. The combined analysis of the legislative review and expert interview data indicates that South Africa is presently in a transitional phase of cryptocurrency adoption, characterised by incremental regulatory incorporation rather than comprehensive legislative reform. Existing legal instruments, including financial conduct regulation, anti-money laundering and counter-terrorist financing (AML/CFT) frameworks, and exchange control measures, are being extended to cover crypto-asset activities through interpretive adaptation rather than the enactment of purpose-built cryptocurrency legislation.

This approach reflects a risk-based regulatory orientation consistent with international standards, where supervisory focus is directed toward crypto-asset service providers and financial activities rather than underlying technologies. However, the absence of an integrated and consolidated crypto-asset legal framework contributes to regulatory uncertainty, institutional caution, and fragmented oversight responsibilities. The findings therefore suggest that South Africa is neither resistant to cryptocurrency adoption nor fully legislatively prepared; instead, it is engaged in a process of progressive regulatory assimilation, in which legacy financial governance structures are gradually being recalibrated to accommodate emerging crypto-asset ecosystems within the cross-border payments environment. The regulatory framework, built on foundations including the Currency and Exchanges Act (1933), National Payment System Act (1998), Financial Intelligence Centre Act (2001), and Financial Sector Regulation Act (2017), provides robust mechanisms for exchange control, payment system governance, and AML/CFT compliance. However, this framework was designed for centralised, intermediary-based systems and requires adaptation to leverage blockchain's unique characteristics.

Industry perspectives reveal that blockchain technology offers unprecedented opportunities for enhancing regulatory compliance through real-time monitoring, automated enforcement, and comprehensive transaction traceability. The technology's potential for financial inclusion through cost reduction and digital identity innovation could address some of South Africa's most pressing developmental challenges. However, realising these benefits requires overcoming significant barriers, including institutional resistance, knowledge gaps, system incompatibility, and regulatory uncertainty. The path forward requires comprehensive regulatory transformation that moves from restrictive gatekeeping to collaborative facilitation of innovation. This transformation must balance innovation promotion with prudential oversight, enhance international cooperation, and invest in capacity building across all stakeholders. Most importantly, it requires recognising that blockchain represents not merely a technological innovation but a strategic opportunity for enhancing South Africa's economic competitiveness, financial inclusion, and regional leadership.

The evidence suggests that with appropriate regulatory frameworks, collaborative governance structures, and sustained commitment, blockchain technology can

transform South Africa's cross-border financial system in ways that enhance regulatory compliance, improve financial inclusion, reduce costs, and increase operational efficiency. The question facing policymakers is not whether this transformation will occur globally, but whether South Africa will lead or follow in its implementation, and whether the benefits will accrue to South African users and institutions or to competitors in more agile jurisdictions.

As the regulatory framework continues to evolve through ongoing consultations and policy development, the insights provided in this chapter offer a foundation for evidence-based reform that balances innovation with integrity, efficiency with security, and technological advancement with regulatory judgement. The successful integration of cryptocurrency into South Africa's cross-border financial ecosystem will require sustained political will, interdepartmental coordination, and an climate that views cryptocurrency not as a threat to regulation but as a tool for achieving regulatory objectives more effectively in the digital age.

CHAPTER 5

GAP ANALYSIS: SOUTH AFRICAN REGULATORY FRAMEWORK FOR CRYPTOCURRENCY-DRIVEN CROSS-BORDER TRANSFERS

Chapter Overview

This chapter builds directly on the regulatory gaps identified in Chapter 4, where four categories of misalignment: regulatory voids, regulatory ambiguities, enforcement deficits, and coordination failures were shown to shape South Africa’s response to cryptocurrency-enabled cross-border transfers. Drawing on these foundational insights, this chapter consolidates the empirical, legislative, and institutional findings into a structured gap analysis that diagnoses the specific barriers constraining blockchain adoption within the South African regulatory environment. By organising these gaps into coherent analytical dimensions, the chapter provides the necessary problem architecture that informs the design of the knowledge model developed in Chapter 6.

Mapping of Chapter 4 Gap Types to Chapter 5 Analytical Dimensions

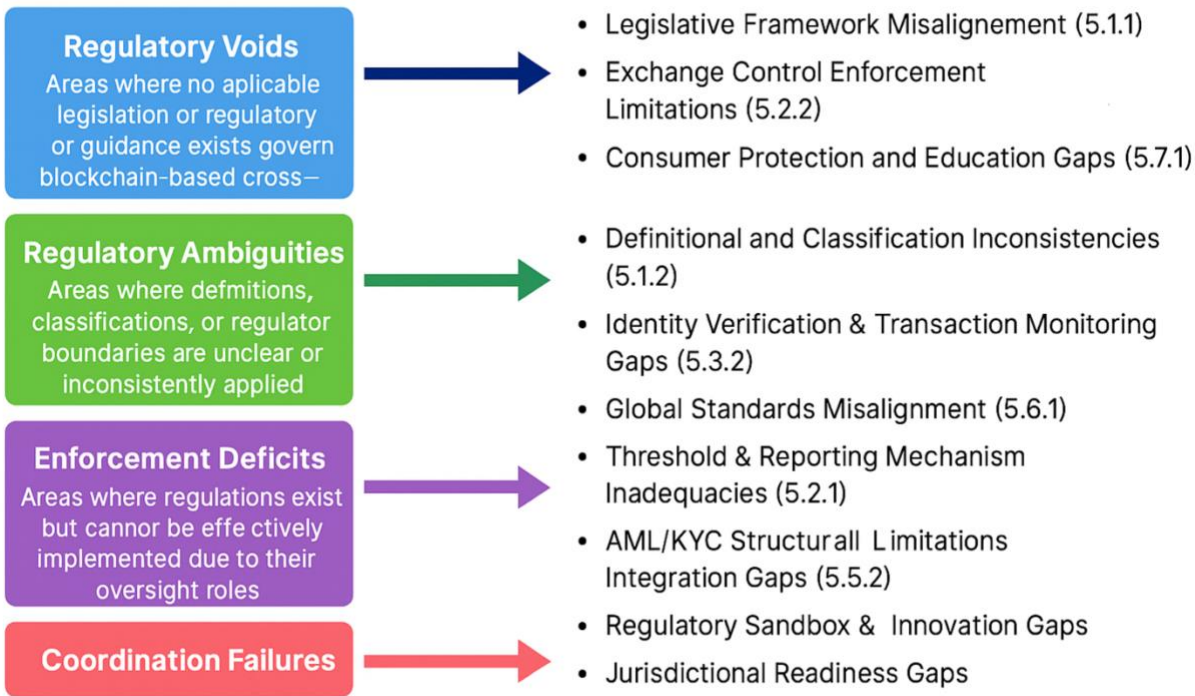


Figure 32. Graphic outlining linkage mapping between Chapter 4 Gap Types and Analytical Dimensions (Researcher)

The analysis reveals a significant disconnect between South Africa's traditional, centralised regulatory framework and the decentralised nature of blockchain and cryptocurrency technology. While South Africa has established comprehensive regulations for conventional cross-border transfers, substantial gaps exist in addressing blockchain-specific challenges, creating regulatory uncertainty that hinders innovation while potentially compromising compliance objectives. South Africa's regulatory architecture for cross-border transfers is mature for traditional, bank-mediated remittances but remains uneven for cryptocurrency-enabled models that are decentralised, pseudonymous, and often borderless. The following research highlight a structural misalignment between statutes and operational instruments designed for centralised intermediaries (e.g., Authorised Dealers and ADLAs) and the realities of distributed ledger technologies (DLT). They also note definitional ambiguities, exchange-control enforcement frictions, AML/KYC implementation constraints, gaps in technical standards, and limited empirical evidence specific to the South African context.

The rapid evolution of cryptocurrency and crypto-asset ecosystems has introduced new complexities into cross-border financial regulation. While distributed ledger technologies provide the underlying infrastructure, they are not themselves the objects of financial governance. Regulation applies to financial instruments, services, activities, and intermediaries, rather than to enabling technologies. Accordingly, this chapter analyses the regulatory environment surrounding cryptocurrency, crypto-assets, and CASPs as they relate to cross-border transfers in South Africa. International regulatory bodies increasingly emphasise this distinction. The FATF clarifies that compliance obligations attach to Virtual Asset Service Providers (VASPs) rather than to blockchain protocols (FATF, 2021). Similarly, the FSB and the Bank for International Settlements (BIS) focus on crypto-asset market structures, stablecoins, and intermediary supervision (FSB, 2023; BIS, 2023). This chapter evaluates how existing South African financial, exchange control, and AML/CFT frameworks interact with cryptocurrency-based cross-border transactions, identifies regulatory misalignments, and considers policy responses aligned with global standards.

Building on these findings, this gap analysis consolidates the evidence into eight dimensions and assesses gaps, root causes, impacts, and actionable recommendations. It also integrates observations on emerging 2025 developments,

including Travel Rule implementation and jurisprudence affecting exchange controls, to highlight a pathway from “centralised oversight” to “centralised-decentralisation” hybrids that embed compliance into technical guardrails. Drawing on innovation and socio-technical theories, it identifies persistent gaps in scalability, cost-effectiveness, user adoption, regulatory frameworks, privacy, interoperability, and empirical evidence. Incorporating recent 2025 updates, such as the finalisation of Directive 9 on the Travel Rule and a High Court ruling exempting cryptocurrency from exchange controls, the analysis reveals evolving opportunities for hybrid models that balance decentralisation with centralised oversight. Directive 9 is a South African FIC directive that requires CASPs to implement the "Travel Rule" for all crypto asset transfers, effective April 30, 2025. The Travel Rule necessitates that CASPs collect and share specific customer information between the sending and receiving institutions to enhance transparency and combat financial crime.

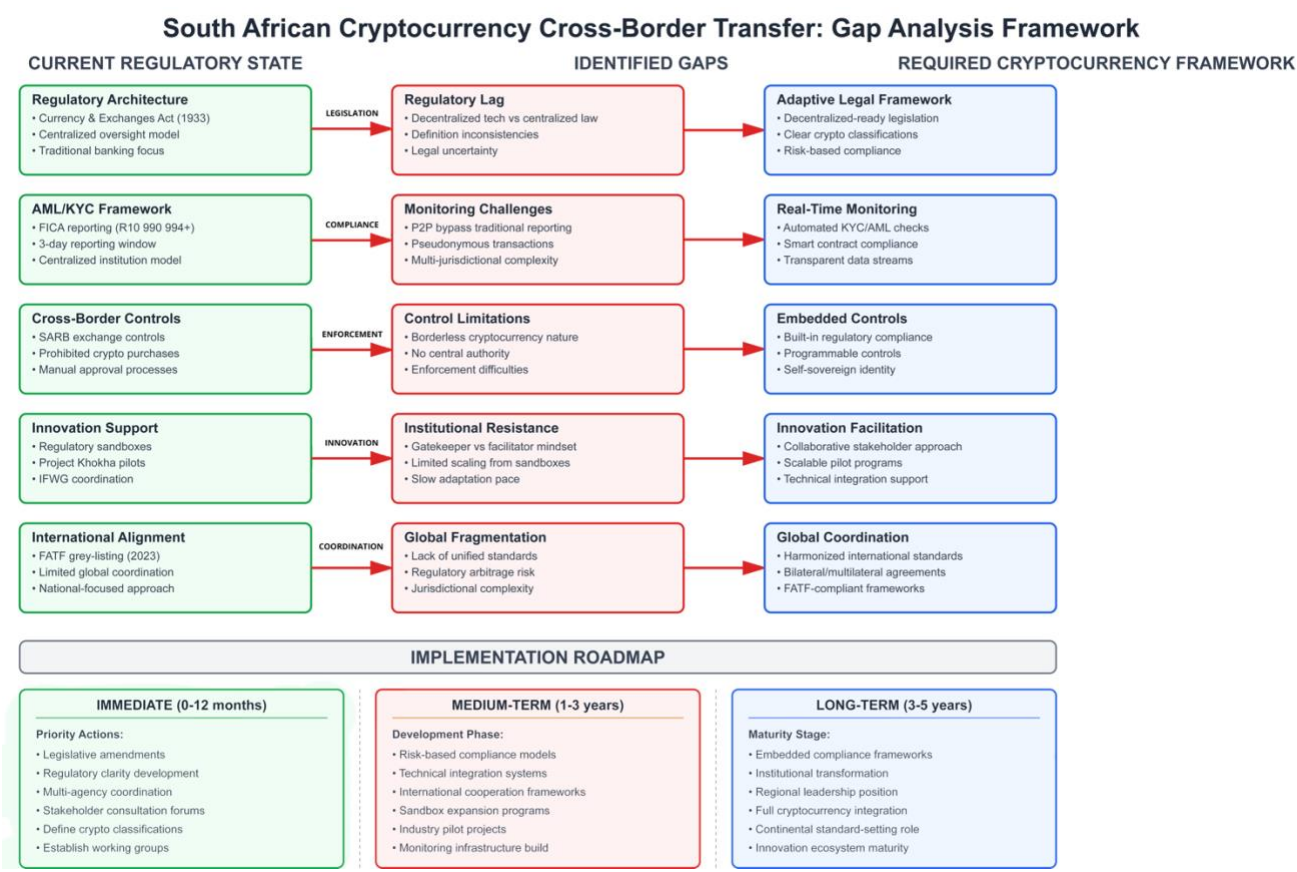


Figure 33. Tabular representation of South African Gap Analysis Framework (Researcher)

5.1 Regulatory Architecture Gaps

5.1.1 *Legislative Framework Misalignment*

Current State: South Africa's regulatory foundation relies primarily on legislation designed for centralised financial systems, including the Currency and Exchanges Act of 1933, which "governs cross-border transactions and remittances, administered by SARB's Financial Surveillance Department" and "prohibits capital exports without National Treasury approval, including crypto asset purchases."

Gap Identified: The research identifies that "the current legal and regulatory framework was not originally designed with decentralised technologies in mind, leading to a state of 'regulatory lag' (Zetzsche et al., 2018 p. 45), where innovation in the market outpaces the ability of legislation and policy to respond."

Impact: This misalignment creates legal uncertainty for cryptocurrency and crypto-asset implementations, as noted in the research: "regulatory uncertainty concerning licensing, compliance obligations, data privacy, and exchange control requirements continues to hamper the deployment of blockchain-based payment infrastructure." South Africa's financial regulatory architecture was designed primarily for bank-centred, fiat-based systems. Consequently, existing laws, including the Banks Act, National Payment System Act, and FICA, do not fully accommodate the operational models of crypto-asset transactions.

This misalignment creates legal uncertainty for cryptocurrency and crypto-asset financial activities, particularly where regulatory provisions assume the presence of identifiable intermediaries such as banks. In crypto-asset ecosystems, intermediation may occur through exchanges, custodians, wallet providers, and stablecoin issuers, entities that do not always align neatly with traditional financial categories.

The absence of asset-specific classifications results in compliance ambiguity for CASPs, who must interpret legacy legislation within novel transaction models. This regulatory gap increases legal risk, discourages institutional participation, and may drive activity toward less regulated jurisdictions (Arner, Barberis & Buckley, 2017).

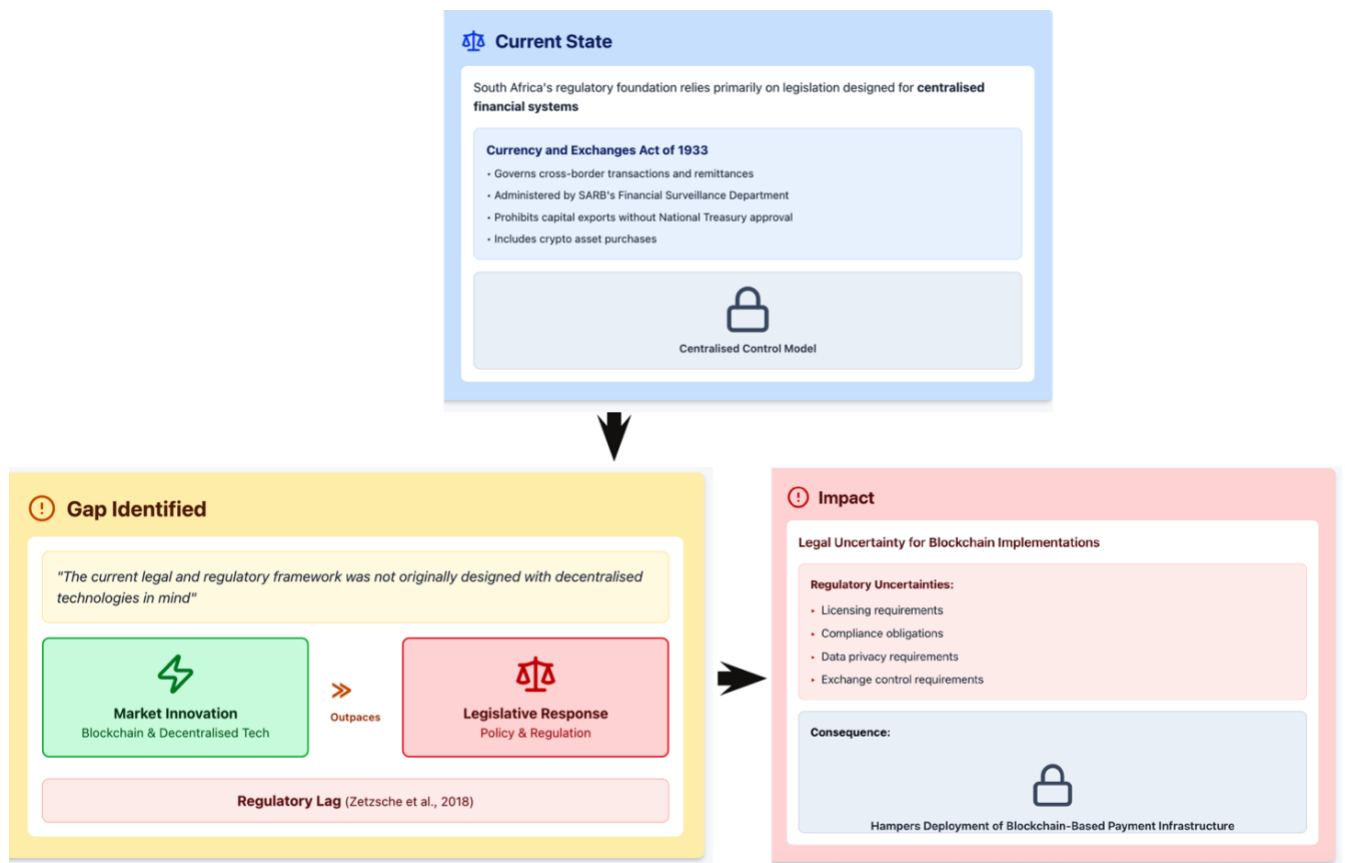


Figure 34. Graphic of the Regulatory Architecture Gaps (Researcher)

5.2 Definitional and Classification Inconsistencies

A central regulatory challenge concerns the classification of crypto-assets. Unlike traditional instruments, crypto-assets may simultaneously function as payment instruments, investment vehicles, or utility tokens. Their regulatory treatment therefore, depends on economic function rather than technological design (Zetzsche et al., 2018).

South Africa's evolving classification frameworks remain fragmented across supervisory mandates. Respondents noted that uncertainty regarding whether a crypto-asset constitutes a security, a commodity, or a payment instrument affects licensing, capital requirements, and reporting obligations. This fragmentation mirrors global regulatory debates and highlights the need for a harmonised taxonomy.

Current Framework: The IFWG Position Paper (2021) defines crypto assets as "digital representations of value not issued by a central bank, used for payment, investment, or utility, and rely on blockchain technology."

Gap: The research highlights that "regulatory authorities struggle to classify cryptocurrency and tokens properly. Is a particular cryptocurrency a security, commodity, currency, or something else entirely? The classification significantly affects how it is regulated."

Consequence: This definitional ambiguity creates compliance challenges, as "the lack of clarity can lead to confusion and inconsistent enforcement."

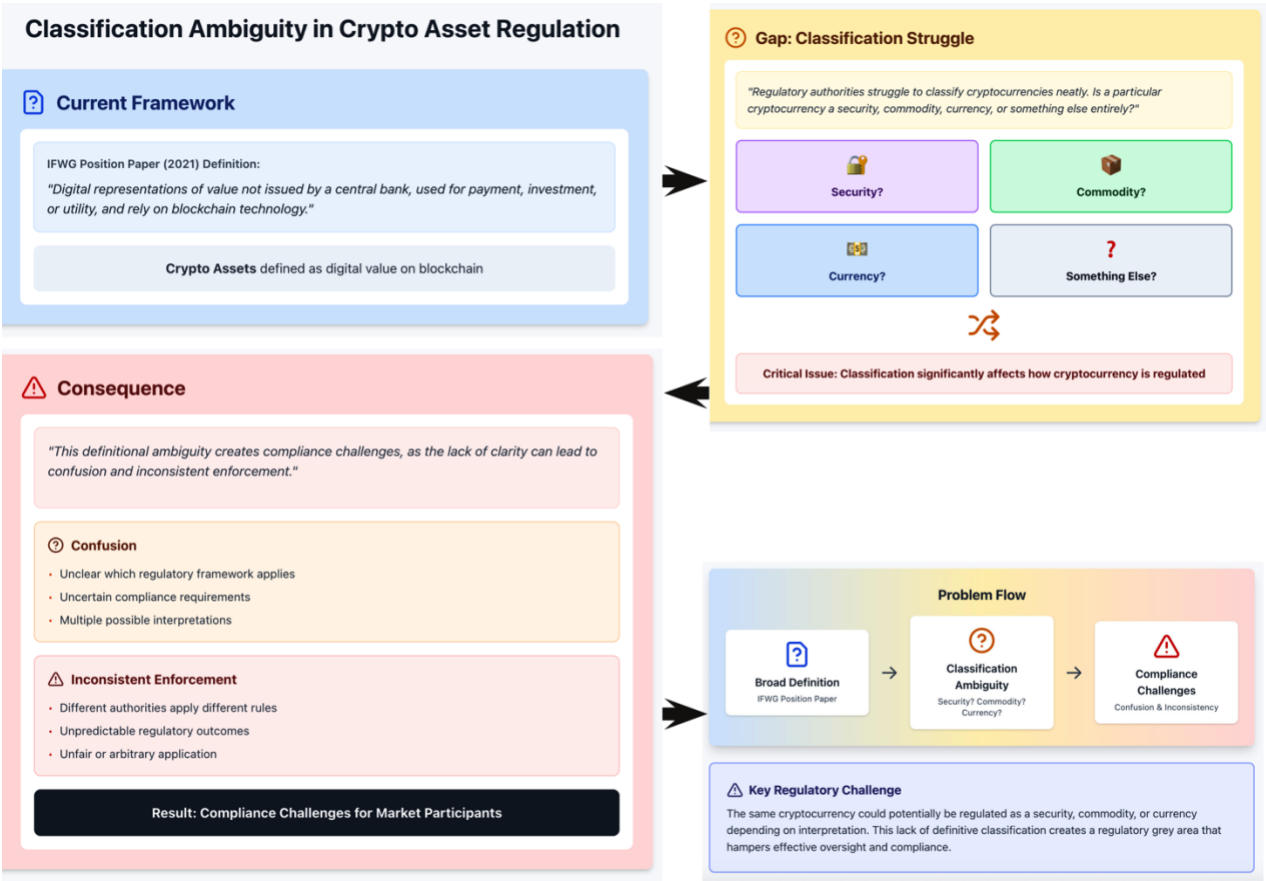


Figure 35. Graphic of the Definitional and Classification Inconsistencies Gaps (Researcher)

5.3. Cross-Border Transaction Oversight Gaps

Traditional cross-border financial oversight relies on reporting through authorised dealer banks. Cryptocurrency transfers, however, may occur through exchanges, peer-to-peer channels, or self-hosted wallets, complicating visibility for regulators.

Non-custodial crypto-asset transactions can bypass conventional reporting frameworks, creating supervisory blind spots. This does not imply regulatory impossibility, but rather necessitates the use of blockchain analytics, Travel Rule compliance, and CASP licensing frameworks to restore transparency (FATF, 2021).

5.3.1 Threshold and Reporting Mechanism Inadequacies

Current Requirements: FICA mandates "reporting of international funds transfers above R19,999.99" with "reports must be submitted within three days of an international funds transfer."

Gap: The research identifies that blockchain's characteristics fundamentally challenge these mechanisms: "The decentralised structure of blockchain poses challenges for traditional regulatory functions, such as verifying identities, monitoring transactions, and enforcing laws across different countries."

Technical Challenge: Traditional reporting assumes identifiable intermediaries, but blockchain enables peer-to-peer transactions that bypass conventional reporting structures.

5.3.2 Cyber-Risk in Blockchain Technologies

Blockchain-based payment systems present a materially different cyber-risk architecture from that of conventional banking infrastructure, characterised by distributed rather than centralised attack surfaces, novel classes of technical vulnerability, and distinct governance challenges for regulatory oversight. A rigorous regulatory treatment of cryptocurrency-enabled cross-border payments must engage with this risk landscape at a level of specificity that goes beyond generic references to cybersecurity.

Protocol-Level Vulnerabilities

At the foundational layer, public blockchain networks, including the Bitcoin and Ethereum networks that underpin most retail crypto-asset activity rely on consensus mechanisms to achieve distributed agreement on the state of the ledger. These mechanisms introduce specific attack vectors. The most theoretically significant is the 51% attack (also termed a majority hash-rate attack), in which an adversary who controls more than half of a proof-of-work network's computational power can, in principle, reverse confirmed transactions and enable double-spending (Nakamoto, 2008; Eyal & Sirer, 2014). While the computational and economic cost of executing a 51% attack on the Bitcoin or Ethereum networks is prohibitive given their scale, smaller and less liquid blockchain networks, including several that have been proposed for cross-border payment applications remain materially vulnerable to such attacks.

The Ethereum Classic network, for example, suffered three confirmed 51% attacks in 2020, resulting in the reorganisation of thousands of blocks and the reversal of confirmed transactions (McCorry et al., 2021). This risk has direct relevance to the regulatory assessment of which blockchain infrastructure is appropriate for institutionally significant cross-border payment functions.

Smart Contract Vulnerabilities

Programmable blockchain platforms, including Ethereum and its derivatives enable the deployment of smart contracts: self-executing code that automates transactional logic without the need for intermediary enforcement. While smart contracts offer significant compliance and operational efficiency benefits, they introduce a class of software vulnerability that has no direct analogue in conventional banking systems. Smart contract code is immutable once deployed on-chain, and therefore coding errors cannot be corrected through standard software patching procedures. They must be addressed through contract migration, governance forks, or, where possible, emergency pause mechanisms built into the original contract design (Atzei et al., 2017).

The most consequential documented smart contract vulnerability is re-entrancy attack, exploited most famously in the 2016 DAO (Decentralised Autonomous Organisation) hack, in which an attacker exploited a recursive call vulnerability to drain approximately USD 60 million in Ether from a decentralised investment fund (Dhillon et al., 2017). Subsequent years have seen ongoing exploitation of smart contract vulnerabilities

across DeFi protocols, with cumulative losses from DeFi hacks exceeding USD 6 billion between 2020 and 2023 (Chainalysis, 2023). In the context of cross-border payment applications, where smart contracts may automate high-value settlement functions, the regulatory requirement for mandatory code auditing, formal verification processes, and bug bounty programmes, as noted by Respondent 8 in Chapter 5 of this thesis takes on heightened urgency.

Key Management and Custodial Risk

A distinctive and underappreciated cyber-risk specific to crypto-asset systems concerns the management of private cryptographic keys. In blockchain-based payment systems, the possession of a private key constitutes *de facto* ownership of the associated digital asset. Unlike conventional banking credentials, private keys cannot be reset or recovered by a central authority if lost or compromised (Antonopoulos, 2017). This characteristic transfers a class of cyber-risk, specifically theft, loss, or compromise of access credentials from the institutional level (where banks maintain centralised identity and access management systems) to the individual or custodial level. CASPs operating as custodians must therefore implement hardware security module architectures, multi-signature wallet protocols, and cold storage arrangements to mitigate key theft and insider threat risks. The collapse of the FTX exchange in 2022, in which inadequate custody arrangements and internal controls contributed to the misappropriation of approximately USD 8 billion in customer assets illustrates the catastrophic consequences of deficient custodial governance, even in the absence of an external cyberattack (Gorton & Zhang, 2023).

Exchange and Infrastructure Attack Surface

Cryptocurrency exchanges and CASPs represent the most frequently targeted components of the crypto-asset ecosystem, functioning as centralised intermediaries within an otherwise decentralised infrastructure. The concentration of liquid assets on exchange platforms creates an attack surface that is, in certain respects, more acute than that of conventional banking systems: exchange security incidents have historically resulted in total asset losses for affected customers, without the deposit insurance safety nets that provide a regulatory backstop in the conventional banking context. The Mt. Gox exchange collapse (2014), the Bitfinex hack (2016), and the Binance breach

(2019) collectively resulted in losses exceeding USD 1 billion, with limited legal recourse available to affected parties (Moore & Christin, 2013; Chainalysis, 2023).

Regulatory Implications for South Africa

For South African regulators, this cyber-risk profile has several concrete implications for the governance of CASPs operating in the cross-border payment space. The SARB's draft Payment System Management Act and the FSCA's CASP licensing framework must incorporate mandatory cyber-risk governance requirements that address: (1) minimum technical standards for key management and custody architecture; (2) mandatory independent code audits for smart contract-based payment systems prior to deployment; (3) incident reporting obligations equivalent to or exceeding those applicable to conventional payment service providers under the SARB's Guidance Note 3/2017; (4) capital or insurance requirements calibrated to reflect the residual cyber-risk of custodial operations; and (5) regulatory engagement with international standards developed by the Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO) in their joint work on crypto-asset risk governance (CPMI-IOSCO, 2022).

Critically, the cyber-risk comparative analysis suggests that the regulatory response to blockchain-based payment systems should not be premised on a presumption of inherent insecurity relative to conventional alternatives. Rather, as the 5-Echelon Model proposed in Chapter 6 of this thesis articulates, the appropriate regulatory response is one of risk-proportionate governance: identifying the specific cyber-risk vectors associated with blockchain infrastructure, developing targeted technical and governance standards to address them, and situating these requirements within a coherent and adaptive regulatory architecture that enables innovation while preserving systemic integrity.

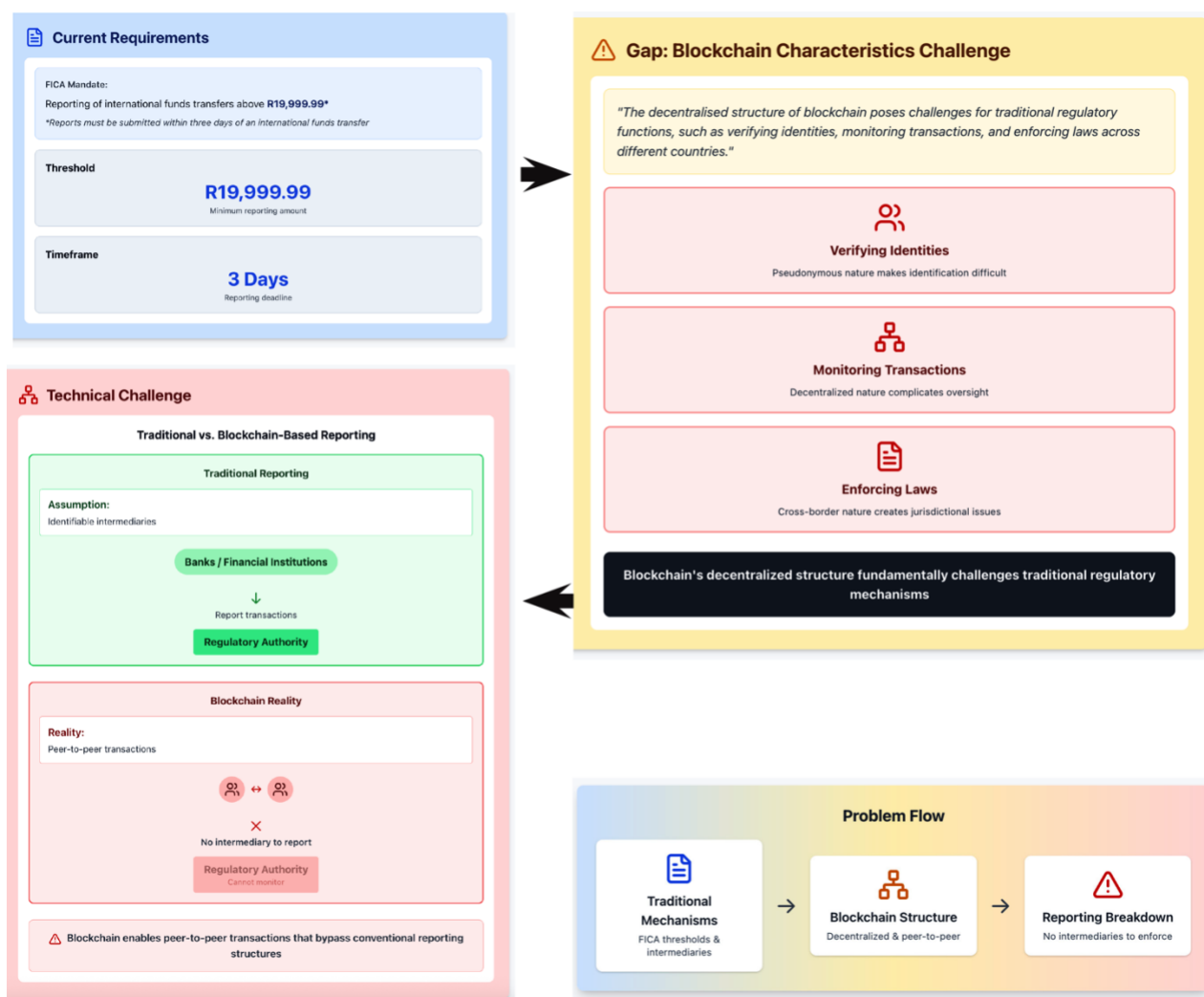


Figure 36. Graphic of the Threshold and Reporting Mechanism Inadequacies Gaps (Researcher)

5.4 Exchange Control Enforcement Limitations

South Africa's exchange control system assumes that cross-border transfers flow through authorised dealer institutions. Crypto-asset transfers occurring outside these channels challenge this model.

The issue arises not from blockchain's borderless architecture, but from the ability of crypto-assets to move value through non-bank settlement pathways. This necessitates exchange control reform that integrates CASPs into reporting systems rather than attempting to restrict technology use (IMF, 2022).

Current Approach: The Currency and Exchanges Manual "prohibits crypto asset purchases abroad" and requires "SARB approval for most outbound flows of capital."

Fundamental Gap: The research notes that "blockchain's borderless nature and decentralised architecture are at odds with these entrenched capital control mechanisms, creating tension between innovation and regulation."

Enforcement Challenge: The decentralised nature means "there is no central authority to impose obligations," making traditional exchange control mechanisms less effective.

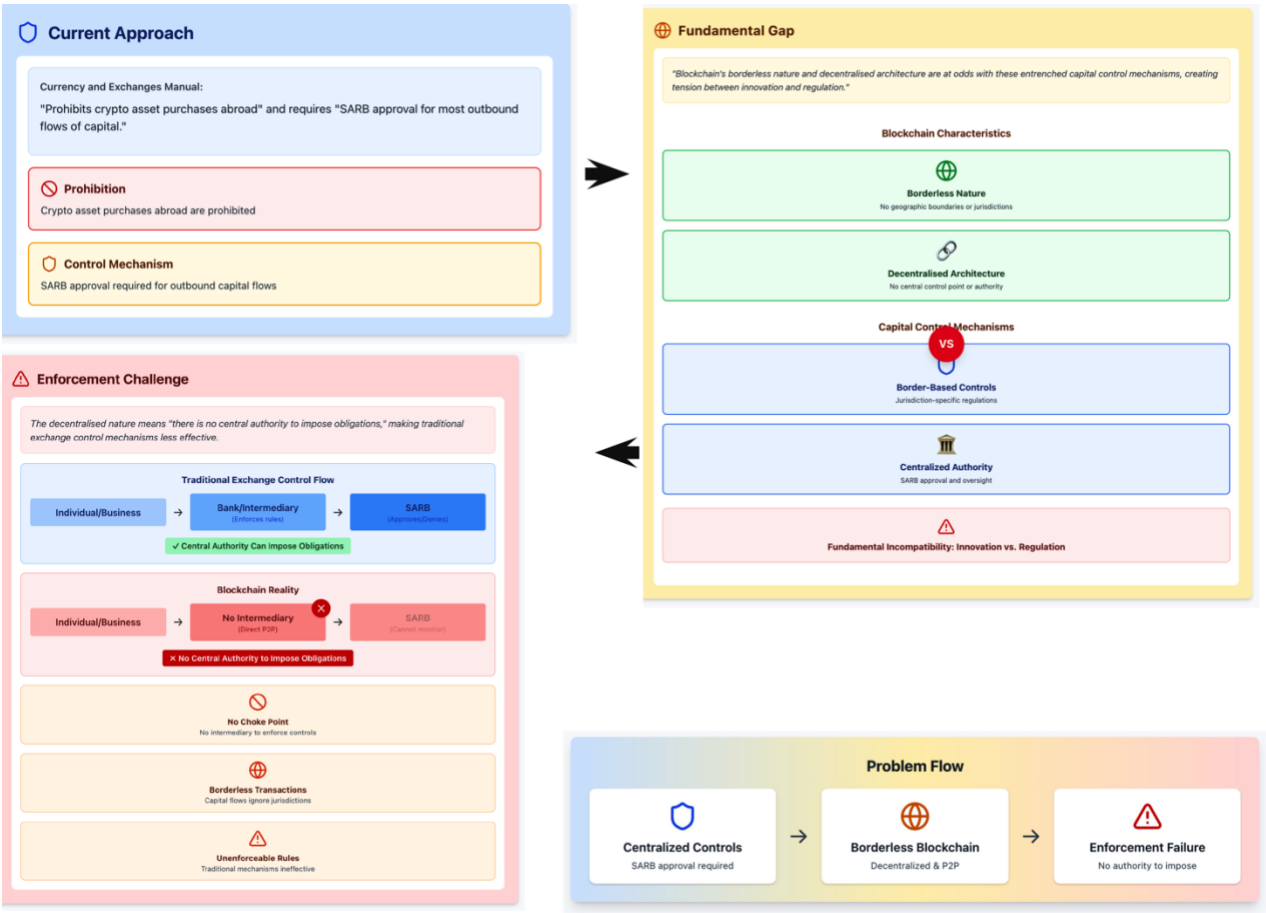


Figure 37. Graphic of the Exchange Control Enforcement Limitations (Researcher)

5.5 Anti-Money Laundering and Know Your Customer Compliance Gaps

AML and KYC concerns feature prominently in crypto-asset regulation. These challenges arise from crypto-asset transaction structures and pseudonymous wallet systems, rather than from distributed ledger technology itself.

FATF Recommendation 15 and its Travel Rule explicitly require VASPs to collect and transmit originator and beneficiary information. This demonstrates that compliance is embedded at the service-provider level. The effectiveness of these measures depends on supervisory capacity and technological integration (BIS, 2023).

5.5.1 AML Framework Structural Limitations

Current Framework: Recent amendments "extended FICA obligations to CASPs to combat money laundering through cryptocurrency," requiring CASPs to "register with the FIC and implement AML/CTF measures."

Critical Gap: The research identifies that "current AML frameworks assume a centralised entity, making them less effective for crypto transactions" because "the decentralised nature of blockchain complicates AML enforcement."

Implementation Challenge: The research emphasises that "Cross-border blockchain transactions often involve multiple jurisdictions, each with its own regulations. This complexity makes it challenging to navigate regulatory requirements, leading to potential compliance issues."

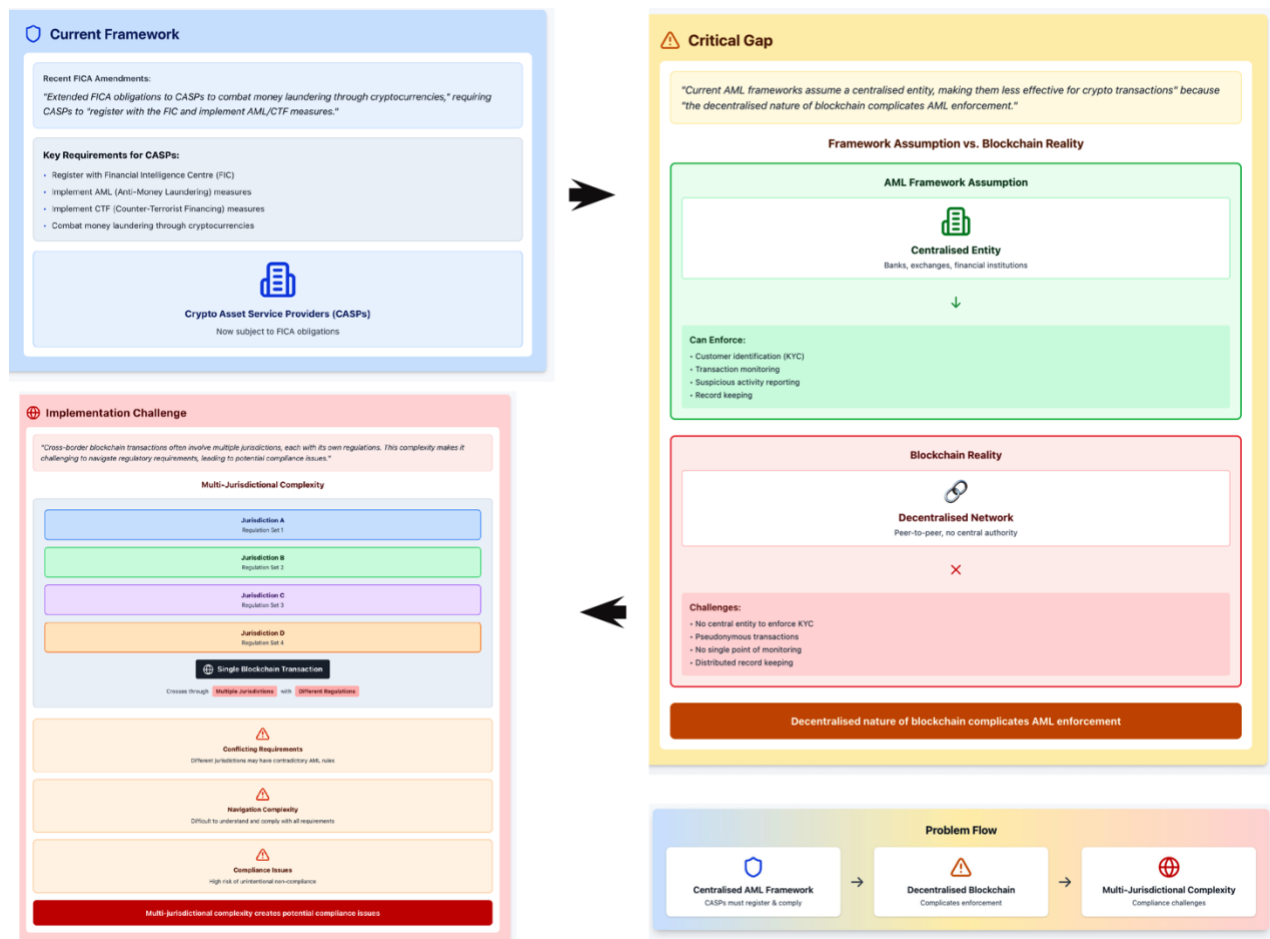


Figure 38. Graphic of the AML Framework Structural Limitations (Researcher)

5.6 Identity Verification and Transaction Monitoring Gaps

Self-custodied wallets present regulatory complexity, as they may operate outside institutional KYC frameworks. However, this mirrors cash transactions rather than representing a novel legal anomaly. Regulatory responses therefore focus on CASP entry and exit points, where customer due diligence can be applied.

Current Requirement: Traditional KYC relies on centralised institutions to verify customer identities and monitor transactions.

Blockchain Challenge: The research notes that blockchain's "pseudonymous and borderless nature" creates challenges for traditional identity verification methods, while the technology's immutable nature means "any coding errors or unintended execution logic can have permanent and irreversible effects."

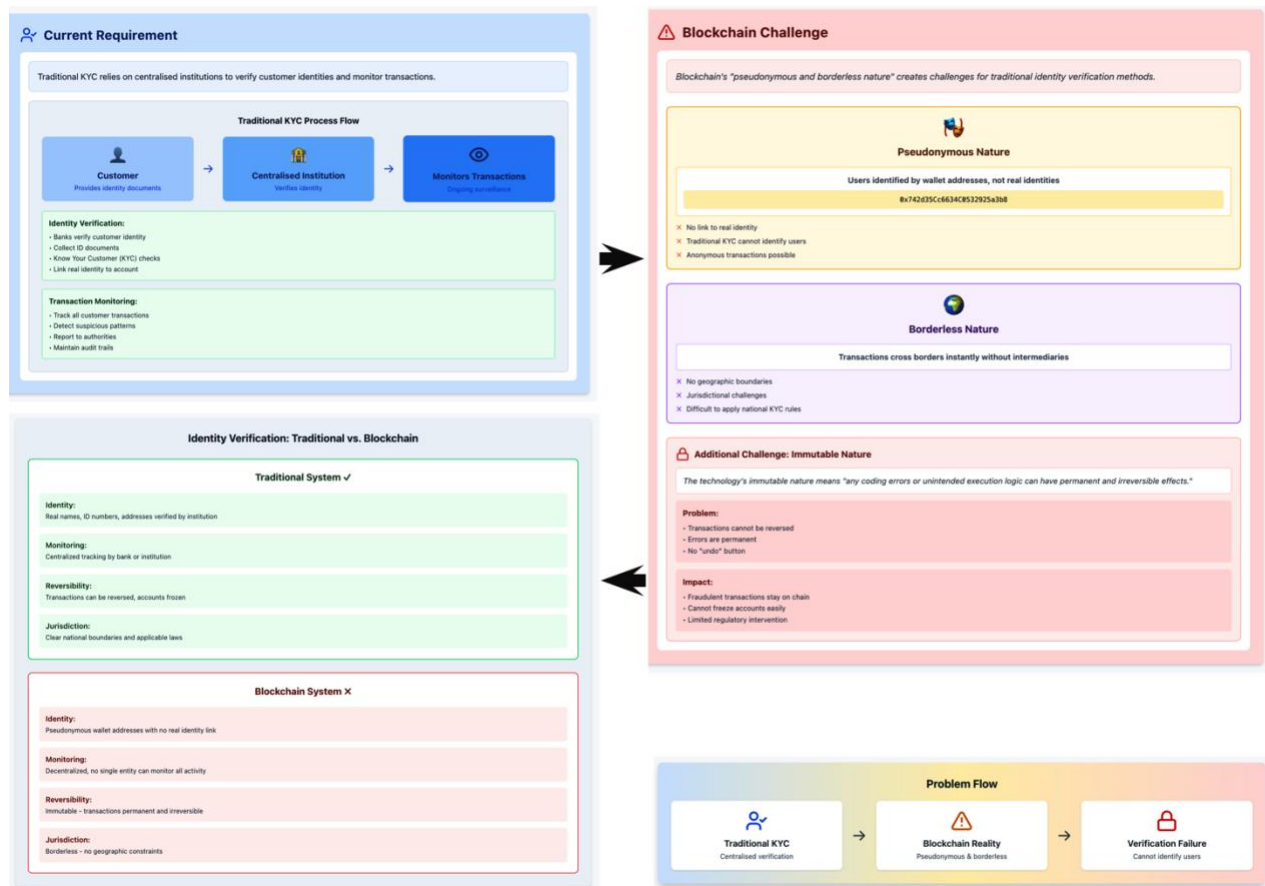


Figure 39. Graphic of the Identity Verification and Transaction Monitoring Gaps (Researcher)

5.7 Innovation and Implementation Gaps

Regulatory sandboxes provide a controlled environment for testing crypto-asset financial services. International experience demonstrates that sandboxes reduce regulatory uncertainty while preserving supervisory oversight (Arner et al., 2017).

South Africa's sandbox initiatives could be expanded to include stable-coin settlement models and cross-border payment pilots.

5.7.1 Regulatory Sandbox Limitations

Current Initiative: The regulatory framework includes "regulatory sandboxes and an Innovation Hub to allow fintechs and blockchain start-ups to test novel solutions in a controlled environment."

Gap: The research indicates that while these exist, "experts highlighted the absence of clear legal guidelines, the lack of unified global standards, and the cautious approach of South African financial institutions as significant barriers to the adoption of blockchain technology."

Scaling Challenge: The sandbox approach doesn't address the fundamental structural issues identified: "These problems are made worse by the newness of blockchain technology and the slow pace at which regulations are adapting to its ever-changing applications."

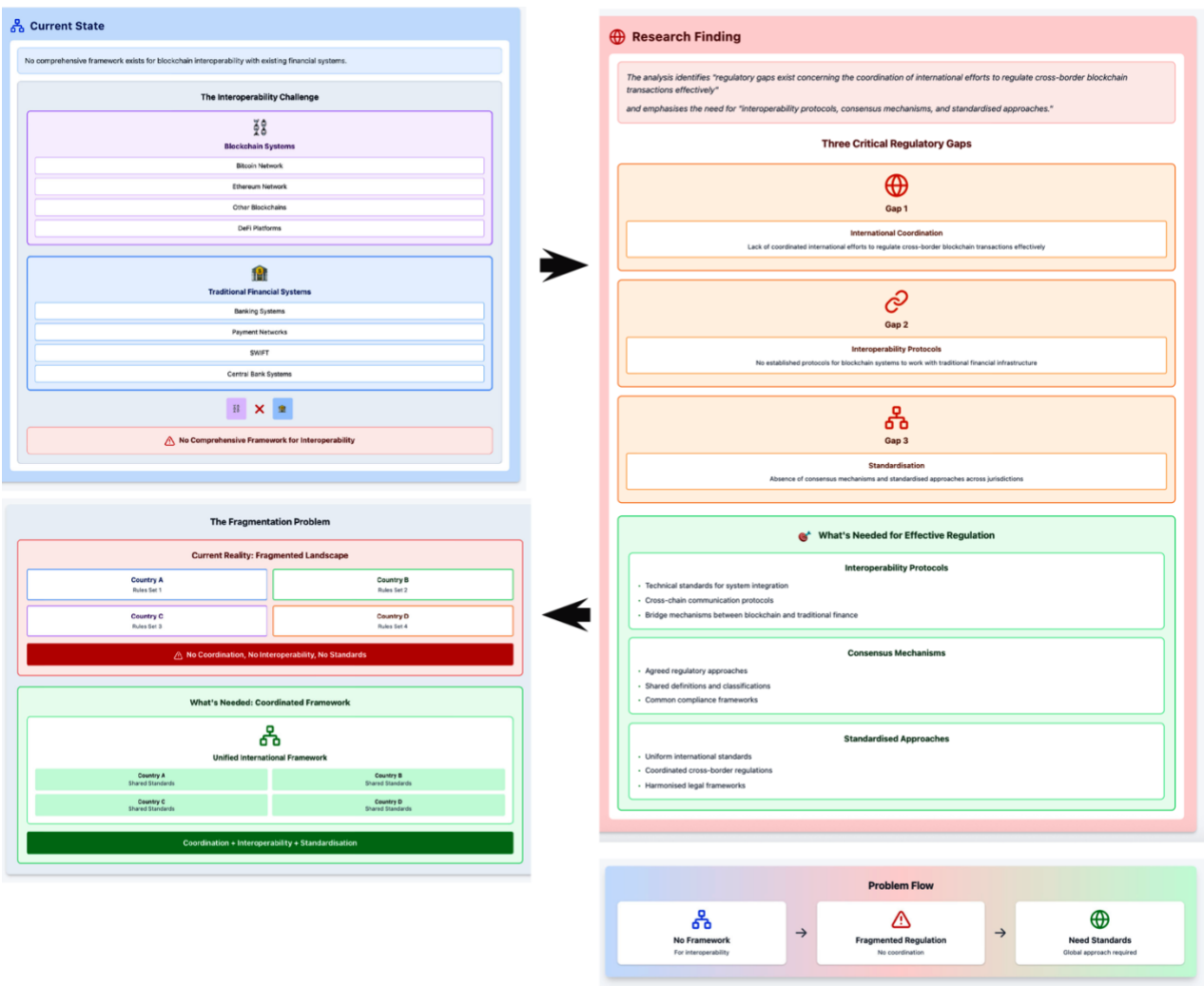


Figure 40. Graphic of the Innovation and Implementation Gaps (Researcher)

5.8 Institutional Readiness Gap

Integration challenges concern interoperability between crypto-asset service platforms and legacy financial infrastructure. This includes payment gateways, reporting systems, and supervisory data interfaces. These issues are institutional rather than technological barriers.

Current Approach: Traditional financial institutions maintain "cautious openness to exploring distributed ledger technologies" as demonstrated by SARB's Project Khokha initiatives.

Cultural/Institutional Gap: The research identifies the need for "a cultural shift required for institutional stakeholders to transition from gatekeepers to facilitators," noting that "achieving significant advancements requires not only changes in legislation but also a shift in institutional mindset from a restrictive gatekeeping approach to a collaborative and innovation-supportive stance."

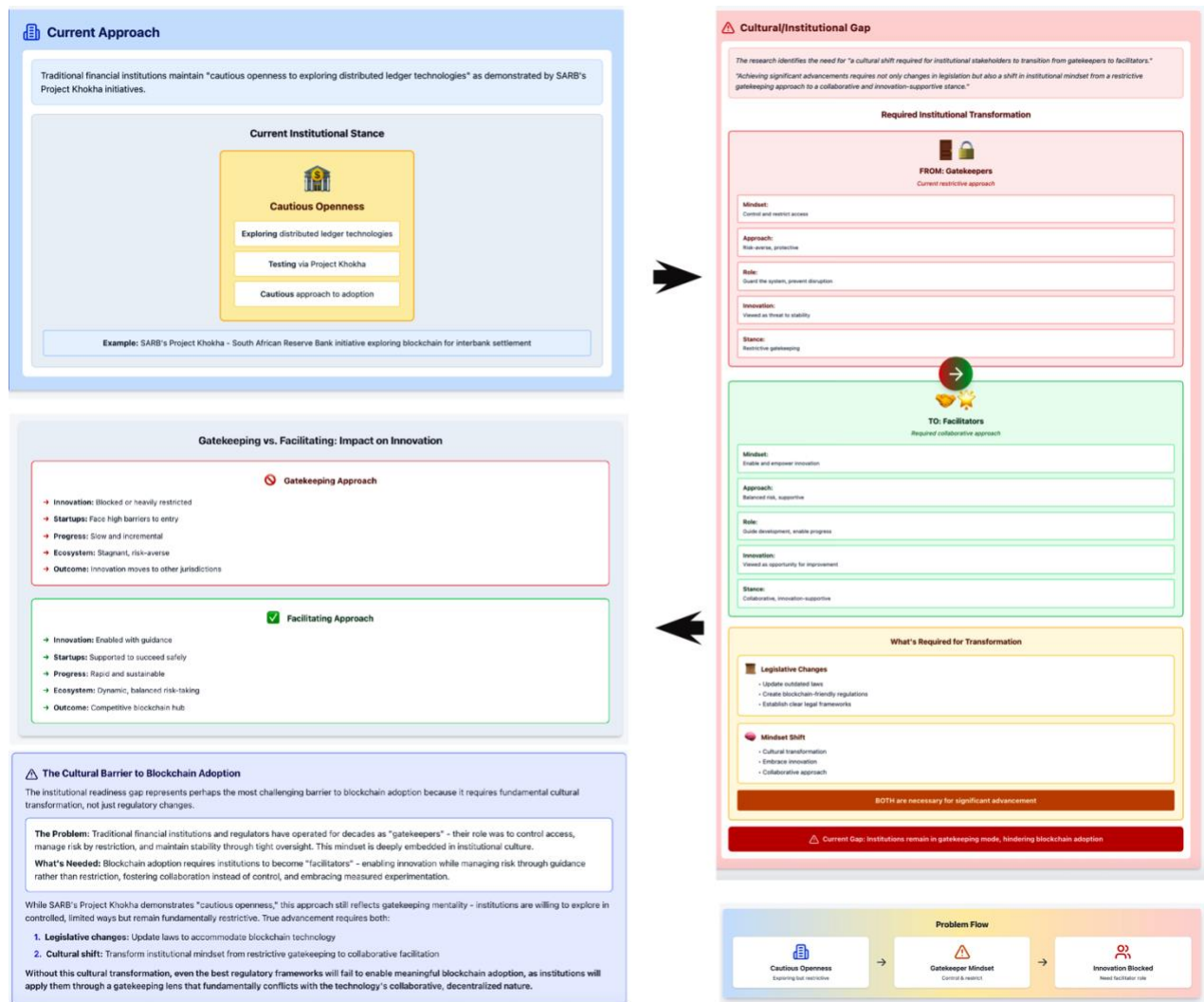


Figure 41. Graphic of the Institutional Readiness Gap (Researcher)

5.9 Technical Integration and Standards Gaps

Advances in blockchain analytics allow regulators to monitor crypto-asset flows more effectively than cash-based systems. Real-time monitoring tools support AML/CFT enforcement and risk assessment (BIS, 2023).

5.9.1 Interoperability and Standards Absence

Current State: No comprehensive framework exists for blockchain interoperability with existing financial systems.

Research Finding: The analysis identifies "regulatory gaps exist concerning the coordination of international efforts to regulate cross-border blockchain transactions

effectively" and emphasises the need for "interoperability protocols, consensus mechanisms, and standardised approaches."

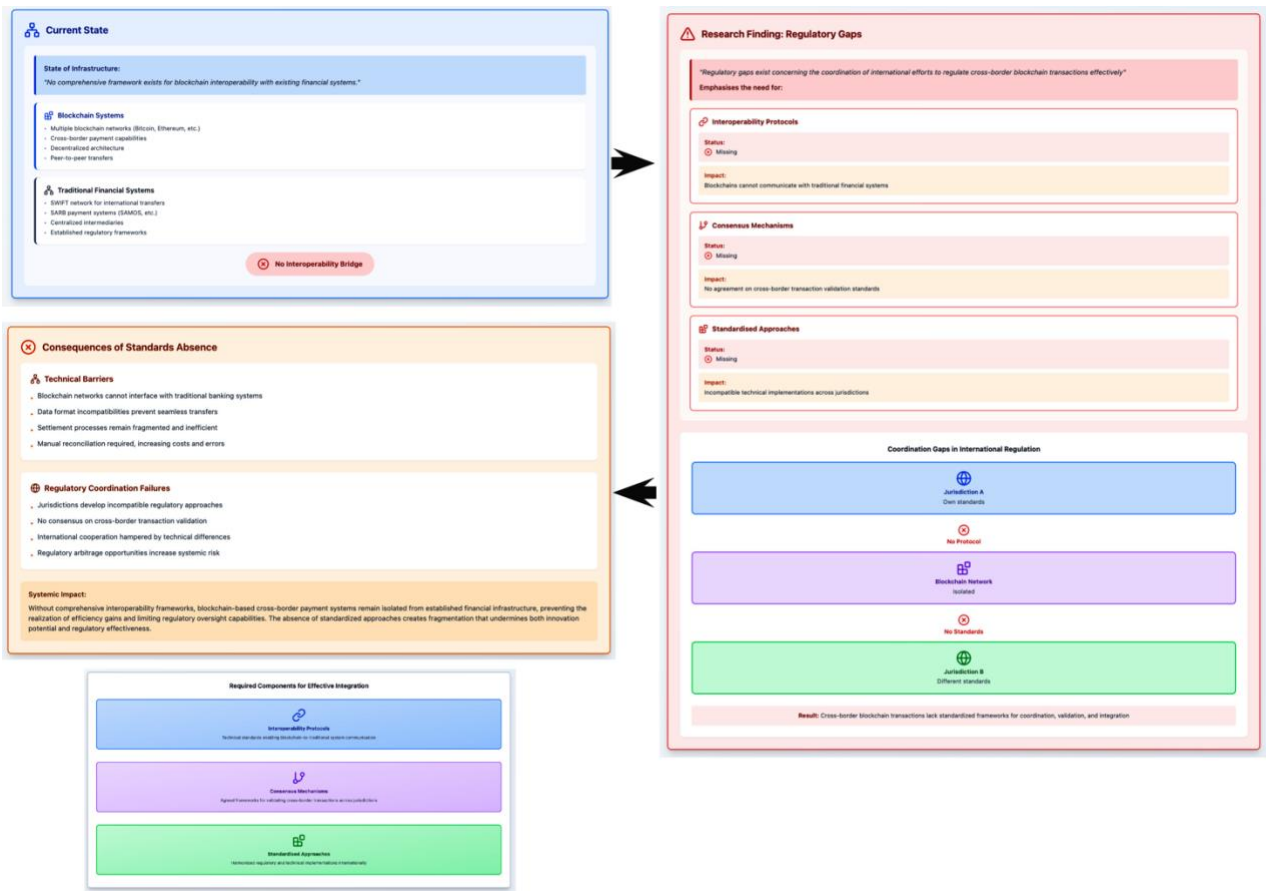


Figure 42. Graphic of the Technical Integration and Standards Gaps (Researcher)

5.10 Real-Time Monitoring and Compliance Integration

Crypto-asset markets operate across jurisdictions. FATF standards, FSB frameworks, and IMF guidance highlight the necessity of international cooperation to prevent regulatory arbitrage. South Africa's participation in global fora is essential for alignment.

Current Limitation: Traditional monitoring systems are not designed for real-time blockchain transaction analysis.

Technical Gap: The research suggests implementing "smart contracts to automate KYC/AML checks, implement tax or exchange control rules, and ensure transaction traceability," but current regulations don't provide frameworks for such automated compliance mechanisms.

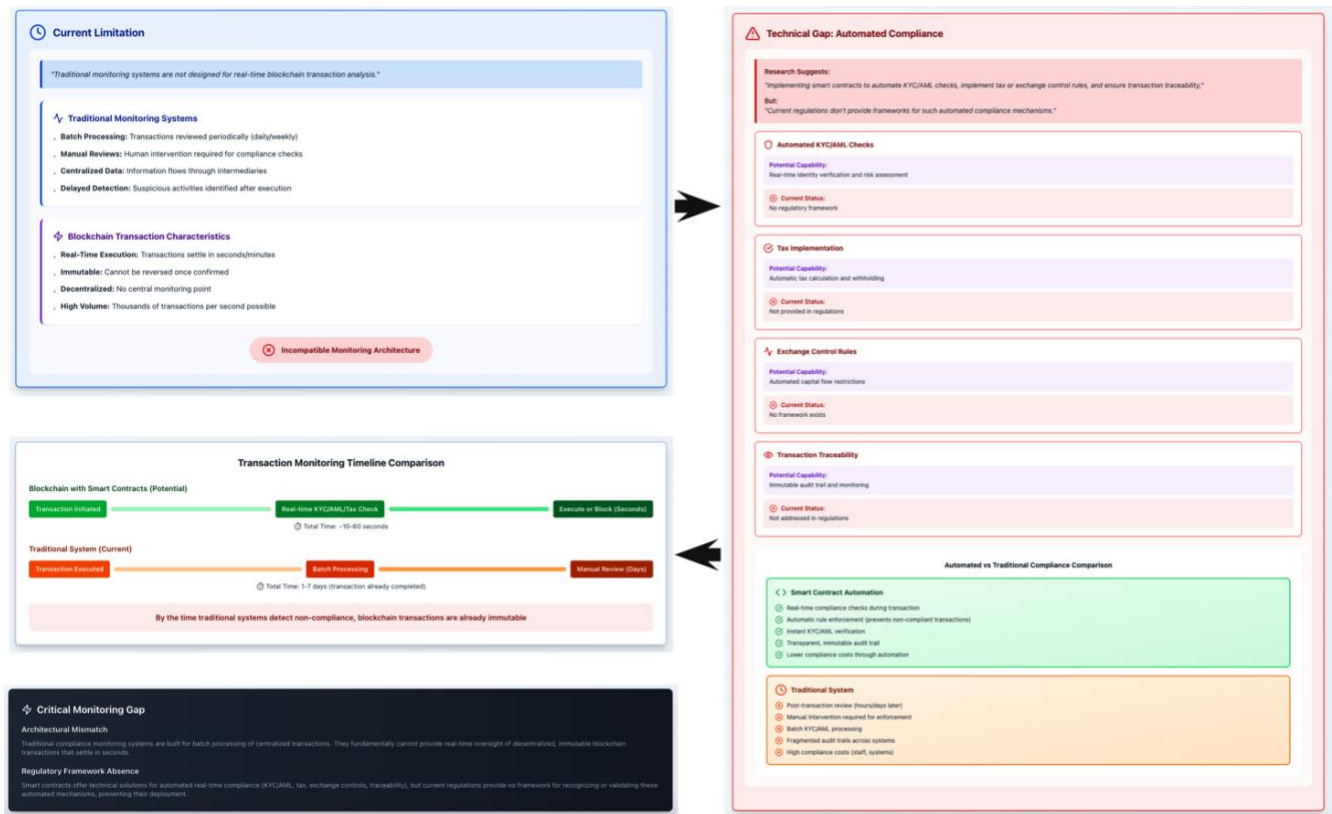


Figure 43. Graphic of the Real-Time Monitoring and Compliance Integration Gaps (Researcher)

5.11 International Coordination and Harmonisation Gaps

5.11.1 Global Standards Alignment

Current Challenge: The regulatory framework operates independently despite global blockchain networks requiring coordinated oversight.

Critical Gap: The research emphasises that "there is a lack of uniformity in blockchain and cryptocurrency regulations globally. Different countries have developed varying regulatory approaches, from embracing blockchain technology to imposing strict restrictions or bans."

FATF Compliance: While South Africa was "grey-listed by the Financial Action Task Force (FATF) in February 2023," the current framework doesn't fully address the complexities of blockchain-based international transfers in compliance with FATF recommendations.

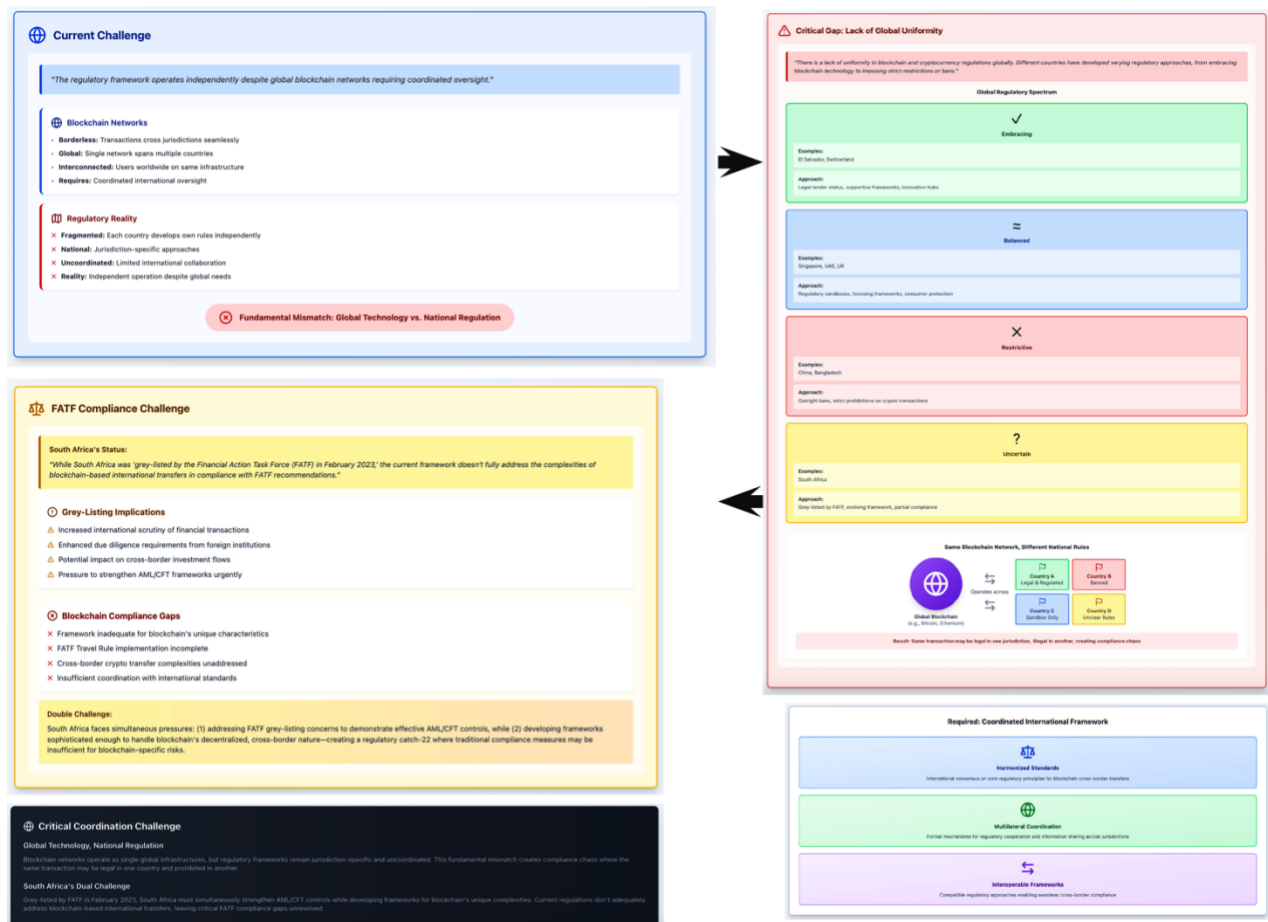


Figure 44. Graphic of the International Coordination and Harmonisation Gaps (Researcher)

5.12 Jurisdictional Arbitrage Prevention

Cryptocurrency represent alternative financial instruments within cross-border ecosystems. The regulatory task is to integrate these instruments into prudential, conduct, and AML/CFT frameworks while leveraging distributed ledger infrastructure as a compliance-enabling tool

Current Limitation: National regulations cannot effectively prevent regulatory arbitrage in decentralised networks.

Research Insight: "Crypto businesses can easily relocate to less stringent jurisdictions, making enforcement difficult unless international coordination is achieved. A harmonised global regulatory framework is necessary to avoid regulatory arbitrage."

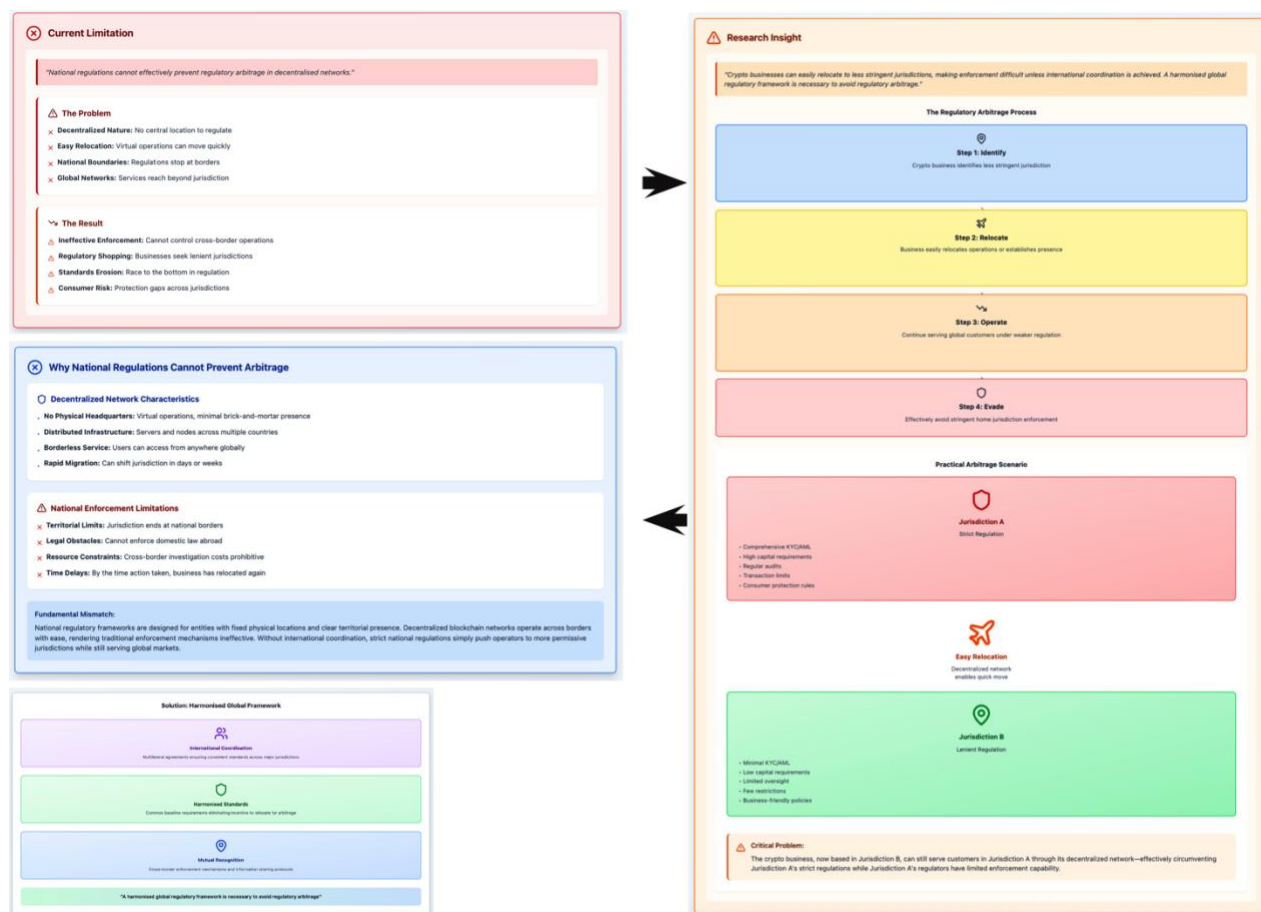


Figure 45. Graphic of the Jurisdictional Arbitrage Prevention (Researcher)

5.13 Consumer Protection and Education Gaps

5.13.1 Consumer Awareness and Protection

Current Focus: Traditional consumer protection mechanisms focus on institutional oversight.

Gap: The research notes that "many consumers lack a comprehensive understanding of crypto risks. Public awareness campaigns and investor education are critical to supplement regulatory efforts."

Technical Literacy: The analysis identifies that "end users often lack the technical literacy to audit smart contracts or understand consensus mechanisms, creating conditions of information asymmetry ripe for exploitation."

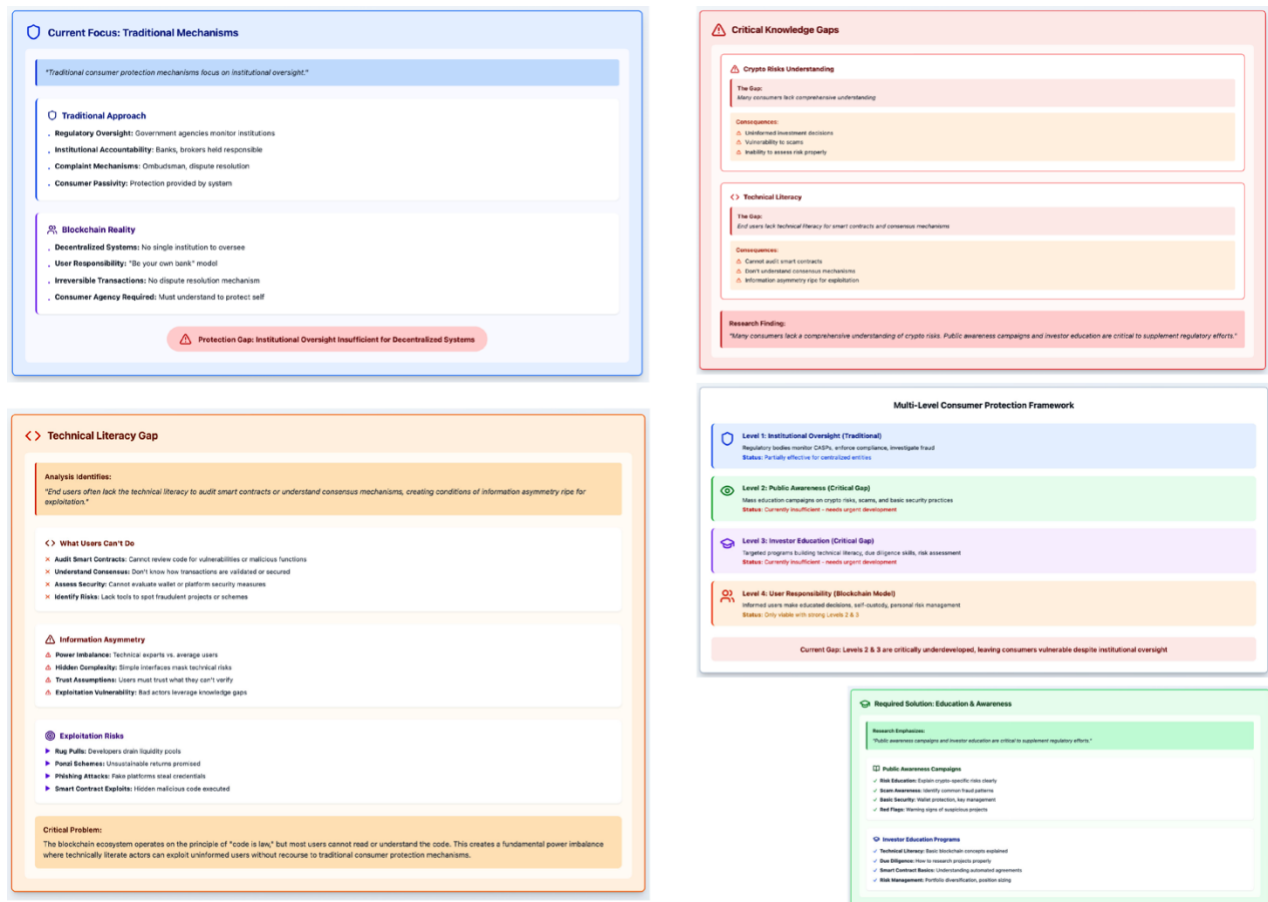


Figure 46. Graphic of the Consumer Protection and Education Gaps (Researcher)

Consolidated Gap Table

Dimension	Current State	Gap	Impact	Key Recommendation
Remittances	Bank-mediated, documented flows	P2P-crypto bypasses	Persisting high costs, slow	Define CASP remittance rules. Pilot stable-coin corridors.
Exchange Control	Prohibitions and approvals dominate	Borderless crypto weakens control points	Arbitrage; uncertainty	Codify crypto exchange control rules. Enable Travel Rule data sharing.
Payment Systems	NPS does not recognize crypto	No standard DLT-NPS interface	Limited integration	Operationalise Travel Rule. Standardize on-chain analytics
AML/CFT & IFTR	CASP obligations under PICA	Pseudonymity complicates	Residual ML/TF risk; high	Integrated CASP framework. Token taxonomy. Stable coins.
Crypto & CASPs	Phased, incomplete regulation	Classification & licensing ambiguity	Consumer harm risk	Integrated CASP framework. Token taxonomy.
Prudential	Systemic oversight in place	Disclosure & redress gaps	Consumer harm risk	Prudential standards DLT corridor stress tests
Tax	Crypto treated as property	Limited guidance on stable coins	Compliance uncertainty	SARS practice notes aligned with exchange-control and IFTR

Table 4. Consolidated Gap Table

5.14 Recommendations for Addressing Identified Gaps

5.14.1 Immediate Actions Required

1. **Legislative Amendment:** Modernise the Currency and Exchanges Act to explicitly address decentralised financial technologies
2. **Regulatory Clarity:** Develop specific guidelines for blockchain-based cross-border transfers
3. **Multi-Agency Coordination:** Enhance IFWG capabilities to provide unified regulatory guidance

5.15 Medium-Term Structural Changes

1. **Adaptive Regulatory Framework:** Implement "risk-based compliance models, where the level of regulatory scrutiny aligns with the associated risks of specific transactions"
2. **Technical Integration:** Develop systems for "real-time, unchangeable ledgers to offer regulators access to transparent data streams"

3. **International Cooperation:** Establish bilateral and multilateral agreements for blockchain transaction oversight

5.16 Long-Term Transformation

1. **Embedded Compliance:** Develop frameworks for "embedding regulatory compliance into cryptocurrency solutions".
2. **Institutional Evolution:** Support the cultural shift from "a restrictive gatekeeping approach to a collaborative and innovation-supportive stance".
3. **Global Leadership:** Position South Africa as a leader in balanced cryptocurrency regulation within the African context.

RECOMMENDATIONS FOR ADDRESSING IDENTIFIED GAPS IN DECENTRALISED FINANCE

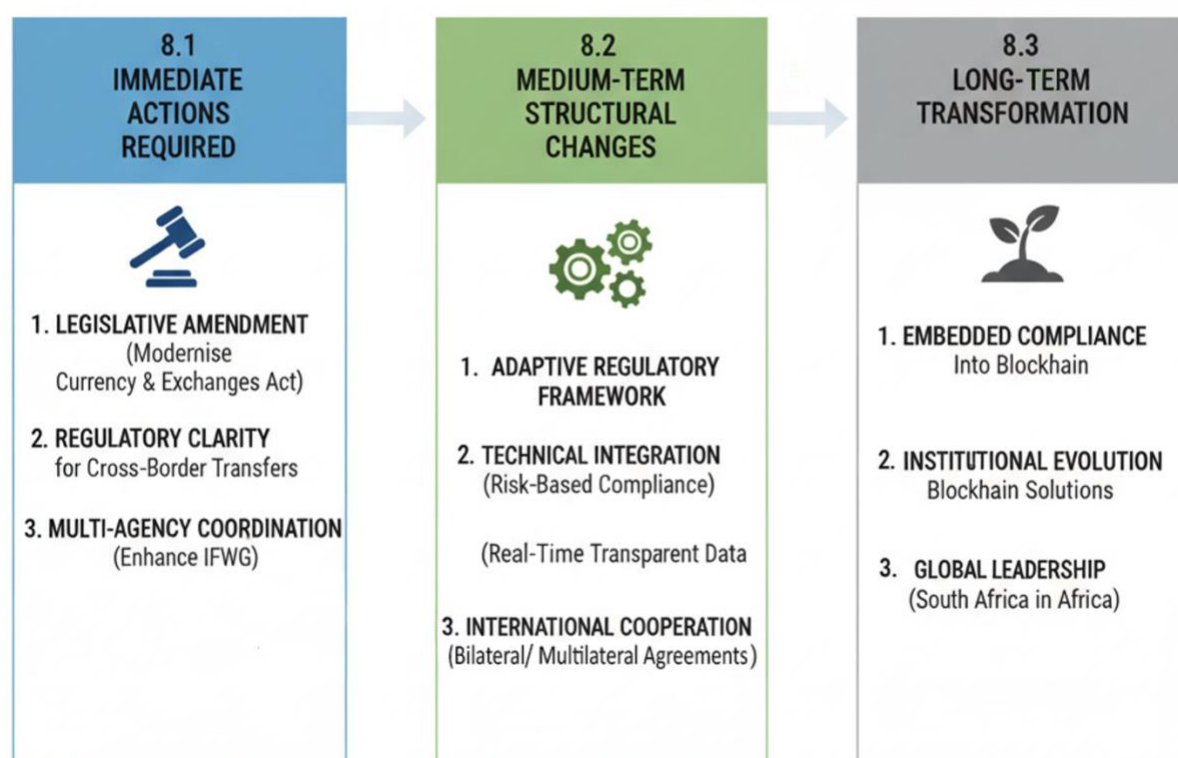


Figure 47. Graphic outlining recommendations to address identified gaps (Researcher)

Integrating Recent Updates and Empirical Insights

The 2025 regulatory landscape marks a pivotal shift. The High Court ruling in June 2025 that "cryptocurrency do not fall within the ambit of South Africa's Exchange Control

Regulations" liberates blockchain from capital export prohibitions, addressing the concern: "Cross-border transfers for purchasing crypto assets are explicitly prohibited" This aligns with the Literature Review's call for jurisdictional clarity (Liu et al., 2019), potentially enabling cryptocurrency remittances without Treasury approval.

Directive 9's Travel Rule implementation, effective April 30, 2025, mandates data sharing for crypto transfers above ZAR 5,000, extending FICA obligations and combating AML risks noted in the documents: "The decentralised nature of blockchain complicates AML enforcement". This "cracking down" approach (Werksmans, 2025) balances innovation with stability.

Empirically, a 2025 study on stablecoins for remittances, based on 866 U.S. respondents, demonstrates adoption driven by efficiency, supporting cost gap closure. The IMF's SSA analysis reveals blockchain's role in digital payments, with empirical data on reduced times. However, SA-specific empirics are sparse; the Africa Blockchain Report notes funding for crypto payments but lacks quantifiable remittance impacts.

Tax implications remain: SARS treats cryptocurrency as intangible assets, with capital gains up to 18%. This could deter adoption unless mitigated. These developments suggest a hybrid model: decentralised efficiency under centralised oversight, as per the dissertation abstract: "The study proposes a hybrid solution, combining cryptocurrency 's decentralised capabilities with centralised oversight". Yet, gaps in interoperability and privacy persist, as cryptocurrency's transparency may conflict with POPIA (Protection of Personal Information Act). Internationally, U.S. crypto bills advancing in 2025 offer models for SA, emphasising collaboration per FATF Recommendation 16.

5.17 Synthesis of Regulatory Framework and Research Findings

5.17.1 Alignment Between Regulatory Intent and Industry Needs

The analysis reveals both alignment and tension between South Africa's regulatory framework and industry perspectives on cryptocurrency implementation. The regulatory framework demonstrates sophistication in traditional financial oversight, with comprehensive exchange control mechanisms, robust AML/CFT requirements, and

well-established payment system governance. However, this framework was designed for centralised, intermediary-based financial systems and struggles to accommodate blockchain's decentralised, peer-to-peer architecture.

Industry experts acknowledge the legitimacy of regulatory concerns regarding financial stability, consumer protection, and illicit financial flows. However, they emphasise that cryptocurrency technology, when properly implemented, can enhance rather than compromise these regulatory objectives. The tension arises not from fundamental incompatibility between cryptocurrency and regulation, but from regulatory frameworks that have not yet adapted to recognise and leverage blockchain's unique compliance-enhancing capabilities.

5.17.2 *Critical Gaps and Reform Priorities*

The integrated analysis identifies several critical gaps requiring urgent attention:

Regulatory Clarity and Legal Certainty: The current regulatory framework lacks clear, comprehensive guidance on blockchain applications in cross-border transfers. The SARB's "wait and see" approach, while prudent, has created regulatory uncertainty that impedes legitimate innovation while potentially driving activity toward unregulated channels.

Digital Identity Infrastructure: South Africa lacks the legal and technical infrastructure for blockchain-based digital identity systems that could simultaneously enhance financial inclusion and strengthen KYC/AML compliance. This gap affects millions of South Africans who cannot access formal financial services due to documentation requirements.

Skills and Capacity Development: Both regulators and traditional financial institutions lack sufficient expertise in cryptocurrency technology. This knowledge gap creates fear-based resistance to innovation and limits the ability to develop appropriate regulatory frameworks that balance innovation with prudential oversight.

International Cooperation Mechanisms: While South Africa participates in various international forums, it lacks proactive leadership in shaping blockchain regulatory

standards for cross-border transfers. This reactive approach risks leaving South Africa subject to standards developed elsewhere without South African input.

Transitional Frameworks: The regulatory framework lacks clear pathways for gradual cryptocurrency integration that would allow experimentation and learning while maintaining system stability. The current binary approach, either full acceptance or prohibition, limits opportunities for iterative development.



Figure 48. Graphic outlining critical gaps and reform priorities (Researcher)

5.17.3 **Recommendations for Regulatory Reform**

Based on the integrated analysis of the regulatory framework and industry perspectives, several recommendations emerge:

Expand and Institutionalise Regulatory Sandboxes: Transform the current limited sandbox program into a permanent platform for blockchain innovation that enables continuous experimentation, regulatory learning, and iterative policy development. This sandbox should include clear pathways for scaling successful pilots into broader implementation.

Develop Principle-Based Blockchain Frameworks: Shift from prescriptive rule-based regulation toward principle-based frameworks that emphasise outcomes (transparency, traceability, consumer protection) rather than specific technologies or implementation methods. This approach would provide flexibility for innovation while maintaining regulatory objectives.

Establish Blockchain-Enabled Digital Identity Infrastructure: Develop legal and technical frameworks for self-sovereign identity systems and NFT-based credentials that can support FICA compliance while expanding financial inclusion. This infrastructure should be designed with privacy protection and interoperability as core principles.

Create Multi-Stakeholder Governance Structures: Establish formal mechanisms for ongoing dialogue between regulators, traditional financial institutions, blockchain and cryptocurrency innovators, and civil society. These structures should ensure that regulatory development benefits from diverse expertise while maintaining appropriate independence and objectivity.

Invest in Capacity Building: Implement comprehensive training programs for regulatory staff, financial institution personnel, and broader public education initiatives. This investment should include international exchanges, secondments, and collaborative research programs with jurisdictions that have successfully implemented blockchain in financial services.

Develop Smart Contract Legal Frameworks: Establish clear legal standards for smart contract development, deployment, and enforcement in financial services. This framework should address security requirements, audit procedures, liability allocation, and dispute resolution mechanisms.

Enhance International Engagement: Adopt a more proactive approach to international blockchain regulatory dialogue, particularly within BRICS and African regional forums. South Africa should position itself as a leader in developing blockchain standards appropriate for emerging markets rather than simply adopting frameworks designed for developed economies.

Implement Phased Adoption Strategy: Develop a clear roadmap for gradual blockchain integration, beginning with specific use cases (such as cross-border remittances) where benefits are clear and risks are manageable, then expanding based on demonstrated success and accumulated experience.

5.17.4 *Strategic Imperatives for South Africa*

The convergence of regulatory framework analysis and industry perspectives reveals that cryptocurrency adoption represents a strategic imperative for South Africa, not merely a technological option. The current cross-border transfer system imposes prohibitive costs on vulnerable populations, excludes millions from formal financial services, and positions South Africa as a passive participant in global financial innovation rather than a leader.

Cryptocurrency technology offers solutions to these challenges while enhancing regulatory compliance capabilities. However, realising this potential requires moving beyond reactive regulatory approaches toward proactive frameworks that enable innovation while maintaining essential safeguards. The window for establishing leadership in cryptocurrency-enabled cross-border finance remains open, but it requires decisive action and sustained commitment. The successful implementation of cryptocurrency for cross-border transfers could position South Africa as a continental leader in financial innovation, enhance financial inclusion, reduce transaction costs for millions of users, and provide regulators with superior tools for oversight and enforcement. Conversely, continued regulatory inaction risks leaving South Africa behind international trends, perpetuating costly and exclusionary financial systems, and missing opportunities for economic development and regional leadership.

RECOMMENDATIONS FOR REGULATORY REFORM



Figure 49. Graphic outlining recommendations for regulatory reform (Researcher)

Recommendations:

To bridge gaps:

1. **Regulatory Sandboxes:** SARB should expand sandboxes for scalability testing, as recommended (Cermeño, 2016).
2. **Empirical Research:** Fund SA-specific studies on blockchain remittances, building on IMF frameworks.
3. **Hybrid Frameworks:** Integrate Travel Rule with privacy tech, ensuring compliance without stifling innovation.
4. **Stakeholder Collaboration:** Partner with fintechs for interoperability standards.
5. **Education Initiatives:** Address user adoption through digital literacy programs. These align with the IFWG's phased approach.

RECOMMENDATIONS TO BRIDGE GAPS IN CRYPTO REMITTANCES



Figure 50. Graphic outlining recommendations to bridge gaps in cryptocurrency remittances (Researcher)

Summary

This gap analysis reveals that while South Africa has established a comprehensive traditional financial regulatory framework, significant gaps exist in addressing cryptocurrency-specific challenges for cross-border transfers. The fundamental tension between centralised regulatory approaches and decentralised cryptocurrency technology requires immediate attention through legislative updates, enhanced international cooperation, and institutional transformation. Addressing these gaps is essential for South Africa to realise the potential cost-reduction benefits of cryptocurrency technology while maintaining regulatory compliance and financial system integrity. The research emphasises that successful cryptocurrency technology implementation requires "not only robust technical design and market fit, but also a proactive engagement strategy with regulators, adaptive compliance mechanisms, and alignment with both domestic and international regulatory standards." This gap analysis provides the foundation for developing such an integrated approach.

The regulatory challenge is not blockchain technology but the governance of crypto-assets and their service ecosystems. Effective oversight depends on aligning financial regulation with evolving transaction models, adopting international standards, and fostering adaptive governance mechanisms. By reframing the regulatory object from

technology to financial activity, policymakers can enable innovation while maintaining financial stability and integrity.

When read in light of the three-dimensional analytical framework established in Chapter 1, the gap analysis presented in this chapter takes on its fullest explanatory significance. Chapter 1 positioned three interrelated dimensions, regulatory challenges, mitigation approaches, and embedded compliance, as the organising lenses through which the regulatory environment for cryptocurrency-based cross-border transfers in South Africa should be examined. The findings of this chapter provide the empirical and structural substance that validates and deepens each of those dimensions. The first dimension, regulatory challenges, anticipated a fundamental tension between decentralised crypto-asset networks and centralised regulatory systems, arising at the asset, intermediary, and service-provider levels rather than at the protocol layer. This chapter confirms that tension in precise institutional terms: the Currency and Exchanges Act of 1933 imposes exchange control obligations designed for centralised intermediaries; FICA's AML/KYC framework assumes identifiable compliance actors that blockchain's pseudonymous peer-to-peer architecture renders absent and definitional inconsistencies across regulatory authorities produce the very fragmentation and compliance uncertainty that

Chapter 1 identified as the primary output of regulatory inertia. Sections 5.1 through 5.6 collectively constitute the empirical map of that first dimension, documenting each barrier, legislative misalignment, classification ambiguity, reporting inadequacy, exchange control friction, AML structural limitation, and identity verification failure, as a concrete manifestation of the systemic gap between the decentralised reality of blockchain and the centralised assumptions of South Africa's inherited regulatory architecture. The second dimension, regulatory mitigation approaches, is equally well served by this chapter's findings. Chapter 1 identified the IFWG Regulatory Sandbox, risk-based compliance models, and the FATF Travel Rule as the primary instruments available to South African regulators; Section 5.7 documents the sandbox's current limitations in scaling beyond controlled experimentation and its failure to resolve the structural issues that persist beneath it; Section 5.11 identifies the FATF grey-listing as both a compliance imperative and a missed opportunity for proactive international engagement, and Section 5.17 explicitly calls for the sandbox to be expanded into a permanent platform, for principle-based frameworks to replace prescriptive rules, and

for multi-stakeholder governance structures to formalise the kind of regulator-industry collaboration that the mitigation dimension demands.

Gap Analysis Through the **Three Dimensions**



Figure 51. Graphic outlining the Gap Analysis through the lens of the 3 dimensions (Researcher)

The chapter therefore not only confirms the mitigations Chapter 1 anticipated but reveals the conditions under which those mitigations have so far fallen short, providing the diagnostic foundation for the more fully specified reform recommendations that follow in Chapter 6. The third dimension, embedding regulation within cryptocurrency design, finds its clearest articulation in Sections 5.10 and 5.17, which identify real-time monitoring, smart contract automation of KYC and AML compliance, blockchain-enabled digital identity infrastructure, and self-sovereign identity frameworks as both urgent gaps and credible solutions. Chapter 1 described this dimension as a shift in how technology is perceived, from one of evasion to an enabler of compliance. This chapter substantiates that reframing through the gap evidence itself. It is precisely because current regulatory tools assume centralised actors and batch-processed oversight that blockchain's capacity for immutable, real-time, programmable compliance has gone unleveraged. Addressing that gap does not require greater restriction of the technology; it requires redesigning regulatory expectations around the technology's own compliance-enhancing capabilities.

Taken together, the three dimensions of Chapter 1 provide the conceptual architecture within which this chapter's gap analysis is most clearly understood: the gaps are not isolated deficiencies but structural expressions of a regulatory environment that has not yet aligned its tools, institutions, and international position with the decentralised, borderless, and technically sophisticated reality of cryptocurrency-based cross-border transfers. The knowledge model developed in Chapter 6 is designed precisely to close that alignment gap.

The research emphasises that successful cryptocurrency implementation requires "not only robust technical design and market fit, but also a proactive engagement strategy with regulators, adaptive compliance mechanisms, and alignment with both domestic and international regulatory standards." This gap analysis provides the foundation for developing such an integrated approach.

CHAPTER 6

DESIGN SCIENCE KNOWLEDGE MODEL FOR REGULATING CROSS-BORDER CRYPTO CURRENCY TRANSFERS

Chapter Overview

While blockchain technology provides the distributed ledger infrastructure underlying cryptocurrency, it is not itself the object of financial regulation. Technologies are not legislated; rather, regulation applies to financial instruments, service providers, and transactional activities conducted using such technologies. Accordingly, this chapter interprets the study findings through the lens of cryptocurrency and crypto-asset regulatory governance, consistent with frameworks developed by the Financial Action Task Force, the Financial Stability Board, and the Bank for International Settlements.

Chapter 6 builds directly on the regulatory gaps identified in Chapter 5 by translating those structural, institutional, technical, and governance deficiencies into a coherent knowledge model for cryptocurrency-enabled cross-border transfers. The model operationalises the findings of the gap analysis by organising the required regulatory, technological, and coordination reforms into a set of interconnected echelons. Each echelon responds to specific gaps diagnosed in the previous chapter, ranging from legislative misalignment and definitional ambiguity to enforcement deficits, interoperability challenges, and coordination failures, thereby providing a structured framework for designing a more adaptive, harmonised, and innovation-enabling regulatory environment for South Africa.

Mapping of Knowledge Model in Chapter 6 to Gaps Identified in Chapter 5

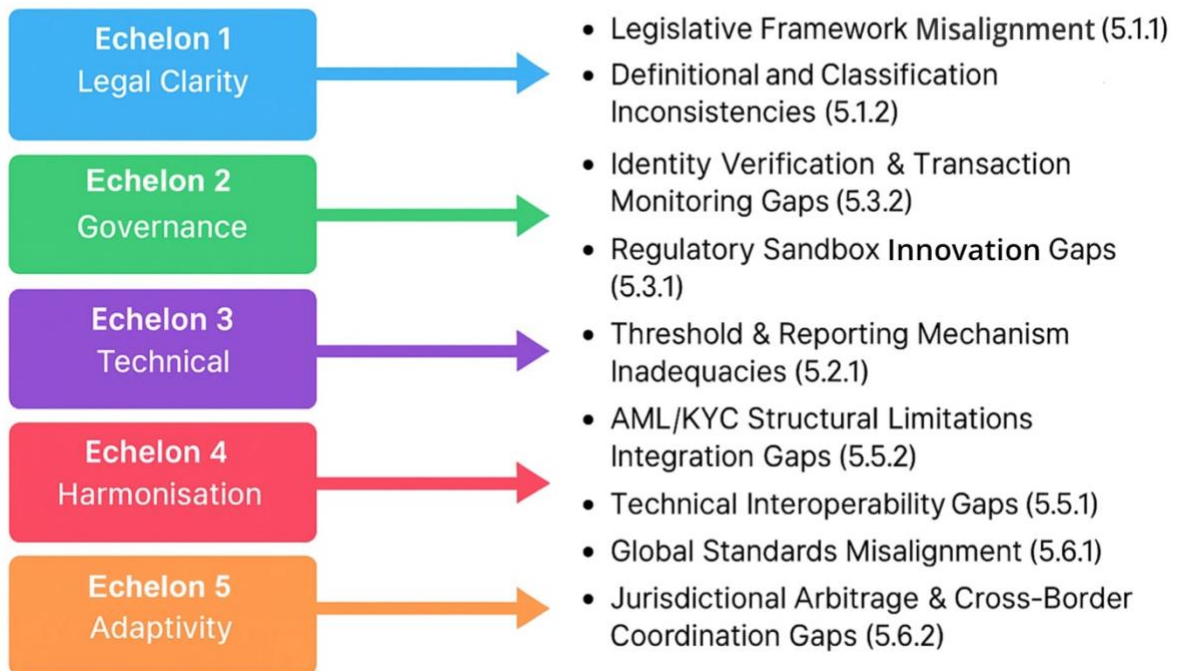


Figure 52. Graphic outlining linkage mapping between Knowledge Model and Gaps Identified (Researcher)

This chapter presents a comprehensive knowledge model designed to address regulatory gaps in South Africa's framework for cryptocurrency-driven cross-border financial transfers. Utilising the echeloned Design Science Research (eDSR) methodology proposed by vom Brocke et al. (2024), the model decomposes the complex regulatory challenge into five hierarchical design echelons. Each echelon represents a logically coherent, self-contained layer progressing from foundational policy elements to adaptive, user-centric mechanisms. Grounded in socio-technical systems theory, institutional theory, innovation diffusion theory, and actor-network theory, this framework proposes a hybrid regulatory approach that balances blockchain's decentralised strengths with necessary centralised oversight. The model directly addresses eight critical dimensions:

1. **cross-border transfers, exchange controls**
2. **payment systems**
3. **anti-money laundering**
4. **combating the financing of terrorism (AML/CFT)**
5. **crypto-assets classification**
6. **market conduct**

7. prudential stability

8. taxation

This chapter expands each echelon with detailed analysis, actionable implementation strategies, and theoretical justifications to position South Africa as a leader in balanced cryptocurrency regulation.

6.1 Introduction

6.1.1 *Background and Context*

The emergence of cryptocurrency has fundamentally challenged traditional paradigms of financial regulation, particularly in the domain of cross-border transfers. As Zetzsche et al. (2018) articulate, the phenomenon of "regulatory lag" occurs when financial technology innovations outpace the adaptive capacity of regulatory frameworks, creating uncertainty and enforcement challenges. This lag is particularly pronounced in emerging markets like South Africa, where colonial-era legislation such as the Currency and Exchanges Act of 1933 remains foundational to financial controls despite being fundamentally misaligned with the decentralised, data-driven nature of blockchain technologies.

The South African regulatory landscape for cryptocurrency-based cross-border transfers is characterised by multiple, intersecting gaps across legislative, operational, and institutional dimensions. These gaps show up as unclear definitions of different types of crypto-assets, weak AML and KYC checks for pseudonymous transactions, difficulties connecting DLT systems with existing payment infrastructure, and a lack of strong international coordination. In 2025, several important regulatory changes took place. These include Directive 9 putting the FATF Travel Rule into effect and a major High Court decision that exempted certain cryptocurrencies from exchange-control rules. Together, these changes create both new opportunities and a strong need for broader regulatory reform.

6.2 Theoretical Foundations

This knowledge model is underpinned by a multifaceted theoretical framework that recognises cryptocurrency regulation as a socio-technical challenge requiring

integration of multiple theoretical perspectives. Socio-technical systems (STS) theory says that good systems work when the social parts: people, organisations, and cultural norms, and the technical parts, such as hardware, software, and processes, are designed together. In the cryptocurrency world, this means that decentralised ledger technologies interact closely with regulators like the SARB and the FIC. Blockchain is not just a technical tool. It is based on socio-technical systems in which user communities, governance structures, and technological rules develop alongside one another. Institutional theory helps explain why organisations and regulators tend to adopt similar governance models when facing pressure to appear credible, operate efficiently, and conform to established norms. These hybrid models try to balance control with flexibility, keeping institutions accountable while allowing enough freedom for innovation to occur, and closing the loopholes that arise when different countries regulate differently. Innovation diffusion theory asks a simpler question: why do some innovations spread quickly while others struggle to gain traction? It looks at whether people see a clear benefit, whether the innovation fits their existing habits, how difficult it is to understand and use, whether it can be tried before full commitment, and whether its benefits are visible to others. In South Africa, these factors go some way toward explaining the slow and uneven uptake of cryptocurrency. Actor-network theory takes a broader view still, treating a blockchain ecosystem as a web of relationships, between regulators, users, developers, and the technology itself, and asking how these relationships are negotiated and stabilised over time.

6.3 Design Science Research Methodology

The methodological backbone of this model is Design Science Research (DSR), which focuses on creating and evaluating artefacts to solve practical problems in information systems. The DSR paradigm, as outlined by vom Brocke et al. (2020), encompasses five core activities: problem identification, objectives definition, design and development, demonstration, and evaluation. This research draws on an extended form of design science research developed by vom Brocke et al. (2024), which breaks complex projects down into manageable, self-contained layers. These self-contained layers are referred to as design echelons. Each layer can be worked on independently or alongside others, and refined over time using feedback from regulatory sandboxes or pilot studies. This layered approach is particularly useful for a project of this complexity, where regulators cannot address everything at once.

The eDSR methodology is particularly suited to cryptocurrency regulation because it accommodates the multilevel, interdependent nature of regulatory challenges while maintaining conceptual clarity and practical implementability. Each echelon represents a logically coherent layer that builds upon previous echelons, creating a pyramid structure where foundational elements support higher-level adaptive mechanisms.

Design Science Research (DSR) is adopted as the methodological foundation because its central objective, which is to “to extend the boundaries of human and organizational capabilities by creating new and innovative artifacts”, aligns directly with this dissertation’s aim of designing a regulatory framework rather than merely analysing one. As Hevner et al. (2004) explain, “knowledge and understanding of a problem domain and its solution are achieved in the building and application of the designed artifact,” underscoring why DSR is appropriate for developing the 5-Echelon Model as a prescriptive intervention rather than a descriptive account. Likewise, March and Smith (1995) classify artefacts, including conceptual models and methods, as legitimate outputs of DSR, noting that design research “creates and evaluates IT artifacts intended to solve identified organizational problems.” When applied to blockchain-enabled cross-border transfers, complex, socio-technical, and multi-jurisdictional challenges, DSR offers a structured, solution-oriented methodology that traditional doctrinal or qualitative approaches cannot provide.

The 5-Echelon Model fits naturally within the DSR artefact taxonomy. March and Smith (1995) distinguish artefacts as “constructs, models, methods and instantiations,” which legitimises the model’s status as a design artefact rather than a theoretical abstraction. Gregor and Jones (2007) further articulate the required structure of design theory, identifying eight components forming the “anatomy of a design theory”, including purpose, constructs, principles of form and function, mutability, and justificatory kernel theories. Using these components strengthens the 5-Echelon Model by grounding it in justificatory knowledge from financial regulation and supervisory practice. The chapter follows the Design Science Research Methodology (DSRM) of Peffers et al. (2007), which defines a six-step process: “problem identification, objectives of a solution, design and development, demonstration, evaluation, and communication.” Where governance contexts require iterative stakeholder interaction, Action Design Research (ADR) complements DSRM by embedding “inseparable and inherently interwoven activities of building the IT artifact, intervening in the organization, and evaluating it concurrently.”

This hybridisation reflects the real-world nature of regulatory design, where frameworks evolve through institutional feedback.

Evaluation is central to ensuring the model's rigour and utility. Venable, Pries-Heje, and Baskerville (2016) emphasise that effective evaluation requires selecting appropriate strategies based on “why, when, how, and what to evaluate.” Two types of evaluation are used in this chapter. The first takes place before real-world testing, relying on expert opinion and criteria-based reasoning to assess whether the framework is sound. The second takes place after the framework has been applied, using structured scenario walkthroughs with regulatory practitioners to see how it holds up in practice. This follows Sonnenberg and vom Brocke's (2012) principle that evaluation must address not only “the usefulness of an artifact but also the evaluation of design decisions made to build an artifact.” DSR is a better method than doctrinal or qualitative approaches because it combines designing a solution with testing it in practice. As Wieringa (2014) explains, design science studies the artefact in its real-world setting. This is especially important in cross-border regulatory environments, where differences in institutional capacity and oversight systems determine what is actually workable. By basing the Five Echelon Model on DSR principles and evaluation methods, this chapter ensures that the regulatory framework developed is well-reasoned, suited to its context, and supported by evidence.

6.4 The 5-Echelon Knowledge Model

6.4.1 *Model Architecture and Hierarchical Structure*

The knowledge model is structured as a hierarchical pyramid comprising five design echelons, progressing from foundational strategic elements to dynamic adaptive mechanisms. This structure reflects the eDSR approach's emphasis on hierarchical organising logic, where each echelon is self-contained yet interdependent, allowing for modular implementation and iterative refinement. The pyramid architecture symbolises the bottom-up dependencies inherent in regulatory frameworks: technical integration capabilities (Echelon 3) depend on clear oversight mechanisms (Echelon 2), which in turn require foundational policy clarity (Echelon 1).

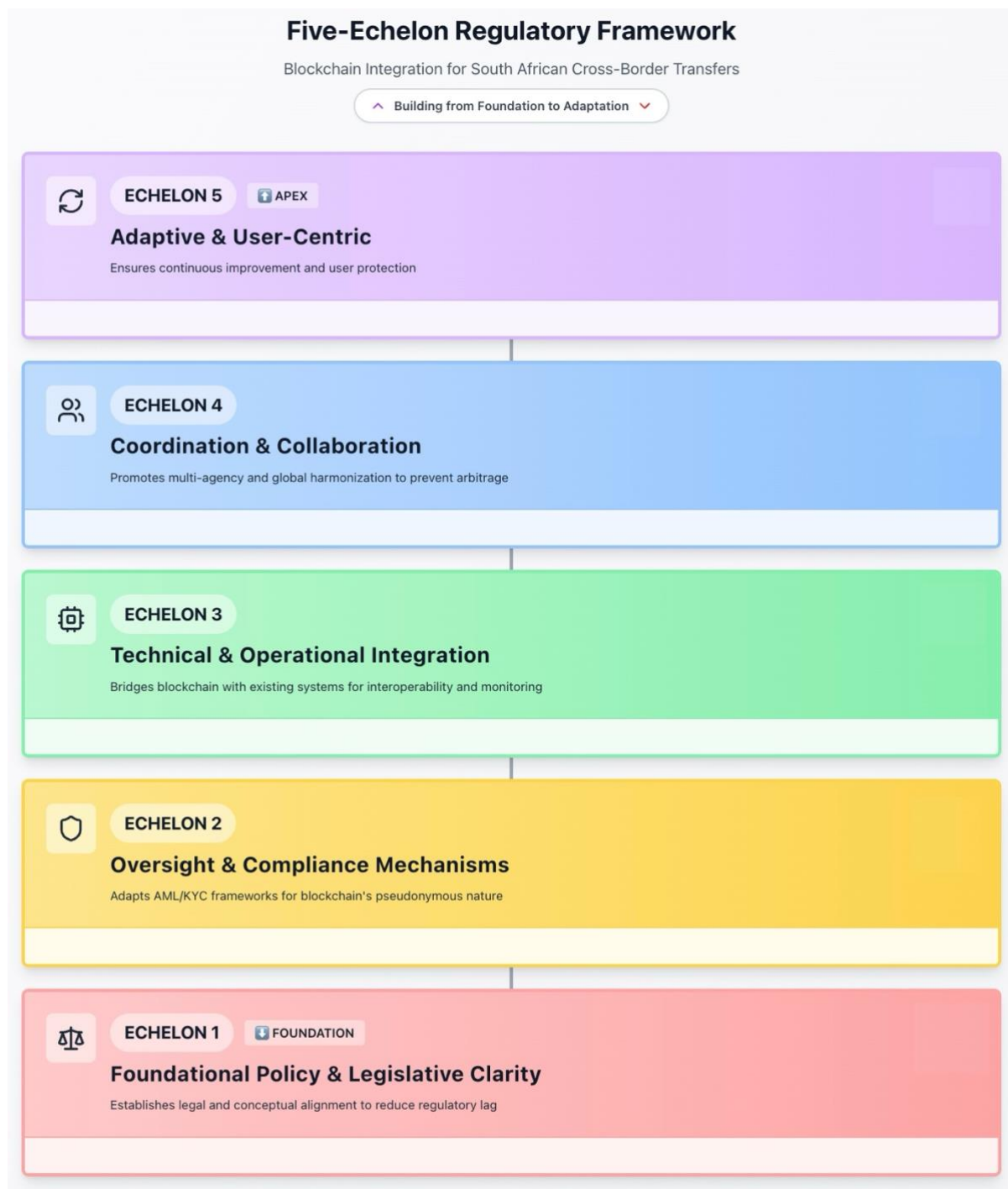


Figure 53. Graphic outlining the pyramid of Echelons (Researcher)

The five echelons are:

1. **Foundational Policy & Legislative Clarity** - Establishing core legal and conceptual alignment

2. **Oversight & Compliance Mechanisms** - Adapting traditional controls for blockchain characteristics
3. **Technical & Operational Integration** - Bridging blockchain with existing systems
4. **Coordination & Collaboration** - Ensuring cohesive domestic and international efforts
5. **Adaptive & User-Centric** - Focusing on continuous improvement and education

This breakdown simplifies complexity by allowing regulators to prioritise specific echelons (e.g., addressing Echelon 1 immediately following 2025 legislative updates) while maintaining a holistic vision for comprehensive transformation. The model directly addresses the eight dimensions identified in the gap analysis: cross-border transfers, exchange controls, payment systems, AML/CFT, crypto-assets, market conduct, prudential stability, and taxation.

6.5 Echelon 1: Foundational Policy & Legislative Clarity

6.5.1 Purpose and Strategic Importance

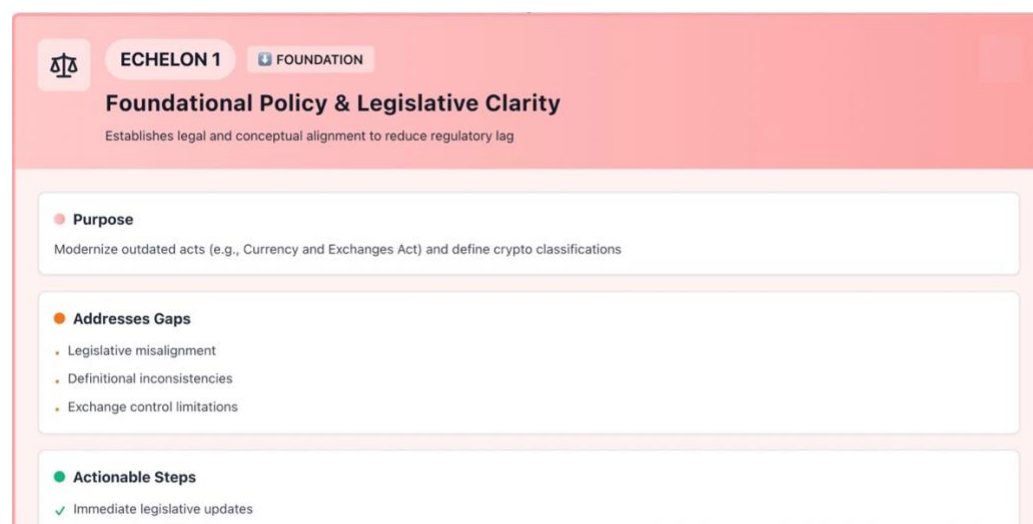


Figure 54. Graphic outlining Echelon 1 (Researcher)

Echelon 1 forms the broad base of the regulatory pyramid, establishing the foundational policy and legislative clarity necessary to reduce regulatory lag and legal uncertainty. This echelon's primary purpose is to create core legal and conceptual alignment that enables innovation while providing sufficient certainty for market participants,

regulators, and financial institutions. As Zetzsche et al. (2018) articulate, regulatory lag occurs when the pace of technological innovation exceeds the adaptive capacity of legal frameworks, creating ambiguity that hampers both compliance and innovation.

In the South African context, this regulatory lag is particularly evident in the persistence of colonial-era legislation such as the Currency and Exchanges Act of 1933, which was designed for a fundamentally different financial paradigm based on physical currency and centralised banking systems. The decentralised, data-driven, and borderless nature of blockchain and cryptocurrency technology creates fundamental incompatibilities with these legacy frameworks, necessitating comprehensive legislative reform rather than incremental adjustments.

6.5.2 Gaps Addressed

Echelon 1 directly addresses three critical gaps identified in the regulatory analysis: legislative misalignment, definitional inconsistencies, and exchange control limitations.

Legislative Misalignment: The current South African legislative framework comprises multiple acts that predate blockchain technology by decades or even centuries. The Currency and Exchanges Act of 1933, for instance, was enacted during the gold standard era and reflects assumptions about currency, value transfer, and financial control that are fundamentally incompatible with distributed ledger technology. Similarly, the Financial Intelligence Centre Act (FICA) and related AML/CFT legislation assume centralised financial intermediaries as primary compliance actors, creating ambiguity regarding the regulatory status and obligations of crypto-asset service providers (CASPs) and decentralised finance (DeFi) protocols.

Definitional Inconsistencies: The absence of clear, legally binding definitions for crypto-assets, cryptocurrency, tokens, and related concepts creates significant uncertainty across multiple regulatory domains. Different regulatory authorities and legislative instruments employ varying terminologies and classification schemes, leading to jurisdictional ambiguities and compliance challenges. The Intergovernmental Fintech Working Group (IFWG) has made progress in developing taxonomies, but these remain guidance documents rather than binding legal definitions, limiting their effectiveness in enforcement and dispute resolution.

Exchange Control Limitations: Until recently, South Africa's exchange control rules treated cryptocurrency as a foreign asset, which meant strict capital controls applied and made it very difficult to use blockchain technology for cross-border transfers. A 2025 High Court ruling offered some relief by exempting certain cryptocurrencies from these controls. This was a notable shift in the legal landscape. But the ruling leaves important questions unanswered: which cryptocurrencies are covered, how broadly it applies, and whether it conflicts with other regulations. These questions are likely to be disputed and clarified through further legal proceedings.

6.5.3 Key Components and Implementation Strategies

The implementation of Echelon 1 requires coordinated action across multiple legislative and policy domains, supported by institutional capacity building and stakeholder engagement.

Legislative Amendment Framework: The starting point for Echelon 1 is updating laws that were written long before blockchain existed. But this cannot be done by simply adding a few new definitions. The deeper problem is that some of these laws are built on assumptions that no longer hold. The Currency and Exchanges Act, 1933 (as amended), 1933 for instance, treats currency as something physical or issued by a government. Digital assets recorded on a blockchain do not fit that description, which means the law needs to be rethought at a more fundamental level, not just patched.

The amendments must address:

- Recognition of cryptocurrency and crypto-assets as legitimate value transfer mechanisms while maintaining appropriate controls
- Clarification of the regulatory status of various blockchain participants (miners, validators, node operators, CASPs, DeFi protocols)
- Establishment of clear jurisdictional boundaries for cross-border blockchain transactions
- Integration with exchange control reforms following the 2025 High Court ruling
- Creation of proportionate regulatory requirements that avoid stifling innovation while ensuring adequate oversight

Definitional Framework and Taxonomy Development: Building on the IFWG's work, Echelon 1 requires elevation of crypto-asset taxonomies from guidance to legally binding definitions. This framework must distinguish between:

- Payment tokens (designed primarily as a means of exchange)
- Utility tokens (providing access to specific products or services)
- Security tokens (representing investment contracts or financial instruments)
- Stablecoins (pegged to fiat currencies or other assets)
- Non-fungible tokens (NFTs) representing unique digital or physical assets
- Wrapped tokens and synthetic assets
- Governance tokens in decentralised autonomous organisations (DAOs)

Each category requires tailored regulatory treatment reflecting its economic substance, risk profile, and functional characteristics. The definitional framework must balance precision with flexibility, allowing for technological evolution while providing sufficient clarity for legal application.

Hybrid Governance Model Integration: Echelon 1 must formally establish the legal basis for hybrid regulatory models that integrate cryptocurrency's decentralised strengths with necessary centralised oversight. This requires explicit legislative recognition of:

- The validity and enforceability of smart contracts and automated compliance mechanisms
- The role of decentralised governance structures alongside traditional regulatory authorities
- Principles for allocating regulatory responsibility across distributed networks
- Standards for interoperability between decentralised and centralised systems

6.5.4 *Root Causes and Impact Mitigation*

The root causes addressed by Echelon 1 stem from what Zetsche et al. (2018) identify as the structural challenge of "regulatory lag" in fintech innovation. Traditional legislative processes operate on multi-year timescales with extensive consultation, drafting, parliamentary procedures, and implementation periods. Cryptocurrency technology does not stand still. New protocols, governance structures, and applications emerge on

a weekly or monthly basis. Regulation, which moves on a much slower cycle, struggles to keep pace, and the result is a persistent gap between what the technology can do and what the rules currently cover.

- The problem goes deeper than regulators simply being slow to respond. Traditional financial regulation was designed around a set of assumptions about how financial systems work. These are assumptions that do not hold in a cryptocurrency environment. These include:
 - Identifiable, licensed intermediaries as primary compliance actors
 - Centralised points of control for enforcement and supervision
 - Geographically bounded jurisdictions with clear territorial sovereignty
 - Transparent, easily auditable financial flows through established channels

Blockchain technology challenges each of these assumptions through pseudonymity, decentralisation, borderlessness, and cryptographic opacity. Echelon 1 addresses these root causes by reconceptualising regulatory frameworks around blockchain's actual characteristics rather than attempting to force-fit blockchain into legacy paradigms.

The impacts mitigated through Echelon 1 implementation include:

Legal Uncertainty Reduction: Clear legislative frameworks reduce compliance costs, enable long-term business planning, and attract foreign investment by providing regulatory certainty. Studies of fintech regulatory sandboxes demonstrate that clarity regarding applicable rules significantly increases innovation activity and market entry.

Innovation Enablement: By establishing clear legal pathways for cryptocurrency-based financial services, Echelon 1 removes barriers that currently prevent or delay innovation. This includes enabling legitimate use cases such as remittances, cross-border payments, and financial inclusion initiatives that could significantly benefit South Africa's large unbanked and underbanked populations.

Risk Management: If regulators are clear about what cryptocurrency is and who is accountable for overseeing it, they are in a much better position to prevent it from being used for money laundering, terrorist financing, or activities that harm consumers or destabilise the financial system. But when the rules are vague or contested, the

opposite tends to happen. People and businesses move their activity outside the regulated system entirely, which makes these risks harder to see and harder to stop.

6.5.5 Actionable Steps and Implementation Timeline

The implementation of Echelon 1 requires immediate action given its foundational nature and the recent 2025 regulatory developments that create both opportunities and imperatives for reform.

Immediate Actions:

- Establish a dedicated legislative reform task force comprising representatives from SARB, FIC, National Treasury, Financial Sector Conduct Authority (FSCA), and industry stakeholders
- Conduct comprehensive review of existing legislation to identify all provisions requiring amendment or clarification
- Draft preliminary legislative amendment proposals based on IFWG recommendations and international best practices
- Develop legally binding definitional framework for crypto-assets, incorporating FATF guidance and local context
- Publish draft amendments for public consultation, engaging cryptocurrency industry, financial institutions, consumer protection groups, and international partners

Short-term Actions:

- Analyse consultation feedback and refine legislative proposals
- Conduct legal impact assessments examining interactions between proposed amendments and existing legal frameworks
- Develop implementation guidelines explaining practical application of new legislative provisions
- Submit finalised legislative amendments to Parliament through appropriate sponsoring ministries
- Establish transitional provisions allowing existing blockchain businesses to achieve compliance without disruption

Medium-term Actions:

- Parliamentary consideration and passage of legislative amendments
- Development of subordinate regulations and regulatory guidelines by relevant authorities
- Establishment of licensing frameworks for CASPs and other blockchain service providers
- Creation of regulatory sandbox mechanisms for testing innovative approaches within controlled environments
- Implementation of training programs for regulators, law enforcement, and judiciary on blockchain technology and applicable legal frameworks

6.5.6 *International Alignment and Comparative Analysis*

Echelon 1's development should draw on international experiences while adapting to South African context. Several jurisdictions provide instructive examples:

The EU's MiCA regulation is one of the most comprehensive attempts to define and regulate crypto-assets anywhere in the world, and it offers useful reference points for South Africa as it develops its own framework. That said, MiCA is a highly detailed and prescriptive set of rules designed for developed European markets. South Africa's situation is different. Its regulatory capacity is still developing and its financial ecosystem needs frameworks that can flex and adapt rather than ones that lock in rigid requirements from the outset.

Singapore chose not to build an entirely new regulatory framework for cryptocurrency. Instead, it brought digital payment services, including those involving cryptocurrency, under its existing Payment Services Act and introduced a licensing requirement for providers. This allowed Singapore to encourage innovation without abandoning consumer protection or anti-money laundering obligations. South Africa faces a similar decision with its National Payment System Act, and Singapore's experience offers a practical guide for how that integration might be approached within Echelon 1.

Switzerland's "DLT Act" amendments to existing financial market legislation show how targeted amendments can modernise legacy frameworks without completely overhauling it. Rather than overhauling its entire regulatory framework, Switzerland

made focused adjustments to accommodate cryptocurrency-based activities while keeping its existing regulatory principles intact. This pragmatic approach offers a useful template for South Africa as it considers legislative reform.

The Financial Action Task Force's updated guidance on virtual assets and virtual asset service providers (VASPs) provides essential standards for AML/CFT aspects of Echelon 1. FATF's risk-based approach and the "Travel Rule" requirements for VASP-to-VASP transactions inform South Africa's Directive 9 implementation and should be fully integrated into Echelon 1's legislative framework.

6.5.7 *Theoretical Justification*

Institutional theory helps explain why South African regulators are moving toward globally aligned cryptocurrency regulation. The process is driven by three converging pressures. The obligation to meet international standards such as those of the FATF, the inclination to learn from countries that have navigated this successfully, and a shared professional sense of what good regulation looks like. Echelon 1 responds to all three, providing a structured pathway for turning these external pressures into coherent domestic policy.

Cryptocurrency technology cannot function effectively in a financial system on technical merit alone. It also requires a supportive social environment, including clear laws and recognised standards. Echelon 1 builds this foundation. By establishing legislative clarity, it gives blockchain protocols the legal standing they need to be recognised and enforced, showing in practice how social and technical development must go hand in hand.

6.6 Echelon 2: Oversight & Compliance Mechanisms

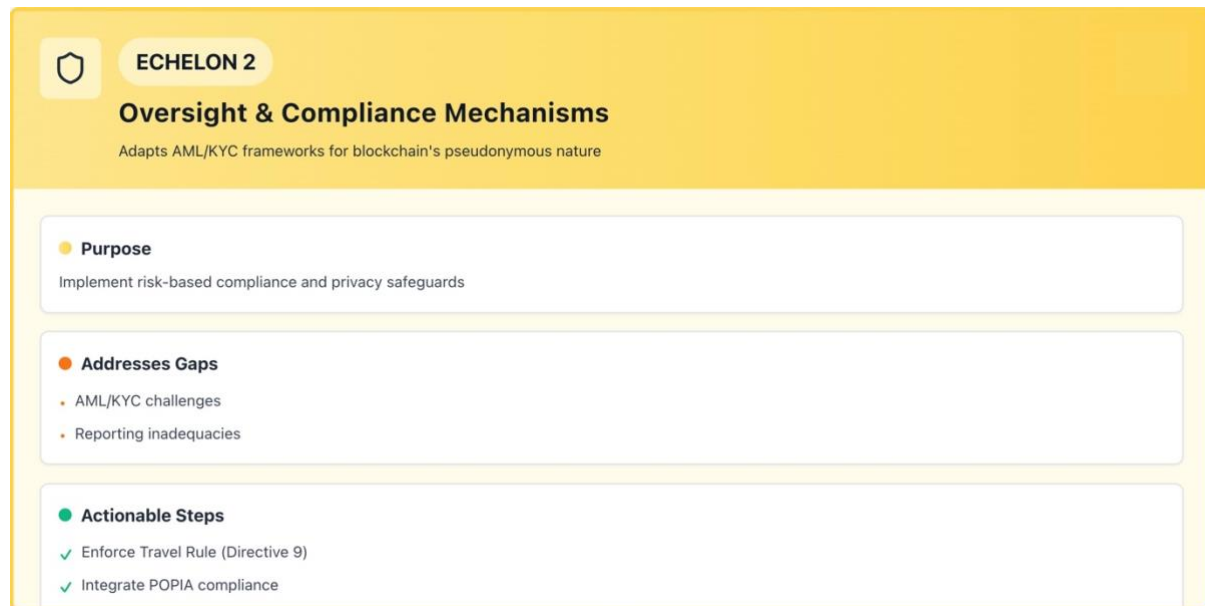


Figure 55. Graphic outlining Echelon 2 (Researcher)

6.6.1 Purpose and Strategic Importance

Echelon 1 establishes the legal framework. Echelon 2 asks a harder practical question: how do you actually enforce it? Traditional financial regulation works by placing compliance responsibilities on banks and other licensed institutions, entities that are known, regulated, and can be held accountable. Blockchain does not work that way. There is no central institution to hold responsible. Instead, activity takes place across a network of users, many of whom are anonymous and may be located anywhere in the world. Designing oversight mechanisms that work in this environment is the central challenge of Echelon 2.

Laws only matter if they can be enforced. Echelon 1 may produce a well-designed legislative framework, but if there are no practical tools to monitor what is happening in the market and hold participants accountable, those laws will have little real effect. Echelon 2 exists to bridge that gap. And in doing so, it has to grapple with a core contradiction: the regulatory systems South Africa has are built around central authority and identifiable institutions, while the technology being regulated is specifically designed to operate without either.

6.6.2 *Gaps Addressed*

Echelon 2 directly addresses three interconnected gaps: AML/KYC challenges in pseudonymous environments, reporting inadequacies for blockchain transactions, and identity verification issues in decentralised systems.

AML/KYC Challenges: Traditional AML/KYC frameworks assume that financial institutions can readily identify customers, verify their identities against authoritative documents, and monitor transactions for suspicious patterns. Blockchain's pseudonymous addressing system, where parties transact using cryptographic public keys rather than legal identities, fundamentally challenges these assumptions. While blockchain transactions are recorded on transparent, immutable ledgers, linking these transactions to real-world identities requires additional mechanisms not inherent to the technology itself.

South Africa's FICA requires financial institutions to check who their customers are, watch for unusual activity, and report anything suspicious. The problem is that it was not written with cryptocurrency in mind, and it is still unclear how far these obligations extend to crypto platforms, peer-to-peer trading, and decentralised finance. There is also a more practical issue: FICA's rules are designed to trigger additional checks when transactions reach a certain size. But on a blockchain, it is easy to move large amounts of value through many small transactions, thereby staying below those thresholds while still evading detection. The existing rules are not well equipped to catch this.

Reporting Inadequacies: The 2025 implementation of Directive 9, incorporating FATF's Travel Rule, requires CASPs to share originator and beneficiary information for transactions exceeding specified thresholds. However, several challenges impede effective implementation:

- Technical incompatibilities between different CASPs' systems for secure information sharing
- Privacy concerns regarding transmission of personal data across borders
- Difficulties identifying counterparties in peer-to-peer transactions or DeFi protocols
- Lack of standardised formats and protocols for Travel Rule compliance

- Jurisdictional ambiguities regarding which transactions trigger reporting requirements

Identity Verification Issues: Standard identity checks rely on passports, biometric data, and proof of address. But in blockchain ecosystems, especially those used by people who are unbanked or who send money across borders, many participants simply do not have these documents. There is also an international dimension: South African platforms may need to verify foreign users against identity standards that vary significantly from country to country.

Newer technologies such as self-sovereign identity systems and privacy-preserving verification methods are being developed to address these gaps, but they are not yet mature enough, legally recognised enough, or compatible enough with existing systems to be relied upon at scale.

6.6.3 *Key Components and Implementation Strategies*

Extension of FICA to CASPs with Blockchain-Specific Provisions: Echelon 2 requires formal amendment of the Financial Intelligence Centre Act to explicitly designate CASPs as accountable institutions while recognising the unique characteristics of blockchain-based services. This extension must include:

- Clear definitions of which blockchain service providers qualify as CASPs (exchanges, wallet providers, protocol developers, validators)
- Risk-based thresholds for customer due diligence reflecting blockchain's transaction characteristics
- Specific provisions for the Travel Rule implementation, building on Directive 9
- Recognition of technological solutions (smart contracts, automated monitoring) as acceptable compliance mechanisms
- Exemptions or modified requirements for truly decentralised protocols where no entity exercises control

Under the proposed Travel Rule, crypto platforms would be required to share customer information for transactions above R 5,000. The idea is to concentrate compliance effort where the risk is highest without making every small transaction burdensome to process. That is a reasonable principle, but the specific threshold only makes sense if

it is based on evidence. It should reflect what we actually know about how cryptocurrency is used in South Africa and how money laundering tends to occur in these markets, rather than being set at an arbitrary figure.

Alignment with POPIA for Privacy Protection: The POPIA creates important constraints on how personal data can be collected, processed, and shared. Echelon 2 must carefully navigate the tension between AML/CFT requirements for information sharing (particularly under the Travel Rule) and POPIA's privacy protections. This requires:

- Legal clarity regarding lawful bases for processing personal data for AML/CFT purposes
- Data minimisation principles ensuring only necessary information is collected and retained
- Security requirements for protecting personal data during transmission and storage
- Cross-border transfer mechanisms compliant with both POPIA and international standards
- Individual rights frameworks allowing data subjects to exercise POPIA rights while maintaining compliance with AML obligations

One of the tensions in cryptocurrency regulation is that AML compliance requires access to personal information, while privacy laws restrict how that information can be shared and used. Certain technologies are being developed that could resolve this tension. Zero-knowledge proofs allow a system to confirm that a transaction is safe and comes from a legitimate user, without anyone actually seeing that user's personal details. Secure multi-party computation allows different organisations to work together to spot suspicious patterns in transaction data, while each organisation's data remains hidden from the others. Both technologies point toward a future where compliance and privacy do not have to be in conflict.

Risk-Based Compliance Models: Not every cryptocurrency transaction poses the same risk. A small peer-to-peer transfer between two verified individuals is very different from a large anonymous transaction moving across multiple jurisdictions. Echelon 2 should treat them differently, applying stricter requirements where the risks are real and

serious, and lighter ones where they are not. This is not a novel idea. The FATF, which sets global standards for combating money laundering and terrorist financing, actively encourages this kind of proportionate, risk-based approach precisely because it makes better use of limited regulatory resources.

For South Africa, risk-based models might incorporate:

- Transaction size and frequency thresholds
- Origination and destination jurisdictions (higher scrutiny for high-risk jurisdictions)
- Customer risk profiles (enhanced due diligence for politically exposed persons)
- Product risk assessments (different requirements for Bitcoin vs. privacy coins)
- Delivery channel risks (person-to-person vs. exchange-mediated transactions)

This approach requires CASPs to conduct enterprise-wide risk assessments, develop risk-based policies and procedures, and demonstrate to supervisors that their compliance frameworks effectively address identified risks.

Blockchain-Specific Monitoring and Reporting Systems: Traditional transaction monitoring systems designed for banking channels may be ineffective or inappropriate for cryptocurrency transactions. Echelon 2 requires development of monitoring capabilities that leverage blockchain's transparency while respecting its pseudonymity:

- Blockchain analytics tools for pattern analysis and suspicious activity detection
- Smart contract-based automated reporting triggers
- Real-time transaction monitoring rather than batch processing
- Network analysis capabilities for identifying complex transaction chains
- Integration with global blockchain intelligence platforms

6.6.4 *Root Causes and Structural Adaptations*

The root causes addressed by Echelon 2 stem from structural limitations in traditional AML/CFT frameworks that assume centralised financial intermediaries as primary compliance actors. As identified in the source document, these frameworks were designed for banking models where:

- Banks know their customers through account opening procedures

- Transactions flow through intermediaries who can monitor and report
- Jurisdictional control is clear based on the intermediary location
- Enforcement is straightforward through intermediary sanctions or license revocation

Blockchain disrupts each of these assumptions through decentralisation, pseudonymity, borderlessness, and disintermediation. Echelon 2 addresses these structural limitations by:

Expanding Compliance Actor Definitions: In traditional finance, compliance is largely the responsibility of banks and other licensed institutions. Blockchain does not have a single institution at its centre. Instead, it has many different participants who keep the system running, including miners, node operators, developers, wallet providers, and ordinary users. Each of these plays a different role and has a different level of influence over how the system operates. Echelon 2 takes this into account by distributing compliance responsibilities across these participants rather than placing the entire burden on one type of actor. It assigns obligations based on who has the most control, who benefits the most, and who is best placed to act.

Leveraging Technology for Compliance: It is easy to see blockchain's features as problems for regulators. Anonymity, decentralisation, and borderless transactions all make oversight harder. But Echelon 2 takes a different view: the same features that create challenges can also be used as compliance tools. Every transaction on a blockchain is permanently recorded and cannot be changed, which makes for a far more reliable audit trail than paper records or editable databases. Smart contracts can be written to automatically apply compliance rules the moment a transaction takes place, removing the need for manual checks. Therefore, because many blockchains are open and transparent, it becomes possible to monitor patterns of activity across the whole network, something that is simply not possible in traditional financial systems.

Implementing Graduated Compliance Frameworks: Recognising that one-size-fits-all requirements are inappropriate, Echelon 2 creates tiered frameworks with proportionate requirements based on risk, scale, and business model.

Addressing Jurisdictional Complexities: When a blockchain transaction crosses national borders, a basic but important question arises: whose rules apply? A platform

might be registered in one country, serve customers in another, and be controlled by people in a third. Physical location alone cannot answer that question. Echelon 2 sets out a clearer way of deciding. It looks at where the real economic activity takes place, where the customers actually are, who is in operational control, and what agreements exist between the relevant countries. Together, these factors provide a more honest and practical basis for assigning regulatory responsibility.

6.6.5 *Impacts Mitigated*

Effective implementation of Echelon 2 mitigates several critical risks while enabling blockchain innovation:

Money Laundering and Terrorist Financing Risks: By establishing clear, enforceable AML/KYC requirements adapted to blockchain characteristics, Echelon 2 reduces South Africa's vulnerability to illicit financial flows. This protects the country's reputation, maintains access to international banking channels, and fulfils FATF obligations.

Consumer Protection Risks: Clear compliance frameworks protect users from fraud, scams, and unscrupulous service providers. By requiring CASPs to implement customer due diligence and monitoring, Echelon 2 creates accountability and recourse mechanisms for consumers.

Systemic Stability Risks: Good oversight allows regulators to spot problems early, before a localised issue in the cryptocurrency market grows into something that threatens the wider financial system. This matters because cryptocurrency prices can be highly volatile and the market is increasingly connected to traditional finance.

Compliance Uncertainty: Clear compliance requirements also benefit legitimate businesses directly. When the rules are known and stable, businesses can plan ahead and attract investment. This draws in responsible operators while making the market less attractive to those who rely on regulatory confusion to operate undetected.

6.6.6 *Actionable Steps and Implementation Timeline*

Medium-term Actions:

- Draft amendments to FICA explicitly designating CASPs as accountable institutions with blockchain-specific provisions
- Develop detailed compliance guidelines explaining obligations, acceptable practices, and supervisory expectations
- Establish technical standards for Travel Rule implementation, potentially through industry consortium or regulatory working group
- Create regulatory reporting systems capable of receiving and processing blockchain transaction data
- Implement CASP registration or licensing system with fit-and-proper requirements for operators
- Develop supervisory capacity within FIC for blockchain-specific oversight, including training programs and recruitment of technical specialists

Medium-term Actions:

- Launch pilot programs testing privacy-enhancing technologies for AML/CFT compliance
- Establish formal coordination mechanisms between FIC, SARB, FSCA, and other relevant authorities for integrated supervision
- Implement risk-based supervision framework conducting on-site and off-site examinations of CASPs
- Develop enforcement guidelines and penalty frameworks for non-compliance
- Create industry feedback mechanisms for continuous improvement of compliance frameworks
- Establish mutual recognition agreements with other jurisdictions' CASP supervisors to address cross-border issues

6.6.7 *International Coordination and FATF Compliance*

Echelon 2's design must ensure full compliance with FATF Recommendations, particularly Recommendation 15 (new technologies) and Recommendation 16 (wire transfers/Travel Rule). The FATF's updated guidance on virtual assets explicitly requires:

- VASPs to be licensed or registered and subject to effective monitoring
- VASPs to be obliged to identify and verify customers

- VASPs to maintain records and report suspicious transactions
- VASPs to comply with the Travel Rule for transfers exceeding USD/EUR 1,000

The ZAR 5,000 threshold cannot simply be asserted. It needs to be backed by a risk assessment that shows it offers a level of protection equivalent to international standards. Echelon 2 should also build in the flexibility that FATF encourages, applying lighter checks where the risk of money laundering or terrorist financing is genuinely low and stricter ones where the risk is higher.

Coordination with other countries needs to go beyond South Africa's FATF obligations. South Africa has significant remittance flows with countries across Southern Africa, Asia, and Europe, and practical arrangements need to be in place with these partners to ensure that the information required under the Travel Rule can actually be shared across borders without breaching data protection laws.

6.7.8 *Theoretical Foundations*

Regulators are used to working through banks and other central institutions. These are entities they can identify, license, and hold accountable. Blockchain has no equivalent. Oversight therefore cannot work the same way. It has to be reinvented for a decentralised environment. Echelon 2 does this by spreading compliance responsibilities across the network and using technology itself as part of the oversight mechanism. This creates a new kind of relationship between the people involved: regulators, platforms, and users, and the technology they use, including smart contracts and automated monitoring tools.

The Travel Rule makes this challenge concrete. It requires centralised banks and decentralised crypto platforms to share information with each other, even though these two systems were not built to work together. This is why crypto-asset service providers end up at the centre of compliance efforts. They sit at the boundary between the decentralised blockchain world and the centralised legal world. This makes them the most practical point at which regulatory requirements can be applied and enforced.

6.8 Echelon 3: Technical & Operational Integration

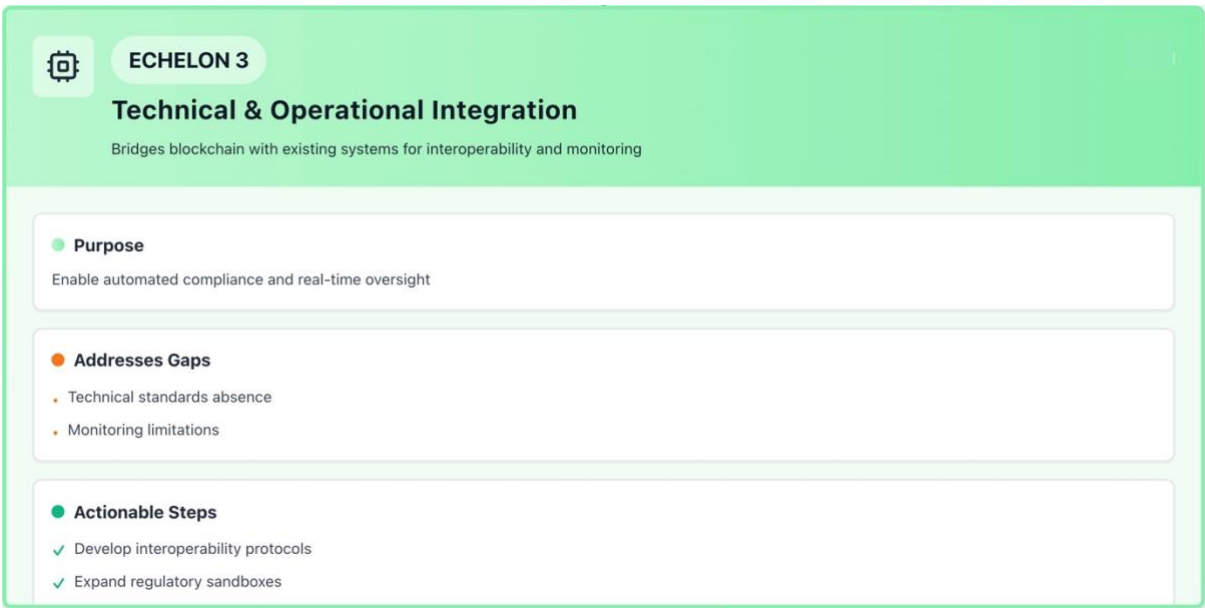


Figure 56. Graphic outlining Echelon 3 (Researcher)

6.8.1 Purpose and Strategic Importance

Echelons 1 and 2 put the legal and oversight foundations in place. Echelon 3 asks the next, more practical question: can these frameworks actually be made to work within South Africa's existing financial systems? Connecting blockchain technology to established infrastructure is not straightforward, and without this connection, even the best-designed regulatory framework cannot be properly enforced or operationally executed. Echelon 3 exists to bridge that gap.

The strategic importance of Echelon 3 lies in its potential to transform blockchain from a parallel, disconnected system into an integrated component of South Africa's financial ecosystem. This integration is essential for realising cryptocurrency's promise of reduced costs, increased speed, greater transparency, and enhanced financial inclusion in cross-border transfers. Without technical and operational integration, cryptocurrency remains siloed, limiting its benefits and creating fragmented, inefficient markets.

6.8.2 Gaps Addressed

Echelon 3 directly addresses three interconnected gaps: interoperability absence between blockchain and traditional systems, real-time monitoring limitations, and innovation implementation barriers.

Interoperability Absence: South Africa's existing payment infrastructure, including the South African Multiple Option Settlement (SAMOS) system, the Southern African Development Community Real Time Gross Settlement system (SADC-RTGS), and various electronic funds transfer networks, was designed without consideration for blockchain integration. This creates technical incompatibilities manifesting at multiple levels:

- Data format and message standard differences (ISO 20022 for traditional systems vs. varied blockchain protocols)
- Settlement finality concepts (immediate on-chain settlement vs. delayed traditional settlement)
- Identity and addressing schemes (bank account numbers vs. cryptographic addresses)
- Transaction validation mechanisms (centralised authorization vs. distributed consensus)
- Cross-border routing (correspondent banking vs. peer-to-peer blockchain networks)

These incompatibilities create friction, requiring manual interventions, reconciliation processes, and workarounds that negate blockchain's efficiency advantages. They also create risks of errors, delays, and compliance failures when transactions traverse blockchain-traditional system boundaries.

Real-Time Monitoring Limitations: Blockchain records every transaction permanently and transparently which should, in theory, make it easier to monitor. But South Africa's regulatory systems were built for a different era. They are designed around periodic reporting, after-the-fact audits, and investigations that begin once something has already gone wrong. By that point, on a blockchain, a great deal can have happened. Blockchain operates twenty-four hours a day, seven days a week, processes enormous volumes of transactions, and can move faster than any manual oversight process.

Waiting for a quarterly report or launching an investigation after the fact is simply not fast enough.

Real-time monitoring requires:

- Technical interfaces for accessing blockchain data
- Analytics capabilities for processing high-frequency transaction streams
- Automated alert systems for triggering regulatory responses
- Forensic tools for investigating complex transaction patterns
- Cross-chain analysis capabilities given the multi-blockchain ecosystem

Innovation Implementation Barriers: Despite recognition of blockchain's potential, practical barriers impede implementation of innovative use cases. These include:

- Lack of standardised APIs between blockchain and banking systems
- Regulatory uncertainty regarding permissible blockchain integrations
- High costs and technical complexity of integration projects
- Skills shortages in both blockchain and traditional financial sectors
- Risk aversion among established financial institutions
- Insufficient testing environments for validating innovations before deployment

6.8.3 *Key Components and Implementation Strategies*

Standards Development for DLT Interoperability: Echelon 3 requires establishment of comprehensive technical standards enabling blockchain systems to interoperate with each other and with traditional financial infrastructure. This standards framework should address:

Messaging Standards: Blockchain and traditional financial systems do not naturally speak the same language. To enable them to exchange data reliably, common messaging standards need to be developed or adopted. A practical starting point would be ISO 20022 the global standard already used for financial messaging, extended to handle blockchain-specific features such as smart contract instructions, cryptographic signatures, and decentralised identifiers.

API Specifications: Software applications need a consistent and standardised way to interact with blockchain networks. This requires clearly defined interfaces that allow

systems to read transaction data, submit new transactions, and retrieve information about the current state of the blockchain. Without these standards, every integration becomes a custom-built solution, costly, inconsistent, and difficult to maintain.

Identity Mapping: People and institutions have identities in traditional financial systems such as bank account numbers, government-issued IDs and separate identities on blockchain networks, typically in the form of public keys or decentralised identifiers. Standards are needed to link these two sets of identities in a way that satisfies KYC requirements without unnecessarily exposing personal information. This would allow the efficiency of blockchain to be preserved while still meeting regulatory obligations around knowing who is transacting.

Settlement Bridging: When a transaction involves both a blockchain and a traditional payment system, the two need to settle in a coordinated way. This raises practical challenges around finality such as confirming that a transaction is complete and cannot be reversed, as well as reconciliation and dispute resolution. Several technical approaches exist to address this, including atomic swaps, hash-time locked contracts, and centralised clearing mechanisms that act as a bridge between the two systems. The right approach will depend on the specific use case and the level of decentralisation required.

The EU's experience with MiCA offers a practical model worth following. MiCA does not try to write every technical requirement into the law itself. Instead, it establishes broad expectations. These are that platforms must be well-run, resilient, and capable of working with other systems, and then tasks a separate regulatory body, ESMA, with developing the specific technical standards that put those expectations into practice. This works well because technology changes faster than legislation can. By keeping the principles in the law and the technical detail outside it, the framework can be updated without needing to go back to parliament every time. Echelon 3 should adopt the same logic: set clear principles, and develop the technical guidance through close collaboration with the industry professionals who understand the systems best.

Smart Contract Integration for Automated Compliance: Smart contracts, self-executing code on blockchain networks, offer unprecedented opportunities for

automating compliance processes that traditionally require manual intervention. Echelon 3 should establish frameworks for deploying smart contracts to automate:

KYC/AML Verification: Rather than checking compliance after a transaction has taken place, smart contracts can be programmed to verify upfront that all participants have completed the required identity checks before a transaction is allowed to proceed. By checking credentials automatically at the point of transaction, compliance becomes built into the system itself. It is not something that has to be separately investigated and enforced after the fact.

Tax Withholding and Reporting: For cross-border transfers, smart contracts can be programmed to calculate the applicable tax automatically, withhold it at the point of transfer, send it directly to the relevant tax authority, and generate the required documentation, all without manual intervention. This directly addresses one of the most persistent gaps in cryptocurrency tax compliance: the fact that transactions often occur faster than reporting systems can track them.

Transaction Limits and Sanctions Screening: Smart contracts can be programmed to enforce transaction limits and automatically check whether the parties involved appear on sanctions lists thereby blocking prohibited transactions in real time before they are completed. This removes the lag that exists in traditional compliance systems, where suspicious transactions may only be identified and acted upon after they have already been processed.

International Precedent: Singapore's Project Ubin Singapore's Monetary Authority (MAS) has actively tested these capabilities through Project Ubin, which explored how smart contracts could be used to automate settlement and compliance checks, including sanctions screening and transaction limits, while still preserving transaction privacy through techniques such as zero-knowledge proofs. The project demonstrated that automated compliance and privacy protection are not mutually exclusive. South Africa's own Project Khokha, led by the South African Reserve Bank, explored similar ground in the context of interbank settlement.

Echelon 3 should build on this foundation by expanding Project Khokha's scope to incorporate automated compliance mechanisms of the kind that Project Ubin demonstrated.

Regulatory Reporting: Instead of requiring institutions to compile and submit reports periodically, smart contracts can generate regulatory reports automatically as each transaction occurs, giving supervisors a real-time view of market activity. MAS has piloted this approach through its regulatory sandbox, where selected fintech firms have tested automated reporting under close regulatory supervision. This model, which is real-time, automated, and continuously verified represents a significant improvement over the periodic manual reporting that currently underpins most regulatory oversight.

Integration with Payment Systems and Project Khokha Expansion: The South African Reserve Bank's Project Khokha (Phase 1 in 2018, Phase 2 in 2021) demonstrated the feasibility of using blockchain for wholesale interbank settlement, processing the full daily volume of South Africa's payment transactions with settlement finality and complete privacy. Echelon 3 should build upon this foundation by:

Extending Khokha to Cross-Border Payments: While Khokha focused on domestic interbank settlement, Echelon 3 should extend this to cross-border scenarios, potentially connecting with similar initiatives in other African countries or major trading partners. The SADC region presents an ideal testing ground given existing monetary coordination through SADC-RTGS.

Retail Integration: Project Khokha was wholesale-focused. Echelon 3 should develop retail payment integrations enabling consumers and businesses to benefit from blockchain efficiency. This might involve SARB issuing a central bank digital currency (CBDC) or creating regulatory frameworks for stablecoin integration with retail payment systems.

Multi-Ledger Interoperability: Each cryptocurrency does not all run on the same network. Ethereum, Bitcoin, and dozens of other public and private blockchains each operate independently, and activity is spread across all of them. If South Africa's Project Khokha infrastructure can only interact with one of these networks, it will have limited reach and effectiveness. Echelon 3 should therefore be designed to work across multiple platforms. Singapore has already shown that this is possible through Project Guardian, which is a joint initiative between MAS and private sector partners that successfully tested how real-world assets could be tokenised and managed across

different blockchain networks simultaneously. South Africa can draw directly on these findings.

Case Study: Singapore's Comprehensive Technical Integration Approach

Singapore's regulatory framework, anchored in the Payment Services Act 2019 and supervised by the Monetary Authority of Singapore (MAS), offers a robust model for implementing Echelon 3: Technical and Operational Integration in cryptocurrency and cryptocurrency regulation. This framework demonstrates several critical success factors that collectively address technical integration challenges in the fintech ecosystem.

Regulatory Sandbox with Technical Focus

MAS pioneered one of the world's first and most sophisticated fintech regulatory sandboxes in 2016, subsequently expanding its scope through enhanced arrangements. Unlike traditional sandboxes that primarily focus on regulatory compliance, MAS's approach emphasises technical validation, requiring participants to demonstrate operational resilience, security protocols, and system interoperability before graduating to full licensing. By 2024, more than 50 blockchain and cryptocurrency projects had participated, generating empirical evidence on integration challenges and solutions (MAS, 2023).

Industry Collaboration through Project Ubin

Between 2016 and 2020, Singapore ran a five-phase initiative called Project Ubin to test how blockchain technology could be integrated into its financial system. The project achieved several practical milestones: 1. connecting blockchain to Singapore's main payment network 2. establishing blockchain-based links with other central banks, 3. testing how foreign exchange could be handled automatically. But perhaps its most lasting contribution was the decision to make all of its technical work publicly available. By publishing its code and specifications openly, Singapore gave other countries a concrete, tested starting point rather than requiring them to begin from scratch. South Africa's Project Khokha is the natural vehicle for applying these lessons locally (Tham, 2024).

API Standardisation through APIX

MAS launched the API Exchange (APIX), a global fintech marketplace and sandbox platform providing standardised APIs for seamless integration between fintech solutions and financial institutions. This initiative significantly reduces technical barriers and accelerates innovation adoption. South Africa could emulate this approach by developing a similar API standardisation platform, potentially leveraging infrastructure from the Payments Association of South Africa (PASA) (MAS, 2023).

Technical Specifications for Stablecoins

In August 2023, MAS finalised a stablecoin regulatory framework under the Payment Services Act, introducing stringent technical requirements for reserve composition, redemption mechanisms, and disclosure standards. These measures aim to ensure that stablecoins function reliably as payment instruments while maintaining monetary stability. Issuers of MAS-regulated stablecoins must maintain 100% reserve backing, provide daily mark-to-market valuations, and guarantee redemption at par within five business days (MAS, 2023).

Implications for South Africa

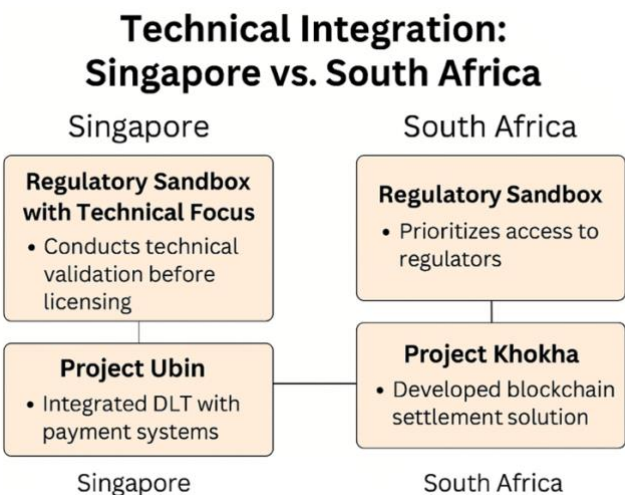


Figure 57. Graphic outlining comparisons between Singapore (Project Ubin) and South Africa’s cryptocurrency arena (Researcher)

Singapore's approach underscores the importance of technical rigour, collaborative innovation, and standardised integration protocols in cryptocurrency regulation. South Africa can draw lessons from these initiatives by:

- Expanding regulatory sandboxes to include technical validation.
- Promoting open-source collaboration through projects akin to Ubin.
- Developing API standardisation platforms to reduce integration friction.
- Establishing stable-coin technical frameworks aligned with global best practices

6.8.4 *Root Causes and Technical Solutions*

Traditional payment systems were built over many decades. They were designed around the assumption that a central institution would be in control, that transactions would be processed in batches rather than continuously, and that the network would be closed to anyone without explicit permission. So much time, money, and organisational effort has been invested in these systems that changing them fundamentally, even when there are good reasons to do so, meets significant resistance. Blockchain was built on entirely different assumptions: no central controller, continuous real-time processing, and open access. These two systems are not just technically different. They reflect different philosophies about how financial infrastructure should work. Connecting them is therefore not a simple technical fix. It requires a deliberate and thoughtful design process that takes the best of both approaches and finds ways to make them work together without forcing either to abandon what makes it valuable.

Technical Solutions for Interoperability:

Wrapped Assets and Token Bridges: Imagine a blockchain token that represents a rand sitting in a South African bank account. The token can be transferred instantly on the blockchain, but the actual rand behind it moves through the traditional banking system in the usual way. This is the concept behind wrapped assets which is a way of making traditional money work on a blockchain without replacing the underlying financial infrastructure. It has been used successfully elsewhere, but it comes with real design challenges: the link between the token and the underlying asset must be secure, someone must hold the asset in custody, and the law must be clear about what the token actually represents. The 2025 High Court ruling makes this more complex still. By exempting certain cryptocurrencies from exchange controls, the ruling created a

distinction that the technical systems underpinning Echelon 3 must be able to recognise and apply. Not all blockchain transactions will be treated the same way under exchange control law and the systems built under Echelon 3 need to be able to tell the difference, potentially through:

On-chain flags or metadata indicating transaction types

- Smart contract logic enforcing exchange control compliance where applicable
- Automated reporting of transactions potentially subject to exchange controls
- Technical interfaces between blockchain systems and the South African Reserve Bank's Financial Surveillance Department

Oracles for Bridging On-Chain and Off-Chain Data: Blockchain systems do not automatically have access to information from the outside world. They cannot, on their own, look up current exchange rates, check a sanctions list, or confirm that a user's identity has been verified. Oracle systems solve this problem by providing a secure, reliable mechanism for bringing external data onto the blockchain. Because the integrity of this data matters enormously, inaccurate or manipulated data could compromise compliance. Echelon 3 should therefore establish clear standards for which oracle providers are authorised to supply this information, and under what conditions. These oracles might be operated directly by regulatory authorities or by licensed private providers, but in either case the standards governing their operation need to be clearly defined.

Layer 2 Solutions for Scalability: Major public blockchains like Bitcoin and Ethereum were not designed to handle the volume of transactions that a national payment system requires. Processing every transaction directly on the main blockchain becomes slow and expensive at scale. Layer 2 solutions address this by handling large volumes of transactions off the main blockchain and then periodically settling the net result on it. This is similar in principle to how a bank might process thousands of internal transfers before settling with another bank at the end of the day. Well-established examples include the Lightning Network for Bitcoin and rollup systems for Ethereum. Echelon 3 should explicitly recognise these architectures in its technical standards and compliance

frameworks, ensuring that transactions processed through Layer 2 systems are subject to the same regulatory requirements as those settled directly on the main blockchain.

6.8.5 Impacts and Benefits of Technical Integration

Effective implementation of Echelon 3 generates multiple positive impacts while mitigating technical risks:

Cost Reduction in Cross-Border Transfers: One of the most immediate and tangible benefits of technical integration is lower costs for cross-border money transfers. This matters enormously in South Africa, where a large migrant worker population regularly sends money to neighbouring countries. World Bank data consistently shows that blockchain-based remittance corridors can cost 40 to 60 percent less than transfers made through traditional correspondent banking networks. But these savings do not happen automatically. Without smooth, reliable connections between blockchain systems and traditional banking infrastructure, easy ways for users to move money in and out of the blockchain, the friction involved can cancel out the cost advantage entirely. Technical integration is what makes the promise of cheaper remittances a practical reality.

Traceability and Transparency: Every transaction recorded on a blockchain leaves a permanent, tamper-proof trail. When regulators can access and analyse this data in real time, it becomes a powerful tool for detecting money laundering, enforcing tax obligations, and investigating fraud. This is far more effective than waiting for periodic reports that may be incomplete or delayed. The EU's MiCA regulation sets a clear benchmark here, explicitly requiring crypto-asset service providers to maintain systems that give regulatory authorities direct access to transaction data. South Africa should aim to meet or exceed this standard through the technical integration work of Echelon 3.

Financial Inclusion: Millions of South Africans do not have traditional bank accounts, but many have mobile phones. Blockchain-based wallets offer a potential route to financial services for this population — but only if those wallets can connect seamlessly with the payment systems people actually use day to day, including merchant payment terminals, bill payment platforms, and government benefit distribution channels. Without this integration, blockchain wallets remain isolated and of limited practical use.

Singapore has shown how this can work: by licensing payment service providers to offer blockchain-based wallets that connect directly to traditional payment infrastructure, it has demonstrated that inclusion and integration can be achieved together.

Innovation Acceleration: When technical interfaces are standardised, new entrants no longer need to negotiate a separate, costly integration agreement with every established institution they want to connect with. They can simply build to the standard and plug in. This lowers the barrier to entry significantly, encourages competition, reduces the concentration of market power among a small number of large players, and ultimately benefits consumers through better services and lower prices. Standardisation does not just make the system more efficient. It makes the market more open.

6.8.6 *Actionable Steps and Implementation Timeline*

Medium-term Actions:

- Establish Technical Standards Working Group comprising SARB, FSCA, PASA, telecommunications providers, banking representatives, and blockchain industry participants
- Conduct comprehensive technical assessment of existing payment infrastructure, identifying integration points and requirements
- Develop prototype API specifications for blockchain-banking integration, using Project Khokha as foundation
- Launch pilot programs testing smart contract automation for specific compliance use cases (e.g., Travel Rule compliance, tax withholding)
- Fund development of regulatory node infrastructure enabling real-time blockchain monitoring by supervisory authorities
- Establish technical requirements for CASP licensing regarding system security, resilience, and integration capabilities
- Create certification program for blockchain integration specialists, addressing skills gaps

Medium to Long-term Actions:

- Deploy production-grade blockchain-banking integration infrastructure based on pilot learnings

- Expand Project Khokha to include cross-border payment corridors with key trading partners
- Implement automated compliance infrastructure using smart contracts and regulatory oracles
- Establish blockchain data analytics centre within FIC or SARB for supervisory monitoring
- Develop technical standards for CBDC or stablecoin integration if policy decisions favour these approaches
- Create public-facing dashboards showing aggregate blockchain payment statistics, promoting transparency
- Implement regular technical reviews and updates to standards reflecting technological evolution

Case Study: EU MiCA's Technical Requirements and Implications

The European Union's Markets in Crypto-Assets Regulation (MiCA), fully applicable from December 2024, introduces a comprehensive regulatory framework for crypto-asset service providers (CASPs) and token issuers. MiCA's technical provisions offer a valuable precedent for South Africa's Echelon 3: Technical and Operational Integration, emphasizing operational resilience alongside legal compliance (European Securities and Markets Authority [ESMA], 2025).

Authorisation and Technical Criteria

MiCA mandates that CASPs obtain authorization from national competent authorities based on stringent technical and organizational requirements. These include:

- Own funds requirements ranging from €50,000 to €150,000 depending on service type.
- Governance and risk management frameworks, including internal control mechanisms.
- Prudential safeguarding of client assets through segregation requirements.
- Outsourcing controls to ensure operational resilience.
- Cybersecurity measures addressing ICT risks and continuity (Norton Rose Fulbright, 2024; ESMA, 2025).

These provisions reflect MiCA's recognition that effective regulation must assess technical and operational capabilities, not merely legal compliance. South Africa's CASP licensing regime should incorporate similar technical assessments to strengthen resilience.

Specific Requirements for Stablecoins

MiCA differentiates between asset-referenced tokens (ARTs) and electronic money tokens (EMTs), imposing stricter obligations on "significant" tokens with systemic impact. Key technical requirements include:

- Reserve composition standards: ARTs must maintain reserves equivalent to token value; EMTs must comply with e-money rules.
- Redemption rights at par value at any time.
- Disclosure obligations: White papers detailing consensus mechanisms, technical vulnerabilities, and operational protocols.
- Operational resilience for distributed ledger systems.
- Interoperability obligations for significant token issuers (InnReg, 2025; Squire Patton Boggs, 2025).

More and more South Africans are using stablecoins which digital currencies pegged to a stable value. This enables them to send money abroad and to protect themselves against the rand losing value. Echelon 3 needs to make sure these stablecoins can work within South Africa's existing payment infrastructure. But it also needs to ensure that consumers are protected and that widespread stablecoin use does not create new risks for the broader financial system.

The EU has developed detailed rules for stablecoins under MiCA, and South Africa can learn from this. However, the EU's rules were designed for a very different context. South Africa will need to adapt them, particularly when it comes to two practical questions: where and how the assets backing a stablecoin are held, and what happens when a user wants to convert their stablecoin back into rand.

Technical Incident Reporting

MiCA obliges CASPs to report major ICT incidents to competent authorities, including:

- Distributed denial-of-service (DDoS) attacks.
- Protocol vulnerabilities.
- Significant operational disruptions.
- Data breaches (CMS LawNow, 2025).

South Africa should adopt similar real-time incident reporting, potentially automated through blockchain monitoring infrastructure.

Limitations and Criticisms

MiCA is thorough, but it has a significant drawback: its requirements are the same for everyone, regardless of size. For large, established firms with dedicated compliance teams, this is manageable. For smaller firms and startups, the cost and complexity of compliance can be prohibitive, and this risks pushing innovative players out of the market before they have had a chance to grow. Singapore has deliberately avoided this problem by setting broad principles rather than detailed prescriptions, giving firms flexibility in how they meet regulatory expectations.

South Africa should take note. Rather than applying the same rules to every firm regardless of its size or risk profile, a tiered approach would be more proportionate, lighter requirements for smaller, lower-risk participants, and more demanding ones for larger firms where the potential consequences of failure are greater (Norton Rose Fulbright, 2024).

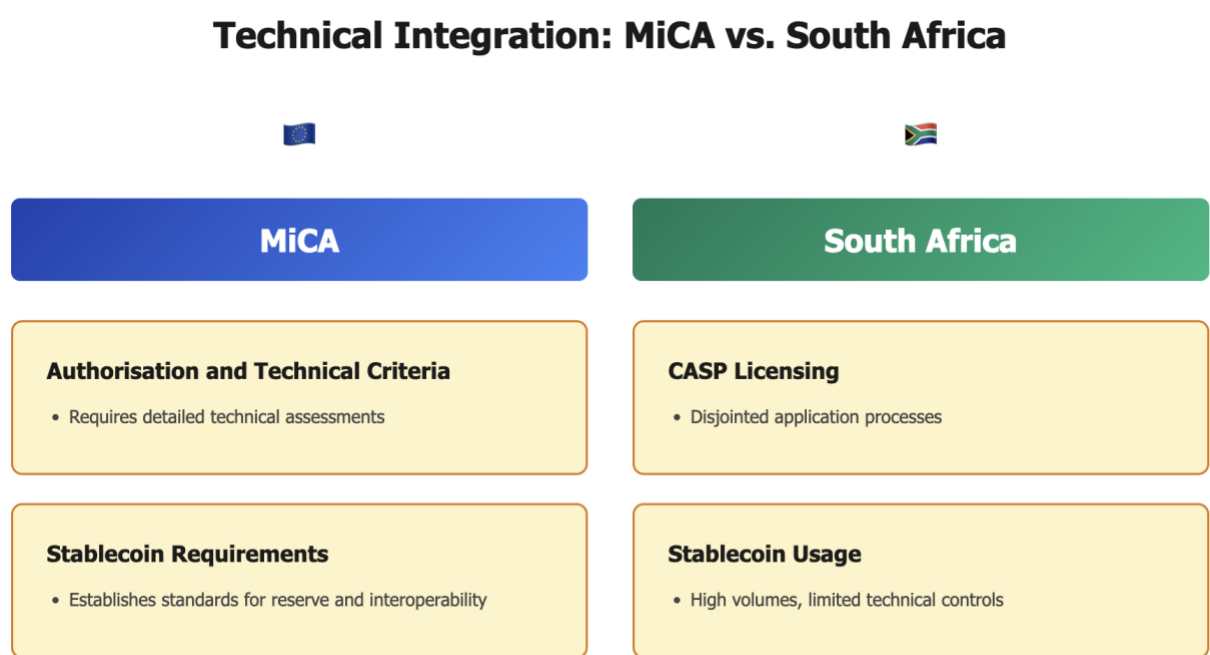


Figure 58. Graphic outlining comparisons between EU (MiCA) and South Africa’s cryptocurrency arena (Researcher)

MiCA demonstrates that technical rigour, governance standards, and operational resilience are essential for crypto regulation. South Africa can leverage MiCA’s framework to:

- Introduce technical licensing criteria for CASPs.
- Develop stable-coin-specific technical standards.
- Implement incident reporting protocols.
- Adopt a risk-based compliance approach to balance innovation and oversight.

6.8.7 Regulatory Sandboxes and Controlled Innovation Testing

One of the most important tools in Echelon 3 is the regulatory sandbox. Rather than requiring new technical solutions to be fully compliant before they can be tested, a sandbox allows innovators to try out their ideas in a real environment under regulatory supervision with some flexibility to learn and adapt along the way. This is valuable for both parties. Innovators get the space to identify and fix problems before they go to market. Regulators get to see how these technologies actually behave in practice,

rather than having to rely on technical documents and theoretical projections. The result is better technology and better regulation, each informed by direct experience of the other.

South Africa's Existing Sandbox Framework: The Intergovernmental Fintech Working Group established a regulatory sandbox in 2020, allowing selected firms to test innovative financial products and services with relaxed regulatory requirements for limited time periods. However, the sandbox has faced criticism for limited participation, unclear application criteria, and insufficient post-sandbox pathways to full licensing and market entry.

Echelon 3 should address these limitations by:

Technical Focus: Emphasising technical validation of integration capabilities, not merely regulatory compliance with modified requirements. Sandbox participants should demonstrate functional prototypes with measurable performance metrics.

Collaborative Approach: Following Singapore's Project Ubin model, involving regulatory authorities as active collaborators rather than passive supervisors. This enables real-time problem-solving and regulatory learning.

Clear Graduation Pathways: Establishing explicit criteria and processes for transitioning from sandbox to full licensing and market deployment. This reduces uncertainty and encourages participation.

Knowledge Sharing: Requiring or incentivising sandbox participants to share learnings (potentially with confidentiality protections for commercially sensitive information), enabling broader ecosystem benefit from individual experiments.

International Connectivity: Exploring connections with sandboxes in other jurisdictions, enabling cross-border sandbox testing reflecting blockchain's borderless nature. The Global Financial Innovation Network (GFIN), comprising 80+ financial regulators worldwide, provides infrastructure for such cross-border testing.

6.8.8 Addressing the Digital Divide and Capacity Building

Technical integration's benefits only materialise if market participants possess necessary technical capabilities. South Africa faces significant digital divides, both between individuals (digital literacy, device access, connectivity) and between organisations (technical sophistication of banks vs. fintech startups vs. traditional businesses).

Echelon 3 must therefore incorporate capacity building initiatives:

Technical Training Programs: Developing comprehensive training programs for:

- Regulators requiring understanding of blockchain technology, smart contracts, and distributed systems
- Traditional financial institutions needing to integrate blockchain capabilities
- Fintech startups requiring knowledge of existing payment infrastructure and regulatory requirements
- Consumers and businesses using blockchain-based payment services

These programs might be delivered through partnerships with universities, industry associations, and international organizations with relevant expertise.

Technical Assistance Mechanisms: Establishing support mechanisms helping smaller entities navigate technical integration challenges. This might include:

- Technical advisory services subsidized or provided by regulatory authorities
- Open-source reference implementations of integration protocols and smart contracts
- Developer communities and forums for knowledge sharing
- Grants or low-interest financing for integration investments by smaller CASPs

Digital Infrastructure Development: Even the best-designed blockchain regulatory framework will have limited impact if people cannot get online reliably or affordably. Blockchain adoption depends on basic digital infrastructure such as internet access, mobile devices, and ways of verifying identity digitally. South Africa has made real progress here: more than 90% of the population has a mobile phone, which is a strong starting point. But having a phone is not the same as having reliable, affordable internet

access and in many rural communities, connectivity remains a genuine obstacle. Echelon 3 needs to acknowledge this reality and work alongside South Africa's broader efforts to improve digital infrastructure, rather than assuming the foundations are already in place everywhere.

6.8.9 *Theoretical Foundations of Technical Integration*

It would be a mistake to treat Echelon 3 as purely a technical exercise. Yes, it involves building connections between blockchain systems and traditional payment infrastructure. The harder challenge is making sure those technical solutions actually work within the real world, within institutions that have their own ways of doing things, markets with established practices, and users with particular habits and expectations. Financial infrastructure is deeply embedded in society. It is not just technology, it is the accumulated result of decades of decisions, habits, investments, and expectations. Changing it means changing more than the systems themselves. It means changing the practices, roles, and assumptions built up around those systems. The technical standards that Echelon 3 produces are therefore not neutral specifications, they are decisions about how blockchain will fit into South Africa's financial life, and they will shape behaviour and expectations long after they are written. Actor-network theory offers a useful way of thinking about this through the concept of translation, the process of taking a group of people and institutions that each have their own interests and priorities, and finding a way to align them around a shared purpose. Echelon 3's technical integration requires translation between:

- Banks interested in defending existing market positions and blockchain innovators seeking disruption
- Regulators prioritising stability and oversight with developers valuing permissionless innovation
- Traditional payment systems are optimised for batch processing and blockchain systems are designed for real-time settlement
- National regulatory frameworks and blockchain's global, borderless architecture

Successful technical integration requires not forcing one perspective to dominate but achieving genuine translation where all actors' interests are accommodated in the resulting socio-technical arrangement.

6.9 Echelon 4: Coordination & Collaboration

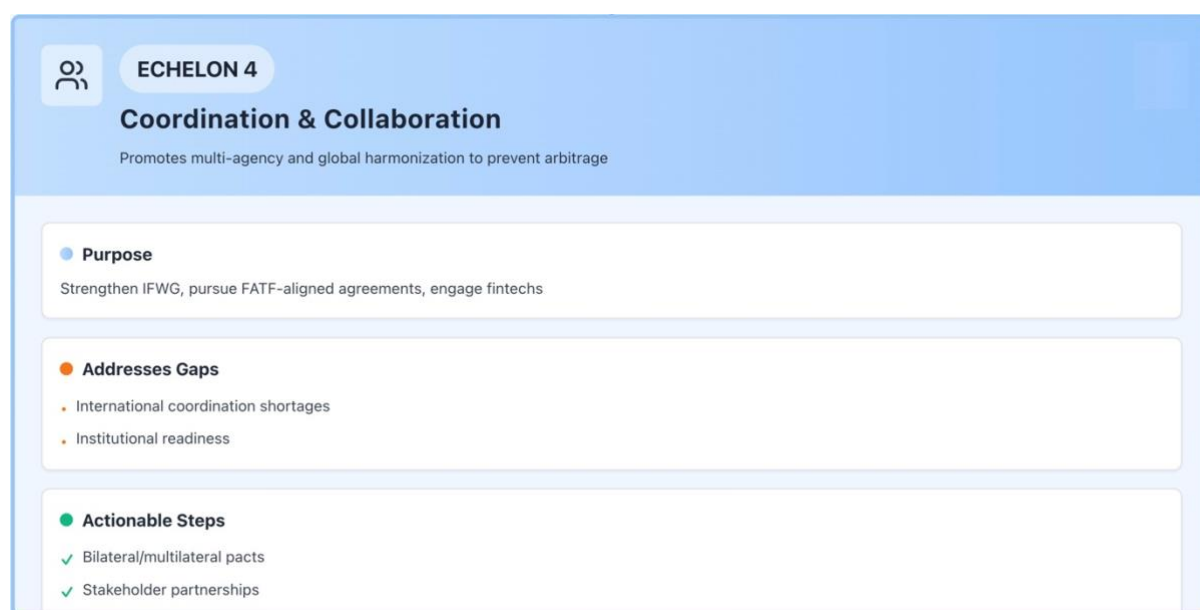


Figure 59. Graphic outlining Echelon 4 (Researcher)

6.9.1 Purpose and Strategic Importance

Echelons 1 to 3 build the domestic foundations: the laws, oversight mechanisms, and technical systems South Africa needs. Echelon 4 looks outward, addressing the fact that these domestic foundations are not enough on their own. Blockchain does not respect national borders, and cryptocurrency regulation that stops at the border will always have gaps that can be exploited. Echelon 4 is therefore about coordination, ensuring South Africa's own regulators work together effectively, and that South Africa engages productively with regulators in other countries to develop consistent standards and share enforcement responsibilities. Three features of blockchain make this coordination particularly important:

Regulatory Arbitrage Risks: The first is regulatory arbitrage. A business operating on a blockchain can be registered in one country, run its servers in another, and serve customers in a third. If the rules differ significantly between jurisdictions, businesses will gravitate toward whichever offers the lightest touch and jurisdictions may feel pressure to lower their standards to attract that business. The solution is coordination: agreeing on minimum standards across jurisdictions so there is no competitive advantage in moving to a less regulated environment.

Network Effects in Standard-Setting: The second is the value of shared standards. Technical standards for how blockchain systems connect, how compliance is automated, how identities are verified are more useful when more people use them. A standard adopted only in South Africa has limited value. The same standard adopted across the region or internationally becomes genuinely powerful. Echelon 4 creates the diplomatic and technical groundwork for this kind of broader adoption.

Shared Learning and Capacity Building: The third is the opportunity to learn from others. No country has fully solved cryptocurrency regulation because it is too new and too complex for that. But some jurisdictions are further along than others, and their experiences, both successes and failures, are enormously valuable. South Africa does not need to learn everything the hard way. Echelon 4 creates structured opportunities to benefit from what others have already discovered.

6.9.2 Gaps Addressed

Echelon 4 directly addresses three critical gaps: international coordination shortages, institutional readiness deficiencies, and jurisdictional complexity challenges.

International Coordination Shortages: A blockchain transaction can cross dozens of national borders in seconds. The international regulatory system was not built for this. It relies on established bodies and bilateral agreements that work well for traditional finance, where transactions are slower, more centralised, and easier to track, but struggle to keep up with the speed and scale of blockchain activity. The FATF has tried to address this by setting global standards for cryptocurrency service providers, including the Travel Rule, which requires companies to share customer information when transferring funds across borders. In principle, this is exactly the kind of coordination that is needed. In practice, the picture is far messier. Some countries have implemented these standards; others have not. Some have introduced their own rules that do not align with anyone else's. Others have banned cryptocurrency altogether. For a business trying to operate legitimately across borders, this inconsistency creates real

compliance headaches. For those trying to move money illicitly, it creates opportunities because there will almost always be a gap somewhere in the global regulatory net.

Institutional Readiness Issues: South Africa has several different regulators, each responsible for a different aspect of cryptocurrency oversight. The SARB looks after payment systems, the FIC handles money laundering concerns, the FSCA regulates how markets are conducted, SARS deals with tax, and National Treasury sets overall policy direction. On paper, the Intergovernmental Fintech Working Group is supposed to bring all of these bodies together. In practice, coordination is still inconsistent. Different regulators sometimes reach different conclusions about the same technology, impose requirements on the same firms that pull in opposite directions, or simply do not communicate with each other as effectively as they should. But coordination is only part of the problem. These regulators were built to oversee banks which usually are institutions with physical offices, established business models, and operating hours. Blockchain does not work like that. It operates globally, continuously, and through technology that many regulators do not yet fully understand. Building the expertise needed to oversee it properly. This happens by hiring people with the right technical backgrounds, training existing staff, and putting in place systems capable of monitoring a market that never closes. This will take time, money, and in some cases a fundamental rethink of how these institutions operate.

Jurisdictional Complexity: When something goes wrong in a traditional financial transaction, it is usually clear which country's laws apply based on where the bank is located, where it is registered, or where the transaction took place. Blockchain removes these familiar reference points. A single transaction can simultaneously involve:

- A user in South Africa
- Using a wallet provided by a service based in Jurisdiction A
- Transacting with someone in Jurisdiction B
- Through a blockchain network operated by validators distributed across Jurisdictions C, D, and E
- With value settlement on a blockchain incorporated as a foundation in Jurisdiction F

Three basic questions arise and currently, none of them has a clear answer. Who has the authority to regulate this transaction? Whose laws govern it? And if something goes wrong, where can the affected party go for legal recourse, and will any judgment actually be enforceable? This uncertainty damages everyone with a legitimate stake in the system. Businesses do not know what rules they are supposed to follow. Regulators do not know whether they have the authority to act. And when things go wrong, there may be no clear path to resolution.

6.9.3 Key Components and Implementation Strategies

Strengthening the Intergovernmental Fintech Working Group (IFWG): South Africa's IFWG, established in 2016 and comprising SARB, National Treasury, FSCA, FIC, the Financial Services Tribunal, and other authorities, provides the foundation for domestic regulatory coordination. Echelon 4 should strengthen IFWG through:

Formalised Coordination Protocols: Moving beyond ad hoc cooperation to structured protocols for information sharing, joint supervisory actions, and coordinated rule-making. This includes establishing clear lead regulator designations for different blockchain activities, avoiding gaps where no authority takes responsibility or overlaps where multiple authorities impose conflicting requirements.

Joint Guidance and Rule-Making: Rather than each authority issuing separate guidance on cryptocurrency regulation, IFWG should issue joint, comprehensive guidance providing market participants with clear, consistent direction across all regulatory dimensions. This follows models from jurisdictions like Singapore, where MAS coordinates across government to provide unified regulatory positions.

Shared Technical Infrastructure: Implementing shared monitoring systems, data analytics platforms, and incident reporting mechanisms accessible to all relevant authorities. This reduces duplication of technical investments while enabling comprehensive oversight.

Regular Stakeholder Engagement: Establishing formal mechanisms for IFWG engagement with blockchain industry, traditional financial institutions, consumer groups, and other stakeholders. This could include regular consultation forums,

advisory committees with industry representation, and public reporting on regulatory developments.

The 2025 implementation of Directive 9 and the High Court ruling on exchange controls demonstrate the criticality of coordination. These developments affect multiple regulatory domains simultaneously, exchange controls (SARB/FinSurv), AML/CFT (FIC), payment systems (SARB/PASA), tax (SARS), and market conduct (FSCA). Without effective IFWG coordination, these authorities might reach inconsistent interpretations or impose conflicting requirements, creating compliance impossibilities.

Pursuing FATF-Compliant International Agreements: South Africa, as a FATF member since 2003, faces obligations to implement FATF Recommendations including those specific to virtual assets. Echelon 4 should pursue international coordination through:

Bilateral Agreements with Key Corridors: Identifying South Africa's most significant cross-border payment corridors (remittance flows to/from Zimbabwe, Mozambique, Nigeria, UK, China, India) and negotiating bilateral agreements with these jurisdictions regarding:

- Mutual recognition of CASP licensing and supervision
- Information sharing for AML/CFT purposes, particularly Travel Rule compliance
- Joint supervisory actions for CASPs operating across both jurisdictions
- Coordination on enforcement against illicit actors

Regional Coordination through SADC: The Southern African Development Community provides existing infrastructure for financial regulatory cooperation. Echelon 4 should promote SADC-wide approaches to cryptocurrency regulation, building on the region's existing monetary coordination through SADC-RTGS. Regional harmonisation would enable efficient cross-border blockchain payments across Southern Africa while preventing regulatory arbitrage among member states.

Engagement with International Standard-Setting Bodies: Active participation in FATF, Basel Committee on Banking Supervision, International Organization of Securities Commissions (IOSCO), and other international bodies where blockchain regulatory standards are being developed. As an emerging market with significant stake in

inclusive financial innovation, South Africa should advocate for standards that enable innovation while ensuring effective oversight, rather than simply adopting standards designed for advanced economies' contexts.

Case Study: Singapore's International Coordination Approach

Singapore provides instructive precedent for international coordination on cryptocurrency regulation through several initiatives:

Bilateral Fintech Cooperation Agreements: MAS has signed over 35 fintech cooperation agreements with financial regulators in other jurisdictions, covering information sharing, referrals of innovative firms, joint innovation projects, and regulatory coordination. These agreements explicitly address blockchain and cryptocurrency regulation, enabling Singapore-based CASPs to benefit from coordinated supervision when expanding internationally.

Project Ubin's Cross-Border Component: Phase 3 of Project Ubin, conducted in partnership with Bank of Canada, explored cross-border payment linkages between blockchain-based payment systems. This demonstrated technical feasibility while identifying regulatory coordination needs. Subsequent work extended to connections with payment systems in multiple jurisdictions, establishing Singapore as a hub for international blockchain payments.

ASEAN Cooperation: Singapore has promoted Association of Southeast Asian Nations (ASEAN) coordination on fintech regulation, including blockchain and cryptocurrency. While ASEAN members exhibit significant regulatory diversity, coordination initiatives have identified common principles and promoted information sharing, reducing fragmentation within the region.

Global Financial Innovation Network (GFIN): MAS actively participates in GFIN, enabling cross-border testing of innovative financial products including blockchain-based solutions. GFIN provides infrastructure for coordinated sandbox testing across multiple jurisdictions simultaneously, reducing barriers for firms seeking to operate internationally.

South Africa should pursue similar initiatives, adapted to African context and focused on key corridors for South African blockchain payments. The African Continental Free Trade Area (AfCFTA) provides potential infrastructure for regulatory coordination, though fintech and payment regulation remain primarily national competencies.

6.9.4 Collaboration with Fintechs and Traditional Institutions

Effective cryptocurrency regulation requires ongoing collaboration between regulatory authorities, blockchain innovators, and traditional financial institutions. Each constituency brings essential perspectives and capabilities:

Blockchain Innovators and Fintechs possess technical expertise, understanding of use cases and user needs, and awareness of technological possibilities and limitations. However, they may lack knowledge of regulatory requirements, compliance processes, and the rationale for existing regulations. Collaboration mechanisms should include:

Regulatory Outreach Programs: Regulators actively engaging with fintech communities through attendance at industry events, hosting of information sessions, and provision of regulatory guidance in accessible formats. The UK Financial Conduct Authority's "regulatory surgeries" where firms can discuss regulatory questions with FCA staff provide a model.

Industry Advisory Committees: Formal committees with fintech and blockchain industry representation providing structured input into regulatory development. These committees should have clear terms of reference, regular meeting schedules, and transparency regarding how their input influences regulatory decisions.

Secondments and Exchanges: Programs enabling blockchain industry experts to work temporarily within regulatory authorities (bringing technical expertise) and regulators to work in industry (gaining practical understanding of operational realities). Singapore's MAS operates such programs, enhancing mutual understanding.

Traditional financial institutions possess existing compliance expertise, relationships with regulatory authorities, and infrastructure connecting to payment systems. However, they may lack blockchain technical expertise and exhibit resistance to innovations

threatening existing business models. Collaboration with traditional institutions should include:

Public-Private Partnership on Integration: Collaborative projects like Project Khokha involving SARB, commercial banks, and technology providers demonstrate effective models. Expanding such partnerships to include blockchain-traditional system integration pilots can accelerate technical integration while building institutional knowledge.

Training and Capacity Building: Programs helping traditional institutions develop blockchain capabilities, potentially subsidized or coordinated by regulatory authorities. This could include executive education, technical training for IT staff, and strategic advisory support for blockchain adoption planning.

Competitive Safeguards: Ensuring that collaboration does not become anti-competitive collusion excluding new entrants. Regulatory authorities should maintain independence, avoid regulatory capture, and ensure that incumbent institutions cannot use their influence to impose barriers against competitors.

6.9.5 Fostering Mindset Shifts from Gatekeeping to Facilitation

A recurring theme in blockchain regulatory challenges is tension between traditional regulatory approaches emphasising control, gatekeeping, and risk avoidance versus approaches emphasising facilitation, innovation support, and managed risk-taking. Echelon 4's coordination and collaboration components should foster mindset shifts among regulators and regulated entities:

From Prohibition to Proportionate Regulation: Rather than defaulting to prohibiting novel, uncertain activities, adopting risk-based approaches that permit innovation with appropriate safeguards. This requires regulatory confidence supported by technical understanding and monitoring capabilities.

From Static Rules to Adaptive Regulation: Recognizing that blockchain technology evolves rapidly, regulatory frameworks must be adaptive, incorporating feedback loops, regular reviews, and mechanisms for rapid updates. Singapore's approach of issuing

guidance that can be quickly revised rather than rigid regulations requiring lengthy amendment processes exemplifies this mindset.

From Unilateral Authority to Shared Stewardship: Acknowledging that effective blockchain oversight requires distributed responsibility, with regulators, industry, and users all playing roles. This contrasts with traditional models assuming regulatory authorities possess complete oversight control.

These mindset shifts are gradual, cultural transformations unlikely to result from mere exhortation. They require:

- Leadership commitment from senior regulatory officials
- Training and development programs embedding new approaches
- Performance metrics and incentives rewarding innovation support alongside risk management
- Structural changes including innovation offices or fintech units within regulatory authorities
- External accountability through public reporting on innovation facilitation efforts

6.9.6 *Addressing Global Standards Misalignment*

While international coordination efforts aim for harmonisation, significant misalignments persist in global cryptocurrency regulation. Different jurisdictions adopt fundamentally incompatible approaches:

Prohibitive Regimes: Some jurisdictions (e.g., China's 2021 ban on cryptocurrency transactions and mining) prohibit blockchain financial activities entirely. While South Africa cannot compel other jurisdictions to permit such activities, it must address implications: South African users may seek to circumvent prohibitions through VPNs or offshore services, and global blockchain networks continue operating despite localised prohibitions.

Permissive Regimes: Other jurisdictions adopt highly permissive approaches, either through deliberate policy (regulatory competitiveness strategies) or simply lack of regulatory development. This creates arbitrage opportunities and safe havens for illicit actors.

Incompatible Technical Standards: Even among jurisdictions adopting regulatory frameworks, technical implementation details may be incompatible. For example, different specifications for Travel Rule compliance or incompatible approaches to digital identity verification.

Echelon 4 should address these misalignments through:

Differentiated Approaches Based on Counterparty Jurisdiction: Applying enhanced scrutiny to transactions involving high-risk jurisdictions (those lacking adequate AML/CFT frameworks or exhibiting significant financial crime) while facilitating transactions with well-regulated jurisdictions. This risk-based approach aligns with FATF guidance while managing practical realities of global standards misalignment.

Advocacy for Harmonisation: Using bilateral relationships, regional forums (SADC, African Union), and international bodies to advocate for regulatory harmonisation. South Africa's perspectives as an emerging market and African leader provide valuable input often underrepresented in standards development dominated by advanced economies.

Unilateral Measures Where Necessary: Where international coordination proves unattainable, implementing unilateral measures protecting South African interests while minimizing negative impacts on legitimate activities. This might include enhanced monitoring of transactions with particular jurisdictions, restrictions on particularly risky activities, or requirements for additional compliance measures.

6.9.7 Case Study: EU MiCA and the Challenges of Unilateral Comprehensive Regulation

The European Union's Markets in Crypto-Assets Regulation represents the most comprehensive unilateral regulatory framework for crypto-assets globally. MiCA establishes EU-wide rules applicable from December 2024, creating regulatory certainty and harmonisation across EU member states' previously fragmented approaches. However, MiCA also illustrates challenges of comprehensive unilateral regulation:

Extraterritorial Implications: MiCA applies to crypto-asset service providers serving EU customers, regardless of provider location. This asserts regulatory jurisdiction based on customer location rather than provider presence, creating compliance obligations for non-EU entities. South African CASPs serving European customers must comply with MiCA requirements, potentially requiring authorisation by an EU member state competent authority. This creates coordination imperatives, South African and EU regulators must cooperate on cross-border supervision, information sharing, and potentially mutual recognition arrangements.

Market Access and Competitive Implications: MiCA's comprehensive requirements may disadvantage non-EU providers unable to meet compliance costs, potentially fragmenting global crypto markets along regulatory boundaries. Conversely, MiCA compliance might become a global standard, with non-EU jurisdictions effectively required to adopt compatible requirements to maintain market access. South Africa must carefully consider whether to pursue MiCA equivalence or compatibility, weighing market access benefits against regulatory autonomy and suitability for local context.

Innovation Impact Debates: MiCA faces criticism from some industry participants for potential over-regulation, particularly regarding stablecoin requirements and authorization burdens that may disadvantage smaller innovators. Others argue MiCA provides necessary consumer protection and market integrity safeguards. South Africa should monitor MiCA's implementation to see whether it successfully balance innovation and protection, or does it drive activity to more permissive jurisdictions?

Coordination Mechanisms: MiCA establishes the European Securities and Markets Authority (ESMA) as coordinator for cross-border supervision of significant crypto-asset issuers and service providers. This centralised coordination addresses fragmentation problems that plagued earlier national-level approaches. South Africa's IFWG could draw lessons from ESMA's coordination role, though adapted to South Africa's unitary rather than federal structure.

6.9.8 Actionable Steps and Implementation Timeline

Long-term Actions

- Negotiate and finalise bilateral fintech cooperation agreements with key corridor jurisdictions (Zimbabwe, Mozambique, Nigeria, UK, China, India)
- Establish SADC working group on blockchain and cryptocurrency regulation, promoting regional harmonisation
- Develop mutual recognition framework for CASP licensing with selected jurisdictions meeting equivalent standards
- Implement cross-border supervisory information sharing systems with partner jurisdictions
- Establish South Africa's participation in international regulatory cooperation networks (GFIN, FATF networks)
- Create public-private sector coordination council for cryptocurrency regulation bringing together IFWG members, industry representatives, consumer groups, and academic experts

Longer-term Actions:

- Evaluate and refine bilateral and multilateral agreements based on implementation experience
- Expand mutual recognition frameworks to additional jurisdictions
- Pursue SADC-wide blockchain payment integration, potentially connecting Project Khokha with other countries' systems
- Develop leadership role in African fintech regulation through African Union or AfCFTA frameworks
- Conduct comprehensive review of international coordination effectiveness, identifying gaps and opportunities
- Establish South Africa as a hub for cross-border blockchain payments in Africa through coordinated regulatory, technical, and market development initiatives

6.9.9 Theoretical Foundations of Coordination and Collaboration

From an institutional theory perspective, Echelon 4 represents response to institutional pressures for isomorphism, the tendency of organisations in similar environments to

become structurally similar. In cryptocurrency regulation, three types of isomorphic pressures operate:

Coercive Isomorphism: FATF requirements, International Monetary Fund conditions, and other external mandates compel adoption of particular regulatory approaches. South Africa's FATF membership creates obligations to implement virtual asset standards, driving regulatory convergence regardless of domestic preferences.

Mimetic Isomorphism: Uncertainty about optimal regulatory approaches encourages imitation of jurisdictions perceived as successful. Singapore's and EU's comprehensive frameworks serve as models others emulate, creating convergence through voluntary adoption of proven approaches.

Normative Isomorphism: Professional networks of regulators, participation in international bodies, and shared educational backgrounds create common understandings of appropriate regulation. Central bankers' attendance at international conferences, participation in Basel Committee work, and similar professional socialization processes foster regulatory convergence.

Echelon 4 strategically navigates these isomorphic pressures, embracing convergence where it serves South African interests (FATF compliance, technical standardization) while maintaining regulatory autonomy where local context demands different approaches (proportionate requirements for emerging market context, emphasis on financial inclusion). Actor-network theory illuminates coordination challenges through concepts of "translation" and "enrolment." Effective international coordination requires translating divergent interests, South Africa prioritising financial inclusion and remittance efficiency, advanced economies emphasizing systemic stability and AML/CFT, into shared objectives around which coalitions can be built. Enrolment involves recruiting allies (other African countries, emerging markets, blockchain industry) to support South Africa's regulatory positions in international forums.

The concept of "regulatory networks" from global governance literature recognizes that contemporary financial regulation increasingly occurs through networks of regulators sharing information, coordinating supervision, and developing soft law, rather than traditional treaty-based international law. Echelon 4 positions South Africa within these

networks, ensuring the country influences rather than merely receives international regulatory standards.

6.10 Echelon 5: Adaptive & User-Centric Mechanisms

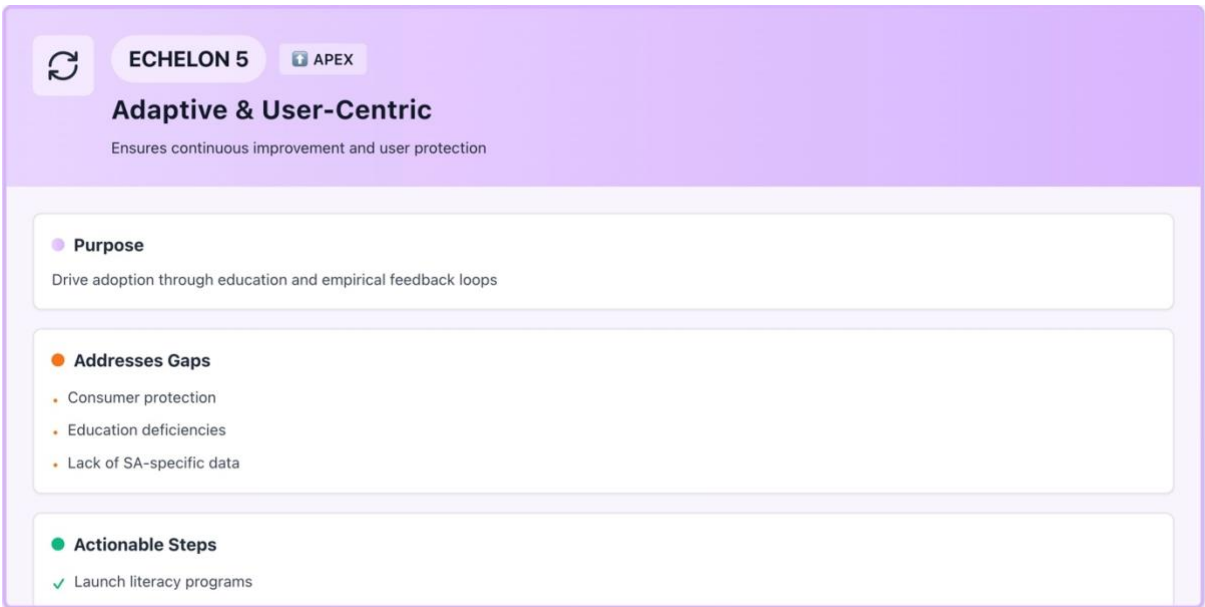


Figure 60. Graphic outlining Echelon 5 (Researcher)

6.10.1 Purpose and Strategic Importance

Echelon 5 represents the apex of the regulatory pyramid, focusing on continuous adaptation, user empowerment, and sustained innovation in cryptocurrency regulation. While Echelons 1-4 establish frameworks, mechanisms, technical systems, and coordination, Echelon 5 ensures these elements remain dynamic, responsive to technological evolution, empirically grounded, and centred on end-user needs and protection. This echelon embodies the principle that effective regulation is never complete but rather constitutes an ongoing process of learning, adaptation, and refinement.

The strategic importance of Echelon 5 stems from blockchain technology's rapid evolution and the fundamental uncertainty characterizing transformative technologies. Regulatory frameworks designed for current blockchain capabilities may become obsolete or inappropriate as technology advances, new use cases emerge, and markets evolve. Static regulation risks two failure modes: becoming irrelevant as innovation outpaces rules, or becoming ossified barriers preventing beneficial

innovation. Echelon 5 addresses these risks through institutionalized mechanisms for continuous learning, evidence-based policy making, stakeholder engagement, and regulatory agility.

Moreover, Echelon 5 recognises that regulatory effectiveness ultimately depends on user adoption, understanding, and protection. The most technically sophisticated and comprehensively coordinated regulatory framework fails if users lack knowledge to engage safely with blockchain systems, if consumer protection mechanisms prove inadequate, or if adoption barriers prevent blockchain's benefits from materializing. User-centricity thus constitutes not merely an ethical imperative but a pragmatic necessity for achieving regulatory objectives.

6.10.2 *Gaps Addressed*

Echelon 5 directly addresses three critical gaps: consumer protection and education deficiencies, empirical evidence scarcity, and market conduct risks in evolving blockchain markets.

Consumer Protection and Education Deficiencies: South Africa's general population exhibits limited understanding of blockchain technology, cryptocurrency, and associated risks. This information asymmetry creates vulnerability to fraud, scams, and poor decision-making. Common risks include:

Investment Scams: Ponzi schemes and fraudulent investment opportunities promising unrealistic returns through cryptocurrency investments. South Africa has experienced several high-profile cryptocurrency scams, including Mirror Trading International (MTI), which collapsed in 2021 after attracting an estimated 280,000 investors and \$1.2 billion in Bitcoin, making it potentially the largest cryptocurrency scam globally at that time.

Technical Vulnerabilities: Users losing access to cryptocurrency holdings through forgotten passwords, phishing attacks, malware, or exchange failures. Unlike traditional banking, blockchain transactions are irreversible and many systems lack customer support or recovery mechanisms.

Volatility Risks: Cryptocurrency price volatility creating unexpected losses for users treating cryptocurrency as stable stores of value or failing to understand speculative nature of crypto investments.

Regulatory Status Confusion: Users uncertain whether cryptocurrency holdings are legally protected, whether gains are taxable, or what recourse exists if service providers fail or engage in misconduct.

Existing consumer protection frameworks in South Africa, including the Consumer Protection Act and financial sector regulations, may not effectively extend to blockchain contexts. The decentralised, pseudonymous, and often cross-border nature of blockchain activities creates jurisdictional and practical enforcement challenges. Furthermore, regulatory authorities have issued warnings about cryptocurrency risks but have not developed comprehensive financial literacy programs specifically addressing blockchain technology.

Empirical Evidence Scarcity: Policy makers and regulators face fundamental knowledge gaps regarding blockchain's actual impacts in South African contexts. Critical questions lacking robust empirical answers include:

- What percentage of the population uses cryptocurrency, and for what purposes?
- How significant are blockchain-based remittances in key corridors (South Africa-Zimbabwe, South Africa-Mozambique)?
- What cost savings do blockchain remittances achieve compared to traditional channels?
- How prevalent are cryptocurrency-related financial crimes (scams, money laundering, terrorist financing)?
- What barriers prevent wider blockchain adoption for legitimate financial inclusion?
- How do different regulatory approaches impact innovation, compliance costs, and market development?
- What risks do stablecoins pose to monetary policy and financial stability in South Africa?

The Intergovernmental Fintech Working Group's 2020 Crypto Assets Regulatory Working Group Position Paper acknowledged these knowledge gaps, recommending

research and data collection. However, systematic, South Africa-specific empirical research remains limited. International studies provide some insights, but blockchain adoption patterns, risk profiles, and regulatory impacts vary significantly across contexts, limiting direct transferability of foreign findings.

Market Conduct Risks: As cryptocurrency markets mature, traditional market conduct risks, including manipulation, insider trading, conflicts of interest, and unfair practices, emerge in blockchain contexts. The pseudonymous nature of blockchain transactions may facilitate manipulation that would be detected in traditional securities markets. Additionally, the concentration of cryptocurrency holdings (a small number of addresses controlling large percentages of many cryptocurrency supplies) creates potential for market manipulation.

South Africa's Financial Sector Conduct Authority regulates market conduct for traditional financial services but faces ambiguity regarding jurisdiction over cryptocurrency markets. The classification of particular crypto-assets as securities, commodities, currencies, or novel asset categories determines applicable regulatory frameworks. The 2025 High Court ruling on exchange controls and ongoing IFWG taxonomy development contribute to clarification, but significant ambiguities persist.

6.10.3 *Key Components and Implementation Strategies*

Comprehensive Financial Literacy and Education Programs: Echelon 5 requires the development and deployment of multi-layered education initiatives targeting different audiences with appropriate content and delivery mechanisms.

Public Awareness Campaigns: Mass media campaigns using television, radio, social media, and print media to reach general populations with basic blockchain and cryptocurrency information. These campaigns should address:

- What blockchain and cryptocurrency are in accessible, non-technical language
- Legitimate use cases versus common scams
- Basic security practices (password management, recognizing phishing)
- Regulatory status and consumer rights
- Where to seek additional information or report fraud

Singapore's approach provides valuable precedent. The Monetary Authority of Singapore has conducted sustained public education campaigns about cryptocurrency risks, including television advertisements, social media content, and educational websites. These campaigns explicitly warn about cryptocurrency speculation risks while acknowledging legitimate uses, striking a balance between protection and not unduly deterring innovation.

School and University Curricula: Integrating blockchain and digital finance content into educational curricula ensures that younger generations develop foundational understanding. This might include:

- Secondary school curricula covering digital financial literacy including cryptocurrency
- University courses on blockchain technology in computer science, finance, and law programs
- Professional education for accountants, lawyers, and financial advisors requiring understanding of cryptocurrency implications for their practices

Targeted Training for Vulnerable Populations: Specific programs addressing populations particularly vulnerable to cryptocurrency scams or particularly likely to benefit from blockchain financial inclusion:

- Elderly populations vulnerable to investment scams
- Migrant workers who could benefit from lower-cost blockchain remittances but may lack technical literacy
- Informal economy participants who might access financial services through blockchain but face barriers
- Rural populations with limited access to traditional banking but increasing mobile connectivity

Industry-Led Education Initiatives: Encouraging or requiring CASPs to provide educational resources to customers. This might include mandatory risk warnings, educational content during account opening, or regular communications about safe practices. The EU's MiCA requires crypto-asset service providers to provide clear information about risks, products, and services, establishing standards South Africa could emulate or exceed.

South Africa-Specific Empirical Research Programs: Addressing knowledge gaps requires systematic research initiatives employing rigorous methodologies to generate reliable evidence for policy-making.

National Cryptocurrency Usage Surveys: Regular (annual or biennial) representative surveys of South African households and businesses measuring:

- Cryptocurrency ownership rates and holdings values
- Purposes of cryptocurrency use (investment, remittances, payments, speculation)
- Sources of cryptocurrency acquisition (exchanges, peer-to-peer, mining, earnings)
- Risk experiences (scams, losses, technical problems)
- Knowledge levels and information sources
- Barriers to adoption or reasons for non-use

These surveys should be conducted by reputable research institutions with appropriate methodological rigor, ensuring representativeness across demographic and geographic dimensions.

Transaction Flow Analysis: Quantitative analysis of blockchain transaction patterns to understand:

- Cross-border payment flows involving South African addresses
- Transaction volumes, values, and patterns over time
- Relationships between cryptocurrency transactions and traditional financial flows
- Concentration and decentralisation of holdings and transactions

This analysis requires blockchain data science capabilities and privacy-preserving methodologies ensuring individual privacy while generating aggregate insights. International precedents include Chainalysis reports on cryptocurrency transaction flows, academic research using blockchain data, and central bank research like the European Central Bank's analyses of cryptocurrency usage.

Stablecoin Impact Studies: Given stable-coin usage in South Africa for hedging and volatility and facilitating payments, specific research should address stable-coin implications:

- Prevalence and volume of stable-coin usage
- Impact on monetary policy transmission mechanisms
- Financial stability risks from stable-coin adoption
- Competition effects on traditional banking
- Regulatory requirements for stable-coin safety and soundness

The International Monetary Fund's research on stablecoins in emerging markets provides methodological frameworks South Africa could adapt. IMF analysis highlights risks including capital flight, dollarization, and reduced monetary policy effectiveness, alongside potential benefits in financial inclusion and payment efficiency.

Regulatory Impact Assessments: Systematic evaluation of regulatory interventions' effects, assessing whether regulations achieve intended objectives, generate unintended consequences, or require adjustment. This includes:

- Compliance cost analysis for regulated entities
- Market development impacts (entry, exit, innovation rates)
- Consumer protection effectiveness
- Financial crime detection and prevention outcomes
- Cross-border competitiveness effects

Singapore's approach includes regular reviews of regulatory frameworks with explicit consideration of impact evidence. The UK Financial Conduct Authority similarly conducts post-implementation reviews assessing whether regulations performed as expected.

Sandbox Outcome Analysis: Systematic evaluation of regulatory sandbox experiences, identifying successful innovations, common failure modes, implementation barriers, and regulatory implications. This evidence should inform decisions about scaling successful innovations and adjusting regulatory frameworks based on sandbox learnings.

Implementation of Feedback Loops and Regulatory Evolution Mechanisms:

Moving beyond static regulation to dynamic, adaptive frameworks requires institutionalised feedback mechanisms.

Regular Regulatory Reviews: Establishing mandatory periodic reviews (e.g., every 2-3 years) of blockchain regulatory frameworks, assessing:

- Whether regulatory objectives are being achieved
- Emerging risks or opportunities not addressed by existing frameworks
- Technological developments requiring regulatory adaptation
- International regulatory evolution and implications for South Africa
- Stakeholder feedback on regulatory effectiveness and burden

These reviews should be transparent, with public consultation and published findings explaining regulatory decisions and changes.

Real-Time Monitoring and Early Warning Systems: Building on Echelon 3's technical monitoring capabilities, Echelon 5 implements analytical frameworks identifying emerging risks or trends requiring regulatory attention:

- Rapid growth in particular crypto-assets or platforms suggesting concentration risks
- Unusual transaction patterns potentially indicating manipulation or financial crime
- Emerging use cases not contemplated in existing regulatory frameworks
- Cross-border developments with potential South African implications

Regulatory Agility Mechanisms: Creating processes enabling rapid regulatory responses to emerging issues without lengthy legislative processes. This might include:

- Empowering regulatory authorities to issue interim guidance or temporary rules
- Fast-track consultation processes for urgent matters
- Modular regulatory frameworks allowing targeted updates
- Sunset provisions requiring regular reauthorization of regulations, forcing periodic review

The Financial Sector Regulation Act provides some flexibility through subordinate regulations and regulatory determinations that can be updated more rapidly than primary legislation. Echelon 5 should maximize use of these mechanisms for cryptocurrency regulation.

Multi-Stakeholder Governance Structures: Establishing permanent forums bringing together regulators, industry, consumers, academics, and civil society for ongoing dialogue on regulatory evolution. These structures should have:

- Clear mandates and decision-making processes
- Regular meeting schedules
- Public transparency regarding deliberations and recommendations
- Diverse representation ensuring all perspectives are heard
- Effective translation of dialogue into regulatory action

6.10.4 Case Studies: Singapore's and EU's User-Centric and Adaptive Approaches

Singapore's Consumer Protection and Education Framework

Singapore's approach to cryptocurrency regulation exemplifies user-centric principles through several mechanisms:

Investor Alerts and Public Warnings: MAS maintains a public register of entities cautioned or prohibited from providing financial services, including cryptocurrency-related services. The authority issues regular investor alerts about cryptocurrency investment risks, specific scams, and unlicensed entities. These communications balance risk warnings with acknowledgment of legitimate uses, avoiding blanket condemnation that might undermine credibility.

Mandatory Risk Warnings: Singapore's Payment Services Act requires digital payment token service providers to display prominent warnings about cryptocurrency risks on their platforms and in advertising. Specific warnings about lack of regulatory protection, volatility risks, and potential for loss must be displayed, ensuring users make informed decisions.

Education Collaboration with Industry: MAS collaborates with licensed payment service providers on consumer education initiatives, encouraging industry to invest in user education while maintaining regulatory independence. This harnesses industry resources and user touchpoints for education while ensuring content meets regulatory standards.

Continuous Regulatory Refinement: Singapore demonstrates adaptive regulation through regular updates to guidance, consultations on emerging issues, and willingness to adjust approaches based on evidence. For example, MAS has progressively refined cryptocurrency advertising restrictions, stable-coin proposals, and licensing requirements based on market evolution and implementation experience.

Academic and Research Engagement: Singapore's regulatory development is informed by academic research, with MAS funding research initiatives, collaborating with universities, and incorporating academic evidence into policy-making. This includes research on cryptocurrency adoption patterns, risk profiles, and regulatory effectiveness.

EU MiCA's Consumer Protection Provisions

The European Union's Markets in Crypto-Assets Regulation incorporates comprehensive consumer protection mechanisms:

Mandatory Disclosures: MiCA requires crypto-asset issuers to prepare and publish detailed white papers containing comprehensive information about the crypto-asset, issuer, rights and obligations, underlying technology, and risks. These white papers must be approved by competent authorities before publication, ensuring completeness and comprehensibility. For asset-referenced tokens and e-money tokens, disclosure requirements are particularly stringent given heightened stability and consumer protection concerns.

Marketing Restrictions: MiCA imposes restrictions on cryptocurrency marketing and advertising, requiring that promotional communications be clearly identifiable as such, fair, clear, and not misleading. This addresses concerns that aggressive, misleading cryptocurrency advertising contributes to uninformed speculation and consumer losses.

Complaint Handling Requirements: Crypto-asset service providers must establish effective and transparent complaint-handling procedures, enabling consumers to submit complaints and receive timely responses. Competent authorities must ensure providers have accessible dispute resolution mechanisms.

Withdrawal Rights: For certain crypto-assets, MiCA establishes withdrawal or cooling-off periods allowing consumers to cancel purchases within specified timeframes, mirroring consumer protection provisions in other financial services contexts.

Ongoing Supervisory Engagement: National competent authorities must actively supervise crypto-asset service providers' conduct, investigating complaints, conducting inspections, and taking enforcement action against unfair practices. This shifts consumer protection from purely private responsibility to public regulatory oversight.

Limitations and Criticisms: Both Singapore's and EU's approaches face criticisms worth considering as South Africa develops Echelon 5:

Paternalism Concerns: Extensive risk warnings and restrictions may be viewed as excessively paternalistic, limiting individual autonomy to make informed risk-taking decisions. Critics argue adults should be free to engage in speculative activities with proper information.

Innovation Dampening: Comprehensive disclosure, registration, and marketing requirements impose costs that may disadvantage smaller innovators unable to afford compliance. This could reduce diversity and competition in cryptocurrency markets.

Effectiveness Questions: Empirical evidence regarding financial literacy programs' effectiveness suggests mixed results, education may increase knowledge without substantially changing behaviour, particularly regarding complex financial products. Risk warnings can become routinised and ignored.

Global Context: Regulations designed for advanced economies with high digital literacy, strong rule of law, and sophisticated financial markets may be inappropriate for emerging market contexts with different characteristics.

South Africa's Echelon 5 should learn from both successes and limitations of international precedents, designing approaches appropriate to local context, capacity, and needs.

6.10.5 *Consumer Protection Mechanisms and Dispute Resolution*

Beyond education, Echelon 5 requires practical mechanisms enabling consumers to seek redress when problems occur and holding service providers accountable for misconduct.

Extending Existing Consumer Protection Frameworks: The Consumer Protection Act and financial sector ombud schemes provide foundations that should be explicitly extended to blockchain contexts:

CASP Accountability: CASPs should be explicitly designated as "service providers" under the Consumer Protection Act, ensuring consumers can invoke protections regarding unfair contract terms, defective services, and deceptive marketing. Regulatory guidance should clarify how Consumer Protection Act provisions apply to blockchain-specific contexts.

Financial Ombud Jurisdiction: The Ombud for Financial Services Providers should have explicit jurisdiction over cryptocurrency-related complaints, enabling consumers to pursue free, accessible dispute resolution. This requires ensuring CASPs are "financial services providers" as defined in relevant legislation and that the Ombud possesses expertise to address blockchain-specific issues.

Compensation Schemes: Consideration should be given to extending deposit insurance or investor protection schemes to cryptocurrency holdings, though this raises complex questions about moral hazard, affordability, and appropriate risk allocation. At minimum, CASPs should be required to maintain professional indemnity insurance or other financial resources ensuring ability to compensate consumers for operational failures or misconduct.

Blockchain-Specific Protection Mechanisms: Some consumer protection challenges in blockchain contexts require novel approaches:

Private Key Recovery: Addressing the problem of users losing cryptocurrency through forgotten passwords or private keys. While blockchain's design makes such losses technically irreversible, CASPs can implement multi-signature wallets, social recovery mechanisms, or custodial services offering recovery processes. Regulation might require CASPs to offer and clearly explain these options.

Transaction Reversal for Fraud: While blockchain transactions are technically irreversible, CASPs can implement internal policies for reversing transactions in cases of demonstrable fraud, similar to chargeback mechanisms in card payments. Regulation might establish standards for when reversals should be considered and processes for investigation.

Smart Contract Insurance: As smart contracts become more prevalent for financial applications, mechanisms for insuring against smart contract failures or exploits become important. This might involve third-party insurance products, CASPs maintaining reserve funds, or mandatory auditing requirements reducing failure risk.

Case Study: The Mirror Trading International Collapse and Regulatory Responses

The collapse of Mirror Trading International (MTI) in 2020-2021 represents South Africa's most significant cryptocurrency-related consumer protection failure, providing critical lessons for Echelon 5 design.

Background: MTI, operating from 2018 to 2020, promised investors returns of 10% monthly through automated Bitcoin trading algorithms. The scheme attracted an estimated 280,000 investors globally (with significant South African participation) and approximately \$1.2 billion in Bitcoin before collapsing when the founder disappeared and withdrawals were suspended.

Regulatory Gaps Exposed: MTI's operation and collapse revealed multiple regulatory deficiencies:

- Lack of clear licensing requirements for cryptocurrency investment schemes enabled MTI to operate without authorisation

- Absence of cryptocurrency-specific marketing restrictions allowed aggressive, misleading promotion
- Limited regulatory capacity for detecting and investigating cryptocurrency schemes permitted extended operation despite warning signs
- Unclear jurisdiction and enforcement authority among multiple regulators (FSCA, FIC, SARS, law enforcement) created coordination failures
- Insufficient consumer awareness about cryptocurrency investment risks contributed to widespread participation

Regulatory Responses: Following MTI's collapse, South African authorities have taken various actions:

- FSCA issued specific warnings about cryptocurrency investment schemes and emphasised that such schemes may constitute financial services requiring licensing
- IFWG accelerated work on comprehensive cryptocurrency regulatory framework
- Law enforcement pursued criminal investigations, though recovery of investor funds faces significant practical barriers
- Increased international cooperation with authorities in jurisdictions where MTI operated or where founders fled

Implications for Echelon 5: MTI's case demonstrates necessity of comprehensive consumer protection mechanisms in Echelon 5:

- **Prevention through Education:** Many MTI investors lacked understanding of cryptocurrency and warning signs of Ponzi schemes. Enhanced financial literacy could prevent similar schemes.
- **Early Detection and Intervention:** Regulatory monitoring capabilities should enable earlier detection of suspicious schemes, allowing intervention before massive consumer losses.
- **Clear Licensing and Enforcement:** Unambiguous licensing requirements and enforcement authority eliminate regulatory gaps that schemes exploit.
- **Effective Redress Mechanisms:** While full recovery may be impossible in fraud cases, consumer protection mechanisms should maximise recovery and provide some recourse.

- **International Coordination:** Cross-border nature of cryptocurrency schemes requires international cooperation for effective enforcement.

6.10.6 *Promoting Financial Inclusion through Blockchain*

A central promise of blockchain technology is enhancing financial inclusion by providing accessible financial services to unbanked and underbanked populations. South Africa, with substantial portions of the population lacking access to traditional banking, stands to benefit significantly if this promise materialises. Echelon 5 should actively promote inclusive blockchain adoption while ensuring appropriate consumer protection.

Barriers to Cryptocurrency Financial Inclusion: Despite potential, several barriers impede blockchain adoption for financial inclusion:

Digital Literacy: Effectively using cryptocurrency wallets and blockchain services requires digital literacy many South Africans lack. User interfaces designed for technically sophisticated users create accessibility barriers.

Device and Connectivity Requirements: Blockchain access requires smartphones or computers and reliable internet connectivity. While South Africa exhibits high mobile phone penetration (over 90%), smartphone ownership is lower (around 60-70%), and connectivity quality and cost remain barriers, particularly in rural areas.

Onboarding Friction: Converting rand to cryptocurrency and vice versa requires interaction with CASPs, often involving KYC processes requiring documentation some populations lack. The very populations most needing financial inclusion may face greatest barriers to blockchain onboarding.

Volatility Risks: Cryptocurrency price volatility creates risks for populations with limited financial buffers. Using Bitcoin for savings or payment exposes users to exchange rate risk that may be unaffordable.

Trust and Awareness: Many unbanked populations lack awareness of blockchain and cryptocurrency, and may distrust unfamiliar technologies, particularly following high-profile scams.

Strategies for Inclusive Blockchain Adoption: Echelon 5 should implement strategies specifically addressing inclusion barriers:

Simplified Onboarding Processes: Regulatory frameworks should permit risk-based KYC, allowing simplified onboarding for low-value accounts or transactions. FATF guidance explicitly permits simplified due diligence in lower-risk scenarios. South Africa could implement tiered KYC where basic identity verification enables access to limited-value accounts, with enhanced verification required for larger holdings or transactions.

Alternative Identity Verification: For populations lacking traditional identity documents, alternative verification mechanisms (biometric registration, community attestation, mobile network operator verification) could enable access. These approaches require careful balancing of financial integrity with inclusion.

Stable-coin Promotion: Encouraging stable-coin usage rather than volatile cryptocurrency reduces exchange rate risk for payment and savings applications. South Africa's regulatory framework should clearly address stablecoins, potentially with preferential treatment for appropriately structured stablecoins serving inclusion objectives.

Public-Private Partnerships: Collaboration between government, telecommunications companies, CASPs, and development organisations can subsidise devices, connectivity, and education for target populations. For example, partnerships might bundle blockchain wallet access with mobile phone contracts, provide subsidised data for financial transactions, or integrate blockchain services with government benefit distribution.

Use Case Development: Actively promoting use cases delivering clear value for target populations, particularly remittances, given South Africa's position in regional labour migration. Demonstrating concrete benefits (lower costs, faster transfers, greater convenience) drives adoption more effectively than abstract technological potential.

Case Study: Crypto Remittances in SADC Region



Traditional Remittance Challenges

- High fees, delays, and cumbersome processes



Cryptocurrency Potential

- Lower costs, faster transfer, mobile convenience

Regulatory Implications



Singapore

Crypto Regulatory Approach

- Legal clarity on exchange controls



South Africa

ECHELON 1

Foundational Policy Architecture

- Legal clarity on exchange controls

ECHELON 2

Operational Frameworks

- Proportionate AML/CFT requirements

ECHELON 5

Adaptive Governance

- User education and protection

Comparative Analysis

Figure 61. Graphic outlining current arena regarding blockchain remittances in the SADC region (Researcher)

Cross-border remittances within the Southern African Development Community represent a particularly promising use case for blockchain financial inclusion. South Africa receives substantial migrant worker populations from Zimbabwe, Mozambique, Lesotho, and other neighbouring countries, with workers sending remittances home to support families.

Traditional Remittance Challenges: Conventional remittance channels (wire transfers, money transfer operators like Western Union) typically charge 5-15% fees for intra-African transfers, among the world's highest remittance costs. Additionally, transfers may take days, require physical presence at agent locations, and involve cumbersome documentation.

Blockchain Potential: Cryptocurrency-based remittances promise significantly lower costs (potentially 1-3% or less), near-instantaneous transfer, and greater convenience through mobile interfaces. Several blockchain remittance startups operate in African corridors, demonstrating technical feasibility.

Regulatory Implications: Realising blockchain remittance potential requires coordinated regulatory action across Echelons:

Echelon 1: Legal clarity that blockchain remittances are permissible under exchange control frameworks (addressed by 2025 High Court ruling but requiring broader implementation)

Echelon 2: Proportionate AML/CFT requirements not imposing prohibitive compliance costs on lower-value remittances

Echelon 3: Technical integration enabling conversion between cryptocurrency and local currencies at both sending and receiving ends

Echelon 4: Bilateral regulatory coordination between South Africa and key receiving countries ensuring consistent treatment

Echelon 5: User education about how to safely use blockchain remittances, consumer protection if service providers fail, and empirical monitoring of adoption and impacts

Preliminary Evidence: While comprehensive data remains limited, available evidence suggests growing blockchain remittance usage in certain corridors. For example, Bitcoin peer-to-peer trading volumes on platforms like Local Bitcoins and Paxful have shown significant growth in countries like Zimbabwe and Nigeria, potentially reflecting remittance usage. However, distinguishing remittance usage from speculation or capital flight remains challenging without better data.

Echelon 5's research agenda should include specific studies of blockchain remittance adoption, barriers, user experiences, and impacts on households and financial inclusion. This evidence should inform regulatory refinements maximizing inclusion benefits while managing risks.

6.10.7 *Actionable Steps and Implementation Timeline*

Long-term Actions:

- Develop and launch national cryptocurrency literacy campaign with multi-media components targeting general public
- Integrate digital financial literacy including blockchain and cryptocurrency into school curricula at appropriate levels
- Establish research partnerships with universities and research institutions for empirical studies on cryptocurrency usage, impacts, and regulation
- Conduct first national cryptocurrency usage survey establishing baseline data on adoption, use cases, and barriers
- Implement enhanced consumer protection frameworks explicitly addressing cryptocurrency contexts
- Establish cryptocurrency consumer complaint mechanisms through financial sector ombud scheme
- Launch targeted financial inclusion initiatives promoting blockchain remittances in key corridors
- Develop monitoring systems tracking financial inclusion impacts of blockchain adoption

Longer-term Actions:

- Conduct regular (biennial) follow-up cryptocurrency usage surveys tracking adoption trends and regulatory impacts
- Implement comprehensive stable-coin research program assessing monetary policy and financial stability implications
- Establish permanent multi-stakeholder forum for ongoing blockchain regulatory dialogue and evolution
- Conduct systematic evaluation of consumer protection effectiveness, identifying gaps and refinements needed

- Develop advanced financial literacy programs building on basic cryptocurrency awareness
- Implement formal regulatory impact assessment process for all significant blockchain regulatory interventions
- Create public research repository making South Africa-specific cryptocurrency research accessible to policymakers, researchers, and public
- Establish South Africa as African leader in evidence-based, inclusive cryptocurrency regulation through research dissemination and capacity building support for other African countries

6.10.8 *Reducing Information Asymmetry and Adoption Barriers*

Beyond education and research, Echelon 5 should address structural information asymmetries and adoption barriers through market structure improvements and transparency initiatives.

Mandatory Transparency and Disclosure: Building on MiCA's white paper requirements, South Africa should mandate comprehensive disclosure by CASPs and crypto-asset issuers:

Service Provider Disclosures: CASPs must clearly disclose fee structures (all fees, not merely headline rates), security measures and insurance coverage, custody arrangements and bankruptcy protections, customer support capabilities and response times, regulatory status and licensing information, and material conflicts of interest.

Crypto-Asset Disclosures: Issuers of new crypto-assets marketed in South Africa must provide detailed information about technology protocols, consensus mechanisms, tokenomics (supply, distribution, inflation), governance structures, development team and funding, use cases and value proposition, and comprehensive risk factors.

These disclosures should be standardized in format, enabling comparison across providers and products. Regulatory authorities should provide templates and review processes ensuring quality and completeness.

Price and Market Information: Cryptocurrency markets exhibit significant price fragmentation across exchanges and geographic regions, with information asymmetries

enabling arbitrage and disadvantaging less informed users. Echelon 5 should promote market transparency through:

Price Reporting Requirements: Requiring CASPs to report transaction prices to regulatory authorities or authorised data aggregators, enabling consolidated price discovery and market surveillance.

Best Execution Obligations: Imposing obligations on CASPs to execute customer orders at best available prices, similar to best execution requirements in securities markets. This protects consumers from overpaying due to information disadvantages.

Market Surveillance: Regulatory authorities using transaction data to detect and investigate market manipulation, insider trading, and other unfair practices. This requires sophisticated analytical capabilities but leverages blockchain transparency.

Simplified Comparison Tools: Given cryptocurrency complexity, users benefit from tools simplifying comparisons and decision-making:

Regulatory Scorecards: Public scorecards showing CASPs' regulatory compliance status, licensing, enforcement actions, and customer complaints. This enables users to quickly assess provider legitimacy and track record.

Fee Calculators: Simple tools allowing users to input transaction parameters and compare total costs across different providers and methods (blockchain vs. traditional remittances, different cryptocurrency routes, etc.).

Risk Ratings: Independent, standardised risk ratings for crypto-assets, similar to credit ratings for debt securities. While not eliminating risk, ratings provide accessible risk information for users lacking expertise for independent assessment.

6.10.9 *Long-term Sustainability and Regulatory Evolution*

Echelon 5's user-centric and adaptive mechanisms must be sustainably embedded in South African regulatory architecture, not merely temporary initiatives.

6.11 Summary: Toward a Balanced, Adaptive, and Inclusive Cryptocurrency Regulatory Paradigm

6.11.1 *Synthesis of the 5-Echelon Knowledge Model*

This study set out to answer a complex question: how should South Africa regulate blockchain technology in the context of cross-border money transfers? The answer it proposes is a structured five-layer model, built using a research methodology developed by vom Brocke et al. (2024) that is specifically designed for tackling problems too complex to solve all at once. Each layer addresses a different aspect of the regulatory challenge, and each builds on the work of the layers before it. Starting with the legal foundations that everything else depends on, and working through to more flexible, people-centred mechanisms. The value of this structure is practical: rather than asking regulators to do everything simultaneously, it gives them a logical, manageable sequence to follow.

Echelon 1: Foundational Policy & Legislative Clarity: Echelon 1 lays the legal groundwork that everything else is built on. The starting point is an uncomfortable reality: some of South Africa's most important financial laws are decades old.

The Currency and Exchanges Act was written in 1933 and were never designed with blockchain or digital assets in mind. Before anything else can work, these laws need to be updated. The 2025 High Court ruling that exempted certain cryptocurrencies from exchange controls was a significant moment, and Echelon 1 takes that further through targeted legislative changes.

These changes would establish clear definitions for crypto-assets, resolving the current confusion about what they are and how they should be treated. Legal standing would need to be given to governance models that combine traditional oversight with the decentralised features of blockchain, and create sensible, proportionate rules that allow legitimate innovation without abandoning necessary controls. The cost of not doing this is clear from South Africa's own recent history. The legal vacuum that existed around cryptocurrency allowed schemes like Mirror Trading International to operate without meaningful oversight, ultimately defrauding thousands of people. Legal clarity is not a bureaucratic nicety. It is the foundation without which no other part of the regulatory framework can function.

Echelon 2: Oversight & Compliance Mechanisms: Echelon 1 establishes the legal framework. Echelon 2 makes it work in practice. This means developing the specific tools and mechanisms needed to monitor and enforce the rules in a blockchain environment, which is fundamentally different from the centralised, intermediary-based systems that existing oversight tools were built for. Two concrete steps give Echelon 2 its structure. First, the Travel Rule, an international standard requiring crypto platforms to share customer information when transferring funds, is formally incorporated into South African law through Directive 9. Second, the Financial Intelligence Centre Act is extended to explicitly include crypto-asset service providers, closing a gap that has allowed some platforms to operate outside the anti-money laundering framework entirely.

Rather than applying the same compliance requirements to every transaction regardless of risk, Echelon 2 concentrates its oversight where the risk of money laundering or terrorist financing is actually highest, reducing the burden on low-risk activity without weakening protection where it matters most. The most significant shift, however, is in how oversight itself is conceived. Instead of relying on periodic reports and after-the-fact investigations, Echelon 2 uses blockchain's own permanent, transparent record as a live monitoring tool. This enables it to embed compliance checks directly into smart contracts so that rules are enforced automatically, at the moment a transaction occurs, rather than reviewed after the fact.

Echelon 3: Technical & Operational Integration: At the moment, blockchain largely operates alongside South Africa's financial system rather than within it. Echelon 3 changes this by building the connections needed to make blockchain a genuine part of how payments work in South Africa. This is not as a separate experiment, but an integrated component of the national infrastructure. The South African Reserve Bank's Project Khokha proved this was technically possible for large interbank transactions. Echelon 3 extends that work to everyday payments, cross-border money transfers, and connections between different blockchain platforms. Common technical standards make it possible for blockchain systems and traditional banking systems to talk to each other reliably. Compliance processes that currently require manual intervention, such as checking identities, withholding tax, screening against sanctions lists, are automated through smart contracts, so they happen instantly and consistently every time a transaction occurs. The practical payoff for ordinary people is significant. South Africa

has a large population of migrant workers who send money home regularly. Better technical integration could reduce the cost of those transfers by 40 to 60 percent. But this can only happen if the infrastructure to support it is built properly. Echelon 3 is how that infrastructure gets built.

Echelon 4: Coordination & Collaboration: Blockchain transactions cross borders constantly, and regulation that stops at the South African border will always have gaps. Echelon 4 is about closing those gaps, both by improving coordination within South Africa and by building stronger relationships with other countries. Inside South Africa, the Intergovernmental Fintech Working Group, which brings together the SARB, FIC, FSCA, SARS, and other regulators, needs to be strengthened so that these bodies speak with one voice rather than issuing contradictory guidance.

Outside South Africa, formal agreements with key remittance partners such as Zimbabwe, Mozambique, Nigeria, and others, would allow regulators to share information, recognise each other's licences, and work together to catch bad actors who currently exploit the gaps between different regulatory systems. At a regional level, working through SADC to align standards across Southern Africa would remove the incentive for businesses to simply relocate to whichever country has the loosest rules. And engaging seriously with international bodies like the FATF would not only keep South Africa compliant with global standards, it would give South Africa, and Africa more broadly, a seat at the table where those standards are decided, rather than simply receiving rules shaped by wealthier economies and asked to implement them.

Echelon 5: Adaptive & User-Centric Mechanisms: The first four echelons built the regulatory framework. Echelon 5 makes sure it does not become outdated the moment it is finished. It does this in three ways. First, it invests in helping people understand cryptocurrency. What it is, how it works, and what the risks are. This matters because uninformed users are easy targets. The Mirror Trading International case is a sobering reminder of this: around 280,000 people lost a combined \$1.2 billion in Bitcoin to a scheme that many did not fully understand. Better financial literacy would not prevent every fraud, but it significantly reduces the pool of potential victims. Second, Echelon 5 fills the evidence gaps that currently make it difficult to design good policy. South Africa needs its own research, particularly into how people are actually using cryptocurrency,

what impact stablecoins are having on the rand, and whether the regulatory measures being introduced are working.

Policy built on evidence from other countries, or on no evidence at all, will always be imperfect. Third, Echelon 5 builds in the ability to adapt. Technology does not stand still, and neither should regulation. Regular reviews, real-time monitoring, forums that give all stakeholders a voice, and clear processes for updating rules when needed. These are the mechanisms that prevent a framework designed for today from becoming a hindrance tomorrow.

6.12 Theoretical Contributions and Scholarly Significance

This knowledge model makes several substantive theoretical contributions advancing scholarly understanding of financial technology regulation, socio-technical system governance, and innovation policy in emerging market contexts.

Integration of Multiple Theoretical Lenses: The model does not rely on a single theory. Instead, it draws on four complementary frameworks: socio-technical systems theory, institutional theory, innovation diffusion theory, and actor-network theory. Each of these highlights a different aspect of the regulatory challenge. Most existing regulatory scholarship takes one of two approaches. It either treats regulation as primarily a technical problem, or primarily an institutional and social one. This model treats it as both simultaneously, recognising that blockchain systems involve technology, social norms, legal structures, and human behaviour all evolving together. Each theory pulls its weight. Socio-technical systems theory explains why technical and social elements must be developed in tandem. Getting the technology right without getting the institutions right, or vice versa, will not produce effective regulation. Institutional theory explains the pressures that shape how regulators behave, the obligation to meet international standards, the tendency to follow what successful countries like Singapore have done, and the influence of shared professional norms. Innovation diffusion theory helps explain why people adopt new technologies or resist them, which directly informs the design of Echelon 5. Actor-network theory frames regulation as the challenge of bringing together people, institutions, and technologies such as smart contracts, protocols, monitoring tools, into relationships stable enough to function reliably.

Different echelons draw on different theories as the focus shifts. Echelon 1 leans most heavily on institutional theory, Echelon 3 on socio-technical thinking, Echelon 5 on innovation diffusion, but the eDSR framework provides a consistent methodology that keeps the whole model coherent. The findings of this study, and the model proposed in response to them, make most sense when read through the three regulatory theories that Chapter 2 established as the study's analytical foundation. Public interest theory explains what is at stake. South Africa's current regulatory gap is not a technical inconvenience. It is a public harm. It allowed Mirror Trading International to operate unchecked. It keeps remittance fees at 8–11% when blockchain could reduce them to under 3%. It leaves 11% of South African adults outside the financial system without a clear pathway in. Every design choice in the 5-Echelon model, from Echelon 1's legislative clarity mandate to Echelon 5's financial literacy investment, is anchored in the public interest obligation to address those harms.

Capture theory explains who the model is pushing back against. The regulatory asymmetries that the interviewed respondents (2024) described: incumbent banks resistant to disruption, compliance frameworks that happen to favour established players, exchange controls that create barriers for CASP entrants, are not accidents. They are the predictable product of a regulatory design process that Stigler (1971) mapped: organised interests shaping rules in their favour while diffuse consumer interests go underrepresented. Echelons 2 and 4 are built to counteract this. It is an activity-based compliance structure that treats equivalent financial functions equivalently, and a coordination architecture that closes the jurisdictional gaps that concentrated interests exploit.

Responsive regulation explains how the model expects regulation to behave once it is in place. The respondents who called for sandboxes, risk-based frameworks, and proportionate enforcement were describing, in practical terms, what Ayres and Braithwaite (1992) theorised: regulation that starts from facilitation, escalates only when necessary, and learns continuously from what it observes. That is what Echelons 3 and 5 are designed to deliver. Not a fixed rulebook, but a regulatory posture capable of adapting as the technology, the market, and South Africa's own institutional capacity continue to develop.

Extension of Design Science Research Methodology: One of this study's contributions is showing that the eDSR methodology developed by vom Brocke et al. (2024) can be applied effectively to regulatory design. This is not just to information systems, which is where it was originally developed. DSR has been used in blockchain governance before, but rarely as comprehensively as here. The five-layer structure is central to why this works: by breaking a highly complex regulatory challenge into distinct, manageable layers. Each with clear connections to the others, with the methodology that makes it possible to develop, test, and refine each component separately before bringing the whole framework together.

This is a real methodological advance, because regulatory scholarship has traditionally been more comfortable describing and analysing existing frameworks than designing new ones. By demonstrating that the rigorous, iterative approach of DSR can be applied to regulation, this study creates a template that future researchers could use to tackle other emerging challenges in financial technology. These would include AI in financial services to decentralised finance and central bank digital currencies.

Conceptualisation of Hybrid Governance Models: Most thinking about governance assumes a simple choice: either control is centralised, that is, held by a single authority, or it is decentralised, spread across many. Blockchain does not fit neatly into either category, and this creates a theoretical problem that the 5-Echelon model helps to solve. Blockchain's technology is deliberately decentralised. No single institution controls it. But it still needs to operate within legal and regulatory systems that are, by their nature, centralised. Rather than trying to force blockchain into one category or the other, the model treats this combination as something new. A hybrid form of governance where centralised and decentralised elements genuinely coexist rather than one compromising the other. Each echelon handles a different aspect of this: Echelon 1 gives legal recognition to decentralised structures while keeping them accountable to a central regulatory framework; Echelon 2 distributes compliance responsibilities while preserving central oversight; Echelon 3 connects decentralised technology to centralised infrastructure; and Echelon 4 manages the tension between national regulatory authority and a technology that ignores borders.

This way of thinking is not only relevant to blockchain. The same challenge, making centralised and decentralised governance work together, arises in platform economies,

federated data systems, and distributed manufacturing, and the conceptual framework developed here offers insights applicable to all of them.

Emerging Market Regulatory Theory: The academic literature on cryptocurrency regulation has a significant blind spot: it is overwhelmingly focused on wealthy countries. The United States, the EU, the UK, Singapore, and Switzerland dominate the scholarship, despite the fact that cryptocurrency is widely used in emerging markets and the challenges these countries face are very different from those of advanced economies. This model is a deliberate attempt to address that imbalance by building a framework rooted in South Africa's actual context rather than imported from elsewhere.

What makes emerging markets different? Several things. Financial inclusion is not a nice-to-have. It is one of the primary reasons cryptocurrency matters in these contexts, and regulation needs to reflect that rather than treating it as an afterthought. Regulatory institutions often have limited capacity and cannot do everything at once. This means reform has to be carefully sequenced and may require outside technical support. International development partnerships offer sources of funding and expertise that wealthy countries do not need to consider.

Regional bodies like SADC provide coordination mechanisms that are essential when neighbouring countries face the same challenges and risk undermining each other's efforts through inconsistency. And large informal economies create regulatory opportunities and complications that simply do not appear in frameworks designed for countries where almost everyone already has a bank account. A lot of regulatory theory assumes its conclusions apply everywhere. This thought process is that if you identify the right general principles, they will work regardless of context. There is some value in this kind of thinking, but it also carries a real risk. Producing recommendations that work well in New York or Brussels but are poorly suited to Johannesburg or Lusaka. This model takes a different approach, it is specific to South Africa, but it is designed in a way that other emerging markets facing similar challenges can learn from and adapt.

6.13 Practical Contributions and Policy Implications

Therefore, beyond theoretical significance, the knowledge model generates substantial practical contributions directly applicable to South African regulatory development and offering lessons for other jurisdictions.

Actionable Implementation Roadmap: A common criticism of regulatory research is that it is good at identifying problems and pointing in the right direction, but weak on the practical detail needed to get there. This model is designed to be different. It does not just describe what South Africa's cryptocurrency regulatory framework should look like, it also sets out, step by step, how to build it. The implementation plan is organised across four timeframes: the first six months, the first year, the first three years, and a longer horizon of up to five years.

Each step identifies who is responsible, what needs to already be in place before it can begin, what it should produce, and how you would know it had been done successfully. To concretise this: in the first six months alone, Echelon 1 calls for the creation of a dedicated legislative reform task force, a thorough review of existing laws that need updating, the drafting of initial amendments, the development of clear legal definitions for crypto-assets, and publication of those drafts for public comment. These are not vague aspirations. They are specific, actionable tasks that South African authorities could begin working on straight away. That is what sets this model apart from most regulatory scholarship. It bridges the gap between analysis and action.

Comprehensive Regulatory Coverage: The Gap Analysis identified eight distinct areas that a comprehensive cryptocurrency regulatory framework needs to cover: cross-border transfers, exchange controls, payment systems, anti-money laundering, crypto-asset classification, market conduct, financial stability, and taxation. The 5-Echelon model addresses all eight, and the fact that it does so in an integrated way matters more than it might initially appear. South Africa's regulatory history provides a clear illustration of what goes wrong when these areas are handled separately. Different authorities have historically addressed different pieces of the puzzle without sufficient coordination, producing a fragmented landscape with gaps in some places and conflicting requirements in others.

The IFWG has made progress, but the problem persists. The model's integrated structure prevents this kind of fragmentation. Consider what happens when someone sends money across a border using cryptocurrency. That single transaction simultaneously involves exchange control rules, anti-money laundering requirements, payment system regulations, coordination with the receiving country's regulators, and consumer protection obligations. If each of these is regulated by a different authority

without a shared framework connecting them, the rules can end up pulling in different directions, creating compliance requirements that simply cannot all be met at the same time. The 5-Echelon model is designed to prevent exactly this, by ensuring that all eight dimensions are addressed together rather than in isolation.

International Best Practice Integration: One of the model's practical advantages is that it does not ask South Africa to figure everything out on its own. Other countries have already been through significant parts of this process, some successfully, others less so. Their experiences offer genuinely valuable lessons. Singapore shows what is possible when regulators take an actively supportive approach to innovation: its sandbox programmes, its technical work through Project Ubin, its balanced approach to consumer protection, and its emergence as a regional fintech hub all offer things worth learning from.

The EU's MiCA shows the benefits of a comprehensive, well-coordinated framework, but also the risks of making rules so detailed and demanding that smaller firms cannot afford to comply. FATF standards are not optional. They set the baseline for anti-money laundering compliance that any country needs to meet to participate in the global financial system. But, they need to be applied thoughtfully to work effectively in a blockchain context. By taking the best of what each of these examples offers and adapting it to South Africa's own circumstances, the model gives South Africa a genuine opportunity to move quickly and intelligently, potentially skipping the trial-and-error phase that other jurisdictions had to go through, and arriving at a sophisticated regulatory framework sooner than might otherwise be possible.

Stakeholder Engagement Framework: No single organisation can regulate cryptocurrency effectively on its own, and the 5-Echelon model is built around this reality. It identifies all the key players: the SARB, FIC, FSCA, National Treasury, SARS, cryptocurrency platforms, traditional banks, consumers, civil society groups, researchers, and international partners, and sets out clearly what each is responsible for and how they should work together.

Each echelon specifies which stakeholders are relevant at that stage and how they should be involved, whether through public consultation, advisory committees, sandbox participation, or research collaboration. Each group in this picture brings something

essential. Regulators have the authority to set and enforce rules, but they cannot do this well without cooperation from industry, engagement from consumers, and evidence from researchers. Cryptocurrency platforms have the technical knowledge that regulators often lack, but they need clear rules and public trust to build viable businesses.

Consumers need to be protected from harm, but they also deserve access to the genuine benefits that blockchain can offer, and shutting those benefits out in the name of protection is its own kind of failure. Civil society organisations hold the system accountable and make sure public interests are not overlooked. International partners make it possible to coordinate across borders. This model creates a structure in which all of these groups have a meaningful role. Governance arrangements are designed to ensure that no single interest, whether commercial, regulatory, or political, is able to dominate at the expense of the rest.

6.14 Positioning South Africa as Cryptocurrency Regulatory Leader in Africa and Globally

Effective implementation of this 5-Echelon knowledge model positions South Africa to assert leadership in cryptocurrency regulation within Africa and achieve recognition as a sophisticated regulator globally. Several factors support this leadership potential and should be strategically cultivated.

Existing Institutional and Technical Capabilities: South Africa has a significant head start compared to most other African countries. Its financial regulatory institutions such as the SARB, FSCA, and FIC are well-resourced, technically capable, and respected internationally. The SARB has already shown it can engage seriously with blockchain technology: Project Khokha successfully tested whether blockchain could be used for settlements between banks, proving that transactions could be kept private using cryptography and completed with certainty. The Johannesburg Stock Exchange, the largest in Africa, brings further institutional strength and sophisticated market infrastructure. All of this means South Africa is not starting from a blank page. The task is not to build a regulatory system from scratch. It is to take what already exists and extend it to cover a new and fast-moving technology.

Strategic Regional Position: South Africa's financial system is the most developed in sub-Saharan Africa, and this gives it an influence that extends well beyond its own borders. Other African countries regularly look to South Africa when designing their own financial regulations, and many turn to it for technical guidance and support. This means that the decisions South Africa makes about cryptocurrency regulation will not only affect South Africans. We will shape how the broader region approaches the issue.

There is a significant opportunity here. By moving decisively and thoughtfully on cryptocurrency regulation, South Africa could establish Johannesburg as Africa's leading fintech hub and the continent's equivalent of Singapore in Southeast Asia or Dubai in the Middle East. The SADC framework makes regional leadership practical. Southern Africa already has substantial cross-border financial flows. Workers based in South Africa send significant sums home to neighbouring countries, and there are considerable trade and investment flows across the region. If SADC countries align their cryptocurrency regulations, blockchain-based payment networks could serve this entire region far more efficiently than the current fragmented system allows. South Africa is best placed to drive this alignment, and in doing so, it would not only benefit its neighbours but ensure that its own regulatory approach becomes the standard the region builds around.

Development Imperatives Creating Implementation Urgency: The case for getting cryptocurrency regulation right in South Africa is not just technical. It is deeply practical and human. Around one in ten South African adults still has no access to formal financial services. Blockchain-based services, accessible through a mobile phone, could change this. Sending money between African countries costs between 8 and 10 cents for every rand transferred on average. This is a significant burden for migrant workers and their families, and one that blockchain could dramatically reduce. With more than 60% of young South Africans out of work, the prospect of a growing fintech sector creating jobs is not a trivial benefit. And in a country where corruption and illicit financial flows cause real and lasting damage, blockchain's transparency offers tools for greater accountability that other systems cannot match. Each of these is an urgent problem with real consequences for real people. That urgency matters, and it could create the political will to push through the kind of regulatory reform that, in other contexts, can easily be delayed or diluted. South Africa's challenges are serious, but they are also a source of momentum.

International Engagement Infrastructure: South Africa has a seat at the table in some of the world's most influential regulatory forums, such as the FATF, the G20, BRICS, and several multilateral development institutions. This matters because the global standards that govern blockchain regulation have largely been written by wealthy countries, for wealthy countries. South Africa has the credibility, the technical capability, and the lived experience of a developing economy to push back on this and to make the case that global standards need to work for countries where financial inclusion is a pressing priority, where regulatory capacity is more limited, and where the stakes of getting this right are particularly high.

Beyond the global stage, the African Continental Free Trade Area opens up a more specific and exciting opportunity. AfCFTA is designed to make trade across Africa easier. Trade, however, requires payment, and cross-border payments in Africa are currently slow, expensive, and fragmented. Blockchain could change this. South Africa could lead the effort to build continent-wide blockchain payment infrastructure under the AfCFTA framework, making the case that seamless digital payments are not just a financial convenience but a foundation for the broader economic integration AfCFTA is trying to achieve. No other African country is better positioned to drive this vision forward.

Balanced Approach Attracting International Recognition: The 5-Echelon model rests on a straightforward but important idea: that good regulation does not have to choose between supporting innovation and protecting people. It can do both, and the international regulatory community is increasingly coming to the same conclusion. Countries that respond to cryptocurrency by banning it or hedging it in with prohibitive rules tend to find that innovation simply moves elsewhere, while their own citizens miss out on the benefits.

Countries that take the opposite approach, such as allowing cryptocurrency to operate with minimal oversight, tend to find that consumers get hurt and that criminal actors take advantage of the gaps. South Africa's model charts a more considered path. It delivers clear rules that give innovators certainty, meaningful protections for consumers, and accountability mechanisms that work with blockchain's decentralised nature rather than against it. Getting this right would not only benefit South Africans, but it would establish South Africa as an example that other emerging markets can learn from, and as a

country that has demonstrated sophisticated regulatory thinking on one of the most complex challenges in modern finance.

6.15 Critical Success Factors and Implementation Challenges

Realising the knowledge model's potential requires addressing critical success factors and navigating implementation challenges that could undermine effectiveness.

Sustained Political Commitment: Reforming blockchain regulation is not a short-term project. It will take years, and progress will need to survive changes in government. South Africa's political landscape makes this a genuine concern. The coalition arrangements that emerged from the 2024 elections and the broader debates about economic direction create real uncertainty about whether regulatory reform will remain a priority as political circumstances shift. Keeping the reform process on track through these transitions will require:

- Broad political consensus across major parties that cryptocurrency regulation merits priority attention
- Institutional arrangements (IFWG, dedicated units within regulatory authorities) with sufficient autonomy to continue implementation despite political changes
- Concrete, visible early successes demonstrating benefits and building constituency support for continued reform
- Civil society and industry advocacy sustaining pressure for continued progress

Resource Mobilisation and Allocation: Effective implementation requires substantial resources, financial, human, and technical, sustained over extended timeframes. South Africa faces competing demands for limited fiscal resources, with immediate priorities including service delivery, infrastructure development, and social spending potentially crowding out blockchain regulatory investment. Resource mobilisation strategies include:

- Demonstrating regulatory investment's economic returns through job creation, fintech sector development, remittance cost savings, and financial inclusion
- Leveraging regulatory fees from CASPs to partially fund supervisory infrastructure

- Securing international development funding from multilateral institutions for technical assistance and capacity building
- Phasing implementation to spread costs over time rather than requiring large upfront investments
- Pursuing public-private partnerships where appropriate for technical infrastructure development

Capacity Development and Retention: The model's technical sophistication requires substantial expertise in blockchain technology, cryptography, data science, and related fields within regulatory authorities. South Africa faces skills shortages in these domains and brain drain as talented professionals emigrate seeking opportunities elsewhere. Capacity development strategies include:

- Competitive compensation and career development opportunities retaining specialised talent within public sector
- Partnerships with universities for training programs and potentially secondments of academics into regulatory roles
- International exchanges and technical assistance bringing global expertise
- Contract arrangements with specialised consultants and technology firms supplement internal capacity
- Long-term investment in education pipeline through university programs and scholarships is developing future regulatory workforce

Stakeholder Coordination and Alignment: The 5-Echelon model requires coordination among multiple regulatory authorities, cooperation between regulators and industry, and international partnerships. Misalignments, conflicts, or breakdowns in coordination can undermine effectiveness. Success factors include:

- Strong IFWG governance with clear mandate, adequate resources, and senior leadership engagement
- Transparent stakeholder engagement processes building trust and legitimacy
- Conflict resolution mechanisms addressing inevitable disagreements
- Regular communication and information sharing preventing misunderstandings and duplications
- Shared incentives aligning different actors' interests around common objectives

Adaptive Capacity and Learning Orientation: Perhaps most crucially, implementation success depends on maintaining adaptive capacity and learning orientation throughout extended implementation period. Blockchain technology will evolve in unforeseen directions, implementation will reveal unexpected challenges, and initial approaches will require adjustment. Success requires:

- Organisational cultures supporting experimentation and accepting that some initiatives will fail
- Feedback mechanisms systematically capturing implementation experience and generating lessons
- Willingness to adjust approaches based on evidence rather than defensive attachment to initial decisions
- Sufficient flexibility in implementation timelines and approaches to accommodate necessary adaptations
- Leadership messaging that implementation is iterative process of continuous improvement rather than one-time reform

Balancing Innovation and Protection: Throughout implementation, maintaining appropriate balance between supporting innovation and protecting consumers and systemic stability will require ongoing monitoring and evaluation. Pressures from industry for permissive treatment and pressures from consumer advocates for strict controls create tension. Neither extreme serves societal interests, excessive permissiveness creates risks while excessive restriction stifles beneficial innovation. Maintaining balance requires:

- Evidence-based policy making using empirical research to assess actual rather than hypothetical risks
- Proportionate regulation calibrating requirements to risk levels rather than applying uniform stringent requirements
- Regulatory agility enabling rapid response to emerging risks without prematurely restricting uncertain innovations
- Diverse stakeholder input ensuring both industry and public interest perspectives inform decisions
- Regular reassessment as evidence accumulates about actual blockchain impacts and regulatory effectiveness

6.16 Future Research Agenda

While this knowledge model provides comprehensive frameworks, implementation will generate questions requiring further research. Priority directions include:

Longitudinal Impact Studies: Good regulation needs to be tested against reality over time, and that requires a sustained commitment to research. The key questions are straightforward: is blockchain adoption growing in the ways the framework intended? Are remittance costs actually falling? Are more people gaining access to financial services? Are the rules working as designed, or are they producing unexpected results? Answering these questions properly requires following the same people and businesses over a number of years rather than taking a single snapshot. It also requires looking at transaction data to spot trends, comparing South Africa's experience with that of countries that have made different regulatory choices, and talking directly to the people affected such as the regulators, businesses, and ordinary users. This is to understand what the framework looks and feels like from the inside. Without this kind of ongoing, rigorous research, the framework risks drifting out of step with the reality it is meant to govern.

Technology-Specific Regulatory Deep Dives: While this model addresses blockchain generally, specific technologies warrant focused research:

- DeFi protocols operating without identifiable service providers challenge traditional regulatory approaches assuming intermediaries as compliance actors. Research should examine how regulatory frameworks can effectively oversee DeFi while maintaining innovation space.
- CBDCs present profound implications for monetary policy, financial stability, and payment systems. Research should assess CBDC design options, regulatory requirements, and macroeconomic impacts in South African context.
- Privacy-preserving technologies like zero-knowledge proofs enable transaction validation without revealing underlying data. Research should examine how these technologies can satisfy AML/CFT requirements while protecting privacy
- Layer 2 scaling solutions introduce complexity regarding regulatory classification and supervision. Research should clarify the appropriate regulatory treatment

Comparative Regulatory Analysis: As more countries introduce cryptocurrency regulation, comparing what works and what does not becomes increasingly valuable. The most important questions are practical ones: which regulatory approaches best balance supporting innovation with protecting consumers? How much does context matter and does the same approach work differently in a developing economy than in a wealthy one? What can South Africa learn specifically from other emerging markets that have faced similar challenges? And how do regulatory frameworks tend to evolve once countries start living with them in practice? South Africa does not need to answer these questions alone. Systematic comparison with other jurisdictions can provide evidence that would take years to generate domestically.

Consumer Behaviour and Decision-Making: Effective consumer protection depends on understanding how South African consumers actually engage with blockchain financial services. what information they use when making decisions, what risks they are aware of, what risks they actually encounter, and how they respond to different kinds of warnings or protections. Research methods that would shed light on this include:

1. Behavioural experiments testing whether different ways of presenting information or risk warnings change how people make decisions.
2. Surveys examining financial literacy and decision-making processes
3. Focus groups that explore what users find confusing, helpful, or frustrating
4. Analysis of complaint data to identify the problems that come up most frequently and that regulation most needs to address.

Regional Coordination Mechanisms: Making cryptocurrency regulation work across Southern Africa requires more than goodwill. It requires well-designed institutions and processes. Research into what makes regional coordination actually function would directly inform SADC harmonisation efforts.

The key questions include: 1. What governance arrangements allow countries to coordinate effectively without giving up meaningful control over their own regulatory decisions?

2. How can technical integration be achieved when SADC countries have very different levels of infrastructure development?
3. What approaches successfully balance the need for common standards with the need for flexibility to suit different national contexts?
4. How can smaller SADC countries with limited regulatory capacity be supported in a way that builds their independence rather than creating long-term reliance on South Africa or other partners?

Environmental Sustainability: Blockchain's energy consumption is attracting growing attention globally, and South Africa cannot ignore this dimension. Research should examine how much energy blockchain activity in South Africa actually uses, what the carbon footprint implications are and whether renewable energy could play a greater role in powering mining operations.

It should also determine whether sustainability-focused regulatory interventions such as incentives for greener mining practices are effective. The goal of this research should be to inform policy that takes environmental concerns seriously without using them as a pretext for restricting blockchain innovation more broadly than the evidence justifies.

6.17 Concluding Reflections: Toward Responsible Innovation in the Digital Age

The 5-Echelon model is about more than cryptocurrency. At its heart, it reflects a way of thinking about how societies can manage powerful new technologies, extracting the benefits while limiting the harms, supporting innovation while maintaining accountability, and protecting people without treating them as passive subjects of regulation. These are challenges that will recur as artificial intelligence, biotechnology, and other transformative technologies continue to develop, and the thinking embedded in this model has relevance well beyond blockchain.

One of the model's central insights is that the apparent conflicts in technology governance: innovation versus protection, decentralisation versus control, freedom versus regulation are ultimately not real choices between opposites. They are tensions that can be productively managed when governance is designed with sufficient sophistication. Decentralised blockchain systems can operate within regulatory

frameworks. Innovation can thrive within clear, well-designed rules. Consumer protection and market development support each other when regulation gets the balance right.

The layered approach has broader applicability too. Many of the most pressing policy challenges of our time such as climate change, pandemic preparedness, economic inequality are similarly complex: multi-dimensional, involving many stakeholders, combining technical and social elements, and requiring both urgent action and long-term commitment. The eDSR methodology used here provides a systematic way of tackling this kind of complexity, and its potential applications extend well beyond financial regulation.

The 5-Echelon model's insistence on feedback loops, empirical research, and adaptability reflects an important truth: you cannot regulate a fast-moving technology once and walk away. Regulatory frameworks need to be learning systems that are capable of updating based on evidence, acknowledging when something is not working, and adjusting accordingly. This requires not just better mechanisms but a cultural shift within regulatory institutions toward humility, curiosity, and a genuine commitment to improvement.

Finally, the focus on users is not incidental. It is foundational. Too often, technology is developed and regulated with little regard for the people who actually use it. Blockchain's potential to extend financial services to those who currently lack them, to reduce the costs borne by migrant workers and their families, and to give individuals greater control over their own financial lives will only be realised if users are treated as active stakeholders rather than passive recipients. Regulation that centres user needs is not just better ethically. It is more likely to work.



Figure 62. Graphic outlining the 5-Echelon Knowledge Model

The 5-Echelon knowledge model is the answer to the question this dissertation began with. Chapter 1 identified three dimensions of the challenge:

1. The regulatory barriers that make cryptocurrency difficult to govern
2. The mitigation strategies that can reduce those barriers
3. The ways compliance can be built directly into cryptocurrency systems.

The 5-Echelon model addresses all three. It turns what began as a theoretical diagnosis into a practical blueprint. The specific problems identified early in the dissertation, such as no clear legal framework, inconsistent international standards, cautious institutions, each find a response in one or more of the echelons. The tools identified as promising such as the regulatory sandboxes, risk-based compliance, the Travel Rule, RegTech, are not left floating as recommendations but embedded within the model's structure, connected to specific actors and specific timeframes.

However, the model is not the end of the story. It is the beginning of a longer one. Cryptocurrency regulation will never reach a final, settled state. Technology will keep changing, new use cases will emerge, and markets will develop in ways that are difficult

to predict. What South Africa needs is not a fixed rulebook but a framework capable of learning and adapting over time. That is what this model is designed to be.

If South Africa implements the model well, the benefits will reach beyond its own borders. The world is watching to see whether emerging markets can engage with transformative technologies on their own terms and not simply adopting frameworks designed for wealthier countries, but developing genuinely innovative approaches that reflect their own circumstances, priorities, and potential.

The 5-Echelon model is an attempt to do exactly that. Its greatest contribution may not be any single policy recommendation, but the demonstration that an emerging market can think carefully, act ambitiously, and lead, rather than follow, in one of the most consequential regulatory challenges of our time.

CHAPTER 7

CONCLUSION

7.1 Key Findings: Insights from the Regulatory Environment

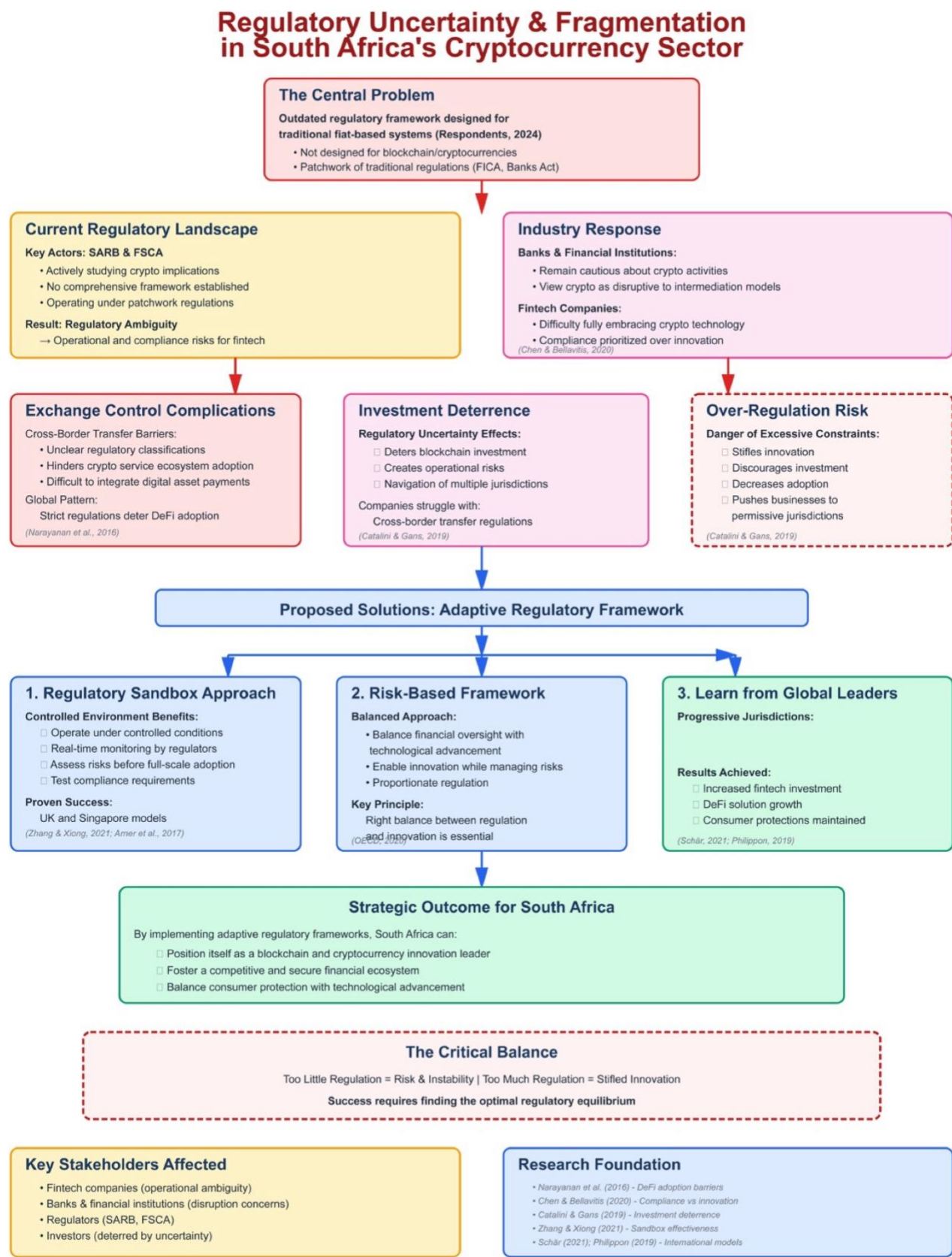
7.1.1 Regulatory Uncertainty and Fragmentation

When asked about South Africa's regulatory environment, Respondents (2024) were largely in agreement on three things. First, the existing framework was not designed with cryptocurrency in mind. It was built around traditional currencies and has not been meaningfully updated to reflect the emergence of digital assets. Secondly, banks and financial institutions are wary of cryptocurrency, seeing it as a disruptive force that threatens the role they currently play in the financial system. Third, exchange controls, which is already a complex area, become particularly problematic when the rules around crypto-assets are unclear, making it genuinely difficult for businesses to build payment solutions that cross borders using blockchain technology. None of this is unique to South Africa.

Research shows that strict financial regulation tends to slow the adoption of decentralised finance (Narayanan et al., 2016), that financial institutions around the world tend to put compliance ahead of innovation (Chen & Bellavitis, 2020), and that uncertainty about the rules deters investment in blockchain technology (Catalini & Gans, 2019). South Africa's situation, as described by respondents, fits squarely within this global pattern. One of the most important themes that emerged from the interviews was the prevailing uncertainty regarding the regulatory status of cryptocurrency. Many interviewees from the regulatory sector highlighted that while South African authorities, most notably the South African Reserve Bank (SARB) and the Financial Sector Conduct Authority (FSCA), are actively studying the implications of crypto-assets, a comprehensive framework has not yet been established.

Currently, South Africa operates under a patchwork of traditional financial regulations, such as the Financial Intelligence Centre Act (FICA) and the Banks Act, which were not originally designed with blockchain or cryptocurrency in mind. As a result, many fintech

companies operating in this space face regulatory ambiguity, leading to operational and compliance risks.



Source: Respondent interviews (2024) and academic literature review
Figure 63. Graphic indicating Cryptocurrency Regulatory Uncertainty in South Africa (Researcher)

Regulatory sandboxes have been instrumental in fostering blockchain innovation in jurisdictions such as the United Kingdom and Singapore (Zhang & Xiong, 2021). These controlled environments enable regulators to monitor cryptocurrency and crypto-asset service ecosystems in real time while assessing risks and compliance requirements (Arner, Barberis & Buckley, 2017). A risk-based regulatory framework could enable South Africa to balance financial oversight with technological advancements (OECD, 2020). Countries such as Switzerland and Estonia have adopted progressive cryptocurrency regulations, leading to increased investment in fintech and decentralised finance solutions (Schär, 2021).

By following these examples, South Africa could position itself as a leader in blockchain and cryptocurrency innovation while ensuring necessary consumer protections (Philippon, 2019). The risk of over-regulation, which could stifle innovation and discourage investment in blockchain start-ups, is also real; studies by Catalini and Gans (2019) indicate that excessive regulatory constraints can lead to decreased blockchain adoption, pushing businesses toward more permissive jurisdictions.

7.1.2 *Blockchain's Potential for Innovation and Transformation*

Despite regulatory challenges, respondents agreed on the transformative potential of cryptocurrency-based payment systems, particularly stablecoin and tokenised settlement models, to improve cross-border remittances and trade finance. Cost reduction arises from reduced intermediation and automated settlement rather than from blockchain as an abstract technology. Blockchain's ability to offer decentralised, transparent, and secure transaction systems was viewed as a key enabler for improving cross-border payments, especially in areas such as remittances, trade finance, and interbank settlements. Many respondents cited the inefficiencies and high costs associated with current cross-border financial systems, which are often slow, expensive, and vulnerable to errors.

Cryptocurrency and crypto-asset service ecosystems, with their near-instantaneous settlement capabilities and reduced reliance on intermediaries, were seen as a solution to many of these inefficiencies. Interviewees noted that blockchain could significantly reduce the costs of cross-border remittances, a major issue for South African migrant

workers sending money home, often to neighbouring African countries. By eliminating the need for traditional correspondent banking networks, blockchain could not only lower fees but also provide greater access to financial services for underserved populations.

7.1.3 Regulatory Concerns: AML, KYC, and Consumer Protection

Those interviewed for this study agreed on one thing above all: South Africa's current regulatory approach is too rigid for a fast-moving technology like blockchain. The solution most commonly proposed was a regulatory sandbox which is a structured environment where cryptocurrency businesses can test their products and services under close regulatory supervision before the full weight of regulation applies. This is not an untested idea. The UK and Singapore have both used sandboxes effectively, giving regulators direct insight into how blockchain works in practice while identifying risks early (Zhang & Xiong, 2021; Arner, Barberis & Buckley, 2017).

Alongside this, respondents called for a risk-based framework, one that applies stricter rules where the risks are genuinely high and lighter requirements where they are not, rather than treating all cryptocurrency activity the same way (OECD, 2020). Switzerland and Estonia both show what progressive regulation can achieve, that by creating clear, welcoming frameworks for cryptocurrency, both countries attracted significant investment in fintech and decentralised finance (Schär, 2021). South Africa could do the same, without abandoning the consumer protections that users need (Philippon, 2019).

But respondents were equally concerned about the opposite problem. Rules that are too strict push businesses and investment to other countries and research confirms that excessive regulation reduces cryptocurrency adoption (Catalini & Gans, 2019). The goal is not maximum regulation or minimum regulation. It is the right regulation, enough to protect people and maintain financial stability, but not so much that it makes South Africa an unattractive place to build and grow a cryptocurrency business.

AML and KYC were identified as a particular area of concern. Because many cryptocurrency transactions are pseudonymous, meaning that they were conducted

without revealing the identity of the parties involved, verifying who is transacting and flagging suspicious activity is genuinely difficult.

Without clear guidelines tailored to cryptocurrency, these gaps could be exploited for money laundering, tax evasion, or financing terrorism. Respondents called for AML and KYC rules designed specifically for the cryptocurrency environment and several pointed to digital identity verification, integrated with blockchain, as a tool that could make compliance more robust and less burdensome at the same time. The importance of clear consumer protection rules was also raised: people using blockchain platforms face real risks such as fraud, hacking, and the possibility of losing funds, and the regulatory framework needs to address these directly.

There is also a widespread misconception worth addressing. Some regulators assume that cryptocurrency makes financial crime easier. The evidence suggests the opposite. Blockchain transactions leave a permanent, traceable record and making them more transparent than cash in many respects. Research indicates that cryptocurrency-based fraud prevention tools can actually outperform traditional systems (Foley, Karlsen & Putniņš, 2019), and the ability to monitor transactions in real time makes it easier, not harder, to detect suspicious patterns (Casino, Dasaklis & Patsakis, 2019).

The FATF's approach of focusing regulation on service providers rather than the technology itself reflects this understanding, and the EU has already shown that blockchain can be integrated into financial oversight frameworks effectively (Tasca & Tessone, 2019). Real challenges remain, however, and they deserve honest acknowledgement. Decentralised finance, where there is no central service provider to regulate, creates enforcement gaps that are difficult to close. Privacy-enhancing technologies like zero-knowledge proofs, which allow someone to prove they meet a compliance requirement without revealing personal data add another layer of complexity (Auer, Cornelli & Frost, 2021).

Regulators will need to find a way to respect people's right to financial privacy while ensuring the system cannot be used to conceal criminal activity. There is no simple answer to this. It requires ongoing judgement, adaptation, and a willingness to revisit decisions as the technology and the regulatory environment continue to evolve (Gai, Qiu & Sun, 2021).

7.1.4 *Need for International Collaboration*

Every interviewee for this study raised the same concern: when different countries regulate cryptocurrency differently, cross-border transactions become unnecessarily complicated and the gaps between regulatory systems get exploited. Cryptocurrency is borderless by design, which means that a transaction can involve multiple countries simultaneously and regulation confined to a single country will always leave gaps. South Africa, as a member of SADC and a significant presence in global financial markets, is well placed to do something about this.

Interviewees called on South African regulators to engage seriously with international bodies like the FATF, align the country's rules with global standards, and, importantly, take an active leadership role in pushing for consistent standards across African countries. The message was consistent: South Africa should not simply wait for international consensus to form and then follow it. It should help shape it.

7.1.5 *Mitigations for Regulatory Challenges*

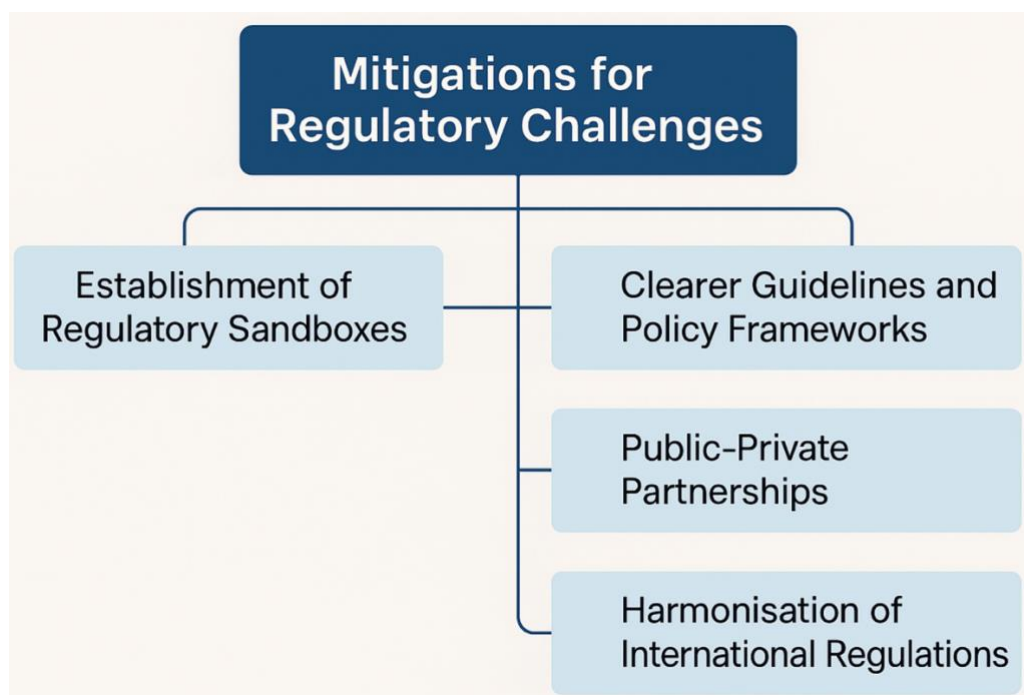


Figure 64. Graphic outlining mitigations for regulatory challenges (Researcher)

The research identified several mitigation strategies to address the regulatory challenges associated with cryptocurrency and crypto-asset service ecosystems technology in cross-border financial transfers:

7.1.6 *Establishment of Regulatory Sandboxes*

The implementation of regulatory sandboxes was one of the most frequently recommended solutions by interviewees. Regulatory sandboxes would allow fintech firms and blockchain innovators to test their products and services in a controlled environment, under the supervision of regulators. This approach provides a safe space for experimentation while enabling regulators to better understand the risks and opportunities of cryptocurrency technology.

Countries like the United Kingdom and Singapore have successfully adopted regulatory sandboxes, and several interviewees advocated for South Africa to follow suit. By creating a sandbox specifically for blockchain applications, South African regulators can foster innovation without compromising financial stability or consumer protection.

7.1.7 *Clearer Guidelines and Policy Frameworks*

All respondents emphasised the need for more transparent and detailed guidelines regarding cryptocurrency and crypto-asset service ecosystems regulation. Currently, the lack of clear crypto-asset classifications has created uncertainty for CASPs, exchanges, and wallet providers. Regulatory bodies such as the SARB and FSCA should take the lead in crafting guidelines that outline how existing laws (such as AML/KYC regulations) apply to blockchain-based systems. Moreover, respondents highlighted the importance of stakeholder engagement in developing these guidelines. Engaging with cryptocurrency and crypto-asset service ecosystems developers, fintech companies, academics, and legal experts in the policymaking process would ensure that regulations are both practical and reflective of the technological advances in the industry.

7.1.8 *Public-Private Partnerships*

Those interviewed for this study were consistent on one point that government and the private sector need to work together more closely on cryptocurrency regulation. At the moment, regulators and industry too often operate at arm's length, which means regulations can end up out of step with how the technology actually works. If South African regulators engage directly with cryptocurrency businesses and blockchain experts, they will be better placed to write rules that are practical, proportionate, and responsive to change.

This is not just common sense as evidenced on research by Schär (2021) and Auer et al. (2021) that shows that this kind of collaboration is one of the key factors in successfully bringing cryptocurrency into the mainstream financial system. Traditional banks and financial institutions also need to take note. Decentralised finance and central bank digital currencies are no longer distant possibilities. They are rapidly becoming part of the financial landscape, and institutions that do not engage with them risk being left behind (Treleaven, Brown & Yang, 2017).

South Africa has a genuine opportunity to use blockchain to bring more people into the financial system and to lead the way on this across the continent. But it will only get there if regulators are willing to work with industry rather than against it and supporting innovation while making sure the right protections are in place.

7.1.9 *Harmonisation of International Regulations*

A cryptocurrency transaction can cross dozens of national borders in seconds. This makes international coordination not a luxury but a necessity because rules that only apply within South Africa's borders will always have gaps that can be exploited. Interviewees stressed that South Africa needs to engage actively with international bodies like the FATF to make sure its regulatory approach is consistent with what other countries are doing. When rules are broadly aligned across jurisdictions, cross-border transactions are easier to facilitate and harder to abuse. When they are not, businesses simply move their operations to whichever country has the loosest rules thereby undermining the purpose of regulation everywhere.

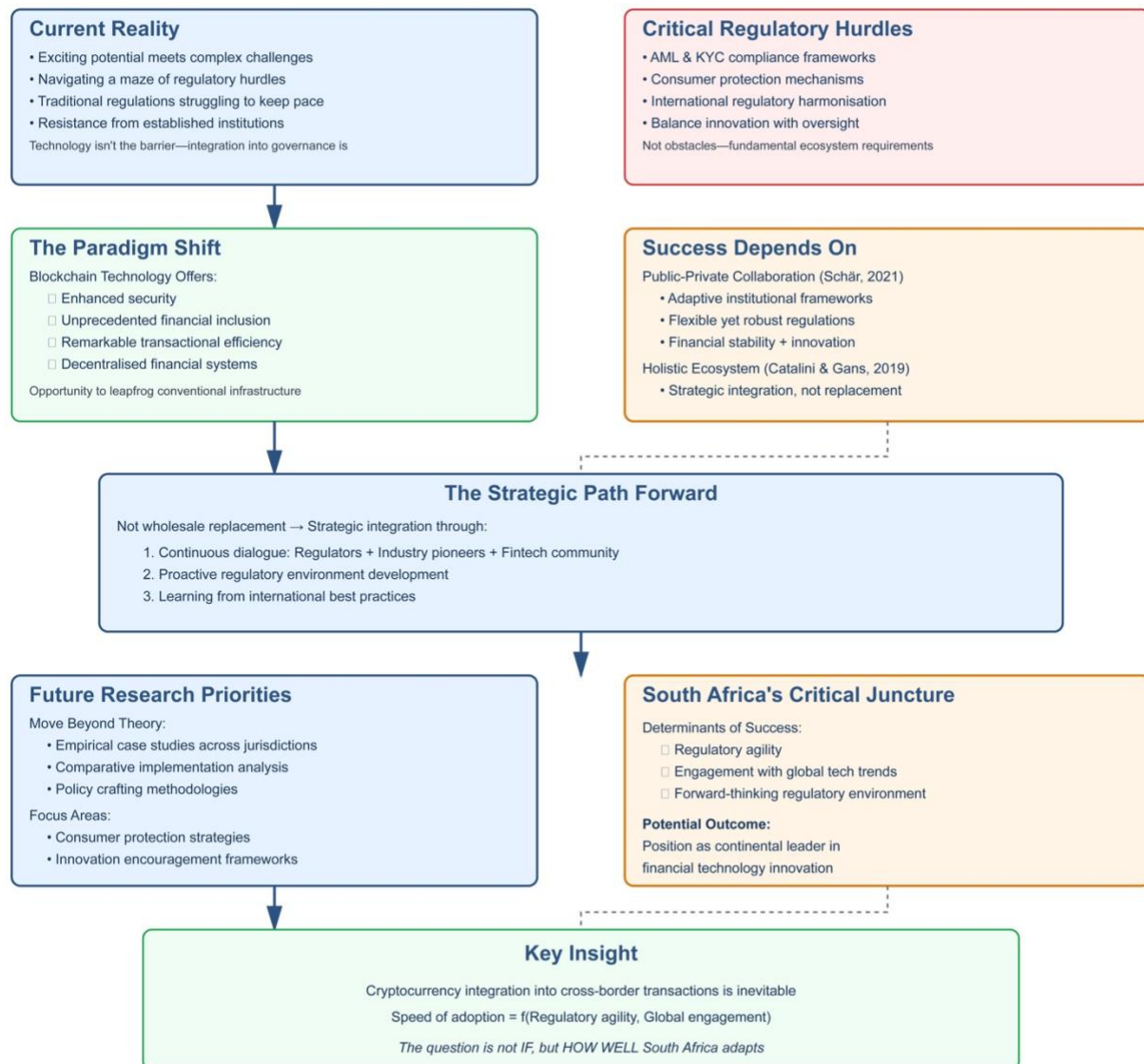
7.1.10 *Contribution to the Field*

This research contributes to understanding how cryptocurrency function as regulated financial instruments within South Africa's cross-border payment environment. The study provides a nuanced exploration of the regulatory challenges cryptocurrency poses and offers practical solutions that could help South Africa navigate these challenges. By combining insights from literature with the views of professionals in the financial regulatory field, this research highlights the key issues regulators and policymakers must address to promote cryptocurrency and blockchain innovation while safeguarding the financial system.

7.1.11 *Conclusion and Recommendations for Future Research*

The potential of cryptocurrency and blockchain technology to revolutionise cross-border financial transfers in South Africa is both exciting and complex. While the technology promises unprecedented transformation, its journey is currently navigating a maze of regulatory challenges that demand careful consideration. At the heart of cryptocurrency adoption lies critical regulatory hurdles. Compliance with AML and KYC frameworks, robust consumer protection mechanisms, and the intricate challenge of international regulatory harmonisation are not mere bureaucratic obstacles, they represent fundamental ecosystem requirements.

Cryptocurrency & Blockchain in South Africa: The Path Forward



Key Citations: Schär (2021), Auer et al. (2021), Treleaven, Brown & Yang (2017), Catalini & Gans (2019)

Core Distinction: Blockchain = Infrastructure | Cryptocurrencies = Financial instruments in payment ecosystems

 Challenges
 Opportunities
 Critical Factors
 Strategic Elements

Figure 65. Graphic outlining the way forward for cryptocurrency (Researcher)

Schär (2021) and Auer et al. (2021) have compellingly argued that the intersection of public and private sector collaboration is pivotal. Their research suggests that seamless cryptocurrency integration isn't just about technological capability but about creating adaptive, responsive institutional frameworks. The financial landscape is rapidly evolving. Traditional institutions are being compelled to reimagine their operational models, with decentralised financial systems and Central Bank digital currencies emerging as potential game-changers (Treleaven, Brown, & Yang, 2017).

For South Africa, this represents more than a technological shift, it's an opportunity to leapfrog conventional financial infrastructures. The researcher's analysis reveals an uncomfortable reality that existing financial regulations are struggling to keep pace with technological innovation. Blockchain isn't just a new technology. It's a paradigm shift offering enhanced security, unprecedented financial inclusion, and remarkable transactional efficiency. However, its path is far from straightforward. The resistance from established financial institutions and regulators represents a significant strategic challenge. Blockchain and cryptocurrency technology's success will hinge on a fine balance between fostering innovation and maintaining rigorous regulatory oversight.

When we draw insights from global thought leaders like Catalini & Gans (2019), it's clear that cryptocurrency's trajectory depends on creating a holistic ecosystem. This means developing regulatory frameworks that are simultaneously flexible and robust, promoting financial stability while embracing technological advancement. Future research must extend beyond theoretical discussions. Empirical case studies comparing cryptocurrency's implementations across different jurisdictions will unlock pertinent insights into effective strategies. As blockchain and cryptocurrency technology continues to mature, ongoing research will be crucial in crafting policies that protect consumer interests while encouraging innovation. The road ahead for blockchain in South Africa's financial sector is, therefore, not about wholesale replacement but strategic integration. Success will emerge from continuous dialogue and collaboration among regulators, industry pioneers, and the broader fintech community. Blockchain serves as infrastructure, but cryptocurrency operate as financial instruments within payment ecosystems. Regulatory challenges therefore arise not from the technology itself but from integrating crypto-asset systems into existing financial governance structures.

The findings of this study, when examined through the three-dimensional analytical framework introduced in Chapter 1 reveal a coherent and mutually reinforcing picture of the regulatory landscape confronting cryptocurrency-based cross-border transfers in South Africa. The first dimension, regulatory challenges, is comprehensively borne out by the empirical data gathered in this study. Respondents 3, 6, 8, 5 and 2 (2024) consistently identified the absence of clear and comprehensive legal guidelines, the

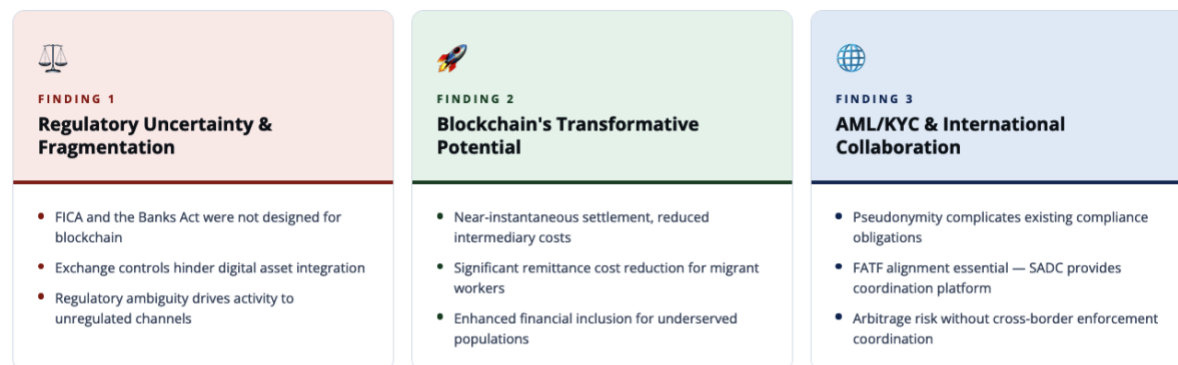
lack of harmonised global standards, and the cautious posture of incumbent financial institutions as the primary structural barriers to adoption. The pseudonymous character of cryptocurrency transactions, the decentralised elimination of traditional intermediaries, and the persistent inertia of a regulatory architecture designed for fiat-based, bank-mediated systems together produce the fragmented compliance environment that Chapter 1 anticipated. These are not incidental frictions but systemic features of the tension between decentralised crypto-asset networks and the centralised financial regulatory paradigm that continues to govern South African financial services.

The second dimension, regulatory mitigation approaches, finds equally strong resonance in the study's findings. The IFWG Regulatory Sandbox emerged as the most prominent and consistently endorsed mitigation mechanism among interviewees, reflecting exactly the kind of adaptive, risk-based, and iterative regulatory experimentation that Chapter 1 identified as essential to bridging the innovation gap.

The advocacy expressed by respondents for clearer policy frameworks, proactive public-private partnerships, and meaningful engagement with FATF Travel Rule requirements at the international level directly mirrors the mitigation strategies theorised at the outset of the study. Critically, however, the research confirms the warning sounded in Chapter 1 that mitigation approaches remain incomplete without a defined post-sandbox regulatory pathway, a structural gap that continues to inhibit scale-up and investor confidence.

The third dimension, the embedding of regulatory compliance within cryptocurrency design, represents the most forward-looking dimension of the framework and the one where the gap between potential and current practice is most pronounced. Interviewees acknowledged the transformative potential of RegTech integration, self-sovereign identity frameworks, and real-time blockchain analytics as tools that reposition technology from a vector of regulatory evasion to an enabler of compliance. This conceptual shift, articulated in Chapter 1 as a defining feature of the study's analytical contribution, is progressively gaining traction globally but remains nascent within South Africa's regulatory and institutional culture.

KEY FINDINGS



MITIGATION STRATEGIES



THREE DIMENSIONS · CHAPTER 1 FRAMEWORK VALIDATED

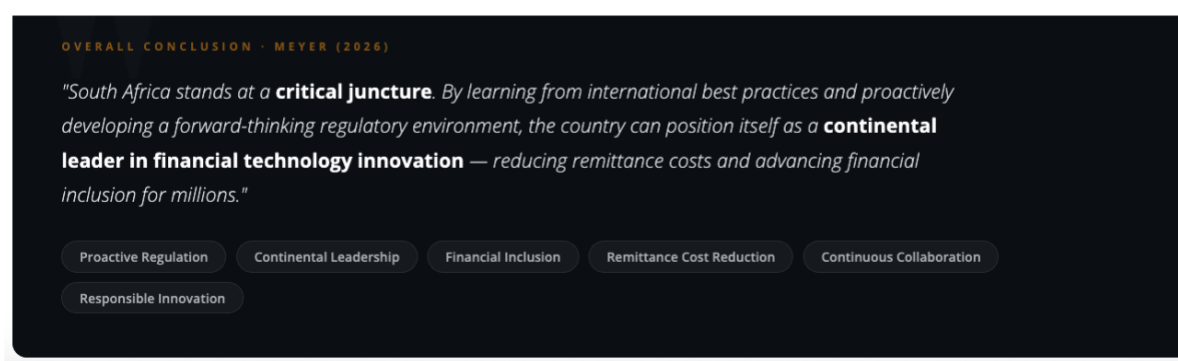


Figure 66. Graphic outlining the key findings and mitigation strategies relating to Chapter 7 (Researcher)

The three dimensions of this study's framework fit together in a logical sequence. The regulatory challenges explain what is standing in the way. The mitigation approaches explain what can be done about it through policy. And embedded compliance points to where the journey ultimately leads, which is a future in which compliance is not an

obstacle layered onto blockchain systems but a capability built into them from the start. The close match between the framework introduced in Chapter 1 and what the empirical research found gives confidence that the study is asking the right questions and that its recommendations are grounded in reality rather than theory alone.

Cryptocurrency is going to play a bigger role in cross-border payments. That much seems clear. What is less certain is how quickly South Africa will be part of that shift, and on whose terms. The answer depends on whether regulators are willing to move fast enough and openly enough to engage with the technology rather than simply manage it from a distance. South Africa has the institutions, the technical foundations, and the regional influence to lead on this. Not just for its own benefit, but as a model for the rest of the continent. Whether it seizes that opportunity will depend on the choices made now.

7.2 CONSOLIDATED RESPONSES TO THE RESEARCH SUB-QUESTIONS

The earlier sections of this chapter presented findings as they emerged from the interviews. This section brings those findings together and uses them to answer each of the three research sub-questions directly. The 5-Echelon model provides the framework for doing so. The three answers are connected. Each builds on the one before it and together they represent the study's central contribution to scholarship on blockchain regulation and cross-border financial transfers in South Africa.

7.2.1 Sub-Question 1: Balancing Innovation with Compliance while Addressing Institutional Resistance and Technical Integration

The first research question asked something fundamental: can South Africa build a regulatory framework that genuinely supports blockchain innovation in cross-border payments while still meeting its compliance obligations? And if so, how does it overcome the institutional resistance and technical barriers that have held progress back? The study found a clear answer. Yes, it is possible, but only if three things are addressed together.

The first is legislation. South Africa's key financial laws are simply too old and too narrowly designed to cover blockchain. The Currency and Exchanges Act was written

in 1933. The National Payment System Act dates from 1998. Both assume that every financial transaction runs through an identifiable, centralised institution that can be licensed, monitored, and held accountable. Blockchain does not work that way because transactions happen directly between parties, often pseudonymously, without a central intermediary. No amount of creative interpretation will make laws designed for one world fit a fundamentally different one (Zetzsche et al., 2017). What is needed is new legislation that defines crypto-assets clearly, sets proportionate licensing requirements for cryptocurrency businesses, and calibrates compliance obligations to actual levels of risk.

The second is institutional culture. This study found, consistently across respondents, that the biggest human barrier to progress is not a lack of technical understanding. It is a deeply ingrained tendency to treat new entrants and new technologies as threats to be controlled rather than opportunities to be enabled. Incumbent banks have a strong interest in keeping things as they are. Regulatory bodies have historically defaulted to caution. This, however, is not simply stubbornness because it reflects real institutional incentives. But it needs to change. The IFWG has begun the work of building a more collaborative, facilitative culture, and this study recognises that. The research is equally clear, however, that this shift is far from complete (Chen & Bellavitis, 2020).

The third is technology. Getting blockchain to work within South Africa's financial system requires it to connect reliably with the infrastructure that system already runs on, particularly SWIFT and the ISO 20022 messaging standard that most international transfers use. This is currently the biggest technical bottleneck. The good news is that South Africa has already demonstrated it can solve this kind of problem. Project Khokha showed that blockchain-based settlement can work at the interbank level while remaining fully compatible with the Reserve Bank's oversight requirements (SARB, 2022). The task now is to build on that foundation and extend it to retail payments and cross-border transfers.

The answer to Sub-Question 1, then, is this: balance between innovation and compliance is achievable in South Africa, but only if the legislative, institutional, and technical pieces are addressed together, in a deliberate sequence, rather than tackled one at a time as separate problems. This is not a theoretical conclusion. Singapore and the EU both demonstrate it in practice. The jurisdictions that have got this right have

done so through careful, coherent policy design, not by slowly patching laws that were never built for the purpose.

7.2.2 Sub-Question 2: Financial Inclusion and the Transition from Gatekeepers to Facilitators

The second research question asked how South Africa can develop cryptocurrency regulation that genuinely supports financial inclusion, and what needs to change in how regulators think about their role. The study's answer is clear that these two goals are not in tension. Done right, they reinforce each other.

Start with the problem. Around one in ten South African adults has no bank account. Sending money between African countries costs between 8 and 11% of the amount transferred, more than twice the level the G20 has identified as a target. Migrant workers, who are among the most economically vulnerable people in the country, consistently pay the highest fees to move money that their families depend on (World Bank, 2023; Rühmann et al., 2020). This is not an accident. It is what happens when a financial system is built for people with stable jobs, fixed addresses, and the right documents, but unfortunately has nothing to offer people whose lives look different.

Blockchain changes the equation, because it separates financial access from the documentation that traditional systems require (Respondents 2, 4, 5 & 8, 2024). A migrant worker without a passport or a formal bank account can establish a verifiable digital identity through a community-based process and use it to send money home at a fraction of current costs. The barriers that have historically kept people out of the financial system are not natural or inevitable. It is features of a particular system design, and a different design can remove them.

However, none of this happens automatically. There are certain things that need to be actively put in place. First, identity verification rules need to be tiered, with lighter requirements for small, low-risk transactions, and more rigorous ones as the stakes increase. Second, getting online needs to be affordable and accessible in the communities that stand to benefit most, which requires investment and public-private partnership, not just policy permission.

Third, the focus needs to be on use cases where the benefits are immediate and visible, particularly sending money across SADC borders, rather than abstract possibilities (FATF, 2021; IMF, 2022). The respondents in this study were consistent on this point that the enabling conditions need to be built deliberately, not wished into existence.

The deepest change required, though, is in how regulators see themselves. For too long, financial regulators in South Africa have operated primarily as gatekeepers. They decided what is and what is not permitted, and defaulting to caution when uncertain. This made sense in a slower-moving financial system. It does not serve South Africa well in a fast-moving technological environment where the cost of excessive caution, like innovation lost, people excluded, competitors gaining ground is just as real as the cost of insufficient oversight.

Ayres and Braithwaite's (1992) work on responsive regulation is relevant where they state that regulatory systems that build on dialogue, trust, and graduated responses produce better outcomes than those built on suspicion and enforcement. The IFWG has begun to move in this direction. The task now is to fully institutionalise it.

The answer to Sub-Question 2, then, is this: financial inclusion and regulatory innovation are the same goal, not competing ones. A regulator that actively helps legitimate innovators navigate the system, invests in the infrastructure that makes financial access possible for everyone, and works with the private sector as a partner rather than an adversary is not being soft on regulation. It is being smart about it, and it is the only approach that will convert blockchain's genuine potential into real and lasting change in people's lives.

7.2.3 *Sub-Question 3: Technically Embedding KYC/AML Compliance in Blockchain-Based Cross-Border Solutions*

The third research question asked something specific and practical: can the compliance requirements that financial regulators need such as identity verification, transaction monitoring, sanctions screening, actually be built into blockchain systems themselves, rather than layered on top of them? The answer this study arrives at is yes, and more than that, doing so produces better results than the traditional approach (Arner, Barberis & Buckley, 2017).

The key insight is about design. When compliance is treated as an afterthought, when rules are added to systems that were not built with them in mind then the result is friction, cost, and gaps that bad actors can exploit. When compliance is treated as a design requirement from the start, built into the system before it goes live, the result is something more reliable, more transparent, and cheaper to maintain. This is not just a theoretical possibility. It is already happening in other jurisdictions, and the evidence from Singapore and the EU supports it.

Three specific mechanisms make this work in practice. The first is the Travel Rule. South Africa's Directive 9 (FIC, 2025) requires cryptocurrency service providers to attach sender and recipient information to transactions above R 5,000, in line with FATF standards. For this to work across borders, which is where remittances go, South African providers need to use common technical standards for how that information is packaged and transmitted, and they need formal agreements with providers in the countries their customers are sending money to, particularly Zimbabwe, Mozambique, and Nigeria.

The second is smart contracts. Instead of relying on people to manually check identities, screen for sanctions, and calculate tax withholding, these processes can be programmed into smart contracts that run automatically every time a transaction occurs (Casino, Dasaklis & Patsakis, 2019). This is faster, cheaper, more consistent, and harder to game. Because any change to a smart contract leaves a permanent, visible record on the blockchain, regulators can be confident that the rules are being applied as intended and cannot be quietly circumvented.

The third is self-sovereign identity. Traditional KYC requires a passport or government-issued ID. Many of the people who depend most on affordable cross-border transfers especially migrant workers, people in rural areas, those who have never had a formal bank account, do not have these documents. Self-sovereign identity systems offer an alternative: people can build a verifiable digital identity through community-based processes, and use that identity to access regulated cryptocurrency services under a tiered compliance framework that matches the level of verification to the level of risk (Respondent 5, 2024). This directly addresses both the financial inclusion challenge and the anonymity problem that makes AML enforcement difficult.

There is one genuine tension that needs to be acknowledged. Technologies like zero-knowledge proofs make it possible to prove compliance with a rule and that is proving that a transaction comes from a verified, non-sanctioned source without revealing any personal information (Auer, Cornelli & Frost, 2021). This is good for privacy and consistent with South Africa's POPIA obligations. But it also means regulators see less detail about individual transactions, which limits their ability to investigate suspicious activity. There is no perfect answer here. It is a trade-off that regulators will need to keep revisiting as technology develops and as they learn more about what oversight actually requires in practice.

The conclusion is therefore straightforward. Compliance can be built into blockchain systems, and when it is, it works better than the traditional alternative. But this will not happen automatically. It requires regulators to make specific decisions, such as mandating common standards for the Travel Rule, recognising self-sovereign identity within the FSCA's licensing framework, and investing in the analytics tools that allow regulators to monitor blockchain activity effectively. Without these choices being made deliberately and soon, the opportunity will be missed.

7.3 LIMITATIONS OF THE STUDY

This study attempts to make a genuine contribution, but being clear about what that contribution is, also means being clear about what it is not. The following limitations are worth highlighting.

The findings are based on interviews with eight people. Those eight individuals were chosen carefully and brought real expertise to the research, but eight expert opinions, however valuable, cannot be treated as representative of the full range of views and experiences across South Africa's cryptocurrency landscape. The insights generated here are best understood as a starting point for further research, not a final answer. The kind of evidence that policy decisions ultimately need, namely large-scale surveys, transaction data and long-term cost studies are still missing and still needs to be produced (Bryman, 2012).

The 5-Echelon model was designed for South Africa. It draws on lessons from Singapore, the EU, and the FATF, but it has been built around South Africa's specific institutions, laws, and circumstances. Another emerging market with a different banking system, different identity infrastructure, or different capital controls might find that the model needs significant adaptation before it is useful in their context.

Things change quickly in this field. Some of the specific regulatory details discussed in this study such as the 2025 High Court ruling, South Africa's progress on Financial Action Task Force (FATF) compliance, the implementation of Directive 9 may look different by the time this work reaches the people who could act on it. The 5-Echelon model is designed to adapt over time, but that does not mean every specific reference will remain accurate (Zetsche et al., 2017). Where this study discusses particular laws or rulings, readers should focus on the broader point being made rather than treating the specific detail as fixed.

The study cannot prove cause and effect. The evidence gathered here points strongly in certain directions, thereby suggesting that clearer regulation would reduce remittance costs and bring more people into the financial system. However, it cannot say by how much, how quickly, or under exactly what conditions. Answering those questions requires a different kind of research, with quantitative methods that this study does not attempt.

The researcher works in the government fintech regulatory space professionally. This opened doors and it meant that expert respondents were willing to speak candidly and in depth. But it also created a risk of unconsciously interpreting findings in ways that confirmed existing views. Careful sampling, checking findings back with respondents, and using Atlas.ti to code the data systematically all helped to manage this risk, though none of them can remove it entirely. These five limitations do not undermine what this study has achieved. But they matter and readers should keep them in mind when deciding how to interpret and apply the findings.

7.4 DIFFERENTIATED RECOMMENDATIONS BY STAKEHOLDER GROUP

The recommendations that follow are tailored to specific groups rather than addressed to everyone equally. This reflects a straightforward reality that regulators, industry participants, institutions, and researchers each have different responsibilities, different resources, and different pressures. A recommendation that is practical and urgent for one group may be irrelevant or premature for another. Organising the recommendations by stakeholder makes it easier to identify what each group can and should do, and in what order.

7.4.1 *Recommendations for Policymakers and the National Treasury*

The single most important thing policymakers and the National Treasury can do is set up a dedicated task force to update South Africa's financial laws. Three pieces of legislation need attention: the Currency and Exchanges Act, 1933 (as amended), the National Payment System Act, and FICA. All three need to be amended so that they explicitly cover cryptocurrency businesses, use clear and consistent definitions, and most importantly, give businesses that have already proved themselves in the IFWG regulatory sandbox a defined legal status and a clear path forward (IFWG, 2021; Zetzsche et al., 2017). This last point matters the most.

The research for this study found the same problem raised on numerous occasions that businesses that have operated successfully within the sandbox, demonstrated that they can meet compliance requirements, and built genuine products are stuck. They cannot grow, they cannot attract serious investors, and they cannot make long-term plans, because they have no clear legal standing. That needs to change. Policymakers should also commission research that South Africa currently lacks. There are no reliable national surveys of how people are actually using cryptocurrency. There is no systematic assessment of what stablecoins are doing to monetary policy. There are no long-term studies tracking whether blockchain is actually making remittances cheaper. Without this data, regulators are making decisions based on caution rather than evidence, which tends to produce rules that are more restrictive than they need to be. Investing in this research will not only improve future regulation but it also will make it

politically easier to introduce, because the case for change will be grounded in facts rather than assumptions.

7.4.2 *Recommendations for the SARB and the FSCA*

This research has two main recommendations for the SARB and FSCA. First, they need to move faster on supervising cryptocurrency businesses in a way that is proportionate to risk. This means investing in the technology needed to monitor transactions in real time, rather than relying on periodic reports, and building on what Project Khokha has already achieved. Project Khokha proved that blockchain-based settlement works at the level of large interbank transactions. The next step is to extend that work so that retail cryptocurrency businesses can participate within a properly regulated environment, and so that cross-border transfers within the SADC region can be handled more efficiently (SARB, 2022).

The IFWG needs to be put on a stronger footing. At the moment, it brings regulators together to share information and coordinate thinking which is valuable, but it does not have the legal authority or the dedicated resources to enforce the Travel Rule across borders or to negotiate the formal cooperation agreements with countries like Zimbabwe, Mozambique, and Nigeria that South Africa's remittance flows require (FATF, 2021; BIS, 2023). Making the IFWG's mandate legally binding and properly resourced is not optional because it is the foundation on which effective cross-border regulation depends.

7.4.3 *Recommendations for the Crypto-Asset Industry and CASPs*

This study has a practical message for cryptocurrency businesses which is, compliance pays. Building proper systems for identity verification, transaction monitoring, and transparent fee disclosure is not just about satisfying regulators. It is about building the kind of reputation that attracts serious investors and earns the trust of customers. Trust is the most valuable thing a cryptocurrency business can have, and it is also the easiest to lose.

The Mirror Trading International case proved this in the most damaging way possible, and when that scheme collapsed, it did not just harm the people who lost money. It made everyone in South Africa more suspicious of cryptocurrency as a whole (FSB, 2023). The businesses that invest in getting compliance right now will be better positioned than those that cut corners, both with regulators and in the market. There is also a strong case, both commercially as well as ethically, for cryptocurrency businesses to invest in reaching South Africa's low-income and migrant communities.

These are the people who currently pay the highest fees to send money home, who have the least access to formal financial services, and who have the most to gain from what blockchain can offer. They are also the people most likely to be harmed if the industry remains poorly regulated and products are designed without their needs in mind. Serving these communities well is not charity. It is an opportunity to reach the largest group of financially underserved people in the country, and to build lasting loyalty in the process.

7.4.4 *Recommendations for Future Researchers*

This study raises as many questions as it answers, and several of the most important ones point toward future research. Firstly, someone needs to track what actually happens over time, researching whether blockchain adoption grows, whether remittance costs fall, and whether the regulatory framework makes a measurable difference across the SADC region. Secondly, the topic of decentralised finance, where there are no licensed intermediaries to regulate and algorithms govern transactions automatically, presents governance challenges that existing frameworks, including the 5-Echelon model, do not fully address. This is a gap that future research needs to fill.

Thirdly, South Africa is not the only African country grappling with cryptocurrency regulation. Nigeria, Kenya, and Ghana are also significant players, and comparing approaches across these countries would produce insights that no single national case study can provide. Lastly, the question of whether and how South Africa should introduce a central bank digital currency, and what that would mean for an economy that manages capital flows as carefully as South Africa does, deserves serious, evidence-based investigation (FSB, 2023; IMF, 2022).

The 5-Echelon model itself also points beyond cryptocurrency. The challenge at the heart of this study, which is how centralised regulatory institutions can govern technologies that are built to be decentralised, is not unique to blockchain. It will arise again with artificial intelligence, with platform businesses, and with digital identity systems. The adaptive layer built into Echelon 5 which creates a mechanism for regulators to learn from experience and update their approach as evidence accumulates, is not just a feature of this model. It is a design principle that future researchers could apply wherever regulation needs to keep pace with fast-moving technology.

7.5 CONCLUDING REMARKS

This study began with a question: how should South Africa regulate cryptocurrency for cross-border transfers? It has answered that question through careful analysis, three research sub-questions, and conversations with eight expert respondents, arriving at a central conclusion. That conclusion is that governing a decentralised technology like blockchain requires regulation that is thoughtful, flexible, and technically informed. The 5-Echelon model is the practical result. It is a clear, step-by-step pathway from reforming outdated laws to building a regulatory system capable of learning and adapting over time.

The overall conclusion is one of genuine possibility. South Africa has more going for it than is often recognised. The IFWG already brings the key regulatory bodies together. Project Khokha proved that blockchain can work for financial settlement in a South African context. The FSCA has started bringing crypto-asset service providers within the regulatory perimeter. And the real, pressing need to reduce the cost of remittances across the SADC region gives the entire project a human purpose that goes beyond regulatory theory. The pieces are largely in place. What is needed now is the commitment to act and to prioritise the reforms, fund them properly, and see them through.

The goal is not to replace South Africa's existing financial system. It is to make blockchain a working part of it where it is integrated thoughtfully, governed well, and

developed through honest and ongoing collaboration between regulators, businesses, and the communities they serve. This study's most important finding may be the simplest one which is that good regulation and good innovation are not enemies. They need each other. Building a financial system in which both can thrive together is not only possible for South Africa, with everything it has to offer and everything it stands to gain, it is the only approach worth pursuing.

REFERENCES

- Adegoke, Y. (2018, April 12). Moving cash within Africa is the untapped opportunity for money transfer firms. Quartz Africa. <https://qz.com/africa/1249472>
- Adu, E. (2023). Digital currencies and regulatory sandboxes in sub-Saharan Africa: Opportunities for cross-border innovation. *Journal of African Business*, 24(3), 371–390.
- African Development Bank (AfDB). (2024). Digital Financial Services and Fintech in Africa: Trends, Opportunities and Challenges. African Development Bank Group Economic Report. <https://www.afdb.org>
- Ahiabenu, K. (2022). A critical analysis of the regulatory framework for the financial technology (FinTech) sector in Ghana. *African Journal of Business and Economic Research*, 17(2), 109–128.
- Alharby, M., & van Moorsel, A. (2018). Blockchain-based smart contracts: A systematic mapping study. *Computer Science Review*, 30(1), 100–125.
- Antonopoulos, A. M. (2017). *Mastering Bitcoin: Unlocking Digital Cryptocurrency*. (2nd ed.). O'Reilly Media
- Arner, D. W., Barberis, J. N., & Buckley, R. P. (2017). FinTech, RegTech and the Reconceptualisation of Financial Regulation. *Northwestern Journal of International Law & Business*, 37(3), 371–413.
- Arner, D. W., Barberis, J. N., & Buckley, R. P. (2017). Fintech and RegTech: Impact on regulators and banks. *Journal of Banking Regulation*, 19(4), 1–14.
- Arner, D. W., Barberis, J., & Buckley, R. P. (2015). The evolution of Fintech: A new post-crisis paradigm? *Georgetown Journal of International Law*, 47(4), 1271–1319.
- Arner, D. W., Barberis, J. N., & Buckley, R. P. 2016. The evolution of Fintech: A new post-crisis paradigm? *Georgetown Journal of International Law*, 47(4), 1271–1319.
- Arner, D. W., Barberis, J. N., & Buckley, R. P. (2017a). FinTech, RegTech and the reconceptualisation of financial regulation. *Northwestern Journal of International Law & Business*, 37(3), 371–413.
- Arner, D. W., Barberis, J. N., & Buckley, R. P. (2017b). Fintech and RegTech: Impact on regulators and banks. *Journal of Banking Regulation*, 19(4), 1–14.
- Arner, D. W., Buckley, R. P., Zetsche, D. A., & Barberis, J. N. (2018). Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation. *Fordham Journal of Corporate & Financial Law*, 23(1), 31–103.

Arner, D. W., Buckley, R. P., Zetsche, D. A., & Veidt, R. (2019). The Future of Data-Driven Finance and RegTech: Lessons from EU Big Bang II. ECGI Working Paper Series in Law.

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts (SoK). In Principles of Security and Trust (POST 2017), Lecture Notes in Computer Science, 10204, 164–186. Springer

Atzori, M. (2015). Blockchain Technology and Decentralised Governance: Is the State Still Necessary? SSRN Working Paper. <https://doi.org/10.2139/ssrn.2709713>

Auer, R., & Böhme, R. (2020). The technology of retail central bank digital currency. BIS Quarterly Review, March, 85-100.

Auer, R., & Claessens, S. (2018). Regulating cryptocurrency: Assessing market reactions. BIS Quarterly Review, September, 51-65.

Auer, R., Cornelli, G., & Frost, J. (2021). Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies. BIS Working Papers No. 880. Bank for International Settlements

Avgouleas, E., 2015. *Governance of Global Financial Markets*. Cambridge University Press.

Ayres, I. and Braithwaite, J., 1992. *Responsive Regulation*. Oxford University Press.

Baldwin, R., Cave, M., & Lodge, M. (2012). Understanding regulation: Theory, strategy, and practice (2nd ed.). Oxford University Press.

Bank of Ghana. (2021). Mobile Money Interoperability Reports. Accra: Bank of Ghana.

Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012). Bitter to better, how to make bitcoin a better currency. International Conference on Financial Cryptography and Data Security (pp. 399-414). Springer.

Basel Committee on Banking Supervision (BCBS). (2023). Prudential Treatment of Crypto-Asset Exposures: Final Standard. Bank for International Settlements. <https://www.bis.org/bcbs/publ/d545.htm>

Baur, D. G., Hong, K., & Lee, A. D. (2018). Bitcoin: Medium of exchange or speculative assets? Journal of International Financial Markets, Institutions and Money, 54, 177-189.

Beck, T. (2016). Finance, Growth, and Stability: Lessons from the Crisis. Journal of Financial Stability, 10(4), 1-9.

Becker, G., 1983. A theory of competition among pressure groups. *Quarterly Journal of Economics*, 98(3), pp.371–400.

BIS. (2022). Cyber security in the financial sector. BIS Annual Economic Report, Chapter III. Bank for International Settlements

BIS (2023) Prudential Treatment of Crypto-Asset Exposures

Biswas, A., Deb, A., Das, S., & Ahamed, S. F. (2020). Blockchain-Based Remittance Systems: A Systematic Review. *Future Internet*, 12(4), 65.

Black, J. (2002). Regulatory conversations. *Journal of Law and Society*, 29(1), 163-196.

Black, J., 2005. The emergence of risk-based regulation. *Public Law*, Autumn, pp.512–549.

Booth, A., Sutton, A., & Papaioannou, D. (2016). *Systematic Approaches to a Successful Literature Review* (2nd ed.). SAGE Publications.

Botha, M. (2020). Cryptocurrency and regulation in South Africa: The regulatory dilemmas of disruptive technology. *SA Financial Journal*.

Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment. IMF Working Paper WP/18/143. International Monetary Fund

Braithwaite, J., 2008. *Regulatory Capitalism*. Edward Elgar.

Brummer, C., 2015. *Soft Law and the Global Financial System*. Cambridge University Press.

Brincker, E. N. (2020). Cryptocurrency - a new frontier for South African tax law. *Journal of the South African Institute of Professional Accountants*, 3(1), 12-18.

Brous, P., Janssen, M., & Herder, P. (2019). The dual effects of blockchain on institutional trust and efficiency. *Information Systems Frontiers*, 23(8), 33–51.

Brummer, C. (2015). Disruptive technology and securities regulation. *Fordham Law Review*, 84(3), 977-1052.

Brummer, C. (2020). *Fintech Law in a Nutshell*. West Academic Publishing.

Brummer, C., & Yadav, Y. (2019). Fintech and the innovation trilemma. *Georgetown Law Journal*, 107(2), 235-307.

Bryman, A. (2012). *Social research methods* (4th ed.). Oxford University Press.

Bryman, A., & Bell, E. (2019). *Business Research Methods*. Oxford University Press.

- Buckley, R.P., Arner, D.W. and Zetsche, D.A., 2023. *FinTech: Finance, Technology and Regulation*. Cambridge University Press.
- Budiman, A., & Connor, P. (2019). Immigrants sent a record amount of money home to sub-Saharan African countries in 2017. Pew Research.
- Calliess, G. P., & Zumbansen, P. (2010). *Rough consensus and running code: A theory of transnational private law*. Hart Publishing.
- Cane, P., & Kritzer, H. M. (Eds.). (2010). *The Oxford handbook of empirical legal research*. Oxford University Press.
- Carlisle, D., & Hernández, K. (2022). Regulating cryptocurrency: Assessing market reactions to the Financial Action Task Force's guidance. *Journal of Financial Crime*, 29(3), 912-929.
- Carson, B., Romanelli, G., Walsh, P., & Zhumaev, A. (2018). Blockchain beyond the hype: What is the strategic business value? McKinsey & Company Digital. <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype>
- Casino, F., Dasaklis, T., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues.
- Catalini, C., & Gans, J. S. (2016). *Some Simple Economics of the Blockchain*. MIT Sloan Research Paper No. 5191-16.
- CBK (Central Bank of Kenya). (2022). *Innovation Sandbox Report*. Nairobi: CBK.
- CBN (Central Bank of Nigeria). (2021). *Payments System Vision 2025*. Abuja: Central Bank of Nigeria.
- Chainalysis. (2021). *The 2021 Geography of Cryptocurrency Report: Analysis of Cross-Border Cryptocurrency Flows*. Chainalysis Inc.
- Chainalysis. (2023). *The 2023 Crypto Crime Report*. Chainalysis Inc
- Chiu, J., Koeppl, T., & Li, Y. (2018). Blockchain as a confidence machine: The problem of trust and challenges of governance. *Journal of Economic Perspectives*, 32(2), 125-146.
- Chishti, S., & Gilitschenski, S. (2018). Legal tender status and the regulation of Bitcoin: A comparative analysis. *Journal of Financial Regulation and Compliance*, 26(2), 261-278.

Claessens, S., & Kodres, L. (2014). The Regulatory Responses to the Global Financial Crisis: Some Uncomfortable Questions. IMF Working Paper.

Claessens, S., & Rojas-Suarez, L. (2016). Financial regulations for improving financial inclusion. Washington, DC: Center for Global Development.

Classen, S. et al. (2008). 'Psychometric testing of SPIDER', Occupational Therapy Journal, 15(3), pp. 120–134.

CMS. (2025). EU Final Regulatory Technical Standards on MiCA. CMS Law-Now. Retrieved May 2026, from <https://cms-lawnow.com/en/ealerts/2025/mica-regulatory-technical-standards>

Coase, R. H. (1937). The Nature of the Firm. *Economica*, 4(16), 386-405.

Coglianese, C. (2012). Measuring regulatory performance: Evaluating the impact of regulation and regulatory policy. OECD.

Coglianese, C., Kilmartin, H., & Mendelson, E. (2009). Transparency and public participation in the federal rulemaking process: Recommendations for the new administration. *George Washington Law Review*, 77(4), 924-972.

Competition Commission. (2021). Market Inquiry into Online Platforms and Fintech Services. Pretoria: Competition Commission.

Cong, L., & He, Z. (2019). Blockchain Disruption and Smart Contracts. *The Review of Financial Studies*, 32(5), 1754-1797.

Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). Blockchain for the internet of things: A systematic literature review. *IEEE/ACS 13th International Conference on Computer Systems and Applications (AICCSA)* (pp. 1-6). IEEE.

Cooke, A., Smith, D., & Booth, A. (2012). Beyond PICO: The SPIDER Tool for qualitative evidence synthesis. *Qualitative Health Research*, 22(10), 1435-1443.

CPMI-IOSCO. (2022). Application of the Principles for Financial Market Infrastructures to stablecoin arrangements. Committee on Payments and Market Infrastructures and Board of the International Organisation of Securities Commissions

Creswell, J. W. (2013). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). SAGE Publications.

Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods Approaches. SAGE Publications.

Creswell, J. W., and Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches. 5th edition. Los Angeles: SAGE Publications.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain Technology: Beyond Bitcoin. *Appl. Innovation* 2, 71.

Currency and Exchanges Manual for Authorised Dealers. (2022). Pretoria: South African Reserve Bank.

Davidson, S., De Filippi, P., and Potts, J. (2018). Blockchains and the Economic Institutions of Capitalism. *Journal of Institutional Economics*, 14(4), 639-658.

Davidson, S., De Filippi, P., and Potts, J. (2018). Economics of Blockchain. SSRN Electronic Journal.

Davidson, S., Potts, J., & Yuma, N. (2016). Institutional Cryptoeconomics. SSRN Electronic Journal.

De Filippi, P. and Wright, A. (2018). Blockchain and the law. Cambridge, MA: Harvard University Press

De Koker, L., & Symington, J. (2011). Taming the cowboys: Enhancing supervision of the money remittance industry. *Journal of Money Laundering Control*, 14(3), 231-271.

De Vaus, D. A. (2002). Research design in social research. SAGE Publications.

Deloitte. (2020). Blockchain and financial regulation: A global perspective. London: Deloitte Insights.

Demirgüç-Kunt, A., Klapper, L., Singer, D., & Ansar, S. (2021). The Global Findex Database.

Dhillon, V., Metcalf, D., & Hooper, M. (2017). Blockchain Enabled Applications. Apress

Dilip, R., et al. (2011). Leveraging Migration for Africa Remittance, Skills, and Investments. Washington: The World Bank.

DiMaggio, P.J. and Powell, W.W., 1983. The iron cage revisited. *American Sociological Review*, 48(2), pp.147–160.

Dixon-Woods, M., Agarwal, S., Jones, D., Young, B., & Sutton, A. (2006) Synthesising qualitative and quantitative evidence: A review of possible methods. *Journal of Health Services Research & Policy*, 10(1), 45–53.

Dlamini, T., & Makaniska, S. (2023). Digital identity gaps and interoperability prospects in Southern Africa. *South African Journal of Information Management*, 25(1), 80–95.

Donovan, K.P. (2012). Mobile money, more freedom? The impact of M-Pesa's network power on development as freedom. *International Journal of Communication*, 6(1), 2647–2669.

Durand, J., Kandel, W., Parrado, E., & Massey, D. (1996). International Migration and Development in Mexican Sending Communities. *Demography*.

ESMA. (2025). Markets in Crypto-Assets Regulation Overview.

European Central Bank (ECB). (2023). Cryptocurrency Adoption and Transaction Patterns in the Euro Area. ECB Occasional Paper Series.

European Commission. (2020). Markets in Crypto-Assets Regulation (MICA).

European Commission. (2020). Proposal for a Regulation on Markets in Crypto-assets (MICA). COM(2020) 593 final.

European Securities and Markets Authority (ESMA). (2024). Technical Standards under the Markets in Crypto-Assets Regulation (MiCA). ESMA Guidelines.

European Union. (2023). Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MICA). Official Journal of the European Union.

Eyal, I., & Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In *Financial Cryptography and Data Security: 18th International Conference, FC 2014, LNCS 8437*, 436–454. Springer

Fan, J., Wang, Z., Zhang, K., & Li, S. (2021). Blockchain technology adoption in supply chain management: A systematic literature review and future research agenda. *Journal of Cleaner Production*, 289, 125533.

FATF, 2014. Guidance for a Risk-Based Approach to Virtual Currencies. Paris: FATF.

FATF, 2019. Guidance for a Risk-Based Approach to Virtual Assets and VASPs. Paris: FATF.

FATF (2021) Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs

FSB (2023) Global Regulatory Framework for Crypto-Asset Activities

Financial Action Task Force (FATF). (2019). Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. FATF, Paris.

Financial Action Task Force (FATF). (2021). Guidance on Virtual Assets and Virtual Asset Service Providers.

Financial Action Task Force (FATF). (2021). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. FATF/OECD.

<https://www.fatfgafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html>

Financial Action Task Force [FATF]. (2021). Anti-money laundering and counter-terrorist financing measures: South Africa mutual evaluation report. FATF.

Financial Action Task Force. (2012). International standards on combating money laundering and the financing of terrorism & proliferation: The FATF Recommendations. Paris: FATF.

Financial Advisory and Intermediary Services Act. (2002). Act No. 37 of 2002, South Africa.

Financial Conduct Authority (FCA). (2021). The Regulatory Sandbox: Lessons Learned.

Financial Intelligence Centre Act. (2001). Act No. 38 of 2001, South Africa.

Financial Intelligence Centre Amendment Act. (2022). Act No. 1 of 2022, South Africa.

Financial Intelligence Centre. (2023). Guidance Note 1 of 2023: Guidance for crypto asset service providers. Pretoria: Financial Intelligence Centre.

Financial Intelligence Centre. (2023). Guidance Note 7: Guidance for accountable institutions on reporting obligations. Pretoria: Financial Intelligence Centre.

Financial Markets Act. (2012). Act No. 19 of 2012, South Africa.

Financial Sector Conduct Authority (FSCA). (2022). Fintech Regulatory Guidelines on Innovation and Market Conduct. Pretoria: FSCA.

Financial Sector Conduct Authority [FSCA]. (2023). Regulatory framework for crypto asset service providers. Position Paper 1 of 2023.

Financial Sector Conduct Authority. (2018). Strategic plan 2018-2021. Pretoria: Financial Sector Conduct Authority.

Financial Sector Conduct Authority. (2022). Position Paper 1 of 2022: Crypto assets. Pretoria: Financial Sector Conduct Authority.

Financial Sector Regulation Act. (2017). Act No. 9 of 2017, South Africa.

Financial Stability Board [FSB]. (2020). Regulation, supervision and oversight of "global stable-coin" arrangements. FSB.

Financial Stability Board [FSB]. (2022). Assessment of risks to financial stability from crypto assets. FSB.

FinMark Trust. (2023). Mobile Money in South Africa: Policy Insights and Market Gaps. Johannesburg: FinMark Trust.

Foley, S., Karlsen, J. R., & Putnins, T. J. (2018). Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrency? *Review of Financial Studies*.

Fosvang, C., & Varberg, D. (2014). Cryptocurrency: An exploratory study of cryptocurrency and the drivers. IT University of Copenhagen, Copenhagen, Denmark.

Gago, J. (2019). Crypto-Based Transfers Can Cut Cross-border payments Costs in Africa by 90%. Bitcoin.

Gai, K., Qiu, M., & Sun, X. (2018). A Survey on FinTech. *Journal of Network and Computer Applications*, 103, 262-273.

Genesis Analytics. (2018). Review of the regulatory framework for money remittances. Johannesburg: Genesis Analytics.

Gilardi, F. (2010). Who learns from what in policy diffusion processes? *American Journal of Political Science*, 54(3), 650-666.

Gillwald, A. (2023). Digital Inequality Paradox: Policy Perspectives on South Africa's Digital Economy. Johannesburg: Research ICT Africa.

Gillwald, A., & Van der Spuy, A. (2022). Structural barriers to policy integration in Africa's digital governance systems. *Digital Policy, Regulation and Governance*, 24(1), 23–45.

Godwin, A., & Ramsay, I. (2015). Twin Peaks regulation of financial services in Australia. *Annals of Corporate Governance*, 1(2), 569-651.

Goforth, C. (2021). The Regulation of Cryptocurrency in the United States.

- Gomber, P., et al. (2018). The FinTech Revolution. *Journal of Management Information Systems*, 35(1), 220-265.
- Gorton, G., & Zhang, J. (2023). Taming wildcat stablecoins. *University of Chicago Law Review*, 90(2), 409–456
- Granovetter, M. (1985). Economic Action and Social Structure: The Problem of Embeddedness. *American Journal of Sociology*, 91(3), 481-510.
- Gregor, S., & Jones, D. (2007). The anatomy of a design theory. *Journal of the Association for Information Systems*, 8(5), 312–335.
- Gunningham, N. (2019). Averting regulatory failure: Emerging lessons from COVID-19. *Regulation & Governance*, 13(4), 679–693.
- Gupta, M. (2021). *Blockchain for dummies* (2nd ed.). Wiley.
- Gupta, S. (2009). Effect of Remittances on Poverty and Financial Development in Sub-Saharan Africa. *Journal of World Development*, 37(1), 104-115.
- Hacker, P., & Thomale, C. (2018). Crypto-securities regulation: ICOs, token sales and cryptocurrency under EU financial law. *European Company and Financial Law Review*, 15(4), 645-696.
- Hanisch, M. (2023). Digital governance: A conceptual framework and research agenda. *Telecommunications Policy*, 47(5), 1–17.
- He, D., Habermeier, K., Leckow, R., Haksar, V., Almeida, Y., Kashima, M., ... & Verdugo-Yepes, C. (2016). *Virtual currencies and beyond: Initial considerations*. Washington, DC: International Monetary Fund.
- Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 28(1), 75–105.
- Hildebrandt, M. (2015). *Smart technologies and the end(s) of law: Novel entanglements of law and technology*. Edward Elgar Publishing.
- Hileman, G., & Rauchs, M. (2017). *Global Blockchain Benchmarking Study*.
- Hood, C., Rothstein, H., & Baldwin, R. (2001). *The government of risk: Understanding risk regulation regimes*. Oxford University Press.

- Hossain Rubel, M. T., Emran, A. K. M., Islam, M. K., Nayem, M. A. I., & Hasan, S. K. (2025). From ledger to ledgerless: Evaluating blockchain-driven real-time financial reconciliation in U.S. public companies. *International Journal of Financial Management and Research*.
<https://www.ijfmr.com/papers/2025/4/49709.pdf>
- Houben, R., & Snyers, A. (2018). *Cryptocurrency and blockchain: Legal context and implications for financial crime*.
- Houben, R., & Snyers, A. (2020). *Crypto-assets: Key developments, regulatory concerns and responses*. Brussels: European Parliament.
- Iansiti, M., & Lakhani, K. (2017). *The Truth about Blockchain*. Harvard Business Review.
- IBM. (2026). *Fueling the financial industry with open-source cross-border payments*.
<https://www.ibm.com/think/topics/cross-border-payments-blockchain>.
- IFWG (Intergovernmental Fintech Working Group). (2022). *Position Paper on Crypto Assets and Innovation*. Pretoria: IFWG.
- IFWG. (2020). *Crypto Assets Regulatory Working Group Position Paper*.
- IMF (2022) *Crypto Assets and Capital Flow Management*
- Income Tax Act. (1962). Act No. 58 of 1962, South Africa.
- InnReg. (2025). *MiCA Regulation Guide*.
- Intergovernmental Fintech Working Group (IFWG). (2020). *Crypto Assets Regulatory Working Group Position Paper*. South African Reserve Bank, Pretoria.
- Intergovernmental Fintech Working Group (IFWG). (2022). *Regulatory Sandbox: Annual Report*. South African Reserve Bank, Pretoria.
- Intergovernmental Fintech Working Group. (2020). *Position Paper on Crypto Assets*. Pretoria: National Treasury.
- International Finance Corporation. (2014). *Digital Access: The Future of Financial inclusion in Africa*.
- International Finance Corporation. (2017). *Mobile Money Offers Africans a Financial Future*.

International Monetary Fund (IMF). (2020). Blockchain and Financial Inclusion in Emerging Markets.

International Monetary Fund (IMF). (2022). Crypto Assets and Capital Flow Management. IMF Policy Paper No. 2022/031. International Monetary Fund. <https://www.imf.org/en/Publications/Policy-Papers/Issues/2022/07/29/Crypto-Assets-and-Capital-Flow-Management-521025>

International Monetary Fund (IMF). (2023). Stablecoins in Emerging Markets: Risks and Policy Considerations. IMF Working Paper WP/23/145.

International Monetary Fund. (2023). Global financial stability report: Financial and climate policies for a high-interest-rate era. Washington, DC: IMF.

ITU (International Telecommunication Union). (2022). Global Mobile Money Policy and Regulatory Frameworks. Geneva: United Nations.

Jack, W., & Suri, T. (2016). The long-run poverty and gender impacts of mobile money. *Science*, 354(6317), 1288–1292.

Johnson, T.N. (2025). Effective Business Strategies and Regulatory Compliance Within Fintechs: A Qualitative Pragmatic Inquiry Study. Minneapolis: Walden University.

Kaal, W. A. (2020). Crypto transaction dispute resolution. *Business Lawyer*, 73(1), 109-152.

Kannenberger, C. (2016). Bitcoin and the South African income tax act: Suggestions for improvement. *Stellenbosch Law Review*, 27(2), 380-398.

Kirsten, M. (2019). The introduction of Twin Peaks in South Africa: Lessons from Australia. *South African Journal of Economic and Management Sciences*, 22(1), a2710.

Koomson, I., & Bukari, C. (2020). Regulating mobile money services and financial inclusion in Ghana: Insights from Unified Theory of Acceptance and Use of Technology. *Telecommunications Policy*, 44(7), 101980.

Kopf, D. (2018). Remittances to Africa cost far too much, more competition would change that. *QZ*.

KPMG. (2020). Blockchain and Data Privacy: The Regulatory Challenges.

Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting and payments. *IEEE Software*, 35(4), 95–99.

Kachingwe, N., & Marco, N. (2019). What's holding back digital disruption in remittances in Southern Africa? Working Paper.

Larkin, J. H., & Simon, H. A. (1987). Why a diagram is (sometimes) worth ten thousand words. *Cognitive Science*, 11(1), 65-100.

Lessig, L., 1999. *Code and Other Laws of Cyberspace*. Basic Books.

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gotzsche, P. C., Ioannidis, J. P. A., Clarke, M., Devereaux, P. J., Kleijnen, J., & Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health-care interventions: Explanation and elaboration. *PLOS Medicine*, 6(7), e1000100.

Liu, D., Xie, S., Li, X., & Deng, Y. (2019). From blockchain technology to smart health applications: Current perspectives.

Magner, N. (2021). The taxation of cryptocurrency in South Africa: A proposal for an adapted capital gains tax model. *Obiter*, 42(2), 368-391.

Magnuson, W. (2018). Regulating fintech. *Vanderbilt Law Review*, 71(4), 1167-1226.

Maloumy-Baka, R., & Kingombe, C. (2016). The Quest to Lower High Remittance Costs to Africa: A Brief Review of the Use of Mobile Banking and Bitcoins (2nd Version).

Malterud, K., Siersma, V.D., & Guassora, A.D. (2016). Sample size in qualitative interview studies: Guided by information power. *Qualitative Health Research*, 26(13), 1753–1760.

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, 15(4), 251–266.

Masciandaro, D., & Quintyn, M. (2016). The governance of financial supervision: Recent developments. *Journal of Economic Surveys*, 30(5), 982-1006.

McKenzie, B. (2018). Blockchain and Cryptocurrency in Africa.

McCorry, P., Hicks, A., & Meiklejohn, S. (2021). Smart contracts for bribing miners. In *Financial Cryptography and Data Security*, LNCS 10957. Springer

Methley, et al. (2014). PICO, PICOS and SPIDER: a comparison study of specificity and sensitivity in three search tools for qualitative systematic reviews. *BMC Health Services Research*.

Miridzhanian, A. (2022). South Africa moves to regulate crypto assets. *Reuters*.

Mohapatra, S. (2011). Remittance Markets in Africa. *World Bank Journal of Directions in Development*.

Monetary Authority of Singapore (MAS). (2019). Payment Services Act 2019. MAS, Singapore.

Monetary Authority of Singapore (MAS). (2020). Project Ubin Phase 5: Enabling Broad Ecosystem Opportunities. MAS and Accenture.

Monetary Authority of Singapore (MAS). (2023). Proposed Regulatory Framework for Stable-coin-Related Activities: Consultation Paper. MAS, Singapore.

Money Laundering and Terrorist Financing Control Regulations. (2002). Government Gazette No. 23496, South Africa.

Moore, T., & Christin, N. (2013). Beware the middleman: Empirical analysis of Bitcoin-exchange risk. In *Financial Cryptography and Data Security*, LNCS 7859, 25–33. Springer

Moshi, G. C., & Mutimukwe, C. (2020). Effective regulation of mobile money in Tanzania and Uganda: Lessons for other developing countries. *Journal of African Law*, 64(1), 81-103.

Moyo, T., & Munyoka, W. (2022). Regulatory fragmentation in Africa's financial sectors: Implications for fintech innovation. *African Journal of Economic Policy*, 29(1), 131–155.

Mutlaq, N. (2020). A blockchain-based mobile money interoperability scheme. *International Journal of Advanced Computer Science and Applications*, 11(1), 134–143.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.

Narula, R. (2020). Enabling the poor through fintech and frugal innovation. *Oxford Development Studies*, 48(1), 1-11.

National Payment System Act. (1998). Act No. 78 of 1998, South Africa.

National Treasury, Republic of South Africa. (2014). Implementing a Twin Peaks model of financial regulation in South Africa. National Treasury.

National Treasury. (2011). A safer financial sector to serve South Africa better. Pretoria: National Treasury.

National Treasury. (2022). 2022 Budget Review. Pretoria: National Treasury.

Njoroge, D. (2018). The PesaLink Model: Bank-Led Interoperability in Kenya. Nairobi: Kenya Bankers Association.

North, D.C. (1990). *Institutions, Institutional Change and Economic Performance*. Cambridge: Cambridge University Press.

North, D.C. (2005). *Understanding the Process of Economic Change*. Princeton: Princeton University Press.

Norton Rose Fulbright. (2024). *Regulating Crypto-Assets in Europe: Practical Guide to MiCA*.

Noveck, B. S. (2009). *Wiki government: How technology can make government better, democracy stronger, and citizens more powerful*. Brookings Institution Press.

OECD. (2020). *Crypto Assets in Financial Markets: Understanding the Risks and Regulatory Approaches*.

OECD. (2020). *Taxing virtual currencies: An overview of tax treatments and emerging tax policy issues*. Paris: OECD Publishing.

Ogunleye, S. (2022). Central bank digital currencies and interoperability in Nigeria's payment systems. *Digital Economy Journal*, 4(2), 45–63.

Owusu-Antwi, G., & Bekoe, A. (2022). Evaluating the socio-economic impact of Ghana's mobile money interoperability initiative. *Financial Innovation*, 8(1), 51–64.

Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review*, 18(4), 329-340.

Paulet, E. (2017). Governing shadow banking in the age of big data: Cyber-risk and the limits of financial regulation. *Journal of Banking Regulation*, 18(4), 310-329.

Peppers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3), 45–77.

Peltzman, S., 1976. Toward a more general theory of regulation. *Journal of Law and Economics*, 19(2), pp.211–240.

Philippon, T. (2020). *On fintech and financial inclusion*. Monetary and Economic Department.

Pieters, G., & Vivanco, S. (2017). Financial regulations and price inconsistencies across Bitcoin markets. *Information Economics and Policy*, 39, 1-14.

Pigou, A.C., 1938. *The Economics of Welfare*. Macmillan.

Pilkington, M. (2016). Blockchain technology: Principles and applications. Research Handbook on Digital Transformations.

Polanyi, K. (1944). The Great Transformation. Beacon Press.

Posner, R.A., 1974. Theories of economic regulation. *Bell Journal of Economics*, 5(2), pp.335–358.

Power, M., 2007. *Organized Uncertainty*. Oxford University Press.

Rameshar, R., & Mwencha, P. (2021). Regulation of cross-border mobile money transfers in the East African Community. *International Journal of Law and Management*, 63(3), 289-305.

Raskin, M., & Yermack, D. (2016). Digital Currencies, Decentralised Ledgers and the Future of Central Banking. NBER Working Paper No. 22238.

Ratha, D., De, S., Kim, E. J., Plaza, S., Seshan, G., & Yameogo, N. D. (2019). Migration and remittances: Recent developments and outlook. Washington, DC: World Bank.

Rauchs, M., Glatz, P., Knottenbelt, W.J., & Pieters, G.C. (2018). Distributed Ledger Technology Systems: A Conceptual Framework. Cambridge: Cambridge Centre for Alternative Finance.

Rella, L. (2019). Blockchain Technologies and Remittances: From Financial Inclusion to Correspondent Banking.

Reuters. (2022). SARB warns on crypto risks to monetary policy.

Rise, D. (2017). Here's How Blockchain Will Eliminate Banks and Democratize Money.

Rogers, E. M. (2003). *Diffusion of Innovations* (5th ed.). Free Press, New York.

Sabilika, K. (2025). Digital Payments in Africa: Can Regulation Keep up With the Rapid Innovation?.

Samuelson, P.A., 1947. *Foundations of Economic Analysis*. Harvard University Press.

Santander InnoVentures, Oliver Wyman, & Anthemis Group. (2015). The Fintech 2.0 Paper: Rebooting financial services.

SARB (South African Reserve Bank). (2021). Vision 2025: An Inclusive National Payment System. Pretoria: South African Reserve Bank.

SARB, 2022. *Financial Stability Review*. Pretoria: South African Reserve Bank.

Schär, F. (2021). Decentralised Finance: On Blockchain- and Smart Contract-Based Financial Markets. Federal Reserve Bank of St. Louis Review.

Schär, F. (2021). Decentralised finance: On blockchain- and smart contract-based financial markets. Federal Reserve Bank of St. Louis Review, 103(2), 153-174.

Schmulow, A. (2015). The four standards of financial sector regulation: When and why they matter. Journal of Financial Regulation and Compliance, 23(4), 387-400.

Schumpeter, J. A. (1942). Capitalism, socialism and democracy. Harper & Brothers.

Scott, W.R., 2001. *Institutions and Organizations*. Sage.

Scott, W.R. (2008). Institutions and Organizations: Ideas and Interests (3rd edn.). Thousand Oaks: Sage.

Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R. (2011). Action design research. MIS Quarterly, 35(1), 37–56

Serfontein, R., & De Vries, J. (2019). Exchange control regulations and cryptocurrency in South Africa: A legal perspective. South African Mercantile Law Journal, 31(3), 378-395.

Shah, R., & Chitnis, K. (2016). Digital Financial Inclusion: How Mobile Money, Mobile Phones, and Cryptocurrency are Changing Africa. Journal of Payments Strategy & Systems, 10(4), 351–.

Sibanda, N. (2023). Policy challenges for digital payments interoperability in sub-Saharan Africa. Telecommunications Policy, 47(9), 1–16.

Smit, B. W., & Mocke, B. A. (2014). The evolution of South Africa's exchange control system. South African Journal of Economic History, 29(1), 72-103.

Sonnenberg, C., & vom Brocke, J. (2012). Evaluations in the science of the artificial – Reconsidering the build–evaluate pattern in design science research. In DESRIST 2012, pp. 381–397. Springer.

South African Banking Risk Information Centre (SABRIC). (2023). Annual Crime Statistics Report 2022. SABRIC

South African Reserve Bank (SARB). (2018). Project Khokha: Exploring the Use of Distributed Ledger Technology for.

South African Reserve Bank (SARB). (2020). Position paper on crypto assets. SARB.

South African Reserve Bank (SARB). (2021). Position Paper on Crypto Assets.

South African Reserve Bank (SARB). (2022). Project Khokha II Final Report.

South African Reserve Bank (SARB). (2023). Financial Stability Review: First Edition 2023. SARB

South African Reserve Bank Act. (1989). Act No. 90 of 1989, South Africa.

South African Reserve Bank. (2014). Position Paper 02 of 2014: Virtual currencies. Pretoria: South African Reserve Bank.

South African Reserve Bank. (2018). Project Khokha: Exploring the use of distributed ledger technology for interbank payments settlement in South Africa. Pretoria: South African Reserve Bank.

South African Reserve Bank. (2020). Guidance Note 3 of 2020: Implementation of Recommendations of the Crypto Assets Regulatory Working Group. Pretoria: South African Reserve Bank.

South African Reserve Bank. (2020). Position Paper: Regulatory and supervisory framework for the National Payment System. Pretoria: South African Reserve Bank.

South African Reserve Bank. (2021). Cyber and information security framework for the South African National Payment System. Pretoria: South African Reserve Bank.

South African Reserve Bank. (2021). Vision 2025. Pretoria: South African Reserve Bank.

South African Reserve Bank. (2022). Guidance Note 8 of 2022: Authorisation as an Authorised Dealer with Limited Authority. Pretoria: South African Reserve Bank.

South African Reserve Bank. (2025). Directive No. 1 of 2025: Low-value cross-border electronic funds transfers within the Common Monetary Area. Pretoria: South African Reserve Bank.

South African Revenue Service. (2018). SARS's stance on the tax treatment of cryptocurrency. Pretoria: South African Revenue Service.

Squire Patton Boggs. (2025). MiCA Legal Framework – How to Comply.

Stander, L. (2021). Cryptocurrency and exchange control: The South African experience. *Journal of International Banking Law and Regulation*, 36(5), 201-213.

Stigler, G.J., 1971. The theory of economic regulation. *Bell Journal of Economics*, 2(1), pp.3–21.

Stokes, R. (2022). Regulating innovation: Adaptive governance for emerging technologies. *Science and Public Policy*, 49(8), 1102–1120.

Stoop, P. N. (2021). Bitcoin and South African law: Regulatory challenges and opportunities. *South African Law Journal*, 138(3), 574-602.

Stoop, P. N. (2023). Regulating crypto assets in South Africa: Mind the gap. *South African Mercantile Law Journal*, 35(1), 48-72.

Streeck, W., & Thelen, K. (2005). Introduction: Institutional change in advanced political economies. In W. Streeck & K. Thelen (Eds.), *Beyond continuity: Institutional change in advanced political economies* (pp. 1-39). Oxford University Press.

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. Sebastopol: O'Reilly Media.

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution*. Penguin.

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. Penguin.

Tapscott, D., & Tapscott, A. (2019). *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrency Is Changing the World*. London: Penguin.

Tasca, P., & Tessone, C. J. (2019). A Taxonomy of Blockchain Technologies: Principles of Identification and Classification. *Ledger*, 4.

Taylor, M. (1995). *Twin peaks: A regulatory structure for the new century*. Centre for the Study of Financial Innovation.

Tenorio, D. (2021). *Blockchain and property rights: Lessons from the developing world*. World Bank Policy Research Working Paper No. 9812.

Tobbin, P. (2013). Towards a model of adoption in mobile banking by the unbanked: A qualitative study. *International Journal of Bank Marketing*, 31(5), 305–325.

Tornatzky, L.G., & Fleischer, M. (1990). *The Processes of Technological Innovation*. Lexington: Lexington Books.

Treleaven, P., Gendal Brown, R., & Yang, D. (2017). Blockchain Technology in Finance. *Computer*, 50(9).

Tricco, A. C., Tetzlaff, J., & Moher, D. (2018). The art and science of knowledge synthesis. *Journal of Clinical Epidemiology*, 64(1), 11–20

Truby, J. (2018). Decarbonizing Bitcoin: Law and Policy Choices for Reducing the Energy Consumption of Blockchain Technologies and Digital Currencies. *Energy Research & Social Science*, 44, 399-410.

Tufte, E. R. (2001). *The visual display of quantitative information* (2nd ed.). Graphics Press.

Van Deventer, M. (2018). Why cryptocurrency such as Bitcoin should be regulated in South Africa. *Potchefstroom Electronic Law Journal*, 21(1), 1-24.

Van Zyl, C. (2018). Twin Peaks: South Africa's emerging financial regulatory framework and its fit with international financial standards. *Law, Democracy & Development*, 22(1), 281-308.

Van Zyl, S. P. (2021). The regulation of crypto assets in South Africa: A comparative analysis. *Potchefstroom Electronic Law Journal*, 24, 1-31.

Venable, J., Pries-Heje, J., & Baskerville, R. (2016). *FEDS*: A framework for evaluation in design science research. *European Journal of Information Systems*, 25(1), 77–89.

Vom Brocke, J., Hevner, A., & Maedche, A. (2020). Introduction to design science research. In J. Vom Brocke, A. Hevner, & A. Maedche (Eds.), *Design science research: Cases* (pp. 1-13). Cham: Springer.

Vom Brocke, J., Winter, R., Hevner, A., & Maedche, A. (2024). Dealing with complexity in design science research: A methodology using design echelons. *Journal of the Association for Information Systems*, 25(1), 1-31.

Walch, A. (2019). Deconstructing "Decentralisation": Exploring the Core Claim of Crypto Systems. In *Crypto Assets: Legal and Monetary Perspectives*.

Walch, A. (2019). Deconstructing "Decentralisation": Exploring the core claim of crypto systems. *Harvard Business Law Review*, 9, 85-118.

Weber, R.H., Staiger, D.N., Rinoldi, L., & Bonnet, C. (2016). Blockchain and algorithmic governance: Emerging regulatory frontiers. *Computer Law & Security Review*, 32(6), 115–126.

Wieringa, R. J. (2014). *Design science methodology for information systems and software engineering*. Springer

Williamson, O. E. (1985). *The Economic Institutions of Capitalism*. Free Press.

Wolman, H. (2018). Bitcoin: A taxing matter. *South African Law Journal*, 135(3), 544-574.

World Bank. (2019). Record high remittances sent globally in 2018.

World Bank. (2021). The Future of Cross-Border Payments: Blockchain and Beyond.

World Bank. (2022). Fintech and the Future of Payments in Africa. Washington, DC: World Bank.

Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. *Financial Innovation*, 5.

Yan, C., & Bellavitis, C. (2020). Blockchain disruption and decentralised finance: The rise of decentralised business models. *Journal of Business Venturing Insights*, 13.

Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance*, 21(1), 7–31.

Zamani, E. D., & Giaglis, G. M. (2018). With a little help from the regulators: The role of watchdogs in the adoption of blockchain-based systems. *Government Information Quarterly*, 35(3), 436–448.

Zavolokina, L., et al. (2019). The FinTech phenomenon: antecedents of financial innovation perceived by the popular press.

Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralised finance. *Journal of Financial Regulation*, 6(2), 172-203.

Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2020). Regulating LIBRA: The transformative potential of Facebook's cryptocurrency and possible regulatory responses. *European Banking Institute Working Paper Series*, 2019/45.

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2017). Regulating a revolution: From regulatory sandboxes to smart regulation. *Fordham Journal of Corporate & Financial Law*, 23(1), 31-103.

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2018). The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators. *Harvard International Law Journal*, 60(2), 267–309.

Zetzsche, D. A., et al. (2017). Regulating a Revolution. *Fordham Journal of Corporate & Financial Law*, 23(1), 31-103.

Zohar, A. (2015). Bitcoin: Under the Hood. *Communications of the ACM*, 58(9), 104-113.

APPENDIX A

Participant Information Sheet (PIS)

Dear Participant

My name is Craig Meyer, and I am currently pursuing a Master's degree in Integrated Digital Knowledge Economic Studies at the Wits University Link Centre. I am conducting research for my dissertation titled ***“Centralised Decentralisation: Investigating the Regulatory Challenges and Mitigations of a Cryptocurrency Solution for Cross-Border Transfers in South Africa”***

I am reaching out to request your permission and consent to participate in an interview as part of my study. My research seeks to explore the potential of blockchain technology in facilitating cross-border transfers while addressing regulatory challenges and developing effective mitigation strategies. Given your expertise in the financial regulatory field, your insights would be invaluable in contributing to a comprehensive understanding of this topic.

The interview will focus on the following areas:

1. Current practices and challenges in cross-border transfers
2. Regulatory frameworks and compliance requirements
3. Potential applications and benefits of blockchain technology
4. Concerns, risks, and challenges associated with implementing blockchain solutions
5. Strategies for mitigating regulatory hurdles and promoting adoption

The interview can be conducted at your convenience, either in person or via video conferencing. Rest assured that all information gathered will be treated with the utmost confidentiality and will be used solely for academic purposes. Participant anonymity will be maintained, and any sensitive information will be appropriately protected. Your participation would significantly contribute to the advancement of knowledge in this emerging field and potentially inform future policy and regulatory developments. Additionally, it would provide valuable insights for organisations looking to leverage blockchain technology while ensuring compliance with relevant regulations.

By participating in the interview, you agree to the following:

1. Participation is voluntary.
2. No remuneration will be provided.
3. Participation will remain anonymous.

I would be grateful if you could grant me permission to conduct the interview. Please let me know if you require any additional information or documentation to facilitate this process.

Thank you for considering my request. I look forward to your positive response.

Sincerely, Craig Meyer

Contact details of the student researcher: Mobile: 084 506 1701

Email: meyer.craig@gmail.com

Contact details of the supervisor: Dr Kiru Pillay Email: kiru2010@gmail.com

APPENDIX B

Participant Consent Form

Title of project:

Centralised Decentralisation: Investigating the Regulatory Challenges and Mitigations of a Cryptocurrency Solution for Cross-Border Transfers in South Africa

Name of researcher: Craig Rolando Meyer

Supervisor: Dr Kiru Pillay

Purpose of the Research:

The research aims to explore the potential of blockchain technology in facilitating cross-border transfers while navigating regulatory challenges and developing mitigating strategies.

I, ..., agree to participate in this research project.

I agree to the following:

(Please circle the relevant options below)

The research study was explained to me. I understand what this study is about.	YES	NO
I understand that I can volunteer to take part in the study.	YES	NO
I agree that the interview may be audio recorded.	YES	NO
I agree that direct quotations from my interview may be used by the researcher in their research report.	YES	NO
I agree that my participation will remain anonymous (my name or other identifying data will not be used by the researcher in their research report.	YES	NO

I agree that other researchers may use the information I provide in my interview (depending on their own ethics clearance being obtained) but my name and any personal information will not be used or passed on

YES

NO

..... (signature of participant)

..... (name of participant)

..... (date)

Craig Meyer

6 September 2024

APPENDIX C

Ethics Clearance Certificate



Research Office

HUMAN RESEARCH ETHICS COMMITTEE (NON-MEDICAL)
R14/49 Meyer

CLEARANCE CERTIFICATE

PROTOCOL NUMBER: H24/06/25

PROJECT TITLE

Centralised Decentralisation: Investigating the Regulatory Challenges and Mitigations of a Blockchain Solution on South African Cross-Border Transfers

INVESTIGATOR(S)

Mr C Meyer

SCHOOL/DEPARTMENT

Wits Link Centre/

DATE CONSIDERED

21 June 2024

DECISION OF THE COMMITTEE

Approved
Risk Level: Minimal

EXPIRY DATE

04 August 2024

DATE

05 August 2024

CHAIRPERSON

A handwritten signature in black ink, appearing to be "JW", written over a horizontal line.

(Professor J Watermeyer)

cc: Supervisor : Dr K Pillay and Prof L Abrahams

DECLARATION OF INVESTIGATOR(S)

To be completed in duplicate and **A SIGNED COPY** returned to the Secretary electronically. Unreported changes to the application may invalidate the clearance given by the HREC (Non-Medical)

I/We fully understand the conditions under which I am/we are authorized to carry out the abovementioned research and I/we guarantee to ensure compliance with these conditions. Should any departure be contemplated from the research procedure as approved I/we undertake to submit an amendment of the protocol to the Committee. **I/we agree to completion of a regular progress report. For Minimal and Low Risk studies, this is due annually on 31 December. For Medium and High Risk studies, this is due twice annually on 30 June and 31 December.**

Signature

____/____/____
Date

PLEASE QUOTE THE PROTOCOL NUMBER ON ALL ENQUIRIES

APPENDIX D

Interview Questions

Centralised Decentralisation: Investigating the Regulatory Challenges and Mitigations of a Blockchain Solution on South African Cross-Border Transfers

1. **What are the main regulatory challenges you see in implementing blockchain-based cross-border payment solutions in South Africa?**
 - This question seeks to identify key obstacles from a regulatory perspective.
2. **How do current South African financial regulations align with or conflict with the use of decentralized technologies like blockchain for cross-border transactions?**
 - Understanding the relationship between existing regulations and decentralized technologies is critical.
3. **What are the primary risks, such as money laundering or fraud, that regulators might associate with blockchain solutions in cross-border transfers, and how can these be mitigated?**
 - This focuses on regulatory concerns about risks and potential solutions.
4. **How do you view the role of centralized institutions (e.g., central banks, financial regulators) in overseeing decentralized blockchain systems?**
 - This helps explore the tension between centralized regulation and decentralized systems.
5. **What specific regulatory frameworks or policy adaptations do you believe are necessary to facilitate the legal use of blockchain for cross-border payments in South Africa?**
 - This question focuses on potential regulatory reforms.

6. **How does the regulatory landscape in South Africa compare to other regions that have adopted or are experimenting with blockchain for cross-border transfers?**
 - Comparing South Africa with other countries provides insights into global trends.
7. **What are the key compliance challenges that financial institutions face when trying to integrate blockchain technology into existing cross-border payment systems?**
 - This explores how traditional institutions deal with compliance issues related to blockchain.
8. **What role do you think public-private partnerships could play in developing a regulatory framework that supports blockchain-based cross-border payments?**
 - Understanding collaborative approaches to regulation is important for policy development.
9. **How can blockchain technology address existing inefficiencies or challenges in cross-border payments that traditional financial systems have failed to resolve?**
 - This focuses on blockchain's potential benefits within the current regulatory system.
10. **Do you foresee any ethical or legal dilemmas arising from the use of blockchain in cross-border transfers, and what measures can regulators implement to address these concerns?**

Addressing ethical and legal concerns helps evaluate the broader impact of blockchain adoption.