The South African legal framework's response to the prevalence of cybercrime in electronic commerce

HI Joynt

orcid.org/0000-0003-1201-4779

Dissertation accepted in fulfilment of the requirements for the degree Master of Law with Trade and Business Law at the North-West University

Supervisor: Prof WJ du Plessis

Co-supervisor: Prof W Erlank

Graduation: June 2023

Student number: 28496159

Abstract

At present, cryptocurrency is not centrally regulated in South Africa. The study aims to determine the extent and capacity of the South African legal framework to regulate and protect all parties to electronic commerce from the dangers that stem from cryptocurrency-related fraud. The research is specifically aimed at determining whether e-commerce and cybercrime legislation may provide a basis for cryptocurrency regulation. This is because, where cryptocurrency is unlawfully employed either as the target of illicit activity or as a means to a further end (such as money laundering), cybercrime legislation automatically applies. This is due to the fact that cybercrime is defined as the unlawful access, interception or alteration of data. The broad definition leaves scope for any sort of fraudulent cyber activity to fall within the boundaries of cybercrime.

The research seeks to determine whether a comprehensive cryptocurrency regulatory structure can be formed from the pre-existing e-commerce legal framework and, if so, what minor amendments can be made to successfully account for cryptocurrency under this legal framework. To complete the research, a full examination of the concepts forming part of e-commerce is required, followed by the cybercrime implications of e-commerce. After that, the correlation between cybercrime and cryptocurrency must be examined. This is to be followed by the international and foreign law positions on cryptocurrency. Finally, the current South African legal framework is examined, followed by possible recommendations.

After a thorough examination of all the above concepts, the study found that the applicable e-commerce and cybercrime legal framework does provide a basis for the regulation of cryptocurrency. Minor legislative amendments can provide a complete overhaul of the South African position on cryptocurrency, thereby creating a regulatory framework for cryptocurrency.

Opsomming

Daar is tans geen sentrale regulering ten opsigte van kripto-geldeenhede in Suid-Afrika nie. Die studie beoog om die vermoëns en kapasiteit van die Suid-Afrikaanse regsraamwerk om die rolspelers in elektroniese handel te beskerm teen die moontlike risiko's wat gepaard gaan met kriptogeldeenhede, te bepaal. Die navorsing fokus spesifiek daarop om die moontlikheid te bepaal dat die huidige regsraamwerk op e-handel en kubermisdaad reeds 'n basis vorm vir die regulering van kripto-geldeenhede. Dit is weens die feit dat wanneer kriptogeldeenhede onregmatig gebruik word, hetsy as hulpmiddel vir verdere kubermisdaad of as die teiken daarvan, sal kuberwetgewing outomaties van toepassing wees. Dit is omdat kubermisdaad gedefinieer word as die onregmatige toegang, onregmatige onderskepping of onregmatige verandering van data. Hierdie breë definisie maak dit moontlik dat enige vorm van bedrieglike kuberaktiwiteite geklassifiseer kan word as kubermisdaad. Die navorsing beoog dus om te bepaal of 'n omvattende regsraamwerk vir kripto-geldeenhede gevorm kan word, voortvloeiend uit die huidige e-handel- en kubermisdaadwetgewing. Om die studie te voltooi sal 'n volledige ontleding gedoen word op die konsep van e-handel. Dit sal gevolg word deur 'n omvattende ontleding van kubermisdaad. Daarna sal die korrelasie tussen kubermisdaad en kripto-geldeenhede ondersoek word. Hieruit volg 'n ontleding van die internasionale asook buitelandse regsraamwerk op kriptogeldeenhede. Eindelik, sal die huidige Suid-Afrikaanse regsraamwerk bestudeer word, asook moontlike aanbevelings gelewer word. Na aanleiding van 'n omvattende studie van al die bogenoemde onderwerpe, word daar bevind dat die toepaslike e-handel- en kubermisdaadregsraamwerk wel 'n basis bied vir die regulering van kriptogeldeenhede. Geringe wetswysigings kan lei tot 'n volledige verandering van die huidige regsposisie op kriptogeldeenhede. Sodoende kan 'n regsraamwerk daargestel word vir kriptogeldeenhede in Suid-Afrika.

Keywords

Cybercrime – Cryptocurrencies – Cyber security - Trade and Commerce – Legal Frameworks – Electronic Commerce – Jurisdiction – Crime Prevention –– Consumer Protection

Acknowledgments

I would like to extend my sincerest graditute to all those who supported me throughout the past two years of study.

To my supervisor, thank you for ensuring the smooth running of the process and your resolute willingness to assist me whenever called upon to do so. To my co-supervisor, thank you for contributing your expertise and insight to the study.

To my mother, thank you for supporting my academic journey, and for introducing me to a life in the legal field. To my father, thank you for your unwavering moral support. To my sister, thank you for your endearing care and support throughout the process.

To my karate *senseis*, Johan and Madelein, as well as my fitness coach, Johanni, thank you for keeping my physical wellbeing at an exceptional standard to ensure optimal mental clarity throughout.

Table of Contents

List of Abbreviations

ABLJ	American Business Law Journal
CPA	Consumer Protection Act 68 of 2008
E-commerce	Electronic Commerce
ECTA	Electronic Communications and Transactions Act 25 of 2002
FIC	Financial Intelligence Centre
FICA	Financial Intelligence Centre Act 38 of 2001
FSCA	Financial Sector Conduct Authority
IEC	International Electronic Commerce
IRS	Internal Revenue Service (USA)
IFWG	The Intergovernmental Fintech Working Group
KYC	Know-Your-Customer
MLEC	Model Law on Electronic Commerce
MLES	Model Law on Electronic Signatures
NFT	Non-Fungible Token
OECD	Organisation for Economic Co-operation and Development
PAJA	Promotion of Administrative Justice Act 03 of 2000
PER/PELJ	Potchefstroom Electronic Law Journal
POCA	Prevention of Organised Crime Act 121 of 1998

POPIA	Protection of Personal Information Act 04 of 2013
RICA	Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002
SALC	South African Law Commission
SARS	South African Revenue Services
SORMA	Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007
THRHR	Tydskrif vir Hedendaagse Romeins-Hollandse Reg (Journal for Contemporary Roman-Dutch Law)
WIPO	World Intellectual Property Organisation
WTO	World Trade Organisation

Chapter 1: Introduction and Problem Statement

1.1 Problem Statement

1.1.1 Background

With each passing day, technology seems to be developing and improving at an unprecedented rate.[1] Consequently, various sectors and industries must keep up and adapt to these changes or risk becoming obsolete. In some instances, industries are vulnerable to misuse. The law is not exempt from the changes in technology and has to continually adapt to keep up with the rapid pace at which technology influences people's daily lives and the industries which they form part of. A new challenge for these industries and the laws governing them, has been the influx in the use of technology to further international trade transactions.[2] The use of the internet as a platform for trading goods and services is known as electronic commerce.[3]

International trade has been affected by the rise of the internet and its accessibility. It has caused the gap between buyer and seller to virtually vanish. This is because electronic commerce platforms have facilitated a common meeting place between consumer and trader, even though either party may be on opposite ends of the earth from each other.[4] The rise in the prevalence of electronic commerce has also facilitated the use of cryptocurrencies.[5]

Cryptocurrency can be described as a digital currency that operates as a cryptographic string of words or digits and is used as a unit of account.[6] Cryptocurrency operates on

---

1 Schwab 2016 https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.
2 OECD 2019 *OECD Going Digital Policy Note* 1.
3 Bloomenthal 2020 https://www.investopedia.com/terms/e/ecommerce.asp.
4 Eiselen 2007 *PER/PELJ* 2.
5 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 71.
6 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 71; Orffer *The Inclusion of Virtual Currencies in the Calculation of Income Tax* 8.

a peer-to-peer basis and is facilitated through the internet.[7] Frankenfield defines cryptocurrency as

> [a] digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. Many cryptocurrencies are decentralised networks based on blockchain technology - a distributed ledger enforced by a disparate network of computers. A defining feature of cryptocurrencies is that they are generally not issued by any central authority, rendering them theoretically immune to government interference or manipulation.[8]

The Intergovernmental Fintech Working Group (IFWG) has, in the wake of the ever-increasing prevalence in the use of cryptocurrency in South Africa, attempted to define the notion of cryptocurrency in a South African context.[9] The IFWG definition focuses on the practical economic influence of cryptocurrency as opposed to a clear-cut clinical or technical definition. The IFWG defines cryptocurrency from a South African point of view as:[10]

> Crypto assets are digital representations or tokens that are accessed, verified, transacted, and traded electronically by a community of users. Crypto assets are issued electronically by decentralised entities and have no legal tender status, and consequently are not considered as electronic money either. It therefore does not have statutory compensation arrangements. Crypto assets have the ability to be used for payments (exchange of such value) and for investment purposes by crypto asset users. Crypto assets have the ability to function as a medium of exchange and/or unit of account and/or store of value within a community of crypto asset users.[11]

In line with the above definition and in close connection thereto, Reddy and Minnaar note that by way of its characteristics, cryptocurrency does not require the intermediary backing from banks or central authorities and can thus not be attributed to a particular sovereign jurisdiction, and therefore, as they put it, can be seen as an

---

7 Maanda *Legal Implications of Virtual Currencies* 2; *Reddy* and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 72.

8 Frankenfield 2021 https://www.investopedia.com/terms/c/cryptocurrency.asp.

9 IFWG 2018 *Consultation Paper on Policy Proposals for Crypto Assets* 1-2. In the report, the IFWG refers to cryptocurrency as crypto assets. For all intents and purposes, unless otherwise indicated, these terms are used interchangeably.

10 IFWG 2018 *Consultation Paper on Policy Proposals for Crypto Assets* 9.

11 IFWG 2018 *Consultation Paper on Policy Proposals for Crypto Assets* 9.

international online currency.[12] However, as noted by the IFWG, it is not a recognised currency in South Africa, although it can be used as a method of exchange. Due to its nature, cryptocurrency has the potential to create legal complications. It may be open to misuse as regulation is challenging for governments and authorities, and South Africa is classified as self-regulating. Therefore, without a structured legal framework for proper regulation, the misuse of cryptocurrencies may provide potential platforms for money laundering and tax evasion, or may even become a tool for the facilitation of other forms of cybercrime and, in some instances, even a target for traditional forms of cybercrime.[13]

Although great for the furtherance of international trade and limiting the gap between buyer and seller,[14] if not properly regulated under the guise of the law, it may leave room for misuse and leave many consumers, traders, companies and the like vulnerable to cybercrime.[15] Desai notes that even though cybercriminals are not gun-wielding masochists, their preferred weapon of choice, a computer mouse, may potentially carry even more devastating effects for citizens.[16] He further notes that governments, banks, individuals and organisations are all at risk and may become potential cybercrime targets if these threats are not neutralised.[17]

With technology becoming ever more accessible to the masses and increasingly more sophisticated, cybercriminals are increasingly more nuanced in commissioning their attacks.[18] The National Cyber Security Hub reported that between 2011 and 2015, in

---

12 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 72.

13 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 74-86; Maanda *Legal Implications of Virtual Currencies* 12-27.

14 Schulze 2006 *SA Mercantile Law Journal* 31.

15 Kouamo *Combating Crime in International Electronic Commerce* 2. The misuse of cryptocurrencies may also fall under the blanket term of 'cybercrime'. This work aims to investigate the consequences of what is traditionally thought of as forms of cybercrime such as hacking, credit card fraud and the like as well as the mismanagement and misuse of cryptocurrencies. For instance, Erasmus and Bowden note that cryptocurrency may potentially be used for money laundering and other financial crimes. Erasmus and Bowden 2020 *Obiter* 310.

16 Desai 2018 *Acta Criminologica: Southern African Journal of Criminology* 149.

17 Desai 2018 *Acta Criminologica: Southern African Journal of Criminology* 150.

18 Desai 2018 *Acta Criminologica: Southern African Journal of Criminology* 150.

excess of six thousand attacks were recorded on economically essential South African infrastructure, businesses, and internet service providers.[19] Furthermore, credit card fraud, money laundering, hacking, gate-crashing, social engineering and the like all fall under the umbrella term of cybercrime. These are all forms that fall within the scope of the Cybercrimes Act 19 of 2020, even though the Act uses different wording.[20]

Cybercrime, if not adequately regulated, can have dire consequences for all parties in respect of electronic trade. This affects not only the parties to the trade itself, but also the essential commercial infrastructure which provides the platform for the trade in question, such as banks, internet service providers and various other stakeholders.

Therefore, with the new *Cybercrimes Act* 19 of 2020,[21] being recently assented to by the President,[22] it is now more than ever a prevalent issue to examine the legal frameworks governing electronic commerce and the prevention of cybercrime. It is important to view cryptocurrency regulation alongside it as it may also be a tool or target for the commission of cybercrime. This, in turn, will show whether South African e-commerce users are safeguarded from the dangers of cybercrime as it relates to cryptocurrency.

1.1.2 Motivation

The Organisation for Economic Co-Operation and Development (hereafter "OCED") notes that digitisation provides a platform for consumers and traders to meet, notwithstanding any physical boundaries and impediments in the distance.[23] They

---

19 Mpuru 2017 *Servamus Community-based Safety and Security Magazine* 44.

20 For instance, in section 2 the Act refers to Unlawful Access. However the section is wide enough to include forms of cybercrime such as hacking or social engineering. The forms of cybercrime and their relation to the provisions of the Act will be discussed in chapter 2 of this work.

21 *Cybercrimes Act* 19 of 2020.

22 Bhagattjee et al 2021 https://www.cliffedekkerhofmeyr.com/en/news/publications/2021/TMT/technology-media-and-telecommunications-sector-newsletter-9-june-regulating-the-fourth-industrial-revolution-south-africas-cybercrimes-bill-is-signed-into-law.html.

23 OCED 2019 *OCED Going Digital Policy Note* 1.

state that this is enabled through services being delivered digitally and that traditional trade systems are furthered by increased connectivity.[24] The OCED further notes that, with the increased reliance on technology and digitisation of trade, new stakeholders emerge, and new business models are designed. Alongside this is an ever-growing scale of transactions.[25] Given the current global economic reach of the internet, traders would be unwise not to engage in e-commerce as it provides numerous advantages, such as greater engagement between potential clients and customers and an efficient and fast trading method.[26]

However, the rise of e-commerce has also brought about certain harmful practices and potential legal dilemmas if not governed competently.[27] Given the vast scope of the internet, it is trite that traditional geographical boundaries cannot contain its reach. This potentially creates an issue in a jurisdictional sense, as the internet does not adhere to traditional jurisdictional rules.[28] Furthermore, the rise of electronic commerce has been accompanied by a rise in cybercrime, and therefore, proper legal regulation is required to circumvent any threats posed by cyber attacks.[29]

Recently, high-level cases of cyber attacks have been on the rise. For instance, on 12 March 2021, a cyber attack was reported to have targeted the insurance and investment group PPS. In this instance, cybercriminals tried to gain access to the company's investment systems. However, they only succeeded in affecting certain interfaces between members and financial advisers.[30] Another notorious attack occurred on 22 July 2021, when it was reported that the state transport parastatal, Transnet, had suffered an unprecedented, significant and damaging cyber attack.[31]

---

24 OCED 2019 *OCED Going Digital Policy Note* 1.
25 OCED 2019 *OCED Going Digital Policy Note* 1.
26 Kouamo *Combating Crime in International Electronic Commerce* 1-2.
27 Kouamo *Combating Crime in International Electronic Commerce* 1-2.
28 Schulze 2006 *SA Mercantile Law Journal* 32.
29 Kouamo *Combating Crime in International Electronic Commerce* 2.
30 PPS 2021 https://www.pps.co.za/malicious-cyber-attack.
31 Reva 2021 https://issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports.

The attack targeted the electronic operational networks of ports and container terminals. The Institute for Security Studies describes the attack as the first instance of an attack in which the operational integrity of the nation's critical maritime infrastructure has been drastically affected.[32] The attack targeted the automated systems regulating the movement of ships in the harbour. It was reported that entries had to be made by hand after the critical electronic systems had collapsed. This caused high levels of backlogging of ships wishing to enter and leave the South African harbours. The impact of the attack on the economy is far-reaching as the basis for economic trade, the transport system, had been severely affected, meaning enormous amounts of trade goods could not reach their respective destinations.[33]

The above incidents highlight that a cyber attack can occur at any time and can target anyone, even major corporate investors or semi-state entities who claim to have high levels of cybersecurity. Therefore, the law must be called upon to crack down on cybercriminals to prevent further attacks of such a nature.

The focus of this dissertation is to examine the regulatory and legal frameworks in South Africa which relate to cyber security and cryptocurrency to determine whether users of electronic commerce platforms are sufficiently safeguarded against malicious infringement. A short explanation of some potential threats of cryptocurrency misuse will follow.

This work will also include discussions on the misuse of cryptocurrency as a form of cybercrime. A short explanation of some of the potential threats of cryptocurrency misuse as a form of cybercrime will follow after an introductory statement on the e-commerce platform in South Africa.

---

32 Reva 2021 https://issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports.

33 Reva 2021 https://issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports.

1.2 Electronic Commerce in South Africa

The World Trade Organisation (WTO) defines electronic commerce as the use of electronic means to distribute, market, produce, deliver or sell goods and services between individuals, enterprises, households, governments or any other private or public institutions.[34] In South Africa, electronic commerce is rising, and most large retailers have taken to the digital sphere to conduct business transactions.[35] To put this in context, the Competition Commission notes that *Takealot.com* (South Arica's biggest online retailer) has grown so exponentially that users have grown reliant on its services in lieu of traditional brick-and-mortar retailers.[36]

Protection is afforded to consumers by way of the *Electronic Communications and Transactions Act* 25 of 2002 (hereafter referred to as ECTA).[37] Additionally, legislation afforded to traditional commercial transactions also applies to online transactions, including the *Consumer Protection Act* 68 of 2008 (hereafter referred to as CPA) and the *Protection of Personal Information Act* 04 of 2013 (hereafter referred to as POPIA).[38] Phora explains that even though ECTA and CPA provide statutory rights that offer protection to online consumers, further legislative enhancement may be required to align the South African legal framework with the rapid growth of online commerce.[39]

The newly assented *Cybercrimes Act* 19 of 2020 aims to address the shortcomings of the previous legal framework by overriding and/or supplementing various other

---

34 Phora *Developing a Legal Framework for E-Commerce in South Africa* 24.
35 Phora *Developing a Legal Framework for E-Commerce in South Africa* 34.
36 Anon 2021 https://businesstech.co.za/news/internet/491029/competition-commission-launches-investigation-into-takealot-ubereats-and-other-online-markets/.
37 *Electronic Communications and Transactions Act* 25 of 2002.
38 Consumer Protection Act 68 of 2008; Protection of Personal Information Act 04 of 2013 as read together with the *Promotion of Administrative Justice Act* 3 of 2000*;* Phora *Developing a Legal Framework for E-Commerce in South Africa* 36.
39 Phora *Developing a Legal Framework for E-Commerce in South Africa* 40.

statutes.[40] Both legal frameworks will be studied for a comprehensive determination on the effectiveness of the South African legal framework on e-commerce.

1.3 Cybercrime and its Regulation

Cybercrime as a concept creates a headache for legal enforcement. Web-based crimes do not adhere to the traditional bounds of jurisdiction.[41] This means that a perpetrator of cybercrime may be on the opposite end of the earth to his potential victim. Cybercrime can reach as far and wide as the internet itself.[42] Kempen is of the opinion that, as a result, states should work together to curb the issue of cybercrime regarding territoriality.[43] However, as of yet, only one international instrument exists to expressly address cybercrime.[44] The *Council of Europe Convention on Cybercrime* of 2001, also known as the *Budapest Convention,*[45] is a multilateral treaty aimed at the creation of a legal framework for the combatting and regulation of crimes committed by way of the internet or utilising computer networks and includes, *inter alia,* computer-related fraud, network security violations and copyright transgressions.[46]

The fact that only one international convention exists for states to work in unison to regulate cybercrime issues, speaks volumes. Cybercrime as a concept knows no territorial borders. Furthermore, technology and, by extension, cybercriminals are becoming ever more sophisticated and complex. Therefore, a convention already two decades old, may be outdated in its efforts to address cybercrime issues.

---

40 Bhagattjee et al 2021 https://www.cliffedekkerhofmeyr.com/en/news/publications/2021/TMT/technology-media-and-telecommunications-sector-newsletter-9-june-regulating-the-fourth-industrial-revolution-south-africas-cybercrimes-bill-is-signed-into-law.html.

41 Kouamo *Combating Crime in International Electronic Commerce* 8.

42 Kempen 2019 *Servamus* 27.

43 Kempen 2019 *Servamus* 27.

44 Kempen 2019 *Servamus* 27. Note that other international instruments such as the *UNCITRAL-Model law on Electronic Commerce* (1996) and the - *Model Law on Electronic Signatures* (2001) and many others also play an important role in the combatting of cybercrime and will be discussed throughout the course of the dissertation.

45 *Council of Europe Convention on Cybercrime* (ETS 185) of 2001.

46 Kempen 2019 *Servamus* 27.

Locally, the *Cybercrimes Act* was signed into law on 26 May 2021.[47] Watney remarks this to be the South African legal system's response to the influx of cybercrime, which has risen since the start of the fourth industrial evolution.[48] The Act aims to criminalise certain conduct related to the interreference of data and impose sanctions thereto. It also aims to better grasp jurisdictional issues related to cyberoffences.[49] This work will examine the *Cybercrimes Act* to determine whether it can succeed in its purposes, as well as whether it has constricted the *lacuna* which has followed under the previous legal framework as a result of the fourth industrial revolution. Furthermore, cognisance will be taken of the Act through the lens of cryptocurrency to determine whether it may lay a basis for cybercrimes related to cryptocurrency.

1.4 Money Laundering

Another potential threat is money laundering. The *Prevention of Organised Crimes Act* 121 of 1998 describes money laundering as an activity by which proceeds from illegal activity are concealed.[50] Cryptocurrencies have the potential to be used in all stages of the money laundering process,[51] and due to their nature, could be used as a means of transforming money illicitly gained into what is known as "clean" money by removing it as far as possible from the commission of the illicit activities whereby it was attained.[52] By doing so, the money cannot be traced back to the illicit activity. This work will aim to give insight into whether the South African framework on cryptocurrency is sufficient to prevent money laundering from taking place in this way.

---

47 De Rebus 2021 https://www.derebus.org.za/new-legislation-august-2021/.
48 Papadopoulos and Snail ka Mtuze *Cyberlaw* 477.
49 Papadopoulos and Snail ka Mtuze *Cyberlaw* 477.
50 S4 of the *Prevention of Organised Crimes Act* 121 of 1998.
51 Maanda *Legal Implications of Virtual Currencies* 13. Maanda refers to this as the three stages of money laundering. He describes it as the placement stage, the layering stage and the reintegration stage. Although this is not a hard and fast rule to determine whether money laundering has *de jure* taken place, it is a useful method for gaining insight into the process of money laundering.
52 Maanda *Legal Implications of Virtual Currencies* 13-14.

1.5 Cryptocurrency Used in the Commission of Cybercrime

The dark web is an internet platform that facilitates commercial transactions of an illicit nature.[53] This includes, *inter alia,* buying and selling illegal goods such as narcotics, firearms and human organs. It can only be accessed with specialised software.[54] By using cryptocurrencies as a payment method on the dark web, it creates an ideal marketplace for quick and anonymous transactions of these illegal goods.[55] Furthermore, cryptocurrencies are used in conjunction with these darknet trading sites as a means by which terrorism is financed.[56] In this instance, it is important to take note of the international legal fraternity's response. Notable investigations and instances to be discussed is that of *Silk Road* and *Darkode,* respectively, and how the South African legal system can respond by implementing such guidelines into its local law.[57]

1.6 Cryptocurrency as a Target for Cybercrime

Not only can cryptocurrency act as a means for the furtherance of cybercrime, but it in itself may fall victim to the dangers of cybercrime. Reddy and Minnaar note that cryptocurrency exchangers and payment processing platforms may also be vulnerable to more traditional forms of cybercrime, such as hacking and phishing.[58] Hacking can be defined as the use of electronic means to gain unauthorised entry into other electronic systems or networks with malicious intent to steal, alter or disable information or devices.[59] In terms of cryptocurrency, hacking is used to either take unauthorised control of someone else's electronic wallet or to redirect the mining pool

---

53 Maanda *Legal Implications of Virtual Currencies* 17.
54 Maanda *Legal Implications of Virtual Currencies* 17.
55 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 74.
56 Maanda *Legal Implications of Virtual Currencies* 18.
57 *United States of America v Ross William Ulbricht Dread Pirate Roberts Silk Road Sealed Defendant* Dpr 15-1815 May 31, 2017; Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 78.
58 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 78.
59 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 78.

to have the cryptocurrency go to the hacker instead of the rightful user.[60] Essentially, most hacking, that concerns cryptocurrency, is used as a means to steal cryptocurrency by following the same underlying principle as a thief who steals physical money from a wallet. Phishing follows the same idea as hacking, the only difference being that in such an instance, social engineering is used in order to deceive an innocent party into handing over essential personal information so that the phisher can gain access to his or her (the innocent party's) cryptocurrency.[61]

1.7 Conclusion

Therefore, an examination into the current South African legal framework in the areas of electronic trade; cybercrime and cybersecurity; cryptocurrency and its inherent dangers when mismanaged or unregulated; as well as safe online regulation and monitoring, both from a domestic law as well as international law perspective, is required to ensure the parties mentioned above are safe to trade and thereby grow the economy; allow platforms for economic innovation and provide for greater worldwide reach for South African trade. The analysis will have to look at potential shortcomings in all of the above-mentioned concepts from a South African legal perspective, and provide insight into these inadequacies and possibly provide remedies. Thus, in today's economic and worldwide climate, it is now, more than ever, necessary to provide insight into how the South African legal system deals with cryptocurrency related fraud, especially with a comprehensive new statute dealing with cybercrime, being enacted.

1.8 Research Question

To what extent is the current South African legal framework equipped to deal with the misuse of cryptocurrencies as it relates to electronic commerce?

---

60 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 78.
61 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 80.

1.9 Research Aims and Objectives

This work aims to determine the extent and capacity of the South African legal framework to regulate and protect all parties to electronic commerce from the potential dangers of the misuse of cryptocurrencies within a cybercrime context. In order to do so, a thorough examination is required on all concepts and principles which fall under the terms relating to electronic commerce, cybercrime and cryptocurrency. Once each concept has been analysed, it is necessary to examine the legal framework encompassing these concepts. After that, it may be determined whether the South African legal framework is effective in its aims or whether any shortcomings are noted. If so, what possible recommendations could be employed to address the relevant *lacuna*?

1.10 Premises, assumptions and hypothesis

1.10.1 Points of Departure

- Fraud relating to the misuse of cryptocurrencies will be considered cybercrime as it is a form of online crime.
- Electronic means to facilitate national and international commercial transactions are growing exponentially, and the legal system needs to incorporate proper boundaries to protect users from criminal and malicious exploitation.
- The use of digital platforms for trade is the way forward for commercial transactions and carries many economic benefits for all parties involved. However, it does require a proper legal framework in which to function.
- Exploitation in the context of e-commerce can take many forms and is covered by the umbrella term of cybercrime.
- The introduction of cryptocurrencies has opened new avenues for cybercriminals to exploit and should be examined within the bounds of what is traditionally thought of as cybercrime.

- The newly promulgated *Cybercrimes Act* 19 of 2020 is a welcome step in the right direction. However, it waits to be seen whether it provides a comprehensive answer to issues of cybersecurity as it relates to cryptocurrencies.

1.10.2 Assumptions

- Developments of the law relating to electronic commerce and the protection of its users are happening at a slower rate than developments in technology and as a result, are leaving a *lacuna* for cybercriminals to exploit.
- An adequate international law response that would allow various states to work in unison regarding issues of cybercrime, is required to circumvent the inherent lack of territoriality that cybercrime holds.
- South Africa's lawmakers are taking cognisance of cybersecurity issues, as is evident by the promulgation of the *Cybercrimes Act* 19 of 2020.

1.10.3 Hypothesis

The South African legal framework on cybercrime already sets the basis for the regulation of cryptocurrency. Minor legislative amendments could lead to a complete ratification of the South African legal framework's regulation of cryptocurrency.

1.11 Research Methods

In order to complete the study into the matter as described above, a literature review of the various legislative statutes and regulations dealing with all aspects of electronic commerce, cybercrime prevention and cryptocurrencies will have to be examined. This includes an analysis of the *Cybercrimes Act* 19 of 2020[62], the *Electronic Communications and Transactions Act* 25 of 2002,[63] the *Prevention of Organised Crime*

62 *Cybercrime and Cybersecurity Bill* (B6-2017).
63 *Electronic Communications and Transactions* Act 25 of 2002.

Act 121 of 1998,[64] the *Financial Intelligence Centre Act* 38 of 2001,[65] and all other relevant statutes and regulations as well as the South African Common-law position.[66]

Additionally, secondary sources dealing with these issues will have to be consulted. This, *inter alia,* includes published works such as studies by the OCED[67] and National Cyber Security Hub[68] and the like. The majority of research shall be obtained from articles contained in peer-reviewed journals such as the *SA Mercantile Law Journal*[69] and *Acta Criminologica*[70]*,* as well as published master's and doctoral theses.[71]

Furthermore, international law conventions and foreign legal systems may provide a normative basis from which to test and compare the South African legislative framework in this context or may provide for solutions to matters currently tasked with and must therefore be referred to. This will include the *UNCITRAL- Model Law on Electronic Commerce* (1996)[72] and the - *Model Law on Electronic Signatures* (2001)[73] as well as other UN and European initiatives such as the *Council of Europe Convention on Cybercrime* (2001)[74] etcetera. Lastly, international discussions and studies published in literature sources or by way of internet sources may provide for a background basis and explanation on certain technical terms, or provide for the important technical and historical foundation of an issue.

1.12 Framework

The following chapters are contained in the dissertation:

---

64 *Prevention of Organised Crime Act* 121 of 1998.
65 *Financial Intelligence Centre Act* 38 of 2001.
66 Kouamo *Combating Crime in International Electronic Commerce* 46-48.
67 OCED 2019 *OCED Going Digital Policy Note* 1-8*.*
68 Mpuru 2017 *Servamus Community-based Safety and Security Magazine* 44-45.
69 Schulze 2006 *SA Mercantile Law Journal* 31-44.
70 Desai 2018 *Acta Criminologica: Southern African Journal of Criminology* 149-160; Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 71-92.
71 Kouamo *Combating Crime in International Electronic Commerce* 1-72.
72 *UNCITRAL Model Law on Electronic Commerce* (1996).
73 *UNCITRAL Model Law on Electronic Signatures* (2001).
74 *Council of Europe Convention on Cybercrime* (2001).

1. Introduction and problem statement.

2. The legal nature of cybercrime, as well as its effects on electronic commerce.

3. Cryptocurrency and its relevance towards cybercrime.

4. International Perspectives on Cryptocurrency.

5. The South African Perspective.

6. Conclusion and recommendations.

1.13 Relevance for the Research Unit

The Research Unit aims to contribute meaningful research to the cause of law, justice and sustainability. The aim of this study is to provide further insight under the project "Finance, Trade and Innovation". One of the core outcomes of the aforementioned project is to examine the interplay between real society and digital society. The project places emphasis on the use of technology and how it can enhance further trade and innovation. This study focuses on how real-world laws can affect digital platforms and how the use of electronic means can wreak havoc if not properly regulated under the guise of the law. Having proper safeguards in place in order to ensure all parties to electronic commerce are protected from exploitation, would mean that online commerce platforms have to be used for their originally intended purpose. The purpose is to connect consumers and traders from anywhere in the world with one another, thereby creating a global market place which is accessible at any time and any place. This, in turn, leads to the promotion of trade and investment. Therefore, this dissertation is relevant to the Research Unit as it carries direct insight into avenues by which the law can be used to regulate technological enhancements into commercial structures and thereby promote finance, trade and innovation.

Chapter 2: The legal nature of cybercrime, as well as its effects on electronic commerce

2.1 Introduction

The rise and development of technology has facilitated the digitisation of marketplaces. This has enabled traders and consumers to conclude contracts beyond the traditionally known means.[75] The internet, for instance, provides a platform for contracting parties to communicate, interact and complete transactions in a manner never before seen. Coetzee notes that business efficiency and streamlined commerce are some of the many benefits gained from the use of e-commerce methods.[76] However, it is not without flaw. E-commerce poses unique challenges and dangers that, if not properly regulated, can wreak havoc on consumers, traders and even economies.[77]

According to Kouamo, at its basis, the notion of crime itself has undergone considerable changes since web-based commercial transactions have become more prevalent. This is because the use of electronic means that facilitate transactions has also had a converse effect; it has also led to new ways and forms for crime to occur.[78] This situation is exacerbated when one considers that cybercrime is borderless and is therefore difficult to prosecute successfully.[79]

The legal system is required to appropriately respond to the threat of cybercrime and enforce sufficient safeguards and regulations to ensure that individuals, businesses, banks and government departments are safe from cyber-attacks, and that those responsible for such attacks are appropriately prosecuted. However, before cognisance can be taken of the legal system's response to cybercrime, it is first required to

---

75 Coetzee 2004 *Stell LR* 501.
76 Coetzee 2004 *Stell LR* 501.
77 Coetzee 2004 *Stell LR* 501; CSIS 2021 https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
78 Kouamo *Combating Crime in International Electronic Commerce* 8.
79 Kouamo *Combating Crime in International Electronic Commerce* 8; Kempen 2019 *Servamus* 27.

understand what falls within the umbrella of cybercrime. It is also necessary to gain insight into the term e-commerce and how cybercrime affects it. Therefore, an explanation of electronic commerce will follow.

2.2 What is electronic commerce?

2.2.1 The Concept: Electronic Commerce

Phora refers to electronic commerce as the transaction of goods and services via an electronic platform.[80] The internet is used to give consumers access to the vast network of goods and services on offer, including the transfer of money, information or data.[81] People are empowered to purchase a vast array of goods and services at the touch of a button from the comfort of their homes and during any time of day. Eiselen iterates that the internet has given people a more convenient, efficient and international means of commerce.[82] International trade is facilitated in this way by the internet. The internet has created a virtual marketplace for consumers and traders to meet up irrespective of time, distance, location or origin.

The concept itself poses challenges in setting adequate boundaries and, therefore, determining a proper definition.[83] The OECD has, on numerous occasions, attempted to define the concept. In 2001, the OECD produced both a wide interpretation and a narrow definition of the concept "e-commerce".[84]

The wide interpretation reads as follows:

---

80 Phora *Developing a Legal Framework for E-Commerce in South Africa* 10.
81 Phora *Developing a Legal Framework for E-Commerce in South Africa* 10.
82 Eiselen 2007 *PER/PELJ* 2.
83 Phora *Developing a Legal Framework for E-Commerce in South Africa* 23.
84 Phora *Developing a Legal Framework for E-Commerce in South Africa* 23.

> An electronic transaction is the sale or purchase of goods or services, whether between businesses, households, individuals, governments and other public or private organisations concluded over computer-mediated networks.[85]

The wide definition lumps together all forms of potential traders and consumers in whatever capacity they may act, and states that these traders and consumers are brought together by an electronic marketplace achieved through computer networks.

The narrow definition is closely connected to the wide interpretation and reads as follows:

> An internet transaction is the sale or purchase of goods and services, whether between businesses, households, individuals, governments and other public or private organisations concluded over the internet.[86]

The narrow definition takes the consumers and traders in their respective capacities, as stated in wide interpretation, and provides that these role-players conclude the purchase or sale of goods and services over the internet instead of an electronic marketplace. The only substantial difference between the two definitions is that the notion of an electronic marketplace achieved through a computer-mediated network is now replaced with the internet in itself. This merely places the definition in its realistic context in that the internet is the main focus that provides for the transaction. This definition accurately reflects the real-world position on e-commerce and removes it from an overly complicated abstract academic concept.

---

85 OECD 2019 https://www.oecd-ilibrary.org/sites/23561431-en/1/2/1/index.html?itemId=/content/publication/23561431-en&_csp_=79ea8e97684c395730e471f402ce000e&itemIGO=oecd&itemContentType=book; Phora *Developing a Legal Framework for E-Commerce in South Africa* 23.

86 OECD 2019 https://www.oecd-ilibrary.org/sites/23561431-en/1/2/1/index.html?itemId=/content/publication/23561431-en&_csp_=79ea8e97684c395730e471f402ce000e&itemIGO=oecd&itemContentType=book; Phora *Developing a Legal Framework for E-Commerce in South Africa* 23.

The OECD expanded on the previous definitions in 2009 (and also updated in 2011)[87] by shifting the focus from the role-players or characteristics of the product to the ordering method and means used to achieve the purchase or sale.[88] This new definition was expanded to read as follows:

> An e-commerce transaction is the sale or purchase of goods and services, conducted over computer networks by methods specifically designed for the purpose of receiving or placing of orders. The goods or services are ordered by those methods, but the payment and the ultimate delivery of the goods or services do not have to be conducted online. An e-commerce transaction can be between enterprises, households, individuals, governments and other public or private organisations. To be included are orders made over the web, extranet or electronic data interchange. The types are defined by the method of placing the order. To be excluded are orders made by telephone calls, facsimile or mutually typed email.

This definition removes all uncertainty and prescribes exactly the requirements to label a transaction under e-commerce. The definition focuses on whether goods and services are bought or sold over computer networks, such as the internet, which were specifically designed with the intention to facilitate the online purchasing and selling of goods or services. The role-players, payment method and delivery are irrelevant when determining whether a transaction qualifies as an e-commerce transaction. Further boundaries placed are on methods that exclude the use of computer networks such as telephone calls or even mutual email correspondence (therefore excluding bilateral agreements). This indicates that the electronic computer network in itself should exist to act as a marketplace for the trade of goods and services before an e-commerce transaction can be said to have taken place.

Therefore, the term e-commerce is used to classify any form of transaction that originates from the internet or other computer networks as an intermediary between buyer and seller. The marketplace itself exists in cyberspace and acts as the link

---

87 OECD 2019 https://www.oecd-ilibrary.org/sites/23561431-en/1/2/1/index.html?itemId=/content/publication/23561431-en&_csp_=79ea8e97684c395730e471f402ce000e&itemIGO=oecd&itemContentType=book

88 OECD 2019 https://www.oecd-ilibrary.org/sites/23561431-en/1/2/1/index.html?itemId=/content/publication/23561431-en&_csp_=79ea8e97684c395730e471f402ce000e&itemIGO=oecd&itemContentType=book.

between buyer and seller. The eventual logistics of payment, delivery, etcetera is irrelevant; it is only the origin of the transaction, i.e., the marketplace that must be examined. E-commerce is, therefore, said to have taken place when an online marketplace is used as facilitator between buyer and seller.

2.2.2 Benefits of Electronic Commerce

The nature of e-commerce, allows for ease of access and convenience in lieu of traditional market restrictions for traders and consumers. The worldwide reach of the internet empowers a merchant to enter into a global marketplace at a relatively low cost of entry.[89] E-commerce empowers traders to enter into a marketplace with full international reach with fewer barriers to entry than would be required for brick-and-mortar stores. This is because the internet is established as a global network of electronic devices.[90] Therefore all consumers with an internet connection, for the most part irrespective of geographical location,[91] can access the merchant's cyberstore. Further, for traders, setting up a web page acting as an electronic marketplace or cyberstore is a great deal less restrictive in terms of legislation and cost than it would be to open a physical store. Regarding consumers, geographical location and proximity to a specific physical store become irrelevant, as the internet facilitates a global meeting place between traders and consumers.

E-commerce is not confined to traditional working hours. Both Stander and Phora specifically mention the full-time accessibility and convenience of e-commerce platforms as major benefits to traders and consumers.[92] These virtual marketplaces do not adhere to the traditional nine-to-five business hours. Cyberstores are accessible

---

89 Stander *Investigating the use of e-commerce to empower South African women* 26.

90 Stander *Investigating the use of e-commerce to empower South African women* 26.

91 Although region-blocking is used in practice to limit access to certain web-locations, the internet, as a concept, acts as an international facilitator between different parties. The internet transcends traditional geographic boundaries and allows users to connect to one another irrespective of distance.

92 Stander *Investigating the use of e-commerce to empower South African women* 27; Phora *Developing a Legal Framework for E-Commerce in South Africa* 27.

around the clock, and consumers are free to purchase goods and services conveniently. Likewise, merchants are empowered to conclude their end of the transaction at a time best suited to them. Further, given the borderless nature of these transactions, the traditional business hours would not be workable as e-commerce transactions transcend hemispheres and time zones.

E-commerce transactions have the potential to take place instantly.[93] This, *inter alia,* specifically relates to incorporeal and digital property transactions. Users are empowered to digitally download or gain access to digital goods and services, for instance, musical albums, films, video games and the like, at the click of a button. Some platforms even allow for automatic access once payment is processed, therefore eliminating the need for the trader to physically grant access to the consumer from their end. This also links to the benefit of timesaving as the need to physically collect goods from a traditional marketplace is dispensed with.[94] According to Stander, the instantaneous processing of transactions adds to merchants' effectiveness and economic output.[95] This natural result also promotes consumer confidence and increases their willingness to engage in further commercial transactions.

Therefore, e-commerce empowers both consumers and traders to access a marketplace for goods and services, irrespective of their physical location or the time of day. The internet links consumers and traders to an international marketplace. It is convenient, instant and easily accessible. It promotes the effectiveness of business whilst simultaneously growing consumer confidence. Likewise, consumers are catered to in terms of productivity and convenience, and as such, their willingness to engage in e-commerce transactions will grow. The effect of it all is that from a macro-economic standpoint, economic growth is continually stimulated as the more businesses grow,

93 Phora *Developing a Legal Framework for E-Commerce in South Africa* 28.
94 Phora *Developing a Legal Framework for E-Commerce in South Africa* 28.
95 Stander *Investigating the use of e-commerce to empower South African women* 28.

the more people are employed and the more spending power consumers have to put back into other businesses.

2.2.3 Challenges of Electronic Commerce

From the above it can be concluded that e-commerce is a welcome concept for all parties involved and should be promoted and pursued. However, it is not without issue. A brief note on certain challenges that users of e-commerce may face in practice will follow.

Traders also face other challenges in obtaining entry into the market. Even though, as shown above, it may be easy to establish a meeting point between consumer and trader, the establishment of an actual distribution network remains a real-world challenge that is not bypassed by e-commerce, especially as it relates to the supply and delivery of corporeal goods and services.[96] The e-commerce platform, i.e., the webpage of the trader, functions as a storefront for would-be consumers. The establishment of a webpage is the easy step. However, the actual establishment of a business and its supply channels still have the same barriers, risks and difficulties as before.

Furthermore, some residents of developing nations and rural areas are excluded from e-commerce due to their socio-economic status.[97] Many economic marginalised groups find difficulty in gaining entry into e-commerce as the cost of internet-connected devices and internet connectivity is exceedingly high.[98] Beyond the cost of internet connectivity, many areas, especially rural areas, do not have the infrastructure to even provide internet activity, meaning these groups of people cannot directly benefit from e-commerce and are essentially left in the dark.

---

96 Stander *Investigating the use of e-commerce to empower South African women* 37.
97 Stander *Investigating the use of e-commerce to empower South African women* 29.
98 Stander *Investigating the use of e-commerce to empower South African women* 3.

Moreover, if not properly regulated, e-commerce transactions can have serious consequences for an unwitting party.[99] This work seeks to examine more damaging dangers that may attach to e-commerce. Stander explains that e-commerce can be perceived as a breeding ground for fraudulent online activities.[100] Most of the fraudulent activities faced by e-commerce platform users fall within the ambit of cybercrime.[101] These concepts are referred to in the following section and will be discussed at length.[102] Furthermore, these concepts will be considered in light of cryptocurrency regulation.[103]

2.3 What is cybercrime?

2.3.1 The Concept: Cybercrime

2.3.1.1 Introduction

As seen in the preceding section, electronic commerce has completely changed the commercial landscape relating to the trade of goods and services. This is accomplished by, at its basis, providing for a more efficient, streamlined and mutually beneficial meeting place between buyer and seller.[104] However, the rise in computers and computer networks for commercial activities has also brought about certain undesirable practices. As the use of computers and computer networks for commercial activity has grown, so has the rise in the use of these interconnected devices with the intention to deceive and defraud.[105] According to Kouamo, certain "age old scams" have also crept into the realm of e-commerce, along with new forms of crimes perpetrated by way of the internet or computer networks.[106] Criminal transgressions

99 Phora *Developing a Legal Framework for E-Commerce in South Africa* 28.
100 Stander *Investigating the use of e-commerce to empower South African women* 36.
101 Albert 2002 *ABLJ* 578-579.
102 See chapter 2.3 of this work.
103 See chapter 3 of this work.
104 Kouamo *Combating Crime in International Electronic Commerce* 2.
105 Kouamo *Combating Crime in International Electronic Commerce* 2.
106 Kouamo *Combating Crime in International Electronic Commerce* 2.

committed by way of a computer is known as cybercrime.[107] The term cybersecurity refers to risk mitigating measures aimed at preventing unauthorised access, use, damage or alterations to interconnected networks or communication systems.[108] Thus, cybersecurity methods are aimed at the prevention of cybercrime.

Cybercrime can have far-reaching implications for the e-commerce sector, and therefore, vigorous legal regulation would be required. However, what should be understood under the definition of cybercrime? Prior to the proclamation of the *Cybercrimes Act*, the relevant legislation in South Africa in relation to cybersecurity was the *Electronic Communications and Transactions Act* 25 of 2002; the *Financial Intelligence Centre Act* 38 of 2001; as well as the *Regulation of Interception of Communications and Provision of Communication-related Information Act* 70 of 2002.[109] In order to have a deeper understanding of the notion of cybercrime, it is necessary to take a look at the many legal definitions thereof.

2.3.1.3 Definitions by Writers

During his early work, Van der Merwe defined cybercrime as:

> Computer crime covers all sets of circumstances where electronic data processing forms the means for the commission and/or object of the offence or represents the basis for the suspicion that an offence has been committed.[110]

Van der Merwe has admitted that his definition may be interpreted too widely. He cites the usage of the phrase "data processing as underlying basis for suspecting that an offence has been committed".[111] Apart from the last-mentioned criticism, the definition is outdated as Van der Merwe's work was published more than twenty years ago.

---

107 Mpuru 2017 *Servamus Community-based Safety and Security Magazine* 44.
108 Mpuru 2017 *Servamus Community-based Safety and Security Magazine* 44.
109 Schultz 2016 *Cybercrime: An Analysis of Current Legislation in South Africa* 9.
110 Van der Merwe 2007 *THRHR* 310.
111 Van der Merwe 2007 *THRHR* 310.

Van der Merwe's later work gives effect to Casey's differentiation between, on the one hand, the commission of crimes involving computers, but not heavily relying thereupon and on the other, a special kind of cybercrime in which Casey draws distinct elements in his explanation of cybercrime.[112] The elements are formed from prominent foreign statutes.[113] Casey draws attention to four elements to note during the commission of cybercrime. Firstly, a computer as the target of the crime. Secondly, a computer used as the means to commit the crime. Thirdly, the computer being supplementary to the crime. Lastly, crimes which are linked to the demand for computers.[114]

Cassim builds upon the elements from Casey to reach his definition.[115] Cassim describes cybercrime as any form of transgression of criminal law perpetrated using the internet or a computer, by which the computer may be an object or the subject of the crime.[116]

2.3.1.3 Statutory Definition

In the section above the definitions of cybercrime by various academic writers are discussed. These definitions give clarity on the concept and the elements found therein. However, it is also necessary to examine any potential statutory definitions in order to establish how these academic definitions are applied in practice. In this way, complete clarity can be obtained on the concept of cybercrime.

The prominent international law treaty aimed at regulating cybercrime is the *Council of Europe Convention on Cybercrime* of 2001, commonly referred to as the *Budapest Convention* (hereafter referred to as the "*Budapest Convention*").[117] However, no express definition for cybercrime is given. Article 1 only goes so far as to define

112 Van der Merwe 2007 *THRHR* 310.
113 Statutes such as the *Computer Fraud and Abuse Act* (US) and the *Computer Abuse Act* (UK). Van der Merwe 2007 *THRHR* 310.
114 Schultz 2016 *Cybercrime: An Analysis of Current Legislation in South Africa* 7.
115 Schultz 2016 *Cybercrime: An Analysis of Current Legislation in South Africa* 7.
116 Cassim 2009 *PER/PELJ* 36.
117 Kempen 2019 *Servamus* 27.

"computer system" and "computer data" respectively.[118] Schultz notes this as problematic, as the treaty's aim is to combat cybercrime. However, it omits to define the concept.[119]

However, even before the implementation of the *Budapest Convention*, South African jurists had started tabling discussions of the concept of cybercrime. Van der Merwe mentions the need for redress of the criminal law by the South African Law Commission.[120] The SALC issued a report on cybercrime in 1998, highlighting key factors of computer-related criminal activities.[121] It compared unauthorised access (as later defined by section 85 of ECTA) to common-law housebreaking. It also deemed the unauthorised altering of data and software as equivalent to malicious injury to property.[122] The report by the SALC led to discussions surrounding the protection of users from cybercriminals, which eventually led to the implementation of ECTA.[123]

ECTA does not expressly define cybercrime but refers to "access" in Chapter 8, section 85. It states:

> In this Chapter, unless the context indicates otherwise-
>
> 'access' includes the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data.[124]

The rest of the chapter goes on to mention specific instances in which access as defined above is prohibited, such as, *inter alia,* the unauthorised access, interception

---

118 A 1 of the *Council of Europe Convention on Cybercrime* (2001); Schultz 2016 *Cybercrime: An Analysis of Current Legislation in South Africa* 9.

119 Schultz 2016 *Cybercrime: An Analysis of Current Legislation in South Africa* 9.

120 Van der Merwe 2007 *THRHR* 312.

121 The South African Law Commission published a paper titled *Computer-Related Crime: Preliminary Proposals for Reform in Respect of Unauthorised Access to Computers, Unauthorised Modification of Computer Data and Software Applications and Related Procedural Aspects* (SALC Project 108) (1998).

122 Van der Merwe 2007 *THRHR* 312.

123 Van der Merwe 2007 *THRHR* 312.

124 Section 85 of the *Electronic Communications and Transactions Act* 25 of 2002

or interference with data;[125] computer-related fraud[126] as well as provisions dealing with attempt, aiding and abetting;[127] and its related penalties.[128] Section 86 is of particular note as it places access, as defined in section 85, in context and thereby sets the parameters of cybercrime within the Act. Section 86 states:

> Unauthorised access to, interception of or interference with data
>
> (1) Subject to the Interception and Monitoring Prohibition Act, 1992 (Act 127 of 1992), a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence.
>
> (2) A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence.
>
> (3) A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence.
>
> (4) A person who utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence.
>
> (5) A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users, is guilty of an offence.[129]

Sections 87-89 read with section 86 of ECTA go on to deliver further provisions relating to cybercrime based on the prohibited actions listed above in section 86. Van der Merwe notes that upon closer inspection, data is the real legal interest which should be safeguarded by this chapter of ECTA.[130]

---

125 Section 86 of the *Electronic Communications and Transactions Act* 25 of 2002.
126 Section 87 of the *Electronic Communications and Transactions Act* 25 of 2002.
127 Section 88 of the *Electronic Communications and Transactions Act* 25 of 2002.
128 Section 89 of the *Electronic Communications and Transactions Act* 25 of 2002.
129 Section 86 of the *Electronic Communications and Transactions Act* 25 of 2002.
130 Van der Merwe 2007 *THRHR* 313.

Almost 18 years after the definition in ECTA, Chapter 2 of the newly promulgated *Cybercrimes Act* (hereafter "the Act") deals with cybercrimes and related offences.[131] The Act follows close suit to ECTA in that it focuses on unlawful access, unlawful alteration and unlawful interception of, *inter alia,* data. In terms of the Act, Section 1 defines data as any form of electronic representation of information.[132] Although the Act does not expressly define cybercrime, it does mention specific actions (or omissions) which would be deemed an offence, and therefore constitute such action as being classified as a cybercrime. It follows closely to the above sections of ECTA and criminalises unlawful access, unlawful alteration and unlawful interception of data.[133]

Therefore, it could be said that cybercrime is any criminal transgression involving the use of a computer, computer networks or any other device/instrument in an attempt to modify, intercept or gain unauthorised access to data; be it on another computer or not. To further place the concept within the context of this work, the object of the unlawful access and/or modification and/or interception would be any user, company, governmental organisation, bank, network, data file or other object used in any way, either directly, indirectly or in conjunction with cryptocurrency.

2.3.2 Cybercrime's Remoteness from Traditional Crime

Throughout history, the common-law principles relating to criminal law have developed with a focus on regulating crimes committed on a physical basis.[134] This means that what is traditionally thought of as criminal law, has a distinct focus on crimes that take place in a physical sense, for example murder or theft, whereas crimes such as cybercrime take up virtual space. However, the effects of such crime (crimes committed in a virtual space) can have real-world implications. Schultz emphasises

131 Chapter 2 of the *Cybercrimes Act* 19 of 2020.
132 Section 1 of the *Cybercrimes Act* 19 of 2020.
133 Sections 2-6 of the *Cybercrimes Act* 19 of 2020. See chapter 5.2 of this work for a further discussion on the Act.
134 Schultz 2016 *Cybercrime: An Analysis of Current Legislation in South Africa* 12.

that laws enforced with the object of regulating a physical medium, have great difficulty being applied to an electronic medium.[135] Another aspect to consider is that cybercrime cannot be confined to a specific geographical jurisdiction or border.[136] This makes prosecution under traditional physical criminal law practically unworkable.

With technology becoming ever more advanced, the gap between traditional physical crime and cybercrime is growing ever larger. Brenner and Clarke highlight four key foundations which are inherent to traditional crime, but which cybercrime lacks. These are proximity; scale; physical limitations and patterns.[137] A comparison of these foundational principles concerning cybercrime, creates the necessary juxtaposition to portray the substantial gap between physical crime and cybercrime.

2.3.2.1 The Elements of Traditional Crime in Relation to Cybercrime

The first foundation of proximity highlights the fact that there is an inherent proximate link between victim and perpetrator in a traditional crime.[138] For context, an example would be: for a murder to take place, the murderer has to be physically approximate to the victim. It would not be possible for the murder to take place if the murderer is on the opposite end of the earth to the victim. They have to be sufficiently close to each other in distance. In contrast, cybercrime is not limited by distance between perpetrator and victim.[139] It is possible and indeed observed that perpetrators of cybercrime and their victims are entire continents apart.

The second foundation of scale is closely linked to the element of proximity above. Scale speaks of the size of the crime. Constraints of physical reality limit a specific traditional crime to victimise one person or groups of persons at one specific time. For instance, a murderer can only commit an attack on one person or group at a time.

---

135 Schultz 2016 *Cybercrime: An Analysis of Current Legislation in South Africa* 12.
136 Schultz 2016 *Cybercrime: An Analysis of Current Legislation in South Africa* 13.
137 Brenner and Clarke 2005 *JCIL* 663; Papadopoulos and Snail ka Mtuze *Cyberlaw* 466.
138 Brenner and Clarke 2005 *JCIL* 663.
139 Kempen 2019 *Servamus* 27.

Brenner and Clarke explain traditional crime as being serial[140] in nature.[141] However, the same cybercriminal can target an unlimited amount of people at once, and the victimisation even has the potential to be automated.[142] This means that limitations of time and space do not apply to cybercrime, and that one cyber-attack can have concurrent consequences on different people in different parts of the world.

The foundation of physical constraints builds upon the former two elements above. Brenner and Clarke explain that even the simplest of crimes require some sort of preparation from the potential perpetrator.[143] The preparation for instance involves the planning of the crime, acquiring the necessary information or tools and the implementation thereof.[144] This could be seen to be true for cybercrime as well. However, the implementation in cybercrime is much less directly involved. The example of a murder can be used once again. A murderer needs to take the time to plan his or her actions, among others, getting to know the routines of the would-be victim and any security hindrances. After the planning phase, he or she, would need to acquire the necessary tools to complete the crime. After that an extraction plan to hide evidence, etcetera, would also be necessary. In contrast, cybercrime only requires a knowledgeable person in front of a computer. It may even be automated. Furthermore, along with the proximity foundation, the restrictions on planning and evasion of the police are a lot simpler than the preparation of a physical crime. This is since with a few clicks of a computer mouse, the crime can be committed and no physical encounter or evidence is ever left behind.

---

140 Real world crime takes place one after the other. One perpetrator can only commit one offence at a specific time and place, before moving on to another, whereas online crimes committed by one perpetrator can run simultaneously. Brenner and Clarke 2005 *JCIL* 663.

141 Brenner and Clarke 2005 *JCIL* 663.

142 Papadopoulos and Snail ka Mtuze *Cyberlaw* 467.

143 Brenner and Clarke 2005 *JCIL* 664.

144 Brenner and Clarke 2005 *JCIL* 664.

Lastly, Brenner and Clarke note that real-world crime falls into patterns.[145] This element describes that when a physical crime takes place, a certain predetermined pattern will always follow.[146] This means that the same premise will always lead to the same conclusion. What this means is that the same crime will always have the same outcome in its effect on society. It also presupposes that crime is mainly concentrated and limited to demarcated and geographical areas. This facilitates law enforcement to focus on concentrated areas and direct crime prevention resources to such areas.[147]

2.3.2.2 Enforcement of Traditional Criminal Law on Cybercrime

Albert notes that, due to the mechanics of internet crime and the relative ease with which information and evidence can be hidden or tampered with, cybercrime is prosecuted differently from traditional crime.[148] Brenner and Clarke add to this by stating that cybercrime is not confined to the characteristics of traditional crime, upon which the model of criminal law enforcement is based.[149] They state that the already limited resources that law enforcement has at its disposal to combat traditional crime, is woefully inadequate to deal with the scourge of cybercrime.[150] This is because from its basic structure, cybercrime differs from traditional crime. It, therefore, cannot be confined to the traditional criminal law enforcement system, because it has to be dealt with in a completely different way from traditional crime.

Apart from the characteristics that differ, other logistical matters also need to be considered. For instance, what may be considered a criminal transgression in one country could be completely lawful in another.[151] Other matters[152] such as the high

145 Brenner and Clarke 2005 *JCIL* 664.
146 Brenner and Clarke 2005 *JCIL* 664.
147 Brenner and Clarke 2005 *JCIL* 664.
148 Albert 2002 *ABLJ* 592.
149 Brenner and Clarke 2005 *JCIL* 666.
150 Brenner and Clarke 2005 *JCIL* 666.
151 Kouamo *Combating Crime in International Electronic Commerce* 10.
152 Kouamo *Combating Crime in International Electronic Commerce* 10; Brenner and Clarke 2005 *JCIL* 667.

cost of prosecution, frequency of cybercrime, anonymity, jurisdiction and locale further contribute to the difficulty in combating cybercrime and further emphasise that cybercrime cannot fit the mould of the traditional criminal law enforcement system.

2.3.3 Conclusion

From the above, it can be seen that legal writers have attempted to define the concept of cybercrime meticulously. In most cases, the definitions by the various jurists do somewhat reconcile with one another. These definitions boil down to the following: cybercrime is a criminal law offence perpetrated by means of a computer, with the object of the crime being another computer, a network, data or any other digital or other device.

The newly proclaimed *Cybercrimes Act* 19 of 2020 attempts to solidify and update the position on cybercrime in South Africa. According to the Act, the position on cybercrime comes down to the unlawful access, interception or alteration of data. This means that no matter how the offence is commissioned, the offence itself will always fall within the ambit of either unlawful access, unlawful interception or unlawful interference.

2.4 Types of Cybercrime

Now that light has been shed on the concept of cybercrime itself, as well as its difference from traditional crime, it is necessary to highlight actions that constitute cybercrime. In order to do so, certain forms and types of cybercrime will now be discussed so that insight can be provided into what type of actions constitute cybercrime. Also, note that even though every attempt is made to give insight as thoroughly as possible into the types of transgressions that fall under the umbrella of cybercrime, this is by no means a *numerus clauses* on every action that constitutes cybercrime.

2.4.1 Identity Theft

Identity theft takes place when someone intentionally or otherwise attempts to gain access to someone else's bank accounts or personal details and uses it for personal gain at the expense of the affected party. This is usually accomplished in instances where the transgressor fraudulently passes off that he is the affected party in order to enter into unauthorised transactions or purchases.[153] In the e-commerce space, it can take place where the identity of an innocent party is used to make authorised purchases or enter into malicious transactions. This is also known as financial identity theft and refers to actions whereby someone uses another person's personal information or identity to obtain credit, enter into contracts for purchase and sale, or gain unsolicited benefits.[154]

Section 1 of the *Protection of Personal Information Act* ("POPIA") defines personal information as:

> "personal information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—
>
> (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
>
> (b) information relating to the education or the medical, financial, criminal or employment history of the person;
>
> (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
>
> (d) the biometric information of the person;
>
> (e) the personal opinions, views or preferences of the person;

153 Mpuru 2017 *Servamus Community-based Safety and Security Magazine* 44.
154 Kagan 2021 https://www.investopedia.com/terms/i/identitytheft.asp.

(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the person; and

(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.[155]

According to Mpuru, identity theft is one of the most prevalent forms of cybercrime in South Africa.[156] The rise in its prevalence is akin to the ever-increasing accessibility to the internet and high levels of corruption coupled with the difficulty of successful prosecution.[157]

2.4.2 Phishing

Closely linked to identity theft above, phishing is the process by which internet users' personal data or information is solicited in the form of falsely represented emails.[158] These emails usually take the form of appearing to be from a reputable source such as the user's bank, e-commerce platform or workplace.[159] These emails are usually unsolicited and contain links to falsified versions of legitimate websites of which the user is a patron. It will then attempt to have the user submit personal information such as passwords or credit card details. The user then effectively gives away his or her personal information to the cybercriminal. This is a way in which identity theft may be committed.[160] The term "phishing" derives from the fact that the cybercriminal is fishing for details by sending out high numbers of such emails to different users in an attempt to "hook" an internet user into unwittingly giving away his or her personal information.

---

155 Section 1 of the *Protection of Personal Information Act* 4 of 2013.
156 Mpuru 2017 *Servamus Community-based Safety and Security Magazine* 44.
157 Mpuru 2017 *Servamus Community-based Safety and Security Magazine* 44.
158 Kouamo *Combating Crime in International Electronic Commerce* 15.
159 Van der Merwe 2007 *THRHR* 316.
160 Van der Merwe 2007 *THRHR* 317.

2.4.3 Pharming

Pharming is closely linked to phishing, as the word suggests. It is sometimes referred to as the act of phishing without using a "lure".[161] Pharming occurs when malicious software is installed onto computers, devices or computer networks. The software then redirects users to falsified versions of legitimate websites including, *inter alia,* e-commerce platforms or banks. This is where users are then, similar to the above, tricked into unwittingly giving away personal information.[162]

2.4.4 Money Laundering

Money laundering plays a significant role in both cybercrime and the misuse of cryptocurrencies and will therefore be an important subject of discussion throughout this work.[163] However, it is necessary to provide a brief definition of the concept at this stage. Section 4 of the *Prevention of Organised Crimes Act* describes money laundering as:

> Money laundering - Any person who knows or ought reasonably to have known that property is or forms part of the proceeds of unlawful activities and— (a) enters into any agreement or engages in any arrangement or transaction with anyone in connection with that property, whether such agreement, arrangement or transaction is legally enforceable or not; or (b) performs any other act in connection with such property, whether it is performed independently or in concert with any other person, which has or is likely to have the effect—
>
> (i) of concealing or disguising the nature, source, location, disposition or movement of the said property or the ownership thereof, or any interest which anyone may have in respect thereof;
>
> (ii) of enabling or assisting any person who has committed or commits an offence, whether in the Republic or elsewhere— (aa) to avoid prosecution; or (bb) to remove or diminish any property acquired directly, or indirectly, as a result of the commission of an offence, shall be guilty of an offence.[164]

---

161 Johansen 2019 https://us.norton.com/internetsecurity-online-scams-what-is-pharming.html.
162 Johansen 2019 https://us.norton.com/internetsecurity-online-scams-what-is-pharming.html.
163 See 3.4.1 of this work.
164 Section 4 of the *Prevention of Organised Crimes Act* 121 of 1998.

The essence of the provision states that money gained from illicit activities is put into other business sources to conceal the actual source from which it originated. Mpuru adds to this by outright stating that money laundering is often linked to organised crime syndicates and these syndicates employ a number of tactics to launder money.[165] Money laundering falls within the ambit of cybercrime as it is a supplementary form to many other forms of cybercrime. For instance, illicit gains from hacking, phishing, identity theft, etcetera can be laundered. Money laundering is prevalent in the e-commerce industry relating to cryptocurrency and will be discussed in greater detail under chapter 3 of this work.

2.4.5 Gate-crashing

Gate-crashing takes place when an online profile is cloned, unbeknownst to the profile's owner.[166] What follows is that the cybercriminals use the cloned profile to lock out the actual owner and, after that, attempt to solicit money from the actual owner's friends and family by posing as such a person. One such case took place in New Zealand where gate-crashers cloned the Facebook profile of a man and posed as him to his friends and family, and solicited banking information from them, reportedly accumulating fifty-five thousand New Zealand dollars.[167] This method employs a similar *modus operandi* to phishing, with the only notable difference being that instead of luring a target and hoping for a response such as in phishing, a more hands-on approach is followed by which a close friend or family member of the cyber victim's online profile is cloned, with the intention to defraud the target by posing as such friend or family member.

---

165 Mpuru 2017 *Servamus Community-based Safety and Security Magazine* 44.
166 Mpuru 2017 *Servamus Community-based Safety and Security Magazine* 44.
167 Smith 2021 https://www.stuff.co.nz/national/125622858/police-warn-of-fake-facebook-profile-scam-thats-cost-one-victim-55000.

2.4.6 Hacking

Hacking is the process by which unlawful access, interference or interception of data takes place by gaining entry thereto through intelligent network practices.[168] The term is sometimes used interchangeably with the term cracking.[169] To best illustrate hacking, it will be placed in a parallel traditional crime context. Hacking is similar to housebreaking in that it employs clever techniques to gain entry to a premise to which access is not allowed. What follows after, be it damage to property, theft or extortion, is a result of the housebreaking. The same can be said for hacking and the repercussions that follow as a result thereof.

2.4.7 Advance Fee Scams

Advance fee scams are mostly sent out in emails to unwitting victims. These emails contain fraudulent messages that the victim is the beneficiary of a large sum of money and merely needs to pay a small amount of money to have the large sum processed and sent to them.[170] Advance fee scams follow the same basic premise as phishing. The only difference is in the structure of the email. Instead of posing as a reputable site in order for victims to enter their personal information, advance fee scams operate on a social engineering basis by trying to persuade victims to pay over a small deposit in order to obtain a large amount of money. The result is that victims pay over their deposit, the scammer is never heard of again and there is no sum of money paid back over to the victim.

2.5 Prevalence of Cybercrime

As seen above, there are many forms of cybercrime. Many forms of cybercrime also interlink with one another, and one form may lead to another. For example, pharming, phishing or gate-crashing could be employed to commit identity theft. Mpuru avers

168 Mpuru 2017 *Servamus Community-based Safety and Security Magazine* 44.
169 Cybercrime.org.za 2021 https://cybercrime.org.za/hacking/.
170 Kouamo *Combating Crime in International Electronic Commerce* 16.

that identity theft is one of the most prevalent forms of cybercrime.[171] This would make sense, especially when viewed through the lens that most forms of cybercrime only exist as a tool to enable identity theft to take place. One notable exception to this fact is money laundering, since it follows a different *modus operandi* in it being a tool to hide illicit monetary and or other financial gains. However, this is not to say that money laundering tactics may not be employed to launder illicit gains from identity theft schemes. Therefore, most forms of cybercrime are used in conjunction with one another by cybercriminals to reach their final objective.

Given the nature of cybercrime, as seen above, countless actions involving electronic devices and the internet fall under the umbrella of cybercrime. South Africa has also, in recent times, experienced an influx of cybercrime. One notable instance being, Transnet in July 2021.[172] As mentioned above,[173] the cyber-attack targeted important shipping ports in South Africa, with massive delays in transport operations caused, creating havoc and causing further delays at already heavily backlogged shipping docks.[174] Another notable recent attack illustrated that not even the South African judiciary is safe from the destructive conduct of cybercriminals. In September 2021, the South African Department of Justice and Constitutional Development was hit by a cyber-attack, wiping out its central networks.[175] The department, which is the overseer of all courts in South Africa, suffered a brutal attack on its IT-systems, causing all court processes to come to an abrupt and prolonged halt. The attack was enabled by ransomware[176] on the department's central systems, meaning that maintenance claims, recording of court transcripts, issuing of letters of authority and all other

171 Mpuru 2017 *Servamus Community-based Safety and Security Magazine* 44.

172 Rall 2021 https://www.iol.co.za/news/south-africa/kwazulu-natal/transnet-cyber-attack-cripples-movement-of-goods-through-port-terminals-3ea4ec21-dab1-4650-922e-47bc0a401bee.

173 See chapter 1.3 above.

174 Rall 2021 https://www.iol.co.za/news/south-africa/kwazulu-natal/transnet-cyber-attack-cripples-movement-of-goods-through-port-terminals-3ea4ec21-dab1-4650-922e-47bc0a401bee.

175 Makhafola 2021 https://www.news24.com/news24/SouthAfrica/News/department-of-justice-says-its-recovering-from-cyber-hack-causing-court-case-delays-20211010.

176 Ransomware is a type of malicious software which blocks a user out of his or her own data files and demands a payment of ransom in return for access thereto. FBI 2022 https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware.

electronic court services were unavailable for over a month, creating further headaches for an already overstretched court system.[177] Not only does this have a practical and inconvenient impact on the public, but it also sends a disparaging message to the public. It illustrates that even the court system, the central enforcer of order and justice, is at the mercy of cybercriminals. It is still to be seen whether these perpetrators are to be held accountable, hopefully restoring public confidence in the South African court system. Hereafter, noteworthy South African case law relating to cybercrime will be discussed.

2.5.1 Fourie v Van der Spuy

The prevalence and rise of cybercrime in South Africa were referenced in an *obiter dictum* by Klein AJ. The judge confirmed that cybercrime was on the rise and its effects ever more prevalent in a judgment of the High Court in *Fourie v Van der Spuy and De Jongh Inc* (65609/2019) [2019] ZAGPPHC 449; 2020 (1) SA 560 (GP).[178]

In Casu, the Applicant, was a client of a law firm. The Respondents acted as attorneys for the Applicant on a previous occasion. The Respondents were instructed to hold their client's (the Respondent's) monies in their trust account for the case they were working on. The attorneys allegedly received numerous emails from an email account that seemed to be their client's. The emails claimed that the client's banking details had changed, and the emails gave new banking details to the attorney. The attorney later paid the trust money to the allegedly new bank account.[179] Only after the payment had been made, the attorney discovered that the Applicant's email account

---

177 Ngqakamba 2021 https://www.news24.com/news24/southafrica/news/justice-departments-it-system-brought-down-in-ransomware-attack-20210909.

178 *Fourie v Van der Spuy and De Jongh Inc* (65609/2019) [2019] ZAGPPHC 449; 2020 (1) SA 560 (GP) (30 August 2019).

179 Bhagattjee and Govuza 2020 https://www.cliffedekkerhofmeyr.com/en/news/publications/2020/technology/tmt-alert-18-february-cybercrime-in-south-africa-attorneys-fall-victim-to-cyber-fraud.html.

had been hacked and that cybercriminals purporting to be the Applicant, had duped the attorney into paying the money over to them.[180]

The legal question before the court was whether the attorney acted negligently in erring to employ sufficient safeguards in following up whether the emails were in fact from the client/Applicant.[181] Further, the court had to determine whether the monetary loss suffered should be carried by the client or by the attorney.

The court ruled in favour of the Applicant, and it was found that the Respondents be held jointly and severally liable for the loss suffered.[182] The court stated that the attorney acted negligently in her duties and therefore failed to act within the necessary levels of care, diligence and skill required of a practising attorney.[183] The court reiterated this sentiment by highlighting that the attorney should have known better, especially given that fraud is prevalent in such a profession.[184]

This case highlights that cybercrime is becoming ever more relevant in South Africa. It furthermore shows that anyone can be a target of cybercrime, and even a law firm can fall victim to the schemes of cybercriminals. Bhagattjee and Govuza note that had the *Cybercrimes Act* been operational at the time of the incident, section 2 thereof, which deals with unlawful access, would have been applicable and therefore, could have led to an investigation by the SAPS to possibly lead to a conviction (in line with the provisions of Section 276 of the *Criminal Procedure Act* 51 of 1977).[185]

---

180 *Fourie v Van der Spuy and De Jongh Inc* (65609/2019) [2019] ZAGPPHC 449; 2020 (1) SA 560 (GP) (30 August 2019) para 24.

181 *Fourie v Van der Spuy and De Jongh Inc* (65609/2019) [2019] ZAGPPHC 449; 2020 (1) SA 560 (GP) (30 August 2019) para 12.

182 *Fourie v Van der Spuy and De Jongh Inc* (65609/2019) [2019] ZAGPPHC 449; 2020 (1) SA 560 (GP) (30 August 2019) order.

183 *Fourie v Van der Spuy and De Jongh Inc* (65609/2019) [2019] ZAGPPHC 449; 2020 (1) SA 560 (GP) (30 August 2019) para 30.

184 *Fourie v Van der Spuy and De Jongh Inc* (65609/2019) [2019] ZAGPPHC 449; 2020 (1) SA 560 (GP) (30 August 2019) para 30.

185 Bhagattjee and Govuza 2020 https://www.cliffedekkerhofmeyr.com/en/news/publications/2020/technology/tmt-alert-18-february-cybercrime-in-south-africa-attorneys-fall-victim-to-cyber-fraud.html.

What is further noteworthy in this case was that the legal system had held the attorneys liable for the loss (which could be argued was fair, given the degree of diligence required when working with trust accounts). However, the cybercriminals themselves got away with the money.[186] Bhagattjee and Govuza also refer to this case as an important showcase for the enactment of the *Cybercrimes Act* (then known as the *Cybercrimes Bill*) and iterates that the Act will go a long way in helping SAPS and the NPA in bringing cybercriminals to justice.[187] A further discussion on the effectiveness of the Act in its aims will be contained in chapter 5 of this work.

2.5.2 Carolissen v DPP

Carolissen v Director of Public Prosecutions[188] is a noteworthy case relating to the extraterritoriality of cybercrime offences, which was heard in the Western Cape High Court. This case shows the global scale upon which a singular cybercrime offence may play out. Briefly, the facts of the case are as follows: An offence of the manufacturing and dissemination of child pornography was committed in South Africa. A video depicting the molesting of a minor child by a man in his forties was manufactured in South Africa and distributed on the internet. The video was eventually disseminated to officials of the Department of Homeland Security in the US. The US sought the extradition of the creator to stand trial before a US court.[189] A Magistrates' Court in South Africa authorised the extradition. The Appellant took the authorisation of his extradition on appeal in the High Court.[190]

The court held that the US does have sufficient jurisdiction to hear the matter before its relevant courts. This is because US legislatures have criminalised the manufacture

---

186 Bhagattjee and Govuza 2020 https://www.cliffedekkerhofmeyr.com/en/news/publications/2020/technology/tmt-alert-18-february-cybercrime-in-south-africa-attorneys-fall-victim-to-cyber-fraud.html.

187 Bhagattjee and Govuza 2020 https://www.cliffedekkerhofmeyr.com/en/news/publications/2020/technology/tmt-alert-18-february-cybercrime-in-south-africa-attorneys-fall-victim-to-cyber-fraud.html.

188 *Carolissen v Director of Public Prosecutions* 2016 (2) SACR 171 (WCC).

189 *Carolissen v Director of Public Prosecutions* 2016 (2) SACR 171 (WCC) para 2.

190 *Carolissen v Director of Public Prosecutions* 2016 (2) SACR 171 (WCC) para 3.

of child pornography and the dissemination and distribution thereof in their territory. Therefore, dissemination and distribution are also regarded as criminal offences. The court held that it was within the US legislature's prerogative to criminalise such actions and provided they had shown sufficient connection to their territorial jurisdiction that extradition was to be valid.[191] A grand jury in a court of the state of Maine found that the Appellant was indictable under American law.[192] The Western Cape High Court ruled that this was a satisfactory ground to show sufficient connection and therefore warrant extradition.[193]

This court, in this case, not only assessed the American position on the manufacture and distribution of child pornography, but it also assessed the South African legal position in such (cyber) offences. The court established that section 20 of the *Criminal Law (Sexual Offences and Related Matters) Amendment Act* 32 of 2007 (hereafter "SORMA") applies to instances of child pornography. [194] Furthermore, the provisions of the *Film and Publications Act* would also apply.[195] In line with this, the extradition treaty between the US and South Africa requires an offence to be punishable to the extent of more than or at least one-year imprisonment. Since neither SORMA nor the *Film and Publications Act* provided applicable penal provisions, the focus was shifted to section 276 of the *Criminal Procedure Act* 51 of 1977.[196] The court then found in respect of the offences at hand, as read with the provisions of Act 51 of 1977, the manufacture and dissemination of child pornography can be punishable to a maximum of life imprisonment.[197]

This case highlights the attitude of the courts regarding the scourge of cyber offences. It shows that states are willing to work together in attempting to stop the influx of

---

191 *Carolissen v Director of Public Prosecutions* 2016 (2) SACR 171 (WCC) paras 36-50.
192 *Carolissen v Director of Public Prosecutions* 2016 (2) SACR 171 (WCC) paras 16-24.
193 *Carolissen v Director of Public Prosecutions* 2016 (2) SACR 171 (WCC) para 50.
194 *Criminal Law (Sexual Offences and Related Matters) Amendment* Act 32 of 2007.
195 *Films and Publications Act* 65 of 1996.
196 Section 276 of the *Criminal Procedure Act* 51 of 1977. This section deals with the nature of punishments after an offence has been committed.
197 *Carolissen v Director of Public Prosecutions* 2016 (2) SACR 171 (WCC) para 65.

cybercrime. It also acts as an important showpiece for further prosecution that states would have to work together to prosecute cybercrime offences as the internet's lack of territoriality and physical boundaries have created a certain legal "no-man's-land". This case sets an important precedent for the territoriality aspect of the enforcement of cybersecurity rules. Section 6(1) of SORMA expressly excludes the extraterritoriality of the Act. However, the South African legislatures would be well advised to follow the American route to have dissemination be a punishable offence, no matter the origin. This would lead to an increase in prosecutions and act as further deterrence of such offences. This is especially important in relation to offences such as those present in the abovementioned case as it deals with vulnerable groups, i.e., minor children, and whose interests should be as far as reasonably practicable be protected. The fact that section 276 of the *Criminal Procedure Act* regards manufacture and/or dissemination of child pornography as an offence punishable up to life imprisonment highlights the seriousness of such an offence. All role players in the commission of the crime, from the person performing the improper acts with the minor, to the person filming, to the person uploading, should be held criminally liable for their actions.

The noteworthy aspect of the *Cybercrimes Act*, is that section 19 thereof expressly deals with sentencing.[198] However, section 19(4) does not restrict punishment to the confines of the Act itself and allows courts to turn yet again to section 276 of the Criminal Procedure Act if so required.[199] This is an illustration of the legislature's willingness to employ a comprehensive legal framework to regulate the prevalence of cybercrime.

2.5.3 Underreporting

As seen from the above, cybercrime and cyber-attacks are on the rise in South Africa, with even the courts experiencing the influx thereof both in its reported case law and

198 Section 19 of the *Cybercrimes Act* 19 of 2020.
199 Section 276 of the *Criminal Procedure Act* 51 of 1977 as read with s19(4) of the *Cybercrimes Act* 19 of 2020.

through first-hand attacks. However, Hubbard is of the opinion that these attacks are merely the tip of the iceberg, with countless incidents going unreported.[200] According to Hubbard, lack of confidence in local authorities is one of the main reasons many cyber-attacks go unreported.[201] The structure of the South African legal framework will be further discussed in subsequent chapters of this work.[202] Given the difficulty to enforce the rules of traditional criminal law on cybercrime, it is perhaps understandable that victims are reluctant to pursue traditional criminal law enforcement in these situations.

2.6 Conclusion

Electronic commerce has opened many new doors for consumers and traders alike. It has brought about many new avenues and platforms to enhance business transactions. It has also nullified the need for a buyer and a seller to even be in the same country, let alone the same room. However, the rise of computers and computer networks for e-commerce, has also brought about certain unwanted and undesirable practices. The rise of the internet as a platform for trade and commerce has also brought with it an influx in issues of cybercrime and cybersecurity. Cybercrime is an umbrella term coined to include many offences in which a computer or computer network is used to defraud or deceive unwitting victims. Cybersecurity methods aim to circumvent cybercrime offences from taking place.

Many writers have attempted to define the concept of cybercrime thoroughly. To a certain extent, most of the definitions overlap with one another, with minor inclusions or exclusions of certain qualifiers. However, the crux of the definitions come down to the following: a criminal law offence perpetrated by means of a computer, with the object of the crime being another computer, a network, data or any other digital or other device.

---

200 Hubbard *Finweek* 37.
201 Hubbard *Finweek* 37.
202 See chapter 5 of this work.

The newly proclaimed *Cybercrimes Act* 19 of 2020 attempts to reconciliate and update the position on cybercrime in South Africa. According to the Act, the position on cybercrime boils down to the following: notwithstanding the various forms of cybercrime, a cyber-offence takes place when data is accessed, intercepted or interfered with in any way, shape or form without the requisite authorisation from the person lawfully entitled to either access, intercept or alter such data. This means that no matter how the offence is commissioned, the offence itself will always fall within the ambit of either unlawful access, unlawful interception or unlawful interference. Therefore, in terms of the South African law on cybercrime, the notion of cybercrime can be defined as any offence involving unlawful access, unlawful interception or unlawful interference with data or computer networks by a party unauthorised by law to do any of the mentioned actions.

Along with understanding what cybercrime is, it is also important to differentiate cybercrime from the traditional offences that constitute crime under criminal law. Four key foundations which are inherent to traditional crime, but which cybercrime dispenses with are proximity; scale; physical limitations; and patterns. These foundations highlight the importance of the differentiation as they also emphasise the fact that traditional forms of crime prevention and criminal law would not be appropriate to regulate cyber offences effectively.

Also noted is the fact that cyber transgressions can take place in many ways, shapes and forms such as, *inter alia,* identity theft, hacking, pharming, phishing, etcetera. However, these terms merely describe the actions which lead to the statutory definition under the *Cybercrimes Act* and therefore can all fall under the sections either relating to unlawful access, unlawful interception or unlawful interference. This means that these sections are wide enough to include wholly or partially any of the forms of cybercrime.

The case law discussed above also builds upon the notion that cybercrime is of a growing concern in South Africa and that the legal framework would require an

adequate response. The *Fourie* case highlights the importance of the new *Cybercrimes Act.* It supports the above statement that the statutory definitions are wide enough to include all forms of cyber-offences. The case also serves as an important reminder that any person, business, or company using e-commerce platforms or devices can become the victim of a cyber-offence. The *Carolissen* case points to the extraterritoriality of cybercrime. It also shows how important it is for states to work *in tandem* to curb the prevalence of cybercrime. The case is an important example to South African legislatures that offences under local cybercrime law can have a wide area of operation. This is because the internet does not adhere to traditional geographical boundaries and legislatures should, in turn, proportionally respond by giving (as evidenced in this case by American law) law enforcement enough freedom to convict cybercriminals from where the effects of the offences are felt (in this case, the United States, by way of dissemination on the internet), and not only confining such laws to where the offences in itself were committed.

In conclusion, cybercrime is a growing and intricate concept related to any form of offences committed by using a computer or electronic device whereby any other form of data is unlawfully altered, accessed, interfered with or intercepted. This directly correlates to e-commerce as the rise in the use of computers, data networks and the internet has only given cybercriminals more incentive to commit these devious offences. The South African legal framework can only adequately respond when considering that the concept of cybercrime does not adhere to traditional norms of criminal law and therefore the law that governs it, should also not be confined to the traditional boundaries of criminal law.

Chapter 3: Cryptocurrency and its relevance towards cybercrime

3.1 Introduction

The rise in e-commerce has also given rise to the use of cryptocurrency.[203] Reddy and Minnaar note that in South Africa traders and merchants who accept cryptocurrency as a valid method of payment, are well into the tens of thousands.[204] Maanda refers to cryptocurrency as intangible, finding existence only in cyberspace and which is accepted as a valid method of payment in certain contexts.[205] Cryptocurrency is not centrally regulated in South Africa and relies on the backing and issuing from private developers.[206] Therefore, cryptocurrency merely operates as a digital representation of value.[207] Due to its nature, it does not take up any real-world physical space; and is not regulated or guaranteed by a central bank such as the Reserve Bank in South Africa. Orffer notes that the defining traits of cryptocurrency are its anonymity and its lack of centralisation.[208] Therefore, it is an untraceable form of payment tender, in which parties to the transaction can keep their identity anonymous to one another. Further, the transaction does not leave a "paper trail"[209] in order for it to be followed and traced. It is also not regulated by any overseeing authority such as a government, bank or central bank. The misuse of cryptocurrency and its proximity to matters of cybersecurity and cybercrime, may carry with it the potential to fall under the umbrella of cybercrime. Can cryptocurrency play a role in cybercrime and what would its relevance in the commission of cybercrime be? In order to evaluate the relevance of cryptocurrency in relation to cybercrime, it is necessary to properly set the boundaries of the definition of cryptocurrency, thereafter an examination of the risks associated

---

203 Maanda *Legal Implications of Virtual Currencies* 1.
204 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 71.
205 Maanda *Legal Implications of Virtual Currencies* 2.
206 Papadopoulos and Snail ka Mtuze *Cyberlaw* 67.
207 Orffer *The Inclusion of Virtual Currencies in the Calculation of Income Tax* 2.
208 Orffer *The Inclusion of Virtual Currencies in the Calculation of Income Tax* 2.
209 Orffer *The Inclusion of Virtual Currencies in the Calculation of Income Tax* 2.

with cryptocurrency has to be done within the context of its potential contribution to cybercrime. To achieve this, many possible instances where cryptocurrency has contributed to cybercrime will need to be examined. Furthermore, any new developments in the field of cryptocurrency must also be investigated. Finally, by taking into consideration the findings on the various discussions, the relevance of cryptocurrency in cybercrime will be made clear.

3.2 Definition

3.2.1 Definition and Classification

The IFWG highlights the importance of a thorough definition of cryptocurrency so that it can be appropriately classified and (in principle be) regulated.[210] As seen above,[211] the South African approach follows a more pragmatic line of reasoning in that it analyses the economic function of cryptocurrency rather than getting lost in the nomenclature thereof.[212]

The IFWG, therefore, looks at the function and place of cryptocurrency in South Africa and states as follows:[213]

> Crypto-assets are digital representations or tokens that are accessed, verified, transacted and traded electronically by a community of users. Crypto-assets are issued electronically by decentralised entities and have no legal tender status, and consequently are not considered as electronic money either. It therefore does not have statutory compensation arrangements. Crypto-assets have the ability to be used for payments (exchange of such value) and for investment purposes by crypto-asset users. Crypto-assets have the ability to function as a medium of exchange, and/or unit of account and/or store of value within a community of crypto-asset users.[214]

This definition is concise in laying the foundation of what cryptocurrency is and where its place in the commerce system of South Africa is. It states that cryptocurrency is an

---

210 IFWG 2018 *Consultation Paper on Policy Proposals for Crypto Assets* 8.
211 See 1.3.1 above.
212 IFWG 2018 *Consultation Paper on Policy Proposals for Crypto Assets* 9.
213 IFWG 2018 *Consultation Paper on Policy Proposals for Crypto Assets* 9.
214 IFWG 2018 *Consultation Paper on Policy Proposals for Crypto Assets* 9.

electronic string or graphical representation of value, which is traded electronically. However, due to the fact that it is not issued by a centralised monetary authority, it is not considered legal tender and therefore not classified as money. This comes with a caveat, of course. As with all things that carry (or represent) value, cryptocurrency may be used as unit of exchange. To place it in context, the use of cryptocurrency from a South African legal perspective, should not be seen as a replacement for money, but rather as another option for trade, similar to where, for example two farmers agree to exchange a number of sheep for a number of chickens equal to the value set between themselves.

The South African Reserve Bank (hereafter "SARB"), South Africa's central bank and authority on legal tender,[215] refers to cryptocurrency as a convertible form of virtual currency, as it does have the potential to be exchanged for money or other forms of legal tender.[216] This does not mean cryptocurrency is directly correlated to other currencies, but that it can have a monetary value attached to it, similar to other forms of incorporeal property. The SARB specifically refers to Bitcoin (a popular cryptocurrency) as a decentralised virtual currency.[217] The central bank goes on to classify Bitcoin (and by extension other forms of cryptocurrency) as a speculative investment rather than a legal form of tender.[218] Orffer agrees with this sentiment, as she highlights that cryptocurrency was established with the purpose of competing with legal tender.[219] This means that cryptocurrency was never intended to be a legal tender itself, but merely an electronic representation of value.

In order to better understand the (non) regulation and classification of cryptocurrency. it is also important to understand how it operates. According to Reddy and Minnaar

---

215 Section 17 of the *South African Reserve Bank Act* 90 of 1989. Where a commodity or currency is recognised as legal tender, it is commonly referred to as fiat money/currency. Lotha 2019 https://www.britannica.com/topic/fiat-money/additional-info#contributors.

216 SARB *Position Paper on Virtual Currencies* 2.

217 SARB *Position Paper on Virtual Currencies* 2.

218 SARB *Position Paper on Virtual Currencies* 3.

219 Orffer *The Inclusion of Virtual Currencies in the Calculation of Income Tax* 20.

there are six essential elements to the working of a cryptocurrency platform.[220] These elements are firstly, open-source software.[221] This means any user can gain access to the cryptonetwork if they download the accompanying computer software.[222] Therefore access to such networks is unrestricted and unlimited.

Secondly, the transactions operate on a peer-to-peer basis. This means that users directly operate in contact with one another, and this eliminates the need for a central monetary authority such as a bank to act as an intermediary to the process.[223] This means that the transaction is instant and not subject to clearance or approval. This also means that the transaction cannot be unilaterally reversed and will require the co-operation of both parties involved. Therefore, in instances such as scams, the user does not have recourse to approach a bank and reverse a transaction from his end.

Thirdly, the system operates on a process called "mining". This process creates, validates and quantifies the operation of cryptocurrencies.[224] "Mining" refers to the mechanical and electronic computer processes which operate to validate the cryptographic strings of data which form the cryptocurrency.[225] It also allocates its unique cryptographic string of code to it in order to protect its integrity.[226]

Fourthly, the transfer process works with a system of what is known as keys. Each transaction uses both private and public keys. Each time ownership of a piece of cryptocurrency changes, the sender and recipient need to electronically sign off on the transaction with these keys.[227]

---

220 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 73.
221 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 74.
222 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 74.
223 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 74.
224 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 74.
225 Orffer *The Inclusion of Virtual Currencies in the Calculation of Income Tax* 3.
226 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 74.
227 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 74.

Fifthly, the basis underpinning the functioning of cryptocurrency is a distributed ledger technology known as blockchain.[228] This refers to a sequence of verified blocks of transactions.[229] It functions as a register which records each transaction of a specific set of "coins"[230] between trading parties. The blockchain is therefore a record book of all transactions wherein the specific chain of cryptocurrency was used.

Lastly, cryptocurrency is stored in what is known as virtual vaults or wallets,[231] the value of which is represented by cryptographic strings of letters and numbers.

Therefore, in line with the above, due to its unique nature, cryptocurrency poses a unique challenge to legal systems in that its regulation will also require a unique approach. South Africa follows a pragmatic approach to cryptocurrency by focusing on its impact and working as opposed to cumbersome academic definitions. South Africa acknowledges the economic influence of cryptocurrency, whilst maintaining that it may possess trade value, but is not recognised as a legal form of tender. The reasoning behind this classification can be placed in perspective when reference is made to the unique characteristics of cryptocurrency. In that it uses open-source software, it operates on a direct peer-to-peer basis and uses mining, keys, blockchain and electronic vault software to come into existence and regulate itself. The unique nature of cryptocurrency poses unique questions to legal systems. Furthermore, as with any form of electronic commerce, it is not impervious to exploitation. Under the umbrella of cybercrime, cryptocurrency can be used not only as a target thereof, but also as a tool to further criminality. Therefore, the benefits and the drawbacks of cryptocurrency from a legal perspective need to be examined.

---

228 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 74.

229 Smit *Does blockchain technology offer a solution to the remaining impediments to the more widespread use of electronic negotiable bills of lading?* 47.

230 This is a term used to refer to a specific chain of digital signatures comprising the units of cryptocurrency. Smit *Does blockchain technology offer a solution to the remaining impediments to the more widespread use of electronic negotiable bills of lading?* 48.

231 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 74.

3.2.2 The Benefits of Cryptocurrency

It goes without saying that some of the main advantages of cryptocurrency are its uses as a quick and efficient tool for exchange.[232] It is not only a quick method for making payments, but also has little to no transaction costs.[233] This is evident when comparing cryptocurrency to electronic money transfers. The latter is subject to bank accounts and bank costs, whereas cryptocurrency operates on a peer-to-peer basis, therefore a transaction is only dependent on each party's contribution and not on third party factors such as interest, bank costs and the like. Following from this is the fact that it is also much easier to send cryptocurrency to any place in the world[234] as long as each of the users has the keys mentioned above, as well as the corresponding software. The transaction is not underpinned by authorisations and clearances from banks. It also does not rely on the existence of a bank account for the "funds" to be deposited.

A notable advantage which Orffer refers to is that of inflation. According to her, the relatively low number of units of Bitcoin, and by extension other forms of cryptocurrency, in international circulation, operates as a tool to regulate inflation.[235] Therefore, cryptocurrency's levels of inflation are more rigidly controlled than that of "real" currency. In addition to this, Mothokoa notes that the fact that cryptocurrency operates as a standard international method of exchange, it is not linked to exchange rates between currencies.[236] This means that cryptocurrency's value is the same anywhere it is used and that its purchasing power is not limited based on where it originates from.

---

232 Orffer *The Inclusion of Virtual Currencies in the Calculation of Income Tax* 11.
233 Orffer *The Inclusion of Virtual Currencies in the Calculation of Income Tax* 11.
234 Orffer *The Inclusion of Virtual Currencies in the Calculation of Income Tax* 11.
235 Orffer *The Inclusion of Virtual Currencies in the Calculation of Income Tax* 11.
236 Mothokoa *Regulating cryptocurrencies in South Africa: The need for an effective legal framework to mitigate the associated risks* 11.

Lastly, both Mothokoa and Orffer are of the opinion that cryptocurrency carries with it the potential to empower the unbanked, due to its nature and affordability.[237] This is because, by its very nature, cryptocurrency and other related goods and services are created as an alternative to traditional forms of banking and payment.

Therefore, cryptocurrency can carry with it a number of advantages, especially when placed under the lens of e-commerce. It exists as an alternative to traditional forms of payment and finance. It is more practical and accessible. It operates as its own system of payment, an international system of payment, between the parties directly. It is also not reliant on any banking systems or accounts other than its own platforms. Therefore, it is an effective, self-reliant and borderless system for affecting payments. It is thus ideal for the facilitation of e-commerce, as it is not confined to any physical boundaries.

3.2.3 The Risks of Cryptocurrency

Alongside the many benefits of cryptocurrency which can be enjoyed by all parties to a transaction, as well as the empowerment and development towards e-commerce, cryptocurrency does come with many unique risks and challenges. The unprecedented nature of cryptocurrency can be a headache for legislatures, as it is an intricate system, which requires sufficient insight to comprehend. The *lacuna* that may exist between legislatures and cybercriminals may be exploited if the drawbacks are not properly exposed in order for insight to be had by lawmakers.

3.2.3.1 Market-Related Risks

The IFWG's most notable concern on cryptocurrency is the incidental creation of a fragmented parallel monetary system.[238] They elaborate on this by mentioning that,

---

237 Mothokoa *Regulating crypto currencies in South Africa: The need for an effective legal framework to mitigate the associated risks* 12; Orffer *The Inclusion of Virtual Currencies in the Calculation of Income Tax* 12.

238 IFWG 2021 *Position Paper on Crypto Assets* 22.

inter alia, the function of a central bank is to implement monetary policy in order for the financial market to run efficiently and effectively.[239] The problem in this instance is that cryptocurrency is self-regulated and operates on a peer-to-peer basis. This means that private individuals determine the monetary system of cryptocurrency and therefore may not always act in the best interests of the market, but in pursuance of self-interests. This would entail a fragmented monetary system coming to fruition in the event that demand increases and there are not any legal or governmental oversights or safeguards in place.

Related to the above, the IFWG highlights its most immediate concern as that of consumer protection as well as market efficiency and integrity matters.[240] They highlight that due to its individually operated nature and lack of centralised regulation, there is an inherent lack of consumer protection in cryptocurrency operated transactions. They are further also concerned with the potential for money laundering and terrorism financing as well as unlawful purchases and uncontrolled/undetected international transactions.[241]

Following from the above, the lack of regulation by the Reserve Bank means that cryptocurrency falls outside the ambit of any of its monetary policies.[242] This means that none of the price stabilisation efforts which apply to fiat currency apply to cryptocurrency.[243] This leaves cryptocurrency at the mercy of the free market, which leads to extreme price instability and subject to continuous fluctuations as supply and demand shift. This poses financial risks to those who invest therein. The risk is amplified when considering that no consumer protection policies govern

239 IFWG 2021 *Position Paper on Crypto Assets* 22.
240 IFWG 2021 *Position Paper on Crypto Assets* 22.
241 IFWG 2021 *Position Paper on Crypto Assets* 22.
242 Mothokoa *Regulating crypto currencies in South Africa: The need for an effective legal framework to mitigate the associated risks* 14.
243 Mothokoa *Regulating crypto currencies in South Africa: The need for an effective legal framework to mitigate the associated risks* 14.

cryptocurrency. Therefore, miscalculated steps can have atrocious results for the consumer.

Cryptocurrency carries the potential for any one of these issues to be exploited and exacerbated if it continues to be unregulated. However, the digital nature of cryptocurrency may have the potential to fall within the ambit of cybercrime, which would then determine that the legal framework surrounding cybercrime and cybersecurity would step in as *de facto* regulators in the absence of a proper financial/banking sector regulator. These risks should be examined under the guise of cybercrime to gain insight whether there, in fact, already may exist a legal framework for the regulation thereof.

3.2.3.2 The Volatility of Cryptocurrency

As seen from the above, the legal regulation of cryptocurrency is at issue. However, the real-world management of cryptocurrency also has issues that need addressing. Alongside the market fluctuations of cryptocurrency, there are a few practicality issues to it as well. According to Mothokoa, cryptocurrency continues to exist on the blockchain, notwithstanding any problems the user may encounter. For instance, where a user should die without passing his or her log-in details to another, the cryptocurrency is lost to perpetuity.[244] That string of cryptography cannot be recovered or replaced. The same applies to cryptocurrency which has been stolen.[245] This applies to cases where the blockchain or accounts are hacked, and the cryptocurrency is unlawfully transferred to another user. A notorious "hack" that took place in South Africa is that of *Africrypt*. The founders of the cryptocurrency investment firm, *Aricrypt*, Ameer and Raees Cajee, allegedly claimed that their firm was subjected to a cyber-attack and that $3.6 billion in cryptocurrency had been stolen.[246] Later it turned out

244 Mothokoa *Regulating cryptocurrencies in South Africa: The need for an effective legal framework to mitigate the associated risks* 13.

245 Mothokoa *Regulating cryptocurrencies in South Africa: The need for an effective legal framework to mitigate the associated risks* 13.

246 Morris https://fortune.com/2021/06/24/bitcoin-ameer-raees-cajee-theft-south-africa/.

that the brothers, alongside the missing cryptocurrency, had disappeared. Morris describes the incident as one of the greatest losses of cryptocurrency ever recorded, should the missing crypto not be recovered.[247] Morris adds that the Financial Sector Conduct Authority (FSCA) was unable to formally trace the cryptocurrency in this incident due to the fact that cryptocurrency is not legally recognised as a form of monetary tender in South Africa and therefore not within the brief of the conduct authority.[248]

As seen from the above, there is no central oversight into cryptocurrency which places consumers at the mercy of the free market with virtually no form of recourse should they encounter issues. Furthermore, the peer-to-peer operation thereof expects an unrealistic "honour system" amongst users for free and fair trade. Unfortunately, whilst a commendable ideal, the practical real-world implications thereof means that cryptocurrency is an ideal tool for exploitation for cybercriminals. What this also means is that users from a market perspective and practical ground level perspective, enjoy no safety net when dealing with cryptocurrency and are rather expected to "govern" one another. Given the influx of cybercrime, the vulnerability of users when dealing with cryptocurrency is at an all-time high. Section 3.3 will follow a closer examination on how cryptocurrency matters are exploited within a cybercrime context.

3.3 Link to Cybercrime

The above sets out the main characteristics of cryptocurrency. This section aims to examine how cryptocurrency can contribute to the broader field of cybercrime. As touched on above, due to its nature, cryptocurrency carries with it characteristic risks.[249] These risks, if exploited, can contribute to, *inter alia,* money laundering and

247 Morris https://fortune.com/2021/06/24/bitcoin-ameer-raees-cajee-theft-south-africa/.
248 Morris https://fortune.com/2021/06/24/bitcoin-ameer-raees-cajee-theft-south-africa/.
249 See chapters 1.3.2 & 3.2.3 above.

can be used as a tool to facilitate further acts of cybercrime. Conversely, its lack of legal regulation may also leave it vulnerable to acts of "traditional" cybercrime as well.

3.3.1 How Cryptocurrency can both Facilitate Cybercrime and be a Target Thereof

The IFWG expressly mentions money laundering as one of the main concerns relating to cryptocurrency.[250] Reddy and Minnaar explain that cryptocurrency trading platforms do not have to comply with any form of regulatory standards and/or due diligence type checks.[251] This means that the origin of the money or other form of gains being offered to cryptotraders in exchange for cryptocurrency is not traced. Cryptocurrency essentially operates on a "no-questions-asked" basis. Therefore, to hide illicit gains (i.e. launder money) is a mere formality. The only step required would be to use the illicit gains in exchange for cryptocurrency.

The IFWG also builds on this notion by mentioning that not only is the origin of the money (or other means) not followed up on, but that these transactions mostly take place anonymously.[252] This means that the purchaser does not need to provide his identity to the cryptocurrency trader. It is at the discretion of the trader whether to implement any regulatory formality such as the identification of purchasers.[253] The discretion, even if exercised, does not guarantee that any of the purchaser's information given will be verified. Furthermore, the trader is not subject to any oversight authority, therefore the time and resources put into any verification would likely not be worth it to the trader. This would cut into his profits and customer turnaround, therefore, there will be no incentive for a trader to put in place any verification safety nets.[254] Even in the extraordinary case where a trader may have

250 IFWG 2021 *Position Paper on Crypto Assets* 23.
251 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 76.
252 IFWG 2021 *Position Paper on Crypto Assets* 23.
253 IFWG 2021 *Position Paper on Crypto Assets* 23.
254 Such as Know-your-customer (KYC) requirements.

such self-made rules, money launderers may merely make their purchases elsewhere, to a less regulated marketplace.

Another way in which money laundering benefits from the trading of cryptocurrency is the international aspect of the market.[255] These are transactions that take place across international borders. This makes any transaction almost entirely untraceable. Anyone can at any time enter into such transactions from anywhere in the world. Local authorities would have to identify the purchaser, i.e. money launderer, then they would have to find the trader and then attempt to trace the illicit money to such trader, wherever he may be situated. The sheer number of resources to attempt to successfully investigate and prosecute such a transaction, with such a small chance of success, may render it a futile exercise.

3.3.1.1 Liberty Reserve

Kats v United States of America, Southern District of New York, 2016 (13) U.S 368 is an example of where cryptocurrency trading was used to facilitate money laundering.[256] *In casu*, the trading platform used was of a Puerto Rican origin, known as Liberty Reserve. The US Department of Justice noted that the platform facilitated money laundering operations for numerous sorts of illicit gains, including credit card fraud, hacking, advance fee scams and the like.[257] The platform was convenient to fraudsters in that it only required basic personal information, which was in any event not verified for accuracy.[258] The money laundering process involved the use of a traditional brick and mortar bank to transfer the money to an anonymous and unregistered third party exchanger. From there it was exchanged to cryptocurrency and went on via Liberty Reserve to other money exchanging services, for instance

255 IFWG 2021 *Position Paper on Crypto Assets* 23.
256 *Kats v United States of America, Southern District of New York*, 2016 (13) U.S 368.
257 US Department of Justice 2016 https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital.
258 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 77.

MoneyGram,[259] in smaller portions for the money launderers to exchange their fiat currency for digital currency.[260] This case solidifies the link cryptocurrency has to what is thought of as traditional forms of cybercrime such as money laundering, identity theft, hacking, etcetera. It also showcases how cryptocurrency can tie into the commission of cybercrime and how it can act as a cog in the cybercrime link by providing an easier route for cybercriminals to launder their illicit gains. The IFWG is justified in its assessment of pointing out that money laundering is one of the biggest risks associated with cryptocurrency.

In addition to the laundering of fiat currency, Reddy and Minnaar state that cryptocurrency can in and of itself, also be laundered.[261] Cyber-money laundering takes place when Dark Web services known as "mixers" are used to scramble or "mix" the cryptographic string of address, effectively pooling it together with prior existing currencies and thereby creating a newly generated cryptographic address.[262] By doing this, the origin of the crypto is hidden as it now has a new cryptographic string attached thereto and its origin is therefore untraceable. An outcome similar to physical money laundering.

3.3.1.2 *Africrypt*

As mentioned above, the use of cryptocurrency to facilitate money laundering and fraud is not only seen in foreign jurisdictions. The infamous *Africrypt* case in South Africa is described as one of the biggest cryptocurrency scams ever seen in South

---

259 MoneyGram is an online peer-to-peer fund transferring service. It allows money transfers to take place internationally through its platforms. In addition to fiat currency transfers, it also allows users to cash in their cryptocurrency in exchange for fiat currency. MoneyGram 2022 https://corporate.moneygram.com/about-moneygram?_ga=2.256835907.994472730.1642529561-111704851.1642529561 & Browne 2021 https://www.cnbc.com/2021/05/12/moneygram-to-let-cryptocurrency-traders-cash-in-their-investments.html.

260 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 77.

261 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 77.

262 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 77.

Africa.[263] What is more harrowing is the fact that at the time of this work, this hack is reported as the biggest heist ever reported globally.[264] It is reported that the Cajee Brothers, the founders of the cryptocurrency platform *Africrypt* defrauded users out of an eyebrow-raising USD $3.6 billion (R51 million) which amounted to sixty nine thousand crypto coins. The FSCA does not have jurisdiction to intervene as cryptocurrency is not centrally regulated. The investigation is ongoing.[265] The fact that this incident is one of the largest ever recorded is of concern. This clearly illustrates that cybercrime and cybersecurity issues are not trivial in a nation rampant with traditional crime. It also points out that issues of cybersecurity are not mere academic constructs or so-called first-world problems. Residents of developing nations, such as South Africa, are just as vulnerable, if not more, to cyber-attacks involving cryptocurrency. Legislative and regulatory intervention will have to be considered by the powers that be if users are to be afforded sufficient protection. The foreign law position of developed nations, as well as the international law position, may provide a proper roadmap for South Africa to follow. These issues will be discussed in the following chapter.

The above *Africrypt* case is not only an incident whereby cryptocurrency itself is used as a tool to facilitate cybercrime, but can also been seen as an example by which cryptocurrency becomes the subject of the cybercrime. "Traditional" methods of cybercrime such as hacking, phishing, social engineering and other forms of malware can just as well be employed to obtain access to a user's cryptocurrency.[266] The only difference in such an instance would be that the focus is then on cryptocurrency as opposed to fiat currency. What is even more worrisome in the case of cryptocurrency, is the fact that no intermediary can be approached to investigate the matter or restore

263 Smith 2021 https://www.news24.com/fin24/companies/sa-brothers-multi-billion-bitcoin-break-is-likely-biggest-ever-crypto-heist-20210624.
264 Smith 2021 https://www.news24.com/fin24/companies/sa-brothers-multi-billion-bitcoin-break-is-likely-biggest-ever-crypto-heist-20210624.
265 Smith 2021 https://www.news24.com/fin24/companies/sa-brothers-multi-billion-bitcoin-break-is-likely-biggest-ever-crypto-heist-20210624.
266 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 78-86.

the *status quo ante* of a victim as the case would have been for fiat currency. A bank or the FSCA for example would have been able to assist a victim of a hack or scam and possibly reimburse his losses. The lack of central regulation in the case of cryptocurrency means that no such recourse is possible. The *Africrypt* incident, in this context, sees the use of phishing and hacking to gain access to the cryptocurrency. The founders of *Africrypt* marketed it as a platform for investment and trading. However, this was only a front for a scam, whereafter the users were defrauded out of their investments. This clearly shows how the usual methods of cybercrime are used to target cryptocurrency. This also illustrates the importance to include cryptocurrency in discussions on cybercrime. The concepts are not mutually exclusive, but are cut from the same cloth, and have implications to users of e-commerce platforms, and should therefore be regulated in an intertwined manner. To protect users of electronic platforms, regulatory frameworks on cryptocurrency as well as a legislative framework on cybercrime will have to work together. Further instances of the use of cryptocurrency under the umbrella of cybercrime will follow below.

3.3.1.3 Silk Road

The case *United States of America v Ross William Ulbricht Dread Pirate Roberts Silk Road Sealed Defendant* Dpr 15-1815 May 31, 2017, commonly referred to as the *Silk Road* case[267], is another notable case which placed a spotlight on the fact that cryptocurrency can be used to further enable other forms of cybercrime.[268] Silk Road was the name given to a dark web e-commerce platform in which users were able to anonymously trade illicit goods and services. These goods and services included, *inter alia,* narcotics, weapons and even the solicitation of "hitmen".[269] Other services available on the platform included "hacking-for-hire", which entails the solicitation of

---

267 The case has gained international notoriety. More of it can be seen in the 2017 documentary film titled *Silk Road* as well as the 2021 motion picture film of the same name.

268 Sommers and Bernstein 2020 https://www.cbsnews.com/news/ross-ulbricht-dread-pirate-roberts-silk-road-fbi/.

269 Sommers and Bernstein 2020 https://www.cbsnews.com/news/ross-ulbricht-dread-pirate-roberts-silk-road-fbi/.

a skilled hacker, to unlawfully hack, intercept or alter the data of another.[270] Sommers and Bernstein note that the platform offered many cybercrimes related services. According to Sommers and Bernstein, what makes this case even more of an anomaly is the fact that the e-commerce platform was run by an individual simply known as "Dread Pirate Roberts",[271] the name of a character from the 1987 film, *the Princess Bride*.[272] The platform became known as the *Amazon.com* for the drug-trade.[273] This statement speaks to the colossal scale of operation and reach of the platform, if Silk Road is comparable to *Amazon*.

Nugent notes that one of the defining characteristics of the Silk Road platform was its pure anonymity. It was only accessible through specific means. It employed the use of Bitcoin as payment method.[274] Although Silk Road only ran for two years between 2011 and 2013, these were fruitful years, in that an estimated revenue of approximately US $1.2 billion was realised.[275] The platform was eventually shut down by the FBI, and the creator, later revealed as Ross Ulbricht, was sentenced to life imprisonment under a number of drug trafficking charges, as well as other cybercrimes such as conspiracy to commit identity fraud, conspiracy to commit money laundering and conspiracy to commit hacking.[276] The anonymity underpinning trading with cryptocurrency, *in casu* Bitcoin, offered the perfect circumstances for illicit trade as neither seller nor buyer had to interact directly with one another and both parties would leave the transaction satisfied. This, coupled with the fact that only certain

---

270 Sommers and Bernstein 2020 https://www.cbsnews.com/news/ross-ulbricht-dread-pirate-roberts-silk-road-fbi/.

271 According to the film's lore, this name was taken up by many pirates in order to gain notoriety from the reputation therewith connected to intimidate their opponents and thereafter they would retire from using the name and pass it on to another. Brock 2019 https://www.litcharts.com/lit/the-princess-bride/characters/the-dread-pirate-roberts.

272 Sommers and Bernstein 2020 https://www.cbsnews.com/news/ross-ulbricht-dread-pirate-roberts-silk-road-fbi/.

273 Sommers and Bernstein 2020 https://www.cbsnews.com/news/ross-ulbricht-dread-pirate-roberts-silk-road-fbi/.

274 Nugent 2019 *Fordham Law Review* 353.

275 Nugent 2019 *Fordham Law Review* 353.

276 Nugent 2019 *Fordham Law Review* 353.

devices and web browsers could access the platform, made tracing the end users even more unlikely. Further, the easy conversion of Bitcoins into fiat currency or its use as an exchange method for goods, creates a simplified process for money laundering.

This case is similar to the *Africrypt* and *Liberty Reserve* cases above, in that it shines the light on the cybercrime implications which can follow from the use of cryptocurrencies in e-commerce platforms. It highlights how the anonymity of the trade creates easy avenues for undesirables to gain access to and participate in marketplaces consisting of illicit goods and services. It also points at how all forms of cybercrime interact with one another. Cryptocurrency in this context is used as a tool to further facilitate other forms of cybercrime such as identity theft, money laundering and hacking.

3.3.1.4 Darkode

Darkode, similar to *Silk Road*, was the name given to a dark-web-based e-commerce platform wherein the goods and services on offer were data obtained through unlawful means. This included personal information, credit card details, server credentials and the like, which hackers sold off to other parties for profit.[277] The anonymity of the platform arises from the fact that the forum itself operated on a blockchain, similar to cryptocurrency, to ensure that law enforcement officials were essentially blocked out.[278] Once again, Bitcoin is the preferred method of payment to avoid being traced.[279] It seems that the forum is continually shut down by law enforcers, with several arrests being made on each occasion. However, the forum keeps re-emerging in different forms.[280] The common denominator between all the above platforms and cases is that all them operate under the auspices of cryptocurrency in order to ensure their illicit

277 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 76.
278 Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology* 76.
279 O'Flaherty 2019 https://www.forbes.com/sites/kateoflahertyuk/2019/04/10/notorious-hacking-forum-darkode-is-back-online/?sh=4761507752e8.
280 O'Flaherty 2019 https://www.forbes.com/sites/kateoflahertyuk/2019/04/10/notorious-hacking-forum-darkode-is-back-online/?sh=4761507752e8.

trade is untraceable, anonymous and opens easy avenues to money laundering. Therefore, cryptocurrency itself is a major contributor to the cybercrime industry. The authorities regulating cybercrime and cybersecurity must take note hereof and must provide sufficient regulation in respect of cryptocurrency, which is used as a means to an end, that being cybercrime. If legislatures do not intervene to eliminate these practices, the future of e-commerce may seem bleak to those most vulnerable to cyber-attacks.

3.4 Conclusion

The above sought to investigate whether there exists a link between cryptocurrency and cybercrime. In order to find a potential link, the characteristics of cryptocurrency were discussed. Further, an examination of the benefits and risks of cryptocurrency took place. Finally, the relevance of cryptocurrency within the context of cybercrime was examined.

The study found that cryptocurrency is an electronic string or graphical representation of value, which is traded electronically. It has no central regulation or backing from banks in South Africa. It is not recognised as a legal form of tender and therefore not classified as money. However, cryptocurrency may be used as a unit of exchange subject to the discretion of merchants in the sale of goods and services. It does, in line with this, have a monetary value attached to it, similar to other forms of incorporeal property.

The characteristics of cryptocurrency are that it operates on an open-source software platform. The transactions operate on a peer-to-peer basis. Further, the system operates on a process called "mining". The transfer process works with a system of what is known as keys. The foundation underpinning the running of cryptocurrency is a distributed ledger technology known as blockchain. Cryptocurrency is stored in what is known as virtual vaults or wallets. The unique nature of cryptocurrency poses unique challenges to legal systems regarding its regulation.

The benefits of cryptocurrency also emanate from its unique characteristics. Due to its nature, it is an effective, self-reliant and borderless system for affecting payments. It is ideal for the simplification of e-commerce, as it is not confined to any physical boundaries.

However, the benefits are not unencumbered. Cryptocurrency carries with it many inherent risks. Due to its individually operated nature and lack of centralised regulation, there is an intrinsic lack of consumer protection in cryptocurrency transactions. It also contains the potential for money laundering and terrorism financing as well as unlawful purchases and uncontrolled/undetected international transactions. Furthermore, consumers are placed at the mercy of the free market with no form of recourse should they encounter problems. Additionally, the peer-to-peer functionality thereof expects an unrealistic "honour system" amongst users for free and fair trade. The implications thereof means that cryptocurrency is an ideal tool for exploitation for cybercriminals.

In line with this, cryptocurrency transactions take place anonymously. A purchaser does not need to provide his identity to a cryptocurrency trader. It is, further, at the discretion of the trader whether to implement any regulatory formality such as the adherence to for instance, know-your-customer requirements. The discretion, even if exercised, does not guarantee that any of the purchaser's information given will be verified for authenticity. The *Kats* case showcases the risks associated to the pure anonymity of cryptocurrency transactions. It also highlights the ease by which illicit gains can be laundered when using cryptocurrency.

The *Africrypt* incident linked the risks of cryptocurrency with the traditional forms of cybercrime. It showed how cryptocurrency itself was used as a tool to facilitate cybercrime, as well as how cryptocurrency became the subject of cybercrime. The lack of central regulation also meant that no recourse was available to the affected consumers through an intermediary such as a bank or an oversight authority. The *Africrypt* incident displayed the use of phishing and hacking to gain access to

cryptocurrency. This shows how the usual methods of cybercrime are used to target cryptocurrency. It illustrates the importance to include cryptocurrency in discussions on cybercrime.

The *Silk Road* and *Darkode* cases built on this by highlighting the fundamental risks that accrue from the inherent anonymity of cryptocurrency transactions. These cases are further showpieces for the ease in which money laundering can take place through cryptocurrency. They further stress the link between cryptocurrency and cybercrime. Throughout the above cases, cryptocurrency was at the centre of the transgressions taking place. It provided the platform for nameless transactions which when tied to traditional forms of cybercrime such as hacking and phishing, which created the perfect tool for cybercriminals to exploit.

Therefore, any discussion on cryptocurrency should intrinsically include a discussion on cybercrime. As seen from the above, cryptocurrency can be and is used as both the target of cybercrime as well as a tool in furthering other forms of cybercrime. The traditional forms of cybercrime as explained in chapter 2, can run rampant when the anonymous and decentralised nature of cryptocurrency become intertwined therewith. As such, a secure legal framework on cybercrime may provide a suitable point of departure for cryptocurrency regulation. It may also ensure security for cryptocurrency consumers and traders in the meantime, whilst a direct regulatory framework on cryptocurrency is lacking. In line with this, an examination on cybercrime legal frameworks, especially as it relates to cryptocurrency regulation, is required. The following chapters will examine cybercrime legal frameworks through the lens of potentially providing for a regulatory structure toward cryptocurrency. Chapter 4 will look at international law as well as certain foreign jurisdictions. Chapter 5 will examine the South African perspective in this regard.

Chapter 4: International Perspectives on Cryptocurrency

4.1 Introduction

The previous chapters elaborate on the concepts of e-commerce, cybercrime and cryptocurrency. Chapter 3 analysed how cryptocurrency can be both the object and target of cybercrime within the context of e-commerce. This chapter aims to provide insight into the international legal community's response to e-commerce with a specific focus on cryptocurrency regulation. To do so, an analysis of prominent international law instruments on e-commerce must be undertaken. Furthermore, an examination into some international and regional instruments as well as specific foreign jurisdictions' position on cryptocurrency, will also take place. This will provide a normative basis for comparing the South African cryptocurrency position.

4.2 International law

4.2.1 UNCITRAL Model Law on Electronic Commerce

The UNCITRAL Model Law on Electronic Commerce (1996) is an internationally accepted set of standards and principles on e-commerce.[281] It was adopted by the United Nations Commission for International Trade Law on 12 June 1996.[282] The key aim of the instrument is to set out a precise set of standards and principles for domestic legislatures to follow when developing their own laws on electronic commerce.[283] Some key provisions in the model law include rules on non-discrimination, technological objectivity, the validity of electronic agreements and principles for establishing when a data message was received.[284] Article 5 states:

---

281 Kouamo *Combating Crime in International Electronic Commerce* 21.

282 Eiselen 2007 *PER/PELJ* 3.

283 Kouamo *Combating Crime in International Electronic Commerce* 21.

284 United Nations date unknown https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce#:~:text=Purpose,legal%20predictability%20for%20electronic%20commerce. Chapter 3 of the *UNCITRAL Model Law on Electronic Commerce* (1996).

> Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.[285]
>
> …that there should be no disparity of treatment between data messages and paper documents.[286]

Article 6 builds on this by giving recognition to data messages where there is written requirement to an agreement:

> Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.[287]

Snail ka Mtuze iterates that the model law is not an international law convention and as such does not have direct application in law, but played a key role in the development of internationally accepted standards and principles for trade.[288]

The model law was an important step for harmonising trade-related rules in e-commerce. However, no mention is made of cybercrime.[289] Given the age of the model law, there is also no provisions on cryptocurrency. Nonetheless, the *Model Law on Electronic Commerce* forms an important primary basis for any legislation on e-commerce as it sets out important internationally accepted norms and principles that can lead to harmonising e-commerce legislation globally.

4.2.2 UNCITRAL Model Law on Electronic Signatures

The *UNCITRAL Model Law on Electronic Signatures* (2001) was established as a supplementary model law to the *Model Law on Electronic Commerce*. It aims to provide an acceptable normative standard for domestic legislation on the recognition,

---

285 A 5 of the *UNCITRAL Model Law on Electronic Commerce* (1996).
286 A 5 of the *UNCITRAL Model Law on Electronic Commerce* (1996).
287 A 6 of the *UNCITRAL Model Law on Electronic Commerce* (1996).
288 Papadopoulos and Snail ka Mtuze *Cyberlaw* 42.
289 Kouamo *Combating Crime in International Electronic Commerce* 21.

acceptance and methods of assessing electronic signatures in e-commerce.[290] Article 6 states:

> Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.[291]

It aims to set out criteria for the recognition of electronic signatures when compared to handwritten signatures.[292] For instance, Article 9(1)(f) provides for a system of checks and balances through a certification services provider.[293] The criteria of which is set out in Article 10:

> For the purposes of article 9, paragraph 1 (f), of this Law in determining whether, or to what extent, any systems, procedures and human resources utilised by a certification service provider are trustworthy, regard may be had to the following factors:
>
> (a) Financial and human resources, including existence of assets;
>
> (b) Quality of hardware and software systems;
>
> (c) Procedures for processing of certificates and applications for certificates and retention of records;
>
> (d) Availability of information to signatories identified in certificates and to potential relying parties;
>
> (e) Regularity and extent of audit by an independent body;
>
> (f) The existence of a declaration by the State, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing; or
>
> (g) Any other relevant factor.[294]

---

290 Kouamo *Combating Crime in International Electronic Commerce* 21.

291 A 6 of the *UNCITRAL Model Law on Electronic Signatures* (2001).

292 United Nations date unknown https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures.

293 A 9(1)(f) of the *UNCITRAL Model Law on Electronic Signatures* (2001).

294 A 10 of the *UNCITRAL Model Law on Electronic Signatures* (2001).

The model law does not expressly address cybercrime matters. However, it sets out important standards and principles for preventing online fraud.[295] The model law is an important step in harmonising international rules for the validity of electronic signatures and, thus, by extension, electronic documents.

4.2.3 Council of Europe Convention on Cybercrime

The *Council of Europe Convention on Cybercrime* (2001), commonly referred to as the *Budapest Convention,* is the foremost multinational treaty on cybercrime.[296] South Africa is a signatory to the treaty.[297] The prominence of the convention lies in the fact that it is the first international treaty regulating cybercrime.[298] It, *inter alia,* has a provision on computer-related fraud.[299] Article 8 of the *Budapest Convention* implores states to criminalise computer-related fraud under their respective domestic laws.[300] The Article is wide in its wording. It reads as follows:

> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:
>
> a) any input, alteration, deletion or suppression of computer data,
>
> b) any interference with the functioning of a computer system,
>
> with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.[301]

The Article is open-ended in its wording. The benefit therein lies in the fact that technological enhancements do not affect the original aim of the Article, it being the prevention of computer-related fraud. It is only required that the elements of the

---

295 Kouamo *Combating Crime in International Electronic Commerce* 21.
296 Clough 2012 *Criminal Law Forum: The Official Journal of the Society for the Reform of Criminal Law* 367-369.
297 Council of Europe 2022 https://www.coe.int/en/web/cybercrime/the-budapest-convention.
298 Council of Europe 2022 https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.
299 Kempen 2019 *Servamus* 27.
300 A 8 of the *Council of Europe Convention on Cybercrime* (2001).
301 A 8 of the *Council of Europe Convention on Cybercrime* (2001).

offence be present. The elements being: damage caused to another, or another's property, culpably and unlawfully by altering data or interfering with a computer system for economic benefit. The open-ended nature of the Article, and non-specific terms used therein, allow it to apply to fraudulent computer activity involving cryptocurrency as well. Thus, if a fraudulent transaction, alteration or interference takes place; along with the necessary elements of unlawfulness and culpability being present; with the conduct being to the economic benefit of the perpetrator, it will also apply to transactions involving cryptocurrency. Domestic legislatures would be wise to apply these elements to possible future statutes regulating cryptocurrency, as this would criminalise any fraudulent activity involving cryptocurrency.

The above showcases the flexibility of the *Budapest Convention* to apply to advances in technology.[302] However, one must keep in mind that the treaty is over two decades old. Kempen iterates that internet usage has developed and evolved drastically over the past twenty years.[303] She further highlights that as daily internet usage has evolved, so have the criminal tactics relating to it.[304] The Council of Europe has taken note hereof and adopted the *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (2022) on 21 November 2021.[305]

The *Second Additional Protocol* addresses the inherent lack of territoriality in the commission of cybercrimes.[306] The Protocol provides methods for tracing cybercriminals through their internet service providers. These methods engage the co-operation of internet service providers by sharing offenders' data, subscriber

---

302 Clough 2012 *Criminal Law Forum: The Official Journal of the Society for the Reform of Criminal Law* 375.

303 Kempen 2019 *Servamus* 27.

304 Kempen 2019 *Servamus* 27.

305 Council of Europe 2022 https://www.coe.int/en/web/conventions/new-treaties. Adopted by the Committee of Ministers of the Council of Europe on 21 November 2021, it is yet to be signed into effect. Signature thereof is set to take place on 12 May 2022.

306 Council of Europe 2022 https://www.coe.int/en/web/conventions/new-treaties.

information and domain information with law enforcement agencies.[307] The Protocol enables law enforcement agencies to trace offenders by gaining access to their subscriber and domain information through mutual assistance from internet service providers.[308]

This is achieved by, *inter alia,* Article 6 of the *Second Additional Protocol*. It states that:

> Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities, for the purposes of specific criminal investigations or proceedings, to issue a request to an entity providing domain name registration services in the territory of another Party for information in the entity's possession or control, for identifying or contacting the registrant of a domain name.[309]

Article 7 is similar in its wording, but with the focus on subscriber information.[310] Article 8 provides the procedural steps to be followed when giving effect to orders for the production of providing domain names or subscriber information.[311] Article 8 states that:

> Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to issue an order to be submitted as part of a request to another Party for the purpose of compelling a service provider in the requested Party's territory to produce specified and stored
>
> a) subscriber information, and
>
> b) traffic data
>
> in that service provider's possession or control which is needed for the Party's specific criminal investigations or proceedings.[312]

---

307 Council of Europe 2022 https://www.coe.int/en/web/conventions/new-treaties.

308 Chapter 2 of the *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (2022).

309 A 6(1) of the *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (2022).

310 A 7 of the *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (2022).

311 A 8 of the *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (2022).

312 A 8(1) of the *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (2022).

Article 9 provides for emergency expedited processes.[313] Finally, Articles 10-12 provide for the mutual assistance and co-operation between states to prosecute computer-related fraud.[314]

As seen from the above development, the *Budapest Convention*, along with its recent *Protocols,* is an important source for international cybersecurity law. It sets out the parameters of computer-related fraud. It also provides for the co-operation between states to investigate and potentially prosecute such fraud. However, its force of law is restricted to signatories and member states.[315] It further does not have express provisions on cryptocurrency regulation. The success of investigations and co-operation between states in terms of the *Second Additional Protocol* is also still to be observed.

4.2.4 United Nations Convention on the Use of Electronic Communications in International Contracts

According to Coetzee, the *United Nations Convention on the Use of Electronic Communications in International Contracts* (2005)[316] builds on the provisions of the two *UNCITRAL* conventions.[317] The purpose of the convention is to provide a level of legal certainty to electronic commerce that is on par with the standards and principles applicable to traditional commercial transactions.[318] Article 5(1) of the convention provides that the convention must be interpreted in a manner reflective of its

---

313 A 9 of the *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (2022).

314 A 10-12 of the *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (2022).

315 A 2(1) of the *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (2022).

316 *United Nations Convention on the Use of Electronic Communications in International Contracts* (2005).

317 Coetzee 2006 *SA Mercantile Law Journal* 248.

318 United Nations date unknown https://uncitral.un.org/en/texts/ecommerce/conventions/electronic_communications#:~:text=The%20Electronic%20Communications%20Convention%20aims,their%20traditional%20paper%2Dbased%20equivalents.

international character.[319] In this way, effect is given to its aims and application by providing for an internationally accepted legal standard for e-commerce.

In line with the above, as well as the *UNCITRAL Model Law on Electronic Commerce*, Article 8 states:

> A communication or a contract shall not be denied validity or enforceability on the sole ground that it is in the form of an electronic communication.[320]

Both Coetzee and Kuoamo explain that the convention's scope is limited to principles regarding electronic contracts and makes no direct reference to online crime.[321] Given the age of the convention, no provisions on cryptocurrency are present. Therefore, the convention cannot clarify the international law position regarding cryptocurrency in electronic commerce. It further cannot provide a legal stance on the cybercrime effects resulting from the fraudulent use of cryptocurrency.

The above conventions, namely the *UNCITRAL Model Law on Electronic Commerce;* the *UNCITRAL Model Law on Electronic Signatures;* the *Council of Europe Convention on Cybercrime;* and the *UN Convention on the Use of Electronic Communications in Electronic Contracts,* set out the prominent international law position on e-commerce. These conventions act as a codification of the most relevant rules and principles underpinning e-commerce transactions. However, save for the *Budapest Convention,* these conventions do not directly address any aspects of cybercrime. The *Budapest Convention* aims to codify the international position on cybercrime but is limited in its scope given its age. International bodies have taken notice hereof and are addressing the issue with the *Second Additional Protocol.* The success of the *Second Additional Protocol* will be seen in its implementation and enforcement.

---

319 A 5(1) of the *United Nations Convention on the Use of Electronic Communications in International Contracts* (2005).

320 A 8(1) of the *United Nations Convention on the Use of Electronic Communications in International Contracts* (2005).

321 Coetzee 2006 *SA Mercantile Law Journal* 256-258; Kouamo *Combating Crime in International Electronic Commerce* 21.

4.2.5 Conclusion

The above highlights that there is, as of yet, no concise and widely agreed upon international law standard on cryptocurrency regulation. This follows that there is currently also no clear international standard for the regulation of cybercrime which follows as a result of fraudulent cryptocurrency use. It is to be seen whether the *Second Additional Protocol* will be successful in its goals to empower states to work together to curb the inherent lack of territoriality of cybercrime and therefore lead to the successful prosecution of these offenders.

An examination of various foreign jurisdictions is necessary for a better picture of the international position regarding cryptocurrency and online fraud. The methods employed by certain developed nations may provide a useful normative basis for South Africa to follow suit.

4.3 Foreign law

4.3.1 Japan

According to the WIPO world innovation index, Japan is one of the world leaders when it comes to the advancement of technology.[322] Thus, it would be well-suited to examine its position on cryptocurrency regulation. According to recent amendments to Japan's *Payment Services Act* 59 of 2006, cryptocurrency is not afforded currency status. However, it is recognised as a valid form of payment tender.[323] Cryptocurrency is fully regulated in Japan, and all cryptocurrency service providers must be registered.[324] A further caveat is placed on Japan's cryptocurrency markets in that all foreign cryptocurrency trade is prohibited.[325] This includes the trade of cryptocurrency into Japan and the flow of cryptocurrency out of Japan. The prohibition includes the

322 WIPO 2021 *Global Innovation Index* 100.
323 A 2(5) of the *Payment Services Act* 59 of 2006.
324 Dube *Regulatory Challenges Posed by the Evolution of Cryptocurrencies* 28.
325 Dube *Regulatory Challenges Posed by the Evolution of Cryptocurrencies* 28.

solicitation of Japanese persons by foreign traders. Registration of a cryptocurrency trader in Japan is dependent on the domicile of such trader (or its representative) in Japan.[326]

The *Payment Services Act* takes a strict approach to cryptocurrency regulation.[327] It does so to curb any possible cybercrime that may flow from cryptocurrency fraud. It further emphasises the prevention of money laundering.[328] The Act uses various accounting safeguards and company oversight mechanisms to ensure that cryptocurrency is not used fraudulently.[329] Doing this ensures that all trade involving cryptocurrency is accounted for, ensuring that fraudulent activity is restrained.

The strict control measures employed in Japan are the way forward for regulating cryptocurrencies. In Japan, cryptocurrency is not a legal currency but a legal form of payment. It is subjected to the various accounting principles and regulations that form part of the monetary regulation in Japan. In this way, cybercrimes related to cryptocurrency use are restricted. The practices imposed in Japan may serve as a good example for South Africa to follow.

Similar to the FSCA, Japan's Financial Service Agency reviews the annual records of companies, the key difference being that the Japanese regulatory body has the authority to review companies trading in cryptocurrency.[330] Therefore, the methods employed in Japan may have substantial merit to be used in South Africa, should the country wish to restrict cybercrime activity that originates from or is targeted by cryptocurrency trade.

However, even a technologically advanced nation such as Japan is not impervious to cybercriminals. Japan recently saw one of its most significant cyber-attacks, where

326 Dube *Regulatory Challenges Posed by the Evolution of Cryptocurrencies* 28.
327 Maanda *Legal Implications of Virtual Currencies* 30.
328 Maanda *Legal Implications of Virtual Currencies* 30.
329 Maanda *Legal Implications of Virtual Currencies* 30.
330 Dube *Regulatory Challenges Posed by the Evolution of Cryptocurrencies* 33.

hackers made off with an estimated US $97 million in cryptocurrency.[331] The hackers converted the stolen cryptocurrencies to Ethereum to prevent any of the stolen proceeds from being frozen. Ethereum is decentralised and makes regulatory attachment thereof difficult.[332] Therefore, due to the online nature of cryptocurrency, it is still difficult to enforce regulations on a domestic level. As seen here, even a solid domestic regulatory framework is not airtight, and cyber-attacks are still possible from outside the country. The decentralised nature of crypto-assets leaves room for cybercriminals to exploit. Thus, a localised regulatory framework must be accompanied by strong enforcement units. An assessment of the US regulatory framework may provide insight into the notion of a stringent legal framework and an enforcement structure.

4.3.2 The United States of America

The US legislative structure empowers individual states to enact laws applicable to their own state. Thus, laws may differ from one state to the other.[333] This is also the case with cryptocurrency.[334] However, this is subject to federal oversight. Federal oversight comes in the form of the *Securities Exchange Act* of 1934.[335] The Act requires cryptocurrency traders to register under the Act's auspices if such trader meets the criteria for securities classification.[336] The US Securities Exchange Commission (SEC) requires cryptocurrency service providers to register in terms of the *Securities Exchange Act*.[337] Cryptocurrency service providers are regulated under federal securities law.[338] The benefit of the US legal system is that it provides a federal safety

---

331 Browne 2021 https://www.cnbc.com/2021/08/19/liquid-cryptocurrency-exchange-hack.html.
332 Browne 2021 https://www.cnbc.com/2021/08/19/liquid-cryptocurrency-exchange-hack.html.
333 Fine 2022 https://www.lexisnexis.com/en-us/lawschool/pre-law/intro-to-american-legal-system.page#:~:text=The%20American%20system%20is%20a,of%20the%20matter%20before%20it.
334 Maanda *Legal Implications of Virtual Currencies* 33.
335 *Securities Exchange Act* of 1934.
336 Dube *Regulatory Challenges Posed by the Evolution of Cryptocurrencies* 33.
337 Dube *Regulatory Challenges Posed by the Evolution of Cryptocurrencies* 34.
338 Dube *Regulatory Challenges Posed by the Evolution of Cryptocurrencies* 34.

net for states. This means that there is a two-tier level of protection due to regulation at both national and state levels. Therefore, in instances where a state's regulation errs, the federal securities law may provide an added layer of regulation and enforcement.

In New York State, for instance, the legal position is similar to Japan in that cryptocurrency traders have to be domiciled in the state and be registered with the appropriate licencing being issued.[339] The support for the Japanese position by influential states such as New York, is a strong indication that regulation through domicile restriction, registration and accounting review may be the way forward for cryptocurrency. The case can be made that these methods are the strongest for preventing cybercrime through cryptocurrency.

The USA recently proved the success of their regulatory framework in the case of *United States of America v Ilya Lichtenstein and Heather Rhiannon Morgan*.[340] US authorities arrested two individuals for conspiracy to commit money laundering through Bitcoin to the value of US $4.5 billion.[341] Thus far, the US Department of Justice has managed to recover and seize $3.6 billion. This recovery is, to date, the highest amount recovered by US authorities.[342] The Department remarked that the formula for success is to follow the money, no matter what form it may take.[343] Although the accused persons tried their best to cover their tracks by obscuring the money trail through sophisticated digital coverups, the cybercrimes unit of the Internal Revenue Service (IRS) was able to follow and stay on the digital trail.[344] What is of note, in this

339 De Kock *Regulating Cryptocurrencies in South Africa* 4.

340 *United States of America v Ilya Lichtenstein and Heather Rhiannon Morgan* case 1:22-mj-0022 (United States District Court for the District of Columbia) (7 February 2022).

341 US Department of Justice 2022 https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.

342 US Department of Justice 2022 https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.

343 US Department of Justice 2022 https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.

344 Hsu 2022 https://www.washingtonpost.com/dc-md-va/2022/02/14/bitcoin-launder-bitfinex-hack/.

case, is that even in cases where cybercriminals are continuously adapting and becoming ever more intelligent, so too are law enforcement officials in that they can pick up on the digital breadcrumbs left behind by cybercriminals.[345] If South African authorities hope to keep ahead of the curve, they would be wise to follow the strategies employed by specialised units such as the IRS Cybercrime Unit. The strategy employed by US authorities, as well as federal legal and regulatory oversight, is required for an effective framework to combat cybercrime related to cryptocurrency.

4.3.3 The European Union

The European Union recognises the use of cryptocurrency in commercial activities.[346] Emphasis is placed on anti-money laundering by legislatures.[347] The EU employed the First Anti-money Laundering Directive[348] in 1990 in order to regulate its financial systems and prevent money laundering. The directive set the preliminary basis for what was to follow and added preventative measures such as client identification, due diligence checks and record-keeping, as well as centralised methods for the reporting of suspicious transactions.[349] The Fifth and latest Directive, adopted on 19 June 2018,[350] has implemented the use of the term "virtual currencies" in an effort to prevent money laundering in relation to various forms of digital currency including cryptocurrency.[351] Furthermore, Financial Intelligence Units in the EU have been given wider scope of authority. The units have the authority to request information even before a suspicious

345 Hsu 2022 https://www.washingtonpost.com/dc-md-va/2022/02/14/bitcoin-launder-bitfinex-hack/.
346 De Kock *Regulating Cryptocurrencies in South Africa* 3; Mothokoa *Regulating cryptocurrencies in South Africa: The need for an effective legal framework to mitigate the associated risks* 52.
347 De Kock *Regulating Cryptocurrencies in South Africa* 3.
348 Council Directive 91/308/EEC.
349 IBA Anti-money Laundering Forum date unknown https://www.anti-moneylaundering.org/Europe.aspx.
350 European Commission 2022 https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-countering-financing-terrorism_en#:~:text=The%20European%20Union%20adopted%20the,the%20purpose%20of%20money%20laundering.
351 De Kock *Regulating Cryptocurrencies in South Africa* 4.

transaction occurs.[352] Therefore, with a wide range of safeguards and a higher level of autonomy from regulators, the EU aims to put a firm grip on any money laundering activities that may stem from cryptocurrency. These safeguards will, by extension, apply to other forms of cybercrime linked to cryptocurrency.

Like its Asian and American counterparts, Europe has seen an influx of cryptocurrency-related cyber-attacks. In 2020, a number of supercomputers[353] were hacked and infected with malware aimed at mining cryptocurrency.[354] The attack saw supercomputers in the UK, Spain and Germany being infected by cryptocurrency mining malware.[355] This, *inter alia,* motivated the EU to fast-track its regulatory frameworks on cryptocurrency. On 7 May 2020, the European Commission resolved to adopt an action plan for a comprehensive policy on the prevention of money laundering and terrorism financing. This action plan included regulations on cryptocurrency providers and wider authority for watchdogs.[356]

It is important to note that the EU continually reviews and implements regulations and action plans to address cyber-security issues regarding cryptocurrency. South African legislatures should take note of the EU's proactive response to stay up-to-date with relevant and current issues. Cybersecurity and cybercrime are not stagnant matters.

---

352 Mothokoa *Regulating crypto currencies in South Africa: The need for an effective legal framework to mitigate the associated risks* 53; European Commission 2022 https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-countering-financing-terrorism_en#:~:text=The%20European%20Union%20adopted%20the,the%20purpose%20of%20money%20laundering.

353 Extremely powerful computers aimed at amongst others scientific or engineering related work which requires high-speed calculations and computations; Hosch 2019 https://www.britannica.com/technology/supercomputer.

354 Moss 2020 https://www.datacenterdynamics.com/en/news/european-supercomputers-hacked-mine-cryptocurrency/.

355 Moss 2020 https://www.datacenterdynamics.com/en/news/european-supercomputers-hacked-mine-cryptocurrency/.

356 European Commission 2022 https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-countering-financing-terrorism_en#:~:text=The%20European%20Union%20adopted%20the,the%20purpose%20of%20money%20laundering.

Issues which stem from cybersecurity are continuously evolving to circumvent lawmakers. Therefore, a systematic and continuous approach to regulation is required to build an effective regulatory framework and thus to prevent cybercrime and protect users.

4.4 Conclusion

This chapter sought to find international perspectives on cryptocurrency regulation related to cybercrime. In order to find the international legal fraternity's perspective on these concepts, it was necessary to take a look at the foremost international law treaties on e-commerce and cybercrime as well as the practices employed in several foreign jurisdictions. The starting point for a conversation on global e-commerce is the *UNCITRAL Model Law of Electronic Commerce* (1996). It aims to establish a standardised model for electronic contracting and trade through various rules and principles. The model law itself takes no stance on cyber-fraud as it merely operates as the starting point to test the validity of an international e-commerce contact. The *UNCITRAL Model Law on Electronic Signatures* (2001) acts as a supplement to the original *UNCITRAL model law.* The 2001 model law does not expressly deal with cybercrime; however, it is an important development in the international perspective on online fraud. It operates as a normative standard for the testing of the validity and authenticity of electronic signatures. Therefore, the *Model Law on Electronic Signatures* was the starting point in international law toward safer cyber-regulation. Later that same year, a treaty dealing expressly with cybercrime and cyber-security was adopted.

The *Council of Europe Convention on Cybercrime* (2001), colloquially known as the *Budapest Convention,* is the leading international convention on cybercrime. Article 8 of the convention specifically criminalises computer-related fraud. The wording of the article is wide enough to support technological advancements without losing the original intention of the legislature, i.e., the prevention and criminalisation of

computer/online fraud. This would naturally apply to the fraudulent use and/or targeting of cryptocurrency, should it be the object or target of cybercriminals. The *Budapest Convention*, although wide in its wording, is not impervious to technological changes and the challenges that accompany it. Therefore, the Council of Europe has recently adopted the *Second Additional Protocol* to the *Budapest Convention*. The *Protocol* empowers nations to work in tandem to circumvent the inherent lack of territoriality that would follow from a cybercrime and thus successfully prosecute any perpetrators.

The *United Nations Convention on the Use of Electronic Communications in International Contracts* (2005) acts as a further building block to e-commerce from the treaties that preceded it. However, once again, the focus of the treaty is on the contractual principles in e-commerce trade and not on cybersecurity itself.

The above iterates the international law position on cybersecurity and the possible effect it can have on the fraudulent use of cryptocurrency in e-commerce. However, only the *Budapest Convention* primarily focuses on creating an international standard for cybersecurity. The *Budapest Convention*, although widely written, is not impenetrable and, therefore, the *Second Additional Protocol* was adopted to act as a supplement to the ageing *Budapest Convention*. The success of the *Second Additional Protocol* is still to be seen in practice. Only time will tell whether further patch jobs of the original *Budapest Convention* will be successful or whether a complete overhaul of the international law on cybercrime and cybersecurity would be necessary.

International law gives one an idea of the wider perspective on these issues. An examination of the methods used by certain foreign jurisdictions indicates a narrower perspective on cryptocurrency regulation as it relates to cybercrime. Japan fully recognises and regulates cryptocurrency under its *Payment Services Act.* All cryptocurrency traders must be registered and have a domicile in Japan. The Act also enforces strict accounting principles and laws on such traders to prevent money

laundering. Japan's Financial Services Agency has wide powers to review the annual statements of companies dealing in cryptocurrency. However, even strong regulations on cryptocurrency do not entirely prevent online fraud with an origin outside of the country, as seen by the recent cyber-attack in Japan. This situation would be a valuable opportunity to use the powers given under the *Second Additional Protocol to the Budapest Convention* for Japanese officials to work in tandem with the perpetrator's country of origin to prosecute such individuals.

The United States of America follows the Japanese system of cryptocurrency regulation closely. However, a noticeable difference is a layered approach to regulation whereby states are free to regulate these matters themselves at the state (provincial) level, in addition to a federal oversight acting as a safety net to state regulation. The federal oversight is very similar in its regulation to Japan in that it requires the registration of traders and enforces strict accounting laws and principles. In addition to the layered approach, the US also makes use of specialised units with proper training and knowledge in cybersecurity. These units, such as the IRS Cybercrime Unit, have a proven track record of success, as evidenced by the *United States of America v Ilya Lichtenstein and Heather Rhiannon Morgan* case, and are essential for any nation to provide a safe e-commerce experience for its residents.

The European Union emphasises cryptocurrency regulation through a strict approach against money laundering. The Anti-money Laundering Directives of the EU have recently been amended to include virtual currencies. The EU has also empowered Financial Intelligence Units to have wide oversight powers to monitor suspected transactions even before any fraudulent activity occurs. In addition to the wide power given to regulators, the EU periodically reviews its action plan on anti-money laundering legislation and directives. In this way, the EU aims to stay one step ahead of potential new threats and technological advancements, thereby avoiding exploiting any possible loopholes.

If South Africa were to apply these principles into its law, a higher level of authority would have to be given to regulators such as the FSCA. The FSCA would have to be empowered to launch investigations into suspicious activities. All cryptocurrency merchants would have to submit their annual reports to the FSCA. In theory, such authority might be a strong deterrent to cybercrime related to cryptocurrency. However, in practice, it might lead to a few issues. The scope of the power given to the FSCA cannot be unfettered. It would have to work on the existing system of checks and balances. Furthermore, POPIA-considerations would have to be applied to such authority. Nonetheless, practical considerations aside, the methods of regulation used in Europe would be strong normative examples for South Africa to follow if it were to impose a regulatory structure on the domestic cryptocurrency trade.

Therefore, what can be learned from the narrow perspective on cryptocurrency regulation as it affects cybercrime, is that each nation takes a strict approach to regulation. The countries recognise cryptocurrency as some form of monetary tender. They therefore apply the same financial laws and principles to it as they would to any other. Registration of traders of cryptocurrency is required. A common similarity among all the countries is that a wide power of authority is given to watchdogs and specialised units to enforce the applicable financial rules and principles as well as launch investigations into suspicious transactions.

The primary international perspective is that although international law has not completely been codified to enforce specific regulation on cyber-security and cryptocurrency fraud, there is a movement in favour thereof. Further, the *Budapest Convention* is being amended continuously to keep up with the latest technological developments. The international movement favours the tandem co-operation of states to prosecute cybercriminals successfully and to overcome the jurisdictional and geographical boundaries to prosecution. Furthermore, on a domestic level, states are moving toward an all-encompassing approach wherein financial intelligence oversight authorities are given a wide range of power to investigate all matters relating to

cryptocurrency. This power ranges from the enforcement of submission of annual reports on one end to probing suspicious transactions on the other. Additionally, the prevalence of specialised investigative units is at the core of the fight against online fraud in e-commerce. These units need to employ the latest technological trends and principles to prosecute perpetrators. South African legislatures would be wise to learn from the normative examples given both in international law as well as foreign law.

What South Africa can take cognisance of, is that the recognition of cryptocurrency cannot be ignored. Recognition will lead to the regulation thereof. It has to be given due recognition for financial laws to attach to it and for oversight authorities such as the FSCA to gain jurisdiction over cryptocurrency transactions. Further, that accounting laws and principles be enforced upon traders of cryptocurrency. In addition, specialised units working for government authorities need to be established to monitor and investigate any committed or potential cybercrime which may stem from cryptocurrency transactions. Finally, a periodic review of the regulatory framework is required to assess whether amendment would be required to keep up to date with the latest trends and practices employed by cybercriminals. South Africa, as a signatory to the *Budapest Convention,* should also employ the latest directives published in accordance therewith. This includes giving its co-operation to other states in investigations under the *Second Additional Protocol*. Therefore, the South African legislature would be wise to incorporate the normative examples from the international practices above into its future regulatory framework.

Chapter 5: The South African Perspective

5.1 Introduction

The previous chapters explored the concepts related to cryptocurrency regulation and how cybercrime legislation can play a role therein, all within the context of e-commerce. Furthermore, chapter 4 examined the international legal community's response to these concepts to determine whether South Africa can use some of these practices in its regulatory framework. This chapter will examine the South African legal framework on cybercrime and financial regulation related to cryptocurrency. This chapter will look to what extent the South African legal framework can provide a basis to deal with cryptocurrency through cybercrime (and financial) legislation in e-commerce. To do this, the development of cybercrime regulation in South Africa will be considered. The current position on both cryptocurrency and cybercrime will also need to be examined. Furthermore, the influence of other regulatory statutes such as FICA, POPIA, etcetera, must be considered to form a holistic view of the South African position. Only once the complete picture has been established, is it possible to determine how the South African legal framework deals with the issue compared to the international framework set out in the previous chapter.

5.2 Preliminary Legal Framework

The preceding chapters of this work attempted to define the concepts of cybercrime and cryptocurrency.[357] The following chapter endeavoured to better understand how cybercrime legislation can affect cryptocurrency regulation.[358] Finally, the international legal fraternity's response to these issues was also examined.[359] Attention will now be turned to the South African response to these issues.

---

357 See chapter 2 of this work.
358 See chapter 3 of this work.
359 See chapter 4 of this work.

As explained earlier, cryptocurrency is not centrally regulated in South Africa.[360] However, South Africa does have a legal framework for cybercrime.[361] Therefore, the moment that online fraud occurs with cryptocurrency, be it as a means to an end or the target itself, cybercrime laws will take effect and thereby provide the legal framework for the situation. Thus, examining the legal framework for cybercrime may provide valuable insight into cryptocurrency regulation in South Africa.

In light of the above, a discussion on the preliminary legal framework for cybercrime will follow.

5.2.1 The Common Law Position

Snyman highlights that the common law is one of South Africa's main sources of criminal law.[362] Accordingly, cognisance must be given to the common law in any discussion on criminal law in South Africa. As regards cybercrime, Schultz is of the opinion that at its core, the principles of common-law theft still apply, even in instances of cybercrime.[363] However, both Schultz and Kuoamo submit that the effectiveness of wide interpretations of the common law is inadequate to prosecute online crimes successfully.[364] Therefore, the common law may help provide the point of departure as common law crimes such as theft and fraud are committed in cybercrime. However, the common law lacks the necessary depth to regulate online crime effectively.

Snyman builds on this point by iterating that the influence of the common law and its Roman-Dutch roots is on the decline in South African criminal law.[365] He gives two main reasons for this reality. Firstly, he is of the opinion that courts have already

---

360 See chapter 3 of this work.
361 See chapter 5.3 below.
362 Snyman *Criminal Law* 5. Even though the common law has to a large extent been codified into case law, it remains an important source of law in South Africa.
363 Schultz 2016 *Cybercrime: An Analysis of Current Legislation in South Africa* 13.
364 Schultz 2016 *Cybercrime: An Analysis of Current Legislation in South Africa* 13; Kouamo *Combating Crime in International Electronic Commerce* 47.
365 Snyman *Criminal Law* 7.

extracted all the necessary rules and principles and reapplied them in other avenues such as case-law and practice directives.[366] Secondly, the advancement of technology has rendered many of the common-law principles outdated and thus moot.[367] Therefore the common law has lost its influence as the main source of criminal law, especially in the technologically orientated society of today.

Nevertheless, even in light of the above, the main principles at their core still function as a point of departure and the legislature should give them the necessary consideration.[368] However, this position will only apply insofar as it is consistent with the Constitution.[369] Van der Merwe *et al* add to this by noting that the Constitutional principle of legality, also known as *nullum crimen sine lege,* determines that the definitions of common law crimes cannot be moulded to fit an "offence" if such conduct was not previously criminalised.[370] They also emphasise that the Constitution obliges courts to develop the common law in line with the Bill of Rights.[371]

Therefore, even though the common law has laid the foundation for criminal law rules and principles, it has lost most of its direct influence in that most of its power has been extracted into other avenues. It has also failed to keep up with the modernisation of technology. Furthermore, its application is limited by Constitutional principles. Thus, the common law may act as a symbolic point of departure and cognisance should be given to it as it relates to crimes such as theft and fraud. However, its direct force and influence are limited.

366 Snyman *Criminal Law* 7.
367 Snyman *Criminal Law* 7.
368 Botha *Statutory Interpretation* 43-44.
369 *Pharmaceutical Manufacturers Association of South Africa: In re Ex Parte President of the Republic of South Africa* (CCT31/99) [2000] ZACC 1; 2000 (2) SA 674; 2000 (3) BCLR 241 (25 February 2000) para 44.
370 Van der Merwe *et al Information and Communications Technology Law* 79.
371 Van der Merwe *et al Information and Communications Technology Law* 79.

5.2.2 ECTA

The *Electronic Communications and Transactions Act* 25 of 2002 sets the basis for regulating electronic-based communication and dealings.[372] Sections 85-89 expressly deal with cybercrime and its regulation.[373] Section 86 of the Act criminalises the unlawful interference, alteration, interception and access to data.[374] As explained above, this section functions as a catch-all provision for all forms of cybercrime, as all the forms of cybercrime would, in one way or the other, fit within the scope of the section.[375] Section 87 builds on this by further criminalising the online fraud that may follow from the unlawful actions described in section 86.[376] Therefore, where section 86 would criminalise, for instance, the hacking into a cryptocurrency wallet under the element of unlawful access, section 87 would criminalise the extortion of the original owner thereof. Section 88 of the Act criminalises any forms of attempt or aiding and abetting of the actions set out in section 86.[377] Finally, section 89 imposes the penalties for the contravention of the preceding sections.[378] The chapter on cybercrime in ECTA is brief but effective as it provides an all-inclusive approach to regulating cyber-offences. It describes what would constitute a cybercrime. It then proceeds to criminalise fraud emanating from such crime and any attempt, aiding and abetting.

Van der Merwe notes that the provisions of ECTA are wide enough to fit the various forms of cybercrime,[379] however, he is critical of section 89 and argues that the penal provisions are not heavy enough to deter would-be cybercriminals.[380] He is also critical of the wording of the sections, which continually refer back to section 86, instead of

372 Kouamo *Combating Crime in International Electronic Commerce* 50.
373 Chapter 13 of the *Electronic Communications and Transactions Act* 25 of 2002.
374 Section 86 of the *Electronic Communications and Transactions Act* 25 of 2002.
375 See 2.3.1.3 of this work.
376 Section 87 of the *Electronic Communications and Transactions Act* 25 of 2002.
377 Section 88 of the *Electronic Communications and Transactions Act* 25 of 2002.
378 Section 89 of the *Electronic Communications and Transactions Act* 25 of 2002.
379 Van der Merwe 2007 *THRHR* 313-318.
380 Van der Merwe 2007 *THRHR* 319.

merely stating "unlawful, interference, access, etcetera."[381] The wording of the sections makes sense from a continuity standpoint. However, the danger of referring back to section 86 lies in the fact that should a new form of cybercrime come to the fore which does not neatly fit into one of the provisions of section 86, a *lacuna* may arise. However, the same can be said for Van der Merwe's alternate proposal to the wording of the sections, as both section 86 and his proposed wording in effect come down to the same interpretation of the particular section, which is the criminalisation of the unlawful interference, access, alteration and interception of data.

In light of Van der Merwe's criticism of the penal provisions, Kouamo similarly argues that the penal provisions are not severe enough, especially in light of those in RICA.[382] She compares section 51 of RICA to section 89 of ECTA, wherein ECTA prescribes imprisonment of up to 5 years at its harshest, whereas RICA doubles the possible term of imprisonment to up to 10 years.[383] Van der Merwe and Kuoamo are justified in their concerns about the penal provisions of ETCA. The influx of cybercrime indicates that the possible penalties for committing cybercrimes are insufficient to deter would-be transgressors. However, Snyman argues that as regards the general theory of deterrence, it is not only the severity of a possible punishment that deters would-be offenders, but also the likelihood of being caught, convicted and accordingly sentenced.[384] Therefore, the penalties imposed by the Act itself are not the only factor required to deter would-be cybercriminals, but also the stringent implementation by law enforcement authorities and the likelihood that this would lead to a prosecution and subsequent conviction.

---

381 Van der Merwe 2007 *THRHR* 319.

382 Kouamo *Combating Crime in International Electronic Commerce* 51; *Regulation of Interception of Communications and Provision of Communication Related Information Act* 70 of 2002. See 5.2.4 below for a full discussion on RICA.

383 Kouamo *Combating Crime in International Electronic Commerce* 51; S89 of the *Electronic Communications and Transactions Act* 25 of 2002; S51 of the *Regulation of Interception of Communications and Provision of Communication Related Information Act* 70 of 2002.

384 Snyman *Criminal Law* 16.

From the above it can be established that ECTA was an important step in addressing cybercrime in South Africa. The sections on cybercrime were written in broad terms to include all forms of cybercrime and all actions flowing from the original commission of the crime. However, as seen above, the success of a penal provision lies in its implementation and enforcement. Further, it may be time for a redress with the Act nearing two decades in age.[385] Nevertheless, the importance of the Act cannot be overstated, as it provided the foundation for cyber-security law and regulation in South Africa.

5.2.3 FICA

The *Financial Intelligence Centre Act* 38 of 2001 was established to supplement the *Prevention of Organised Crime Act* 121 of 1998 to, *inter alia,* combat money laundering activities and terrorism financing.[386] One of the main objectives of FICA is to establish the Financial Intelligence Centre.[387] The principal aim of the Financial Intelligence Centre is to identify the origin of transactions to detect whether the proceeds thereof are from unlawful activities.[388] Section 3 of FICA states that:

> The principal objective of the Centre is to assist in the identification of the proceeds of unlawful activities and the combating of money laundering activities.[389]

FICA operates to regulate financial activities and, in this way, prevent money laundering.[390] It establishes regulatory principles such as effective client identification, record-keeping standards, compliance requirements and the like, all in a bid to create a legal framework for financial transactions to be traceable.[391] In addition to the regulatory principles imposed, FICA also provides for information kept by the Financial

385 Mpuru 2017 *Servamus Community-based Safety and Security Magazine* 45.
386 Preamble of the *Financial Intelligence Centre Act* 38 of 2001.
387 Orffer *The Inclusion of Virtual Currencies in the Calculation of Income Tax* 54.
388 Orffer *The Inclusion of Virtual Currencies in the Calculation of Income Tax* 54.
389 Section 3(1) of the *Financial Intelligence Centre Act* 38 of 2001.
390 Hlongoane *Access to Information Held by the Financial Intelligence Centre* 2.
391 Hlongoane *Access to Information Held by the Financial Intelligence Centre* 3.

Intelligence Centre to be shared with regulatory and investigative authorities.[392] Thus, FICA provides an oversight authority to regulate financial transactions to prevent money laundering.

For FICA to be effective in its principal aims, it places a duty on what it calls "accountable institutions". Schedule 1 of the Act lists accountable institutions, including attorneys, trustees, bankers, stockbrokers, real estate agents, accountants and many others.[393] The common trait between these institutions is that they deal with monetary transactions. These institutions are also obligated to subscribe to know-your-client (KYC) requirements.[394] Failure to keep a proper record of their clients and customers can lead to prosecution for the institution under FICA.[395] This duty places the obligation on the accountable institution to ensure the transactions they process are from legitimate sources. In this way, money laundering is curbed.

Snail ka Mtuze highlights that in order to comply with anti-money laundering legislation, as it stands, cryptocurrency exchangers will have to register in terms of FICA and comply with the duties of accountable institutions.[396] Certain exchanges are registered under FICA.[397] However, according to Orffer, the duty on a cryptocurrency exchange as an accountable institution is unclear, given that cryptocurrency exchanges are not listed in schedule 1 of FICA as accountable institutions.[398]

FICA may be of great use to the South African legislature in addressing money laundering (and other cybercrimes) through cryptocurrency. For regulation through FICA, a duty would have to be placed on cryptocurrency traders and exchanges by listing them as accountable institutions in terms of Schedule 1. This would mean

---

392 Hlongoane *Access to Information Held by the Financial Intelligence Centre* 3.
393 Schedule 1 of the *Financial Intelligence Centre Act* 38 of 2001.
394 Section 21 of the *Financial Intelligence Centre Act* 38 of 2001.
395 Orffer *The Inclusion of Virtual Currencies in the Calculation of Income Tax* 54.
396 Papadopoulos and Snail ka Mtuze *Cyberlaw* 69.
397 Orffer *The Inclusion of Virtual Currencies in the Calculation of Income Tax* 55.
398 Orffer *The Inclusion of Virtual Currencies in the Calculation of Income Tax* 55; Schedule 1 of the *Financial Intelligence Centre Act* 38 of 2001.

cryptocurrency exchanges would be obligated to ascribe to know-your-client requirements, thereby relinquishing the anonymity issues that stem from cryptocurrency transactions. Furthermore, these traders would be required to report their annual statements to the Financial Intelligence Centre, which may provide support to law enforcement agencies when investigating suspicious transactions. Therefore, with a few changes, FICA may be useful in providing a legal framework for cryptocurrency in South Africa.

5.2.4 RICA

Another significant statute in the regulation of the e-commerce sphere is the *Regulation of Interception of Communications and Provision of Communication Related Information Act* 70 of 2002, also known as RICA.[399] According to Schultze, RICA provides the legislative basis for a justifiable limitation to section 14 of the Constitution's right to privacy.[400] RICA provides that no person, who is not a party to a conversation or who lacks the requisite authority may intercept, interfere or procure any electronic communication in the course of its occurrence between other parties.[401] RICA is a statute that provides authority to monitor or intercept electronic communication in certain instances. Section 51 of the Act criminalises any communication interception, not falling within the specified exceptions.[402] Therefore, similar to ECTA, the unauthorised interception of data constitutes a cybercrime, notwithstanding the means employed to achieve this interception.

Section 2 of RICA places a blanket ban on communication interception unless specified exceptions are complied with.[403] Schultz mentions that the Act's object is to authorise

---

399 Schultz 2016 *Cybercrime: An Analysis of Current Legislation in South Africa* 16.
400 Schultz 2016 *Cybercrime: An Analysis of Current Legislation in South Africa* 16.
401 Section 2 of the *Regulation of Interception of Communications and Provision of Communication Related Information* Act 70 of 2002.
402 Section 51 of the *Regulation of Interception of Communications and Provision of Communication Related Information Act* 70 of 2002.
403 Section 2 of the *Regulation of Interception of Communications and Provision of Communication Related Information Act* 70 of 2002.

law enforcement agencies to identify the users of mobile phones and track criminal activities employing the use of mobile phones.[404] This regulatory power is similar to those given to oversight authorities in Japan and the EU. If used effectively, this power may be a strong deterrent to the unlawful interception of communication.

Further, section 47 empowers authorities to admit into evidence any intercepted communication in terms of, *inter alia,* criminal proceedings brought under the *Prevention of Organised Crimes Act* 121 of 1998.[405] It states that:

> Information regarding the commission of any criminal offence, obtained by means of any interception or the provision of any real-time or archived communication related information, under this Act, or any similar Act in another country, may be admissible as evidence in criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act.[406]

In the context of cryptocurrency, RICA finds its application as any communication regarding safeguarding cryptocurrency wallets, blockchains, mining software, etcetera, is also protected from unlawful interference. Therefore, should unlawful interference again be used as a means to an end, with the end being unlawful access to cryptocurrency, RICA would apply.

However, on 4 February 2021, RICA was declared unconstitutional by the Constitutional Court in *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services.*[407] RICA was challenged by the Appellants on the grounds that it did not provide the subject of interference from law

---

404 Schultz 2016 *Cybercrime: An Analysis of Current Legislation in South Africa* 16.

405 Section 47 of the *Regulation of Interception of Communications and Provision of Communication Related Information Act* 70 of 2002.

406 Section 47(1) of the *Regulation of Interception of Communications and Provision of Communication Related Information Act* 70 of 2002.

407 *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others* (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) (4 February 2021).

enforcement with notification of such interference;[408] that it provides a member of the Executive an unfettered discretion to appoint a judge to issue directives in terms of RICA, thus providing an independence issue;[409] RICA does not provide safeguards for the sharing and storing of the information obtained during surveillance;[410] RICA does not provide special circumstances where the subject of the surveillance is an attorney or journalist.[411]

The question before the court was whether there are enough safeguards in place to the authority given to law enforcement agencies under RICA to be a justifiable limitation to the right of privacy.[412]

The Court held that the interception and surveillance of an individual's communication is a highly invasive infringement on the individual's right to privacy and is thus inconsistent with section 14 of the Constitution.[413] The Court thus declared RICA unconstitutional with a suspension of the order for three years to allow the national legislature to rectify the identified issues.[414] Furthermore, the Court provided,

---

408 *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others* (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) (4 February 2021) para 16.

409 *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others* (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) (4 February 2021) para 17.

410 *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others* (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) (4 February 2021) para 18.

411 *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others* (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) (4 February 2021) para 19.

412 Ongeso and Dyer 2021 https://www.bowmanslaw.com/insights/mergers-and-acquisitions/south-africa-constitutional-court-upholds-declaration-of-invalidity-of-rica/.

413 Ongeso and Dyer 2021 https://www.bowmanslaw.com/insights/mergers-and-acquisitions/south-africa-constitutional-court-upholds-declaration-of-invalidity-of-rica/; S14 of the *Constitution of the Republic of South Africa*, 1996.

414 Ongeso and Dyer 2021 https://www.bowmanslaw.com/insights/mergers-and-acquisitions/south-africa-constitutional-court-upholds-declaration-of-invalidity-of-rica/.

notwithstanding the suspension of the order, that persons subject to surveillance under RICA be notified thereof[415] and that attorneys and journalists are awarded special protection under RICA.[416]

Even though RICA is flawed from a constitutional standpoint as it infringes too greatly on the right to privacy, its point of departure does have a basis to justify its existence. The intention of the legislature was to give authority to law enforcement agencies in order to intercept communication that could be linked to criminal transgressions, wherein cybercrime was given sufficient consideration. Therefore, at its core, RICA should be a commendable effort from South African lawmakers. Cybercrime, due to its lack of geographical confinement, is inherently difficult to prosecute. Therefore, allowing authorities to track and intercept possible communication among cybercriminals is an essential step to eventual prosecution. This would include the interception of illicit cryptocurrency transactions. Therefore, the South African legislature would be wise to rectify the constitutional issues identified by the court to retain RICA as a statute under South African law.

5.2.5 Prevention of Organised Crimes Act

The *Prevention of Organised Crimes Act* 121 of 1998 was enacted to, *inter alia,* criminalise money laundering activities, prevent certain gang-related activities and provide methods for the recovery of the proceeds of unlawful activity.[417] Kersop highlights that the *Prevention of Organised Crimes Act* is the main statutory source criminalising money laundering activities in South Africa.[418] POCA is to be used in

415 A post-surveillance notification requirement be read into the existing sections.
416 Ongeso and Dyer 2021 https://www.bowmanslaw.com/insights/mergers-and-acquisitions/south-africa-constitutional-court-upholds-declaration-of-invalidity-of-rica/.
417 Preamble of the *Prevention of Organised Crimes Act* 121 of 1998.
418 Kersop *Anti-money laundering regulations and the effective use of mobile money in South Africa* 25.

conjunction with FICA for a full picture of the anti-money laundering legislation in South Africa.[419]

According to Kersop, POCA, among others, establishes the broad criminalisation of money laundering whilst FICA is, *inter alia*, used to implement measures for the prevention thereof.[420] Therefore, this subsection will examine whether the main South African source of money laundering legislation may provide for a regulatory measure related to cryptocurrency.

To determine whether cryptocurrency and its role in money laundering will be subject to the Act, one must examine its various definitions. The definition of unlawful proceeds is relevant here. The definition states the following:

> "Proceeds of unlawful activities", means any property or part thereof or any service, advantage, benefit or reward which was derived, received or retained, directly or indirectly, in connection with or as a result of any unlawful activity carried on by any person, whether in the Republic or elsewhere…... and includes property representing property.[421]

The definition refers explicitly to property derived as a result of unlawful activities as opposed to money. In light hereof, examining the definition of property within the Act is also necessary. The Act defines property as follows:

> "property" means money or any other movable, immovable, corporeal or incorporeal thing and includes any rights, privileges, claims and securities and any interest therein and all proceeds thereof.[422]

The keyword in the definition of property is incorporeal thing.[423] This would be wide enough to include cryptocurrency, as cryptocurrency is an incorporeal form of

---

419 Kersop *Anti-money laundering regulations and the effective use of mobile money in South Africa* 25.

420 Kersop *Anti-money laundering regulations and the effective use of mobile money in South Africa* 25.

421 Section 1 of the *Prevention of Organised Crimes Act* 121 of 1998.

422 Section 1 of the *Prevention of Organised Crimes Act* 121 of 1998.

423 Although reference is made to an incorporeal thing, it may be assumed to include incorporeal property. According to Van der Walt and Pienaar the most important categories of property are

property.[424] Therefore, it would be equated to intangible property representing property rights and interests.

Erlank affirms this position by noting that, in line with international case law,[425] where digital assets have a value attached, be it sentimental or financial, it will be capable of being subject to the rules and principles under property law. What's key from Erlank's discussion is the word "digital asset" as opposed to "digital property".[426] He highlights that the term digital asset would even extend beyond the natural parameters of traditional property law and would rather be akin to "asset" in the sense of estate law wherein anything that adds to the value of the deceased estate is regarded as an asset.[427] Therefore, according to this position cryptocurrency is an asset that would extend a person's patrimony and should accordingly be regarded as property in terms of section 1 of POCA.

Recent developments by the South African legislature seem to agree on this position. Currently, section 1 of the *Protection of Constitutional Democracy Against Terrorist and Related Activities Act* 33 of 2004, shares the definition of "property" verbatim with the definition thereof in section 1 of POCA.[428] However, on 19 July 2022, an Amendment Bill was introduced to Parliament.[429] Section 1(n) of the *Protection of Constitutional Democracy Against Terrorism and Related Activities Amendment Bill* reads as follows:

> by the substitution in subsection (1) for the definition of "property" of the following definition: "property" means money or any other movable, immovable, corporeal or

---

corporeal things as well as incorporeal rights and interests i.e., things. Van der Walt and Pienaar *Introduction to the Law of Property* 9.

424 Van der Merwe *et al Information and Communications Technology Law* 653-657.

425 *Bragg v Linden Research Inc.*, 487 F.Supp.2d 593 E.D.Pa 2007; *Li Hong Chen v Beijing Arctic Ice Technology Development Company* (2003, Beijing Second Intermediate Court). Van der Merwe *et al Information and Communications Technology Law* 649-653.

426 Van der Merwe *et al Information and Communications Technology Law* 654.

427 Van der Merwe *et al Information and Communications Technology Law* 654.

428 Section 1 of the *Protection of Constitutional Democracy Against Terrorist and Related Activities Act* 33 of 2004.

429 Parliament of the RSA 2022 https://www.parliament.gov.za/bill/2304183.

> incorporeal thing, and includes any rights, privileges, claims and securities and any interest therein and all proceeds thereof, or any digital representation of perceived value, such as a crypto-currency, that can be traded or transferred electronically within a community of users of the internet who consider it as a medium of exchange, unit of account, or store of value and use it for payment or investment purposes, but does not include a digital representation of a fiat currency or a security as defined in the Financial Markets Act 19 of 2012.[430]

The definition is expressly expanded to include, *inter alia,* cryptocurrency as property. Even though the *Bill* is in its early stages of development, this is a reflection of the legislature's attitude toward cryptocurrency regulation[431]. This amendment showcases the legislature's willingness to create a regulatory framework for cryptocurrency and to have cryptocurrency afforded protection under cyber and commercial laws. With the definition in the *Protection of Constitutional Democracy Against Terrorist and Related Activities Act* potentially being expanded, this may also pave the way to have the definition under POCA expanded since both statutes share the same definition of property.

What can be seen from the broad definitions in POCA as well as the position of cryptocurrency as a digital asset, is that the current position on cryptocurrency is sufficiently wide enough to include it as an object of money laundering. The *Protection of Constitutional Democracy Against Terrorism and Related Activities Amendment Bill* also showcases that the legislature is willing to let cryptocurrency be included as an object of money laundering. Therefore, even though there is no central regulation of cryptocurrency yet, the use thereof to conceal proceeds from illicit gain is already outlawed and, thus, regulated. This again highlights that the cybercrime legal framework is in place to regulate the misuse of cryptocurrencies.

---

430 Section 1(n) of the *Protection of Constitutional Democracy Against Terrorism and Related Activities Amendment Bill* (B15-2022).

431 However, the *Bill* has been criticised for lacking clarity, in that it defines "terrorism" too broadly. This creates the danger that protesting government action, or even just criticising government may be likened to terrorist activity. It is to be seen whether the vagueness is addressed by the legislature. Ryan 2022 https://www.moneyweb.co.za/moneyweb-crypto/controversial-bill-aims-to-clamp-down-on-crypto-for-terrorism-financing/.

5.3 Cybercrimes Act

From the above, it can be seen that the current legislative framework on cybersecurity is wide and uses several statutes to work in tandem. Briefly, the common law provides the basis for regulating cyber issues. This is because when stripped down to its most basic form, cyber-offences can be equated to common-law crimes such as theft, malicious injury to property or fraud.

ECTA was later established to codify the South African position on cybercrime by shifting the focus to unlawful access, interception or interference with data. POCA and FICA operate simultaneously to regulate, amongst others, money laundering activities, including money laundering via e-commerce platforms. Further, RICA, although constitutionally questionable, enables law enforcement to intercept communication which may be linked to any of the cyber-offences mentioned throughout the listed Acts.

The above is a summary of the main sources regulating e-commerce and the issues that may stem from it. ECTA is the focal point for cyber-offences as it codified the South African position on cybercrime. However, given its advancing age and the rapid development of technology, the South African legislature thought it wise to revise the legislative position on cybercrime and enacted the *Cybercrimes Act* 19 of 2020.[432]

Watney notes that the principal aim of the legislature in enacting the *Cybercrimes Act* was to create new offences for cyber-transgressions as well as to modernise how existing cyber-offences are dealt with.[433] The principal objectives of the Act are to establish further offences and penal sanctions over cybercrime; to criminalise the spreading of harmful data communications and messages and to give law enforcement agencies the requisite authority to properly investigate cyber-offences.[434] Therefore,

---

[432] Burger-Smidt 2021 https://www.werksmans.com/legal-updates-and-opinions/your-actions-in-cyberspace-can-land-you-in-prison/; *Cybercrimes Act* 19 of 2020.

[433] Papadopoulos and Snail ka Mtuze *Cyberlaw* 477.

[434] Papadopoulos and Snail ka Mtuze *Cyberlaw* 477.

the *Cybercrimes Act* aims to modernise the South African legal framework on cyber-offences whilst also empowering law enforcement to properly investigate such offences, which would expectantly lead to higher levels of prosecution.

Section 2(1) of the *Cybercrimes Act* creates the offence of cybercrime and reads as follows:

> (1) Any person who unlawfully and intentionally performs an act in respect of—
>
> (a) a computer system; or
>
> (b) a computer data storage medium,
>
> which places the person who performed the act or any other person in a position to commit an offence contemplated in subsection (2), section 3(1), 5(1) or 6(1), is guilty of an offence.[435]

This subsection sets the basis of the commission of cybercrime whilst also referring to other sections[436] that make provision for the specific commissio or omissio to enable the crime to occur. Subsection (2) gives effect to unlawful access of data. It provides:

> (2) (a) Any person who unlawfully and intentionally accesses a computer system or a computer data storage medium, is guilty of an offence.
>
> (b) For purposes of paragraph (a)—
>
> (i) a person accesses a computer data storage medium, if the person—
>
> (aa) uses data or a computer program stored on a computer data storage
>
> medium; or
>
> (bb) stores data or a computer program on a computer data storage
>
> medium; and
>
> (ii) a person accesses a computer system, if the person—
>
> (aa) uses data or a computer program held in a computer system;

---

435 Section 2(1) of the *Cybercrimes Act* 19 of 2020.

436 Sections 2(2), 3(1),5(1) and 6(1) of the *Cybercrimes Act* 19 of 2020.

(bb) stores data or a computer program on a computer data storage medium forming part of the computer system; or

(cc) instructs, communicates with, or otherwise uses, the computer system.

(c) For purposes of paragraph (b)—

(i) a person uses a computer program, if the person—

(aa) copies or moves the computer program to a different location in the computer system or computer data storage medium in which it is held or to any other computer data storage medium;

(bb) causes a computer program to perform any function; or

(cc) obtains the output of a computer program; and

(ii) a person uses data, if the person—

(aa) copies or moves the data to a different location in the computer system or computer data storage medium in which it is held or to any other computer data storage medium; or

(bb) obtains the output of data.[437]

Section 2(2)(a) of the Act expressly states that unlawful access to a computer or computer system is an offence. Sections 2(2)(b) and 2(2)(c) go on to describe what is meant by unlawful access and how unlawful access is obtained. This subsection thoroughly sets out the grounds on which an act can constitute cybercrime. It provides that if data is, in any way, unlawfully accessed, breached, used or obtained, such action will constitute cybercrime. This sets up the legal basis that data (as defined) deserves legal protection and that any person who gains entry to such data when

[437] Section 2(2) of the *Cybercrimes Act* 19 of 2020.

he/she is not the lawful owner or holder of a right in respect of that data, has committed an offence.

Whilst section 2(2) provides for cybercrime actions involving the unlawful access of data, section 3(1) gives effect to the unlawful interception of data. This section states:

> (1) Any person who unlawfully and intentionally intercepts data, including electromagnetic emissions from a computer system carrying such data, within or which is transmitted to or from a computer system, is guilty of an offence.[438]

Section 3(1) of the Act provides that any unlawful interception of computer data shall be an offence and constitute the commission of a cybercrime. Section 3(4) of the Act sets the grounds for unlawful interception. It provides that any form of viewing, capturing or copying by any kind of device, be it those contemplated in section 4(2)[439] or any other, of another's data to make it available to any other person other than the lawful owner or holder of such data, shall constitute the unlawful interception of data.[440] This section builds on section 2, as it criminalises the unlawful access to data and criminalises the unlawful interception. This means that even if, for example, someone merely intercepts data without opening it and passes it on to another against (illicit) payment, such a person would also be guilty of an offence. Therefore, any form of middleman in the transaction would also be implicated in the process.

The above sections deal with the unlawful access of data and the unlawful interception of data, respectively. Section 5(1) refers to the unlawful interference with data or with a computer program. It reads as follows:

> (1) Any person who unlawfully and intentionally interferes with—
>
> (a) data; or
>
> (b) a computer program,

---

438 Section 3(1) of the *Cybercrimes Act* 19 of 2020.

439 Section 4(2) of the *Cybercrimes Act* 19 of 2020. This section sets out the forms of hardware and/or software tools which can be used in the furtherance of unlawful acts in terms of the Act.

440 Section 3(4) of the *Cybercrimes Act* 19 of 2020.

is guilty of an offence.[441]

This section is to the point in its aims. It states that an offence is committed when data or a computer program is unlawfully interfered with. Section 5(2) lists ways in which data or a computer program may be interfered with. Briefly, it mentions that deletion, alteration, damage, obstruction or encoding of data or computer programs are ways in which the offence of unlawful interference is committed.[442]

Section 6(1) of the Act is closely related to section 5 in criminalising unlawful interference.[443] The difference is the object of the interference. Section 5 focuses on data and computer programs, whilst section 6 regulates the unlawful interference with computer data storage mediums and/or computer systems. Similar to section 5(2), section 6(2) also sets out how unlawful interference can occur. Section 6 of Act 19 of 2020 reads as follows:

(1) Any person who unlawfully and intentionally interferes with a computer data storage medium or a computer system, is guilty of an offence.

(2) For purposes of this section "interfere with a computer data storage medium or a computer system" means to permanently or temporarily—

(a) alter any resource; or

(b) interrupt or impair—

(i) the functioning;

(ii) the confidentiality;

(iii) the integrity; or

(iv) the availability,

of a computer data storage medium or a computer system.[444]

---

441 Section 5(1) of the *Cybercrimes Act* 19 of 2020.
442 Section 5(2) of the *Cybercrimes Act* 19 of 2020.
443 Section 6(1) of the *Cybercrimes Act* 19 of 2020.
444 Section 6 of the *Cybercrimes Act* 19 of 2020.

What is evident from this section is that it expands the offence of unlawful interference from data at its baseline to a more expansive offence in that it criminalises any kind of action (or non-action) which would result in the unlawful interference with the storage mediums or networks by which data is saved or transferred. This allows for deeper legal protection to users, as their data itself is protected, and the instruments upon which they house their data are also protected.

Thus sections 2, 3, 5 and 6 of the Act exist to create the offences related to any form of access, interception or tampering with any form of data or computer storage medium. Therefore, in South African law, cybercrime can be defined as any offence involving unlawful access, unlawful interception, or unlawful interference with data or computer networks by a party unauthorised by law to do so.

From the above, it is evident that the relevant sections of the *Cybercrimes Act* correlate in many respects with sections 86-89 of ECTA. The basic point of departure is that a cyber-offence is committed when data is unlawfully accessed, altered or intercepted. However, the strength of the *Cybercrimes Act* lies in the fact that it builds upon these concepts to further regulate other offences that may or may not be committed in connection with the unlawful access, alteration or interception of data. Furthermore, it casts a wider net of protection to include not only data as the object of the offence, but also computer programs and systems.

In line with the discussion on ECTA, the *Cybercrimes Act* would also apply to the unlawful access, alteration or interception of data where the data in question (or article as per section 1)[445] relates to cryptocurrency. Therefore, the Act would act as a form of legal regulation for cryptocurrency commerce. Further, it would allow aggrieved persons to take recourse by relying on law enforcement officials to investigate matters where cryptocurrency has been either the tool or the target of cybercrime.

[445] Section 1 of the *Cybercrimes Act* 19 of 2020.

Additionally, section 1 of the *Cybercrimes Act* defines a person as a natural and juristic person.[446] This means that the Act applies to natural persons, companies and other juristic entities.[447] The implication is that companies and ordinary people may benefit from the protections afforded by the Act. Conversely, companies and ordinary people may also be prosecuted in terms of the Act.

An interesting question arises when examining sections 14 and 15 of the Act. Section 14 of the *Cybercrimes Act* criminalises the use of electronic communications to incite violence against the property belonging to another.[448] Section 15 criminalises the use of electronic communication to threaten damage against property belonging to another. These may seem like all-inclusive provisions, but where does this leave cryptocurrency? As seen in the preceding chapters, cryptocurrency is an incorporeal form of property. The question then arises: would these sections apply to violence being incited/threatened against a cryptocurrency wallet? The Act itself does not define property. Does disseminating a message to another to incite or threaten violence on a digital basis against a cryptocurrency platform constitute violence against property as per sections 14 or 15? Or would it fall under the other cybercrime sections, such as unlawful alteration?

The rules of statutory interpretation state that the words of a section, if unclear, need to be weighed up against the context of the legislation as a whole.[449] The above points out that the modernisation of existing cybersecurity rules was one of the main aims of the Act. Modernisation and protection of digital data and assets gave rise to the Act in the first place.[450] Given the fact that the focus of the Act is to protect digital assets, it

---

446 Section 1 of the *Cybercrimes Act* 19 of 2020.

447 Bhagattjee *et al* 2021 https://www.cliffedekkerhofmeyr.com/en/news/publications/2021/TMT/technology-media-and-telecommunications-sector-newsletter-9-june-regulating-the-fourth-industrial-revolution-south-africas-cybercrimes-bill-is-signed-into-law.html.

448 Section 14(a) of the *Cybercrimes Act* 19 of 2020.

449 Botha *Statutory Interpretation* 132.

450 Preamble of the *Cybercrimes Act* 19 of 2020.

would seem illogical for property, as per sections 14 and 15, not to include incorporeal property and, by extension, cryptocurrency. It follows, therefore, that sections 14 and 15 would criminalise the incentivisation or threatening of damage, in whatever form, to cryptocurrency belonging to another.

Therefore, the newly enacted *Cybercrimes Act* builds upon the foundation set by ECTA. It also broadens and modernises the current cyber-offences established in ECTA whilst simultaneously creating new offences and targeting not only the offenders themselves, but anyone party to the commission of the offence as a whole, be it intermediaries, instigators and accessories after the fact. It sets a basis for cryptocurrency protection and regulation as digital assets or data when subjected to any of the offences above. Finally, it is a vital step forward for modernising South African law in the fourth industrial era. As Burger-Smidt puts it, the only thing left to see is whether the implementation by the courts and law enforcement can live up to the promises made by the legislation itself.[451]

5.4 POPIA Implications

Another statute to consider is the *Protection of Personal Information Act* 4 of 2013. Although not directly linked to e-commerce regulation, it may have potential consequences on implementing the above statutes. The statutes mentioned above, specifically the *Cybercrimes Act* and RICA, empower authorities to collect and process personal information.[452] POPIA, *inter alia,* regulates the lawful processing, collecting and storing of personal information.[453] POPIA also places a duty on the lawful holders to properly store and safeguard the personal information of others in its possession.[454]

---

451 Burger-Smidt 2021 https://www.werksmans.com/legal-updates-and-opinions/your-actions-in-cyberspace-can-land-you-in-prison/; *Cybercrimes Act* 19 of 2020.

452 Chapter 4 of the *Cybercrimes Act* 19 of 2020; chapter 2 of the *Regulation of Interception of Communications and Provision of Communication Related Information Act* 70 of 2002.

453 Papadopoulos and Snail ka Mtuze *Cyberlaw* 469.

454 Section 19 of the *Protection of Personal Information Act* 4 of 2013.

This duty further requires lawful holders to report to the Information Regulator[455] any suspected or actual breach whereby personal information has been unlawfully accessed.[456] Furthermore, an unlawful breach into, for instance, a server containing the personal information of the users of an e-commerce platform can lead to sanctions under POPIA and the *Cybercrimes Act*.[457]

Bhagattjee *et al* note an interesting correlation between section 22 of POPIA and section 54 of the *Cybercrimes Act*. According to them, both sections impose a duty to report suspected breaches whereby unlawful access is gained.[458] What is noteworthy, for the sake of the discussion on potential cryptocurrency regulation, is the wording of the latter section. Section 54 specifically imposes the duty on electronic communications service providers and financial institutions.[459] Thus, whether a cryptocurrency exchange would also be considered a financial institution arises. Section 1 of the *Cybercrimes Act* refers to a financial institution defined in the *Financial Sector Regulation Act* 9 of 2017.[460] Section 1 of the *Financial Sector Regulation Act* defines a financial institution as:[461]

> "Financial institution‟" means any of the following, other than a representative:
>
> (a) A financial product provider;
>
> (b) a financial service provider;
>
> (c) a market infrastructure;

---

455 The Regulator established in terms of s39 of the *Protection of Personal Information Act* 4 of 2013.

456 S22 of the *Protection of Personal Information Act* 4 of 2013.

457 Bhagattjee *et al* 2021 https://www.cliffedekkerhofmeyr.com/en/news/publications/2021/TMT/technology-media-and-telecommunications-sector-newsletter-9-june-regulating-the-fourth-industrial-revolution-south-africas-cybercrimes-bill-is-signed-into-law.html.

458 Bhagattjee *et al* 2021 https://www.cliffedekkerhofmeyr.com/en/news/publications/2021/TMT/technology-media-and-telecommunications-sector-newsletter-9-june-regulating-the-fourth-industrial-revolution-south-africas-cybercrimes-bill-is-signed-into-law.html.

459 Section 54 of the *Cybercrimes Act* 19 of 2020.

460 Section 1 of the *Cybercrimes Act* 19 of 2020.

461 Section 1 of the *Financial Sector Regulation Act* 9 of 2017.

(d) a holding company of a financial conglomerate; or

(e) a person licensed or required to be licensed in terms of a financial sector law.[462]

Sections 2 and 3 elaborate on the meanings of financial product providers and financial service providers, respectively.[463] However, from the wording of these sections, it would seem that cryptocurrency marketplaces are currently not included in the scope of financial institutions. It would make sense, as things currently stand, because cryptocurrency is not classified as legal tender, but as a form of incorporeal property. Therefore, currently, there cannot be a legal duty on cryptocurrency providers to report suspected breaches of unlawful access as envisaged by both section 22 of POPIA and section 54 of the *Cybercrimes Act*. The omission of this duty in respect of cryptocurrency marketplaces may be dangerous as these traders are under no obligation to report potential breaches of its systems or the subsequent theft that it may lead to.

5.5 The Way Forward

The above highlights the current legal framework wherein cryptocurrency can be regulated through prominent cybercrime and financial legislation. The law on cybercrime applies to cryptocurrency as soon as it is used as a tool in the commission of cybercrime. It also applies when cybercrime techniques are used to target cryptocurrency unlawfully. In line with the cybercrime framework, authorities are also empowered to launch investigations into suspicious transactions. Therefore, it would seem that the South African legislative framework has a tight grip on the potential fraud that may stem from cryptocurrency misuse. However, there is still room for a further tightening of this grip.

For instance, the fact that FICA does not mention cryptocurrency marketplaces as accountable institutions, may leave open room for cybercriminals to exploit in the form

462 Section 1 of the *Financial Sector Regulation Act* 9 of 2017.
463 Sections 2-3 of the *Financial Sector Regulation Act* 9 of 2017.

of fraud and money laundering. This may be a worrisome loophole. Further, the fact that there is no onus placed on cryptocurrency providers to report possible breaches under POPIA and the Cybercrimes Act, may be an incentive for cybercriminals to grasp an already seemingly lucrative opportunity to exploit.

According to Strydom, South African authorities have hinted at the potential change in its stance toward cryptocurrency regulation.[464] According to him, a few proposed regulations are expected within the coming year. This includes the amendment of Schedule 1 of FICA to include cryptocurrency asset providers.[465] Meaning crypto-currency asset providers will also be regarded as accountable institutions and, therefore, must comply with FICA's accounting principles, as described above.[466] It also includes the declaration of cryptocurrency as "financial product" under the *Financial and Intermediary Services Act* 37 of 2002.[467] Another amendment possibly on the table is the inclusion of cryptocurrency service providers into the definition of financial institution under the *Financial Sector Regulation Act*.[468] In this way, section 54 of the *Cybercrimes Act* and section 22 of POPIA would impose duties to report potential breaches of its databases to authorities.

Should the small amendments above be made, it would open the door for a complete overhaul of cryptocurrency regulation in South Africa and, in turn, create a much safer experience for consumers, as many of the shortcomings, threats and vulnerabilities of cryptocurrency trade would be nullified. It waits to see whether the legislature will take this leap in its cryptocurrency management.

---

464 Strydom 2022 https://www.michalsons.com/blog/crypto-regulations-in-south-africa/56081.
465 Strydom 2022 https://www.michalsons.com/blog/crypto-regulations-in-south-africa/56081.
466 See 5.2.3 above.
467 Strydom 2022 https://www.michalsons.com/blog/crypto-regulations-in-south-africa/56081; S1 of the *Financial and Intermediary Services Act* 37 of 2002.
468 Strydom 2022 https://www.michalsons.com/blog/crypto-regulations-in-south-africa/56081.

5.6 Conclusion

The above sought to determine whether South African legislation on cybercrime, including financial regulatory legislation, can provide an adequate basis to regulate cryptocurrency. What was seen is that the common law provides the point of departure for any discussion relating to criminal law, and that cybercrime, in its barest form, is no different from the common law crimes of theft, fraud and malicious injury to property. Further, ECTA was found to be the codification of cybercrime in South Africa. Other notable statutes relating to cybercrime, particularly anti-money laundering, include POCA and FICA.

POCA criminalises, *inter alia,* money laundering while FICA implements the accounting principles and procedures to combat money laundering. RICA, on the other hand, establishes the rules relating to the interception and investigation of suspicious communications to enforce the laws set out in the other statutes.

Furthermore, the *Cybercrimes Act* was recently enacted to, amongst others, modernise the South African cybercrime law and further clamp down on online fraud. POPIA also establishes rules, principles and duties relating to, among other things*,* the safekeeping of personal information. What can thus be seen from the above legal framework is that the basis for protection regarding cryptocurrency is there. A few tweaks and amendments are what is required to protect users and their cryptocurrency fully.

ECTA and the *Cybercrimes Act* already protect the unlawful access, alteration or interception of someone's cryptocurrency, and in this way, cybercrime laws currently attach protection to cryptocurrency. POCA enhances this stance by criminalising the hiding of illicit gains, including property. Although, whether incorporeal property such as cryptocurrency is included, needs further judicial authority. The legislature would expectantly have deemed it to be included. This statement is supported by having cryptocurrency expressly included within the definition of property in the *Protection of Constitutional Democracy Against Terrorism and Related Activities Amendment Bill*.

For further financial and regulatory protection to attach to cryptocurrency, a few amendments must be made. Some of these amendments include the widening of accountable institutions under Schedule 1 of FICA, the inclusion of cryptocurrency asset providers as a financial institution under the *Financial Sector Regulation Act* and providing watchdogs and authorities wider powers to investigate misconduct relating to the cryptocurrency trade. It seems that the legislature has taken note hereof and will soon make some of these changes to enhance the protection afforded to users.

Therefore, the basis for cryptocurrency regulation, to an extent, has been laid, and the implementation of small changes may have a large effect on the future of cryptocurrency in South Africa. The future and success of cryptocurrency regulation in South Africa are yet to be seen, but the ball is in the legislature's court. The legislature would be wise to follow suit with the rest of the world, as seen in the preceding chapter, and implement these small changes to existing legislation to create a safer experience for e-commerce users regarding cryptocurrency.

Chapter 6: Conclusion and recommendations

6.1 Introduction

This work aimed to determine the extent and capacity of the South African legal framework to regulate and protect all parties to electronic commerce from the potential dangers of the misuse of cryptocurrencies within a cybercrime context. To do so, a thorough examination took place of all concepts and principles which fall under the terms relating to electronic commerce, cybercrime and cryptocurrency. After each concept was analysed, it became necessary to examine the legal framework surrounding these concepts. Further, a link between all concepts was investigated to determine whether they do, in fact, relate to one another insofar as potential regulation is concerned. Further, the legal frameworks relating thereto were examined from an international law perspective. Certain foreign jurisdictions were also assessed. Following therefrom was an assessment of the current legal framework on cybercrime, and by extension cryptocurrency security and regulation, in South Africa. From the findings a conclusion can be made on whether the South African legal framework is effective in its aims or whether any shortcomings are noted.

6.2 E-commerce and cybercrime

The starting point for the discussion was to properly determine the boundaries of what would constitute e-commerce. The term e-commerce is used to categorise any form of transaction that initiates from the internet or from other computer networks acting as an intermediary between buyer and seller. The marketplace itself exists in cyberspace and creates the link between buyer and seller. E-commerce is said to have taken place when an online marketplace is used as facilitator between buyer and seller. E-commerce, as a concept, does not rely on the logistical factors for a transaction to be completed, but is said to exist where an online marketplace links a buyer to a seller.

E-commerce allows consumers and traders to access a marketplace for goods and services, irrespective of their physical location or the time of day. It links consumers and traders to an internationally accessible marketplace. It is convenient, instant and easily reachable. However, e-commerce platforms can be apparent breeding grounds for fraudulent online activities. Most of the fraudulent activities faced by e-commerce platform users fall within the scope of cybercrime.

Cybercrime as a concept is trite with academic definitions. The definitions by various jurists and academics do somewhat reconcile with one another. However, these definitions mainly come down to the following: cybercrime is a criminal law offence committed by means of a computer, with the object of the crime being another computer, a network, data or any other digital or other device. The *Cybercrimes Act* 19 of 2020 attempts to solidify and update the position on cybercrime in South Africa. From the Act, it can be learnt that cybercrime comes down to the unlawful access, interception or alteration of data. This means that irrespective of the action leading to an offence, the elements of the offence will have to fall within the ambit of either unlawful access, unlawful interception or unlawful interference for cybercrime to have taken place.

Furthermore, the discussion above noted that due to the inherent differences between cybercrime and physical crime, the traditional criminal law cannot adequately regulate cyber-offences. This is because cybercrime differs greatly from traditional crime. Apart from the characteristics that differ, other logistical matters also create difficulties. High cost and difficulty of prosecution, the frequency of cybercrime, anonymity, jurisdictional issues and locale further emphasise that cybercrime cannot fit the mould of the traditional criminal law enforcement system.

Furthermore, the *Fourie v Van der Spuy and De Jongh Inc* case highlights the importance of the wide interpretation of cybercrime under the *Cybercrimes Act*. It supports the position, later taken by the Act, that the way in which the offence is committed is irrelevant, but that the elements of an offence require the unlawful

access, interception or alteration of data. The case also showcases that any user of e-commerce platforms can fall victim to cybercrime. The *Carolissen v Director of Public Prosecutions* case highlights the extraterritoriality of cybercrime. It shows the importance of states to work together to prosecute cybercrime. The case points out that a wide interpretation of the effects of a cyber-offence is also required. As with the definition not confining to rigid academic concepts but rather the effects of the offence, so too must the effects of where a cyber-offence is felt, be recognised as important as to where the offence originates from.

Therefore, cybercrime is a wide concept related to any form of offence committed by using a computer or electronic device and where any form of data is unlawfully altered, accessed, interfered with or intercepted. This directly correlates to e-commerce as the rise in the use of computers, data networks and the internet has only given cybercriminals more incentive to commit these offences. The correlation between e-commerce, cybercrime and cryptocurrency was discussed in chapter 3.

6.3 The correlation between cryptocurrency and cybercrime

The rise of e-commerce also gave rise to the use of cryptocurrency. The number of e-commerce merchants accepting cryptocurrency as a method of payment has been steadily growing over recent years. Cryptocurrency is an intangible graphical representation of value, finding existence only in cyberspace and which is accepted as a valid method of payment. It is traded electronically. It is not issued by a centralised monetary authority, and thus not considered legal tender and therefore not classified as money or fiat currency. However, it does represent value and is considered to be of value by the free market and as such, cryptocurrency can be used as unit of exchange. The SARB considers cryptocurrency to be a convertible form of virtual currency, therefore, it does have the potential to be exchanged for money or other forms of legal tender.

The characteristics of cryptocurrency are that it operates on an open-source software platform. This means that any person with the required software can gain access thereto. The transactions operate on a peer-to-peer basis. Thus, there is no intermediary backing from banks or governments. The transactions are between consumers and traders themselves. The value thereof is left to the free market. Further, the system operates on a process called "mining". Mining refers to the computer processes which operate to validate the cryptographic strings of data which form the cryptocurrency. The transfer process works with a system of what is known as keys. Each time ownership of cryptocurrency changes, the sender and recipient need to electronically sign off on the transaction with these keys. The foundation underpinning the running of cryptocurrency is a distributed ledger technology known as blockchain. The blockchain operates as a record book of all transactions wherein the specific chain of cryptocurrency was used. Cryptocurrency is stored in what is known as virtual vaults or wallets. Due to these unique characteristics, cryptocurrency poses an anomaly to legal systems regarding regulation, especially as it relates to consumer protection.

Cryptocurrency trading platforms, generally, are not subject to regulatory standards and/or due diligence checks. This means that the origin of the money or other form of payment being offered to cryptocurrency traders in exchange for cryptocurrency is not traced or verified. Cryptocurrency essentially operates on a "no-questions-asked" basis. Further, the transaction takes place anonymously, without either party knowing each other's identity. Therefore, to launder money through cryptocurrency channels would be a trivial exercise.

The *Africrypt* incident displayed the risks of cryptocurrency in corroboration with the traditional forms of cybercrime. It showed how cryptocurrency can in and of itself be used as a tool to facilitate cybercrime. It also showed how cryptocurrency can become the target of cybercrime. The worrisome factor of the incident became the fact that the FSCA could not offer any form of recourse since it lacked the inherent jurisdiction

to investigate the matter. Further, the incident showcased the use of the so-called traditional forms of cybercrime to gain unlawful access to cryptocurrency. The incident acts as a showpiece that the concepts of cybercrime and cryptocurrency fraud are inextricably linked.

The *Kats v United States of America, Southern District of New York* case highlights the above position, as *in casu,* cryptocurrency was used as a tool to launder money gained from illicit activity. The cryptocurrency platform, known as *Liberty Reserve*, was convenient to money launderers in that it only required basic personal information, which was in any event not verified for accuracy. The case solidifies the correlation between cryptocurrency and cybercrimes such as money laundering, identity theft, hacking, etcetera. It showcases how cryptocurrency can tie into the commission of cybercrime by acting as a component to cybercrime by providing an easier route for cybercriminals to launder their illicit gains.

The infamous *United States of America v Ross William Ulbricht Dread Pirate Roberts Silk Road Sealed Defendant*, colloquially referred to as the *Silk Road* case and the *Darkode* case, a case with similar merits, build on this by emphasising the ultimate risks that accrue from the characteristic anonymity of cryptocurrency transactions. These cases are further illustrations of the relative ease in which money laundering is facilitated through cryptocurrency. They further illuminate the link between cryptocurrency and cybercrime. In both these cases, cryptocurrency was the focal point of discussion. Cryptocurrency provided the platforms for nameless transactions which, when corroborated by traditional forms of cybercrime, created the perfect means for cybercriminals to exploit.

Therefore, from the above, it can be seen that technology and the practices by cybercriminals have developed to such a point that the terms "cybercrime" and "cryptocurrency fraud" cannot be seen as mutually exclusive. Both concepts inherently contain a link to each other. The distinction being that cryptocurrency is sometimes

used as a means to facilitate another end, for example in the case when using it as a payment method for further illicit transactions. Other times it is used as the target of cybercrime itself, for example when hacking or phishing is used to gain unlawful access to an unwitting victim's cryptocurrency wallet. In line with this, the legal framework on cybercrime may provide the platform for regulation on cryptocurrency. In order to assess the possibility thereof, an examination of the international legal community's regulation of these concepts is required. Further guidance may also be found in certain foreign jurisdictions and as such a further examination into these jurisdictions would be beneficial.

6.4 International and foreign legal frameworks

To find the international legal fraternity's perspective on cybercrime relating to cryptocurrency, it was necessary to take a look at the principal international law treaties on e-commerce and cybercrime. Further investigation into the practices employed in several foreign jurisdictions also gave insight on whether cybercrime legislation can provide a regulatory framework for cryptocurrency.

The *UNCITRAL Model Law of Electronic Commerce* (1996) is the leading model law on global e-commerce. It aims to establish a standardised model for electronic contracting and trade through standardising various rules and principles. The model law itself makes no mention of cyberfraud since it merely operates as the starting point to test the validity of an international e-commerce contact. The *UNCITRAL Model Law on Electronic Signatures* (2001) acts as a supplement to the original *UNCITRAL Model Law.* The 2001 model law does not expressly deal with cybercrime. However, it is an important development for the international perspective on cyberfraud due to the fact that it serves as a normative standard for the testing of the validity and authenticity of electronic signatures. The *Model Law on Electronic Signatures* is, thus, the point of departure in international law towards a safer e-commerce landscape.

In line with this, the *United Nations Convention on the Use of Electronic Communications in International Contracts* (2005) builds on the provisions of the two *UNCITRAL* model laws. The object of the convention is to provide legal certainty to electronic commerce that is equated to the standards and principles applicable to traditional commercial transactions. However, the focus of the convention is restricted to electronic contracts and as such makes no direct reference to cyberfraud.

The *Council of Europe Convention on Cybercrime* (2001), commonly known as the *Budapest Convention,* is the foremost international law treaty on cybercrime. Article 8 thereof explicitly criminalises computer-related fraud. The wording of the article is wide enough to support technological advancements without fear of becoming outdated due to its open wording. What is noteworthy from the Article, is that it focuses on the criminalisation of the unlawful access, interference or alteration of a computer system, rather than rigid rules pertaining to the forms of cybercrime. The Article works as an all-encompassing provision. This would, therefore, by extension also include the fraudulent use and/or targeting of cryptocurrency. The *Budapest Convention*, although wide in its wording, is not resistant to technological advances and the challenges that follow therefrom. Therefore, the Council of Europe has recently adopted the *Second Additional Protocol* to the *Budapest Convention*. The *Protocol* empowers nations to work together to prosecute any perpetrators. The *Protocol* establishes guidelines and principles for states to work together as a solution to the inherent lack of territoriality which stems from cybercrime. Thus, the *Budapest Convention*, and its *Protocols,* are an important source for international cybersecurity law. It sets out the parameters of computer-related fraud, as well as its prosecution. It also provides for the co-operation between states to prosecute such fraud. However, its force of law is restricted to signatories and member states.[469] It further does not have express provisions on cryptocurrency regulation.

[469] A 2(1) of the *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (2022).

The above highlights that there is, as of yet, no concise and widely accepted international law standard on cryptocurrency regulation. In line with this, there is currently no clear international standard for the regulation of cybercrime which follows as a result of fraudulent cryptocurrency use. Therefore, a more focused analysis in respect of certain foreign jurisdictions may provide a better understanding of cryptocurrency regulation in e-commerce.

Japan fully regulates cryptocurrency under the auspices of its *Payment Services Act.* All cryptocurrency traders must be registered and have a domicile in Japan. The Act imposes strict accounting laws on such traders to prevent money laundering. Japan's Financial Services Agency is given wide powers to review the annual statements of companies dealing in cryptocurrency. However, even a strong regulatory framework on cryptocurrency does not entirely prevent cyberfraud with an origin outside of the country. This links back to the fact that cyberfraud cannot be confined to a singular jurisdiction.

The United States of America follows the Japanese system of cryptocurrency regulation closely. However, a layered approach is used wherein the states themselves are free to impose regulations at state level, being subject to federal oversight. The federal oversight requires the registration of cryptocurrency traders. It also enforces strict accounting laws. The US also makes use of specialised units with proper training and knowledge in cybersecurity to act as watchdogs.

The European Union approaches cryptocurrency regulation through a strict policy against money laundering. The Anti-money Laundering Directives of the EU include virtual currencies. The EU has also given Financial Intelligence Units wide oversight powers to, *inter alia,* monitor suspected transactions. Further, the EU periodically reviews its action plan on anti-money laundering legislation and directives. In this way, the EU aims to stay one step ahead of developing practices by cybercriminals as well as technological advancements.

Therefore, the common thread throughout, from the above foreign jurisdictions, is that they each give cryptocurrency its due legal recognition. Furthermore, they each ascribe to the enforcement of strict accounting laws and principles in respect of cryptocurrency traders. Additionally, watchdogs and oversight authorities are given wide powers to investigate potentially fraudulent activity. In this way a strict approach to regulation is taken. For South Africa to possibly incorporate these principles into its law, an examination of the current South African perspective on cryptocurrency and cyberfraud regulation will need to be undertaken, after which, potential amendments to the existing framework can be discussed.

6.5 The South African legal framework

Cybercrime laws in South Africa, at its core, are derived from the criminal law which is based off of the common law. The common law provides the point of departure since cybercrime offences. From a theoretical perspective, when stripped down to its barest elements, cyber-offences are no different to common law crimes. Cybercrimes can in this way, be likened to theft, fraud, malicious injury to property and housebreaking with the intent to commit a crime. However, given the intricacy of cyber regulation, the common law has lost most of its influence. Furthermore, many of the common-law principles have been codified into other sources such as case law and case directives. Therefore, the common law has little to no practical effect, other than symbolic and academic significance, in respect of cybercrime regulation.

The *Electronic Transactions and Communications Act* (ECTA) became the first statute to codify the South African legal framework on cybercrime. It notably criminalised the unlawful access, unlawful interception and unlawful alteration of data. The broad wording used in the Act serves as all encompassing provisions for all forms of cybercrime. Furthermore, the wording also serves as a safety net for technological advancement whereby focus is shifted to the object being protected, i.e. data, and the

way it is tampered with rather than getting lost in overly academic technological jargon.

ECTA criminalised cyber-offences, whilst other statutes such as the *Prevention of Organised Crimes Act* (POCA) and the *Financial Intelligence Centre Act* (FICA) operate closely to one another to enforce, *inter alia,* strict anti-money laundering laws. One of the main aims of POCA is to prevent the proceeds of unlawful activity from being concealed. According to POCA, "property" is included under potential proceeds of unlawful activity. Further, the Act defines "property" in such a way to include incorporeal things. The notable question thus arising, is whether this definition would include cryptocurrency. As seen above, cryptocurrency plays a major role in money laundering. Therefore, a potential *lacuna* arises if anti-money laundering legislation would not include cryptocurrency under the definition of "property". The South African legislature has potentially provided the answer in the form of a new Bill, known as the *Protection of Constitutional Democracy Against Terrorism and Related Activities Amendment Bill*. The Bill contains the exact definition of property as it is in POCA, however, it broadens the definition to explicitly include cryptocurrencies. This clearly demonstrates the legislature's willingness for anti-money laundering legislation to cover cryptocurrency.

FICA, operates closely alongside POCA. FICA establishes the Financial Intelligence Centre (FIC) to, *inter alia,* monitor and oversee financial transactions in order to trace whether these transactions emanate from legitimate sources. Schedule 1 of the Act lists accountable institutions which are subject to the rules and principles imposed by FICA. These rules and principles include strict accounting principles and oversight by the FIC. Schedule 1 does not as of yet list cryptocurrency traders as accountable institutions and thus currently limits the operation of the Act in respect of cryptocurrency traders. However, the possible amendment to include cryptocurrency traders in schedule 1 is being considered by the legislature. In this way, much greater oversight will be had over cryptocurrency markets in South Africa.

The *Cybercrimes Act* was recently enacted to, *inter alia*, modernise the South African cybercrime law and further clamp down on online fraud. The principal objectives of the Act are to establish further offences and penal sanctions for cybercrime transgressions; to criminalise the spreading of harmful data communications and messages; and to give law enforcement agencies the requisite authority to properly investigate cyber-offences. The Act follows the premise of ECTA and builds upon the foundation set by ECTA. It broadens and modernises the current cyber-offences established by ECTA, whilst also creating new offences. It further clamps down on offenders, as well as accomplices, intermediaries and accessories after the fact. Cryptocurrency will thus also be regulated under the Act if it is in any way used as either a tool in the commission of a cyber offence or when unlawful cybercrime techniques are used to target it.

Other statutes such as the *Regulation of Interception of Communications and Provision of Communication Related Information Act* (RICA),[470] the *Protection of Personal Information Act* (POPIA), the *Financial Sector Regulation Act* and the *Financial and Intermediary Services Act* also add further layers of protection to e-commerce and financial transactions. They lay the basis for possible cryptocurrency regulation and already have the adequate rules and principles in place. However, their operation is currently restricted as cryptocurrency is not expressly provided for in either Act.

What is thus noteworthy from the South African legal framework on cybercrime and e-commerce is that it lays the foundational building blocks for a comprehensive cryptocurrency regulatory framework. The cybercrime laws attach to all forms of cyber fraud and would as a result also include cyberfraud where cryptocurrency is involved. The anti-money laundering legislation is shifting to an ever-increased emphasis on

---

[470] Although its operation is currently suspended due to constitutionality issues. See *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others* (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) (4 February 2021.

cryptocurrency and would likely in the near future include cryptocurrency as property, as evidenced by the Bill above, subject to money laundering. The other financial oversight and regulatory statutes also provide the basis for regulation of the e-commerce industry, but stops just short of cryptocurrency regulation. The potential for regulation is thus primed under the current legal framework. With a few amendments of the current framework, a comprehensive framework on the regulation of cryptocurrency can be put into place.

6.6 Conclusion

The above study sought to establish whether the South African legal framework is equipped to deal with cryptocurrency misuse as it relates to e-commerce. The study leads with a hypothesis that the current legal framework on cybercrime and e-commerce may already set the basis for the regulation of cryptocurrency. If indeed so, minor legislative amendments may provide for a full ratification of the South African position on cryptocurrency, and could thus possibly lead to full regulation. To test the hypothesis and provide an answer to the research question, an examination of e-commerce and cybercrime took place. Following from this, an extensive correlation between cybercrime and cryptocurrency was investigated, after which an analysis of the international legal community's approach to cybercrime, and by extension cryptocurrency misuse, took place. These principles were then viewed in light of certain well-developed foreign jurisdictions. Lastly, the South African current legal framework was examined in consideration of each concept that preceded.

The study found that e-commerce is a system acting as an online intermediary, linking consumers with traders. However, it also acts as a breeding ground for fraudulent online activity. Fraudulent online activity is collectively known as cybercrime. Cybercrime takes place when data is unlawfully accessed, unlawfully altered or unlawfully intercepted. The regulation of cybercrime is continuously more intricate to

that of traditional crime due to its inherent differences. As such, cybercrime has to be approached differently to traditional crime, by legislatures.

Flowing from the definition of cybercrime, as above, it was found that there exists a correlation between cybercrime and cryptocurrency. Cryptocurrency, due to its characteristics, generates many risks for consumers and leaves open the door for exploitation by cybercriminals. Cryptocurrency provides the platform for faceless transactions which, when exploited by the different forms of cybercrime, creates the perfect means for cybercriminals to target. The study showed many instances highlighting the fact that the practices by cybercriminals have developed to such a point that differentiating between cryptocurrency misuse/fraud and cybercrime would be a futile exercise as these concepts work hand-in-hand. Cryptocurrency is often used as a means to facilitate another end of online fraud, such as money laundering. It is also targeted by cybercrime, in and of, itself.

The study sought to find whether the international legal community can provide a model for regulation of cryptocurrency through its cybercrime laws. It was found that there is currently no concise and all-encompassing international standard for the regulation of cryptocurrency. Further, international laws on cybercrime are increasing in age and are potentially becoming outdated. To combat this, the *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* aims to update the international framework on cybercrime and also provide a procedure for states to work together in the prosecution of online crime.

The study then focused its attention to certain developed foreign jurisdictions to possibly find a normative standard for the regulation of cryptocurrency. The similarities throughout, from the above foreign jurisdictions, is that they each take a strict approach to cryptocurrency regulation. They each enforce strict accounting laws and principles in respect of cryptocurrency traders. Regulators and oversight authorities are given wide powers to investigate potentially fraudulent activity.

Finally, having examined all correlations between e-commerce, cybercrime and cryptocurrency, and viewing them in the light of international and foreign law, the study could turn its attention to the South African legal framework. It was found that ECTA codified the South African position on cybercrime. This position was then enhanced by, and modernised by, the *Cybercrimes Act*. The focus once again given to the object of the offence, being unlawful access, unlawful interception and unlawful alteration of data. Furthermore, POCA and FICA operate in *tandem* to prevent, *inter alia,* money laundering. Lastly, RICA and POPIA add further levels of protection to the e-commerce sector by providing, among others, for the safe storing of personal information and for the investigation of suspicious transactions.

Therefore, having learned that cybercrime accompanies e-commerce, and that cryptocurrency is inherently correlated to cybercrime, it can be said that the legal principles governing cybercrime would provide an effective platform for the regulation of cryptocurrency. Given the strong legal framework governing cybercrime and e-commerce in South Africa, the present legal framework would be sufficiently equipped to provide for the regulation of cryptocurrency. The existing legal framework on e-commerce and cybersecurity could, therefore, with minor amendments, provide the basis for the regulation of cryptocurrency in South Africa.

6.7 Recommendations

The above study sought to establish whether the existing e-commerce and cybercrime legal framework would be able to provide a platform for the regulation of cryptocurrency. It found that, with a number of minor legislative amendments, it could possibly provide a comprehensive ratification of the South African regulatory framework on cryptocurrency.

Cybercrimes involving cryptocurrency are already covered by the *Cybercrimes Act*. Given the wording of the Act and the sections on cybercrime, it would already include cryptocurrency-related online fraud. This is due to the fact that, from its nature, online

fraud involving cryptocurrency, either as a tool or target of cybercrime, would in any event fall under the unlawful access, interception or alteration of data.

For certainty on whether cryptocurrency is covered by anti-money laundering legislation, one has to examine the term "property" as defined in POCA. If cryptocurrency would fall under the definition of property, it would mean that it is considered to be an asset that can be subjected to money laundering. The *Protection of Constitutional Democracy Against Terrorism and Related Activities Amendment Bill* takes the definition of "property" verbatim from POCA and broadens it to specifically include cryptocurrency. It is, therefore, recommended that POCA be amended and that the wording used in the Bill be followed for certainty to be had that cryptocurrency is definitely included as an asset capable of being laundered.

For the FIC to be empowered to properly oversee cryptocurrency exchangers, schedule 1 of FICA should be amended to include such cryptocurrency exchangers. In this way, cryptocurrency exchangers would be obligated to ascribe to the same accounting rules and principles as other financial institutions. This would include ascribing to, for instance, KYC-requirements. This would circumvent a lot of the fraud that stems from the anonymity of cryptocurrency transactions. This is also in line with the practices used in Japan and the United States.

Linked to this, RICA may also be an invaluable tool to monitor suspicious transactions relating to cryptocurrency. Therefore, it is recommended that RICA's unconstitutional provisions be rectified and safeguards be implemented as soon as possible. The sooner the unconstitutional provisions are rectified, the sooner the suspension of RICA can be ended.

Finally, sections 2 and 3 of the *Financial Sector Regulation Act* could possibly be amended to include cryptocurrency exchangers as a "financial institution", and in this way, financial laws would attach to cryptocurrency transactions. This would also include the provisions of both section 22 of POPIA and section 54 of the *Cybercrimes*

Act. In doing so, cryptocurrency exchangers would be obliged to report suspected breaches of data.

Bibliography

Literature

Albert 2002 *ABLJ*

Albert MR "E-Buyer Beware: Why Online Auction Fraud Should be Regulated" 2002 *American Business Law Journal* 575-643

Botha *Statutory Interpretation*

Botha C *Statutory Interpretation An Introduction for Students* 5th ed (Juta Cape Town 2017)

Clough 2012 *Criminal Law Forum: The Official Journal of the Society for the Reform of Criminal Law*

Clough J "The Council of Europe Convention on Cybercrime: Defining 'Crime' in a Digital World" 2012 *Criminal Law Forum: The Official Journal of the Society for the Reform of Criminal Law* 363-391

Coetzee 2006 *SA Mercantile Law Journal*

Coetzee J "The Convention on the Use of Electronic Communications in International Contracts: Creating an International Legal Framework for Electronic Contracting" 2006 *SA Mercantile Law Journal* 245-258

Coetzee *et al A Student's Approach to Income Tax*

Coetzee K *et al A Student's Approach to Income Tax Natural Persons* 2020 ed (LexisNexis South Africa 2020)

De Kock *Regulating Cryptocurrencies in South Africa*

De Kock WM *Regulating Cryptocurrencies in South Africa* (MPhil-dissertation University of Cape Town 2019)

Desai 2018 *Acta Criminologica: Southern African Journal of Criminology*

Desai A "Cybercrime, Cybersurveillance and State Surveillance in South Africa" 2018 *Acta Criminologica: Southern African Journal of Criminology* 149-160

Dlagnekova 2009 *Fundamina*

Dlagnekova P "The Need to Harmonise Trade-Related Laws Within Countries of The African Union: An Introduction to The Problems Posed by Legal Divergence" 2009 *Fundamina* 1-37

Dube *Regulatory Challenges Posed by the Evolution of Cryptocurrency*

Dube L *Regulatory Challenges Posed by the Evolution of Cryptocurrency* (LLM-dissertation University of Pretoria 2019)

Eiselen 2007 *PER/PELJ*

Eiselen S "The UNECIC: International Trade in the Digital Era" 2007 *PER/PELJ* 1-49

Erasmus and Bowden 2020 *Obiter*

Erasmus D and Bowden S "A Critical Analysis of South African Anti-Money Laundering Legislation with Regard to Cryptocurrency" 2020 *Obiter* 309-327

Hlongoane *Access to Information Held by the Financial Intelligence Centre*

Hlongoane KKM *Access to Information Held by the Financial Intelligence Centre* (LLM-dissertation University of Pretoria 2018)

Hubbard *Finweek*

Hubbard J "SA Businesses Underplaying the Danger of Cybercrime?" *Finweek* (7 March 2019) 37-38

IFWG 2018 *Consultation Paper on Policy Proposals for Crypto Assets*

Intergovernmental Fintech Working Group "Consultation Paper on Policy Proposals for Crypto Assets" 2018 *IFWG Consultation Paper on Policy Proposals for Crypto Assets* 1-32

IFWG 2021 *Position Paper on Crypto Assets*

Intergovernmental Fintech Working Group "Position Paper on Crypto Assets" 2021 *IFWG Position Paper on Crypto Assets* 1-49

Kempen 2019 *Servamus*

Kempen A "Cybercrime Knows No Borders" 2019 *Servamus Community Based Safety and Security Magazine* 27-31

Kersop *Anti-money laundering regulations and the effective use of mobile money in South Africa*

Kersop M *Anti-money laundering regulations and the effective use of mobile money in South Africa* (LLM-dissertation North-West University 2014)

Kouamo *Combating Crime in International Electronic Commerce*

Kouamo JA *Combatting Crime in International Electronic Commerce* (LLM-dissertation North-West University 2013)

Lewis L *et al* 2021 *Intellectual Property and Technology Law Journal*

Lewis L *et al* "Non-Fungible Tokens and Copyright Law" *Intellectual Property and Technology Law Journal* 18-19

Maanda *Legal Implications of Virtual Currencies*

Maanda MH *Legal Implications of Virtual Currencies* (LLM-dissertation University of Pretoria 2019)

Mothokoa *Regulating crypto-currencies in South Africa: The need for an effective legal framework to mitigate the associated risks*

Mothokoa K *Regulating crypto-currencies in South Africa: The need for an effective legal framework to mitigate the associated risks* (LLM-dissertation University of Pretoria 2017)

Mpuru 2017 *Servamus Community-based Safety and Security Magazine*

Mpuru L "Cyber Security Concerns in South Africa: Current Legislative Framework" 2017 *Servamus Community-based Safety and Security Magazine* 44-45

Nugent 2019 *Fordham Law Review*

Nugent TJ "Prosecuting Dark Net Drug Marketplace Operators Under the Federal Crack House Statute" 2019 *Fordham Law Review* 345-379

OECD 2019 OECD *Going Digital Policy Note*

Organisation for Economic Co-Operation and Development "Trade in the Digital Era" 2019 *Going Digital Policy Note* 1-8

Olivier 2012 *De Jure*

Olivier L "Capital Versus Revenue: Some Guidance" 2012 *De Jure* 172-177

Orffer *The Inclusion of Virtual Currencies in the Calculation of Income Tax*

Orffer M *The Inclusion of Virtual Currencies in the Calculation of Income Tax* (LLM-dissertation North-West University 2018)

Papadopoulos and Snail ka Mtuze *Cyberlaw*

Papadopoulos S and Snail ka Mtuze S *Cyberlaw @ SA The Law of the Internet in South Africa* 4th ed (Van Schaik South Africa 2022)

Phora *Developing a Legal Framework for E-Commerce in South Africa*

Phora JS *Developing a Legal Framework for E-Commerce in South Africa* (LLM-dissertation University of Pretoria 2019)

Reddy and Minnaar 2018 *Acta Criminologica: Southern African Journal of Criminology*

Reddy E and Minnaar A "Crypotcurrency: A Tool and Target for Cybercrime" 2018 *Acta Criminologica: Southern African Journal of Criminology* 71-92

SARB *Position Paper on Virtual Currencies*

South African Reserve Bank National Payment System Department 2014 "Position Paper on Virtual Currencies" *SARB Position Paper on Virtual Currencies* 1-13

Schulze 2006 *SA Mercantile Law Journal*

Schulze C "Electronic Commerce and Civil Jurisdiction, with Special Reference to Consumer Contracts *SA Mercantile Law Journal*" 2006 *SA Mercantile Law Journal* 31-44

Schwonwetter 2006 *SA Journal of Information and Communication*

Schwonwetter T "The Fair Use Doctrine and the Impact of Digitising from a South African Perspective" 2006 *Southern African Journal of Information and Communication* 32-52

Smit *Does blockchain technology offer a solution to the remaining impediments to the more widespread use of electronic negotiable bills of lading?*

Smit JJ *Does blockchain technology offer a solution to the remaining impediments to the more widespread use of electronic negotiable bills of lading?* (LLM-dissertation University of Cape Town 2020)

Snyman *Criminal Law*

Snyman CR *Criminal Law* 6th ed (LexisNexis South Africa 2014)

Stander *Investigating the use of e-commerce to empower South African women*

Stander Am *Investigating the use of e-commerce to empower South African women* (MBA-dissertation North-West University 2015)

Van der Merwe *et al Information and Communications Technology Law*

Van der Merwe DP *et al Information and Communications Technology Law* 3rd ed (LexisNexis South Africa 2021)

Van der Walt and Pienaar *Introduction to the Law of Property*

Van der Walt AJ and Pienaar GJ *Introduction to the Law of Property* 7th ed (JUTA Cape Town 2016)

WIPO 2021 *World Innovation Index*

World Intellectual Property Organisation "Tracking Innovation through the COVID-19 Crisis" 2021 *Global Innovation Index* 1-226

Case Law

AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) (4 February 2021)

Bragg v Linden Research Inc., 487 F.Supp.2d 593 E.D.Pa 2007

Carolissen v Director of Public Prosecutions 2016 (2) SACR 171 (WCC)

Fourie v Van der Spuy and De Jongh Inc (65609/2019) [2019] ZAGPPHC 449; 2020 (1) SA 560 (GP) (30 August 2019)

Kats v United States of America, Southern District of New York, 2016 (13) U.S 368

Li Hong Chen v Beijing Arctic Ice Technology Development Company (2003, Beijing Second Intermediate Court)

Pharmaceutical Manufacturers Association of South Africa: In re Ex Parte President of the Republic of South Africa (CCT31/99) [2000] ZACC 1; 2000 (2) SA 674; 2000 (3) BCLR 241 (25 February 2000)

United States of America v Ilya Lichtenstein and Heather Rhiannon Morgan case number: 1:22-mj-0022 (United States District Court for the District of Columbia) (7 February 2022)

United States of America v Ross William Ulbricht Dread Pirate Roberts Silk Road Sealed Defendant Dpr 15-1815 May 31, 2017

Legislation

Constitution of the Republic of South Africa, 1996

Consumer Protection Act 68 of 2008

Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007

Criminal Procedure Act 51 of 1977

Cybercrimes Act 19 of 2020

Electronic Communications and Transactions Act 25 of 2002

Films and Publications Act 65 of 1996

Financial and Intermediary Services Act 37 of 2002

Financial Intelligence Centre Act 38 of 2001.

Financial Sector Regulation Act 9 of 2017

Income Tax Act 58 of 1962

Payment Service Act 59 of 2006 (Japan)

Prevention of Organised Crime Act 121 of 1998

Promotion of Administrative Justice Act 03 of 2000

Protection of Constitutional Democracy Against Terrorism and Related Activities Amendment Bill (B15-2022)

Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 Of 2004

Protection of Personal Information Act 04 of 2013

Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002

Securities Exchange Act of 1934 (USA)

South African Reserve Bank Act 90 of 1989

International Instruments

Council of Europe Convention on Cybercrime (ETS 185) (2001)

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (2022)

The Council Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (the Brussels Regulation) 44/2001

UNCITRAL Model Law on Electronic Commerce (1996)

UNCITRAL Model Law on Electronic Signatures (2001)

United Nations Convention on the Use of Electronic Communications in International Contracts (2005)

Internet Sources

Anon 2021 *Competition Commission launches investigation into Takealot, UberEats and other online markets* https://businesstech.co.za/news/internet/491029/competition-commission-launches-investigation-into-takealot-ubereats-and-other-online-markets/ accessed 7 June 2021

Bhagattjee P and Govuza A 2020 *Cybercrime in South Africa - attorneys fall victim to cyber fraud* https://www.cliffedekkerhofmeyr.com/en/news/publications/2020/technology/tmt-

alert-18-february-cybercrime-in-south-africa-attorneys-fall-victim-to-cyber-fraud.html accessed 5 September 2021

Bhagattjee P *et al* 2021 *Regulating the Fourth Industrial Revolution – South Africa's Cybercrimes Bill is signed into law* https://www.cliffedekkerhofmeyr.com/en/news/publications/2021/TMT/technology-media-and-telecommunications-sector-newsletter-9-june-regulating-the-fourth-industrial-revolution-south-africas-cybercrimes-bill-is-signed-into-law.html accessed 3 August 2021

Bloomenthal A 2020 *Electronic Commerce (E-Commerce)* https://www.investopedia.com/terms/e/ecommerce.asp accessed 28 February 2021

Brock Z 2019 *The Princess Bride Characters: The Dread Pirate Roberts* https://www.litcharts.com/lit/the-princess-bride/characters/the-dread-pirate-roberts accessed 10 March 2022

Browne R 2021 *MoneyGram to let cryptocurrency holders' cash in their investments* https://www.cnbc.com/2021/05/12/moneygram-to-let-cryptocurrency-traders-cash-in-their-investments.html accessed 18 January 2022

Browne R 2021 *More than $90 million in cryptocurrency stolen after a top Japanese exchange is hacked* https://www.cnbc.com/2021/08/19/liquid-cryptocurrency-exchange-hack.html accessed 19 May 2022

Burger-Smidt A 2021 *Your Actions in Cyberspace can Land You in Prison!* https://www.werksmans.com/legal-updates-and-opinions/your-actions-in-cyberspace-can-land-you-in-prison/ accessed 31 May 2022

Conti R and Schmidt J 2022 *What Is an NFT? Non-Fungible Tokens Explained* https://www.forbes.com/advisor/investing/nft-non-fungible-token/ accessed 16 February 2022

Council of Europe 2022 *Details of Treaty No. 185* https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 accessed 26 April 2022

Council of Europe 2022 *New Treaties* https://www.coe.int/en/web/conventions/new-treaties accessed 26 April 2022

Council of Europe 2022 *The Budapest Convention and its Protocols* https://www.coe.int/en/web/cybercrime/the-budapest-convention accessed 27 April 2022

Cybercrime.org.za 2021 *Hacking Definition* https://cybercrime.org.za/hacking/ accessed 27 February 2022

De Rebus 2021 *New Legislation – August 2021* https://www.derebus.org.za/new-legislation-august-2021/ accessed 3 August 2021

European Commission 2022 *Anti-money laundering and countering the financing of terrorism* https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-countering-financing-terrorism_en#:~:text=The%20European%20Union%20adopted%20the,the%20purpose%20of%20money%20laundering accessed 18 May 2022

Federal Bureau of Investigation 2022 *Ransomware* https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware accessed 13 September 2022

Fine TM 2022 *Basic Concepts of American Jurisprudence* https://www.lexisnexis.com/en-us/lawschool/pre-law/intro-to-american-legal-system.page#:~:text=The%20American%20system%20is%20a,of%20the%20matter%20before%20it accessed 15 May 2022

Hosch WL 2019 *Supercomputer* https://www.britannica.com/technology/supercomputer accessed 19 May 2022

Hsu SS 2022 *Husband jailed; wife freed in alleged laundering of $3.6 billion in hacked bitcoin funds* https://www.washingtonpost.com/dc-md-va/2022/02/14/bitcoin-launder-bitfinex-hack/ accessed 19 May 2022

IBA Anti-Money Laundering Forum date unknown *History of the European Union Anti-Money Laundering and Financing of Terrorism Directives* https://www.anti-moneylaundering.org/Europe.aspx accessed 18 May 2022

Lotha G 2019 *Fiat Money* https://www.britannica.com/topic/fiat-money accessed 6 September 2022

Makhafola G 2021 *Department of Justice says its recovering from cyber hack causing court case delays* https://www.news24.com/news24/SouthAfrica/News/department-of-justice-says-its-recovering-from-cyber-hack-causing-court-case-delays-20211010 accessed 27 February 2022

Merriam-Webster 2022 *Hit man* https://www.merriam-webster.com/dictionary/hit%20man accessed 10 March 2022

Michaelson L 2019 *Complying with RICA – A Guide* https://www.michalsons.com/blog/complying-with-rica/1157 accessed 29 May 2022

MoneyGram 2022 *About Money Gram* https://corporate.moneygram.com/about-moneygram?_ga=2.256835907.994472730.1642529561-111704851.1642529561 accessed 18 January 2022

Morris C 2021 *South African brothers disappear along with $3.6 billion in Bitcoin* https://fortune.com/2021/06/24/bitcoin-ameer-raees-cajee-theft-south-africa/ accessed 28 October 2021

Moss S 2020 European supercomputers hacked, apparently to mine cryptocurrency https://www.datacenterdynamics.com/en/news/european-supercomputers-hacked-mine-cryptocurrency/ accessed 19 May 2022

Ngqakamba S 2021 *Justice department's IT system brought down in ransomware attack* https://www.news24.com/news24/southafrica/news/justice-departments-it-system-brought-down-in-ransomware-attack-20210909 accessed 27 February 2022

O'Flaherty K 2019 *Notorious Hacking Forum and Black Market Darkode Is Back Online* https://www.forbes.com/sites/kateoflahertyuk/2019/04/10/notorious-hacking-forum-darkode-is-back-online/?sh=4761507752e8 accessed 10 March 2022

OECD 2019 *Understanding E-Commerce* https://www.oecd-ilibrary.org/sites/23561431en/1/2/1/index.html?itemId=/content/publication/23561431-en&_csp_=79ea8e97684c395730e471f402ce000e&itemIGO=oecd&itemContentType=book accessed 22 February 2022

Ongeso JP and Dyer L 2021 *South Africa: Constitutional Court Upholds Declaration of Invalidity of RICA* https://www.bowmanslaw.com/insights/mergers-and-acquisitions/south-africa-constitutional-court-upholds-declaration-of-invalidity-of-rica/ accessed 29 May 2022

Parliament of the Republic of South Africa 2022 *Protection of Constitutional Democracy Against Terrorism and Related Activities Amendment Bill (B15-2022)* https://www.parliament.gov.za/bill/2304183 accessed 13 September 2022

PPS (Professional Provident Society) 2021 *Press Release: Malicious Cyber-Attack* https://www.pps.co.za/malicious-cyber-attack accessed 6 June 2021

Rall S 2021 *Transnet cyber attack cripples movement of goods through port terminals* https://www.iol.co.za/news/south-africa/kwazulu-natal/transnet-cyber-attack-

cripples-movement-of-goods-through-port-terminals-3ea4ec21-dab1-4650-922e-47bc0a401bee accessed 27 February 2022

Rattue R 2019 *Days Numbered for Entirely Unregulated Cryptocurrency Marketplace* https://issuu.com/newmediab2b/docs/mm_march19?e=29764265/68263616 accessed 24 May 2021

Reeva D 2021 *Cyber attacks expose the vulnerability of South Africa's ports* https://issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports accessed 9 September 2021

Ryan C 2022 *Controversial bill aims to clamp down on crypto for terrorism financing* https://www.moneyweb.co.za/moneyweb-crypto/controversial-bill-aims-to-clamp-down-on-crypto-for-terrorism-financing/ accessed 10 October 2022

SARS 2021 *Crypto Assets and Tax* https://www.sars.gov.za/individuals/crypto-assets-tax/ accessed 5 January 2022

Schwab K 2016 *The Fourth Industrial Revolution: what it means, how to respond* https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/ accessed 28 February 2021

Sharma R 2021 *Non-Fungible Token (NFT) Definition* https://www.investopedia.com/non-fungible-tokens-nft-5115211 accessed 7 February 2022

Smith C 2021 *SA brothers' massive crypto 'heist': Financial watchdog says it was outside its ambit* https://www.news24.com/fin24/companies/sa-brothers-multi-billion-bitcoin-break-is-likely-biggest-ever-crypto-heist-20210624 accessed 2 February 2022

Sommers C and Bernstein E 2020 *Inside the FBI takedown of the mastermind behind website offering drugs, guns and murders for hire*

https://www.cbsnews.com/news/ross-ulbricht-dread-pirate-roberts-silk-road-fbi/ accessed 10 March 2022

Strydom J 2022 Crypto regulations in South Africa https://www.michalsons.com/blog/crypto-regulations-in-south-africa/56081 accessed 1 June 2022

United Nations Commission for International Trade Law date unknown *UNCITRAL Model Law on Electronic Commerce (1996) with additional article 5 bis as adopted in 1998* accessed 26 April 2022

United Nations Commission for International Trade Law date unknown *UNCITRAL Model Law on Electronic Signatures (2001)* accessed 26 April 2022

United Nations Commission for International Trade Law date unknown *United Nations Convention on the Use of Electronic Communications in International Contracts (2005)* accessed 13 May 2022

United States Department of Justice 2016 *Founder of Liberty Reserve Pleads Guilty to Laundering More Than $250 Million through His Digital Currency Business* https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital accessed 18 January 2022

United States Department of Justice 2022 *Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency* https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency accessed 19 May 2022

World Trade Organisation 2021 *Electronic Commerce* https://www.wto.org/english/thewto_e/minist_e/mc11_e/briefing_notes_e/bfecom_e.htm accessed 9 September 2021

Last updated: October 2022