Regulating cryptocurrencies in South Africa

William Chandler De Kock

DKCWIL004

A dissertation submitted to the Faculty of Commerce, University of Cape Town, in partial fulfilment of the requirements for the degree of Master of Philosophy.

February 05, 2019

MPhil in Financial Technology, University of Cape Town.

Declaration

I declare that this dissertation is my own, unaided work. It is being submitted for the Degree of Master of Philosophy to the University of Cape Town. It has not before been submitted for any degree or examination.

Abstract

Cryptocurrencies are one of the most exciting financial technologies that have emerged since the global financial crisis. It has spurred on a new financial ecosystem looking to enhance the traditional financial system. Many of the economic functions such as payments, investment, trading and capital raising have made it to the cryptocurrency industry. Regulators, who have not universally agreed on how to approach regulating cryptocurrency activity, are seeking the best approaches to ensuring financial stability. This paper looks at the risk posed by cryptocurrencies and how to regulate the activities. It applies this directly to the South African context and finds that cryptocurrency activities are easily accommodated within the South African regulatory framework with a set of minor definition changes.

Acknowledgements

Thanks to Co-Pierre Georg for giving continuous feedback that shaped this paper. The School of Economics at the Facility of Commerce for allowing the course to take place, the future of the South African financial industry is better off as a result of it. Tony Sneedon for allowing me to do the course when it was not easy for you to say yes, and Marius Reitz for being supportive and understanding throughout the year – I look forward to shaping the future with both of you. A massive thank you to friends and family who helped along the way, especially Leila Stein, who helped with proofreading this document and has been the most supportive person through the research process.

Table of Contents

Introduction

The focus of this paper is to demonstrate that the activities of cryptocurrencies fit within the South African regulatory framework. Cryptocurrencies are one of the most innovative developments in the financial industry. An active industry with many stakeholders that act on the fringes of the regulatory landscape due to the staggered approaches of various regulators. The global scope of cryptocurrency networks has received a disjointed approach as each monetary authority, or regulatory body has looked to respond to the emergent technology and as a result fragments it's status in many markets. The phenomena of cryptocurrencies pose a risk to the global regulatory world, not for the risks currently observed but due to the lack of a defined framework which encompass the activities seen in cryptocurrency activity.

This paper looks at the regulatory response to cryptocurrencies thus far on the global stage. It identifies the critical areas that regulators are interested in addressing, with respect to cryptocurrencies. Issues around money-laundering, terrorism financing and consumer protection, among others, are noted by the various regulators as a concern. The concerns are centred around the acknowledgment from regulators on the limited optics they have toward the activities of the industry. The response is best described as differing and segmented. This segmentation opens the risk for global regulatory arbitrage to occur.

The risks noted by the regulators are of valuable concern. To address the concerns from regulators as well as extend some of the other emerging threats, this paper notes the following risks: Monetary policy risks centred around a dual monetary system. The effects of an inelastic supply of new coin issuance resulting on the credibility of cryptocurrency as a means of payment. The misalignment in incentives through the

use of Initial Coin Offering's (ICO) between the founders of the ICO project and the users of the token resulting in diverging trajectories for the ICO project. The level of security and risk management of cryptocurrency service providers exposing consumers unknowingly at risk to a potential loss of funds through hacks or negligence. Investing and speculative behaviours creating cryptocurrency backed derivatives that are not regulated and also, have increased risk exposure due to their volatile nature.

Addressing the concerns, coupled with available cryptocurrency monitoring tools, this paper finds that regulating the economic functions as opposed to the activity brings cryptocurrency stakeholders (such as exchanges and service providers) into the regulatory framework as accountable financial service providers within South Africa. The use of the monitoring tools is required to expose the cryptocurrency activity to regulators in a more detailed manner. Following this, a series of principles that should be employed when drafting regulations should apply. These principles are to ensure the safety and efficiency of the financial industry, increase consumer protections, reduce regulatory arbitrage, while maintaining the social welfare aspects of the technology. This paper uses the framework set out by the Financial Conduct Authority.

Applying this to regulating the South African cryptocurrency market, it is shown that Exchange Controls, which are present in South Africa, is a challenge but not impossible to enforce with an active cryptocurrency market. By requiring service providers to act as a version Authorised Dealer and make use of monitoring tools, maintaining exchange controls is possible. The inclusion of cryptocurrencies into the Financial Intelligence Centre Act as well as the Financial Markets Act ensures that the financial protection of those Acts extends to consumers. It also ensures that service providers adhere to the code of conduct. By including cryptocurrencies to these Acts, the risks around money-laundering are addressed.

The naming convention of cryptocurrencies is not standard yet as a result of the development of various differing currency uses. Cryptocurrencies, Virtual Currencies, Virtual Assets, Crypto Assets, Tokens, Crypto Tokens and the abbreviated version Crypto, have all been used in the past. These different definitions have nuanced subtleties in the way they operate. However, for this paper, a broader and technology-agnostic approach applies. The importance is not on the specific implementation of cryptocurrencies but more on the general development of technology and the resulting activities.

The regulatory response to cryptocurrencies

The global response to cryptocurrencies is varied at best from jurisdictional markets. The response has ranged from differing degrees of permissible acceptance to deterrent warnings. The new prominence and evolving development of cryptocurrencies means that the responses from different regulatory is also expected to evolve. The increasing interest in cryptocurrencies as a payment mechanism, a new investment class or an innovative approach to financial technology has galvanised the regulators around the world to respond. The following section is a synopsis of the responses from various jurisdictions. The information is a collection of statements made by the central bank of each jurisdiction as well as regulatory bodies that have enforced cryptocurrency regulations.

Europe

The European Union's (EU) response has allowed the continuation cryptocurrency of activities but cite the risks surrounding the use of cryptocurrencies for money laundering purposes (Study on Cryptocurrencies and Blockchain 2018, 45). The main point of contention from the European Union Parliament is the pseudo-anonymity

around cryptocurrency transaction coupled with the lack of optics the regulatory bodies have on the industry. The approach from the EU is to amend the definition of Anti Money Laundering Directive 5 to include "virtual currencies". Which will ensure that service providers are obligated to do customer due diligence and report suspected transaction to financial intelligence centres (Study on Cryptocurrencies and Blockchain 2018, 45). The next phase following the inclusion of cryptocurrencies into the regulatory framework is to assess the nature of cryptocurrency activities and apply a tailored framework in line with the associated risk. The European Union seeks to lead a unified regulatory approach at a G20 level (Study on Cryptocurrencies and Blockchain 2018, 81).

United States

The United States has implemented regulation at both a federal level as well as at the various state levels. Agencies such as the Securities and Exchange Commission (SEC), the Commodities and Futures Trading Commission (CFTC) and the Federal Trade Commission (FTC), among other agencies, have all engaged together and with stakeholders to approach cryptocurrency regulations. The various states in the United States, such as New York, have issued a licence for activities relating to cryptocurrency activities which are called a BitLicense. In New York, this is administered through the New York State Department of Financial Services (2017). The scope of the licence encompasses people residing in, located in, having a place of business in, or conducting business in the State of New York

(Department of Financial Services 2017, 6). The limited scope of the BitLicense to only New York shows that there are movements within the United States to regulate cryptocurrencies, it has not universally adopted at the Federal level. The state of Hawaii has also introduced cryptocurrency regulations through the Division of Financial Institutions (2017). Of particular importance is that between the two states laws, different requirements mandated to the service providers within each state. In

New York, custodians and exchanges are required to hold the equal value of cryptocurrency of customers in reserve denominated in any cash or cryptocurrency (Department of Financial Services 2017, 16). The Hawaiian legislation requires custodians and exchanges to hold the funds of customers backed by cash collateral as the value attributed to cryptocurrency was not recognised (Department of Finacial Services 2017). The effects of having two different sets of requirements between Hawaii and New York will be explored later as an example of the adverse effects of different regulatory approaches.

India

India has not banned the use of cryptocurrencies, but the Reserve Bank of India (RBI) has issued a refusal for any regulated entity to engage with cryptocurrencies (Sinha 2018). The effect bans service providers from financial services. The Indian government, with the inclusion of the RBI, has set-up an interdisciplinary task force to measure the state of cryptocurrencies in India, the global regulatory stance and the measures used to address money laundering and consumer protection.

China

China has also had a history of having a regulation for cryptocurrencies that is restrictive without an outright ban. Similar to India, Chinese regulators have not banned the use of cryptocurrencies in the market but instead prohibit regulated institutions from dealing with cryptocurrencies (The Peoples Bank of China 2017). There is also an outright ban on exchange service providers and the use of an ICO to raise capital. Thus, the use of cryptocurrencies is exceptionally restricted other than sending and receiving between peers. In addition to the concerns around well-documented money-laundering from other jurisdictions, the People's Bank of China

notes the risk of cryptocurrencies being used to circumvent exchange controls (The Peoples Bank of China 2017). In China, there are strict currency controls for both individuals and corporates who require approval from the State Administration of Foreign exchange (SAFE). The regulatory bodies of China have identified the use of cryptocurrencies as a risk to destabilise the strict controls in place. As a measure to protect against the use of cryptocurrencies to transfer abroad is considered part of an individual or corporate limit. For example, if an individual in China sends more than $50 000 abroad using cryptocurrencies, it will violate their limitations.

Africa

The two biggest economies in Africa, South Africa and Nigeria, have permissive stances towards cryptocurrencies. In both markets, the central banks have issued warnings to the public stating some of their concerns. The Central Bank of Nigeria has stated it will endeavour to regulate cryptocurrencies shortly, but without a timeline for implementation (Central Bank of Nigeria 2017).

Countries in East Africa, such as Kenya, Tanzania, Uganda and Rwanda, have not published any substantive stance toward cryptocurrencies. In all cases, the central banks of each market have issued a public statement on the risks of cryptocurrencies. In Southern Africa, Botswana and Zambia central banks have followed a similar tactic of issuing a public warning and then adopting a "wait and see" stance.

There are a few markets in Africa with a confirmed prohibitive or banned status, such as Namibia and Zimbabwe in southern Africa; and Morocco, Algeria and Libya in North Africa. The ban in Namibia attributes to the Currency and Exchanges Act, No. 9 of 1993 prohibiting the set-up of any virtual currency exchanges in Namibia, of which, cryptocurrency is considered a part (Bank of Namibia 2018). The status quo in Zimbabwe is undetermined as the central bank forced a local exchange, Golix, to close

all accounts and operation, which is in dispute in the High Court of Zimbabwe (Tinashe 2018). Even with the court providing a temporary interdict, the outcome of the case is undetermined, and the overall stance of the Zimbabwean central bank not made sufficiently clear.

The other market in Africa that is showing a progressive stance, apart from South Africa and Nigeria, is Mauritius. Mauritius has issued a call to make use of its licensed regulatory sandbox (Economic Development Board n.d.). The intention is to attract start-up companies and financial technology innovators to Mauritius. The regulatory environment has been accommodating and to some extent, promoted in Mauritius.

Response Summary

As the understanding of cryptocurrencies activities improves, the approach to regulating them will converge to a series of outcomes. The common trends and themes seen in the response are as follows:

- Some jurisdictions have reduced the overall scope in which cryptocurrencies are allowed to operate in a market. This tactic prohibits regulated institutions in engaging with cryptocurrency activities. The regulator has not given an outright illegal status to cryptocurrencies but certainly does not consider it legal tender. The common reason attributed to this course of action is a risk mitigating stance from the regulator as each regulator forms its understanding of cryptocurrency activities. The restrictive policies are designed to reduce the overall scope of who can engage with cryptocurrencies, thereby reducing overall risk in India, China and Zimbabwe.

- The second approach is categorised by a "wait and see" style of policy response. The typical behaviour is to issue a form of blanket public warning on the risk of cryptocurrencies without any substantial detail as to the actual economic risk. This approach, in some cases, is prudent in terms of allowing the activities to continue, having warned their public, and stepping in when required. On the other hand, it does leave a level of uncertainty from consumers, businesses, stakeholders and service providers on how to approach the new technology on a detailed level. As the consensus of how to regulate cryptocurrencies evolves and as the detailed understanding of the risks evolve, these stances will change considerably in a relatively short time. While this stance does not mean that the local regulator leans towards a permissive or restrictive view, it means that their stance has not fully formed.

- The last theme that formed is an open, permissive and in some cases, accommodating approach — portrayed by allowing the industry to operate without direct intervention. While public warnings have been issued in these markets, they have not been followed-up with restrictive actions. Permissible and accommodative nature does not imply that regulators will not seek to impose regulations on the industry. The risk associated with cryptocurrencies is obvious and addressing the risk is an equally obvious endeavour. Pursuant to this, regulators have engaged with cryptocurrencies stakeholders to formulate a better understanding. The approach on a surface level is to respond with regulations in a manner that is appropriate to the risks seen in the market and ensure the benefits that the new technology enables remains.

Risks of cryptocurrencies

This section documents the risks associated with the economic functions of cryptocurrency, the activities of the industry and the risks posed by stakeholders. To varying degrees of reported detail, regulators have raised issues around money laundering, the legal tender status of cryptocurrencies, illicit behaviour and consumer risk. The activities in the cryptocurrency industry are not dissimilar to the traditional financial system and as a result, have overlapping risks. This section discusses the risks in detail.

Understanding the risk associated with the new technology may not be as trivial as initially noted. As innovation develops, new and differing risks emerge as new use cases appear. Cryptocurrencies have shown that many unique, nuanced and innovative features are created to solve particular frictions. Some cryptocurrencies emulate securities, others redeemable tokens on a particular platform and others a means of payment. The diverging use cases mean that the scope of regulation would need to be considerate of the particular paths the implementation intends to follow. The responses to any new developments would thus need to be adaptive to changes that open new risks. The following sections detail risks that have been identified.

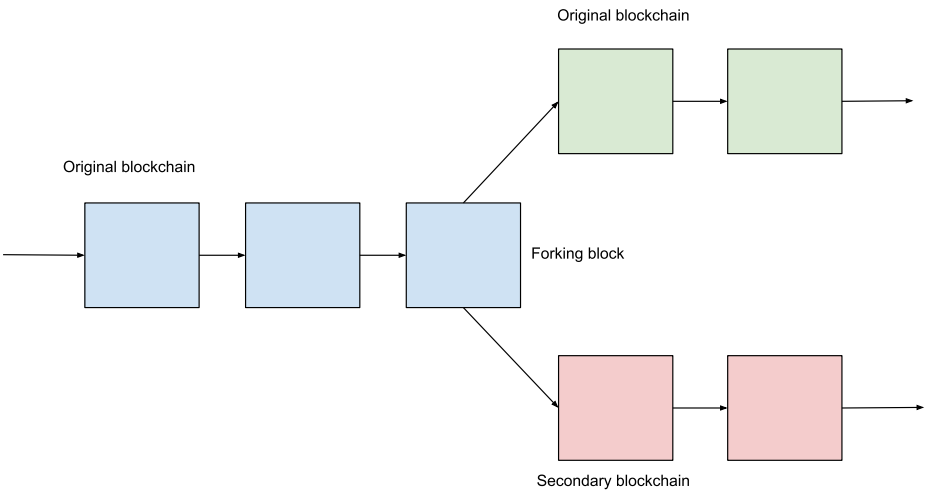
Monetary policy concerns

The currency-like features of cryptocurrencies raise the concern of whether cryptocurrencies are a challenge to central banks. A central bank monetary system relies on the ability of the central bank to control the money supply effectively. Adding a secondary independent monetary system such as cryptocurrencies has a wide range of potential risk for the efficiency of a central bank's policy instrument which may result in a loss of it's mandate. The current state of cryptocurrencies technology is not advanced enough to challenge or replace the functioning of a monetary authority

(Claeys, Demertzis, and Efstathiou 2018). While the protocols for cryptocurrencies can advance to such an extent to replace monetary systems, the risk, for the time being is relatively small. In order for cryptocurrencies to replace a monetary system, three main features would need to appear: i) cryptocurrencies would need to act as an instrument that affects an economy ii) the supply of currency will need to respond to liquidity shocks iii) the issuance of currency by the issuer, whether it be a decentralised protocol or central bank needs to be held accountable to principle (public) of the currency (Claeys, Demertzis, and Efstathiou 2018, 11). Given that many cryptocurrencies do not currently have any of these features, especially accountability (iii), limits the threat they pose to monetary authority's sole mandate as the issuer of money.

The monetary supply of cryptocurrencies in general also does not respond to any specific supply shocks to its issuance of new currency. Instead, through hard-forks, or splitting of chains, money supply expansion happens through the diverging protocol changes on a blockchain.

Figure 1 – Depicting the a blockchain fork to illustrate monetary expansion



Hard forks are where the blockchain of a particular cryptocurrency diverges into two different protocols which result in the expansion of a new cryptocurrency, in effect

expanding the monetary supply (Bank for International Settlements 2018, 96). Hard forks are typically protocol changes in a blockchain that change nature by the community that develops them. The original blockchain in a fork has a transactional record of all the activity on that blockchain. At some point in time, when there are two diverging proposals on changes to how the protocol of the blockchain is to be handled, a fork may emerge which illustrated as the forking block in Figure 1. The following result is a split of the original blockchain into two copies of itself. From there, the two blockchains act independently and are often not interoperable. The details of the mechanics of how forks happen are outside the scope of this paper, except for the critical point that forks are a version of monetary expansion independent of demand.

The first instance of a fork occurred is when the Bitcoin blockchain split into Bitcoin and Bitcoin Cash. After the split, both Bitcoin and Bitcoin Cash acted as separate and divergent protocols on separate blockchains which were not interoperable. Bitcoin continued the use of the original blockchain protocol, and Bitcoin Cash used the divergent version. The result was a doubling of the number of coins in circulation and also doubling the future supply. The cause of these splits is not a result of any monetary policy actions but instead of differing incentives of actors within the community, demonstrating the lack of independence or accountability of cryptocurrencies to maintain a credible monetary policy (Vigna 2017).

Consumer protection:

The fact that cryptocurrencies are not regulated but so closely emulate currency has implications for consumer protection. Consumers unknowingly enter cryptocurrency markets with a few realisations of the risk that pertain to the market. Without ensuring there is a standard protection framework in place, fraudulent management, opaque pricing and market manipulation, all with potential risk for consumers to lose funds, are left open to the broader public.

A history of lost consumer funds has been present in the cryptocurrency market. The infamous Mt Gox hack demonstrated the risks that service providers expose their customers to when entrusting them with their funds and not having adequate security measures in place (Frunza 2015, 66). The unknown state of many service providers security standards will continue to permeate the risk to consumers unknowingly.

There is also the notion of custody of funds which needs to be addressed. The consumer can have custody of their own funds or a service provider can offer a custody solution to consumers. Much like in the Mt Gox incident, the custodians of funds have full control over the safe keeping of funds. Not only is this an exposure to the potential for custodians to lose funds through negligence but there are implications for mismanagement of consumer funds. With no statutory requirements on how funds are managed by service provider custodians or requirements to how funds are used, misappropriations of funds are distinctly possible. Where the customer is the custodian of the funds, all risks of safeguarding the funds rests solely with the customer. This risk to the customer requires an understanding of the risk associated with being the sole owner of the funds. Loss of the funds in any shape or form has little to no recourse.

An integral part of ensuring consumer protection is consumer education. A more informed consumer is better able to discern the risks associated with entry to the market. Public warnings by central banks have been an attempt to expose the risk of cryptocurrencies. This broad stroke, while useful, does not address the risks on a micro-level. A more detailed and nuanced approach is required, which holds service providers responsible for ensuring there are no predatory practices taking place. Typical financial regulatory frameworks ensure fair and transparent practices, and if cryptocurrencies are to become financial products, the same measure are essential for the protection of the consumer.

Initial Coin Offerings:

Initial Coin Offering (ICO's) are funding mechanisms used to raise funds without the need for a traditional bank loan or equity sales for a particular project or platform through the issuance of digital coins or tokens. ICO's are an attractive mechanism for capital raising as the funds raised in an ICO can be larger than that of equity or debt financing alternatives (Catalini and Gans 2018). While the proposed solution of ICO's varies slightly, their general intended outcome is to solve market friction by making use of a token to transact on the platform (Cong, Li, and Wang 2019a, 2). The core component of an ICO is the whitepaper, which is to illustrate the solution to the friction. The whitepaper is meant to translate the technical aspects of the project, the roadmap, the key dates and milestones, the management of funds and the team behind the project (Merriam-Webster n.d.).

In an ICO an open and public funding round is made available to external investors to raise capital through token issuance. The token or coin being sold, often at a discount, will give the holder of the token access to the features of the platform. Access to the platform may be in the form of licences, rights to specific actions or transactional ability on the platform. The open and public feature of this type of financing means there is little to no barriers to enter an ICO. Forming a "crowd-funding" type mechanism but differs as there is no pre-sale commitment to token holders (Catalini and Gans 2018, 2). As a result of this lack of commitment to the token holder, coupled with the broad public investment scope, it is no surprise ICO's have been used to defraud investors. Some reports are indicating that around 80% of ICO's are scams (Dowlat 2018).

Outside of traditional financing options, ICO's offer the ability for platforms to realise network effects sooner as a result of the expected appreciation of the tokens value

(Cong, Li, and Wang 2019a). Consumers value both the productivity gains of the platform as well as the value gains of the token. It is giving the platform a reliable signalling mechanism to consumers if there is an expectation that the value of the token will increase. Under this result, the over-hyping of potential gains is more of a selling point for ICO's than the productivity gains which incentives the misleading and false information about the value of the ICO. A proposal for the safety of users is that a body vet any ICO's alleged promises, be it professional or regulatory, to ascertain the validity of claims.

An ICO needs to commit to issuance policy or a predetermined rate of issuance for the token. However, the capital raised from the ICO is maximized when the token growth rate is set to zero (Catalini and Gans 2018). A monetary supply commitment is needed as the value of the token is underpinned to the expectations set by that supply commitment. The project founders will always want to restrict the supply as a decrease in token supply increases the value of their holdings via the value of the token through scarcity. This is in contrast to the network effect growth of the platform, which is determined by user adoption which in turn is a function of token growth (Catalini and Gans 2018)(Cong, Li, and Wang 2019b). The opposing incentives bring into question the ability for the project founders to commit to the issuance of new tokens as it does not align with their maximal attainable value. This risk is a real economic incentive risk, and commitment devices have been into the codebases of various ICO's such as Ethereum.

ICO's are highly speculative with little ability for the investor to recoup their investments at a later stage. As with any new business venture, a large amount of risk is placed on the investor for the failure of the company, and thus proper due diligence on the venture is often required by investors. The lack of skill in a "crowd-funded" setting for investors to correctly discern if the project has viable merit means many

ICO projects reach funding goals but fail to recoup investors pledges. Educational requirements and standards for ICO's are required and public disclaimers for any investor to understand the risks associated with the investment.

The development of any new technology, especially on a mechanism and protocol level, brings about cybersecurity concerns. The robustness and protections available to the users of the platform are not known before investment. The unknown nature of these vulnerabilities follows the same scale and scope of other critical software protects.

Money laundering:

Money Laundering and Tax evasion are one of the most-cited risks of cryptocurrencies. While the risk is of great concern, the use of cryptocurrencies to launder money is no different from any other layering technique. Money launderers have benefited and exploited the lack of regulatory scrutiny or oversight of cryptocurrency. Many cryptocurrency exchanges and service providers are aware of this issue and implemented steps to reduce this specific risk by imposing standard money laundering practices such as "Know Your Customer" (KYC) (Brenig, Accorsi, and Günter 2015, 8). Even with voluntary compliance, this does not cover all exchanges and does not mandate a standard to comply.

The KYC requirements by exchanges are not fully enforced or mandated. The lack of any enforced standard means the lack of certainty on upholding AML across service providers. Without the standard to ensure KYC compliance, there is also no requirement to act on any information in the event of a money-laundering case as the service provider has no obligations to hand over customer information. The obligations of cryptocurrency service providers are quickly changed in across the globe in an attempt to combat money-laundering, with global guidelines from the *Financial Action*

Task Force (FATF 2019) including cryptocurrency. Given the urgency and need to solve money laundering risks, based off the associated risk, solving this will attract the most regulatory attention and action.

Payments:

The first use case for cryptocurrencies is as a means of secured and trusted payment. The risks associated with payments, is as a money-laundering and terrorism financing as mentioned previously. However its scope is of global significance(Brenig, Accorsi, and Günter 2015). The lack of monitoring and reporting requirements for cryptocurrency transactions is a gaping hole that has the potential to be used for money-laundering and terrorism financing. This risk has been mentioned extensively by various regulatory bodies around the world and is even tabled in the G20 agenda (Татьяна 2019). It is one of the crucial points for the global regulatory consensus to effectively mitigate money laundering and terrorism financing.

The use of cryptocurrency as a payment mechanism is suboptimal as a direct result of its constant and inflexible monetary supply. Purchasing power changes are drastic for any business to manage as a result of the volatile nature of cryptocurrencies (Harwick 2014). The purchasing power changes are a function of the constant monetary policy of cryptocurrency. In the Fisher equation of exchange MV = PT (M = Money supply, V= Velocity of circulation, P= Price level and T = Transactions), M is constant and known with cryptocurrencies and has no elasticity to its supply as the currency in circulation forms the money stock. With no flexibility to adjust supply, the price level must increase as a function of money demands. For this reason, there is little keeping the price level constant other than constant demand and resulting in the purchasing power of cryptocurrencies being dependant on its demand, which does not make for an exchangeable stable store of value.

To accept multiple currencies is an operational and technological cost for any merchant. The technological overhead of having to accept multiple currencies and the conversion between them being rather challenging for adoption. Additionally, the cross-currency exposure of multiple currencies, especially with the current volatility, is an even more of a deterrent. The price movements between cryptocurrencies are highly correlated, meaning there is some respite to the currency exposure risk but not enough to consider accepting multiple currency types. This overhead reduces the overall benefits present in using cryptocurrencies. This issue is also of particular concern when the notion of hard-forks create new coins outside of the consumers need.

To combat the overall effectiveness of cryptocurrency as a money-laundering and terrorism financing option, the Monetary Authority of Singapore has included the use of cryptocurrencies as part of its Payments Act (Monetary Authority of Singapore 2019). Ensuring all service providers be responsible for ensuring that the correct controls are in place to combat money-laundering.

Investing and speculation

Speculation on the price of cryptocurrencies has been the main driving force for much of the cryptocurrency activity. Traders make use of trading platforms, such as exchanges, OTC desk or peer-to-peer trades. The risks posed by speculative activities are related to service providers exposure to risk for consumers and tax avoidance.

There are few established frameworks for tackling the taxation of cryptocurrency, partly due to its different use cases. The definition of what form of cryptocurrency profits is to be classified as is a function of its economic function. In the case where cryptocurrency is an asset, it taxed through capital gains, and where it is a payment for goods and services, it is classified as income tax. While the uncertainty of how to

handle the taxation of cryptocurrencies will become apparent over time, there is an issue of the reporting of cryptocurrency activities to tax authorities (Houben and Snyers 2018, 53).

Service providers who facilitate speculative activities, such as trading, pose the most significant risk. Exchanges, custodial wallet providers, OTC desks all have similar roles to analogous service providers in the authorised financial industry. The holding of funds on behalf of customers, the facilitation of trades, the ability to transact all form part of the product service suite offered by cryptocurrency service providers but do not have the same rigorous requirements designed to ensure safe conduct. These protections are essential on a multitude of fronts such as money-laundering, regulatory arbitrage and consumer protection, which are imperative for a safe and stable financial sector. In some cases, limited KYC measures have been put in place but without any standard requirements, there is no certainty to the standard of KYC service providers in this space offer.

Service providers who hold funds on behalf of customers are also not required to ensure the correct security measures are put in place to safeguard funds held on behalf of customers. With the historical record of cyber-security hacks, such as the infamous Mt Gox, the need to ensure service providers are providing adequate protection is imperative.

Crypto derivative products:

In the run-up to the significant price rally, the returns to owning currency price by far yielded some of the highest returns, even with the returns being characteristic of an asset price bubble (Fry and Eng-Tuck 2016). Shortly after the bubble burst, investors sought alternative ways to recoup some of their losses. Giving scope for cryptocurrency derivative products gain attractiveness.

Some examples of these products are lending platforms such as Nexo and Genesis, margin trading on Kraken and finance and futures contracts with platforms like Gemini. The derivative products are analogous to other derivative markets with the underlying asset being a crypto asset base.

The emergence of crypto asset-backed investment vehicles has shed light on the lack of a defined legal framework for these instruments. The lack of classification and definition of crypto assets still means that these asset classes remain outside regulatory provisions and protections, which also implies a lack of a framework to handle derivate based products. The crypto asset-backed market can also be characterised by too much capital chasing too few borrowers. This incentive more risk-taking behaviour from lenders.

The volatility of crypto assets means its credibility as a store of value is not reliable enough to be considered a stable long-term investment (Bank for International Settlements 2018). Instead, crypto assets are, for the most part, considered a speculative investment. The high current volatility also means that pricing according to volatility for any cryptocurrency based derivative products becomes costly. While the advent of stablecoins has gained traction as a derivative product, its long-term viability is yet to be proven. A stable coin is a collateralized derivative of a basket of assets (cryptocurrencies or fiat) to synthetically create a stable cryptocurrency pegged to the underlying asset (Hayes 2019).

Uncorrelated price movements of cryptocurrencies to unsystematic factors but the highly correlated movements within the cryptocurrency markets does indicate that the cryptocurrency market has not been well-diversified (Griffin and Shams 2018). The international scope of cryptocurrencies means that the market may not ever follow

local market systemic factors. Indicating a risk factor for any cryptocurrency derivative product as the exposure to precise price movements has limited diversification potential.

Security and risk management:

While security and risk management are mentioned previously, it warrants its separate risk category. In almost all financial markets, a security and risk management framework is set in place for financial services companies and is required to keep up with best practices. Cryptocurrency service providers and also entrepreneurs who make use ICO's tend to hold funds on behalf of customers, personal data and transactional data. The funds and data, as with any company, is required to be safely maintained and secured according to best practises, an example being the Financial Services Sector Cybersecurity guide (2018). While the reputational harm of data breaches and hacks is a deterrent enough to be taken seriously by stakeholders in the industry, there are no requirements to ensure best security practises are maintained, and risk registers are updated. This opens up uncertainty to whether the security and risk-management practises of exchanges are indeed robust enough for adequate mitigation of the risks.

Monitoring cryptocurrency activity

For any regulator to have practical insight into an industry, it needs to be able to monitor the activities of that industry correctly. Monitoring the cryptocurrency industry is no different in this respect. This section will introduce the tools and stakeholders that are available to regulatory bodies to monitor.

Public and private keys

Before the discussion on how cryptocurrency transactions are monitored, the need to introduce essential public and private key cryptography is required. Public and private

key cryptography is used to verify and secure transactions between accounts or wallets over the specific cryptocurrency's network. The private key is used to cryptographically sign a transaction that is verified by using the public key to verify the transaction (Menezes, Van Oorschot, and Vanstone 1997). Public and private keys can have various relationship types. However, for this discussion it is limited to three generic types which are: i) a one-to-one relationship, ii) a many-to-one relationship also commonly known as a hierarchical deterministic wallet and iii) a one-to-many which can also be referred to as a multi-signature wallet (Wuille 2012).

I. A one-to-one relationship is where one private key links to one and only one public key. Only the private key can digitally sign transactions from the public key
II. Many-to-one or hierarchical deterministic key pair is where one private key can sign multiple public keys. It is not known that there is one private key to these multiple wallets
III. A one-to-many or multi-signature wallet is where more than one private key signs one public key transaction. This is a version of multiple authorisation wallet.

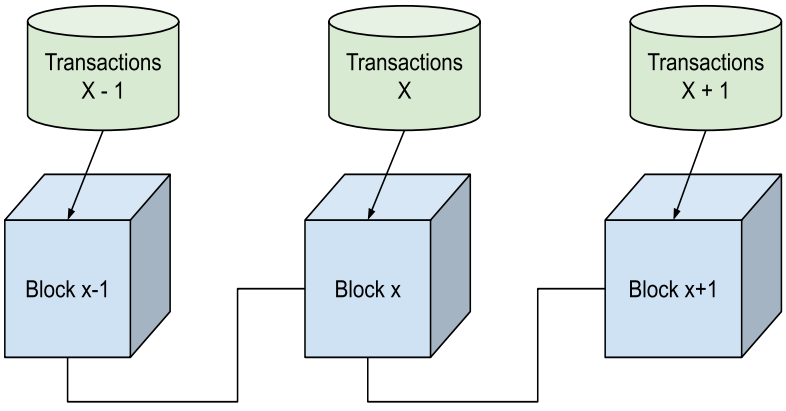
The introduction of custodial and non-custodial terminology is required as well. A custodial solution is one where a service provider has ownership of the private key and by implication control over the operations of the wallet. The customer of the service provider would then instruct the service provider to do an action (e.g. a transaction), and the service provider would then authenticate that action using the private key. The benefit for the user is that the lack of need to manage the safekeeping of the private key but is reliant on the service providers ability to do so. A non-custodial solution is one where software is developed to enable a customer to have full ownership of the private key. By implication, all actions would then also need to be authenticated

by the customer. The ownership and safekeeping of the private key are left to the customer in a non-custodial solution. The critical part worth noting is that ownership of the private key implies the ability to authenticate any action.

Not all cryptocurrencies employ these exact types of wallet structures, but in many instances, there is a variation of keys functionality. The vital point to be aware of is that ownership of the private key(s) dictates ownership of the funds held in the wallet. Loss compromised or stolen private keys means the value held within the wallet is at risk.

Blockchain data:

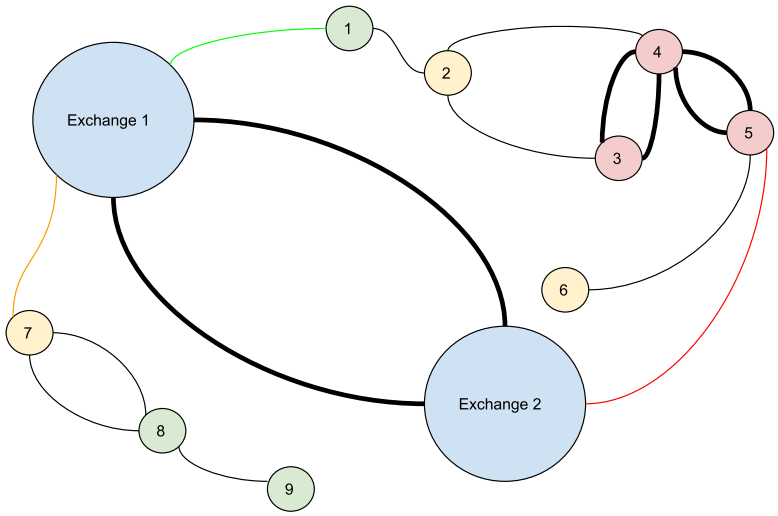
Figure 22 - Transaction chain showing the construction of a blockchain and the interlinking transactions



That many cryptocurrencies are built off of has a unique feature in which transactions are linked. Access to the data is open and verifiable. The entire database of all transactions and wallet balances are open for anyone to view and can be verifiable on the blockchain. Figure 1 depicts how each transaction is linked to the previous transaction in a chain format by using clustering and conventional spend analysis

techniques on linked blockchain data, common behavioural patterns can be identified. These tools have been used in the past, specifically to stop criminal behaviour (Malik 2018). This, however, can be translated to various other use cases. Transaction monitoring, identification of known entities, common financial flows, and allowing illicit flow are all possible. Two companies, Chain Analysis (Chain Analysis n.d.) and Elliptic (Elliptic n.d.) are examples of companies that have demonstrated the capabilities of these techniques. Below is a basic description of how these techniques are employed.

Figure 3 - Transactional flow between wallets derivate from open blockchain data



The critically challenging part of digesting the open blockchain data into tangible insights is possible by translating blockchain transactions into transaction chains. By making use of open transactional data and sorting by a wallet's history, then using the clustering techniques, a spend analysis pattern can emerge as In Figure 3.

In the figure above, the two large blue entities represent two large exchanges. The size of the circles as well as the thicker line connecting them represent a large number of funds held at the exchange and a large number of funds being transferred between them. The green entities are meant to represent known addresses or addresses that

have a positive score on them; the yellow entities are unknown due to a lack of transaction history on the blockchain or the lack of interaction with positive or negative clusters. The red addresses are marked as known addresses that have a history of transactions with other red addresses or have documented proof of risky behaviour. The connections between the accounts show the flow of funds between the account, the green being marked a safe transaction action, a yellow being marked an unknown transaction and the red being a risky transaction.

Even with this simple representation of blockchain analytics, a compelling picture can be built to demonstrate the transactional monitoring tool available. The richness of the data scales with the number of transactions between addresses that occur. To illustrate a series of hypothetical examples on the above figure based on, the following scenario can occur:

A response to the above monitoring tool is the development of a mixer. A mixer layers the inputs of transactions to mask the original input or source of funds (Chohan 2017). Mixers are well known to services like Chain Analysis and Elliptic and have been marked as high risk. This can be seen as a cluster of *red entities (numbered 3, 4, 5)* and also a large number of transactions between the addresses used to layer the source of funds by the thicker line. The red transaction thus going to or from *Exchange 2* can then be flagged as risky by a regulator or the exchange. Additionally, the unknown status of the *yellow entity 2* can be marked as risky, depending on the monitoring users risk preference. *Yellow entity 6*, may also be marked red, but due to a little history of transactional history with *red 5*, it cannot be determined if it is indeed partaking risky behaviour.

The yellow transaction to *yellow entity 7* oppositely can most likely be marked green as its transactional history has been with green *entity 8*, who also interacts with green entity 9, thus likely forming a cluster of low-risk entities.

Transactions between exchanges occur frequently and in large volumes. The addresses linked of exchange's services are known to blockchain analytics services, and where an exchange has required identity documents of its users, flows between exchanges, to and from exchanges and within the exchange are then linked to a person by the exchange.

Exchanges and storage providers:

As discussed previously, the use of transaction monitoring services by leveraging open blockchain data provides a powerful tool for a regulatory to have active optics into cryptocurrency transactions. This is only part of the equation that is required as the design of security mechanisms used by companies like exchanges that store a large number of concurrency coins on their platform breaks much of the linking of inflows and outflows of funds to and from exchanges.

A security mechanism used by cryptocurrency exchanges is a hot wallet and cold wallet storage solution. A hot wallet is defined as a cryptocurrency wallet that has its private key store online, whereas a cold wallet is not stored on the internet. This solution is meant to mitigate the cyber-security risk of hacking of the private keys (access to the funds) held by the exchange. The private keys being kept securely offline reduces the risk of them being exposed or compromised. The figure below shows how this works along with the use of various key structures to manage and maintain the funds between the hot and cold wallets.

Figure 4 - Hot and cold wallet set-up for cryptocurrency storage showing the difference between send and receive wallets at exchanges

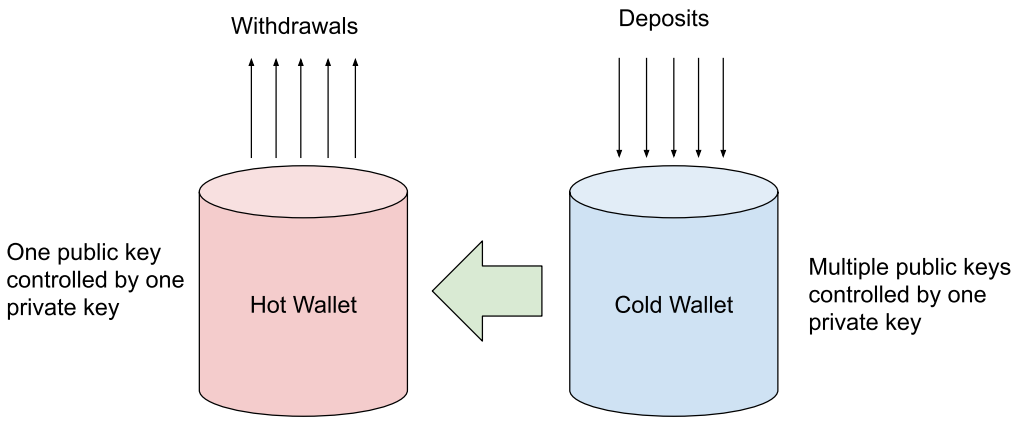


Figure 4 shows an example of the flow of funds of customers of exchanges using cryptocurrencies. Customers are able to deposit and withdrawal funds from their respective accounts at the exchange. Exchanges use a hot wallet and cold wallet storage solution to reduce the overall value of crypto assets that are sorted online as a security measure. The deposit of funds is sent to a public key that is linked to a customer's profile; this is generated for each customer receive address and is unique to the customer. This is illustrated as the deposits being received by the exchange's blue storage. The private key which is matched to the customers public key is in control of the exchange. This means there is a many to one relationship between the public keys and private keys on exchanges storage solutions.

Funds are sent out via a hot wallet which is a wallet that is meant to keep a reduced number of coins on a wallet that is online. Transactions sent out from the hot wallet are withdrawal instructed by customers but actioned by the exchange. The public and private key of this address is owned and operated by the exchange in a one-to-one relationship. The hot wallet is topped up by funds from the cold wallet periodically by the exchange to ensure there is always enough funds in the hot wallet to meet customer

withdrawal requests. This can be seen as the green arrow in the Figure 4. Critically, this step is in control of the exchange and is where transactions on exchanges lose their chain data. This is due to the number of deposits coming into the cold wallet, being transferred to the hot wallet and then being sent out of the hot wallet is linked via the opaque operations of the exchange. The exchange, however, does have the customer information on hand to be able to report on the receive and send addresses of each customer.

This set-up illustrates how exchanges obfuscate and mask the transactions done by customers as the deposit transaction done by a customer on an exchange is not the same address that does the withdrawal transaction. The security enhancements of not having the crypto assets held online are of an obvious customer safety benefit but do reduce the account optics for regulators. In the same vein, the exchange is also a valuable node in the transaction chain to be able to link and identity to a transaction.

This set-up shows that exchanges and service providers, in general, are critical stakeholders as their operations are pivotal to ensuring full exposure of cryptocurrency activity to any regulatory body.

Regulating crypto assets:

While many regulators have reacted differently to cryptocurrency, a consensus is forming around how to handle cryptocurrencies. Regulators' approaches have been somewhat divided with some markets even making it illegal to trade, such as China, or prohibiting financial institutions from interacting with cryptocurrencies companies, like India. While some of the responses have been hasty interventions, there is a more permissive tone emerging around how to regulate the cryptocurrency. This paper argues that the perception is due to a better understanding of how the technology

works and a realisation that many of the economic functions that are present in the cryptocurrency industry are not dissimilar to many other functions which fall within the regulations of traditional financial industry players.

Principles of regulations

This section deals with the framework used to guide the principles of regulating cryptocurrencies. The framework used in building up the principles of regulation is that employed by the Financial Conduct Authority (FCA). Their approach is data driven, pro-active and intelligence-led with the intend outcomes to promote competition, consumer protection and the advancement of welfare enhancing technologies. The applicability of using the FCA's principles are due to their extensive work with cryptocurrencies specifically. Their approach, guided off their principles, gives an effective framework off which to tackle the unregulated nature of cryptocurrencies. The following is the principles off which regulation should be based within the cryptocurrency industry. Following this, a Sandbox approach is discussed as a possible solution for regulators to handle the unknowns of new technologies. Lastly, the importance of a unified and consistent approach is required when handling the international nature of the new technology.

The task of regulating cryptocurrencies should encompass a series of objectives that are designed to put in place a framework on which policies should be based. The *safety and efficiency* of the financial system and financial institutions should be upheld. Additionally, *consumer and investor protection* must be put in place, and a concerted effort in education be undertaken as the economic functions are developing and will take time for the understanding of underlying risks to emerge. The tools to monitor and combat money laundering, illicit financial flows and tax evasion, among other nefarious behaviours will need to be developed and be used to combat those activities

effectively. Regulators will need to ensure that their specific policy stance does not create the environment for *regulatory arbitrage* both at the local level as well as the international level due to the global nature of cryptocurrencies. Finally, the framework should be permissible to the *advancement of financial technology development* in a manner that is responsible and where possible, even endeavour to support such developments.

Approaching the task of setting up a framework will require a series of guidelines on which to form policy. These guidelines have, in many cases, been done before, and the approach is not novel. The application is simply a translation of the various approaches to the new industry.

Many regulators have adopted a risk-based approach and simply states that the regulatory response should be in line with the identified risks associated with the activity. Critically, the risk needs to be correctly identified, and the response should be in line with mitigating the risk to the magnitude of the risk (Financial Conduct Authority 2020). The response needs to be technology-neutral and devoid of any specific implementation; instead, it should be directly based on the principles of the economic function. These facets have been well understood and implemented successfully in many jurisdictions, such as the United Kingdom under the advisory role of the FCA (Financial Conduct Authority 2016).

A phased approach to regulating the industry is also required as the technology itself is in development and will undergo changes. A phased approach adds complementariness to a risk-based approach as actions by regulators have the proper understanding of economic functions and intervene in a manner that is appropriate to the risk. A phased response also allows the benefits of being explored and any welfare benefits be allowed to continue, while simultaneously and continuously assessing the

risks that emerge. A phased approach also offers a more adaptive model which is imperative to a changing landscape.

Sandbox Approach

Many regulators have also adopted a sandbox approach when dealing with new technologies. Sandboxes are designed to test new business models, products or services in a time and scope limited manner (Financial Conduct Authority 2015). The intention of sandboxes, as stated by the FCA, is to determine the appropriate regulatory response and ascertain if a specific technology can safely operate in the marketplace. By allowing a sandbox testing environment, regulators can learn about the new technological developments, remove or stop detrimental innovations and allow incumbents the opportunity to test their products in a supported manner legally. The endeavour promotes a collaborative approach by allowing regulators to review and adopt regulations according to the outcomes of the sandbox testing and reduces the legal costs for firms to get their innovations accepted.

Innovation-linked sandboxes are a form of sandbox validation that encourages new innovative market entrants and then validates their business models. An example of this is the FCA which practises a cohort-based process. The intention is to gain real-time insights and understanding of the actual market developments. The sandbox encourages new market entrances and learns from the findings from cohort to cohort. There is a reduction in the cost of regulation as regulators get to be part of the development of innovations from inception.

Policy-linked sandboxes, on the other hand, are designed for discerning what policies are creating frictions for innovators. The outcomes are to encourage a modernisation of policies that are inhibitors to innovative technology. This has successfully been implemented by the Monetary Authority of Singapore (MAS). On the other hand, it

is challenging to discern which policies require re-writing and also what the change should reflect (MAS 2016b). The policy type is designed to encourage policy modernisation. Learnings from the sandbox are indented to identify the regulatory frictions innovators come across and to address them (MAS 2016c).

Unified approach

Consequent to the diverse reactions many regulators have had towards cryptocurrency means there is no unified approach to tackling the global phenomena. The opportunity arbitrage two differing implementations becomes more accessible as the interconnectedness of cryptocurrencies spans a global scale. A diverging set of requirements also imposes friction on companies wishing to be compliant with local regulations. To illustrate an example of this, the result of New York and Hawaii's local cryptocurrency service requirements mentioned earlier is used to show potential frictions.

Cryptocurrency service providers in New York have to comply with the New York BitLicense, similarly for the service providers in Hawaii. A service provider who operates in both markets will need to comply with both requirements. In New York, the service provider is required to hold all customer funds in cryptocurrency or cash reserves to ensure that all customer deposits can be called upon (fully collateralized). In Hawaii, the same requirement of having customer deposits in reserve is present with the difference being that the cryptocurrency reserve will have to be denominated in cash. These differing requirements imply that any service provider who operates in both markets is required to hold all customers funds in both cryptocurrency as well as the equivalent in cash. This, in effect, means the service provider would have to over-collateralize their reserve to comply with Hawaiian law, which did not deem cryptocurrency of value. Coinbase, a US-based cryptocurrency service provider, exited

the Hawaiian market expressing the inability to comply with both jurisdictional requirements simultaneously (Coinbase 2018).

Cryptocurrency regulation in South Africa

The South African Reserve Bank has been aware of developments in the cryptocurrency industry for some time and issued a position paper in 2014 clarifying a permissive but cautionary stance on the activities related to cryptocurrencies (SARB 2014). The need to expand on the scope of the regulation in South Africa is required to ensure the appropriate protections according to the size of the risks, to be in line with global regulatory developments and bring economic functions within the broader financial regulatory framework.

The economic function of cryptocurrencies needs to be regulated by the body that most appropriately covers that function and to be in line with the guidelines mentioned in the *Principles of regulations* section. If the economic function has no clear and discernible course of action, a sandboxed approach will allow the innovation to continue in a controlled manner with the regulator. The learning from the sandbox will inform policy decisions subsequently.

The initial step of regulating cryptocurrencies within South Africa would be to ascertain which legal and regulatory frameworks should be amended to encompass the activities. This is done by mentioning the regulatory bodies and acts that govern South Africa. From there the application to economic activities is applied to the respective frameworks is done. Where the inclusion of the activity is easily mapped to the current framework, the suggested path to do so is mentioned. In activities that do not have a defined body to regulate the activity, the recommended approach is to set-up a regulatory sandbox and ascertain the appropriate steps.

South African regulatory bodies

The most appropriate regulatory frameworks in South Africa that currently are applicable to discuss within the context of cryptocurrencies economic function in South Africa are the following: Exchanges Act (No. 9 of 1933), The Banks Act (1990), Financial Intelligence Centre Act (2001), Financial Markets Act (2012), National Payment Systems Act (1998) and the Financial Sector Regulation Act (2017). This section mentions the focus of each act and is used as the reference for which economic activity is most applicable in regulating cryptocurrencies within South Africa.

Currency and Exchanges Act (No. 9 of 1933), limits the number of funds that enter and leave South Africa. The SARB uses authorised dealers, mainly banks, to ensure compliance on this requirement. Currency controls in South Africa take the form of Single Discretionary Allowance (SDA's) for individuals which allows them to expropriate R1 million per year or an additional R10 million per year with a tax certificate (Currency and Exchanges Act 9 1993). This act has specific mention due to cryptocurrencies payments being able to circumvent currency controls.

The Banks Act (1990), requires any entity that carries out the business of a bank to be regulated as a bank. This regulation applies to monies being deposited at the entity being used to finance the activities or be used in any lending activity (SARB 1990).

Financial Intelligence Centre Act (2001) (FICA), is focused on combating money-laundering and terrorism financing within South Africa. The act imposes compliance-related obligations to accountable institutions as listed in Schedule 1 of the Act. This involves individual institutions being required to register with the Financial Intelligence Centre (FIC) and imposes obligations to the accountable institution to identify and verify its customers. As part of the obligations of the accountable

institutions, all suspicious transactions to the FIC (Financial Intelligence Centre Act 2001).

Financial Markets Act (2012) (FMA), provides for the regulation of financial markets and specifically the licensing of securities exchanges. According to the FMA, any entity who provides the infrastructure that (i) brings together buyers and sellers of securities, (ii) matches bids and offers for securities (iii) concludes a transaction where a bid and ask are successfully matched, is considered an exchange. The Act attempts to prohibit market abuse and outlines a code of conduct (Financial Markets Act 2012).

National Payment Systems Act (1998) (NPS), is overseen by the Payments Association of South Africa (PASA) which is a self-regulating body recognised by the SARB to oversee the payments infrastructure in South Africa (National Payment System Act 1998).

Financial Sector Regulation Act (2017) (FSR Act), ensures the financial stability within South Africa. The act has established the Financial Sector Conduct Authority (FSCA), which has the ability, with the addition of the Minister of Finance to amend and change legislation where appropriate (Financial Sector Regulation Act 2017).

Exchange control

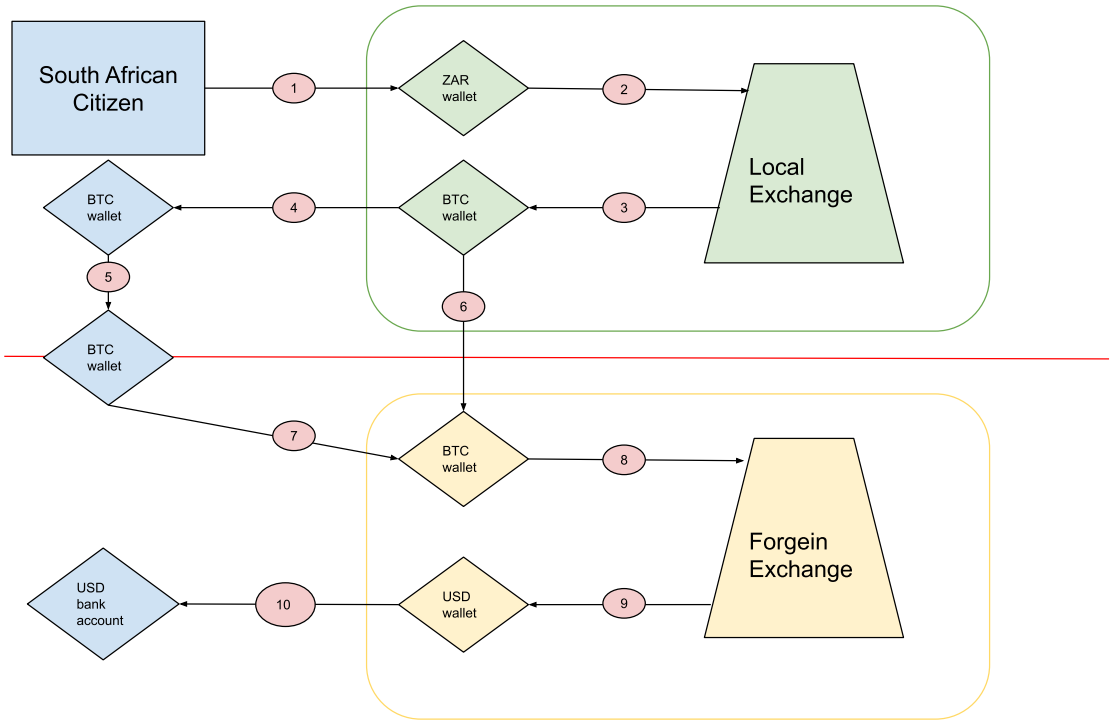
Exchange control regulations are easily circumvented with the use of cryptocurrency. This has previously been mentioned as an issue in China and has been acknowledged by the SARB, as mentioned in a clarification piece (SARB 2019). The challenge with enforcing exchanges controls with an active cryptocurrency market requires an appropriate level of monitoring to determine the extent at which exchange controls are being circumvented.

Exchange controls in South Africa is determined by section 9 of the Act and enforced by the designation of authorised dealers by the SARB, which are mainly banks. Control is maintained by only allowing authorised dealers to be able to send and receive foreign payments with approval from the SARB. Rights to approve and reject payments only sit with the SARB. This control effectively manages how the SARB is able to monitor cross-border financial transactions.

The lack of any particular authorised dealer in the cryptocurrency industry means there are no authorising requirements on any service provider. The natural suggestion would be to include the cryptocurrency service providers as authorised dealers, but this poses a distinct challenge as the mechanism on how a cryptocurrency transaction is authorised would require the SARB to have facilities to be able to authorise/reject cryptocurrency transactions which it currently does not have.

The following section will outline a typical transaction flow of a South African using Rands to buy cryptocurrency, sending the cryptocurrency to a different exchange, selling the cryptocurrency for a foreign denominated value. Following that, a series of points on how to approach currency controls with an active cryptocurrency market is made based on a phased approach.

Figure 5 - Transactions flow showing the flow of Rands to Dollars using cryptocurrencies



All items in Figure 5 show a specific colour which relates to wallets or accounts that are controlled by individual players in this flow. Blue is a South African person or business with foreign accounts; green is a South African cryptocurrency exchange and yellows a foreign cryptocurrency exchange. Bitcoin (BTC), Rands (ZAR) and Dollars (USD) are used as example currencies, but any combination of cryptocurrency or foreign currency can be used. The red numbered dots indicate the order of the flow of funds. The red line represents the exchange boundaries between Rands and foreign currency.

Additionally, the definition of a virtual wallet is a digital representation of a person's funds at an exchange in the form of a custodian wallet. The virtual wallet is operated by the person but controlled by the exchange (e.g. a customer of the exchange instructs

a Bitcoin send, the exchanges code executes the send function using the exchanges private key):

1. A person deposits Rands from their personal South African bank account to a South African cryptocurrency exchange. This deposit can happen in a variety of ways, but the most popular method is bank transfer. Other payment mechanisms can also include credit/debit card payments, PayPal or mobile money transfers. This is dependent on the payment integrations exchanges have with various payment mechanisms.
2. Once the payment is complete, the person has access to Rands in their virtual Rand wallet represented on the cryptocurrency exchange's interface, the most common method to house the aggregated funds are in a bank account that is operated by the exchange. The funds in the person's virtual wallet are used to place an order on the exchange.
3. After the order is completed, the Rand wallet is debited, and the Bitcoin wallet is credited. The counterparty to this transfer is another local person who is on the sell side of the order which debits Bitcoin and credits Rand. The exchange rate is the order book's market-clearing price. Much like the virtual Rand wallet, the Bitcoin wallet is a virtual representation of the person's Bitcoin held on the cryptocurrency exchange.
4. Once the Bitcoin has been traded it is available to be sent out to another Bitcoin address using the sending feature of the Bitcoin network. An important point to note at transaction 4 is that once the Bitcoin has been sent from the virtual Bitcoin wallet on the exchange, it leaves the control of the local exchange. The cryptocurrency exchange has ownership of the private key of the virtual wallet of the person's account, which means the exchange controls the ability for transaction 4 to be sent.

5. The Bitcoin network allows for transfer between any address. Given that the Bitcoin network is not in any one country, the transfer in point 5 shows that the Bitcoin address could be in any region. This is represented by the wallet being in between borders without any exact knowledge as to where it is. It is also important to note that once a Bitcoin payment has been made, it cannot be reversed.
6. Another possibility is that the Bitcoin can be sent between exchange wallets. One of the use cases is for the person to make use of their wallets at various cryptocurrency exchanges. The difference between doing a transfer between the person owned accounts and the virtual accounts between exchanges is that the exchanges are in control of these virtual wallets housed within their platform.
7. Additionally, transfers between these wallets can result in Bitcoin being deposited into the virtual wallet that originates from a series of previous transactions.
8. Bitcoin can then be sold on the foreign exchanges much in the same way they were bought, using an exchange with an order book and market clearing price; instead, the counterparty currency is not in the same that was used to buy the coin.
9. The value is now converted to US Dollar (or any other currency) and housed in the virtual wallet of the exchange
10. Funds are sent out of the account where the exchange keeps the funds and back to the person's bank account, denominated in a different currency.

The transactional flow above brings up a series of points that present itself in light of the Exchange Controls:

a) The denomination of funds being sent out in all cases is Bitcoin, and no Rands leave the borders of South Africa.

b) Once the conversion of Rands to Bitcoin has occurred, only transactions 4 and 6 can be controlled by the exchange. With the use of tools such as Chain Analysis, transaction 6 can be identified as being sent to a known address that is housed outside of South Africa. Transaction 4 and 5 can be between accounts that have not been identified.
c) Transaction 4, 5 and 7 are all unknown as to who the owner of the address or location of the address.

There is no distinct way to approach handling the use of cryptocurrencies to circumvent exchange controls as there is always level of uncertainty. The positioning of exchanges in this transaction flow, coupled with the transactional monitoring tool does provide a potential solution to be able to monitor some cryptocurrency flows and allieviate much of the uncertainty. Requiring exchanges to comply with identity verification requirements, in line with FICA, means there is an identity linked to cryptocurrency transactions. The transactions initiated by the person on the exchange can be monitored using a transaction monitoring tool. Depending on the known status of the receipt address, a decision can be made if the transaction does qualify for foreign payment send and thus count to the persons SDA.

If a risked-based and phased approach is to be undertaken, exchange control monitoring will need to leverage the position of exchanges and service providers with the transaction monitoring tools to identify the risk that cryptocurrencies pose on exchange controls. While the risk is well known, it is also vital for a clear understanding as to the magnitude of the risk. The response should be appropriate for this risk.

The suggested solution this paper puts forward is to leverage the stakeholders and tools indeed to correctly identify the magnitude that cryptocurrencies are being utilised to circumvent exchange controls. A simple blanket approach would be to state that all

trades from fiat to cryptocurrency are considered foreign currency conversions and would count to a person's SDA. This approach would, in effect then require exchanges to report all individual cryptocurrency trades and have that be part of their SDA. This blanket approach does ensure compliance with the Exchange Control Act but is heavy-handed and may stifle the use cases of other economic functions. It immediately limits the use of cryptocurrencies as a means of payment within the borders of South Africa; it reduces the possible size of investment any person can make and most importantly it reduces the potential of any future cryptocurrency product that has potential welfare enhancing benefits given that any exchange of cryptocurrency is counted towards SDA irrelavant of use.

A more progressive solution is to require cryptocurrency wallet providers and exchanges still to be brought into the Exchange Control regulation through being made Authorised Dealers and thus allowing the SARB to hold these providers accountable. However, instead of requiring all cryptocurrency trades to be declared as counting towards SDA, it counts towards SDA if the economic function being used realises funds outside of South Africa. This makes sense in light that most cryptocurrencies are being used as speculative investments and not cross-border payments (Dirk G Baur, Kihoon Hong, and Adrian D. Lee 2017). This can be in the form of a transaction between two wallets where the recipient wallet is known to be residing outside of South Africa. The benefit of this approach is that it limits the restrictions for individuals to want to make use of cryptocurrencies in South Africa for activities that are not in contravention of exchange controls (i.e. speculative investing). The task for the regulator to do is to asscerain the criteria for cryptocurrency transactions that count towards SDA and which do not.

While the latter suggested approach is more open and permissive, it does not address how to ensure that funds being sent out are being correctly identified and accounted.

This task is not trivial and would require a deeper engagement with stakeholders and the regulator. This is achievable if there is cross-collaboration between the SARB's Financial Surveillance Department and the service providers within South Africa with the use of monitoring tools to investigate guidelines on cryptocurrency transactions that comply with Exchange Control. The goal of the cross-collaboration is to map out scale and scope of the risks posed directly, identify mitigation solutions with the use of the transaction monitoring tools and implement regulation based on the specific economic function without restricting other sections.

Exchanges and OTC traders

Exchanges and OTC traders are the conversion point where fiat gets exchanged for cryptocurrency at a market-clearing price. The most appropriate forms of regulation that apply here are the Financial Markets Act and the Financial Intelligence Centre Act.

The Financial Markets Act, which, according to the definition above, appropriately matches the definition of the activities that occur in cryptocurrency trading. The scope of the Act is defined as only securities which do not include cryptocurrencies. By implication, exchanges fall outside of the scope of the FMA even if the activities are directly analogous to a traditional securities exchange. The inclusion of the cryptocurrencies to the scope of the Act requires an amendment to the definition of a security. Inclusion would thus mandate the need for exchanges to comply with the rules and code of conduct set out by the FMA. The intended goal is to ensure that the activities on cryptocurrency exchanges are not abusive to the general market, ensure the safety and security of the funds held on the exchange, and ensure the proper protections are in place for the consumer.

Financial Intelligence Centre Act is proposed by the Intergovernmental FinTech Working Group (IFWG) to be amended such that cryptocurrency exchanges are considered accountable institutions to the Financial Intelligence Centre (FIC) by amending Schedule 1 of the FICA (IFWG 2019). This obligates exchanges to ensure sufficient identity and verification customers or Know Your Customer (KYC) is done according to a risk-based approach. The identity verification must be in line with the Financial Action Task Force (FATF), a global set of recommendations to combating money laundering and recognised by the FIC. Currently, no cryptocurrency companies are considered an accountable institution and thus are not required to comply with FICA. As of now, this is voluntary as the FIC in South Africa does have cryptocurrency exchanges volunteering to share information. By including cryptocurrency activity in FICA as per the IFWG suggestion, the ability for the FIC to regulate and enforce AML through cryptocurrency exchanges improves significantly (IFWG 2019, 23). This requirement also allows for the leveraging of cryptocurrency transactions to no longer be pseudo-anonymous but instead have an identity linked to them when going through wallet service providers.

The Banking Act applies to companies that make use of deposit-taking to fund their leveraging activities. In the cases of exchanges, the deposits are used for trading and thus do not fall within the scope of the Banking Act's scope.

Wallet Service Providers:

Wallet service providers in many instances are also linked to exchanges service, and thus their appropriate regulation should go hand in hand with that suggested for exchanges. In both exchange and wallet service provider cases, the Financial Intelligence Centre Act applies as the activities of wallet service provides, act in many ways as transactional wallets or would be bank accounts. In order to keep money-

laundering activities in check, requiring a service provider who offers custodial wallets to the customer to ensure there are sufficient identity and verification services. It is important to note that there is a specific distinction of this being a custodial wallet service where the service provider is in ownership of the private keys. The actions of the customer are performed by the code base of the service provider. Meaning there is a control point that can be controlled by the exchange to intervene if nefarious actions are being taken by the customer.

The benefits of this service are that customers of the wallet are not at risk of personal loss of funds but then are entrusting the service provider to have sufficient security in place to manage the control of the funds. This service comes at the risk of any cyber-security risks, internal company fraud and negligence. There are methods and guidelines to manage these risks, ensuring that they are implemented for service providers who hold funds on behalf of others. Finding the appropriate regulatory framework for this may not be neatly housed within one particular Act. The FMA provides for the safekeeping of securities deposits which would enforce standard cyber-security, financial risk management and accountability to providers. Requiring the FMA to regulate wallet service providers makes more sense if the wallet service provider is linked to an exchange. The Banking Act also ensures the correct measures are put in place, but without the scope of wallet service providers having the activities of a bank, it should not be excluded. Without question, the need to guarantee that wallet service providers be required to uphold proper security practices is clear.

The National Payment Systems Act is meant to regulate payments within South Africa but is not applicable to regulate cryptocurrency payments. Given that many service providers offer various forms of payment solutions (payments being transfers as well) it is useful to look at the merit of the NPS's scope to be applied. Cryptocurrency activity does not fall into this for precisely two reasons, (i) cryptocurrency it is not a

form of legal tender according to SARB and (ii) merchants are under no obligations to accept cryptocurrency payments as a means of payment.

Exchanges that accept fiat payments in exchange for cryptocurrency do not offer a payment service as a primary source of business. Instead, payment services are used to support the main exchange business. The payment function of cryptocurrency exchanges or services is not on behalf of third parties. Besides, much of the payment infrastructure used by exchanges make use of payment service providers such as banks and credit card payment processors which themselves are regulated. If a merchant accepts cryptocurrencies as payment, it is at the sole discretion of the merchant and the buyer to agree on the method, and it will not be subject to the protections of the NPS. In the event that cryptocurrency payments become a viable alternative, their testing via a Sandbox is recommended.

The NPS is concerned with money-laundering activities and thus would seek to protect against the risk. Given that much of the money-laundering requirements would be covered in the FICA and the responsibility be placed on the service provider to report, there is minimal scope at present to include cryptocurrency payments within the NPS.

Moving over to the non-custodial wallet solution, where the software is provided to the customer gives them ownership of the private key, the ownership of response also shifts to the customer at their own risk. There is very little oversight that can be provided to customers that choose to operate their custodial wallet solution. Ensuring the customer is educated in the operations, implications and risk associated with using a custodial solution are needed. The risk of using this solution and the activities that follow rests solely with the user. Given that there is no accountable entity who controls the funds other than the user, there is little recourse for users.

Cryptocurrency derivative products:

Cryptocurrency derivative products are again an analogous version of traditional derivative products with the underlying asset being cryptocurrency assets. The most notable regulatory body that regulates derivative instruments is the FMA. Where the FMA would need to amend the wording of the act to include exchanges, the wording of the definition of a derivative instrument is not specific on the underlying asset. This means that any derivative instrument created using cryptocurrencies are classified as derivative instruments contingent on cryptocurrencies being recognised as a financial product. This also means that any company trading, creating or holding derivative instruments would need to confirm the FMA's rules.

Banking Act only applies to crypto companies that are making use of deposit-taking and leveraging funds. This does not hold too much weight as there are no crypto lending platforms in South Africa, but the activity is present and needs to be accounted for. This section also takes note of how crypto lending platforms are different from mutual funds as they are lending funds directly to other consumers with no investments.

The Financial Markets Act, 2012 (FMA) regulates derivative instruments. The definition of 'derivative instrument' in the FMA is agnostic as to the nature of the underlying or referenced asset, and it would, therefore, be possible to create a derivative instrument regarding crypto assets as an underlying asset.

Service providers that offer derivative products cryptocurrencies as the underlying asset class should, as with any other derivate product, be required to register with the financial market's authority and obtain a licence to trade. The conduct of derivate service providers would then need to conform to the requirements of the act, which

brings about significant consumer protection, market conduct protection and stability to cryptocurrency denominated derivatives.

Initial Coin Offerings

ICO issuance has a varying amount of risk. The framework for regulating ICO's does not currently exist in South Africa. As such, the proposed solution should be in line with the principle of regulation and address the risk associated. The following is a series of proposed solutions:

a) A framework set in place to ensure that ICO's in South Africa is vetted by professionals before being opened to the public. The outcome of the vetting should then be disclosed to potential investors. The selection of professionals should be made by an appropriate regulatory body
b) Ensure there is a credible commitment by the founding team to maintain the proposed token issuance to address the risk of shirking their proposed token issuance.
c) All funds raised in an ICO, be kept in a segregated account where it is mandated that the handling of those funds be in line with the mission statement of the project. This is to prevent prevalent cases of fraud.
d) Limit the ability for coin value gains to be the leading marketing component; instead, ICO projects should be considered on the merit of the social welfare enhancing attributes.

These solutions are designed around the risks highlighted in the *Risks of cryptocurrencies* section. The mitigation of these risk ensures the incentives of using an ICO to raise capital are in line with maximising consumer welfare.

Conclusion

Regulating cryptocurrency has not been a standard process throughout the world. With differing responses coming from different jurisdictions, the approach to regulating cryptocurrencies has not fully been determined. As a result, a series of risks are exposed, such as money-laundering, consumers being exploited through ICO's, risky derivative products and security standards not being implemented. These risks are analogous to any financial industry and are not unique to the cryptocurrency technology. This means the standard practises of other financial service providers through being regulated can be applied to the cryptocurrency industry. By including the cryptocurrency activities into the scope of regulatory frameworks, the ability to effectively mitigate against the exposed risks becomes possible.

Tools to effectively monitor and have oversight is paramount for any regulator to be able to enforce welfare enhancing behaviours. This is done by making use cryptocurrency transaction monitoring tools specifically used for regulatory purposes such as Chain Analysis and Elliptic. Transaction monitoring tools, coupled with service providers, such as exchanges, are positioned to be able to ensure effective monitoring activities.

To guide how regulation should be applied in South Africa, the principles of the FCA are used as a framework to base cryptocurrency regulations on. These principles are intended to ensure the efficiency of the financial industry, ensure consumer protection and promote the advancement of welfare enhancing technologies. Where there is uncertainty to how the technology will impact the financial industry or consumers, a sandbox approach is used to have the technology and regulator work hand in hand to understand the mechanics. There is also the need to ensure that regulations of any sort

for cryptocurrencies be in line with global trends to ensure there is no regulatory hurdles or regulatory arbitrage being created.

In the South African context, cryptocurrency regulation can easily be encompassed within the regulatory frame with a few amendments to certain financial Acts. Concerns around money-laundering and terrorism financing are addressed by including cryptocurrency service providers as accountable institutions to the Financial Intelligence centre through the Financial Intelligence Centre Act. Consumer protection and market conduct risks are addressed by mandating that service providers adhere to the code of conduct set out by the Financial Markets Act. In cases where cryptocurrency derivative products are being developed, licensing from the Financial Markets Authority is required.

The non-trivial task of maintaining exchange controls with an active cryptocurrency market requires cross-collaboration between service providers and the South African Reserve Bank to identify and classify cryptocurrency transactions that circumvent exchange controls. The use of monitoring tools such as Chain Analysis and Elliptic, which are designed for cryptocurrency regulation, is the pre-eminent tools for classifying transactions.

The full extent of cryptocurrency innovation has not yet been realised, and thus any regulatory action should not stifle innovative developments. Instead, it should be permissible to the possible welfare enhancing benefits as the technology matures. The risks created by the innovation to be addressed in a manner most appropriate to the size of the risk. Correctly identifying, and mitigating the risks is paramount to maintain financial stability and consumer protections.

References

Bank for International Settlements. 2018. 'V. Cryptocurrencies: Looking beyond the Hype'. https://www.bis.org/publ/arpdf/ar2018e5.htm (November 12, 2019).

Bank of Namibia. 2018. 'Revised Position on Cryptocurrencies'. https://www.bon.com.na/CMSTemplates/Bon/Files/bon.com.na/9a/9ab34d1a-07d7-45b3-859a-6e51814d690b.pdf (October 12, 2019).

Brenig, Christian, Rafael Accorsi, and Müller Günter. 2015. 'Economic Analysis of Cryptocurrency Backed Money Laundering'.

Catalini, Christian, and Joshua S Gans. 2018. 'Initial Coin Offerings And the Value of Crypto Tokens'. : 1–23.

Central Bank of Nigeria. 2017. 'Circular to Banks and Other Financial Institution on Virtual Currency Operations'. https://www.cbn.gov.ng/Out/2017/FPRD/AML%20January%202017%20Circular%20to%20FIs%20on%20Virtual%20Currency.pdf (November 12, 2019).

Chain Analysis. 'Building Trust in Blockchains'. https://www.chainalysis.com (November 12, 2019).

Chohan, Usman W. 2017. 'The Cryptocurrency Tumblers: Risks, Legality and Oversight'. *SSRN Electronic Journal*. https://www.ssrn.com/abstract=3080361 (January 21, 2020).

Chris Lee, and Mark Nakashima. 2017. 'Hawaii House Bill 1481'. https://legiscan.com/HI/bill/HB1481/2017.

Claeys, Grégory, Maria Demertzis, and Konstantinos Efstathiou. 2018. 'Cryptocurrencies and Monetary Policy'. https://www.agefi.fr/sites/agefi.fr/files/fichiers/2018/08/cryptomonnaies_bruegel.pdf (October 12, 2019).

Coinbase. 2018. 'Coinbase Accounts - Hawaii'. https://support.coinbase.com/customer/en/portal/articles/2754027-coinbase-accounts---hawaii (November 12, 2019).

Cong, Lin William, Ye Li, and Neng Wang. 2019a. 'Token-Based Platform Finance'. : 44.

———. 2019b. 'Tokenomics: Dynamic Adoption and Valuation'. : 43.

Currency and Exchanges Act 9 of 1933. 1993. 9 https://www.resbank.co.za/RegulationAndSupervision/FinancialSurveillanceAndExchangeControl/Legislation/Documents/Exchange%20Control%20Regulations,%201961.pdf (December 11, 2019).

Department of Financial Services. 2017. 'Part 200. Virtual Currencies'. https://web.archive.org/web/20170328214158/http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf.

Dirk G Baur, Kihoon Hong, and Adrian D. Lee. 2017. 'Bitcoin: Medium of Exchange or Speculative Assets?' *SSRN*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2561183.

Dowlat, Sherwin. 2018. 'Cryptoasset Market Coverage Initiation: Network Creation'. *Bloomberg*. https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ (January 21, 2020).

Economic Development Board. 'REGULATORY SANDBOX LICENCE'. http://cryptomauritius.io/licenses/regulatory-sandbox-licence/ (December 10, 2019).

Elliptic. 'Empowering Financial Institutions And Businesses To Deliver Safe And Trusted Services In Cryptocurrency'. https://www.elliptic.co (November 12, 2019).

FATF. 2019. 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers'. http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html (September 14, 2019).

Financial Conduct Authority. 2015. 'Regulatory Sandbox'. https://www.fca.org.uk/firms/innovation/regulatory-sandbox (November 12, 2019).

———. 2016. 'Principles of Good Regulation'. https://www.fca.org.uk/about/principles-good-regulation (September 12, 2019).

———. 2020. 'The FCA's Approach to Supervision'. https://www.handbook.fca.org.uk/handbook/SUP/1A/3.pdf (January 21, 2020).

Financial Intelligence Centre Act. 2001. 38 https://www.fic.gov.za/Documents/FIC%20Act%20with%202017%20amendments%20(1)%20(1).pdf (November 12, 2019).

Financial Markets Act. 2012. 19 No. 36121 https://www.gov.za/sites/default/files/gcis_document/201409/36121a.pdf (November 12, 2019).

Financial Sector Regulation Act. 2017. 9 http://www.treasury.gov.za/legislation/acts/2017/Act%209%20of%202017%20FinanSectorRegulation.pdf (December 11, 2019).

Frunza, Marius-Cristian. 2015. *Solving Modern Crime in Financial Markets: Analytics and Case Studies*. Academic Press.

Fry, John, and Cheah Eng-Tuck. 2016. 'Negative Bubbles and Shocks in Cryptocurrency Markets'. *Elsivier* 47: Pages 343-352.

Griffin, John M., and Amin Shams. 2018. 'Is Bitcoin Really Un-Tethered?' *SSRN Electronic Journal*. https://www.ssrn.com/abstract=3195066 (January 20, 2020).

Harwick, Cameron. 2014. 'Crypto-Currency and the Problem of Intermediation'. *The Independent Review* 20(4): 569–88.

Hayes, Adam. 2019. 'Stablecoin'. *Investopedia*. https://www.investopedia.com/terms/s/stablecoin.asp.

Houben, Dr Robby, and Alexander Snyers. 2018. 'Cryptocurrencies and Blockchain'. : 103.

IFWG. 2019. 'Consultation Paper on Policy Proposals for Crypto Assets'. https://www.fsca.co.za/Regulatory%20Frameworks/Documents%20for%20Consultation/CAR%20WG%20-%20Consultation%20paper%20on%20crypto%20assets.pdf (December 11, 2019).

Malik, Nikita. 2018. 'How Criminals And Terrorists Use Cryptocurrency: And How To Stop It'. *Forbes*. https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/ (November 12, 2019).

MAS. 2016b. 'Response to Feedback Received FinTech Regulatory Sandbox Guidelines'.

Menezes, A. J., Paul C. Van Oorschot, and Scott A. Vanstone. 1997. *Handbook of Applied Cryptography*. Boca Raton: CRC Press.

Merriam-Webster. 'White Paper'. *The Merriam-Webster.com Dictionary*. https://www.merriam-webster.com/dictionary/white%20paper (December 11, 2019).

Monetary Authority of Singapore. 2019. 'Consultation on the Payment of Services Act 2019: Scope of E-Money and Digital Payment Tokens'.

National Payment System Act. 1998. 22 https://www.resbank.co.za/AboutUs/Legislation/Documents/NPS%20Act/NPS%20Act%20-%20No.%2078%20of%201998.pdf (December 11, 2019).

SARB. 1990. No. R. 1029 *Banks Act*. https://www.gov.za/sites/default/files/gcis_document/201409/35950rg9872gon1029.pdf (December 11, 2019).

———. 2019. 'Virtual Currencies / Crypto-Currencies'. https://www.resbank.co.za/RegulationAndSupervision/FinancialSurveillanceAndExchangeControl/FAQs/Pages/VirtualCurrenciesCryptocurrencies.aspx (December 11, 2019).

Sinha, Saurav, ed. 2018. 'Prohibition on Dealing in Virtual Currencies'.

'Study on Cryptocurrencies and Blockchain'. 2018. http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf.

The Peoples Bank of China. 2017. 'Public Notice of the PBC, CAC, MIIT, SAIC, CBRC, CSRC and CIRC on Preventing Risks of Fundraising through Coin Offering'. http://static.iris.net.co/dinero/upload/documents/bitcoin-popular-bank-of-china.pdf (December 12, 2019).

Tinashe, Nyahasha. 2018. 'Golix Challenges The Reserve Bank Ban Of Cryptocurrency At The High Court'. *TechZim*. https://www.techzim.co.zw/2018/05/breaking-golix-challenges-the-reserve-bank-ban-of-cryptocurrency-at-the-high-court/ (January 20, 2020).

Vigna, Paul. 2017. 'Bitcoin Rival Launches in Volatile First Day Retrieved'. *Wall Stree Journal*.

Wuille, Pieter. 2012. *Hierarchical Deterministic Wallets*. https://github.com/bitcoin/bips/wiki/Comments:BIP-0032.

Татьяна, Чепкова. 2019. 'Cryptocurrency Regulations on the Agenda for World Finance Leaders at G20 Summit'. *Bein Crypto*. https://beincrypto.com/cryptocurrency-regulations-on-the-agenda-for-world-finance-leaders-at-g20-summit/ (January 12, 2019).