



UNIVERSITY OF THE WESTERN CAPE

FACULTY OF LAW

DEPARTMENT OF MERCANTILE AND LABOUR LAW

**CRYPTOCURRENCY INTERMEDIATION IN AFRICA: TOWARDS A
REGULATORY FRAMEWORK FOR CRYPTOCURRENCY
INTERMEDIARIES**

*UNIVERSITY of the
WESTERN CAPE*

Roswitha Mildred Melina Gomachas

Student Number: 3865684

Supervisor: Prof. Riekie Wandrag

**A mini-thesis submitted in partial fulfilment of the requirements for the LLM
Degree in International Trade, Business and Investment Law**

TABLE OF CONTENTS

PLAGIARISM DECLARATION	8
DEDICATION	9
ACKNOWLEDGEMENTS	10
KEYWORDS	11
CHAPTER 1: CRYPTOCURRENCY INTERMEDIATION IN AFRICA	
INTRODUCTION	12
1.1 Research Background.....	13
1.1.1 History and salient features of cryptocurrency.....	14
1.1.2 Examples of cryptocurrency.....	15
1.1.3 Acquiring cryptocurrency.....	16
1.1.4 The introduction of intermediation into the cryptocurrency environment.....	17
1.2 Research objective(s).....	19
1.3 Significance of the problem.....	20
1.4 Methodology.....	21
1.5 Overview of chapters.....	21
1.6 Definitions.....	22
CONCLUSION	24
CHAPTER 2: CRYPTOCURRENCY BASED-INTERMEDIARIES: AN OVERVIEW	
INTRODUCTION	25
2.1 Types of cryptocurrency-based intermediaries.....	26

2.1.1	Cryptocurrency-based exchanges.....	26
(a)	Currency conversion function performed by cryptocurrency-based exchanges.....	27
(b)	Access to users' private keys.....	28
(c)	Categories of cryptocurrency-based exchanges.....	28
(d)	The shadow payment system and cryptocurrency-based exchanges.....	29
2.1.2	Electronic Wallet Providers.....	30
(a)	Custodial wallets.....	30
(b)	Non-custodial wallets.....	31
2.1.3	Cryptocurrency-based remittance service providers.....	31
2.2	Examples of cryptocurrency-based intermediaries operating within South Africa, Nigeria and Kenya.....	32
2.2.1	Luno.....	32
2.2.2	Belfrics.....	36
2.2.3	BitPesa.....	39
2.3	Potential risks that may affect cryptocurrency-based intermediaries and users.....	41
2.3.1	Risks particular to cryptocurrency-based intermediaries.....	42
(a)	Risk of exchange breach.....	42
(b)	Other potential risks.....	46
2.3.2	Risks particular to users.....	47
CONCLUSION	48



CHAPTER 3: REGULATION OF CONVENTIONAL FINANCIAL INTERMEDIARIES AND THE APPLICATION THEREOF TO CRYPTOCURRENCY-BASED INTERMEDIARIES: A CASE STUDY OF SOUTH AFRICAN, NIGERIAN AND KENYAN LAW

INTRODUCTION	50
3.1 Conventional Financial Intermediaries.....	51
3.2 Legislation governing conventional financial intermediaries and the application thereof to cryptocurrency-based intermediaries.....	52
3.2.1 South Africa.....	52
(a) Financial Advisory and Intermediary Services Act 37 of 2002.....	52
(b) Financial Services Act 9 of 2017.....	54
(c) Banks Act 94 of 1990.....	57
3.2.2 Nigeria: Banking and Financial Institutions Act Cap B3, Laws of Federation of Nigeria, 2004.....	61
3.2.3 Kenya: Banking Act Cap 488 of 1995.....	63
3.3 Legislation governing conventional currency exchanges service providers and the application thereof to cryptocurrency-based currency exchanges.....	65
3.3.1 South Africa: Currency and Exchanges Act 9 of 1933 and Exchange Control Regulations, 1961.....	66
3.3.2 Nigeria: Foreign Exchange (Monitoring and Miscellaneous Provisions) Act Chapter F34 (Decree NO. 17 of 1995).....	67
3.3.3 Kenya: Part VIA of the Central Bank of Kenya Act 15 of 1966.....	68
3.4 Legislation governing conventional money remittance service providers and the application thereof to cryptocurrency-based currency exchanges.....	69



3.4.1 South Africa: Currency and Exchanges Act 9 of 1933 and Exchange Control Regulations, 1961.....	70
3.4.2 Nigeria: Operation of International Transfer Services in Nigeria Guidelines.....	71
3.4.3 Kenya: Part VIA of the Central Bank of Kenya Act 15 of 1966 and Money Remittance Regulations, 2013.....	73
3.5 Additional issues that requires compliance by conventional financial intermediaries and their application thereof to cryptocurrency-based intermediaries.....	75
3.5.1 Anti-money laundering.....	75
3.5.2 Consumer protection.....	77
3.6 Suitability of the existing legislation regulating conventional financial intermediaries to cryptocurrency-based intermediaries' regulation.....	78
CONCLUSION.....	79



CHAPTER 4

THE RATIONALE FOR CRYPTOCURRENCY-BASED INTERMEDIARIES' REGULATION AND GLOBAL REGULATORY RESPONSES TO CRYPTOCURRENCY-BASED INTERMEDIARIES

INTRODUCTION.....	81
4.1 The rationale for regulation of cryptocurrency-based intermediaries.....	82
4.2 Global regulatory responses to cryptocurrency-based intermediaries.....	83
4.2.1 Prohibition or frustration of conducting cryptocurrency-based business: China and India....	83
(a) China.....	84
(b) India.....	84
4.2.2 Application of existing legislation: Philippines, the United States of America Financial Crimes Enforcement Network (FinCen), Australia, Japan.....	85

(a) Philippines.....	86
(b) FinCen.....	87
(c) Australia.....	88
(d) Japan.....	89
4.2.3 Self-regulation: South Korea.....	90
4.2.4 Introduction of new regulations: Abu Dhabi and the New York State Department of Financial Services' (NYSDFS) Regulations.....	91
(a) Abu Dhabi.....	92
(b) New York State Department of Financial Services' (NYSDFS) Regulations.....	93
CONCLUSION	97

CHAPTER5: CONCLUSION AND RECOMMENDATIONS

INTRODUCTION	99
5.1 Conclusion.....	100
5.1.1 Chapter one.....	100
5.1.2 Chapter two.....	101
5.1.3 Chapter three.....	102
5.1.4 Chapter four.....	102
5.2 Recommendations.....	103
5.2.1 The recommended regulatory approach to cryptocurrency-based intermediaries: rules-based and/or risk-based approach.....	103
5.2.2 The rationale for cryptocurrency-based intermediaries' regulation: public law and/or private law purpose.....	104
5.2.3 Salient provisions of the recommended regulatory legal framework for cryptocurrency-based intermediaries.....	105

(a)	Scope of the recommended regulatory legal framework.....	105
(b)	Public law aspects.....	108
(c)	Private law aspects.....	113
5.3	Administrator of the recommended regulatory legal framework.....	116
5.4	Additional issues that may not fall within the recommended regulatory legal framework..	116
5.5	Application of the recommended regulatory legal framework within Africa.....	116
FINAL THOUGHTS.....		117
BIBLIOGRAPHY.....		118



PLAGIARISM DECLARATION

I declare that '**Cryptocurrency intermediation in Africa: Towards a Regulatory Framework for Cryptocurrency Intermediaries**' is my own work, that it has not been submitted before for any degree or examination in any other university, and that all the sources I have used or quoted have been indicated and acknowledged as complete references.



Student: Roswitha Mildred Melina Gomachas



Supervisor: Prof. Riekie Wandrag

DECEMBER 2018

DEDICATION

I dedicate this work to my daughters, **Amy and Amirah Gomachas**; to my mother, **Lena Gomachas**; and my late father, **Gottlieb Gomachab**. Thank you for allowing me to take this little time to advance my own interests. It is because of the four of you that I am and that I could undertake this adventurous path.



ACKNOWLEDGEMENTS

To **God**, the Almighty, for guiding me through this LLM Program;

To **Professor Riekie Wandrag**, thank you for making this course an invaluable part of my life that I can never forget nor replace, and I am extremely grateful for your guidance in completing a thesis on the topic researched in this thesis;

To **my family** for allowing me to undertake this path and achieve the dream I had for many years, without your support this whole process would have been too stressful to undertake; and

To the **Lecturers of this LLM Program** for imparting your valuable knowledge during the course of this LLM Program.



KEY WORDS

Africa

Cryptocurrency intermediation

Cryptocurrency-based intermediaries

Cryptocurrency-based exchanges

Cryptocurrency wallet providers

Cryptocurrency-based remittance service providers

Cryptocurrency-based intermediaries' regulation

Financial regulation

Kenya

Nigeria

South Africa



CHAPTER 1

CRYPTOCURRENCY INTERMEDIATION IN AFRICA

INTRODUCTION

There is a lot of speculation regarding potential benefits that the adoption of cryptocurrency use and cryptocurrency intermediation may have for the African continent due to the macro-economic instability of African financial markets caused by hyperinflation; high rate of unbanked populations; and the need for an alternative currency to the weak; and sometimes unavailable and unreliable African fiat money.¹

Preiss notes that the intangible nature of cryptocurrency means that governments have no access to such cryptocurrency and cannot physically remove wealth from the citizens.² He further notes that cryptocurrency not only provides a solution to the unbanked but is also a method of allowing economically and politically subjugated populations to control their wealth.³

Cryptocurrency intermediation in the form of cryptocurrency remittance services have been established in Africa as an alternative to Western Union,⁴ MoneyGram and many others.⁵ Examples include cryptocurrency remittance and transfer services provided by cryptocurrency-based intermediaries, which are third parties facilitating cryptocurrency related transactions, and in some cases provide storage of cryptocurrency to their users.⁶ In Africa, examples of such cryptocurrency-based intermediaries include, such as BTCGhana; BitPesa and Belfrics.⁷

¹ Boateng K 'Despite risks, cryptocurrency prints an exciting opportunity for Africa' 14 June 2018 available at <https://globalriskinsights.com/2018/06/cryptocurrency-opportunity-africa/> (accessed 04 November 2018); Preiss RM 'Cryptocurrency is the great African opportunity' 08 August 2017 available at <https://www.ntusbfcas.com/african-business-insights/content/cryptocurrency-is-the-great-african-opportunity> and <https://www.howwemadeitinafrica.com/cryptocurrency-great-african-opportunity/59402/> (accessed 04 November 2018) (hereinafter referred to as 'Preiss (08 August 2017)').

² Preiss (08 August 2017).

³ Preiss (08 August 2017).

⁴ The Western Union is a global cross-border and cross-currency money movement provider that assists people and businesses to move money across the world. See Western Union 'About Us' available at <https://corporate.westernunion.com/index.html> (accessed 05 November 2018).

⁵ International Fund of Agricultural Development 'Sending Money to Home to Africa Remittance Markets enabling environment and prospects' October 2009 available at https://www.unicef.org/socialpolicy/files/sending_money_home_to_africa.pdf (accessed 05 March 2019) 6.

⁶ Tu KV and Meredith MW 'Rethinking Virtual Currency Regulation in the Bitcoin Age' *Washington Law Review* 90 (2015) 273 (hereinafter referred to as 'Tu and Meredith (2015)').

⁷ Preiss (08 August 2017).

On the BTCGhana platform, users can make Bitcoin purchases through established platforms, and can, within minutes, send payment to local remittance platforms such as TigoCash, Airtel Money and MTN Mobile Money.⁸ These services allow African users to redeem cash at a local remittance outlet without having to deal with complex withdrawal and deposit methods involving bank accounts and credit cards, which are difficult and time consuming to obtain;⁹ and is further an illustration of the presence of cryptocurrency use and cryptocurrency-based intermediation in Africa.

The purpose of this research is to advance a case for cryptocurrency-based intermediation regulation aimed at ensuring that the use of cryptocurrency and cryptocurrency-based intermediation provides adequate protection to users and intermediation is provided within the purview of the law.

To this end, this Chapter is aimed at outlining the research background; the research objective(s); the significance of the research problem; research methodology followed; the chapter outlines; and the relevant definitions applicable to this research.

1.1 RESEARCH BACKGROUND

As a background, it is pertinent to point out the history and the salient features of cryptocurrency; how cryptocurrency is acquired; and examples of existing cryptocurrency, as is done below.

This discussion is necessary to provide an understanding of cryptocurrency and its uses; and in addition, cryptocurrency-based intermediation.

1.1.1 History and salient features of cryptocurrency

Cryptocurrency is a math-based;¹⁰ decentralised;¹¹ and anonymous virtual currency, which is not backed by any State; that is protected by cryptography;¹² and generated by computation

⁸ Preiss (08 August 2017).

⁹ Preiss (08 August 2017).

¹⁰ Financial Action Task Force *FATF Report: Virtual Currencies - Key Definitions and Potential AML/CFT Risks* (2014) 5 (hereinafter referred to as 'FATF (2014)').

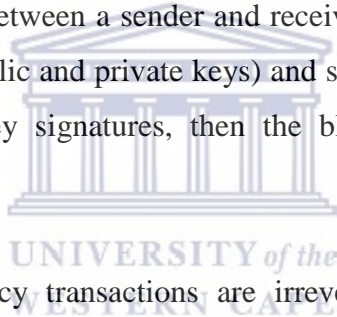
¹¹ FATF (2014) 5.

(“mining”), purchase, or trade.¹³ It is stored and tracked using peer-to-peer technology, which can be compared to file sharing systems such as torrent, and because cryptocurrency relies on distributed computing, it does not require a central clearing house, unlike government issued currency.¹⁴

Cryptocurrency relies on public and private keys to transfer value from one person to another, and must be cryptographically signed each time.¹⁵ A person would use his or her private key address to send cryptocurrency to another person’s public key address; and the latter would then access such cryptocurrency by using his or her private key address.¹⁶

Cryptocurrency has no physical presence and its ownership is verified by entries in a blockchain¹⁷, which is maintained over a peer-to-peer network;¹⁸ and it is a protocol that allow for the validation of transactions without the need of a trusted third party such as a bank, a credit card company or a recording agency¹⁹.

Cryptocurrency transactions between a sender and receiver are signed using the participants’ cryptographic credentials (public and private keys) and sent to the network for validation.²⁰ If the network validates the key signatures, then the blockchain is updated to reflect the transaction.²¹



Once validated, cryptocurrency transactions are irreversible, unless the recipient of the cryptocurrency resends the cryptocurrency to the rightful owner.²² There is no central

¹² FATF (2014) 5.

¹³ Engle E ‘Is Bitcoin Rat Poison: Cryptocurrency, Crime and Counterfeiting (CCC)’ (2016) 16 *Journal High Technology Law* 341-2 (hereinafter referred to as ‘Engle (2016)’).

¹⁴ Engle (2016) 341-2.

¹⁵ FATF (2014) 5.

¹⁶ Turpin JB ‘Bitcoin: The Economic Case for a Global Virtual Currency Operating in an Unexplored Legal Framework 21 *IND. J. GLOBAL LEGAL STUD* (2014) 337-8 referenced in Engle (2016) 341.

¹⁷ A blockchain is computer system that authenticates, verifies and keeps a record of all peer-to-peer transactions undertaken on a cryptocurrency network. For a complete definition see Paragraph 1.6.1 below.

¹⁸ Hughes SJ and Middlebrook ST ‘Advancing a Framework for Regulating Cryptocurrency Payment Intermediaries’ (2015) *Yale Journal on Regulation* 505 (hereinafter referred to as ‘Hughes and Middlebrook (2015)’).

¹⁹ Marian O ‘A Conceptual Framework for the Regulation of Cryptocurrencies’ (2017) 1 *University of Chicago Law Review Online* 82 55 (hereinafter referred to as ‘Marian (2017)’).

²⁰ Hughes and Middlebrook (2015) 505.

²¹ Hughes and Middlebrook (2015) 505.

²² Tu and Meredith (2015) 297.

authority that validates the transactions; instead, the blockchain is maintained by a group of miners²³ who are periodically rewarded for their service by receiving newly created bitcoin.²⁴

Therefore, the general features of cryptocurrency include anonymity or rather pseudonymity;²⁵ irreversibility; no government control; no central government authority validation; conducting transactions directly with another person without the involvement of a third-party (in the conventional sense, referred to as ‘an intermediary’); and protection through cryptography.

1.1.2 Examples of cryptocurrency

Bitcoin, the first cryptocurrency, was created in 2009 by ‘a member of a cryptography mailing list known as ‘Satoshi Nakamoto’, which is a pseudonym.²⁶ Nakamoto published paper entitled ‘*Bitcoin: A Peer-to-Peer Electronic Cash System*’²⁷ proposing a payment system based on cryptographic proof instead of trust allowing any two willing parties to transact directly with each other without the need of a trusted third party.²⁸ Following the release of Nakamoto’s paper, various other cryptocurrencies were created, building on and sophisticating the idea released by Nakamoto, which are discussed below.

Hughes notes that each cryptocurrency has unique features. Bitcoin is one example of a cryptocurrency, however there are many other forms of cryptocurrency, such as Ethereum, Ripple, Litecoin, Dash and Metal.²⁹ For the purpose of this discussion, reference will only be made to Bitcoin, Ethereum and Ripple.

²³ Miners provide computational services to the cryptocurrency network by essentially confirming a cryptocurrency transaction. See the complete definition under Paragraph 1.6.8 below.

²⁴ Hughes and Middlebrook (2015) 505.

²⁵ Transacting parties are not identified by their actual proper names or otherwise used identifiers but by cryptocurrency account addresses. Account owners who execute a transaction with their accounts (receive or send cryptocurrency units) reveal part of their anonymity to the owner of the other transaction account. If a user pays for a good in a store using cryptocurrency, the merchant knows that the account from which the payment was sent belongs to that user. Then the level of the account anonymity depends on the level of the user’s physical anonymity towards the merchant, that is, whether the merchant knows the user by name, or can recognise the user by face. Account owners can voluntarily reveal their identity. See Lansky J ‘Possible State Approaches to Cryptocurrencies’ *Journal of System Integration* (2018) 21 (hereinafter referred to as ‘Lansky (2018)’).

²⁶ Guadamaz A ‘New Kids on the Blockchain’ (2018) 2018 *Jotwell: The Journal of Things we like (Lots)* 1. Guadamaz provides a review of Gerard D *Attack of the 50 Foot Blockchain: Bitcoin, Blockchain and Smart Contracts* (2017).

²⁷ Nakamoto S ‘Bitcoin: A Peer-to-Peer Electronic Cash System’ 31 October 2008; also published in (2017) 1 *Blockchain Technology and Digital Currency National Institute A-1-[i]* (hereinafter referred to as ‘Nakamoto (2008)’).

²⁸ Nakamoto (2008) 1. Also see Gerard VC ‘Virtual Currencies: Growing Regulatory Framework and Challenges in Emerging Fintech Ecosystem’ (2107) 21 *North Carolina Banking Institute* 132.

²⁹ Hughes (2017) 4.

Bitcoin is considered to be the most prominent cryptocurrency and has the largest market capitalisation followed by Ethereum and Ripple.³⁰ Ethereum and Ripple networks have different design features from the Bitcoin protocol.³¹ Ethereum allows users to program smart contracts that mimic physical contracts but are stored on a decentralised and distributed blockchain database.³²

In contrast with the Bitcoin and Ethereum technologies, Ripple is referred to as a closed or private blockchain whereby specific users control which transactions are verified on the network.³³ This is in contrast with the open or public structure of the Bitcoin and Ethereum blockchains that employ a decentralised decision-making model whereby any user, with a given amount of investment, can become a transaction validator.³⁴

1.1.3 Acquiring cryptocurrency

Users may obtain cryptocurrency in three (3) ways:

- (a) **Computation (mining):** New cryptocurrency may be mined by users that offer their computational resources to the various cryptocurrency networks to perform the computational work needed to support the system. In return for providing computational resources such users are rewarded with new bitcoin based on their share of computation used. As this process is analogous to gold prospectors using their equipment to mine for gold, the process is referred to as mining.³⁵

³⁰ Hughes (2017) 4-5.

³¹ Hughes (2017) 4-5.

³² Hughes (2017) 4-5.

³³ Hughes (2017) 5.

³⁴ Hughes (2017) 5.

³⁵ Martinson JP & Masterson CP 'Bitcoin and the Secured Lender' (2014) 33 *Banking & Fin. Services Pol'Y Rep.* 13-14; referred to in Engle (2016) fn 5 341 insofar as it relates to Bitcoin; Hamilton D 'Ethereum Mining vs. Bitcoin Mining: Which is more profitable?' 04 October 2018 available at <https://coincentral.com/ethereum-mining-vs-bitcoin-mining-which-is-more-profitable/> (accessed 05 March 2019), which provides that "the primary functions behind Ethereum mining process are the same as Bitcoin"; Orgera S 'Is Litecoin the same as Bitcoin?' 12 February 2019 available at <https://www.lifewire.com/what-is-litecoin-4151693> (accessed 05 March 2019), which provides that miners acquire Litecoin through the mining process.

- (b) **Purchase:** Cryptocurrency can be purchased on currency exchanges in a similar manner to exchanging fiat (nationally designated) currency (for instance the US Dollar) for any other fiat currency (for instance Euro).³⁶
- (c) **Trade:** Goods and services may be purchased by using cryptocurrency as means of payment.³⁷

1.1.4 The introduction of intermediation in the cryptocurrency environment

The growing acceptance of Bitcoin has resulted in the development of various third-party services designated to facilitate the use of Bitcoin.³⁸ Such intermediaries, acting as custodians of cryptocurrency or cryptocurrency credentials originally belonging to their clients; and facilitating and clearing transactions for users.³⁹

Where an intermediary is involved in cryptocurrency transactions, the transactions are characterised as either “off the block chain”⁴⁰ or “on the blockchain”.⁴¹ Cryptocurrency transactions are undertaken by either centralised cryptocurrency-based intermediaries as is in the case of “off the blockchain” transactions or decentralised cryptocurrency-based intermediaries, as is in the case of “on the blockchain” transactions.⁴²

On the one hand, decentralised cryptocurrency-based intermediaries by undertaking “on the blockchain” transactions merely link and pair buyers and sellers of cryptocurrency.⁴³ The buyer and seller conduct their transaction peer-to-peer on the particular cryptocurrency network.⁴⁴

³⁶ Martinson JP & Masterson CP ‘Bitcoin and the Secured Lender’ (2014) 33 *Banking & Fin. Services Pol’Y Rep.* 13-14; referred to in Engle (2016) fn 5 341 insofar as it relates to Bitcoin.

³⁷ Martinson JP & Masterson CP ‘Bitcoin and the Secured Lender’ (2014) 33 *Banking & Fin. Services Pol’Y Rep.* 13-14; referred to in Engle (2016) fn 5 341 insofar as it relates to Bitcoin.

³⁸ Tu and Meredith (2015) 275.

³⁹ Hughes and Middlebrook 497.

⁴⁰ Hughes and Middlebrook (2015) 497- 498.

⁴¹ Hughes and Middlebrook (2015) 497- 498.

⁴² The Mission Daily ‘Decentralised Cryptocurrency Exchanges: A Comprehensive Overview 21 February 2018 available at <https://medium.com/the-mission/decentralized-cryptocurrency-exchanges-a-comprehensive-overview-a154a92ac1cb> (accessed 01 August 2018).

⁴³ Hughes and Middlebrook (2015) 497- 498.

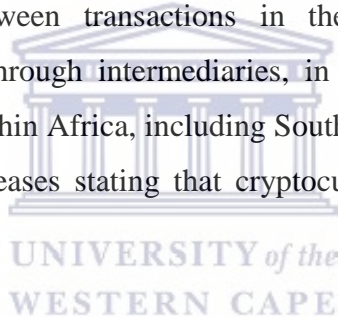
⁴⁴ Hughes and Middlebrook (2015) 497- 498.

On the other hand, centralised cryptocurrency-based intermediaries facilitate the conduct “off the blockchain” transactions, which may not appear in the public ledger at all, or if they do, they appear as transactions involving not the sender and the receiver, but the intermediaries.⁴⁵

Examples of cryptocurrency-based intermediaries operating within Africa include, but are not limited to, BitPesa; Luno; Belfrics; and BTCGhana. All of these cryptocurrency-based intermediaries provide services ranging from connecting buyers and sellers of cryptocurrency; acting as buyers and sellers of cryptocurrency; storage and holding of cryptocurrency; the exchange of cryptocurrency for other forms of cryptocurrency and/or fiat (national or local) currency; and the provision of remittance services.

Intermediaries to cryptocurrency transactions act similar to intermediaries to transactions in traditional payment systems. They pose similar types of credit and liquidity risks to consumers, market participants, and national economies.⁴⁶

Despite the similarities between transactions in the traditional payment system and cryptocurrency transactions through intermediaries, in 2014, 2015 and 2018 respectively, central banking authorities within Africa, including South Africa, Kenya and Nigeria,⁴⁷ issued position papers and press releases stating that cryptocurrency was not recognised as legal tender.⁴⁸



None of these position papers and press releases makes reference to cryptocurrency-based intermediaries or the application of legislation regulating conventional financial intermediaries to cryptocurrency-based intermediaries. It is therefore prudent to undertake an analysis of the relevant legislation to determine whether such legislation may be applicable to cryptocurrency-based intermediaries, the services they provide and their operations.

If the analysis concludes that current legislation governing, supervising and regulating conventional financial intermediaries is not applicable or cannot be applied even with some

⁴⁵ Hughes and Middlebrook (2015) 497- 498.

⁴⁶ Hughes and Middlebrook (2015) 498.

⁴⁷ South African Reserve Bank ‘Position Paper on Virtual Currencies’ (2014) (hereinafter referred to as ‘SARB (2014)’); Central Bank of Kenya ‘Public Notice: Caution to the Public on Virtual Currencies such as Bitcoin’ (2015) (hereinafter referred to as ‘CBK (2015)’); Central Bank of Nigeria ‘Press Release: Virtual Currencies not Legal Tender in Nigeria’ (2018) (hereinafter referred to as ‘CBN (2018)’).

⁴⁸ SARB (2014) 2; CBK (2015); and CBN (2018).

modification, then this research is aimed at finding and proposing a regulatory framework suitable and adequate to regulate cryptocurrency-based intermediaries.

1.2 RESEARCH OBJECTIVE(S)

The main objective of this research is to design a cryptocurrency-based intermediaries' regulatory legal framework for Africa. To this end, the main objective will be achieved through addressing the following sub-objectives:

1.2.1 What are cryptocurrency-based intermediaries; which type of activities and/or services do they provide; and which types of risks emanate from the provision and use of such activities and/or services?

1.2.2 Whether existing regulatory legal frameworks within South Africa, Kenya and Nigeria can be applied to cryptocurrency-based intermediaries?

1.2.3 If not, whether such legislation would be suitable to regulate cryptocurrency-based intermediaries within Africa?

1.2.4 If existing regulatory legal frameworks are insufficient, which regulatory approach or approaches is/are best suited for cryptocurrency-based intermediaries' regulation within Africa?

1.3 SIGNIFICANCE OF THE PROBLEM

Despite the position of the central banking authorities in South Africa, Nigeria and Kenya postulated above, cryptocurrency-based intermediary regulation becomes significant if one considers potential losses that may be suffered by users of services of cryptocurrency-based intermediaries and explore potential remedies that may be available to such users.

Furthermore, the potential use of cryptocurrency as a tool to fund illicit activities through cryptocurrency-based intermediaries warrants the question of the applicability of public law measures applicable to money-laundering; theft; illicit drugs; terrorism financing and many others. In the absence of such application, cryptocurrency-based intermediaries may become complacent in such activities.

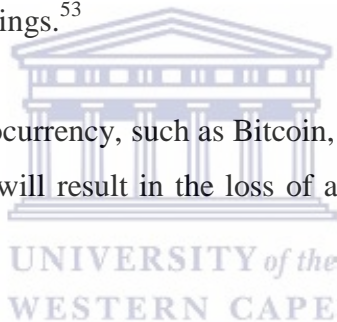
Motsi-Omoijiade⁴⁹ points out several risks that are akin to cryptocurrency exchanges and wallet providers. In relation to cryptocurrency exchanges, she notes that the most frequent manifestation of risk has to do with loss of funds held in escrow by hacking.⁵⁰ In addition, the possible use of exchange services for money laundering, terrorist funding and tax avoidance is another concern.⁵¹

In respect of cryptocurrency wallet providers, Motsi-Omoijiade notes that the main risk for wallet providers has to do with the possibility of loss or theft of stored cryptocurrency mainly through hacking.⁵²

There are various examples of cryptocurrency intermediaries that were and are potentially being hacked globally and the most noticeable examples of hacked cryptocurrency intermediaries include MTGox and Coinbase. Mt. Gox, once Bitcoin's biggest exchange, suspended trading in February 2014, shuttered its website, and filed for bankruptcy after announcing that more than \$400 million worth of customer Bitcoins had vanished without recourse due to computer hackings.⁵³

In addition, the value of cryptocurrency, such as Bitcoin, has increased significantly therefore, cryptocurrency-related losses will result in the loss of a substantial amount of money to the cryptocurrency owner.⁵⁴

Therefore, as it is already evident that cryptocurrency intermediaries provide services as outlined above, it is only prudent, considering the risks involved, that cryptocurrency-based intermediaries' regulation is significant and necessary.



⁴⁹ Motsi-Omoijiade ID 'Financial Intermediation in Cryptocurrency Markets – Regulation, Gaps and Bridges in Chuen DLK et al (eds) *Handbook of Blockchain, Digital Finance, and Inclusion: Cryptocurrency, FinTech, InsureTec and Regulation* vol 1 (2018) (hereinafter referred to as 'Motsi-Omoijiade (2018))'

⁵⁰ Motsi-Omoijiade (2018) 211.

⁵¹ Motsi-Omoijiade (2018) 211.

⁵² Motsi-Omoijiade (2018) 215.

⁵³ Griffith ME 'Virtual Currency Businesses: An analysis of the evolving regulatory landscape' (2015) 16 *Tex. Tech. Admin. L.J.* 305 (hereinafter referred to as 'Griffith (2015)'); Also see Trautman L 'Virtual Currencies: Bitcoin & What Now after Liberty Reserve, Silk Road, and Mt. Gox' 4 *Richmond Journal of Law and Technology* XX (2014) 100-01 (hereinafter referred to as 'Trautman (2014)'); Also see Motsi-Omodijiade (2018) 208.

⁵⁴ Tu K 'Perfecting Bitcoin' (2018) 52 *Georgia Law Review* 521.

1.4 METHODOLOGY

1.4.1 The research, for the purpose of this mini-thesis will be desktop based, largely relying on library resources and internet sources.

1.4.2 In order to examine the applicability and suitability of existing legislation governing comparable or similar services to that which is provided by cryptocurrency-based intermediaries, existing legislation regulating such comparable or similar services within South Africa, Kenya and Nigeria will be examined.

The identified African countries are selected for such examination for illustrative purposes and due to the existence and prominence of cryptocurrency-based intermediaries within those African countries. Furthermore, drawing an analysis of all African countries is not possible, however it is envisaged that the outcome of this research will be relevant across Africa due to the nature of cryptocurrency.

1.4.3 In order to explore global regulatory responses to cryptocurrency-based intermediaries and determine the most suitable regulatory approach to cryptocurrency-based intermediaries' regulation in Africa, countries such as China and India (prohibits the conducting of cryptocurrency-related activities or frustrates the provision of such activities); Philippines, the United States of America Financial Crimes Enforcement Network; Australia and Japan (amends existing legislation to incorporated cryptocurrency-based intermediaries' regulation); and Abu Dhabi Global Market Guidance and the New York State Department of Financial Services' Regulations (enacted new legislation to govern cryptocurrency-based intermediaries) will be examined.

1.5 OVERVIEW OF CHAPTERS

1.5.1 **Chapter One** provides an overview of cryptocurrency intermediation in Africa; and an overview of cryptocurrency, examples of cryptocurrency and its acquisition. It further sets out the research objectives and the significance of the research; the methodology that will be followed; and the relevant definitions.

1.5.2 **Chapter Two** examines cryptocurrency-based intermediaries, the various forms of cryptocurrency-based intermediaries; examples of cryptocurrency-based intermediaries

operating within Africa, more particularly within South Africa, Nigeria and Kenya; and the potential risks that may affect users of the cryptocurrency-based intermediaries' services and risks particular to the provision of such services.

1.5.3 **Chapter Three** outlines and analyses various legislation that governs conventional financial intermediaries in Africa, more particularly within South Africa, Nigeria and Kenya. The aim of this analysis is to determine whether such legislation is applicable to cryptocurrency-based intermediaries.

In addition, this chapter further explores the suitability of such existing legislation to govern cryptocurrency-based intermediaries.

1.5.4 **Chapter Four** examines global regulatory responses to cryptocurrency-based intermediaries with the aim of identifying the most suitable regulatory response to cryptocurrency-based intermediaries' regulation.

1.5.5 **Chapter Five** provides a brief overview of conclusions reached in the preceding chapters; and provides recommendations on the regulatory legal framework for cryptocurrency-based intermediaries' regulation; the scope of application of such recommended regulatory legal framework; relevant aspects that should form part of such recommended regulatory legal framework; issues that fall outside of scope of such recommended regulatory legal approach; and the application of the recommended regulatory legal framework within Africa.

1.6 Definitions

Due to the technical nature of this research, it is pertinent to define the following terms:

1.6.1 'Blockchain' is a trustless technology, which enables exchanges for value over a computer network that can be verified, monitored, and enforced without the presence of a trusted third party or central institution;⁵⁵ an authentication and verification technology, which enables more efficient title transfers and ownership verification;⁵⁶ is decentralised as it can perform its

⁵⁵ Nakamoto S 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2009) 8 available at <https://bitcoin.org/bitcoin.pdf> (accessed 15 July 2018) (hereinafter referred to as 'Nakamoto (2009)').

⁵⁶ Back A et al 'Enabling Blockchain Innovations through Pegged Sidechains' (2014) 7, 15-16 referenced by Kiviat TI 'Beyond Bitcoin; Issues in Regulating Blockchain Transactions' (2015) 65 *Duke Law Journal* 574 fn 33-4 (hereinafter referred to as 'Kiviat (2015)').

functions with minimal trust without using centralised institutions;⁵⁷ and it is borderless and frictionless as it can provide cheaper and faster infrastructure for exchanging units of value;⁵⁸

1.6.2 ‘Convertible (or open) virtual currency’ has an equivalent in real currency and can be exchanged back-and-forth for real currency. Examples include Bitcoin;⁵⁹

1.6.3 A ‘cryptocurrency wallet’ is a means, such as a software application or other mechanism or medium, for holding; storing and transferring cryptocurrency;⁶⁰

1.6.4 ‘Cryptography’ is the manner or means by which digital information and transactions are secured;⁶¹

1.6.5 ‘Decentralised cryptocurrencies’ are distributed, open source math-based peer-to-peer virtual currencies that have no central administering authority and no central monitoring or oversight. Examples include Bitcoin;⁶²

1.6.6 ‘Decentralised public ledger’ is a complete record of all past transactions on the cryptocurrency network and refers to the blockchain;⁶³

1.6.7 ‘Distributed’ refers to the manner in which each transaction on a virtual currency network is distributed among a network of participants who run the algorithm to validate the transaction;⁶⁴

1.6.8 A ‘miner’ is an individual or entity that participates in a decentralised virtual currency network by running special software to solve complex algorithms in a decentralised proof-of-work or other distributed proof system used to validate transactions in virtual currency system;⁶⁵ and mining has a corresponding meaning;

⁵⁷ Nakamoto (2009) 1.

⁵⁸ Swanson T ‘Great Chain of Numbers: A Guide to Smart Contracts, Smart Property and Trustless Asset Management (2014) 67 referenced by Kiviat (2015) 574 fn 37.

⁵⁹ FATF (2014) 4.

⁶⁰ FATF (2014) 7.

⁶¹ Katz J and Lindell Y ‘Introduction to Modern Cryptography: Principles and Protocols (2007) 3 referenced by Kiviat (2015) 577 fn 47.

⁶² FATF (2014) 5.

⁶³ Nakamoto (2009) 3; Also see Kiviat (2015) 578 fn 58 indicating that Nakamoto’s paper does not refer to blockchain.

⁶⁴ FATF (2014) 14 fn 13.

⁶⁵ FATF (2014) 7.

1.6.9 ‘Peer-to-Peer’ means from one party to another without going through a financial institution;⁶⁶

1.6.10 ‘Virtual Currency’ is a digital representation of value that can be digitally traded and functions as a medium of exchange; and/or a unit of account; and/or a store of value but does not have legal tender status in any jurisdiction.⁶⁷ Virtual currency can either be convertible or non-convertible.⁶⁸

During discussions in this research, more particularly in chapter four, reference is made to ‘virtual currency’, which shall mean ‘cryptocurrency’; and reference to ‘Bitcoin’ includes all forms of cryptocurrency, unless the context provides otherwise.

CONCLUSION

This chapter provided an overview of the aspects that will be examined, explored, analysed and considered in this research with the aim of proposing a regulatory legal framework for cryptocurrency-based intermediaries.

The next chapter will provide an overview of cryptocurrency-based intermediaries and identify the potential risks to which users will be susceptible when using the services of cryptocurrency-based intermediaries and, in addition those risks to which cryptocurrency-based intermediaries themselves are exposed and susceptible.

⁶⁶ Nakamoto (2009) 1.

⁶⁷ FATF (2014) 4.

⁶⁸ FATF (2014) 4.

CHAPTER TWO

CRYPTOCURRENCY-BASED INTERMEDIARIES: AN OVERVIEW

INTRODUCTION

In chapter one, the concept of cryptocurrency was introduced, which, as indicated in chapter one, is a digital currency neither issued nor controlled or backed by any government. It can be bought or sold, exchanged or transferred, or stored and transactions are recorded on a decentralised network neither owned nor controlled by any person or government; it can be used to buy goods and services from merchants that accept it as a method of payment; and cryptocurrency transactions can take place person-to-person without any involvement of a third-party.

However, as further indicated in chapter one, the advent of need for cryptocurrency-based intermediaries was a necessity in order to alleviate user challenges regarding exchanging cryptocurrency for national currency; and storing cryptocurrency securely.

The advent of cryptocurrency-based intermediaries resulted in the creation of several types of business models of cryptocurrency-based intermediaries, which are third parties facilitating cryptocurrency-related transactions and providing storage for cryptocurrency.

These business models of cryptocurrency-based intermediaries are all aimed at facilitating the purchase and sale of cryptocurrencies; providing online and offline storage and holding of cryptocurrencies; exchanging cryptocurrencies for fiat (national) currencies and other cryptocurrencies; finding buyers and sellers of cryptocurrencies and facilitating the sale and purchase of cryptocurrencies; and facilitating the remittance of cryptocurrency.⁶⁹

Intermediation within the cryptocurrency market is mainly undertaken by cryptocurrency-based exchanges, cryptocurrency wallet providers, and cryptocurrency-based remittance service providers.⁷⁰

⁶⁹ Tu and Meredith (2015) 273. Also see New York Department of Financial Services 'Proposed New York Codes, Rules and Regulations: Regulation of the Superintendent of Financial Services: Virtual Currencies' (2015) referred to in Motsi-Omoijiade (2018) 209.

⁷⁰ Motsi-Omoijiade (2018) 209.

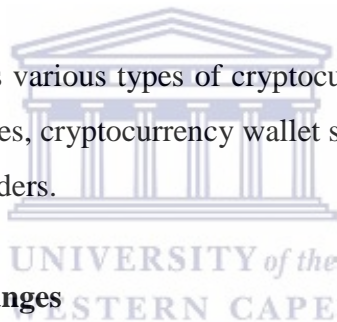
It is the purpose of this chapter to provide an overview of cryptocurrency-based intermediaries, the activities they conduct, services they provide, the potential risks the use of their services pose to users of such services, and the potential risks that may materialise from conducting such activities or provision of such services.

This overview is necessary to provide an understanding of the subject-matter, which will form the basis of the recommended regulatory legal framework aimed at governing cryptocurrency-based intermediaries.

This chapter will further provide examples of selected cryptocurrency-based intermediaries that operate within selected African countries; and examples of cryptocurrency-based intermediary failure and/or hacking in order to identify and highlight potential risks that cryptocurrency-based intermediaries and their users may be susceptible to.

2.1 Types of cryptocurrency-based intermediation

The following section outlines various types of cryptocurrency-based intermediaries, namely cryptocurrency-based exchanges, cryptocurrency wallet service providers and cryptocurrency-based remittance service providers.



2.1.1 Cryptocurrency-based exchanges

Hileman and Rauchs define a cryptocurrency-based exchange as any entity that allows customers (users) to exchange (buy or sell) cryptocurrencies for other forms of money or cryptocurrencies.⁷¹

Cryptocurrency-based exchanges play an essential role in the cryptocurrency economy by offering a marketplace for trading, liquidity, and price discovery.⁷² The primary role of cryptocurrency-based exchanges is to convert cryptocurrencies into fiat currency⁷³ or other forms of cryptocurrency.⁷⁴

⁷¹ Hileman G and Rauchs M *Global Cryptocurrency Benchmarking Study* (2017) 28 (hereinafter referred to as 'Hileman and Rauchs (2017)').

⁷² Hileman and Rauchs (2017) 28.

⁷³ The phrase 'fiat (national) currency' refers to coin and paper money of a country that is designated as legal tender; circulates and is customarily used and accepted as medium of exchange in the issuing country. See FATF (2014) 4.

⁷⁴ Motsi-Omoijiade (2018) 210.

In addition, cryptocurrency-based exchanges are the primary hub for cryptocurrency trading activities (including derivatives) with some offering limited storage facilities for cryptocurrency-denominated investments to their customers.⁷⁵

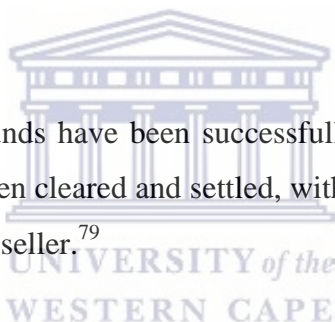
(a) **Currency conversion function performed by cryptocurrency-based exchanges**

Cryptocurrency-based exchanges perform the currency conversion function in two operationally distinct ways, which is as follows:

First stage: During this stage the cryptocurrency-based exchange matches buyers and sellers of cryptocurrencies such as Bitcoin and other currencies.⁷⁶

Second stage: During this stage the prospective seller transfers Bitcoin to the cryptocurrency-based exchange for sale.⁷⁷ The buyer is then responsible for ensuring that it provides the cryptocurrency-based exchange with sufficient funds, denominated in appropriate currency, to complete the purchase.⁷⁸

Once the Bitcoin and other funds have been successfully transferred to the cryptocurrency-based exchange, the trade is then cleared and settled, with Bitcoin transferred to the buyer and the corresponding funds to the seller.⁷⁹



Therefore, the cryptocurrency-based exchange acts as a platform that links or matches the buyer and the seller; acts as a conduit for conducting the purchased and sale of cryptocurrency transaction.

Furthermore, the seller deposits the cryptocurrency into a wallet provided by the cryptocurrency-based exchange; and the buyer deposits funds (money in the form of fiat/national currency) into an account provided by the cryptocurrency-based exchange.⁸⁰ The transaction is then complete once the cryptocurrency is transferred to the buyer and the seller receives payment.

⁷⁵ Motsi-Omoijiade (2018) 210.

⁷⁶ Awrey D and Van Zwieteren K 'The Shadow Payment System' 4 (2017-2018) 43 *Journal of Corporation Law* 797-798 (hereinafter referred to as 'Awrey and Van Zwieteren (2017-2018)').

⁷⁷ Awrey and Van Zwieteren (2017-2018) 797-798.

⁷⁸ Awrey and Van Zwieteren (2017-2018) 797-798.

⁷⁹ Awrey and Van Zwieteren (2017-2018) 798.

⁸⁰ Motsi-Omoijiade (2018) 211.

(b) **Access to users' private keys**

In order to ensure constant and adequate liquidity to execute transactions in near real-time, cryptocurrency-based exchange have access to the private keys assigned to each of its users.⁸¹

The act of depositing bitcoin in an cryptocurrency-based exchange and ceding exclusive use of private key to the cryptocurrency-based exchange invokes fiduciary duties and the need for trust between the exchange the customer. Additionally, the exchange requests and has access to customer's bank details and other identity markers against invoking a duty of trust in the protection of customers' data.⁸²

(c) **Categories of cryptocurrency-based exchange**

Cryptocurrency-based exchange can be categorised as either centralised or decentralised, the difference between the two are represented by the following factors:⁸³

Control of funds:⁸⁴ In a decentralised cryptocurrency-based exchange platform, users transact directly with their peers without the need for a central server, and funds are controlled by the users and participants in the platform; whereas in a centralised cryptocurrency platform, users make deposits to the exchange in order to facilitate an exchange trading transaction, and funds are controlled by the exchanged service.

Anonymity:⁸⁵ In a decentralised cryptocurrency-based exchange platform anonymity is key feature, whereas in a centralised cryptocurrency-based exchange platform may or can allow anonymous trading.

Authentication:⁸⁶ In a decentralised cryptocurrency-based exchange platform there is no need to rely on a third-party intermediary. By means of smart contracts and a number of

⁸¹ Motsi-Omoijiade (2018) 211.

⁸² Motsi-Omoijiade (2018) 211.

⁸³ The Mission Daily 'Decentralise Cryptocurrency Exchanges: A Comprehensive Overview 21 February 2018 available at <https://medium.com/the-mission/decentralized-cryptocurrency-exchanges-a-comprehensive-overview-a154a92ac1cb> (accessed 01 August 2018).

⁸⁴ The Mission Daily 'Decentralise Cryptocurrency Exchanges: A Comprehensive Overview 21 February 2018 available at <https://medium.com/the-mission/decentralized-cryptocurrency-exchanges-a-comprehensive-overview-a154a92ac1cb> (accessed 01 August 2018) (hereinafter referred to as The Mission Daily (21 February 2018)').

⁸⁵ The Mission Daily (21 February 2018)

⁸⁶ The Mission Daily (21 February 2018)

blockchain protocol implementations, the entire system is built to provide trust-less authentication and authorisation of cryptocurrency-based exchange transactions.

On the other hand, in a centralised cryptocurrency-based exchange platform users rely on the platform to authenticate and authorise their transactions, and therefore, in a way, the platform is a third-party intermediary providing trusted cryptocurrency-based exchange services.⁸⁷

(d) **The shadow payment system and cryptocurrency-based exchange**

According to Awrey and Van Zweiten,⁸⁸ cryptocurrency-based exchanges are one of the new financial innovations or rather financial intermediaries that operate outside of the conventional financial system providing services similar to conventional financial intermediaries. The system with which these new financial intermediaries operate is referred to as the ‘shadow payment system’.⁸⁹

According to Awrey and Van Zweiten, these new financial intermediaries share two core features, namely performing the same basic payment functions as conventional deposit-taking banks and providing customers with custodial and transactional storage, and liquidity.⁹⁰

Therefore, cryptocurrency-based exchange are marketplaces or platforms providing exchange services as set out above; they are categorised as either centralised conducting transactions off-the-blockchain⁹¹ or decentralised conducting transactions on-the-blockchain.⁹²

In addition, a user intending to use the services of a cryptocurrency-based exchange is required to create a cryptocurrency wallet with the cryptocurrency-based exchange; deposit cryptocurrency into the created wallet, and fiat currency into an account identified by the cryptocurrency-based exchange.

⁸⁷ The Mission Daily (21 February 2018)

⁸⁸ Awrey and Van Zweiten (2017-2018) 4.

⁸⁹ Awrey and Van Zweiten (2017-2018).

⁹⁰ Awrey and Van Zweiten (2017-2018) 796.

⁹¹ See Paragraph 1.6.9 of Chapter 1 for a definition of ‘off-the-blockchain’ transacting.

⁹² See Paragraph 1.6.10 of Chapter 1 for a definition of ‘on-the-blockchain’ transacting.

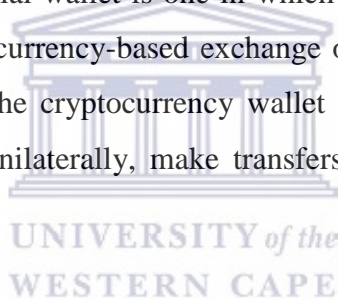
2.1.2 Cryptocurrency Wallet Providers

Cryptocurrency wallet providers hold cryptocurrency on behalf of the user and have cryptographic control over all the users' cryptocurrency wallet.⁹³ Cryptocurrency wallet providers are exclusively concerned with the storage of cryptocurrency.⁹⁴

Cryptocurrency wallet services providers offer storage facilities either online (hot storage) or offline (cold storage) with most offline storage services being offered at a fee and online storage often taking place at no direct cost to the customers.⁹⁵ Cryptocurrency wallet services providers are accessed by the user either through mobile applications, web interfaces, desktop clients (which requires downloading of software) or a combination of the three.⁹⁶

There are two ways in which cryptocurrency wallets can be stored or held, namely custodial and non-custodial cryptocurrency wallets, which are discussed below:

- (a) **Custodial wallets:**⁹⁷ A custodial wallet is one in which the user's private key is stored by a third party, such as an cryptocurrency-based exchange or wallet service providers. The user entrusts his/her/its wallet to the cryptocurrency wallet provider. The cryptocurrency wallet service provider is able to, unilaterally, make transfers from a user's account without the user's authorisation.⁹⁸



However, reputable wallet services implement technical, procedural and sometimes legal measures to ensure transactions are authorised by the users, but there is no cryptographic block to keep wallet service providers from confiscating customer funds.⁹⁹

⁹³ Veksler D 'Introduction to Bitcoin custody options' 08 March 2018 available at <https://vellum.capital/2018/03/08/introduction-to-cryptocurrency-custody-options/> (accessed 07 November 2018). See the custodial wallet discussion below on the clarification of cryptographic control.

⁹⁴ Motsi-Omoijiade (2018) 214.

⁹⁵ Motsi-Omoijiade (2018) 214.

⁹⁶ Motsi-Omoijiade (2018) 215.

⁹⁷ Medium 'Custodial vs Non-Custodial Wallet Benefit of light wallets' available at <https://medium.com/guarda/%EF%B8%8Fcustodial-vs-non-custodial-wallet-s-%EF%B8%8F-benefits-of-light-wallets-87cf701054d1> (accessed 05 August 2018). Also see Schwarz M 'What is a custodial wallet?' last updated 27 June 2018 available at <https://www.abitgreedy.com/custodial-wallet/> (accessed 05 August 2018).

⁹⁸ Veksler D 'Introduction to Bitcoin custody options' 08 March 2018 available at <https://vellum.capital/2018/03/08/introduction-to-cryptocurrency-custody-options/> (accessed 07 November 2018). See the custodial wallet discussion below on the clarification of cryptographic control (hereinafter referred to as 'Veksler 08 March 2018').

⁹⁹ Veksler (08 March 2018).

- (b) **Non-custodial wallets:**¹⁰⁰ This may be web, paper, mobile, desktop and hardware wallets, which is the case also with custodial wallets, however non-custodial wallets allow the user to fully control his/her/its funds and is regarded as more secure. This type of wallet does not require the services of a wallet service provide and the cryptocurrency owner keeps custody of his/her/its own wallet.

Therefore, users can store their cryptocurrency in a custodial or a non-custodial wallet. The use of non-custodial wallet does not require the use of cryptocurrency wallet services providers, whereas the use of a cryptocurrency wallet services provider results in custodial wallet storage.

2.1.3 Cryptocurrency-based remittance services providers

Cryptocurrency-based remittance services providers ('cryptocurrency remittance provider') exploit the distributed ledger technology's ability to transfer and exchange value in near real time to and from anywhere in the world, leveraging the exchangeability of any cryptocurrency into any fiat currency across the world.¹⁰¹

Cryptocurrency remittance providers allow the transfer of value that can be effected quickly, requiring users only to have network access and a smartphone to transact from anywhere in the world.¹⁰²

The use of cryptocurrency remittance provider permits users to send fiat currency to a recipient who receives a payout in fiat currency.¹⁰³ The cryptocurrency remittance provider uses blockchain technology to transfer funds and subsequently convert cryptocurrency into the recipient's fiat currency for them to withdraw through a bank account, mobile phone or teller.¹⁰⁴

In a nutshell, a cryptocurrency remittance provider intermediates the transfer of cryptocurrency from one person at one end and pays to another fiat currency at the other end. Cryptocurrency

¹⁰⁰ Medium 'Custodial vs Non-Custodial Wallet Benefit of light wallets' available at <https://medium.com/guarda/%EF%B8%8Fcustodial-vs-non-custodial-wallet-s-%EF%B8%8F-benefits-of-light-wallets-87cf701054d1> (accessed 05 August 2018). Schwarz M 'What is a custodial wallet?' last updated 27 June 2018 available at <https://www.abitgreedy.com/custodial-wallet/> (accessed 05 August 2018).

¹⁰¹ Motsi-Omoijiade (2018) 217-18.

¹⁰² Cotton J 'Sending a Bit more coin home? An analysis of retail user protection in Bitcoin Remittance Markets' (2018) 49 *Victoria University Wellington Law Review* 113 (hereinafter referred to as 'Cotton (2018)').

¹⁰³ Cotton (2018) 114.

¹⁰⁴ Cotton (2018) 114.

remittance providers facilitate the remittance of cryptocurrency from one person to another irrespective of where in the world both persons find themselves, which is no different from the remittance services undertaken by conventional remittance providers.

2.2 Examples of cryptocurrency-based intermediaries operating within South Africa, Kenya and Nigeria

There are various cryptocurrency-based intermediaries that operate across Africa. Examples include Luno operating in South Africa and Nigeria; Belfrics operating in Kenya, Nigeria and Tanzania; and BitPesa that operating in Kenya, Nigeria, Tanzania, Ghana, DRC, Senegal and Uganda.

2.2.1 Luno

Luno is a company registered in terms of the South African Companies Act 71 of 2008 and the Nigerian Companies and Allied Matters Act Cap. C20 of 2004.¹⁰⁵ Luno provides cryptocurrency-based intermediary services in South Africa; Nigeria; and other countries globally.

Luno is a cryptocurrency-based platform that connects potential buyers and sellers of cryptocurrency. Luno does not buy or sell cryptocurrency neither does it set the exchange rate, meaning that the rate of exchange is determined sole by the buyer and the seller.¹⁰⁶

Users of Luno services are required to commit to and comply with Terms of Use.¹⁰⁷ The following salient features of the Terms of Use are pertinent to this discussion:

(a) Paragraph 6: Identity Verification

Luno claims to maintain the highest level of ‘Know your customer’ processes and controls as part of combating fraud and assisting in the prevention money laundering and terrorist

¹⁰⁵ Luno ‘Company Information’ available at <https://www.luno.com/en/legal/impressum> (accessed 22 October 2018).

¹⁰⁶ Luno Help Centre ‘How does Luno work?’ available at <https://www.luno.com/help/en/articles/11000001992-how-does-the-luno-exchange-work> (accessed 22 October 2018) (‘Luno Terms of Use’).

¹⁰⁷ Luno Terms of Use.

financing.¹⁰⁸ Therefore, users are required to provide certain personal details and documents when opening a Luno account.

(b) **Paragraph 7: The Luno Wallet**

The Luno Wallet allows a holder to send, receive and store cryptocurrency. The Luno Wallet is only available in relation to cryptocurrency that Luno, in its sole discretion decides to support (supported cryptocurrency).

The Luno Wallet further permits the deposit of local currency, which may only be used for the purchase of supported currency; and the withdrawal to an approved bank account.

Under Paragraphs 8 and 9, the Terms of Use further elaborates various aspects that will govern deposits and withdrawals, which are as follows:

Deposits: Luno requires identity verification before a user can deposit local currency into the Luno Wallet by depositing funds in a Luno bank account (referred to as ‘the deposit’). Luno provides the details of the Luno bank account into which the deposit is to be made.

Withdrawals: Where the user adds his or her bank account details to the Luno account, the user may withdraw funds from his or her Luno Wallet to his or her bank account. This is referred to as ‘withdrawal’.

Furthermore, Luno processes transactions according to the user’s instructions. The user accepts and agrees that Luno does not:

- (i) guarantee the identity of any user, receiver or other third party to a Luno Wallet transaction. It is therefore the sole responsibility of the user to ensure that all transaction details are correct and to verify all transaction information prior to submitting transactions to Luno; and
- (ii) has no control over, or liability in relation to, the delivery quality or any other aspect of any goods or services that the user may buy from or sell to any third party.

¹⁰⁸ Luno Terms of Use.

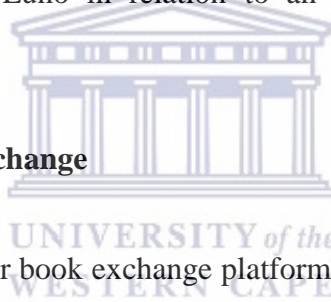
Insofar as it relates to the receipt of cryptocurrency, the user may receive supported cryptocurrency into his/her Luno Wallet by providing a sender with a receiver address generated in his or her Luno Wallet. The user's Luno Wallet will only be credited with supported cryptocurrency sent to a receive address generated through the user's Luno Wallet and associated with that supported cryptocurrency.

For instance, the user's Luno Wallet will be credited with ETH, which is the Ethereum currency, when it is sent to ETH receive address generated through the user's wallet.

(c) **Paragraph 10: Instant buy or sell**

Luno wallet holders may use the instant buy or sell service to buy or sell a chosen amount of supported cryptocurrency at the quoted exchange rate. In using the instant buy or sell, the user accepts and agrees, amongst other things, that Luno is not acting as the user's broker, intermediary, agent or advisor or in any fiduciary capacity and no information or communication provided by Luno in relation to an instant buy or sell transaction will constitute advice.

(d) **Paragraph 11: The Luno Exchange**



The Luno Exchange is an order book exchange platform for cryptocurrencies intended for use by users. In using the Luno Exchange, users agree and accept the following:

- (i) that all trades are executed automatically, based on customer's order instructions and cannot be reversed; and
- (ii) that Luno makes no guarantee that Luno Exchange will be available without interruption; that there will be no delays, failures, errors, omissions or loss of transmitted information; or that any order will be executed, accepted, recorded or remain open.

(e) **Paragraph 13: Account Security**

Luno securely stores cryptocurrency private keys associated with any Luno account. The user accepts and agrees that Luno retains full ownership and control of the private keys associated

with his or her Luno account. The user has no control of, access to, or the ability to use such private keys.

(f) **Paragraph 15: Transaction on cryptocurrency networks**

When the user uses his or her Luno account to send or receive cryptocurrency, the transaction must be recorded in the cryptocurrency public ledger associated with the relevant cryptocurrency network. The cryptocurrency network is solely responsible for verifying and confirming any such transaction.

Luno does not or cannot confirm, cancel or reverse transactions on cryptocurrency network, other than confirming that the network has completed the transaction.

(g) **Paragraph 16: Account inactivity**

Local currency deposited into a Luno Wallet may only be used to purchase supported cryptocurrency and/or withdrawal to an approved bank account. The Luno wallet should not be used for the purpose of storing local currency.

In the event that the Luno Wallet holds funds and Luno has no record of any use of the Luno account for years or Luno is unable to contact the user, Luno will contact and deliver such funds to the relevant authorities as unclaimed property.

(h) **Paragraph 27: Disputes**

In terms of Paragraph 27, the Terms of Use are governed by the Law of Singapore and the user and the parties (Luno and the user) submit any dispute arising from the Terms of Use to the exclusive jurisdiction of the courts of Singapore.

Therefore, Luno is an example of a decentralised cryptocurrency-based exchange, meaning that transaction conducted through Luno are recorded ‘on the blockchain’; and provides custodial wallet storage services to its users, meaning that Luno retains full ownership of the users private keys. Luno however submits that it will only conduct transactions on the instruction of the user.

In addition, it is clear that the relationship between Luno and its users is government by contract as postulated in the Terms of Use. Therefore, the users only obtain the rights and incur the obligations

set out in the Terms of Use; and any dispute arising between the user and Luno will be resolved in terms of the Terms of Use.

Luno further does not allow users to hold fiat currency for any other purpose but to purchase cryptocurrency. Luno further claims to adhere to strict ‘know-your-customer’ rules, processes and controls aimed at combating fraud; prevention of money laundering and terrorist financing. To this end, Luno requires its users to provide verifiable identity information and in addition, similar information for third parties that such users may trade with.

2.2.2 Belfrics

The use of Belfrics’ services is subject to Terms and Conditions, which requires user subscription. Belfrics provides a payment gateway, which allows its customers to pay in cryptocurrency; store their funds in a free cryptocurrency wallet; exchange cryptocurrency; provides a cryptocurrency trading platform.¹⁰⁹

Terms and Conditions¹¹⁰ of using Belfrics’ services provide the following:

(a) **Paragraph 1: Preliminary Provisions**

Paragraph 1.3.3 provides that all members are users but not all users are members. For consistency purposes, these terms will be used according to their applicability to this discussion. Furthermore, in terms of Paragraph 1.2 users may access certain public areas of the Belfrics website, however only members may use the Exchange or ancillary services.

(b) **Paragraph 2: Explanation of Membership and Exchange**

Belfrics does not provide or issue members any cryptocurrency. All cryptocurrency traded or exchanged by and between members originate from and between members themselves.

¹⁰⁹ Belfrics ‘About Belfrics: A secure cryptocurrency exchange in Kenya’ available at <https://kenya.belfrics.com/about/> (accessed 24 October 2018).

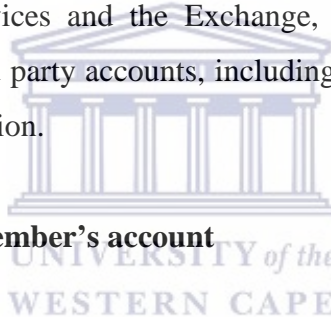
¹¹⁰ Belfrics ‘Terms and Conditions’ available at <https://kenya.belfrics.com/terms-conditions/> and <https://nigeria.belfrics.com/terms-conditions/> (accessed 24 October 2018).

All cryptocurrency transferred to Belfrics by the members for use within the exchange is held in an omnibus client account controlled by the Exchange. The Exchange maintains an internal ledger recording the amount of cryptocurrency each member possesses in the omnibus client account and all transactions between the members are based on such ledger.

Paragraphs 2.3 and 2.4 further provide that the member's accounts and any available currency therein is not a credit card, bank account or deposits; and that Belfrics' services are not financial instruments. Furthermore, no interest will be paid on any funds or currency. Belfrics maintains depository accounts with a reputable bank for the customers.

In order to use the Exchange, members must create an account. The account would be used to store various cryptocurrency amounts as deposited by the member. In opening an account, the member will be required to provide personal information, which will be subject to verification by Belfrics.

In order to use Belfrics services and the Exchange, the member is required to disclose information pertaining to third party accounts, including the member's bank account, Bitcoin addresses and related information.



(c) **Paragraph 2.14: Funding Member's account**

After creating the account, the member may be able to fund his or her account by transferring bitcoin from his or her accounts with such third party cryptocurrency providers into the account operated by the Exchange.

For instance, to fund his or her account with 10 bitcoin (BTC), the member would use the third party software to transfer his or her own pre-existing 10 BTC to the Exchange's Bitcoin address for omnibus client account. The Exchange would then credit the member's account with 10 BTC on the Exchange's ledger and the member would be able to trade this BTC for Kenyan shilling on the Exchange.

(d) **Paragraph 2.15: Trading**

After the member has funded his or her account, the member may commence trading cryptocurrency with other users. Trading is achieved through bids and offers to buy and sell

cryptocurrency. Matching bids and offers to buy and sell cryptocurrency are automatically paired by the Exchange and the Exchange will notify the respective members that the order has been executed.

The members may only sell as much cryptocurrency as is recorded by Belfrics in the Exchange ledger, plus the applicable fee. Once the order has been executed; the appropriated currencies have been credited and debited from the member's account, then the transaction is perceived as completed and irreversible.

(e) **Paragraph 2.19: Withdrawing currency**

The members are allowed to withdraw their cryptocurrency upon requests from Belfrics. The members may withdraw all or some of their cryptocurrency, and are not required to keep a certain limit in their accounts.

(f) **Paragraphs 14.1: Binding arbitration and Governing Law**

In terms Paragraph 14.1 any dispute arising out of the Belfrics (Nigeria) Terms and Conditions must be resolved, first through negotiation, and in the event that negotiation fails, through binding arbitration in accordance with the Arbitration Rules of Lagos Court of Arbitration International Centre of Arbitration.

The same process is stipulated in Belfrics Kenya Terms and Conditions, except that the applicable rules for arbitration are the Arbitration Rules of the Nairobi Center of International Arbitration.

The relevant law governing any dispute between the parties is, in terms of Belfrics Nigeria Terms and Conditions, Nigerian Law; and that disputes between parties is, in terms of Belfrics Kenya Terms and Conditions, Kenyan Law.

Other service: Belfrics also provides remittance services.¹¹¹

¹¹¹ Admin 'Belfrics Global Launches Bitcoin Exchange in Kenya' 13 August 2017 available at e-labz.info/blog/belfrics-bitcoin-exchange-kenya/ (accessed 25 October 2018).

Therefore, Belfrics provides a whole range of services, such as electronic wallet storage for cryptocurrency; exchange (trading) platform; and remittance services. Similar to Luno, Belfrics provides custodial wallet services; and ensure that user and member identity information is provided and verified.

Cryptocurrency exchanged by the members are transferred into an account that is controlled and managed by Belfrics; and all transactions are recorded on an internal ledger maintained by Belfrics. This means that Belfrics authenticates and verifies all transactions conducted through their exchange, which is different from how transactions are recorded on the Luno Exchange. Luno does not verify any transaction, but requires same to undertaken on a ledger held on a particular cryptocurrency exchange.

2.2.3 BitPesa

In contrast to the services provided by BitPesa and in relation to the determination of the exchange rate, Luno clearly indicates that it does not determine the exchange rate, rather it is determined by agreement between the transacting users. Whereas, the Belfrics' website is silent on who determines the exchange rate, BitPesa agrees on an exchange rate with the users.

All users intending to use BitPesa Services are required to accept and agree to conduct transactions and use services in accordance with the Terms and Conditions of Service.¹¹² Users are further required to register as users and provide verifiable identity information to BitPesa. In addition, the user must also provide verifiable identity information of third parties that they may conduct transactions with.

Users may conduct exchange or purchase transaction using BitPesa Services, which, in terms of the Paragraphs 2.3 and 2.4 respectively, occurs as follows:

- (a) Paragraph 2.3 provides for Exchange transactions conducted using BitPesa. In terms of Paragraph 2.3, to initiate an exchange transaction, the user needs to transfer cryptocurrency to his or her BitPesa account; agree with BitPesa on an exchange rate; designate a Payee account into which the National Currency is to be deposited; and confirm the Exchange transaction.

¹¹² BitPesa 'Terms and Conditions of Service' available at <https://www.bitpesa.co/terms/> (accessed on 20-21 October 2018).

If the user's change transaction involves selling cryptocurrency for national currency, the customer is responsible for buying cryptocurrency from a third party. All transactions are subject to verification.

Once the exchange transaction is confirmed, the user has irrevocably authorised BitPesa to debit the designated amount of cryptocurrency from the user's BitPesa account and the user may not cancel the Exchange Transactions. The corresponding amount of cryptocurrency debited from the user's BitPesa account becomes the property of BitPesa.

Upon debiting the designated amount of cryptocurrency from the customer's BitPesa account, BitPesa will deposit the designated amount of National Currency to the designated Payee account specified by the user.

- (b) Paragraph 2.4 provides for Purchase transactions conducted using BitPesa. In terms of Paragraph 2.4, to initiate a purchase transaction, the user needs to have sufficient funds in his or her bank account or mobile wallet account; agree on an exchange rate with BitPesa; designate a Payor account in to which the cryptocurrency is to be deposited; and confirm the purchase transaction.

If the user uses a bank account, once the customer confirms a Purchase transaction, the user will either be required to transfer the use of the corresponding amount in the National Currency from the customer's bank account or another payment instrument; the user irrevocably authorise BitPesa to debit the designated amount of National Currency from the valid bank account linked, and the user may not cancel the Purchase transaction.

BitPesa, in terms of Paragraph 3.7, 3.9 and 3.11 of its Terms and Conditions of Service, warns users against the risk of loss of holding cryptocurrency in their BitPesa accounts; the risk of change in law, which may adversely affect the use, transfer, exchange and value of cryptocurrency; and the risk of loss of private keys, which may result in the inability of the user to access their external cryptocurrency wallets and which may result in the permanent loss of cryptocurrency.

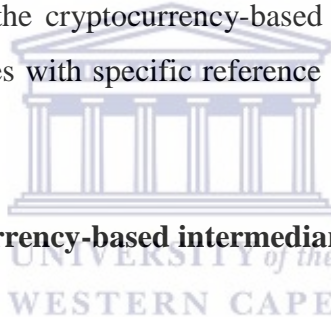
Insofar as it relates to the governing law applicable to the Terms and Conditions, Paragraph 13.1 specifies the governing law as the Law of Luxembourg.

2.3 Potential risks that may affect cryptocurrency-based intermediaries and users

The most pertinent risk cryptocurrency-based intermediaries and users of services provided by cryptocurrency-based intermediaries can be susceptible to is the risk of an exchange breach.¹¹³ Other additional potential risks include money laundering risk, and liquidity and solvency risks.

In addition, the main risk that users are susceptible to is the risk of loss of cryptocurrency, through the aforementioned risks. In addition, users are further susceptible to loss of cryptocurrency through the risk of unauthorised use of private keys and therefore unauthorised transfer of users' cryptocurrency; the risk of closure or shutdown of the cryptocurrency-based intermediary holding and storing users' cryptocurrency private keys; insolvency of a cryptocurrency-based intermediary; and the risk of an administrator or employee absconding with users' cryptocurrency.

The aforementioned risks to the cryptocurrency-based intermediaries and the users will be discussed below, in some cases with specific reference to examples of manifestation of such risks.



2.3.1 Risks particular to cryptocurrency-based intermediaries

The provision of cryptocurrency-related activities and/or services exposes cryptocurrency-based intermediaries to certain identifiable potential risks, which are discussed below.

(a) Exchange breach risk

An exchange breach is defined as an event, during the life of an exchange, which result in the loss of users' funds due to the negligence or misconduct by the operators of the exchange'.¹¹⁴ Moore *et al* further identify four (4) scenarios that can lead to an exchange breach, namely security breach; data loss; insider scam; and legal action.¹¹⁵

¹¹³ Moore T, Christin N, and Szurdi J 'Revisiting the risks of Bitcoin Currency Exchanges' (2016) A:5 available at <https://tylermoore.utulsa.edu/toit17.pdf> (accessed 08 November 2018) (hereinafter referred to as 'Moore *et al* (2016)').

¹¹⁴ Moore *et al* (2016) A:5.

¹¹⁵ Moore *et al* (2016) A:5.

The risk of exchange breach may take various forms, namely security breach, data loss, insider scam or legal action, which may manifest in the following manner:

- (i) **Security breach:** A security breach is described as one where a malicious entity exploits the vulnerabilities in the exchange's software, hardware or system configuration to steal cryptocurrency.

The manifestation of this type exchange breach risk can be illustrated by reference to that which has occurred with cryptocurrency-based intermediaries such as MtGox and other cryptocurrency-based intermediaries mentioned below:

(aa) **MtGox**

MtGox was launched in 2010 as a Tokyo based online marketplace and considered, at that time, the largest Bitcoin exchange.¹¹⁶ During the time of its operations, which was 2010 to 2014, MtGox handled seventy (70) percent of Bitcoin transactions.¹¹⁷

As narrated by Zhou,¹¹⁸ on the MtGox site, a user was required to add a state-backed currency to his or her account, thereafter the user could directly buy Bitcoins from MtGox using money in the linked bank account.¹¹⁹ Despite the requirement of linking a bank account or PayPal account, the website facilitated exchanges in relative anonymity.¹²⁰

On 07 February 2014, MtGox stopped all bitcoin withdrawals claiming that it was merely pausing withdrawal requests to obtain a clear technical view of the currency process.¹²¹ On 24 February 2014, the exchange suspended all trading and the website went offline.¹²² On 25

¹¹⁶ Trautman (2014) 100.

¹¹⁷ Lee J, Long A, McRae M, et al 'Bitcoin Basics: A Primer on Virtual Currencies' (2015) 16 *Business Law International* 25 (hereinafter referred to as 'Lee et al (2015)').

¹¹⁸ Zhou S 'Bitcoin Laundromats for Dirty Money: The Bank Secrecy Act's Inadequacies in Regulating and Enforcing Money Laundering Laws over Virtual Currencies' (2014) 3 *Journal of Law and Cyber Warfare* 117 (hereinafter referred to as 'Zhou (2014)').

¹¹⁹ Zhou (2014) 117.

¹²⁰ Zhou (2014) 117.

¹²¹ Norry A 'The history of the MtGox hack: Bitcoin's biggest heist' 2 July 2018 available at <https://blockonomi.com/mt-gox-hack/> (accessed 30 October 2018) (hereinafter referred to as 'Norry (July 2018)'). Also see Pollock D 'The mess that was MtGox: Four years on' available at <https://cointelegraph.com/news/the-mess-that-was-mt-gox-four-years-on> (09 March 2018) (accessed 30 October 2018) (hereinafter referred to as 'Pollock (09 March 2018)').

¹²² Norry (July 2018). Also see Pollock (09 March 2018).

February 2014, MtGox announced the disappearance of eight hundred and fifty (850 000) Bitcoin.¹²³

During that same period, a leaked MtGox document indicated that hackers had raided the MtGox exchange and stole seven hundred and forty-four thousand (744 000) bitcoins belonging to MtGox customers, as well as an additional hundred thousand (100 000) bitcoins belonging to MtGox, resulting in MtGox being declared insolvent.¹²⁴ On 28 February 2014 MtGox filed for bankruptcy protection in Japan, and later in the United States of America.¹²⁵

It is suspected that the first hack of MtGox occurred during June 2011 as a result of a compromised computer belonging to an auditor of MtGox.¹²⁶ Norry states that, in this instance, the hacker(s) used their access to the exchange to artificially alter the nominal value of bitcoin to one cent and then transferred an estimated two thousand (2 000) bitcoin from customer accounts, which were sold.¹²⁷

Norry provides that subsequent investigations had shown massive hacking of MtGox began as early as September 2011. As a result, MtGox was operating while technically insolvent for almost two (2) years and had practically lost all its bitcoin by mid-2013. Additional evidence suggested that MtGox was already missing eighty thousand (80 000) bitcoins even before 2011.¹²⁸

Although it remains unclear how exactly the hackers gained access and stolen the bitcoin from the MtGox wallets (both hot (online) or cold storage), Norry relays the following speculation:¹²⁹

Hot storage: Prior to September 2011, the MtGox private key was encrypted and it would appear that it was stolen via a copied *wallet.dat* file, either by hacking or through an insider.

¹²³ Lee et al (2015) 25.

¹²⁴ Norry (July 2018). Also see Pollock (08 March 2018).

¹²⁵ Norry (July 2018). Also see Pollock (08 March 2018).

¹²⁶ Norry (July 2018). Also see Pollock (08 March 2018).

¹²⁷ Norry (July 2018). Also see Pollock (08 March 2018).

¹²⁸ Norry (July 2018). Also see Pollock (08 March 2018).

¹²⁹ Norry July 2018.

Once the file was hacked, the hacker(s) were able to access and cipher bitcoins gradually from wallets associated with MtGox's private keys without the hack having being detected.

Cold storage: In respect to access to bitcoin held in the MtGox cold storage, theories ranges from suggestion that the storage may have been compromised by an individual with on-site storage access to suggestions that the cold storage coins were gradually deposited into the MtGox exchange system when a hot storage wallet ran low and that the lack of accountability among the staff meant that there was no awareness that wallets were being drained by hackers.

A Japanese Court has recently lifted MtGox out of bankruptcy, opening the door for one (1) billion US dollar worth of cryptocurrency to be paid to the MtGox former customers. This will allow the distribution of the remaining MtGox assets to ex-customers in the form that they seek, inclusive of bitcoin.¹³⁰

- (bb) Bitfloor, a New York based exchange and trading platform, suffered a security breach when thieves gained access to the backups of the private keys controlling cash flow accounts on the exchange, and used this access to steal an estimated twenty-four thousand and eighty-six (24 086) Bitcoins.¹³¹ The Bitfloor exchanges Bitcoin loss was estimated at two hundred and fifty-one thousand six hundred (256 600) US Dollars at the time of the loss.¹³²
- (cc) In August 2016, Bitfinex, a Hong Kong based cryptocurrency exchange, was hacked, suffering a loss of one hundred and nineteen thousand seven hundred and fifty-six (119 756) Bitcoin valued at sixty-eight (68) million US Dollars loss at the time.¹³³
- (dd) In April 2018, the Korean police arrested the chief of Coinnest, a Korean cryptocurrency-based exchange, for allegedly embezzling tens of millions of dollars from users' accounts.¹³⁴

¹³⁰ Wieczner J '\$1 Billion Bitcoins lost in the MtGox hack to be returned to victims' available at <http://fortune.com/2018/06/22/bitcoin-price-mt-gox-trustee/> (accessed 30 October 2018).

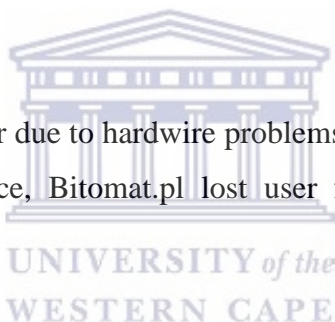
¹³¹ Moore *et al* (2016) A:5.

¹³² Lee M 'Bitcoin exchange robbed of US 250 000, all trading halted' 5 September 2012 available at <https://www.zdnet.com/article/bitfloor-exchange-robbed-of-us250000-all-trading-halted/> (accessed 08 March 2019).

¹³³ Chen. LY and Nakamura Y 'Hacked Bitcoin Exchange Says Users May Share \$68 Million Loss' (2016) <https://www.bloomberg.com/news/articles/2016-08-05/hacked-bitcoin-exchange-says-it-will-spread-losses-among-users> referred to in Moore *et al* (2016) A:2. Also see Higgins S 'The Bitfinex Bitcoin hack: What we know (and don't know)' 03 August 2016 updated 20 June 2018 available at <https://www.coindesk.com/bitfinex-bitcoin-hack-know-dont-know> (accessed 08 March 2019).

- (ee) In April and December 2017, Youbit, a South Korean cryptocurrency-based exchange, was hacked and had to file for bankruptcy after losing seventeen (17) percent of its assets during a second cyber attack.¹³⁵
- (ff) On 11 June 2018, Coinrail, a South Korean cryptocurrency-based exchange, was subject to hacking attack that resulted in the loss of various forms of cryptocurrency valued at forty (40) million US Dollars.¹³⁶
- (gg) On 20 June 2018, Bithumb, a South Korean cryptocurrency-based exchange, announced that it suffered a hacking attack that resulted in the loss of Ripple valued at approximately thirty-one (31) million US Dollars.¹³⁷

Investigations into most of the mentioned hackings found that the majority of cryptocurrency-based exchanges operated without adequate security measure and information technology infrastructure.¹³⁸



- (ii) **Data loss:** Data loss may occur due to hardware problems that can result in unrecoverable loss of cryptocurrency, for instance, Bitomat.pl lost user funds in a data loss caused by an improper server restart.¹³⁹
- (iii) **Insider scam:** This occurs when unscrupulous exchange operators steal user funds.¹⁴⁰ In April 2018, the Korean Police arrested the chief of Coinnest, a South Korean cryptocurrency-based exchange, alleging that he embezzled tens of millions of dollars from customers' accounts.¹⁴¹

¹³⁴ Park N, Kim M and Lee D 'Cryptocurrency laws and regulations in South Korea' 12 July 2018 available at <https://www.vantageasia.com/cryptocurrency-law-south-korea/> (accessed 15 November 2018) (hereinafter referred to as 'Park *et al* (12 July 2018)').

¹³⁵ Park *et al* (12 July 2018).

¹³⁶ Park *et al* (12 July 2018). Also see Zhao W 'Coinrail Exchange hacked, losses possibly \$ 40 million in cryptos' 18 June 2018 available at <https://www.coindesk.com/coinrail-exchange-hacked-loses-possibly-40-million-in-cryptos> (accessed 08 March 2019).

¹³⁷ Park *et al* (12 July 2018)

¹³⁸ Park *et al* (12 July 2018).

¹³⁹ Moore *et al* (2016) A:5.

¹⁴⁰ Moore *et al* (2016) A:5.

¹⁴¹ Park *et al* (12 July 2018).

(iv) **Legal action:** Legal action that can result in confiscation and subsequent loss of cryptocurrency.¹⁴²

(b) **Other potential risks: Money laundering risk**

The process of money laundering conducted through a cryptocurrency-based exchange encompasses the following:

- (i) The criminal purchases a basic cryptocurrency at cryptocurrency-based exchange, by often employing strawmen with clean records and corroborated employment;¹⁴³
- (ii) Once the strawmen has been verified by the cryptocurrency-based exchange, fiat currency or bank transfers are used to purchase primary cryptocurrency, such as Bitcoin, Ethereum or Litecoin; and primary cryptocurrency is then used to purchase altcoins¹⁴⁴ from an advanced cryptocurrency-based exchange.¹⁴⁵ Altcoins have particular specifications, some of which are privacy cryptocurrency offering an elevated level of anonymity.¹⁴⁶
- (iii) In order to obscure the primary cryptocurrency's audit trail, money launderers use a tactic referred to as mixing or tumbling, which involves the use of mixing services such Bitmixer or Helix to swap primary cryptocurrency addresses for temporary digital wallet addresses to fool the blockchain and to break audit traceability.¹⁴⁷
- (iv) The money launderers layer multiple privacy cryptocurrency (altcoins), cryptocurrency-based exchanges and cryptocurrency addresses to sever the audit trail, effectively preparing illicit funds by cleansing them for integration into the traditional financial system.¹⁴⁸
- (v) having severed the audit trail, the money launderer has several options for withdrawing cleansed funds from cryptocurrency to obtain fiat currency, namely by exchanging privacy cryptocurrency for primary cryptocurrency, and thereafter exchanging primary

¹⁴² Moore *et al* (2016) A:5.

¹⁴³ Spenger P and Balsiger F 'Anti-money laundering in times of cryptocurrencies' June 2018 available at <https://assets.kpmg.com/content/dam/kpmg/ch/pdf/anti-money-laundering-in-times-of-cryptocurrency.pdf> (accessed 01 December 2018) (hereinafter referred to as 'Spenger and Balsiger (June 2018)').

¹⁴⁴ These are cryptocurrency that are alternatives to Bitcoin.

¹⁴⁵ Spenger and Balsiger do not advance any explanation as to the meaning of an 'advanced cryptocurrency-based exchange', but despite such clarification, their explanation regarding the process of cryptocurrency-related money laundering is relevant to the discussion of the involvement of cryptocurrency in money laundering.

¹⁴⁶ Spenger and Balsiger (June 2018).

¹⁴⁷ Spenger and Balsiger (June 2018).

¹⁴⁸ Spenger and Balsiger (June 2018).

cryptocurrency for fiat currency which can be withdrawn; or transfer the storage of cryptocurrency from an online (hot) wallet storage to offline (cold) wallet storage¹⁴⁹, which can be transported anywhere in the world.¹⁵⁰

An investigation conducted by the Wall Street Journal alleged that over forty-six (46) cryptocurrency-based exchanges assisted criminals in laundering more than USD 88 million since 2016. Examples of such alleged cryptocurrency-based exchanges include ShapeShift AG, an altcoin cryptocurrency-based exchange.¹⁵¹

The Wall Street Journal Report presented evidence from security researchers alleging that criminals used ShapeShift to exchange Bitcoin for Monero, an anonymity centric cryptocurrency.¹⁵²

The risks mentioned in this sub-paragraph will collectively be referred to as the ‘cryptocurrency-based intermediaries’ related risks’ in this research.

2.3.2 Risks particular to users



Users using cryptocurrency-based intermediary services are susceptible to the following risks:

- (a) the risk of loss of cryptocurrency due to the risks discussed under Paragraph 2.3.1 above;
- (b) the risk of unauthorised use of user cryptocurrency where the user has ceded the control of the cryptocurrency private key to the cryptocurrency wallet provider as is the case with Luno;
- (c) the risk of closure of cryptocurrency-based intermediary and shut down of website, which results in the inability to access cryptocurrency held by the cryptocurrency-based intermediary;¹⁵³

¹⁴⁹ Offline (cold) wallet storage can range from a piece of paper on which the public or private key information is written or can be a USB, which contains details of the public and private key.

¹⁵⁰ Spenger and Balsiger (June 2018).

¹⁵¹ Bitcoin Crime ‘Cryptocurrency Exchanges have been used to launder \$88 million since 2016: WSJ’ 29 September 2018 available at <https://www.cnn.com/cryptocurrency-exchanges-have-been-used-to-launder-88-million-since-2016-wsj/> (accessed 02 December 2018) (hereinafter referred to as ‘Bitcoin Crime (29 September 2018)’).

¹⁵² Bitcoin Crime (29 September 2018).

¹⁵³ This occurred in the MtGox matter discussed under Paragraph 2.3.1(a)(i)(aa) above.

- (iv) the risk that user may not be reimbursed for the losses on account of the aforementioned risks, including those affecting the cryptocurrency-based intermediary; and
- (vii) the risk of loss when the cryptocurrency exchange becomes insolvent or when a cryptocurrency wallet provider absconds with the users' cryptocurrency.¹⁵⁴

The risks mentioned in this sub-paragraph will collectively be referred to as 'user related risks' in this research.

Therefore, the most prominent risk that cryptocurrency-based intermediaries are susceptible to is the risk of security breach through hacking, and this same risk results in significant losses to the users.

Furthermore, the three cryptocurrency-based intermediaries, namely Luno, Belfrica and BitPesa referred to in Paragraph 2.2, and any other cryptocurrency-based intermediaries operating within Africa, are similarly susceptible to the risks identified in Paragraph 2.3 above.

CONCLUSION

This chapter provided a basic overview of cryptocurrency-based intermediaries by making reference to the types of cryptocurrency-based intermediaries; the activities they conduct and the services they provide; the risks that they are susceptible to; and the risks that may materialise for users using such services.

In providing this overview, this chapter further provided insight into various categories of cryptocurrency-based exchanges, namely centralised and decentralised cryptocurrency-based exchanges; and various types of cryptocurrency wallet storage categories, namely custodial and non-custodial wallets.

In addition, and as an illustration, this chapter explored the terms of use (in the case of Luno) or terms of condition (in the case of Belfrics and BitPesa) of selected cryptocurrency-based intermediaries operating within South Africa, Nigeria and Kenya.

¹⁵⁴ Motsi-Omoijiade (2018) 211.

This chapter further identified, amongst other listed, that the materialisation of the risk of security breach is the most prominent risk to cryptocurrency-based intermediaries; and the risk of loss through the actions of cryptocurrency-based intermediaries the most prominent risk to users.

The potential risks identified in this chapter necessitate the need for a regulatory legal framework aimed at the detection, monitoring and mitigation of such potential risks with the objective of ensuring secure provision of cryptocurrency-based intermediaries' activities and/or services; and to achieve user protection.

Chapter three will then examine, analyse and determine whether existing legislation regulating conventional financial intermediaries apply to cryptocurrency-based intermediaries and whether such legislation will be suitable to address the risks identified in this chapter.



CHAPTER THREE

REGULATION OF CONVENTIONAL FINANCIAL INTERMEDIARIES AND THE APPLICATION THEREOF TO CRYPTOCURRENCY-BASED INTERMEDIARIES: A CASE OF SOUTH AFRICAN, NIGERIAN AND KENYAN LAW

INTRODUCTION

Before designing a cryptocurrency-based intermediaries' regulatory legal framework, it is pertinent to provide some understanding of cryptocurrency-based intermediaries and to identify the risk that may materialise from the use of such services and the conduct of such services, which was done in chapter two.

It is further pertinent to analyse and examine existing legislation regulating and supervising institutions or actors that conduct similar and/or comparable activities or services, such as conventional financial intermediaries. This analysis and examination is aimed at determining whether such existing legislation is applicable to cryptocurrency-based intermediaries; and/or suitable to address cryptocurrency-based intermediaries' related risks identified in chapter two.

For the purpose of this analysis, existing legislation regulating and supervising conventional financial intermediaries within Africa, more particularly, South Africa, Nigeria and Kenya will be examined.

This chapter will therefore identify and discuss existing legislation regulating conventional financial intermediaries in general, if any; and specifically, regulating financial institutions, financial services and product providers; conventional exchanges; and conventional remittance or money transfer service providers. In each instance of the analysis and examination of existing legislation, the applicability of such legislation of cryptocurrency-based intermediaries will be canvassed.

In addition, this chapter will examine the suitability of existing legislation identified and discussed herein to regulate cryptocurrency-based intermediaries; and cryptocurrency-based intermediaries' and users' risk.

3.1 Conventional Financial Intermediaries

Conventional financial intermediaries act as middlemen¹⁵⁵ and matchmakers¹⁵⁶ that facilitate trade within the conventional financial market with the general purpose of effectuating more efficient transactions.¹⁵⁷

In comparison to conventional financial intermediaries, and as is postulated in chapter two, cryptocurrency-based intermediaries provide similar matchmaking services; act as middlemen; and further aim to effectuate and facilitate efficient transactions within the cryptocurrency market.

Conventional financial intermediaries provide services that include taking deposits from the general public and safeguarding such deposits;¹⁵⁸ exchanging currency (national and/or foreign) for other currency (national and/or foreign);¹⁵⁹ and remittance transfer services aimed at facilitating and guaranteeing the flow of money from a sender to a recipient.¹⁶⁰

The provision of the aforementioned services requires compliance with regulatory and supervisory legislation in the selected African jurisdictions, as is pointed out below.

It is pertinent to point out that South Africa is the only jurisdiction, from the selected African countries, that has legislation specifically aimed at regulating advisory and intermediary services within the financial sector.

However, reference to conventional financial intermediary, for the purpose of this discussion, will include deposit-taking because of its similarity to cryptocurrency wallet services; conventional money remittance services because of its similarity to cryptocurrency-based remittance services; and conventional currency exchanges because of its similarity to cryptocurrency-based exchanges.

¹⁵⁵ McCoy PA ‘Degrees of Intermediation’ (2015) 50 *Wake Forest Law Review* 554. Also see Ansari SA *Financial Intermediaries and Industrial Development* (1998) 7.

¹⁵⁶ Lin TCW ‘Infinite Financial Intermediation’ (2015) *Wake Forest Law Review* 646.

¹⁵⁷ Lin (2015) 648.

¹⁵⁸ Lin (2015) 643.

¹⁵⁹ Lin (2015) 643.

¹⁶⁰ Orozco M ‘Market and Financial Democracy: The Case for Remittance Transfers’ (2005) 1 *Journal for Payment Systems Law* 166-167.

Therefore, all regulatory legislation governing the aforementioned services within South Africa, Nigeria and Kenya will be discussed in the sequence of cryptocurrency-based intermediaries, including a discussion of deposit-taking; banking; financial service and products provision; money remittance services; and currency exchanges.

3.2 Legislation governing conventional financial intermediaries and the application thereof to cryptocurrency-based intermediaries

This section discusses existing legislation regulating and supervising conventional financial intermediaries; and services and products they provide within South Africa, Nigeria and Kenya.

3.2.1 South Africa

Financial intermediaries, banking institutions, financial products and services providers are governed by three different pieces of legislation in South Africa, namely the Financial Advisory and Intermediary Services Act 37 of 2002; the Banks Act 94 of 1990; and the Financial Services Regulator Act 9 of 2017.¹⁶¹

(a) Financial Advisory and Intermediary Services Act 37 of 2002 (FAIS Act, 2002) (as amended by the Financial Services Regulation Act 9 of 2017)

The FAIS Act, 2002 is aimed at, amongst other things, the regulation relating to the rendering of certain financial advisory and intermediary services to clients.

The FAIS Act, 2002 requires financial services providers and their representatives to obtain a licence before acting or offering to act as a financial services provider.¹⁶² The FAIS Act, 2002 further requires financial services providers and their representatives to comply with fit and proper requirements issued under section 6A of the FAIS Act, 2002.

¹⁶¹ This research takes cognisance of the fact that some parts of the FSR Act, 2017, although passed, are still not in operation at this point in time.

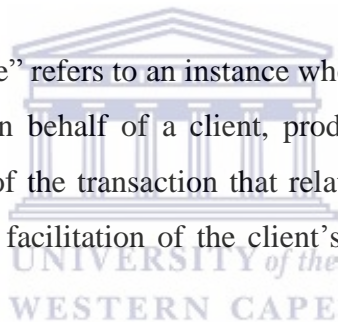
¹⁶² Section 7 of the FAIS Act, 2002.

It defines a ‘financial service provider’ as any person that gives advice in respect of financial products and/or provides intermediary services, as a regular feature of the business of such a person.¹⁶³

The FAIS Act, 2002 further provides that a financial product includes the products that are offered or serviced by a financial services provider. Examples of such products include shares, debentures, money-market instruments, insurance, benefits provided by pension funds and friendly societies and deposits (as defined by the Banks Act, 1990).¹⁶⁴

The term “advice” encompasses any recommendation, guidance or proposal of a financial nature provided to any client, specifically, in relation to the purchase or investment of any financial product; or incurring of any liability or the acquisition of any right or benefit in respect of any financial product; or on the variation of any term or condition applying to a financial product, on the replacement of any such product, or on the termination of any purchase of or investment in any such product.¹⁶⁵

The term “intermediary service” refers to an instance where a person does not provide advice, but performs any other act on behalf of a client, product or supplier.¹⁶⁶ The intermediary facilitates the administration of the transaction that relates to the financial product, whereas advisory services refer to the facilitation of the client’s decision in respect of the financial product.¹⁶⁷



Conducting financial products or services without the necessary authorisation in terms of section 7 of the FAIS Act, 2002 constitutes an offence in terms of section 36(1) of the FAIS Act, 2002 and any person doing so will, on conviction be liable to a fine or imprisonment or both a fine and imprisonment.

The determination whether the FAIS Act, 2002 applies to cryptocurrency-based intermediaries depends on whether cryptocurrency-based intermediaries provide advice; an

¹⁶³ Section 1 of the FAIS Act, 2002; Jones MW & Schoeman HC *An Introduction to South African Banking and Credit Law* (2006) 22 (hereinafter referred to as ‘Jones & Schoeman (2006)’).

¹⁶⁴ Section 1 of the FAIS Act, 2002; Jones & Schoeman (2006) 22.

¹⁶⁵ Section 1 of the FAIS Act, 2002.

¹⁶⁶ Jones & Schoeman (2006) 22.

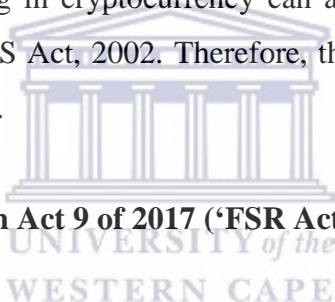
¹⁶⁷ Jones & Schoeman (2006) 22.

intermediary service; or is a financial service provider as contemplated by the FAIS Act, 2002.

The FAIS Act defines all the aforementioned terms in relation or relative to a financial product. The FAIS Act provides a comprehensive list of that which entails a financial product,¹⁶⁸ none of which includes cryptocurrency or the act of trading in cryptocurrency¹⁶⁹ as postulated in chapter one.

A financial service provider is perceived as one who provides advice and/or an intermediary service in relation to a financial product, which then results in the same conclusion, that is, that cryptocurrency or the act of trading in cryptocurrency does not satisfy the list provided in the definition of ‘financial product’.

Therefore, cryptocurrency-based intermediaries do not provide financial services or intermediary services or any advice in relation to financial products as contemplated by the FIAS Act, 2002. Cryptocurrency or the act of trading in cryptocurrency can also not be considered as a financial product as contemplated by the FIAS Act, 2002. Therefore, the FIAS Act, 2002 does not apply to cryptocurrency-based intermediaries.



(b) Financial Services Regulation Act 9 of 2017 (‘FSR Act, 2017’)

The purpose of the FSR Act, 2017 is to, amongst others, regulate and supervise financial product providers and financial services providers; to preserve and enhance financial stability; to improve market conduct in order to protect financial consumers; to provide for making regulatory instruments including prudential standards, conduct standards and joint standards; and to provide for a licensing regime.¹⁷⁰

Section 2 provides a similar definition of ‘financial product’ as the FAIS Act, 2002, with the addition that ‘any facility or arrangement may be designated as a financial product’.

¹⁶⁸ A financial product further includes a deposit as defined in the Banks Act, 1990. Whether the services provided by cryptocurrency-based intermediaries includes deposit taking will be discussed under Paragraph 3.2.1(c) below.

¹⁶⁹ The reference to ‘the act of trading in cryptocurrency’ means, for the purpose of this discussion, the exchange of cryptocurrency; the provision of a platform to users to exchange cryptocurrency; the purchase and sale of cryptocurrency; matching buyers and sellers to purchase and sell cryptocurrency; and the remittance of cryptocurrency.

¹⁷⁰ Preamble of the FSR Act.

In terms of section 2(2), any facility or arrangement may, through Regulations, be designated as a financial product, provided that it is not regulated by any other financial sector law, and if, doing so would advance the object of the FSR Act;¹⁷¹ and the facility or arrangement is the one through which, or through the acquisition of which a person conducts lending; makes a financial investment and manages financial risk.

In terms of section 3, a financial service refers to any activity conducted in South Africa in relation to a financial product, foreign financial product, a financial instrument or a foreign financial instrument. In terms of section 3, these activities ranges from offering, promoting, marketing or distributing; providing advice, recommendations or guidance; operating or managing; payment services; intermediary services as defined by the FAIS Act, 2002; to services relating to the buying and selling of foreign exchange.

The FSR Act, 2017 defines a financial product provider and financial service provider as a person that, as a business, provides a financial product or service, respectively.

Furthermore, section 111 of the FSR Act, 2017, requires that any person providing financial services, financial products and foreign financial products must attain a licence before providing such product or services.

In addition and in terms of section 266 of the FSR Act, 2017, any person who conducts a financial service or a financial product without obtaining a licence in terms of the section 111 of the FSR Act, 2017 commits an offence and is, upon conviction, guilty of a fine or imprisonment or both a fine and imprisonment.

The determination whether the FSR Act, 2017 applies to cryptocurrency-based intermediaries depends on whether cryptocurrency-based intermediaries provide a financial product or financial service; or whether cryptocurrency can be designated as a financial product, as contemplated by the FSR Act, 2017.

¹⁷¹ In terms of section 7(1), the object of the FSR Act, 2017 is to achieve a stable financial system that works in the interests of financial customers and that supports balanced and sustainable economic growth in South Africa.

(i) **Whether cryptocurrency-based intermediaries are financial products providers as contemplated by the FSR Act, 2017?**

The FSR Act, 2017 defines a financial product provider as a person that provides financial products. The FSR Act, 2017 defines a financial product in a similar manner as the FAIS Act, 2002.

Therefore, it is trite to conclude that cryptocurrency-based intermediaries do not provide a financial product, unless ‘cryptocurrency’ or the ‘act of trading in cryptocurrency’ is designated as a financial product in terms of section 3 of the FSR Act, 2017.

(ii) **Whether cryptocurrency or the act of trading in cryptocurrency can be designated as a financial product as contemplated by the FSR Act, 2017?**

Any facility or arrangement can be designated as a financial product provided that it is not regulated by another financial sector law; and if such designation is aimed at achieving the objects of the FSR Act, 2017, and such facility or arrangement serves as a conduit through, which a person conducts lending, makes a financial investment and manages financial risk.

The FSR Act, 2017 however, does not define ‘a facility’ or ‘an arrangement’, neither does it provide any direction regarding the form such facility or arrangement can take. Whether cryptocurrency or the act of trading in cryptocurrency can be designated as a financial product would depend on whether it complies with the aforementioned requirements.

(iii) **Whether cryptocurrency-based intermediaries are financial service providers as contemplated by the FSR Act, 2017?**

A financial service provider is one that provides a financial service. A financial service is any activity conducted in relation to a financial product. Therefore, for cryptocurrency-based intermediaries to provide a financial service, they must be engaged in an activity that relates to a financial product. It was previously concluded that cryptocurrency or the act of trading in cryptocurrency is not a financial product, and the same conclusion applies in this instance.

In addition, any cryptocurrency-related services conducted by cryptocurrency-based intermediaries will not qualify as the provision of a financial service, and therefore

cryptocurrency-based intermediaries are not financial service providers as contemplated by the FSR Act, 2017.

Therefore, the FSR Act, 2017 does not apply to cryptocurrency-based intermediaries, unless cryptocurrency or the act of trading in cryptocurrency are designated as financial products, which is not the case currently.

(c) **Banks Act 94 of 1990 ('Banks Act, 1990') (as amended by the FSR Act)**

The purpose of the Banks Act, 1990 is to provide for the regulation and supervision of the business of public companies taking deposits from the public.¹⁷²

The Banks Act, 1990 defines a 'bank' as "a public company registered as a bank in terms of the Banks Act. Furthermore, section 13(2) requires a bank to be incorporated as a public company in terms of the Companies Act 71 of 2008";¹⁷³ and the business of a bank as encompassing, amongst other things, acceptance of deposits from the general public as a regular feature of business in question",¹⁷⁴ including any activity that may be designated as the business of a bank by the Registrar after consultation with the Governor of the Reserve Bank;¹⁷⁵

In addition, the Banks Act, 1990 defines a 'deposit' as an amount paid by the depositor to the bank subject to an agreement in terms of which the amount or part thereof is repayable, conditionally or unconditionally, on a date, specified or unspecified or under circumstances agreed upon; and no interest is payable by the bank.¹⁷⁶

Section 11 provides that no person can conduct the business of banking unless such a person is a public company and registers as a bank before conducting the business of a bank. In addition, a person intending to conduct the business of banking is required to seek

¹⁷² Preamble of the Banks Act.

¹⁷³ Section 1 of the Banks Act.

¹⁷⁴ Section 1 of the Banks Act.

¹⁷⁵ Part (e) of the definition of 'the business of a bank' under section 1 of the Banks Act, 1990. Also see Government Notice 498 GG 17895 of 27 March 1997 entitled 'Designation of Activities that are the Business of a Bank' and having perused this Notice, which declares business practices to include schemes, practice or method of trading, including any marketing or distribution to be a business of a bank. There is no indication that the designated activities listed therein can qualify as cryptocurrency-based intermediaries conducting a business of a bank.

¹⁷⁶ Section 1 of the Banks Act.

authorisation to, first, establish a bank;¹⁷⁷ and secondly, to apply for registration to conduct the business of banking.¹⁷⁸

The determination whether the Banks Act, 1990 applies to cryptocurrency-based intermediaries and the taking into custody of cryptocurrency wallets depends on whether cryptocurrency-based intermediaries are banks or provide the business of a bank; or taking custody of cryptocurrency wallet is a deposit, as contemplated by the Banks Act, 1990.

The question that needs to be considered is whether cryptocurrency-based intermediaries take deposits from the general public as regular feature of business and thus provide the business of a bank as contemplated by the Banks Act, 1990? This question requires the following questions:

(i) **Whether the act of taking custody of cryptocurrency wallets can be considered as deposits as contemplated by the Banks Act, 1990?**

A deposit is considered as an amount paid by the depositor to the depository based on agreement, repaid conditionally or unconditionally by the depository to the depositor.

As is illustrated by Paragraph 13 of Luno's Terms of Use¹⁷⁹ referred to in chapter two, the user transfers ownership of his/her/its cryptocurrency wallet to Luno who then retains full ownership and control of the private keys associated with the user's Luno account. Paragraph 13 further provides that the user has no control of, or access to, or the ability to use such private keys.

In contrast, and as previously indicated in chapter two,¹⁸⁰ a bank, although retaining control and ownership over the deposit, is required to repay such a deposit to the depositor when the depositor so requires. Furthermore, the depositor has access to the deposit at any time and can effect payment to a third party on the depositor's instruction.

¹⁷⁷ Section 12 of the Banks Act.

¹⁷⁸ Section 16 of the Banks Act.

¹⁷⁹ See Paragraph 2.2.1(f) of chapter two.

¹⁸⁰ See the discussion under Paragraph 2.1.2(a) of chapter two.

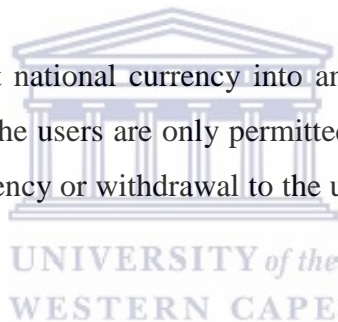
The relationship between Luno and its user is contractual and no amount or something resembling an amount is kept in the cryptocurrency wallet. The cryptocurrency wallet contains access keys, but does not contain any currency or money, which is generally denominated in a certain amount.

Therefore, the taking into custody by the cryptocurrency-based intermediary and the deposit taking activities are different and cannot be perceived as similar conduct by these types of intermediaries.

In light of the aforementioned analysis alone, a cryptocurrency wallet is not a deposit and taking custody of a cryptocurrency wallet by the cryptocurrency-based intermediaries does not amount to taking a deposit as contemplated by the Banks Act, 1990.

(ii) **Whether the acceptance of a deposit of local currency by a cryptocurrency-based intermediary be considered as a deposit in terms of the Banks Act, 1990?**

Luno permits users to deposit national currency into an account identified by Luno for the purchase of cryptocurrency. The users are only permitted to use such local currency deposits for the purchase of cryptocurrency or withdrawal to the users' bank accounts, but for no other purpose.¹⁸¹



However, despite the aforementioned, it is pertinent to examine the acceptance of local currency by cryptocurrency-based intermediaries against the definition of 'deposit' in the Banks Act, 1990.

The Banks Act, 1990 requires a deposit to be made from one person to another, based on contract and repayable conditionally or unconditionally on a specified or unspecified date. The Banks Act, 1990 provides a definition of the term 'deposit' to qualify the conduct of the business of a bank.

Therefore, whether cryptocurrency-based intermediaries accept deposits, insofar as it relates to the local currency, cannot be determined solely on the elements of the definition of a

¹⁸¹ See Paragraph 2.2.1(b) of chapter two.

‘deposit’, but must be considered in the context of conducting ‘the business of a bank’ as is done in Paragraph (cc) below.

(iii) **Whether the cryptocurrency-based intermediary take deposits as a regular feature of business and therefore, conduct the business of banking as contemplated by the Banks Act, 1990?**

Considering the discussion undertaken and conclusion reached in Paragraph (bb), the question whether cryptocurrency-based intermediaries conducts the business of a bank warrants further consideration.

The business of a bank requires acceptance of deposits from the general public as a regular feature of business.¹⁸² In addition, the definition of the term ‘business of a bank’ further provides that a person conducting the business of a bank must also solicit or advertise for deposits; use moneys received as deposits for granting of loans to others; invest such moneys; or finance business activities.¹⁸³

In addition, the definition excludes the acceptance of a deposit by any person that does not purport to accept deposits on a regular basis; and who has not advertised for or solicited such deposits, provided that such a person does not hold deposits of more than twenty (20) persons or deposits amounting to more than R 500 000.¹⁸⁴

There is no indication that Luno or any other cryptocurrency-based intermediary accepts deposits from the general public but rather from its users/customers/members; or does it accept the deposits as a regular feature of business. Furthermore, neither Luno nor any other cryptocurrency-based intermediary advertises for or solicits deposits.

The Banks Act, 1990 does not apply to cryptocurrency-based intermediaries, neither does the holding in custody of cryptocurrency wallets nor the local currency accepted as deposit qualify as a deposit as contemplated by the Banks Act, 1990.

¹⁸² In terms of the *Registrar of Banks v Net Income Solutions and three (3) others* (3056/13) [2013] ZAWCHC [40] ‘regular feature of business’ means as ‘part of the operations of such business’.

¹⁸³ Part (b) and (c) of the definition of ‘the business of the bank’ contained in section 1 of the Banks Act, 1990.

¹⁸⁴ Part (aa)(i) of the definition of ‘the business of the bank’ contained in section 1 of the Banks Act, 1990.

In light of the aforementioned, none of the legislation discussed above governing conventional financial intermediaries in South Africa can be applied to cryptocurrency-based intermediaries, neither can taking into custody of cryptocurrency wallets be considered as deposit-taking.

3.2.2 Nigeria

Banks and other financial institutions in Nigeria are regulated by the Banks and Other Financial Institutions Act Cap B3, Laws of Federation of Nigeria, 2004 (as amended) ('BOFI Act, 2004'). The purpose of the BOFI Act, 2004 is to regulate banking and other financial institutions.¹⁸⁵

Section 1(5)(a) provides that a person is deemed to receive money as a deposit if the person accepts deposits from the general public as a regular feature of business or if it issues and advertisement or solicits for such deposits. Section 1(5)(b) further provides that deposits must be money received in fixed amounts, repayable either conditionally or unconditionally on a specified or unspecified date.

In terms of section 2(1) only a person that is a company incorporated in Nigeria and holds a valid banking licence can conduct banking business in Nigeria. The BOFI Act, 2004 defines a 'banking business' as a business that receives deposits; or provides financing; or conducts any other business as may be determined.¹⁸⁶

In addition, Part II, more particularly section 58(1), provides only insurance and stockbroking activities can be carried on in Nigeria as other financial business except if such financial business is a company duly incorporated in Nigeria and holds a valid licence.¹⁸⁷

In terms of section 2(2) an section 59(6) of the BOFI Act, 1991, any person conducting a business or financial business without obtaining a valid licence is guilty of an offence, and will, upon conviction, be liable to a fine or imprisonment or both a fine and imprisonment.

¹⁸⁵ Preamble of the BOFI Act, 2004.

¹⁸⁶ Section 66 of the BOFI Act, 1991.

¹⁸⁷ Section 59(1) of the BOFI Act, 1991.

The determination whether the BOFI Act, 2004 applies to cryptocurrency-based intermediaries and the taking into custody of cryptocurrency wallets depends on the following questions:

- (a) **Whether the act of taking custody of cryptocurrency wallets can be considered as deposits as contemplated by the BOFI Act, 2004?**

The analysis undertaken and the conclusion reached under Paragraph 3.2.1(c) above regarding the same question in relation to the South African Banks Act, 1990 equally applies in the instance of a deposit as contemplated in the BOFI Act, 2004. The taking into custody of cryptocurrency wallets by cryptocurrency-based intermediaries does not constitute deposit taking or a deposit as contemplated by the Banking Act.

- (b) **Whether the acceptance of local currency as deposits by cryptocurrency-based intermediaries qualify as deposits in terms of the BOFI Act, 2004?**

The acceptance of deposit of local currency by a cryptocurrency-based intermediary (as is the case of Luno, which also operates in Nigeria) does not qualify as a deposit as contemplated by the BOFI Act, 2004, because first, the local currency is not received from the general public but from members/users/customers of the cryptocurrency-based intermediary.

Secondly, the deposit of local currency accepted by cryptocurrency-based intermediaries is to fund the potential purchase of cryptocurrency and not as a general feature of business.

- (c) **Whether cryptocurrency-based intermediaries conduct a banking business as contemplated by the BOFI Act, 2004?**

The receiving of deposits; and the provision of financing are the only activities, unless additional activities are designated, that qualify as banking business in terms of the BOFI Act, 2004. It is therefore trite to point out that cryptocurrency-based intermediaries neither receive deposits nor provide financing, or otherwise conduct any activity are designated as banking business.

(d) **Whether cryptocurrency-based intermediaries carry on activities as ‘other financial business’ as contemplated by the BOFI Act, 2004?**

Considering that the BOFI Act, 2004 provides that only insurance and stockbroking activities are recognised as other financial business, and that cryptocurrency-based intermediaries conduct neither of those activities, it is trite to conclude that cryptocurrency-based intermediaries do not provide other financial business as contemplated in the BOFI Act, 2004.

Therefore, the BOFI Act, 2004 does not apply to cryptocurrency-based intermediaries, neither does keeping in custody of cryptocurrency-wallets qualify as deposits nor the local currency accepted in deposit by cryptocurrency-based intermediaries as contemplated by the BOFI Act, 2004.

3.2.3 Kenya

The banking and financial institutions in Kenya are regulated by the Banking Act Cap 488 of 1995 (“Banking Act, 1995”), the purpose of which is to regulate business of banking in Kenya.

The conducting of banking and financial business in Kenya requires a valid licence,¹⁸⁸ which may be granted with or without conditions in terms section 5, and revoked in terms of section 6.

A ‘bank’ means a company, which carries on, or proposes, to carry on, banking business in Kenya; and the ‘business and financial business’ means accepting from members of public money on deposit repayable on demand or at the expiry of a fixed period or after notice; and employing of money held on deposit.¹⁸⁹

Furthermore, a ‘financial institution’ means a company, other than a bank, which carries on, or proposes to carry on, financial businesses and include any other company, which the Minister may declare to be a financial institution for the purpose of this Act.¹⁹⁰

¹⁸⁸ Section 3(1) of the Banking Act.

¹⁸⁹ Section 2 of the Banking Act, 1995.

¹⁹⁰ Section 2 of the Banking Act, 1995.

In terms of section 16(2), a ‘deposit’ is defined as “a sum of money paid on terms under which it will be repaid, with or without interest or a premium, and either on demand or at a time or in circumstances agreed by or on behalf of the person making the payment and the person receiving it”.

In terms of section 16(5) a business is a deposit-taking business if, in the course of the business money received by way of deposit is lent to others; or any other activity of the business is financed, wholly or to any material extent, out of the capital of or the interest on money received by way of deposit.

The determination whether the Banking Act, 1995 applies to cryptocurrency-based intermediaries and the taking into custody of cryptocurrency wallets depends on the following questions:

- (a) **Whether the act of taking custody of cryptocurrency wallets can be considered as deposits as contemplated by the Banking Act, 1995?**

The analysis undertaken and the conclusion reached under Paragraphs 3.2.1(c) and 3.2.2(a) above regarding the same question in relation to the Banks Act, 1990 and BOFI Act, 2004 equally applies in the instance of a deposit as contemplated in the Banking Act, 1995. The taking into custody of cryptocurrency wallets by cryptocurrency-based intermediaries does not constitute deposit taking or a deposit as contemplated by the Banking Act, 1995.

It is additionally also prudent to conclude that as they do not accept deposits, cryptocurrency-based intermediaries do not conduct a deposit-taking business as contemplated by the Banking Act, 1995.

- (b) **Whether cryptocurrency-based intermediaries conduct banking and financial business as contemplated by the Banking Act, 1995?**

In terms of the Banking Act, 1995, banking and financial institutions accept deposits. As cryptocurrency-based intermediaries do not accept deposits as contemplated by the Banking Act, 1995, they do not conduct banking and financial business.

(c) **Whether cryptocurrency-based intermediaries are financial institutions as contemplated by the Banking Act, 1995?**

Cryptocurrency-based intermediaries do not conduct financial business, and therefore, are not financial institutions as contemplated by the Banking Act, 1995.

Therefore, as cryptocurrency-based intermediaries do not take deposits nor conduct banking or financial institutions or can be considered as financial institutions as contemplated by the Banking Act, 1995 does not apply to the cryptocurrency-based intermediaries.

3.3 Legislation governing conventional currency exchanges service providers and the application thereof to cryptocurrency-based currency exchanges

Conventional currency exchanges provides services that allow users to exchange one fiat (national) currency for another currency whilst subject to legislation that governs their services and operations within the currency exchange market. Similarly, and as chapter 2 points out,¹⁹¹ cryptocurrency-based exchanges allow users to exchange cryptocurrency for other cryptocurrencies or fiat currency.

The only difference between the services provided by the conventional currency exchanges and cryptocurrency-based exchanges is that the former exchanges currency designated as 'legal tender';¹⁹² and the latter exchanges currency not designated as legal tender with another that is designated as legal tender.

The conventional currency exchanges operate within a regulated environment and the discussion in this section will focus on the relevant legislation within South Africa, Nigeria and Kenya that regulate and supervise the conventional currency exchanges and the services they provide. In addition, this section will discuss whether such legislation applies to cryptocurrency-based currency exchanges.

¹⁹¹ See Paragraph 2.1.1 of chapter two.

¹⁹² Currency designated as legal tender is currency designated or impressed by law as legal tender, which then means that a creditor cannot lawfully refuse payment in such a currency. See Chung JJ 'Money as Simulacrum: The Legal Nature and Reality of Money' 5 *Hastings Business Law Journal* (2009) 113.

3.3.1 South Africa

The exchange of foreign currency in South Africa are governed by the Currency and Exchange Control Act 9 of 1933 (the Currency and the Exchange Control Act, 1933) and Exchange Control Regulations, 1961 (the Exchange Control Regulations).¹⁹³ The purpose of the Currency and Exchange Control Act, 1933 is to regulate legal tender, currency exchange and banking.

The exchange of foreign currency in South Africa is governed by the Currency and Exchange Control Act 9 of 1933 and the Exchange Control Regulations. Only an authorised dealer¹⁹⁴ is permitted to buy, sell, send, consign or deliver foreign currency¹⁹⁵.

In terms of Regulation 1, only an authorised dealer can deal in foreign currency, which refers to currency that is not legal tender in South Africa. The term ‘money’ further includes foreign currency, any bill of exchange or any negotiable instrument.

Therefore, to ascertain whether cryptocurrency-based intermediaries are currency exchanges as contemplated by the Currency and Exchange Control Act 9 of 1933 and the Exchange Control Regulations, it needs to be determined whether cryptocurrency is a foreign currency. Cryptocurrency-based exchanges allow the exchange of cryptocurrency for other cryptocurrency, and cryptocurrency does not qualify as foreign currency in terms of the Exchange Control Regulations.

Therefore, neither the Currency and Exchange Control Act, 1993 nor the Exchange Control Regulations apply to the exchange services provided by cryptocurrency-based intermediaries in South Africa.

¹⁹³ As promulgated by Government Notice R.1111 of 1 December 1961 and amended up to Government Notice No. R.445 in Government Gazette No. 35430 of 8 June 2012.

¹⁹⁴ The Exchange Control Regulations, Regulation 1, defines an ‘authorised dealer’ as, in respect of any transaction in respect of gold, a person authorised by the Treasury to deal in gold, and in respect of any transaction in respect of foreign exchange a person authorised by the Treasury to deal in foreign exchange.

¹⁹⁵ The Exchange Control Regulations, in Regulation 1, define ‘foreign currency’ as any currency, which is not legal tender in the Republic, and includes any bill of exchange, letter of credit, money order, postal order, promissory note, traveller’s cheque or any other instruments for the payment of currency payable in a currency unit, which is not legal tender in the Republic.

3.3.2 Nigeria

The foreign currency exchanges in Nigeria are governed by the Foreign Exchange (Monitoring and Miscellaneous Provisions) Act Chapter F 34 (Decree No. 17 of 1995), the purpose of which is to establish an Autonomous Foreign Exchange Market (the Market); and to provide for the monitoring and supervision of transactions conducted in the Market.

Section 41 of the Foreign Exchange (Monitoring and Miscellaneous Provisions) Act, 1995, the Market means “a market in which authorised dealers, authorised buyers, foreign exchange end-users and the Central Bank of Nigeria are participants”.

Section 41 further states that an ‘authorised dealer’ refers to any bank licensed under the BOFI Act, 2004 and, which is issued with a licence to deal in foreign currency; and an ‘authorised buyer’ refers to a *bureau de change*, a hotel or other corporate body appointed as such by the Central Bank of Nigeria.

Section 41 also defines a ‘foreign currency’ as currency other than Nigerian currency, designated as legal tender outside of Nigeria.

Section 1(1) provides that foreign exchange transactions must be conducted in the Market in accordance with the provisions of the Foreign Exchange (Monitoring and Miscellaneous Provisions) Act, 1995; and in terms of Section 2(1), all transactions must be conducted in convertible foreign currency.

In terms of section 5(1) only an authorised dealer or buyer of foreign currency, which can either be a bank or a non-banking corporate organisation, showing evidence of sufficient resources and capacity, can operate within the Market.

Therefore, currency exchange transactions in Nigeria are conducted by Market participants within the Market established in terms of the Foreign Exchange (Monitoring and Miscellaneous Provisions) Act, 1995. The Market participants must be either authorised dealers or buyers; or foreign exchange end-users; or the Central Bank of Nigeria.

In order to ascertain whether cryptocurrency-based intermediaries conduct currency exchange transactions as contemplated by the Foreign Exchange (Monitoring and Miscellaneous

Provisions) Act, 1995, it needs to be determined whether cryptocurrency is a foreign currency. Cryptocurrency-based exchanges allow the exchange of cryptocurrency for other cryptocurrency, and cryptocurrency does not qualify as foreign currency in terms of the Foreign Exchange (Monitoring and Miscellaneous Provisions) Act, 1995.

Therefore, considering that cryptocurrency-based exchanges conduct exchange transaction in cryptocurrency, the Foreign Exchange (Monitoring and Miscellaneous Provisions) Act, 1995 does not apply to cryptocurrency-based exchanges.

3.3.3 Kenya

Conventional currency exchanges in Kenya are governed by Part VIA of the Central Bank of Kenya Act 15 of 1966, which deals with the regulations of foreign exchange dealings.

In terms of section 33A(1), no person other than an authorised dealer, which includes an authorised bank; an authorised money remittance provider; an authorised micro-finance bank; or an authorised bureau,¹⁹⁶ is permitted to conduct a foreign exchange business; and in terms of section 33B(1), any person conducting a foreign exchange business must acquire a licence.

In terms of section 2 of the Central Bank of Kenya Act, 1966 'currency' refers to Kenyan currency; 'foreign currency' refers to currency other than Kenyan currency, which has been declared as legal tender in any territory outside Kenya; and 'a foreign exchange bureau' refers to a company incorporated in Kenya with the main object of buying and selling foreign currency.

Section 2 also defines 'a foreign exchange business' as a business that conducts activities of buying, selling, borrowing or lending foreign currency; or any other business involving transactions in foreign currency; and the settling of payments to or from Kenya or in Kenya between residents and non-residents.

In order to ascertain whether cryptocurrency-based intermediaries conduct foreign currency exchange business as contemplated by the Central Bank of Kenya Act, 1966, it needs to be determined whether cryptocurrency is a foreign currency. Cryptocurrency-based exchanges

¹⁹⁶ Section 2 of the Central Bank of Kenya Act, 1966.

allow the exchange of cryptocurrency for other cryptocurrency, and cryptocurrency does not qualify as foreign currency in terms of the Central Bank of Kenya Act, 1966.

Cryptocurrency-based exchanges are not foreign exchange businesses as they do not conduct activities of buying, selling, borrowing or lending foreign currency as contemplated by Part VIA of the Central Bank of Kenya Act, 1966. In fact, they do not conduct any activities related to foreign currency. Therefore, the Central Bank of Kenya Act, 1966 does not apply to cryptocurrency-based exchanges.

The aforementioned legislation is the only legislation that regulates and supervises currency exchange in the selected jurisdictions.

As noted in Paragraph 2.1.1¹⁹⁷ and Paragraph 2.2¹⁹⁸ of chapter 2, cryptocurrency-based exchanges act much like conventional currency exchanges, the only difference being that the former exchanges cryptocurrency for local currency designated as legal tender in the jurisdictions they operate, for instance cryptocurrency for the South African Rand if the cryptocurrency-based exchange operates within South Africa.

However, although cryptocurrency-based exchanges provide the service of exchanging cryptocurrency for fiat currency or vice versa, the legislation discussed only recognizes the exchange of one fiat currency for another, for instance South African Rand for United States Dollar, and therefore considering such legislation, the currency exchange services provided by cryptocurrency-based exchanges do not qualify as foreign exchange services.

3.4 Legislation governing conventional money remittance service providers and the application thereof to cryptocurrency-based remittance service providers

Conventional money remittances assume the form of cash or credit transfers and transfers in kind (involving transfers of goods).¹⁹⁹ Cash transfers are sent in either the foreign currency or the local currency by means of physical transfer of cash. Credit transfers are based on

¹⁹⁷ Paragraph 2.1.1 of chapter two discusses cryptocurrency-based exchanges.

¹⁹⁸ Paragraph 2.2 of the chapter two provides examples of selected cryptocurrency-based intermediaries in South Africa, Nigeria and Kenya.

¹⁹⁹ IMF International Transactions in Remittances: Guide for Compilers and Users (2009) 6-7 ('IMF (2009)').

payment instructions from providers in the sending country to providers in the receiving country.²⁰⁰

In contrast, and as postulated in Paragraph 2.1.3 of chapter two, cryptocurrency-based remittance remittances transfer cryptocurrency instead of money (whether cash or credit).

This section analysis and examines legislation regulating and supervising conventional money remittances service provision in South Africa, Nigeria and Kenya.

3.4.1 South Africa

South Africa does not have legislation that specifically regulates conventional remittance services provision or remittance service providers, however the Exchange Control Regulations control the taking and sending of South African Rand in or out of South Africa as pointed out below.

In terms of Regulation 3(1)(*bis*), only a person granted permission by the Treasury or a person authorised by the Treasury may, amongst other things, take or send any South African Rand in or out of South Africa; or in terms of Regulation 3(1)(c), make any payment, to, or in favour, or on behalf of a person resident outside South Africa, or any sum to the credit of such person.

As remittance service providers receive South African Rand for transmission out of South Africa or facilitate payment to a person resident outside South Africa, the aforementioned sub-Regulations become relevant to their operations, which means, remittance service providers require permission from the Treasury or from a person authorised by the Treasury.

Cryptocurrency-based remittance services do not remit local currency, but receive cryptocurrency from the sender and remit such cryptocurrency to the recipient, who then receives local currency from a cryptocurrency-based remittance service provider.

²⁰⁰ IMF (2009) 6-7.

Therefore, although providing remittance services, the cryptocurrency-based remittance service providers do not remit any national currency, but rather cryptocurrency, which is not recognised as foreign currency²⁰¹ or legal tender.

3.4.2 Nigeria

A letter dated 26 September 2014 and issued by the Central Bank of Nigeria contains the Guidelines for the Operation of International Transfer Services in Nigeria issued by the Central Bank of Nigeria (the 2014 Guidelines)²⁰².

The aforementioned letter is addressed to the members of the public, authorised dealers and money transmission service operators advising them to operate within the ambit of the 2014 Guidelines.

The 2014 Guidelines address business rules governing the operation of international money transfer services in Nigeria. In addition, it sets the basis for the regulation of services offered at different levels and by diverse participants.²⁰³

The following paragraphs of the 2014 Guidelines are relevant to this discussion:

- (a) Paragraph 9 of the 2014 Guidelines defines a ‘money transfer operator’ as an international money transfer service operator that is incorporated in Nigeria; a ‘transaction’ as a transfer sent or a transfer received as the case may be; and a ‘transfer amount’ as funds collected from the sender for a transfer, excluding applicable fees;
- (b) Paragraph 2.1 of the 2014 Guidelines requires any person conducting international money transfer services to acquire a valid licence; and in terms of Paragraph 8.1 of the 2014 Guidelines, any person conducting such services without a valid licence will be sanctioned and/or prosecuted in accordance with the BOFI Act, 2004;

²⁰¹ See definition of foreign currency under Paragraph 3.3.1(a) above.

²⁰² Guidelines for the Operation of International Transfer Services in Nigeria issued by the Central Bank of Nigeria date 26 September 2014 (hereinafter referred to as ‘the 2014 Guidelines’).

²⁰³ Paragraph 1.2 of the 2014 Guidelines.

- (c) Paragraph 3.6.4 of the 2014 Guidelines requires currency to be given to a money transfer operator for transfer out of Nigeria to be in the form of Naira, the Nigerian national currency; and in terms of Paragraph 4.3 of the 2014 Guidelines, money transfer operators must make payment to customers only in Naira;
- (d) Paragraph 3.12 of the 2014 Guidelines requires money transfer operators to comply with Anti-Money Laundering and Combating of Terrorism in Banks and Other Financial Institutions Regulations, 2013; and all other applicable laws and regulations;
- (e) Paragraph 4.1 of the 2014 Guidelines require the money transfer operator to disclose to its customers the details of the exchange rate; meaning of technical terms and acronyms used; and prevailing exchange rates at all times; and
- (f) Paragraph 5.1 of the 2014 Guidelines requires money transfer operators to set up a complaints management unit to resolve complaints or disputes submitted by its customers; and Paragraph 6.1 of the 2014 Guidelines requires money transfer operators to request from customers some form of identification authentication before making use of their services.

Cryptocurrency-based intermediaries' transactions encompass the same as the transfer sent of funds or receiving funds as defined by the 2014 Guidelines. The terms defined in the 2014 Guidelines postulate a form of service that indicate sending and receiving funds from a sender to a recipient using a money transfer operator subject to applicable legislation and regulations; and the 2014 Guidelines.

This is no difference in the services provided by cryptocurrency-based remittance service providers or those described in the 2014 Guidelines and provided by conventional money transfer operators in Nigeria, save for the fact that cryptocurrency-based remittance service providers receive cryptocurrency for transfer from a sender and give as payment to the recipient, in this case, Naira.

A person can only provide remittance services if such a person is licensed and should only transfer Naira. This means that cryptocurrency-based remittance service providers are in breach of the 2014 Guidelines by providing similar services and transferring an unrecognised currency.

As the provision of money transfer services in Nigeria requires licensing and as cryptocurrency-based remittance service providers in Nigeria provide similar services as indicated in the 2014 Guidelines, it is correct to conclude that cryptocurrency-based remittance services are subject to 2014 Guidelines and the BOFI Act, 2004, but only as far as it relates to remittance service provision.

3.4.3 Kenya

Part VIA of the Central Bank of Kenya Act, 1966 and the Money Remittance Regulations, 2013²⁰⁴ governs remittance service providers.

Section 2 of the Central Bank of Kenya Act, 1966 provides the following definitions:

- (i) An ‘authorised remittance service provider’ should be a money remittance operator licensed to provide the business of money remittance; and a money remittance provider accepts monies for the purpose of transmitting it to persons resident within Kenya or another country; and
- (ii) A ‘money remittance operator’ is defined as a company incorporated in Kenya whose main object consists of the acceptance of monies for the purpose of transmitting them to persons in Kenya or another country as prescribed by the Central Bank of Kenya by regulations.

Regulation 2 of the Money Remittance Regulations, 2013 further provides the following definitions:

- (iii) A ‘money remittance business’ means “a service for the transmission of money or any representation of monetary value without any payment account created in the name of the payer and the payee where the money is received for the sole purpose of transferring a corresponding amount to payee or to another payment service operator acting on behalf of the payee; or funds received on behalf of, and made available to the payee”; and
- (iv) A ‘money remittance operator’ means a person licensed to undertake money remittance business.

²⁰⁴ Kenya Gazette Supplement No. 56 date 19 April 2013.

The Money Remittance Regulations, 2013 further provides, in terms of Regulation 4, that conducting money remittance business requires incorporation as a limited liability company under the Companies Act; and licensing.

The issue of whether a cryptocurrency-based remittance service providers in Kenya provide money remittance services as contemplated by the Central Bank of Kenya Act, 1996 and the Money Remittance Regulations, 2013 is considered in the case of *Lipisha Consortium Limited and BitPesa Limited v Safaricom Limited*²⁰⁵ (the *BitPesa Case*).

In this case the Court considered, amongst other things, whether the Second Petitioner (BitPesa Limited) was engaging in illegal activities by conducting remittance services, which services the Second Petitioner admitted to providing,²⁰⁶ without the approval of the Central Bank of Kenya.²⁰⁷

In terms of Paragraph 17 of the *BitPesa Case*, and according to the Respondent (Safaricom Limited), the Respondent had previously asked the Second Petitioner to obtain formal approval from the Central Bank of Kenya. The Central Bank of Kenya however declined to grant approval to the Second Petitioner.

When the Second Petitioner sought approval from the Central Bank of Kenya as a money remittance services provider, the Central Bank of Kenya declined to approve as the Second Petitioner dealt in bitcoin, and as long as the Second Petitioner dealt in bitcoin it could not use the word “money remittance” or “money transfer”. The Central Bank of Kenya further stated that it did not regulate cryptocurrency.²⁰⁸

In the Court’s preliminary view, when the Second Petitioner stated that it engaged in the business of accepting bitcoin from various countries of the world and exchanging it for local African currencies, including but not limited to the Kenyan Shilling, the Second Petitioner was engaged in money remittance business. The Court’s preliminary view was based on the

²⁰⁵ *Lipisha Consortium Limited and BitPesa Limited v Safaricom Limited* [2015] eKLR available at <https://www.kenyalaw.org> (accessed 24 October 2018) (hereinafter referred to as ‘the *BitPesa Case*’).

²⁰⁶ *BitPesa Case* Paragraph 33.

²⁰⁷ *BitPesa Case* Paragraphs 16 and 76.

²⁰⁸ *BitPesa Case* Paragraph 76.

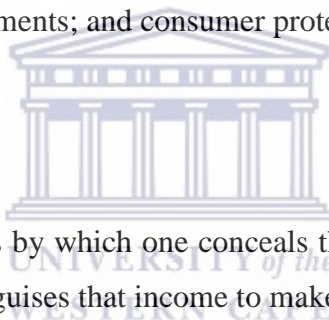
definition of “money remittance business”, more particularly the part of the definition referring to “or any representation of money value”.²⁰⁹

The Court thus, relying on the aforementioned part of the definition of “money remittance business”, concluded that bitcoin represented monetary value and therefore, is the only reason it can be exchanged for the Kenyan shilling.²¹⁰

Therefore, the Kenyan Court has clearly concluded that cryptocurrency-based remittance service providers are providing money remittance business and therefore subject to the Central Bank of Kenya Act, 1966 and the Money Remittance Regulations, 2013.

3.5 Additional issues that require compliance by conventional financial intermediary and the application thereof to cryptocurrency-based intermediaries

For the purpose of this discussion, all conventional financial intermediaries must comply with anti-money laundering requirements; and consumer protection measures. For instance:



3.5.1 Anti-money laundering

Money laundering is a process by which one conceals the existence, illegal source, or illegal application of income, and disguises that income to make it appear legitimate.²¹¹

The prohibition and elimination of money laundering is addressed in South Africa, Nigeria and Kenya through the legislation that follows below:

- (a) In South Africa, the Prevention of Organised Crime Act 121 of 1998 criminalises money laundering; introduces measures to combat money laundering; provides for the prohibition of money laundering and for an obligation to report information.

Furthermore, the Financial Intelligence Centre Act 38 of 2001 (FICA, 2001) is aimed at imposing certain duties on institutions and other persons who might be used for money

²⁰⁹ *BitPesa Case* Paragraph 78.

²¹⁰ *BitPesa Case* Paragraph 79.

²¹¹ President's Commission on Organised Crime, Interim Report to the President and Attorney-General The Cash Connection: Organised Crime, Financial Institutions, and Money Laundering (1984) 7 referred to in Mann TT 'Money Laundering' 2 (2007) 44 *American Criminal Law Review* 769 (hereinafter referred to as 'Mann (2007)').

laundering purposes, and the financing of terrorist and related activities; to provide for customer due diligence measures; and to provide for a risk based approach to client identification and verification.

In terms of the FICA, 2001, an accountable institution is precluded from establishing a business relationship or entering into a transaction with an anonymous client or a client with an apparent false identity or fictitious name;²¹² and to identify and verify a client's identity before entering into a business relationship or a single transaction.²¹³

- (b) In Nigeria, the Money Laundering (Prohibition) Act 25 of 2011 enhances the scope of money laundering offences and customer due diligence measures; imposes a duty to report international transfer of funds and securities exceeding a prescribed amount by indicating the nature and amount of the transfer, the name and addresses of the sender and receiver of the funds and securities;²¹⁴ and requires identification and verification of the identity of a customer, to identify and take reasonable measures to verify the identity of a beneficial owner.²¹⁵
- (c) In Kenya, the Proceeds of Crime and Anti-Money Laundering Act 9 of 2009 governs money laundering activities in Kenya, the purpose of which is to provide for the offence of money laundering and to introduce measures for the combating the offence; to provide for identification, tracing, freezing and confiscation of the proceeds of crime.

The Proceeds of Crime and Anti-Money Laundering Act 9 of 2009 requires a reporting institution to monitor unusual, suspicious or large transactions; and if such transactions seem suspicious, to report the transactions;²¹⁶ to take reasonable measures to satisfy itself of the true identity of any applicant seeking to enter into a business relationship with the reporting institution;²¹⁷ and to establish and maintain customer records.²¹⁸

²¹² Section 20A of the FICA, 2001.

²¹³ Section 20A of the FICA, 2001.

²¹⁴ Section 2 of the Money Laundering (Prohibition) Act 25 of 2011.

²¹⁵ Section 3 of the Money Laundering (Prohibition) Act 25 of 2011.

²¹⁶ Section 44 of the Proceeds of Crime and Anti-Money Laundering Act 9 of 2009.

²¹⁷ Section 45 of the Proceeds of Crime and Anti-Money Laundering Act 9 of 2009.

²¹⁸ Section 46 of the Proceeds of Crime and Anti-Money Laundering Act 9 of 2009.

The aforementioned legislation imposes requirements on conventional financial intermediaries to monitor suspicious activities and transaction; and they are further required to identify and verify the identities and sources of income of their customers.

Cryptocurrency-based intermediaries are not under any obligation to disclose the identities of the users, neither are they obligated, under any law, to require their users to disclose their identities or the sources of their income.

3.5.2 Consumer protection

- (a) In South Africa, legislation aimed at consumer protection within South Africa includes the Consumer Protection Act 68 of 2008; the FAIS Act, 2002; the FRS Act, 2017; and the Banks Act, 1990.

The Consumer Protection Act, 2008 regulates the provision of goods and services, inclusive of financial services,²¹⁹ to consumers; and the FSR Act, 2017 is aimed at the improvement of market conduct in order to protect the financial consumer,²²⁰ which can be at a equivalent to or higher than the standard of protection afforded by the Consumer Protection Act, 2008²²¹.

- (b) In Nigeria, the Consumer Protection Council Act Chapter Cap 25 of 2004 establishes the Consumer Protection Council (section 1(1)) to promote and protect the interest of the consumers over all products and services.
- (c) In Kenya, Article 46 of the Constitution of Kenya provides for consumer rights, which applies to all goods and services offered by public entities and private persons. In addition, the Consumer Protection Act 46 of 2012 provides for the protection of the consumer to prevent unfair trade practices in consumer transactions.

The aforementioned legislation on consumer protection generally applies across all sectors, inclusive of the financial sector and covers all good and services. In South Africa, the FSR Act, 2017 makes specific provision for the protection of the financial consumer.

²¹⁹ See definition of ‘service’ in section 1 of the Consumer Protection Act, 2002.

²²⁰ The FSR Act, 2017 defines a financial customer as “a person to, or for whom, a financial product, financial instrument or a financial service is provided”.

²²¹ Section 85 of the FSR Act, 2017.

Needless to say, the general nature of application of the aforementioned consumer protection legislation extends the scope of application to cryptocurrency-based intermediaries as they provide services, irrespective of their nature, to their users.

3.6 Suitability of existing legislation regulating conventional financial intermediaries to cryptocurrency-based intermediaries' regulation

The suitability of the aforementioned legislation to regulate cryptocurrency-based intermediaries and their related risks lies in the effectiveness and adequacy of such legislation to regulate cryptocurrency-based intermediaries, the service they provide and the activities they conduct; and to address their related risks.

As pointed out in chapter two, cryptocurrency related risks include the risk of exchange breach, which include security breach, data loss, insider scam, legal risk and money laundering risk. For the user of such cryptocurrency-based intermediaries, includes the risk of loss of cryptocurrency, the risk of closure and inability to access the website of cryptocurrency-based intermediary, the risk of irrevocable transactions and the inability to be reimbursed for losses suffered, the insolvency of the cryptocurrency-based exchange.

It is evident from the aforementioned that cryptocurrency-based intermediaries' regulation requires regulation that addresses cryptocurrency-based intermediaries' risk in addition to rules and requirements relating to technical compliance. These essentially means that cryptocurrency-based intermediaries' regulation require a risk-based and rules-based approach to regulation.

The risk-based and rules-based approaches encompass the following as pointed out by Nicholls:²²²

3.6.1 The rules-based approach is referred to as the 'traditional notion of regulation exerting public authority through a system of rules and laws in which the regulator ensures technical compliance by the regulated.'²²³

²²² Nicholls A 'The challenges and benefits of risk-based regulation in achieving scheme outcomes' (Paper presented to the Actuaries Institute Schemes Seminar during 08 to 10 November 2015) 2 available at <https://www.actuaries.asn.au/Library/Events/ACS/2015/NichollsRegulation.pdf> (accessed 02 November 2018) (hereinafter referred to as 'Nicholls (2015)').

²²³ Nicholls (2015) 2.

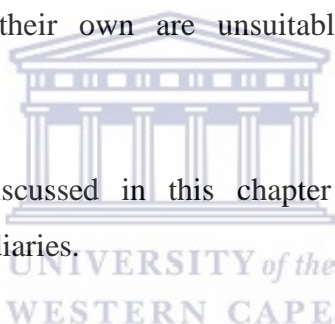
Nicholls criticises this approach by noting that it is reactive, focused on enforcement and may miss critical emerging risks because regulators consider such falling ‘outside the scope regulation’.²²⁴

3.6.2 The risk-based approach to regulation focuses on risks and harm prevention, the promotion of outcomes and to choose appropriate instruments to achieve performance.²²⁵

The legislation discussed in this chapter impose rules and regulations that require compliance by the regulated industry, for instance, the aforementioned legislation requires licensing or registration or authorisation before conducting the regulated activities;²²⁶ and imposes penalties for non-compliance.²²⁷

Although the requirement of obtaining some form of authorisation to conduct regulated services and non-compliance with such a requirement results in penalties does not cause the aforementioned legislation unsuitable to regulate cryptocurrency-based intermediaries, those rules and requirements on their own are unsuitable to address cryptocurrency-based intermediaries’ related risks.

Therefore, the legislation discussed in this chapter will not be suitable to regulate cryptocurrency-based intermediaries.



CONCLUSION

This chapter explored and examined the applicability to and suitability of existing legislation regulating conventional financial intermediaries to cryptocurrency-based intermediaries. In the former instance, this chapter determined that, save for the legislation governing consumer protection and the applicability of Kenyan money transfer laws by virtue of the *Bitpesa case*, is not applicable to cryptocurrency-based intermediaries.

²²⁴ Nicholls (2015) 2.

²²⁵ Nicholls (2015) 2.

²²⁶ The licensing or registration or seeking authorisation requirements are indicated in the previous paragraph. All conventional financial intermediaries require authorisation in the form of a licence or registration to conduct regulated services and products.

²²⁷ See the discussion under the previous paragraph, more particularly, the discussion pertaining to conventional financial intermediaries.

In the latter instance, this chapter determined that existing legislation discussed in this chapter will not be suitable to regulate cryptocurrency-based intermediaries as such legislation is rules-based instead of risk-based. It will therefore not address the risks identified in chapter two.

Chapter four will discuss the rationale for cryptocurrency-based intermediaries' regulation; and the global regulatory responses to cryptocurrency-based intermediaries in order to explore the most suitable regulatory approach to cryptocurrency-based intermediaries.



CHAPTER FOUR

THE RATIONALE FOR CRYPTOCURRENCY-BASED INTERMEDIARIES' REGULATION AND GLOBAL REGULATORY RESPONSES TO CRYPTOCURRENCY-BASED INTERMEDIARIES

INTRODUCTION

Designing a cryptocurrency-based intermediaries' regulatory framework requires an understanding of the nature of cryptocurrency-based intermediation, services they provide and the risks their use may pose, as is pointed out in chapter two. This means that chapter two dispensed of the first sub-objective of this research.²²⁸

Furthermore, designing of cryptocurrency-based intermediaries' regulation further requires an analysis and determination of the applicability of existing legislation governing comparable or similar institutions, namely conventional financial intermediaries and/or intermediation and the services provided by such institutions, as is undertaken in chapter three.

Chapter three concluded that current regulatory legislation applicable to conventional financial intermediaries, save for consumer protection, which is of a general application; and legislation regulating money transfer services within Kenya; is not applicable or suitable to regulate cryptocurrency-based intermediaries. This means that chapter three dispensed of the second and third sub-objectives of this research.²²⁹

This chapter is aimed at addressing the third sub-objective, that is, to explore potential regulatory approaches to cryptocurrency-based intermediaries, which will speak to the ultimate design of a cryptocurrency-based intermediaries' regulatory framework.

Therefore, this chapter will first, explore the rationale for cryptocurrency-based intermediaries' regulation; and secondly, examine current global regulatory responses to cryptocurrency and

²²⁸ The first sub-objective related to the provision of an understanding of cryptocurrency-based intermediaries and identifying potential cryptocurrency-based intermediaries' and users' related risks.

²²⁹ The second and third sub-objective related to an analysis and examination of existing legislation governing conventional financial intermediaries and determining the applicability and suitability of such legislation to regulate cryptocurrency-based intermediaries.

cryptocurrency-based intermediaries; and thirdly, identify, if possible, a suitable approach to cryptocurrency-based intermediaries' regulation in Africa.

The proposed regulation may take the form of self-regulation; or characterisation and/or integration of cryptocurrency and cryptocurrency-based intermediaries into existing legislation; or designing an entirely new cryptocurrency-based intermediaries' regulatory legal framework aimed at addressing the potential risks identified in chapter two.

4.1 The rationale for regulation of cryptocurrency-based intermediaries

The rationale for cryptocurrency-based intermediaries' regulations can be ascertained by the various potential risks identified in chapter two²³⁰ ranging from the need for user protection; prevention, detection and monitoring of cyber attacks, security breaches, insider scams; unauthorised use of users private key; to prevention, detection and monitoring of money laundering activities.

Therefore, any regulation of cryptocurrency-based intermediaries must be aimed at addressing, mitigating, controlling and monitoring the aforementioned potential risks; to achieve adequate user protection; to detect, deter and mitigate money laundering; and to contribute towards enhanced transparent and well-functioning cryptocurrency-based intermediaries.²³¹

Hughes and Middlebrook place the aforementioned rationale in three categories, namely regulation for public law purposes (user protection,²³² anti-money laundering programs and conduct of business); regulation for private law purposes (governing the relationship between the cryptocurrency-based intermediaries and the user); and regulation aimed at the contribution toward transparency and well-functioning markets.²³³

²³⁰ See Paragraph 2.3 of chapter two on the potential identifiable risks.

²³¹ See Hughes and Middlebrook (2015) 501-502, 516-517 on the various purposes for cryptocurrency-based intermediaries' regulation; and Pansford MP 'A Comparative Analysis of Bitcoin and Other Decentralised Virtual Currencies: Legal Regulation in the People's Republic of China, Canada and the United States' (2015) 9 *Hong Kong Journal of Legal Studies* 29 (hereinafter referred to as Pansford (2015)').

²³² Pansford proposes regulation for user protection purposes, aimed at creating awareness of the potential risks that may materialise from the use of cryptocurrency and services provided by cryptocurrency-based intermediaries. See Pansford (2015) 9.

²³³ Hughes and Middlebrook (2015) 501-502, 516-517.

The regulation for public law purposes entails and includes regulatory rules aimed at the prevention, detection and deterrence of money laundering; or tax evasion^{234,235}; the regulation for private law purposes includes establishment of default rules to govern the relationship between parties and defining the nature of such relationship;²³⁶ and the regulation towards enhancement of transparency and well-functioning markets may include licensing and registration before operating or conducting the licensable or registrable activities.²³⁷

Therefore, the most suitable regulatory framework for cryptocurrency-based intermediation will be one that addresses all public and private issues, with emphasis on strong user-protection and a clarification of the relationship between users and cryptocurrency-based intermediaries; and transparency and accountability to enhance well-functioning cryptocurrency-based markets.

Having taken cognisance of the aforementioned rationale for cryptocurrency-based intermediaries' regulation, the section that follows below sets out the various regulatory approaches undertaken globally to address and regulate cryptocurrency-based intermediaries.

4.2 Global regulatory responses to cryptocurrency-based intermediaries

Various regulatory responses have been undertaken globally ranging from self-regulation to licensing to conduct cryptocurrency-related activities examples of which are indicated in this section.

4.2.1 Prohibition or frustration of conducting cryptocurrency-based business: China and India

China prohibits the conduct of cryptocurrency-related business activities; and on the other hand, although not prohibiting such activities, India prohibits regulated entities, which excludes cryptocurrency-based intermediaries, from conducting or engaging in cryptocurrency-related business activities. Both China and India's regulatory approaches are discussed below.

²³⁴ Tax evasion and the relevant legislation applicable will not be discussed in this research.

²³⁵ Hughes and Middlebrook (2015) 501, 516-517.

²³⁶ Hughes and Middlebrook (2015) 502.

²³⁷ Hughes and Middlebrook (2015) 502.

(a) **China**

On 09 September 2017, seven (7) government agencies of China jointly issued a Public Notice entitled '*Prevention of Risks of Token Offerings and Financing*' (the China Public Notice).²³⁸

The China Public Notice prohibits any platform providing trading and exchange services from exchanging legal tender for virtual currencies; or from engaging in proprietary trading between legal tender and virtual currencies; or from providing price determination or information intermediary services for virtual currencies.²³⁹

The trading and exchange of virtual currencies for fiat and vice versa forms the basis of the activities of a cryptocurrency-based exchange business; and by prohibiting such activities the Chinese Government essentially prohibits the cryptocurrency-based exchange business.

(b) **India**

In terms of Circular RBI/2017-18/154 entitled '*Prohibition on dealing in Virtual Currencies*' (the Indian Reserve Bank Circular) and dated 06 April 2018, the Indian Reserve Bank prohibits regulated entities from dealing in virtual currencies or providing services for facilitating any person or entity in dealing with or settling virtual currencies.²⁴⁰

The IRB Circular further describe the aforementioned services as including the maintenance of accounts, registering, trading, settling, clearing, giving loans against virtual currencies, accepting virtual currencies as collateral, opening accounts of exchanges dealing with virtual currencies, and transfer or receipt of money in accounts related to the sale or purchase of virtual currencies.²⁴¹

²³⁸ Public Notice of PBC, CAC, MIIT, SAIC, CBRC, CSRC and CIRC on *Prevention of Risks of Token Offerings and Financing* dated 09 September 2017

²³⁹ Paragraph III of the China Public Notice; Also see Wenhao S 'Cryptocurrency laws and regulations in China' 12 July 2018 available at <https://www.vantageasia.com/cryptocurrency-law-china/> (accessed 16 November 2018). Also see Pilarowski G and Lu Y 'China bans Initial Coin Offerings and Cryptocurrency Trading Platforms' 21 September 2017 3 available at <http://www.pillarlegalpc.com/en/news/wp-content/uploads/2017/09/PL-China-Regulation-Watch-Cryptocurrency-2017-09-22.pdf> (accessed 26 November 2018).

²⁴⁰ IRB Circular Paragraph 2.

²⁴¹ IRB Circular Paragraph 2.

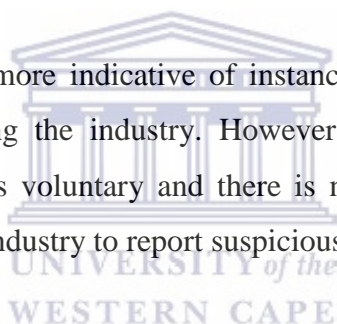
In addition, regulated entities already providing the aforementioned services are required to exit the relationship within three (3) months from the date of the IRB Circular.²⁴²

Despite the implications of the IRB circular, cryptocurrency-based intermediaries continue to operate within India, and due to the unregulated nature of cryptocurrency-based exchanges, some cryptocurrency-based exchanges operating within India are self-regulating, employing customer identification procedures and monitoring transactions of suspicious nature.²⁴³

These cryptocurrency-based exchanges have even formed an association known as the ‘*Digital Assets and Blockchain Foundation*’ working towards awareness and best industry practices.²⁴⁴

In comparison to China, which prohibits activities conducted by cryptocurrency-based exchanges and platforms, India simply cuts-off the means of trading of cryptocurrency-based exchanges without prohibiting the services provided by cryptocurrency-based exchanges.

The India example is furthermore indicative of instances where the industry itself designs self-regulatory rules governing the industry. However, such self-regulatory rules are not legally binding, compliance is voluntary and there is no obligation on the industry or the entities operating within that industry to report suspicious activity.



4.2.2 Application of existing legislation: Philippines, United States of America, Australia and Japan

The Philippines, United States of America, Australia and Japan apply existing legislation with necessary amendments to cryptocurrency-based exchanges. The Philippines and FinCen apply money transfer legislation; Australia applies legislation applicable to anti-money laundering; and Japan applies legislation applicable to payment systems. The aforementioned regulatory approaches are discussed below.

²⁴² IRB Circular Paragraph 3.

²⁴³ Sharma M ‘Cryptocurrency and the Regulators Dilemma’ 1 August 2017 13 available at https://idsa.in/system/files/comments/sf_cryptocurrencies_msharma.pdf (accessed 26 November 2018) (hereinafter referred to as ‘Sharma (1 August 2017)').

²⁴⁴ Sharma (1 August 2017).

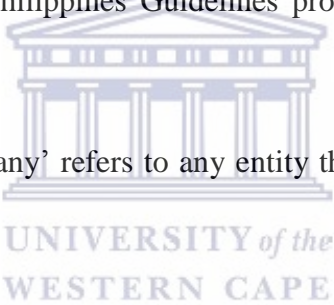
(a) **Philippines**

On 06 February 2017, the Philippines issued Circular No. 994 of 2017 entitled ‘*Guidelines of Virtual Currency Exchanges*’ (the Philippines Guidelines), which is incorporated as section 4512N of the Manual of Regulations for Non-Banking Financial Institutions.

The Philippines Guidelines are aimed at regulating virtual currencies when used for delivery of financial services, more particularly for payment and remittances, which have a material impact on anti-money laundering, terrorist financing, consumer protection and financial stability.²⁴⁵

The Philippines Guidelines apply to virtual currency exchanges offering services or engaging in activities that provide a facility for conversion or exchanges virtual currencies for fiat currencies and vice versa.²⁴⁶

Sub-section 4512N.2 of the Philippines Guidelines provides, amongst other, the following definitions:

- 
- (i) a ‘remittance or transfer company’ refers to any entity that provides money or value transfer services;
 - (ii) a ‘money or value transfer service’ as a financial service that involves the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, a transfer or a clearing network; and
 - (iii) a ‘virtual currency’ as any type of digital unit used as a medium of exchange or a form of digitally stored value.

In terms of sub-section 4512N.3 of the Philippines Guidelines, any virtual currency exchange may only operate as a remittance or transfer company once it has obtained a Certificate of Registration. Furthermore, and subsequent to being issued a certificate of registration, virtual

²⁴⁵ Sub-section 4512N of the Philippines Guidelines.

²⁴⁶ Sub-section 4512N.1 of the Philippines Guidelines.

currency exchanges are required to register with the Anti-Money Laundering Council Secretariat.²⁴⁷

Virtual currency exchanges are further required to put in place adequate risk management and security control mechanisms to address, manage and mitigate technology risks associated with virtual currencies.²⁴⁸

In addition, virtual currency exchanges providing wallet services for holding, storing and transferring virtual currencies are required to establish effective cyber security programs consisting of storage and transactional security requirements to ensure the integrity and security of virtual currency wallets and transactions.²⁴⁹

(b) United States of America

The Financial Crimes Enforcement Network (FinCen), a bureau of the United States Department of Treasury, issued the FinCen 2013 Guidance²⁵⁰ on 18 March 2013, which serves as an interpretive guidance to clarify the applicability of the regulations implementing the Bank Secrecy Act (the BSA) to persons creating, obtaining, distributing, exchanging, accepting or transmitting virtual currencies.²⁵¹

The FinCen's Regulations define a 'money transmitter' as a person that provides money transmission services or any person that engages in the transfer of funds; and a 'money service business' as the acceptance of currency, funds or other value that substitutes currency to another location or person by any means.²⁵²

The FinCen's 2013 Guidance indicates that a user obtaining virtual currency to purchase goods and services is not considered as a money transmitter;²⁵³ however the case is or may be different for administrators and exchangers.

²⁴⁷ Sub-section 4512N.3 of the Philippines Guidelines.

²⁴⁸ Sub-section 4512N.6 of the Philippines Guidelines.

²⁴⁹ Sub-section 4512N.6 of the Philippines Guidelines.

²⁵⁰ The FinCEN 2013 Guidance is entitled 'Application of FinCen's Regulations to Persons Administering, Exchanging or using virtual currencies' FIN-2013-G001 (hereinafter referred to as 'FinCen's 2013 Guidance').

²⁵¹ FinCen's 2013 Guidance 1.

²⁵² FinCen's Regulations section 1010.100(ff)(5)(i)(A) referred to in FinCen's 2013 Guidance 3.

²⁵³ FinCen's 2013 Guidance 2.

An exchanger is defined as a person engaged as a business in exchange of virtual currencies for real currencies, funds or other virtual currencies; and an administrator as a person engaged as a business in issuing (putting into circulation) a virtual currency and who has the authority to redeem such virtual currency.²⁵⁴

An administrator or exchanger that accepts and transmits; or buys or sells a convertible virtual currency, is a money transmitter under FinCen's Regulations. The FinCen's 2013 Guidance indicates that the definition of 'money transmitter' does not differentiate between real currency and convertible virtual currencies; and any person accepting or transmitting anything to value that substitutes currency is considered a money transmitter.²⁵⁵

(c) **Australia**

On 03 April 2018, the Australian Transaction Reports and Analysis Centre (AUSTRAC) commenced regulation of digital currency exchanges under the anti-money laundering and counter terrorism financing (AML/CTF) laws by amending the Anti-Money Laundering and Counter Terrorism Financing Act 2006 (the Act).²⁵⁶

The Act requires any person providing registrable digital currency exchange services, such as any service that involves the exchange of any fiat currency, whether Australian dollars or not to cryptocurrency and vice versa, and which must be conducted in the course of the carrying on digital currency exchange business, to register with AUSTRAC.²⁵⁷

Once registered, digital currency exchanges are subject to AML/CFT compliance and reporting obligations; to collect and store information on customers' identities; have a system to monitor suspicious activity, report any suspicious transactions; and establish an AML/CFT compliance program.²⁵⁸

The Act further introduces a policy principles period, which commenced on 03 April 2018 and expired on 02 October 2018. During that period digital currency exchanges were not

²⁵⁴ FinCen's 2013 Guidance 2.

²⁵⁵ FinCen's 2013 Guidance 3.

²⁵⁶ Whittaker S, Ng S and Lee H 'New AML/CFT Regulations for cryptocurrency exchanges' 23 April 2018 1 available at www.pwc.com.au (accessed 18 November 2018) (hereinafter referred to as 'Whittaker et al (23 April 2018)').

²⁵⁷ Whittaker et al (23 April 2018) 1.

²⁵⁸ Whittaker et al (23 April 2018) 1.

subject to enforcement action as long as they took reasonable steps to implement compliance obligation.

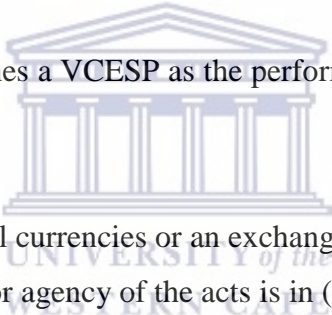
They were, however, required to establish an AML/CFT compliance program and implement necessary procedures to support AML/CFT compliance; and now that the period has expired, all digital currency exchanges must be registered and must be AML/CFT compliant.²⁵⁹

(d) **Japan**

Japan introduced its first regulation of virtual currency exchange service providers (VCESP) by amending its Payment System Act.

The Payment System Act amendment creates a new category referred to as the VCESP, which was added to three (3) existing categories, namely the issuer of payment securities; fund transfer service provider; and the clearing institution for interbank fund transfer.²⁶⁰

The Payment System Act defines a VCESP as the performance of any of the following acts in the course of trade:²⁶¹

- 
- (i) the purchase and sale of virtual currencies or an exchange with other virtual currencies;
 - (ii) the intermediation, brokerage or agency of the acts in (i); and
 - (iii) the management of users' money or virtual currency in connection with the acts in (i) and (ii).

Registration is required in order to provide a virtual currency exchange service. In order to ensure user protection, other provisions concerning the segregation of virtual currencies/cash belong to the service and the users, information management, explanations to prevent users from mistaking virtual currencies as legal tenders, information regarding fees and an external audit by a certified public accountant or an audit corporation on the status of segregated management.²⁶²

²⁵⁹ Whittaker et al (23 April 2018) 1.

²⁶⁰ Ishikawa M 'Designing Virtual Currency regulation in Japan: Lessons from the MtGox Case' (01 March 2017) 3 *Journal of Financial Regulation* 128 (hereinafter referred to as 'Ishikawa (2017)').

²⁶¹ Ishikawa (2017) 128.

²⁶² Ishikawa (2017) 128.

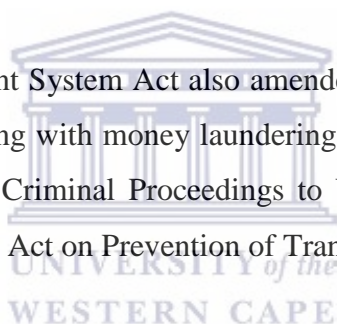
Regulators will supervise annual reports and reports on the amount of virtual currencies and cash management by VCESPs, as well as conduct on-site inspections, in terms of the Payment System Act.²⁶³

The new section 63-10 of the Payment System Act states that VCESP must provide explanations to customers to prevent them from misidentifying virtual currencies as Japanese or foreign currencies; and to provide information on fees, other terms and conditions of contracts pertaining to virtual currency exchange service, and other measures necessary of the protection of users.²⁶⁴

In the case of customer disputes, the amendment to the Payment System Act requires the VCESP to seek a resolution through the so-called financial alternative dispute resolution.²⁶⁵

The amended Payment Service Act requires that users' funds and virtual currencies are managed separately from the VCESP's own cash or virtual currencies.²⁶⁶

The amendment to the Payment System Act also amended the Act on Prevention of Transfer of Criminal Proceedings dealing with money laundering, extending the provisions of the Act on Prevention of Transfer of Criminal Proceedings to VCESP. This means that VCESP is subject to the provisions of the Act on Prevention of Transfer of Criminal Proceedings.²⁶⁷



4.2.3 Self-regulation: South Korea

On 30 January 2018, the South Korean Government issued an administrative decision aimed at digital currency exchanges.²⁶⁸ This administrative decision prohibits anonymous trading, and trading by foreigners and minors through digital currency exchanges.²⁶⁹

²⁶³ Ishikawa (2017) 129.

²⁶⁴ Ishikawa (2017) 129.

²⁶⁵ Ishikawa (2017) 130-131.

²⁶⁶ Ishikawa (2017) 131.

²⁶⁷ The Law Library of Congress 'Regulation of Cryptocurrency: Japan' available at <https://www.loc.gov/law/help/cryptocurrency/japan.php> (accessed 31 October 2018).

²⁶⁸ Park *et al* (12 July 2018)'.²⁶⁹

²⁶⁹ Park *et al* (12 July 2018)'.²⁶⁹

Under these regulations, digital currency exchanges are required to share users' transactions data with banks. South Korea users are required to use bank accounts in their legal name that matches the name on the digital currency accounts.²⁷⁰

On 17 April 2018, representatives²⁷¹ of fourteen (14) Korean digital currency exchanges released self-regulatory, but non-legal binding guidelines for digital currency exchanges in South Korea.²⁷² The self-regulation guidelines involve an inspection of all member cryptocurrency exchanges and require the satisfaction of the following five conditions:²⁷³

- (a) managing of clients' digital coins and their own separately;
- (b) coping with abnormal transactions quickly;
- (c) floating new digital currency with enhanced protection systems;
- (d) holding a minimum equity of KRWs billion (USD 1,8 million); and
- (e) publishing regular audit and finance reports.

Save for the regulations prohibiting anonymous trading and requiring users to use identifiable names when trading, cryptocurrency-based exchanges within South Korea are self-regulated. It is trite to point out that self-regulation does not place an obligation on the self-regulated industry to for instance, report suspicious activities to any regulator or law enforcement agency. Self-regulation rules and regulation are not binding and remains voluntary.

4.2.4 Introduction of new regulations: Abu Dhabi and the New York State Department of Financial Services' (NYSDFS) Regulations

The Abu Dhabi and NYSDFS Regulations are new enactments, which are specifically designed to regulate cryptocurrency-based exchanges and cryptocurrency wallet provision as is set out below.

²⁷⁰ Park *et al* (12 July 2018).

²⁷¹ The exchange representatives consist of members of the Korea Blockchain Association.

²⁷² Park *et al* (12 July 2018).

²⁷³ Park *et al* (12 July 2018).

(a) **Abu Dhabi**

On 25 June 2018, the Abu Dhabi Global Markets introduced Guidance Regulations of Cryptocurrency Asset Activities (the ADGM Guidance) under section 15(1) of the Financial Services and Markets Regulations.

The ADGM Guidance applies to any person carrying on regulated activity of operating a crypto asset business; and any authorised person in respect of its carrying on the regulated activity of crypto asset business.²⁷⁴

Paragraph 9 of the ADGM Guidance refers to cryptocurrency as ‘crypto asset’, which is a digital representation of value that can be digitally traded and functions as a medium of exchange; and/or a unit of account; and/or a store of value, but is not legal tender or government issued.

In terms of Paragraph 10, crypto assets are treated as commodities, and crypto asset exchanges dealing or managing crypto assets are required to obtain a licence or approval before operating as such. In addition, all authorised crypto asset businesses must comply with the Anti-Money Laundering and Sanctions Rules; and Rules of Market Conduct.²⁷⁵

Paragraph 15 of the ADGM Guidance provides the following definitions:

- (i) ‘crypto asset activity’ include the buying, selling or exercising any right in accepted crypto assets; managing accepted crypto assets belonging to another person; and operating a crypto asset exchange or as a crypto asset custodian;
- (ii) a ‘crypto asset exchange’ means the trading, exchange or conversion of a crypto asset for fiat currency or vice versa; or one accepted crypto asset into another accepted crypto asset; and
- (iii) a ‘crypto asset custodian’ means the safeguarding, holding, storing or maintaining custody of accepted crypto asset belonging to another person; or controlling or maintain accepted crypto asset for the aforementioned purpose.

²⁷⁴ Paragraph 2 of the ADGM Guidance.

²⁷⁵ Paragraph 17 of the ADGM Guidance.

Paragraph 19 identifies the risk areas and mitigation thereof as pointed out below:

- (iv) money laundering risk, which should be mitigated by reporting;
- (v) consumer risk, which should be mitigated by provision of all risks associated with crypto assets to the customer and disclosure of all services and products to the customer; and
- (vi) technology governance risk, which must be mitigated by putting in place systems and controls in relation to crypto asset wallets, private keys, origin and destination of crypto asset fund, security, risk management and systems recovery.

Furthermore, and in terms of Paragraph 19.4, crypto asset exchanges are required to put in place market surveillance, settlement processes, transaction recording, transparency and public disclosure, and exchange-like operational systems and controls.

Insofar as it relates to crypto asset wallet custodial services and in terms of Paragraph 19.5, the service provider will be required to conduct frequent reconciliations and reporting of crypto assets.

(b) **New York State Department of Financial Services' (NYSDFS) Regulations**

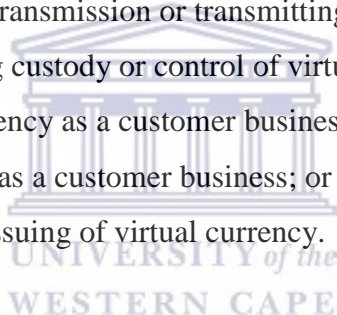
The NYSDFS introduced the BitLicence in June 2015 contained under the New York Codes, Rules and Regulations, Title 23 Department of Financial Services, Chapter 1 Regulations of the Superintendent of Financial Services, Part 200 Virtual Currencies; and aimed at regulating the virtual currency sector (NYSDFS Regulations).

The NYSDFS Regulations exempts merchants or consumers that use virtual currency solely for the purchase or sale of goods or services from the application of the NYSDFS Regulations.²⁷⁶

Section 200.2 of the NYSDFS Regulations define, amongst other terms, the following relevant terms:

²⁷⁶ Section 200.3(c)(2) of NYSDFS Regulations. Also see Gamble (2017) 352.

- (i) a ‘cyber security event’ entails “an act or an attempt, successful or unsuccessful, to gain unauthorised access to, or disrupt or misuse of a Licensee’s electronic system or information stored on such a system”;²⁷⁷
- (ii) an ‘exchange service’ as “the conversion of fiat currency into virtual currency or vice versa; or the exchange of one form of virtual currency into another form of virtual currency”;²⁷⁸
- (iii) a ‘transmission’ as “the transfer, by or through a third party, of virtual currency from a person to a person, including the transfer from an account or storage repository of a person to an account or storage repository of another person”;²⁷⁹
- (iv) a ‘virtual currency’ as “any type of digital unit that is used as a medium of exchange or a form of digitally stored value”;²⁸⁰
- (v) a ‘virtual currency business activity’ includes the following:²⁸¹
 - (aa) receiving virtual currency for transmission or transmitting virtual currency;
 - (bb) storing, holding or maintaining custody or control of virtual currency on behalf of others;
 - (cc) buying and selling virtual currency as a customer business;
 - (dd) performing exchange services as a customer business; or
 - (ee) controlling, administering or issuing of virtual currency.



Section 200.9(a) requires all Licensees to maintain a surety bond of trust account for the benefit of its customers’ in the form and amount as is acceptable with the superintendent for the protection of Licensee’s customers.

In addition, where the Licensee stores, holds, or maintains custody or control of virtual currency on behalf of another person, the Licensee is required to hold virtual currency of the same type and amount as that which is owed or obligated to another person.²⁸²

Section 200.15 deals with the anti-money laundering requirements that a Licensee must comply with, which requires a Licensee to conduct an initial risk assessment that will

²⁷⁷ Section 200.2(b) of the NYSDFS Regulations.
²⁷⁸ Section 200.2(d) of NYSDFS Regulations.
²⁷⁹ Section 200.2(o) of NYSDFS Regulations.
²⁸⁰ Section 200.2(p) of NYSDFS Regulations.
²⁸¹ Section 200.2(q) of NYSDFS Regulations.
²⁸² See section 200.9(b) of the NYSDFS Regulations.

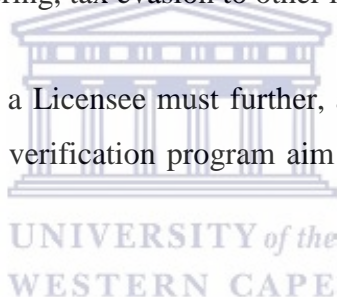
consider legal, compliance, financial and reputational risk associated with the activities conducted by the Licensee; and shall establish, maintain and enforce an anti-money laundering program based thereon.²⁸³

The licensee is thereafter required to conduct an annual assessment or more frequently as the risks change, and to modify its anti-money laundering program accordingly.²⁸⁴ The anti-money laundering program must further contain a written anti-money laundering policy.²⁸⁵

In terms of section 200.15(c)(1), the anti-money laundering program must, at the minim, amongst other things, provide for a system of internal controls, policies and procedures designed to ensure ongoing compliance.

The Licensee must, as part of the anti-money laundering program, maintain information of all virtual currency transactions involving payment, receipt, exchange, conversion, purchase, sale, transfer or transmission of virtual currency;²⁸⁶ and monitor virtual currency transactions that may signify money laundering, tax evasion to other illegal or criminal activity.²⁸⁷

In terms of section 200.15(h), a Licensee must further, as part of the anti-money laundering program, maintain a customer verification program aim at identifying and verifying account holders.



Section 200.16 requires a Licensee to establish and maintain a cyber security program to ensure the availability and functionality of the Licensee' electronic systems; and to protect those systems and any sensitive data from unauthorised access, use or tampering.

The Licensee must further implement a cyber security policy stipulating the Licensee's policies and procedures for the protection of its electronic system; and customer and counter-party data stored on those systems.²⁸⁸

Section 200.19 deals with consumer protection and requires a Licensee, as part of establishing a relationship with its customer, to disclose all material risks associated with the use of its

²⁸³ See section 200.15(b) of the NYSDFS Regulations.

²⁸⁴ See section 200.15(b) of the NYSDFS Regulations.

²⁸⁵ See section 200.15(d) of the NYSDFS Regulations.

²⁸⁶ See section 200.15(e)(1) of the NYSDFS Regulations.

²⁸⁷ See section 200.15(e)(3) of the NYSDFS Regulations.

²⁸⁸ See section 200.16(b) of the NYSDFS Regulations.

products, services and activities; and virtual currency generally, before entering into an initial transaction with a customer.²⁸⁹

Such information must, at the minimum, include that virtual currency is not legal tender; that legislative and regulatory changes may adversely affect the use, transfer, exchange or value of virtual currency; that transactions in virtual currency are irreversible and losses due to fraudulent and accidental transactions may be irrecoverable; that the volatility and the unpredictability of virtual currency relative to fiat currency may result in significant losses over a short period of time; and the nature of virtual currency may result in increased risk of fraud and losses.²⁹⁰

Section 200.19(g) requires the Licensee not to engage in fraudulent activity and to take reasonable steps to detect and prevent fraud, including the establishment and implementation of an anti-fraud policy.

The anti-fraud policy must, at the minimum include, the identification and assessment of fraud-related risk areas; procedures and controls to protect against identified risks; allocation of responsibility for monitoring risks; and procedures for the periodic evaluation and revision of anti-fraud procedures, controls and monitoring mechanisms.²⁹¹

Therefore, globally, cryptocurrency-based intermediaries' regulation can take various forms, namely a complete prohibition or frustration of conduct of cryptocurrency-related services; regulation under existing legislation with the necessary amendments; self-regulation; and enactment of legislation aimed specifically at cryptocurrency-based intermediation and service provision.

Furthermore, where authorities choose to regulate cryptocurrency-based intermediaries such regulation may encompass acquisition of a licence or require registration or authorisation; compliance with anti-money laundering and user protection requirements; and the establishment and implementation of cyber security and anti-fraud policies.

²⁸⁹ See section 200.19(a) of the NYSDFS Regulations.

²⁹⁰ See section 200.19(a) of the NYSDFS Regulations.

²⁹¹ See section 200.19(g)(1) to (4) of the NYSDFS Regulations.

However, the aforementioned regulatory responses are first, mostly rules-based requiring cryptocurrency-based intermediaries to comply with technical requirements, save for the ADGM Guideline and NYSDFS Regulations, which incorporate risk-based requirements.²⁹²

Secondly, the aforementioned regulatory responses are aimed at enhancing public law purposes with an indirect private law purpose, in other words, achievement of user protection through addressing public law issues such as anti-money laundering, cyber security, user protection and anti-fraud.

The aforementioned regulatory approaches therefore fail to define the scope of the relationship between the users and cryptocurrency-based intermediaries; dispute resolution in the event a dispute arises between the user and cryptocurrency-based intermediaries; or recovery and reimbursement of losses a user may suffer in the event that a cryptocurrency-based intermediary becomes insolvent or absconds with the users' cryptocurrency.

CONCLUSION

This chapter identified the rationale for cryptocurrency-based intermediaries' regulation and explored the various global regulatory responses to cryptocurrency-based intermediaries.

This chapter further discovered that cryptocurrency-based intermediaries' regulation may take various forms with varying impact on the risks identified in chapter two, namely:

- (a) the prohibition, which does not detect, address and mitigate any of the risks identified in chapter two;
- (b) the application of existing legislation, which is aimed at governing cryptocurrency-based intermediaries as if they are providing similar services as those entities and services regulated by the existing legislation without proper regard to the risks identified in chapter two, therefore this does not effectively detect, address and mitigate all the risks identified in chapter two;

²⁹² See the discussion on rules-based and risk-based approach to regulation in Paragraph 3.6 of chapter 3.

- (c) self-regulation, which is voluntary and lacks accountability on the part of the self-regulated industry, and, which does not effectively detect, address and mitigate all the risks identified in chapter two; and
- (d) the enactment of legislation specifically designed to regulate cryptocurrency-based intermediaries and the services they provide, which has the potential of effectively detecting, addressing and mitigating the risks identified in chapter two with necessary addition of certain rules and requirements.

The rules and requirements referred to in Paragraph (d) above should include:

- (i) identifying and governing the relationship between a user and the cryptocurrency-based intermediaries;
- (ii) dispute resolution mechanisms;
- (iii) clearly stipulated punitive measure for non-complying cryptocurrency-based intermediaries; and
- (iv) reimbursement or refund of users' funds in the event of insolvency of cryptocurrency-based intermediary or loss of users' cryptocurrency suffered due to failure to maintain adequate internal controls and security systems and criminal consequences upon abscondment of cryptocurrency-based intermediary administrators or employees.

The aforementioned, and more particularly Paragraph (d) above with the suggested modifications, will form the basis of recommendations aimed at designing a legal framework that should govern cryptocurrency-based intermediaries in Africa, which is discussed in chapter five.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

INTRODUCTION

As previously suggested in chapter one, cryptocurrency-based intermediation has found its way into Africa as exemplified by referenced examples of cryptocurrency-based intermediaries, such as Luno, Belfrics and BitPesa indicated in chapter two.

These cryptocurrency-based intermediaries conduct their services outside the scope of regulatory legislation applicable in countries such as South Africa, Kenya and Nigeria, some of which operate, in addition to their operation within the aforementioned countries, in other African countries.

In order to test whether existing legislation regulating conventional financial intermediaries providing comparable or similar services as cryptocurrency-based intermediaries may apply to cryptocurrency-based intermediaries, an examination was conducted in chapter three of this research. This concluded that such legislation was not applicable and unsuitable to regulate cryptocurrency-based intermediaries.

Furthermore, this research considered global regulatory responses to cryptocurrency-based intermediaries in order to ascertain the most suitable regulatory approach to cryptocurrency-based intermediaries in Africa.

The aforementioned were dispensed of the sub-objectives identified in chapter one in order to determine the most suitable design for cryptocurrency-based intermediation in Africa, which was the main objective of this research.

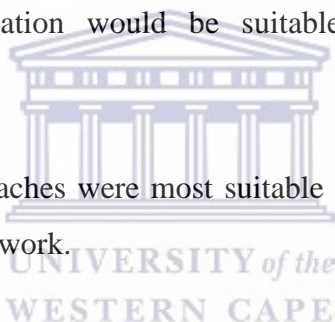
To that end, this chapter is aimed at providing a summary of discussions, examinations and explorations undertaken in chapters one to four of this research and to recommend the most suitable approach to cryptocurrency-based intermediaries' regulation in Africa.

5.1 Conclusion

The main objective of this research was to design a cryptocurrency-based intermediaries' regulatory legal framework for Africa aimed at user protection and regulating the conduct of cryptocurrency-based intermediaries in Africa. To this end, additional sub-objectives were designed to achieve the main objective.

These sub-objectives included the following:

- (a) providing an understanding of cryptocurrency-based intermediaries and identifying potential cryptocurrency-based intermediaries' risks and users' risks;
- (b) conducting an analysis into whether existing legislation applying to conventional financial intermediaries could be applied to cryptocurrency-based intermediaries;
- (c) if not, whether such legislation would be suitable to regulate cryptocurrency-based intermediaries; and
- (d) if so, which regulatory approaches were most suitable to design such cryptocurrency-based intermediary regulatory framework.



To achieve and dispense of the aforementioned objectives, chapters one to four provided the following:

5.1.1 Chapter One

Chapter one introduced the research into cryptocurrency intermediation in Africa; identified and specified the research objectives and questions relevant to this research; the significance of this research; the chapter outline; the methodology undertaken and provided the relevant definitions.

Chapter one further provided a basic overview of cryptocurrency by setting out the history and salient features of cryptocurrency; the manner in which cryptocurrency is acquired and referred to some examples of cryptocurrency, the purpose of which was to clarify the role of cryptocurrency in the cryptocurrency-based intermediaries' service provision.

5.1.2 Chapter Two

Chapter two dispensed of the first sub-objective by providing an overview of cryptocurrency-based intermediaries; the type of cryptocurrency-based intermediaries; the activities and/or services conducted by such intermediaries; and the potential risks they pose to the users through their conduct.

This chapter provided an overview on the following pertinent issues:

- (a) cryptocurrency-based intermediaries, by using cryptocurrency as a medium of exchange or method of payment, links buyers and sellers of cryptocurrency;
- (b) cryptocurrency-based intermediaries exchange cryptocurrency for other cryptocurrency, and if they are centralised, records such exchanges on their own systems, however if they are decentralised, the transaction is recorded on the ledger of the relevant cryptocurrency network;
- (c) cryptocurrency-based intermediaries exchange cryptocurrency for fiat currency much like the exchange or currency conversion that occurs when exchanging for instance a US dollar for South African Rand;
- (d) cryptocurrency-based intermediaries remit cryptocurrency from a sender to a recipient in the same country or in another country, and convert or exchange such cryptocurrency for fiat currency or cryptocurrency;
- (e) cryptocurrency-based intermediaries provide cryptocurrency wallet storage services, online and/or offline, to users; and
- (f) that the use of cryptocurrency-based intermediary services may pose some risks to users; and/or result in some potential risks for cryptocurrency-based intermediaries providing the aforementioned services. The potential risks identified in chapter two are as follows:
 - (i) Cryptocurrency-based intermediaries related risks, namely the risk of exchange breach, which included security breach, data loss, insider scam, data loss, legal action; and additionally, the risk of money laundering (cryptocurrency-based intermediaries related risks);



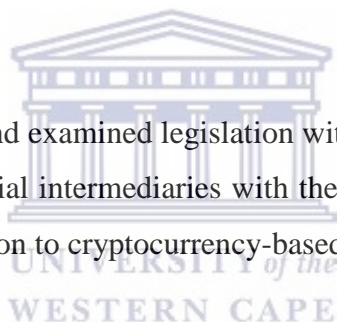
- (ii) Users' risks, namely, the risk of loss of cryptocurrency on account of cryptocurrency-based intermediaries' related risks.

In addition, the risk of unauthorised use of cryptocurrency private key where user entrusts and cedes control and access to the cryptocurrency-based intermediaries; the risk of closure of cryptocurrency-based intermediary and shut down of website; risk of inability to access and loss of cryptocurrency held with cryptocurrency-based intermediaries as a result of such closure and shut down; risk of insolvency cryptocurrency-based intermediary and the application of existing insolvency legislation that may not reimburse user in cryptocurrency; and the risk of and administrator of cryptocurrency-based intermediary absconding with user cryptocurrency.

5.1.3 Chapter Three

Chapter three dispensed of the second and the third sub-objectives by undertaking the following:

- (a) Chapter three first identified and examined legislation within South Africa, Nigeria and Kenya regulating conventional financial intermediaries with the aim of determining the applicability and suitability of such legislation to cryptocurrency-based intermediaries.



This chapter concluded that such legislation, save for those that apply to consumer protection and due to the determination made by the Kenyan Court in the BitPesa case, the Kenyan legislation applicable to money remittance service providers, did not apply to cryptocurrency-based intermediaries.

- (b) Secondly, this chapter concluded that such legislation was not suitable to regulate cryptocurrency-based intermediaries insofar as it related to addressing the potential risks identified in chapter two.

5.1.4 Chapter Four

This chapter addressed the fourth sub-objective, which was aimed at identifying the possible regulatory approaches to cryptocurrency-based intermediaries' regulation. Chapter four

identified the rationale for cryptocurrency-based intermediaries' regulation; and explored various global regulatory responses to cryptocurrency-based intermediaries.

To this end, this chapter identified and examined a complete prohibition to conduct cryptocurrency-based intermediaries' services (China) and frustrating the conduct of such services (India); application of existing legislation to regulate cryptocurrency-based intermediaries (Philippines, FinCen, Australia and Japan); self-regulation (South Korea); and enactment of new regulation to regulate cryptocurrency-based intermediaries (Abu Dhabi Global Markets Guidance and New York State Regulations).

This chapter concluded that the Abu Dhabi Global Markets Guidance and New York State Regulations provide the most suitable regulatory approach, in form and substance, to address the risks posed to users and to cryptocurrency-based intermediaries, and form the basis of regulating cryptocurrency-based intermediaries in Africa.

5.2 Recommendations

The recommended regulatory legal framework for cryptocurrency-based intermediaries (the recommended regulatory legal framework) should be based on and be informed by the issues canvassed in chapters one to four, more particularly the potential risks identified, the regulatory approaches recommended and the rationale for regulation clearly postulated in those chapters.

This research proposes the following regulatory approach to cryptocurrency-based intermediaries' regulation and regulatory legal framework for cryptocurrency-based intermediaries in Africa:

5.2.1 The recommended regulatory approach to cryptocurrency-based intermediaries: rules-based and/or risk-based approach

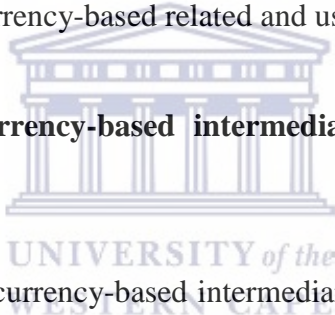
This research proposes an integrated approach to cryptocurrency-based intermediaries' regulation, namely regulation aimed at the identification, monitoring and mitigation of risks; and regulation consisting of a system of rules through which the regulator should ensure technical compliance by cryptocurrency-based intermediaries.

As previously postulated in chapter three a rules-based regulatory approach is essentially aimed at setting laws, rules and requirements for technical compliance such as licensing and penalties for non-compliance, which, on its own, will not be suitable for cryptocurrency-based intermediaries' regulation²⁹³ due to failure of such a regulatory approach to address the cryptocurrency-based intermediaries' related risks and users risks.

Therefore, in addition, to prescribing rules and requirements for technical compliance, the recommended framework for cryptocurrency-based intermediaries must also impose an obligation on cryptocurrency-based intermediaries to establish, and continuously develop risk identification and assessment tools and mitigate such risks. In addition, the failure to establish and implement such tools must be subject to some consequence.

The aforementioned approach is recommended to enable regulators to exercise some control over cryptocurrency-based intermediaries and the conduct of their activities whilst imposing an obligation on cryptocurrency-based intermediaries to identify, continuously assess, monitor and mitigate cryptocurrency-based related and users' risks.

5.2.2 The rationale for cryptocurrency-based intermediaries' regulation: public law and private law purpose



This research proposes cryptocurrency-based intermediaries' regulatory legal framework that is based on a two-fold rationale as postulated in chapter four,²⁹⁴ which is aimed at achieving a public law purpose and a private law purpose.

In addition, the public law purpose should be achieved through the enactment of a regulatory legal framework that follows both a risk-based and rules-based approach. Insofar as it pertains to achieve the private law purpose, it recommended that mandatory contractual terms be incorporated into the contractual arrangements entered into between the users and cryptocurrency-based intermediaries.²⁹⁵

²⁹³ See Paragraph 3.6 of chapter three for a discussion on the suitability of rules-based regulation to cryptocurrency-based intermediaries.

²⁹⁴ See Paragraph 4.1 of chapter 4 insofar as it relates to a discussion pertaining to the rationale for cryptocurrency-based intermediaries' regulation.

²⁹⁵ Paragraph 2.2 of chapter two indicates that, before using the services of Luno, Belfric and BitPesa, the user is required to accept agree to standardised Terms and Conditions of the respective cryptocurrency-based intermediaries.

Furthermore, this research proposes the enactment of a new regulatory legal framework similar to the Abu Dhabi Global Markets Guidance Regulations of Cryptocurrency Asset Activities (ADGM Guidance) and the New York State Department of Financial Services' (NYSDFS) Regulations²⁹⁶ insofar as it relates to public law aspects.

5.2.3 Salient provisions of the recommended regulatory legal framework for cryptocurrency-based intermediaries

This sub-paragraph postulates the salient provisions of the recommended regulatory legal framework for cryptocurrency-based intermediaries in two ways, namely by first defining the scope of application of the recommended regulatory legal framework to cryptocurrency-based intermediaries; and secondly, by specifying public law aspects and the private law aspects.

(a) Scope of application of the recommended regulatory legal framework

As cryptocurrency-based intermediaries take various forms²⁹⁷ therefore, the recommended regulatory legal framework must define the scope of application to cryptocurrency-based intermediaries, that is, whether the recommended regulatory legal framework will apply to or regulate, generally, all types of cryptocurrency-based intermediaries²⁹⁸ and their sub-categories, if any, or be specifically aimed at types of cryptocurrency-based intermediaries or simply the activities conducted by such cryptocurrency-based intermediaries.

For instance, the ADGM Guidance regulates any person conducting the regulated activity of operating a cryptocurrency asset business, which means that the ADGM Guidance regulation is two-fold, namely it regulates the cryptocurrency-based intermediary and the activity conducted by such cryptocurrency-based intermediary.²⁹⁹

In the instance of ADGM Guidance, the activity of carrying on cryptocurrency asset activity includes the buying, selling or exercising any right in accepted crypto assets; managing accepted crypto assets belonging to another person; and operating a crypto asset exchange or as a crypto asset custodian.³⁰⁰

²⁹⁶ See Paragraph 4.2.4 of chapter 4.

²⁹⁷ See Paragraph 2.1 of chapter two on the discussion of types of cryptocurrency-based intermediaries.

²⁹⁸ See Paragraph 2.1.1 of chapter two discussing the types of cryptocurrency-based intermediaries.

²⁹⁹ See Paragraph 4.2.4(a) of chapter four in this regard.

³⁰⁰ See Paragraph 4.2.4(a) of chapter four in this regard.

Another example is the NYSDFS Regulations³⁰¹ regulating virtual currency business activity, which includes receiving virtual currency for transmission or transmitting virtual currency; storing, holding or maintaining custody or control of virtual currency on behalf of others; buying and selling virtual currency as a customer business; performing exchange services as a customer business; or controlling, administering or issuing of virtual currency.³⁰²

Therefore, and insofar as it relates to the application of public law aspects, it is proposed that the recommended regulatory legal framework applies to both the cryptocurrency-based intermediaries and the activities they conduct, which includes all activities listed or specified in the ADGN Guidance and the NYSDFS Regulations.

However, a distinction should be drawn between the categories of cryptocurrency-based exchanges, namely centralised and decentralised cryptocurrency-based exchanges;³⁰³ and custodial and non-custodial wallet storage,³⁰⁴ as is set out below.

(i) Scope of application to centralised and decentralised cryptocurrency-based exchanges

As postulated in chapter two, cryptocurrency-based exchanges are categorised either as centralised or decentralised.³⁰⁵ These two types of cryptocurrency-based exchanges provide intermediation to users either simply linking purchasers and sellers of cryptocurrency;³⁰⁶ or acting as a merchant selling cryptocurrency to its users;³⁰⁷ or providing a platform through which purchasers and seller buy and sell cryptocurrency³⁰⁸.

³⁰¹ This does not mean that other global regulatory legal frameworks governing cryptocurrency-based intermediaries do not sufficiently defined the scope of application of such legal frameworks to cryptocurrency-based intermediaries, but that the scope of application of the NYSDFS Relations and the ADGM Guidelines provide more clarity in that regard.

³⁰² See Paragraph 4.2.4(b) of chapter four in this regard.

³⁰³ See Paragraph 2.1.1(c) of chapter two regarding the discussion of the categories of cryptocurrency-based exchanges.

³⁰⁴ See Paragraph 2.1.2(a) of chapter two regarding the discussion of custodial and non-custodial wallets.

³⁰⁵ See Paragraph 2.1.2(c) of chapter two regarding the discussion on the categories of cryptocurrency-based exchanges.

³⁰⁶ Luno is an example of a cryptocurrency-based intermediary providing these services. See Paragraph 2.2.1 of chapter two in this regard.

³⁰⁷ BitPesa is an example of a cryptocurrency-based intermediary providing these services. See Paragraph 2.2.3 of chapter two in this regard.

³⁰⁸ Belfrics is an example of a cryptocurrency-based intermediary providing these services. See Paragraph 2.2.2 of chapter two in this regard.

There are inherent differences between the aforementioned types of cryptocurrency-based exchanges relating to control of funds; anonymity and authentication of transactions conducted on the cryptocurrency-based exchanges.³⁰⁹

The transactions on a decentralised cryptocurrency-based exchange is conducted anonymously, and verified and authenticated on the relevant cryptocurrency network. In contrast, on a centralised cryptocurrency-based exchange, transactions may or can be conducted anonymously.³¹⁰ The risk of money laundering is intensified where cryptocurrency-related transactions are conducted anonymously.³¹¹

Therefore, the following is proposed insofar as it relates to the application of the recommended regulatory legal framework to centralised and decentralised cryptocurrency-based exchanges:

- (aa) the recommended regulatory legal framework should apply to all types of cryptocurrency-based exchanges; and
- (bb) anonymous trading should be prohibited; and
- (cc) the recommended regulated legal framework requires record-keeping and reporting of all transactions conducted on a cryptocurrency-based exchange, however such requirement should not be imposed on a decentralised cryptocurrency-based exchange because transactions are recorded on the blockchain (recorded on the decentralised network of the cryptocurrency traded).

(ii) Scope of application to cryptocurrency wallet service providers

As postulated in chapter two, a cryptocurrency wallet service provider does not provide non-custodial storage services. This type of wallet storage does not require the services of a wallet service provider. In this instance a cryptocurrency owner provides his/her/its own storage.³¹²

³⁰⁹ See Paragraph 2.1.1(c) of chapter two regarding the discussion of the differences between centralised and decentralised cryptocurrency-based exchanges.

³¹⁰ See paragraph 2.1.1(c) of chapter two regarding the distinction on the categories of cryptocurrency-based exchanges.

³¹¹ See Paragraph 2.3.1(b) of chapter two on the discussion of money laundering risk.

³¹² See Paragraph 2.1.2(b) of chapter two discussion non-custodial storage of cryptocurrency.

A cryptocurrency service provider provide custodial wallet storage services, which can be storage services either online (hot) or offline (cold). The risk of exchange breach in the form of a security breach is higher in online storage.³¹³

The risk of exchange breach in the form of a security breach is less likely with cold storage, which is offline, providing storage facilities on a physical site, theft of cryptocurrency can only be achieved by physically stealing cryptocurrency private keys held in a cold storage.

In both instances of storage, the cryptocurrency wallet provider is entrusted with cryptocurrency (private keys) belonging to users, and should be required to ensure safe keeping of such cryptocurrency and secure internal systems. The recommended cyber security requirements are discussed elsewhere in this chapter.

In light of the aforementioned reasons, the recommended regulatory legal framework should thus apply only to custodial storage provision by cryptocurrency wallet providers.

(iii) **Scope of application to cryptocurrency-based remittance service providers**

Cryptocurrency-based remittance service providers use blockchain technology to remit cryptocurrency. Cryptocurrency-based remittance service providers further accept cryptocurrency from a sender and transmit such cryptocurrency to a recipient and/or convert such cryptocurrency transmitted by a sender into fiat currency for the recipient.

It is recommended that the scope of application of the recommended regulatory legal framework should include cryptocurrency-based remittance service providers.

(b) **Public law aspects**

The public law provisions should address market conduct, which should include licensing requirements; impose obligation to establish and implement anti-money laundering programs, user protection programs, cyber security programs and anti-theft programs; continuous risk assessment; and address miscellaneous issues.

³¹³ See Paragraph 2.1.2(a) of chapter two discussion custodial storage of cryptocurrency.

This sub-paragraph sets out and provides a clarification of the public law aspects specified in Paragraph 5.2(a) above that should be contained in the recommended regulatory legal framework.

(i) **Market conduct**

It is proposed that the recommended regulatory legal framework introduces a licensing or registration regime to allow a relevant authority to have the power to have control over cryptocurrency-based intermediaries and the services they provide.

Therefore, the conducting of cryptocurrency-based intermediaries' activities must be subject to a licence, meaning that any person conducting such activities must obtain a licence from a relevant authority (licensing authority).

The licensing authority must not impose strict requirements to obtain such a licence or require the payment of exorbitant fees. The licensing authority must be empowered to either grant, with or without conditions, or refuse to grant a licence; and revoke or withdraw such a licence; or modify the conditions of such licence.

(ii) **Addressing the cryptocurrency-based intermediaries' related risks**

Chapter two identifies two types of risks to which cryptocurrency-based intermediaries are susceptible, namely exchange breach risk consisting of security breach, data loss, insider scam, and legal action; and money laundering risk.³¹⁴

It is recommended that, in order to detect, monitor and mitigate this risk, cryptocurrency-based intermediaries must be required to undertake the following actions:³¹⁵

- (aa) conduct an initial risk assessment that will consider legal, compliance, financial and reputational risk associated with the activities conducted by the cryptocurrency-based intermediaries;
- (bb) establish, maintain and enforce programs based on the aforementioned risk assessment;

³¹⁴ See Paragraph 2.3 of chapter two on the identified cryptocurrency-based intermediaries' related risk.

³¹⁵ The recommendation made to address cryptocurrency-based intermediaries' related risk is based on the NYSDFS Regulations and the ADGM Guidance discussed under Paragraph 4.2.4 of chapter four.

- (cc) conduct an annual assessment of the aforementioned risks or more frequently as the risks changes, and modify its risk programs; and
- (dd) designate a department or individual responsible for compliance, coordination and monitoring of the day-to-day compliance with the various risk programs.

In addition, and insofar as it relates specifically to money laundering risk, maintain information of all cryptocurrency transactions involving payment, receipt, exchange, conversion, purchase, sale, transfer or transmission of cryptocurrency;³¹⁶ a user verification program aimed at verifying and identifying account holders;³¹⁷ and the detection and reporting of suspicious transactions.

In relation to keeping record of transactions, care should be taken regarding the fact that decentralised cryptocurrency-based intermediaries might not be able to comply with the requirement due to the decentralised nature of authentication and verification of transactions conducted on such cryptocurrency-based exchanges.

(iii) In order to address users' risk

In both the ADGM Guidance and NYSDFS Regulations, licensed cryptocurrency-based businesses are required to warn users against material risks attributable to the use of cryptocurrency and the use of such services.³¹⁸

The NYSDFS Regulations indicate that such information may include:³¹⁹

- (aa) that cryptocurrency is not legal tender;
- (bb) that legislative and regulatory changes may adversely affect the use, transfer, exchange or value of cryptocurrency;
- (cc) that transactions in virtual currency are irreversible and losses due to fraudulent and accidental transactions may be irrecoverable;

³¹⁶ Similar to that which is required under section 200.15(a) of the NYSDFS Regulations discussed in Paragraph 4.2.4(b) of chapter four.

³¹⁷ Similar to that which is required under section 200.15(h) of the NYSDFS Regulations discussed in Paragraph 4.2.4(b) of chapter four.

³¹⁸ See Paragraph 4.2.4 (a) and (b) of chapter four in this regard.

³¹⁹ See Paragraph 4.2.4(b) of chapter four in that regard, and in addition, section 200.19(a) of the NYSDFS Regulations.

- (dd) that the volatility and the unpredictability of cryptocurrency relative to fiat currency may result in significant losses over a short period of time; and
- (ee) that the nature of cryptocurrency may resulting in increased risk of fraud and losses.

It is suggested that the recommended regulatory legal framework requires the disclosure of similar (in scope and form) information to the user at the time the user initiates the use of the cryptocurrency-based intermediary's business.³²⁰

In addition, the recommended regulatory legal framework should impose a duty upon the cryptocurrency-based intermediaries to keep and provide records of cryptocurrency transferred and received into the users account;³²¹ or provide access to a user to be able to check the amount of cryptocurrency standing to the credit of the user at intervals prescribed or at any time a user wishes to ascertain such information.³²²

Furthermore, where the cryptocurrency-based intermediary provides custodial wallet storage services to users and, thus store and hold cryptocurrency on behalf of users, such a cryptocurrency-based intermediary should hold cryptocurrency of the same type and amount as that which is held on behalf of users.³²³

This requirement is aimed at curbing the risk that users may not be reimbursed in the event of insolvency of the cryptocurrency based intermediary; and/or when an administrator of the cryptocurrency-based intermediary absconds with users' cryptocurrency.³²⁴

In order to further ensure user protection, the cryptocurrency-based intermediary should segregate cryptocurrency and funds belonging to its users from its own cryptocurrency and funds.³²⁵

³²⁰ When such a disclosure should be made is a requirement in terms of section 200.19(a) of the NYSDFS Regulations as referenced in Paragraph 4.2.4(b) of the NYSDFS Regulations.

³²¹ Kindly please see Paragraph 5.2.1(a)(i)(cc) of this chapter regarding the proposal not to subject a decentralised cryptocurrency-based exchange from keeping records of transaction for reasons postulated in the said paragraph.

³²² The ADGM Guidelines imposes a similar requirement in 19.5. See Paragraph 4.2.4(a) of chapter four in that regard.

³²³ Section 200(9)(b) of the NYSDFS Regulations imposes a similar requirement. See Paragraph 4.2.4(b) of chapter four in that regard.

³²⁴ See Paragraph 2.3.1(b)(iv) of chapter two insofar as it relates to the risk.

³²⁵ See the discussion under Paragraph 4.2.2(d) of chapter four on Japan's amended Payment Systems Act.

(vi) **Provisions dealing with insolvency of cryptocurrency-based intermediaries**

If one considers the bankruptcy of cryptocurrency-based intermediaries such as MtGox and loss of users' cryptocurrency in various ways discussed in chapter two, it becomes pertinent to ensure that the bankruptcy of cryptocurrency-based intermediaries is addressed in the recommended regulatory legal framework.

This should include the manner in which users will be reimbursed in the event of insolvency of a cryptocurrency-based intermediary.

Clarity should be provided how users' cryptocurrency held in custody should be dealt with in the event a cryptocurrency-based intermediary is declared insolvent. It should be clear from the outset the return of cryptocurrency should be the main consideration.

Existing legislation governing the liquidation and distribution of assets of a liquidated company should not be applied to insolvent cryptocurrency-based intermediaries. The manner in which the liquidation of cryptocurrency-based intermediaries should be dealt with should be provided for in the recommended regulatory legal framework.



(vii) **Miscellaneous issues**

Miscellaneous issues are matters related to the regulated subject-matter. It should thus include punitive measures and/or penalties for non-compliance, breach of conditions imposed and contravention of the regulatory framework as well as transitional aspects.

(aa) **Transitional period for implementation**

Due to the relative new nature of the recommended regulatory legal framework it is trite to introduce and define a transitional period within which all existing cryptocurrency-based intermediaries should be allowed to put in place mechanisms and programs introduced by the recommended regulatory legal framework.³²⁶

³²⁶ This is introduced by the Australian Anti-Money Laundering and Counter Terrorism Financing Act 2006. Kindly please see Paragraph 4.2.2(c) of chapter four.

It is thus recommended that cryptocurrency-based intermediaries operating within Africa, or specifically within African countries, will be granted a transitional period to develop the various programs set out in the recommended regulatory legal framework. The awarding of a final licence will be conditional upon the development and implementation of such programs.

(bb) **Punitive measures**

Non-compliance with regulatory obligations should result in some form of punitive consequences, for instance the failure to obtain a licence to conduct cryptocurrency-related services should carry a discontinuance of business and a fine; or the failure to establish and implement programs contemplated in the recommended regulatory legal framework should carry a fine or even conditional continuance of licensed services.

Therefore, it is proposed that the recommended regulatory legal framework explicitly set out punitive measures and consequent penalties to ensure that non-compliance with the provisions of the recommended regulatory legal framework is punishable in some or other form.

(c) **Private law aspects**

As previously indicated in this chapter, this research recommends the incorporation of mandatory contractual terms into the contractual arrangements between the users and cryptocurrency-based intermediaries; and to impose an obligation on the cryptocurrency-based intermediary to allow the user to negotiate any other terms to contractual agreement.

(i) **Mandatory contractual terms**

This paragraph sets out the recommended mandatory contractual terms, which are as follows:

(aa) **Define the types of service provided by the cryptocurrency-based intermediary**

The cryptocurrency-based intermediary must ensure that the contractual arrangement clearly defines essential terms; and the services provided.

(bb) **Authorisation to transfer cryptocurrency**

It should be a mandatory term of contract that cryptocurrency wallet providers, inclusive of cryptocurrency-based exchanges providing such services, only effect transactions involving a user's key with the written authorisation of the user.

The cryptocurrency-based intermediary should further commit that affecting the transfer of the user's cryptocurrency without authorisation will be inconsistent with the terms of the contract; amount to breach of contract; and that the user will be entitled to the immediate return of the cryptocurrency.

(cc) **Responsibility to ensure the safe-keeping of the user's cryptocurrency wallet**

The mandatory contractual terms must impose an obligation on the wallet service provider to accept responsibility for the safe-keeping of the user's cryptocurrency wallet, inclusive of affirming the responsibility regarding the secure nature of its internal security systems.

In addition, if a security breach is due to weak internal security system, the contract terms must impose a responsibility on the cryptocurrency-based intermediary to reimburse the user for any losses in cryptocurrency suffered by the user, even if such reimbursement is in a monetary value instead of cryptocurrency.

(dd) Assurance that the cryptocurrency-based intermediary will warn the user in advance of possibility inaccessibility of its website and shut down of website

(ee) Provision of information related to any hacking and loss of cryptocurrency at the time of occurrence of such hacking or as soon as reasonably practicable after such hacking

(ff) **Right of withdrawal**

The user must be allowed to withdraw any cryptocurrency held in a cryptocurrency storage wallet at any time that the user requires, including complete withdrawal and transfer of such cryptocurrency to another cryptocurrency-based intermediary or form of storage, for instance from online storage to offline storage of the user's choosing.

(gg) Dispute resolution

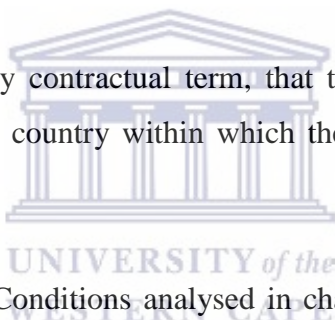
Belfrics terms and conditions impose an obligation on the parties to resolve disputes arising for the terms and conditions by way of consultation, and if such consultation fails, by way of binding arbitration.³²⁷ The same approach to dispute resolution is proposed as a mandatory contractual term.

(hh) Governing law

The resolution of disputes, in respect of Luno are resolved through the Law of Singapore and the parities submit to the exclusive jurisdiction of the courts of Singapore,³²⁸ and in respect of BitPesa, the governing law is specified as the law of Luxembourg.³²⁹

In both instances, disputes are governed by country laws outside of Africa and users are required to ascribe exclusive to the Courts of such countries in order to resolve a dispute.

It is proposed, as a mandatory contractual term, that the governing law applicable in this instance should be law of the country within which the cryptocurrency-based intermediary operates.



The Terms of Use and Terms and Conditions analysed in chapter two³³⁰ of cryptocurrency-based intermediaries operating within South Africa, Nigeria and Kenya specify some of the mandatory contractual term recommended in this paragraph however, in order to address the user related risks, the aforementioned mandatory contractual terms are proposed.

(ii) Negotiation of terms not recommended as mandatory contractual terms

Any other terms of contract to utilise cryptocurrency-based intermediaries' services must be subject to negotiation between the cryptocurrency-based intermediary and the user. In other words, the user must be afforded an option to negotiate any other contractual term that is not a mandatory contractual term.

³²⁷ See Paragraph 2.2.2(e) of chapter two in this regard.

³²⁸ See Paragraph 2.2.1 of chapter two in this regard.

³²⁹ See Paragraph 2.2.3 of chapter two in this regard.

³³⁰ See Paragraph 2.2 of chapter two on the discussion of the contractual terms of Luno, Belfrics and BitPesa.

5.3 Administrator of the recommended regulatory legal framework

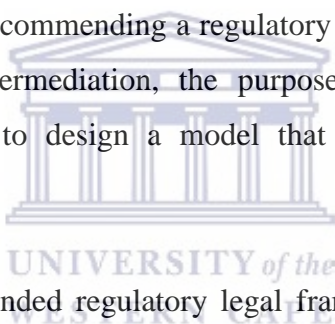
As can be attested by the discussion in chapter three, cryptocurrency-based intermediaries provide financial services similar to those provided by conventional financial intermediaries therefore, regulators tasked with the regulation of conventional financial intermediaries should be tasked to regulate cryptocurrency-based intermediaries.

5.4 Additional issues that may not fall within the scope of regulation

The recommended regulatory framework must additionally impose a duty on regulators to propose and influence change in criminalizing cryptocurrency theft where the prevailing definition of theft does not include, as an offence, the theft of cryptocurrency.

5.5 Application of the recommended regulatory legal framework within Africa

It is trite to point out that in recommending a regulatory legal framework for cryptocurrency-based intermediaries and intermediation, the purpose was to allow for its application uniformly within Africa, or to design a model that can point out pertinent issues for regulation.



The aforementioned recommended regulatory legal framework is based on the operational nature of cryptocurrency-based intermediaries. For instance, as postulated in chapter two, Luno, Belfrics and BitPesa operate across Africa by conducting services within various African countries.

If each of those African countries within which these cryptocurrency-based intermediaries operate have different legislation governing cryptocurrency-based intermediaries, users may not obtain the same type of protection, and a cryptocurrency-based intermediary may choose to operate in a country with little or no regulation.

This will result in inadequate and ineffective user protection and will additionally allow cryptocurrency-based intermediaries to shop around for a country within Africa with the weakest regulatory framework increasing the risk of money laundering, theft of cryptocurrency, increased cyber security breaches and poor user protection.

The aim of this research ultimately was to design a regulatory legal framework aimed at addressing, detecting, minimizing, mitigating and monitoring the aforementioned risks within the African context; and to maximize the safe, secure and trusted use of the services provided by cryptocurrency-based intermediaries in Africa.

Such safe, secure and trusted use will only be intensified if users, whichever cryptocurrency-based intermediary they utilise, for instance in South Africa, know that the regulatory framework is the same or closely related, providing similar protection anywhere else in Africa.

This essentially means that the aforementioned recommended regulatory approach may be adopted by regional economic communities in Africa and applied uniformly within that regional economic community; or by a continental body such as the African Union.

FINAL THOUGHTS

The aim of this research was to make a case for cryptocurrency-based intermediaries' regulation in Africa, and thereafter to design a regulatory framework for cryptocurrency-based intermediaries.

The aforementioned was the result of discussion undertaken throughout this research; and for identification, detection, monitoring and mitigation of cryptocurrency-based intermediaries' related risks and users' risks.

The recommended regulatory framework should be implemented in such a manner that it does not stifle innovation and block the potential benefits that cryptocurrency-based intermediation may provide to African countries and their citizens.

It should essentially be aimed at creating and building of trust in the services provided by cryptocurrency-based intermediaries, whilst addressing the potential risk such service provision and the use of such services may pose to users.

Finally, the recommended regulatory legal framework for cryptocurrency-based intermediaries advanced herein will be suitable and adequate to identify, detect, monitor and mitigate cryptocurrency-based intermediaries' related risks and users' risks.

BIBLIOGRAPHY

BOOKS

Ansari SA *Financial Intermediaries and Industrial Development* (1998) New Delhi: Ashish Aph Publishing.

Jones MW & Schoeman HC *An Introduction to South African Banking and Credit Law* (2006) Durban:LexisNexus Butterworths.

Motsi-Omodijiade ID 'Financial Intermediation in Cryptocurrency Markets – Regulation, Gaps and Bridges in Chuen DLK et al (eds) *Handbook of Blockchain, Digital Finance, and Inclusion: Cryptocurrency, FinTech, InsureTec and Regulation* vol 1 (2018) Academic Press: London.

Mwenda KK *Legal Aspects of Financial Services Regulation and the Concept of a Unified Regulator* (2006) The International Bank for Reconstruction and Development / The World Bank: Washington.



JOURNAL ARTICLES

Awrey D and Van Zwieten K 'The Shadow Payment System' 4 (2017-2018) 43 *Journal of Corporation Law* 775-816.

Chung JJ 'Money as Simulacrum: The Legal Nature and Reality of Money' 5 *Hastings Business Law Journal* (2009) 109-168.

Cotton J 'Sending a Bit more coin home? An analysis of retail user protection in Bitcoin Remittance Markets' (2018) 49 *Victoria University Wellington Law Review* 101-132.

Engle E 'Is Bitcoin Rat Poison: Cryptocurrency, Crime and Counterfeiting (CCC)' (2016) 16 *Journal of High Technology Law* 340-393.

Gerard VC 'Virtual Currencies: Growing Regulatory Framework and Challenges in Emerging Fintech Ecosystem' (2107) 21 *North Carolina Banking Institute* 131-176.

Griffith ME 'Virtual Currency Businesses: An Analysis of the Evolving Regulatory Landscape' (2015) 16 *Tex. Tech. Admin. L.J.* 303-331.

Guadamaz A 'New Kids on the Blockchain' (2018) 2018 *Jotwell: The Journal of Things we like (Lots)* 1-2.

Hughes SJ and Middlebrook ST 'Advancing a Framework for Regulating Cryptocurrency Payment Intermediaries' (2015) *Yale Journal on Regulation* 497- 559.

Ishikawa M 'Designing Virtual Currency regulation in Japan: Lessons from the MtGox Case' (01 March 2017) 3 *Journal of Financial Regulation* 125-131.

Lee J, Long A, McRae M, et al 'Bitcoin Basics: A Primer on Virtual Currencies' (2015) *Business Law International* 21-48.

Lin TCW 'Infinite Financial Intermediation' (2015) *Wake Forest Law Review* 643-669.

Mann TT 'Money Laundering' 2 (2007) 44 *American Criminal Law Review* 769-792.

Marian O 'A Conceptual Framework for the Regulation of Cryptocurrencies' (2017) 1 *University of Chicago Law Review Online* 82 53-68.

McCoy PA 'Degrees of Intermediation' (2015) 50 *Wake Forest Law Review* 551-578.

Nakamoto S 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2017) 1 *Blockchain Technology and Digital Currency National Institute* A-1-[i].

Orozco M 'Market and Financial Democracy: The Case for Remittance Transfers' (2005) 1 *Journal for Payment Systems Law* 166-215.

Pansford MP 'A Comparative Analysis of Bitcoin and Other Decentralised Virtual Currencies: Legal Regulation in the People's Republic of China, Canada and the United States' (2015) 9 *Hong Kong Journal of Legal Studies* 29-50.

Trautman L 'Virtual Currencies: Bitcoin & What Now after Liberty Reserve, Silk Road, and Mt. Gox' 4 *Richmond Journal of Law and Technology* XX (2014) 1-108.

Tu K 'Perfecting Bitcoin' (2018) 52 *Georgia Law Review* 505-580.

Tu KV and Meredith MW 'Rethinking Virtual Currency Regulation in the Bitcoin Age' *Washington Law Review* 90 (2015) 271-347.

Zhou S 'Bitcoin Laundromats for Dirty Money: The Bank Secrecy Act's Inadequacies in Regulating and Enforcing Money Laundering Laws over Virtual Currencies' (2014) 3 *Journal of Law and Cyber Warfare* 103-142.

CASE LAW

Lipisha Consortium Limited and BitPesa Limited v Safaricom Limited [2015] eKLR.

Registrar of the Bank and Net Income Solutions and three (3) others (3056/13) [2013] ZAWCHC 92.



PAPERS

Central Bank of Kenya 'Public Notice: Caution to the Public on Virtual Currencies such as Bitcoin' (2015).

Central Bank of Nigeria 'Press Release: Virtual Currencies not Legal Tender in Nigeria' (2018).

European Banking Authority 'EBA Opinion on virtual currencies' (2014).

Financial Stability Board 'Consumer Finance Protection with particular focus on credit' (2011)
Financial Stability Board: Basel.

IMF International Transactions in 'Remittances: Guide for Compilers and Users' (2009).

South African Reserve Bank 'Position Paper on Virtual Currencies' (2014).

South African Reserve Bank 'Currency and Exchanges guidelines for individuals' (2018).

United Nations Conference on Trade and Development 'Manual on Consumer Protection' (2017)
United Nations Conference on Trade and Development: Geneva.

REPORTS

Financial Action Task Force FATF Report *Virtual Currencies Key Definitions and Potential AML/CFT Risks* (2014) Financial Action Task Force: France.

Hileman G and Rauchs M *Global Cryptocurrency Benchmarking Study* (2017) Cambridge Centre for Alternative Finance: Cambridge.

LEGISLATION

Abu Dhabi Global Markets

Guidance Regulations of Cryptocurrency Asset Activities introduced under section 15(1) of the Financial Services and Markets Regulations



Australia

Anti-Money Laundering and Counter Terrorism Financing Act 2006

China

Public Notice on the Prevention of Risks of Token Offerings and Financing dated 09 September 2017

India

Circular on the Prohibition on dealing in virtual currencies dated 06 April 2018 Circular RBI/2017-2018/154

Japan

Payment System Act

Kenya

Banking Act Cap 488 of 1995

Central Bank of Kenya Act 15 of 1966

Money Remittance Regulations, 2013 Kenya Gazette Supplement No. 56 dated 19 April 2013

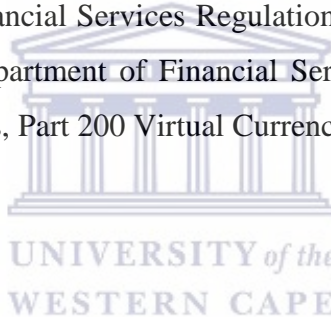
Proceeds of Crime and Anti-Money Laundering Act 9 of 2009

Article 46 of the Constitution of Kenya

Consumer Protection act 46 of 2012

New York State

New York State Department of Financial Services Regulations issued under the New York Codes, Rules and regulations, Title 23 Department of Financial Services, Chapter 1, Regulations of the Superintendent of Financial Services, Part 200 Virtual Currencies



Nigeria

Banks and Financial Institutions Act Cap B3, Laws of the Federation of Nigeria, 2004

Foreign Exchange (Monitoring and Miscellaneous Provisions) Act Chapter F 34 (Decree No. 17 of 1995)

Guidelines for the Operation of International Transfers dated 26 September 2014 issued by the Central Bank of Nigeria

Money Laundering (Prohibition) Act 25 of 2011

Consumer Protection Council Act Cap 25 of 2004

Philippines

Circular on the Guidelines of Virtual Currency Exchanges Circular No. 994 of 2017 incorporated as section 4512N of the Manual of Regulations for Non-Banking Financial Institutions

South Africa

Financial Advisory and Intermediary Services Act 37 of 2002

Financial Service Regulation Act 9 of 2017

Banks Act 94 of 1990

Currency and Exchanges Control Act 9 of 1933

Exchange Control Regulations GN R1111 GG R445

Prevention of Organised Crime Act 121 of 1998

Financial Intelligence Centre Act 38 of 2001

Consumer Protection Act 68 of 2008

United States of America

United States of America Financial Crimes Enforcement Network 2013 Guidance issued 18 March 2013

INTERNET REFERENCES

Admin 'Belfrics Global Launches Bitcoin Exchange in Kenya' 13 August 2017 available at e-labz.info/blog/belfrics-bitcoin-exchange-kenya/ (accessed 25 October 2018).

Belfrics 'Terms and Conditions' available at <https://kenya.belfrics.com/terms-conditions/> (accessed 24 October 2018).

Belfrics 'About Belfrics: A secure cryptocurrency exchange in Kenya' available at <https://kenya.belfrics.com/about/> (accessed 24 October 2018).

Bitcoin Crime 'Cryptocurrency Exchanges have been used to launder \$88 million since 2016: WSJ' 29 September 2018 available at <https://www.ccn.com/cryptocurrency-exchanges-have-been-used-to-launder-88-million-since-2016-wsj/> (accessed 02 December 2018).

BitPesa 'Terms and Conditions of Service' available at <https://www.bitpesa.co/terms/> (accessed on 20-21 October 2018).

Boateng K ‘Despite risks, cryptocurrency prints an exciting opportunity for Africa’ 14 June 2018 available at <https://globalriskinsights.com/2018/06/cryptocurrency-opportunity-africa/> (accessed 04 November 2018).

Chen. LY and Nakamura Y ‘Hacked Bitcoin Exchange Says Users May Share \$68 Million Loss’ (2016) <https://www.bloomberg.com/news/articles/2016-08-05/hacked-bitcoin-exchange-says-it-will-spread-losses-among-users> referred to in Moore *et al* (2016) A:2.

Hamilton D ‘Ethereum Mining vs. Bitcoin Mining: Which is more profitable?’ 04 October 2018 available at <https://coincentral.com/ethereum-mining-vs-bitcoin-mining-which-is-more-profitable/> (accessed 05 March 2019).

Higgins S ‘The Bitfinex Bitcoin hack: What we know (and don’t know)’ 03 August 2016 updated 20 June 2018 available at <https://www.coindesk.com/bitfinex-bitcoin-hack-know-dont-know> (accessed 08 March 2019).

International Fund of Agricultural Development ‘Sending Money to Home to Africa Remittance Markets enabling environment and prospects’ October 2009 available at https://www.unicef.org/socialpolicy/files/sending_money_home_to_africa.pdf (accessed 05 March 2019).



Lee M ‘Bitcoin exchange robbed of US 250 000, all trading halted’ 5 September 2012 available at <https://www.zdnet.com/article/bitfloor-exchange-robbed-of-us250000-all-trading-halted/> (accessed 08 March 2019).

Luno ‘Terms of Use: Know the rules of using Luno’ available at <https://www.luno.com/en/legal/terms> (accessed 22 October 2018).

Luno ‘Company Information’ available at <https://www.luno.com/en/legal/impressum> (accessed 26 October 2018).

Luno Help Centre ‘How does Luno work?’ available at <https://www.luno.com/help/en/articles/11000001992-how-does-the-luno-exchange-work> (accessed 22 October 2018).

Medium ‘Custodial vs Non-Custodial Wallet Benefit of light wallets’ available at <https://medium.com/guarda/%EF%B8%8Fcustodial-vs-non-custodial-wallet-s-%EF%B8%8F-benefits-of-light-wallets-87cf701054d1> (accessed 05 August 2018).

Moore T, Christin N, and Szurdi J ‘Revisiting the risks of Bitcoin Currency Exchanges’ (2016) available at <https://tylermoore.utulsa.edu/toit17.pdf> (accessed 08 November 2018).

Nicholls A ‘The challenges and benefits of risk-based regulation in achieving scheme outcomes’ (Paper presented to the Actuaries Institute Schemes Seminar during 08 to 10 November 2015) 2 available at <https://www.actuaries.asn.au/Library/Events/ACS/2015/NichollsRegulation.pdf> (accessed 02 November 2018).

Norry A ‘The history of the MtGox hack: Bitcoin’s biggest heist’ 2 July 2018 available at <https://blockonomi.com/mt-gox-hack/> (accessed 30 October 2018) (hereinafter referred to as ‘Norry July 2018’).

Orgera S ‘Is Litecoin the same as Bitcoin?’ 12 February 2019 available at <https://www.lifewire.com/what-is-litecoin-4151693> (accessed 05 March 2019).

Park N, Kim M, Lee D ‘Cryptocurrency laws and regulations in South Korea’ 12 July 2018 available at <https://www.vantageasia.com/cryptocurrency-law-south-korea/> (accessed 15 November 2018).

Pollock D ‘The mess that was MtGox: Four years on’ available at <https://cointelegraph.com/news/the-mess-that-was-mt-gox-four-years-on> (accessed 30 October 2018).

Preiss RM ‘Cryptocurrency is the great African opportunity’ 08 August 2017 available at <https://www.ntusbfcas.com/african-business-insights/content/cryptocurrency-is-the-great-african-opportunity> and <https://www.howwemadeitinafrica.com/cryptocurrency-great-african-opportunity/59402/> (accessed 04 November 2018).

Sprenger P and Balsiger F ‘Anti-money laundering in times of cryptocurrencies’ June 2018 available at <https://assets.kpmg.com/content/dam/kpmg/ch/pdf/anti-money-laundering-in-times-of->

cryptocurrency.pdf (accessed 01 December 2018) (hereinafter referred to as ‘Spenger and Balsiger (June 2018)’).

Sharma M ‘Cryptocurrency and the Regulators Dilemma’ 1 August 2017 13 available at https://idsa.in/system/files/comments/sf_cryptocurrencies_msharma.pdf (accessed 26 November 2018) (hereinafter referred to as ‘Sharma (1 August 2017)’).

The Law Library of Congress ‘Regulation of Cryptocurrency: Japan’ available at <https://www.loc.gov/law/help/cryptocurrency/japan.php> (accessed 31 October 2018).

The Mission Daily ‘Decentralise Cryptocurrency Exchanges: A Comprehensive Overview’ 21 February 2018 available at <https://medium.com/the-mission/decentralized-cryptocurrency-exchanges-a-comprehensive-overview-a154a92ac1cb> (accessed 01 August 2018).

Veksler D ‘Introduction to Bitcoin custody options’ 08 March 2018 available at <https://vellum.capital/2018/03/08/introduction-to-cryptocurrency-custody-options/> (accessed 07 November 2018).

Western Union ‘About Us’ available at <https://corporate.westernunion.com/index.html> (accessed 05 November 2018).



Whittaker S, Ng S and Lee H ‘New AML/CFT Regulations for cryptocurrency exchanges’ 23 April 2018 available at www.pwc.com.au (accessed 18 November 2018).

Wieczner J ‘\$1 Billion Bitcoins lost in the MtGox hack to be returned to victims’ available at <http://fortune.com/2018/06/22/bitcoin-price-mt-gox-trustee/> (accessed 30 October 2018).

Zhao W ‘Coinrail Exchange hacked, losses possibly \$ 40 million in cryptos’ 18 June 2018 available at <https://www.coindesk.com/coinrail-exchange-hacked-loses-possibly-40-million-in-cryptos> (accessed 08 March 2019).