BANK of ZAMBIA

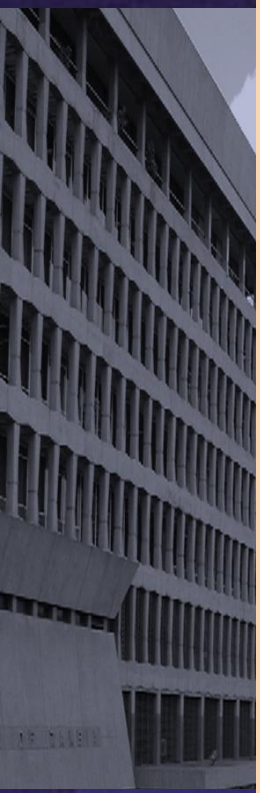
CRYPTOCURRENCY AND ITS PLACE IN COMMERCE AND CRIME

COMMONWEALTH LAW CONFERENCE HELD FROM 8-12 APRIL 2019 AT AVANI HOTEL

BY

Leonard Nkole Kalinde (Dr)(Notary Public)

Director - Legal Services and General Counsel, Bank of Zambia



BANK of ZAMBIA

OVERVIEW OF PRESENTATION

- Introduction
- The Concept of Cryptocurrency
- Commercial and/or Legitimate Usage of Cryptocurrency
- Potential Risks and/or Criminal Abuse of Cryptocurrency
- How to Manage Risks Posed by Cryptocurrency
- Conclusion

BANK of ZAMBIA

INTRODUCTION

- Cryptocurrencies —particularly Bitcoin—have garnered increasing attention, two popular narratives have emerged:(1)cryptocurrencies are the wave of the future for payment systems; and (2) cryptocurrencies provide a powerful new tool for criminals, terrorist financiers and other sanctions evaders to move and store illicit funds, out of the reach of law enforcement and other authorities.
- Regulators are looking at whether — and how — to regulate cryptocurrencies. Up till now there is no universal view on how to do that. In any event, there are compelling reasons why cryptocurrencies should be under more scrutiny by regulators and supervisors. The threat of price volatility, speculative trading, hack attacks, money laundering and terrorist financing all call for stricter regulation.
- This paper examines the potential use of cryptocurrencies in commerce and the risks and potential abuse of cryptocurrencies.

1.0. The Concept of Cryptocurrency

- The creation and issuance of currency in any jurisdiction is widely considered to be the role of a central bank or central government.

- However, cryptocurrency is "a digital representation of value that (i) is intended to constitute a peer-to-peer ("P2P") alternative to government-issued legal tender, (ii) is used as a general-purpose medium of exchange (independent of any central bank), (iii) is secured by a mechanism known as cryptography and (iv) can be converted into legal tender and vice versa". It is not issued nor guaranteed by any central bank or central government and fulfils the above functions only by agreement within the community of users of the cryptocurrency.

- Cryptography is the technique of protecting information by transforming it (i.e. encrypting it) into an unreadable format that can only be deciphered (or decrypted) by someone who possesses a secret key.

- As digital representations of value, cryptocurrencies fall within the broader category of digital currencies. However, they differ from other digital currencies, such as e-money, which is a digital payment mechanism for (and denominated in) fiat currency. Cryptocurrencies, on the other hand, are not denominated in fiat currency and have their own unit of account.

BANK of ZAMBIA

- Cryptocurrencies schemes comprise two key elements: (i) the digital representation of value or "currency" that can be transferred between parties; and (ii) the underlying payment and settlement mechanisms, including the distributed ledger system (blockchain technology).

- Cryptocurrencies schemes have different levels of convertibility to real-world goods, services, national currencies, or other cryptocurrencies.

- Non-convertible cryptocurrencies (or closed schemes) operate exclusively within a self-contained virtual environment. Under these systems, the exchange of cryptocurrencies with fiat currency (or other cryptocurrencies) or its use in payments for goods and services outside of the virtual domain is significantly restricted.

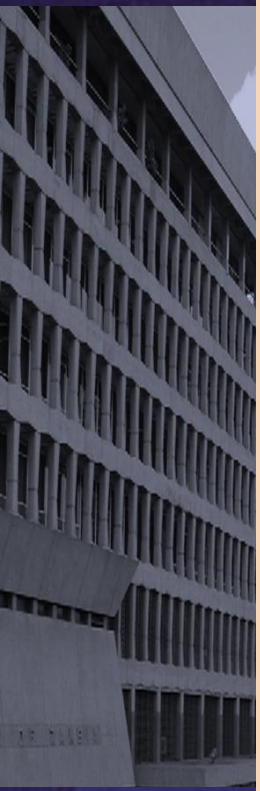
- In contrast, convertible cryptocurrencies (or open schemes) allow for the exchange of the cryptocurrencies with fiat currency (or other cryptocurrencies) and for payments for goods and services in the real economy.

- The level of contact between convertible (open schemes) cryptocurrencies and the real economy is much greater than is the case with non-convertible cryptocurrencies (closed schemes).

BANK of ZAMBIA

- Cryptocurrency relies on public and private keys to transfer value from one person (individual or entity) to another, and must be cryptographically signed each time it is transferred.

- The safety, integrity and balance of cryptocurrency ledgers is ensured by a network of mutually distrustful parties (referred to as miners) who protect the network in exchange for the opportunity to obtain a randomly distributed fee (in Bitcoin, a small number of newly created bitcoins, called the "block reward" and in some cases, also transaction fees paid by users as a incentive for miners to include their transactions in the next block).



2.0. COMMERCIAL AND/OR LEGITIMATE USAGE OF CRYPTOCURRENCY

BANK of ZAMBIA

- Like other new payment methods, cryptocurrency has legitimate uses, with prominent venture capital firms investing in cryptocurrency start-ups.

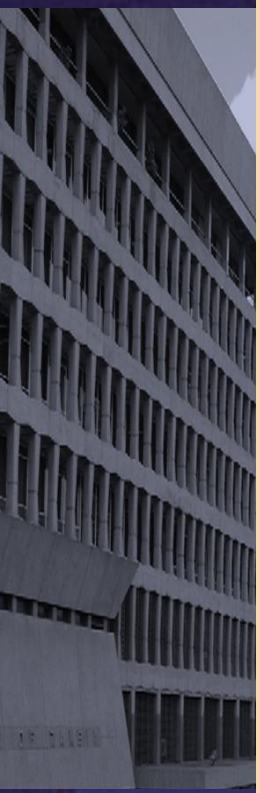
- Cryptocurrency has the potential to improve payment efficiency and reduce transaction costs for payments and fund transfers. For example, Bitcoin functions as a global currency that can avoid exchange fees, is currently processed with lower fees/charges than traditional credit and debit cards, and may potentially provide benefit to existing online payment systems, like Paypal.

- cryptocurrency may also facilitate micro-payments, allowing businesses to monetise very low-cost goods or services sold on the Internet, such as one-time game or music downloads. At present, as a practical matter, such items cannot be sold at an appropriately low per/unit cost because of the higher transaction costs associated with e.g., traditional credit and debit.

- Cryptocurrency may also facilitate international remittances and support financial inclusion in other ways, as new cryptocurrency-based products and services are developed that may potentially serve the under- and un-banked.

- Cryptocurrency - notably, Bitcoin- may also be held for investment.

BANK *of* ZAMBIA



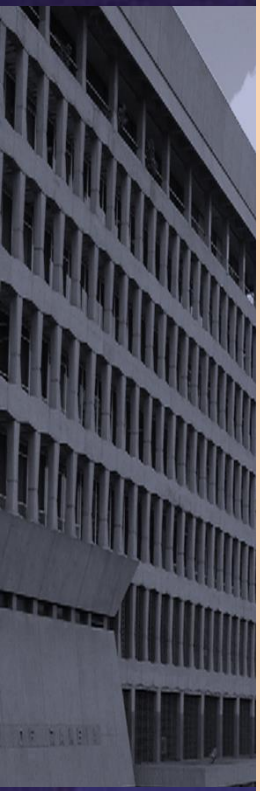
- While blockchain technology is often associated with cryptocurrency schemes, payments and financial services, its scope is much wider. Blockchain technology can theoretically be applied in a large variety of sectors (e.g. trade and commerce, healthcare, governance). In addition, it has numerous potential applications. It could have an impact on the pledging of collateral, on the registration of shares, bonds and other assets, on the transfer of property tiTles, on the operation of land registers etc.

- Blockchain technology simplifies the execution of a wide array of transactions that would normally require the intermediation of a third party (e.g. a custodian, a bank, a securities settlement system, broker-dealers, a trade repository). In essence, blockchain is all about decentralizing trust and enabling decentralized authentication of transactions. Simply put, it allows to cut out the "middleman". In many cases this will likely lead to efficiency gains.

- However, it is important to underscore that it may also expose interacting parties to certain risks that were previously managed by these intermediaries. For instance, the Bank for International Settlements ("BIS") recently warned in a report of 2017 titled Distributed ledger technology in payment, clearing and settlement, that the adoption of blockchain technology could introduce new liquidity risks. More in general it seems that when an intermediary functions as a buffer against important risks, such as systemic risk, he cannot simply be replaced by blockchain technology.

BANK of ZAMBIA

- These potential benefits of cryptocurrencies need to be carefully analysed, including whether claimed cost advantages will remain if cryptocurrency becomes subject to regulatory requirements similar to those that apply to other payments methods, and/or if exchange fees for cashing out into fiat currency are factored in, and whether volatility, consumer protection and other factors limit their potential for financial inclusion.



3.0. POTENTIAL RISKS AND/OR CRIMINAL ABUSE OF CRYPTOCURRENCY

- Cryptocurrencies that can be exchanged for real money or other cryptocurrencies are potentially vulnerable to money laundering and terrorist financing abuse for many reasons.

- First, they may allow greater anonymity than traditional non-cash payment methods. Cryptocurrency systems that can be traded on the Internet, are generally characterised by non-face-to-face customer relationships, and may permit anonymous funding (cash funding or third-party funding through virtual exchangers that do not properly identify the funding source). They may also permit anonymous transfers, if sender and recipient are not adequately identified.

- Decentralised systems are particularly vulnerable to anonymity risks. For example, by design, Bitcoin addresses, which function as accounts, have no names or other customer identification attached, and the system has no central server or service provider. The Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real world identity. There is no central oversight body, and no AML software currently available to monitor and identify suspicious transaction patterns.

BANK of ZAMBIA

- Law enforcement agencies cannot target one central location or entity (administrator) for investigative or asset seizure purposes (although authorities can target individual exchangers for client information that the exchanger may collect). It thus offers a level of potential anonymity impossible with traditional credit and debit cards or older online payment systems, such as PayPal.

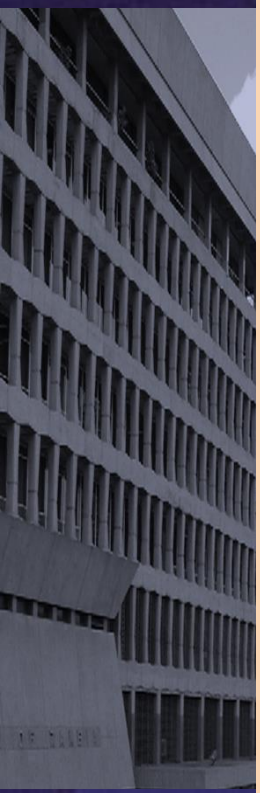
- Cryptocurrency's global reach likewise increases its potential AML/CFT risks. Cryptocurrency systems can be accessed via the Internet (including via mobile phones) and can be used to make cross-border payments and funds transfers. In addition, cryptocurrencies commonly rely on complex infrastructures that involve several entities, often spread across several countries, to transfer funds or execute payments. This segmentation of services means that responsibility for AML/CFT compliance and supervision/enforcement may be unclear.

- Moreover, customer and transaction records may be held by different entities, often in different jurisdictions, making it more difficult for law enforcement and regulators to access them. This problem is exacerbated by the rapidly evolving nature of decentralised cryptocurrency technology and business models, including the changing number and types/roles of participants providing services in cryptocurrency payments systems.

BANK of ZAMBIA

- And importantly, components of a virtual currency system may be located in jurisdictions that do not have adequate AML/CFT controls. Centralised cryptocurrency systems could be complicit in money laundering and could deliberately seek out jurisdictions with weak AML/CFT regimes. Decentralised convertible cryptocurrencies allowing anonymous person-to-person transactions may seem to exist in a digital universe entirely outside the reach of any particular country.

- Law enforcement is already seeing cases that involve the abuse of cryptocurrency for money laundering purposes. Examples include:



1.0. LIBERTY RESERVE

In what is to date the largest online money-laundering case in history, in May 2013, the US Department of Justice charged Liberty Reserve, a Costa Rica-based money transmitter, and seven of its principals and employees with operating an unregistered money transmitter business and money laundering for facilitating the movement of more than 6 billion USD in illicit proceeds. In a coordinated action, the Department of the Treasury identified Liberty Reserve as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act, effectively cutting it off from the US financial system.

- Established in 2006, Liberty Reserve was designed to avoid regulatory and law enforcement scrutiny and help criminals distribute, store, and launder the proceeds of credit card fraud, identity theft, investment fraud, computer hacking, narcotics trafficking, and child pornography by enabling them to conduct anonymous and untraceable financial transactions. Operating on an enormous scale, it had more than a million users worldwide, including more than 200 000 in the United States, and handled approximately 55 million transactions, almost all of which were illegal. It had its own cryptocurrency, Liberty Dollars (LR), but at each end, transfers were denominated and stored in fiat currency (US dollars).

- To use LR currency, a user opened an account through the Liberty Reserve website. While Liberty Reserve ostensibly required basic identifying information, it did not validate identities. Users routinely established accounts under false names, including blatantly criminal names ("Russia Hackers," "Hacker Account," "Joe Bogus") and blatantly false addresses ("123 Fake Main Street, Completely Made Up City, New York"). To add a further layer of anonymity, Liberty Reserve required users to make deposits and withdrawals through recommended third-party exchangers—generally, unlicensed money transmitting businesses operating in Russia, and in several countries without significant governmental money laundering oversight or regulation at that time, such as Malaysia, Nigeria, and Vietnam.

- By avoiding direct deposits and withdrawals from users, Liberty Reserve evaded collecting information about them through banking transactions or other activity that would create a central paper trail. Once an account was established, a user could conduct transactions with other Liberty Reserve users by transferring LR from his or her account to other users, including front company "merchants" that accepted LR as payment. For an extra "privacy fee" (75 US cents per transaction), users could hide their Liberty Reserve account numbers when transferring funds, making the transfers completely untraceable. After learning it was being investigated by US law enforcement, Liberty Reserve pretended to shut down in Costa Rica but continued to operate through a set of shell companies, moving millions through their accounts in Australia, Cyprus, China, Hong Kong, Morocco, Russia, Spain and elsewhere.

SILK ROAD

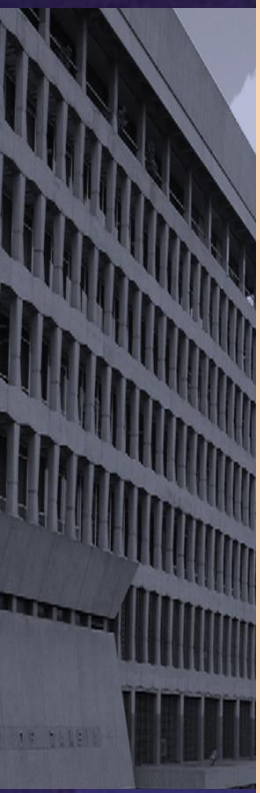
- In September 2013, the US Department of Justice unsealed a criminal complaint charging the alleged owner and operator of Silk Road, a hidden website designed to enable its users to buy and sell illegal drugs, weapons, stolen identity information and other unlawful goods and services anonymously and beyond the reach of law enforcement agents, with narcotics trafficking, computer hacking, and money laundering conspiracies.

BANK of ZAMBIA

- The Justice Department also seized the website and approximately 173 991 bitcoins, worth more than USD 33.6 million at the time of the seizure, from seized computer hardware. The individual was arrested in San Francisco in October and indicted in February 2014; the investigation is ongoing.

- Launched in January 2011, Silk Road operated as a global black-market cyber bazaar that brokered anonymous criminal transactions and was used by several thousand drug dealers and other unlawful vendors to distribute unlawful goods and services to over a hundred thousand buyers, a third of whom are believed to have been in the United States. It allegedly generated total sales revenue of approximately USD 1.2 billion (more than 9.5 million bitcoins) and approximately USD 80 million (more than 600 000 bitcoins) in commissions for Silk Road. Hundreds of millions of dollars were laundered from these illegal transactions (based on bitcoin value as of dates of seizure). Commissions ranged from 8 to 15 percent of total sales price.

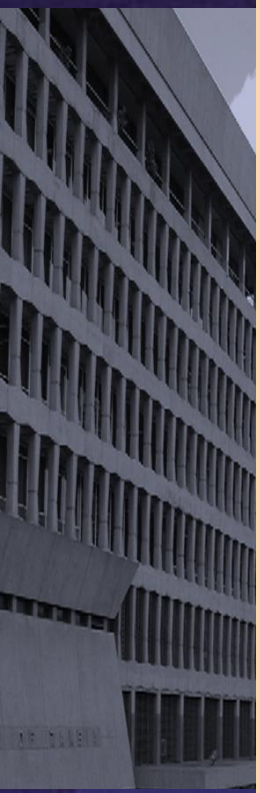
- Silk Road achieved anonymity by operating on the hidden Tor network and accepting only bitcoins for payment. Using bitcoins as the exclusive currency on Silk Road allowed purchasers and sellers to further conceal their identity, since senders and recipients of peer-to-peer (P2P) bitcoin transactions are identified only by the anonymous bitcoin address/account. Moreover, users can obtain an unlimited number of bitcoin addresses and use a different one for each transaction, further obscuring the trail of illicit proceeds. Users can also employ additional "anonymisers," beyond the tumbler service built into Silk Road transactions.



- Silk Road's payment system functioned as an internal Bitcoin bank, where every Silk Road user had to hold an account in order to conduct transactions on the site. Every Silk Road user had at least one Silk Road Bitcoin address (and potentially thousands) associated with the user's Silk Road account, stored on wallets maintained on servers controlled by Silk Road. To make a purchase, a user obtained bitcoins (typically through a Bitcoin exchanger) and sent them to a Bitcoin address associated with his or her Silk Road account to fund the account. When a purchase was made, Silk Road transferred the user's bitcoins to an escrow account it maintained, pending completion of the transaction, and then transferred the user's / buyer's bitcoins from the escrow account to the vendor's Silk Road Bitcoin address. As a further step, Silk Road employed a "tumbler" for every purchase, which, as the site explained, "sen[t] all payments through a complex, semi-random series of dummy transactions ... --making it nearly impossible to link your payment with any [bit]coins leaving the site."

WESTERN EXPRESS INTERNATIONAL

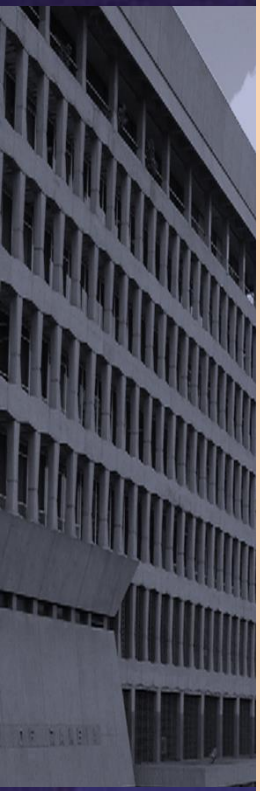
- An eight-year investigation of a multinational, Internet-based cybercrime group, the Western Express Cybercrime Group, resulted in convictions or guilty pleas of 16 of its members for their role in a global identity theft/cyber fraud scheme. Members of the cybercrime group interacted and communicated primarily through Internet "carding" web sites devoted to trafficking in stolen credit card and personal identifying information and used false identities, anonymous instant messenger accounts, anonymous email accounts, and anonymous cryptocurrency accounts to conceal the existence and purpose of the criminal enterprise; avoid detection by law enforcement and regulatory agencies; and maintain their anonymity.



- The criminal enterprise was composed of vendors, buyers, cybercrime services providers, and money movers located in numerous countries, ranging from Ukraine and throughout Eastern Europe to the United States. The vendors sold nearly 100 000 stolen credit card numbers and other personal identification information through the Internet, taking payment mostly in e-Gold and WebMoney. The buyers used the stolen identities to forge credit cards and purchase expensive merchandise, which they fenced (including via reshipping schemes), committing additional crimes, such as larceny, criminal possession of stolen property, and fraud, and generating about USD 5 million in credit card fraud proceeds. The cybercrime services providers promoted, facilitated, and aided in the purchase, sale and fraudulent use of stolen credit card numbers and other personal identifying information by providing computer services to the vendors and the buyers. The money mover laundered the cybercrime group's illicit proceeds in a variety of high-tech ways, moving more than USD 35 million through various accounts.

- The hub of the entire operation was Western Express International, Inc., a New York corporation based in Manhattan that operated as a cryptocurrency exchanger and unregistered money transmitter to coordinate and facilitate the Internet payment methods used by the criminal enterprise, and to launder the group's proceeds. One of the largest cryptocurrency exchangers in the United States, Western Express International exchanged a total of USD 15 million in WebMoney and USD 20 million in e-Gold for the cybercrime group and used banks and traditional money transmitters to move large sums of money. It also provided information and assistance through its websites (including Dengiforum.com and Paycard2000.com) on ways to move money anonymously and to insulate oneself from reporting requirements.

Western Express International and its owner/operator, a Ukrainian national, plead guilty in February 2013 in New York State to money laundering, fraud, and conspiracy offenses. (In February 2006, Western Express was also indicted for running an illegal check cashing/wire transfer service.) Three other defendants were convicted after trial in June 2013; several more plead guilty in August 2009. Two indicted defendants remain fugitives. The investigation was conducted jointly by the US Secret Service and the Manhattan (New York County) District Attorney's Office and was successfully prosecuted by the Manhattan District Attorney's Office.



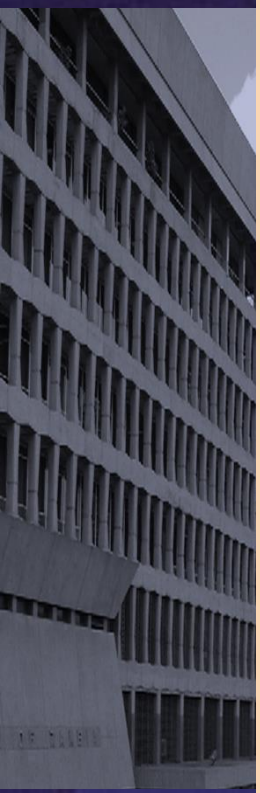
BANK of ZAMBIA

HOW TO MANAGE RISKS POSED BY CRYPTOCURRENCY

- The key issue that needs to be addressed in order to adequately capture cryptocurrencies and cryptocurrency players, particularly users, in legislation is to unveil the anonymity, varying from complete anonymity to pseudo-anonymity, that surrounds them.

- This is the biggest problem for combating money laundering and countering terrorist financing: the anonymity prevents cryptocurrency transactions from being adequately monitored, allowing shady transactions to occur outside of the regulatory perimeter, allowing criminal organisations to use cryptocurrencies to obtain easy access to "clean cash" (both cash in/out). Relating to terrorist financing, the story of Ali Shukri Amin who provided instructions over Twitter on how to use Bitcoin to mask the provision of funds to Daesh (Islamic State) is a striking example of the risks brought by the anonymity surrounding cryptocurrencies.

- Anonymity is also the major issue when it comes to tax evasion. Entering into taxable cryptocurrency transactions without paying taxes is tax evasion. But, when a tax authority does not know who enters into the taxable transaction, because of the anonymity involved, it cannot detect nor sanction this tax evasion. This makes cryptocurrencies a very attractive means for tax evaders. By some commentators instruments such as Bitcoin were even described as "tomorrow's tax havens"

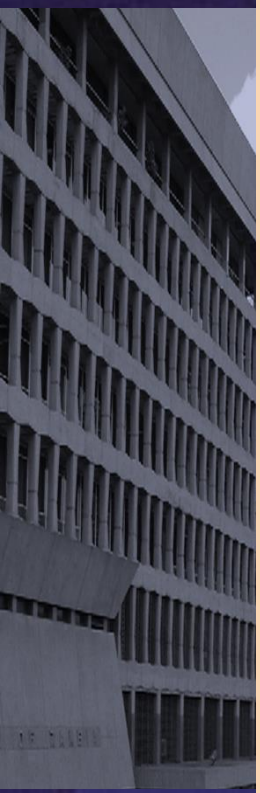


- This being said, and as apparent from our overview of cryptocurrencies above, it should be noted that some cryptocurrencies are pseudo-anonymous, which basically means that if great effort is made and complex techniques are deployed, it is possible for authorities to find out users' identities.

- Although this can already be a help in the fight against money laundering, terrorist financing and tax evasion in some cases, it does not allow a standardized approach to tackle money laundering, terrorist financing and tax evasion more widely: discovering identities in this way is too complex and costly to become the general answer to tackling this issue - and moreover, it will not certainly lead to any result.

- In addition to anonymity, the intrinsically cross-border nature of cryptocurrencies, crypto markets and crypto players is a major challenge for regulators. One of the issues is e.g. that crypto markets and crypto players can be located in jurisdictions that do not have effective money laundering and terrorist financing controls in place.

- The cross-border nature of cryptocurrencies, crypto markets and crypto players probably means that rules will only be adequate when they are taken at a sufficiently international level.



- Another factor of importance challenging the fight against money laundering, terrorist financing and tax evasion is that there is often no central intermediary, such as an issuer, that would normally be the focal point of regulation. Therefore, an important question is to which players in the crypto market should regulation be attached, absent a central intermediary.

- There are simply no rules unveiling the anonymity associated with crypto-currencies, making the question whether they are taken at the right level or to whom they apply a superfluous one. Because of the absence of rules unveiling anonymity, more substantive rules that currently could already have cryptocurrencies in scope completely miss effect. So, the crux of the matter is how can we unveil the anonymity related to cryptocurrency transactions so as to be able to track the illegal transactions.

BANK of ZAMBIA

CONCLUSION

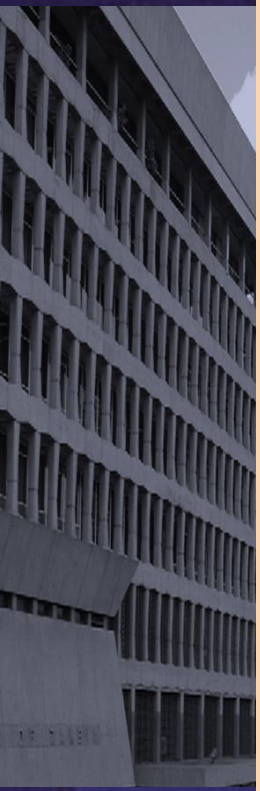
- It is important to note that the cryptocurrency landscape is still new and rapidly changing. It is therefore not possible to fully predict the future direction and importance of these evolving technologies or to identify specific longer-term policy responses.

- Any policy response to cryptocurrency will need to strike an appropriate balance between forcefully addressing risks and abuses while avoiding overregulation that could stifle innovation. The initial focus should be on the most pressing concerns related to cryptocurrencies —including financial integrity, consumer/investor protection, and tax evasion—while leaving less immediate risks (for example, financial stability, monetary policy) to a later stage.

- Effective policy coordination will therefore be required at the national and international levels. More could be done at the international level to facilitate the development of appropriate policy responses. As experience is gained, developing international standards and best practices could be considered to provide guidance on the most appropriate regulatory responses in different fields, thereby promoting harmonization across jurisdictions.

- Such standards could also set out frameworks for cooperation and coordination across countries over such questions as the sharing of information and the investigation and prosecution of cross-border offenses

BANK of ZAMBIA



THANK YOU FOR YOUR KIND ATTENTION AND GOD BLESS YOU ALL