



## **VIRTUAL ASSETS AND VIRTUAL ASSETS SERVICE PROVIDERS (VASPS): FROM THE ZAMBIAN PERSPECTIVE**

### **1. INTRODUCTION**

Global trends are changing both the technology businesses use and the tools and techniques regulators need to adopt in order to help manage the risks they are exposed to by these new technological advancements. Without a doubt, the changing landscape in global technology is in itself a good thing for efficiency and being able to compete in this fast changing world. Change in technology has the potential to spur financial innovation and efficiency and improve financial inclusion, but it also creates new opportunities for criminals and terrorists to launder their proceeds or finance their illicit activities. One of the most prominent technological developments in the last decade has been the launching of Virtual Assets (VAs) which are in a form of decentralized digital currency or virtual currency. Examples of Virtual Assets are cryptocurrencies such as bitcoins.

The subject of cryptocurrencies has been scrutinized by various policy makers and different international organizations, which have each touched upon the subject in a different way. Below, we summarize some of the definitions of cryptocurrencies:

- i. The European Central Bank ("ECB") has classified cryptocurrencies as a subset of virtual currencies. It defined such currencies as a form of unregulated digital money, usually issued and controlled by its developers, and used and accepted among the members of a specific virtual community.
- ii. The International Monetary Fund ("IMF") like the ECB, has categorised cryptocurrencies as a subset of virtual currencies, which it defines as

digital representations of value, issued by private developers and denominated in their own unit of account.

- iii. The Committee on Payments and Market Infrastructures ("CPMI"), a body of the Bank for International Settlements ("BIS"), has qualified cryptocurrencies as digital currencies or digital currency schemes. These schemes are said to exhibit the following key features: i. they are assets, the value of which is determined by supply and demand, similar in concept to commodities such as gold, yet with zero intrinsic value; ii. they make use of distributed ledgers to allow remote peer-to-peer exchanges of electronic value in the absence of trust between parties and without the need for intermediaries; and iii. they are not operated by any specific individual or institution.
- iv. The European Banking Authority ("EBA") has suggested to refer to cryptocurrencies as virtual currencies, which it defines as digital representations of value that are neither issued by a central Bank or public authority nor necessarily attached to a fiat currency but are used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically.
- v. The European Securities and Markets Authority ("ESMA") has recently also referred to cryptocurrencies as virtual currencies, in a pan-European warning issued in cooperation with the European Insurance and Occupational Pensions Authority ("EIOPA") and the EBA. Fully in line with the EBA's definition, virtual currencies are defined as digital representations of value that are neither issued nor guaranteed by a central bank or public authority and do not have the legal status of currency or money.
- vi. The World Bank has classified cryptocurrencies as a subset of digital currencies, which it defines as digital representations of value that are denominated in their own unit of account, distinct from e-money, which is simply a digital payment mechanism, representing and denominated in fiat money. Contrary to most other policy makers, the World Bank has also defined cryptocurrencies itself as digital currencies that rely on cryptographic techniques to achieve consensus.

- vii. The Financial Action Task Force (“FATF”) like many other policy makers has approached cryptocurrencies as a subset of virtual currencies, which it defines as digital representations of value that can be digitally traded and function as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but do not have legal tender status (i.e., when tendered to a creditor, are a valid and legal offer of payment) in any jurisdiction. It further suggests that virtual currencies can be divided into two basic types: i. convertible virtual currencies that have an equivalent value in real currency and can be exchanged back-and-forth for real currency; ii. Non-convertible virtual currencies that are specific to a particular virtual domain or world. Cryptocurrencies like Bitcoin are virtual currencies of the first type, that can, according to the FATF, be defined as math-based, decentralized convertible virtual currencies that are protected by cryptograph.

The main conclusion that can be drawn from the different perspectives set out above is that there is no generally accepted definition of the term cryptocurrencies available in the regulatory space. However, amongst those cited above, only the World Bank and the FATF have put forward a clear-cut definition which are globally preferred. If we try to summarize all the above definitions, a good summary could be that a 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”.

In June, 2019 the FATF updated its Recommendations and defined **Virtual Assets (VAs) as a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes**. VAs does not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations. The FATF further defines Virtual Asset Service Providers (VASPs), as any natural or legal person who is not covered elsewhere under the FATF Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- i. exchange between virtual assets and fiat currencies;
- ii. exchange between one or more forms of virtual assets;
- iii. transfer of virtual assets;
- iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
- v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Subsequently, the Financial Action Task Force (FATF) issued guidance for a Risk-Based Approach (RBA) to VAs and VASPs in June 2019. The guidance is intended to help national authorities in understanding and developing regulatory and supervisory responses to VA activities and VASPs, and to help private sector entities seeking to engage in VA activities, in understanding their AML/CFT obligations and how they can effectively comply with these requirements.

The updated FATF recommendations (June 2019) require countries to ensure that VASPs are licensed or registered and subjected to effective systems for monitoring or supervision by a competent authority. Further, countries are required to identify and assess the money laundering and terrorist financing risks emerging from virtual asset activities and the activities or operations of VASPs. Based on the understanding of the risks, apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. VASPs are further required to take appropriate steps to identify, assess, manage and mitigate their money laundering and terrorist financing risks they face.

In this regard VASPs are supposed to be subjected to AML/CFT requirements among others conducting customer due diligence, ongoing monitoring, record-keeping, and reporting of suspicious transactions.

As already alluded to, virtual assets are produced by a public network, rather than any government or Central Bank, that uses cryptography to make sure payments are sent and received safely. Encryption techniques regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank or any government.

The first virtual asset to capture the public imagination was Bitcoin, which was launched in 2009 by an individual or group known under the pseudonym, Satoshi Nakamoto. As of February 2019, there were over 17.53 million bitcoins in

circulation with a total market value of around \$63 billion (although the market price of bitcoin can fluctuate quite a bit). Bitcoin's success has spawned a number of competing cryptocurrencies such as Litecoin, Namecoin and Peercoin, as well as Ethereum, and Cardano. Today, there are literally thousands of virtual assets in existence, with an aggregate market value of over \$120 billion. Bitcoin currently represents more than 50% of the total value.

## **2. GLOBAL RESPONSE TO VIRTUAL ASSETS**

Globally, in the recent past, we have seen a spur in virtual assets i.e. cryptocurrencies, prompting more national and regional authorities to grapple with their regulation. The expansive growth of virtual assets makes it possible to identify emerging patterns. A survey conducted in June 2018 by the Staff of Global Legal Research Directorate entitled, *“Regulation of Cryptocurrency around the World,”* found that, one of the most common actions identified across the surveyed jurisdictions is government-issued notices about the pitfalls of investing in the cryptocurrency markets. Many of the warnings issued by various countries note the opportunities that cryptocurrencies create for illegal activities, such as money laundering and terrorism financing, the survey found.

The survey conducted by the Staff of Global Legal Research Directorate further asserts that, some countries go beyond simply warning the public and have expanded their laws on money laundering, counter-terrorism, and organized crime to include cryptocurrency markets, and require banks and other financial institutions that facilitate such markets to conduct all the due diligence requirements imposed under such laws. For instance, Australia, Canada, and the Isle of Man recently enacted laws to bring cryptocurrency transactions and institutions that facilitate them under the ambit of money laundering and counter-terrorist financing laws. On the other hand, some countries such as Algeria, Bolivia, Morocco, Nepal, Pakistan, and Vietnam ban any and all activities involving cryptocurrencies while Qatar and Bahrain have a slightly different approach in that they bar their citizens from engaging in any kind of activities involving cryptocurrencies locally, but allow citizens to do so outside their borders. The survey further concludes that there are also countries that do not ban their citizens from investing in cryptocurrencies but rather impose indirect restrictions by barring financial institutions within their borders from facilitating transactions involving cryptocurrencies. Such countries include Bangladesh, Iran, Thailand, Lithuania, Lesotho, China, and Colombia.

## **2.1 African Countries**

As in many other parts of the world, Africa has taken a cautious approach when it comes to regulating virtual assets activities. Most African regulators recognize both the adverse effects and the potential benefits of virtual assets. Despite recognizing the potential benefits of virtual assets, many African countries have been reluctant to authorize virtual assets transactions and largely remain concerned about the potential risks.

According to the Africa report an online media publication, there has been no common agreed upon regional regulatory environment in Africa, whether favorable or unfavorable. For example, South Africa and Swaziland offer the most conducive regulatory landscape on Cryptocurrency whereas Namibia prohibits cryptocurrencies. The majority of African countries have issued warning statements to their citizens on the use of cryptocurrency while a number of other countries have not made any policy statement on Cryptocurrency. The general consensus in the countries where warning statements have been issued is that, people in these countries use cryptocurrency at their own risk. Such warnings, mostly issued by central banks, are largely designed to educate the citizenry about the difference between actual currencies, which are issued and guaranteed by the state, and cryptocurrencies, which are not. Most government warnings note the added risk resulting from the high volatility associated with cryptocurrencies and the fact that many of the organizations that facilitate such transactions are unregulated. Most also note that citizens who invest in cryptocurrencies do so at their own risk and that no legal recourse is available to them in the event of loss.

## **2.2 European Union**

On 19<sup>th</sup>, June, 2018, the fifth European Union Anti-Money Laundering Directive (EU AMLD 5) was published in the official journal of the European Union. In particular, the EU AMLD 5 amended the fourth Anti-Money Laundering Directive (AMLD 4) released in 2015 to extend the scope to cover virtual currency platforms and wallet providers. The EU AMLD 5 will now apply to virtual currency exchange service providers and electronic wallet providers in order to cover the risks associated with virtual currencies like bitcoins. The EU AMLD 5 requires EU member countries to identify, understand and mitigate the risks related to money laundering and terrorist financing. The EU Anti-Money Laundering Directives are issued in order to prevent the misuse of the financial system for the purpose of money laundering in European Countries. The EU AMLD 5 went into

force on 9th July, 2018. Member states are obliged to transpose the modified directives into national law by 20th January, 2020.

As can be seen from the above, the EU has responded to virtual asset by requiring member countries to incorporate the virtual asset platforms and service providers into national AML/CFT regulatory frameworks as required by the FATF Recommendations.

### **3. VIRTUAL ASSETS FROM THE ZAMBIAN PERSPECTIVE**

Are people trading in virtual assets i.e. cryptocurrencies such as bitcoins in Zambia? Certainly yes! Websites such as localBitcoins.com and many others that offer platforms where traders can buy and sell cryptocurrencies are available to Zambians. LocalBitcoins.com is a startup company based in Helsinki, Finland which facilitates trading of local currency for bitcoins. Users post advertisements on the website, where they state exchange rates and payment methods for buying or selling bitcoins. A number of individuals in Zambia are involved in the trade of Bitcoins and other cryptocurrencies.

However, in Zambia, virtual assets are a relatively new phenomenon and have emerged in the absence of regulation. As such, some Supervisory Authorities have issued statements to give their position on Virtual assets i.e. cryptocurrencies. In February 2018, the Securities and Exchange Commission (SEC) issued a notice on cryptocurrencies and other digital products. The Commission urged “any individuals or entities that are currently investing in or intend to invest in cryptocurrencies and related products/assets to exercise restraint and caution as they do so because the products/assets are largely unregulated and not subject to the jurisdiction of the Commission.” While SEC did not ban their operation, they cautioned platforms that facilitate cryptocurrency transactions “to ensure that they are not in any way abrogating any part of the Securities Act and that those that meet the description of securities in accordance with the Act are registered with the Commission.

In a similar stance, on 12<sup>th</sup> October, 2018, the Bank of Zambia (BOZ) issued a press statement on Cryptocurrencies. BOZ noted the increasing public interest in Cryptocurrencies as evidenced by the growing number of enquiries it had been receiving on the subject matter. The BOZ stated that while cryptocurrencies have some monetary characteristics, such as, being used as a means of payment on a person to person basis, they are not legal tender in Zambia. In order to safeguard the interests of members of the public and maintain the

integrity of the financial system in Zambia, the BOZ indicated that it has not issued any form of cryptocurrencies and neither does it oversee nor regulate the cryptocurrency landscape. Consequently, any activities related to the buying, trading or usage of Cryptocurrencies is performed at owner's risk. The BOZ advised the general public to be fully aware and understand the risks associated with the use of Cryptocurrencies which include money laundering, financing activities of terrorism and general consumer protection risks such as fraud and hacking. This is because in most cases, no legal recourse would be available to customers due to the unregulated nature of Cryptocurrency related transactions. In conclusion the BOZ stated that it will continue to monitor the developments relating to Cryptocurrencies in Zambia.

Having interacted with a number of potential VASPs, the FIC has keenly been observing the developments relating to virtual assets with a view to collaborating with stakeholders in order to manage the potential ML/TF risks that VAs activities pose. The FIC has noted with a concern an increase in the number of individuals and business entities purporting to be dealing and investing in virtual assets in particular Bitcoins when in fact they are not. Members of the public are lured into investing into such schemes, thereafter the money is diverted into something else or used for personal gains and is not invested in VAs.

Further, FIC has noted that some entities dealing in VAs i.e. cryptocurrencies have been derisked by Commercial Banks. Derisking is a process by which Commercial Banks cut off the business relationship with individuals or business firms due to posing a high ML/TF risk to the Bank.

#### **4. POTENTIAL BENEFITS AND ML/TF RISKS ASSOCIATED WITH CRYPTOCURRENCY**

VAs comes with both benefits and risks. It is a complex subject that encompasses not only AML/CFT issues, but also other regulatory matters, including consumer protection, prudential safety, tax and soundness regulation, and network Information Technology security standards. For purposes of this article the risks are limited to ML/TF risks.



## **4.1 BENEFITS OF VIRTUAL ASSETS**

Like other new payment methods, virtual assets have legitimate use. Virtual Assets i.e. cryptocurrency hold the promise of making it easier to transfer funds directly between two parties, without the need for a trusted third party like a bank or credit card company. These transfers are instead secured by the use of public keys and private keys. 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 and is also currently processed with lower fees/charges than traditional credit and debit cards. Further, this functionality may potentially provide benefit to existing online payment systems, like Paypal. Cryptocurrency may also facilitate micro-payments, allowing businesses to monetize very low-cost goods or services sold on the Internet, such as one-time game or music downloads.

## **4.2 POTENTIAL ML/TF RISKS OF VIRTUAL ASSETS**

The international economy continues to be afflicted with problems of money laundering, terrorist financing and other financial crimes which are perpetuated through various financial services including through cryptocurrency. Virtual assets operations or schemes pose risks to the financial system in a number of different areas. In his presentation at the Law Association of Zambia (LAZ) Annual Conference held from 5-6 April 2018, Dr. Leonard Nkole Kalinde, Director-Legal Services and General Counsel of the Bank of Zambia stated that the potential for rapid change in the financial industry created by cryptocurrencies is a challenge for financial regulators and supervisors. He stated that risks that come with cryptocurrency are diverse, with immediate and pressing concerns about financial integrity vis-à-vis Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT). According to the FATF assessment, virtual assets may come with a number of money laundering and terrorist financing risks. Below are the potential ML/TF risks posed by virtual assets:

### **i. Tool for Criminals**

Virtual assets 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. The inherently global nature of the digital asset ecosystem makes digital asset activities particularly well suited for carrying out and facilitating crimes that are transnational in nature.

ii. **Borderless Nature of Virtual Assets Activities or Operations**

Customers and service providers can transact and operate with little regard to national borders, creating jurisdictional hurdles for regulators and law enforcement. Virtual assets commonly rely on complex infrastructures 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.

iii. **Decentralized Nature of Virtual assets**

There is no central oversight body of Virtual Assets Service Providers or traders. Law enforcement 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. Further, there is no central authority, government, or corporation that has access to the funds or personal information of virtual currency traders to enable them track criminals in cases of illegal activities. This problem is exacerbated by the rapidly evolving nature of decentralized virtual currency technology and business models, including the changing number and types of participants providing services in virtual currency payments systems.

iv. **Anonymous Nature of Virtual Assets**

Virtual Assets may allow greater anonymity than traditional non-cash payment methods. Virtual Assets activities are generally characterized 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.

## 5. WHAT NEXT?

Proponents of Virtual Assets operations believe virtual asset is the future. This is because the way people use and think about money is constantly evolving. The existing financial system was built for a non-digital age, ignoring the needs of the modern individual and with a lot of inefficiencies. As it has been noted, the world now has access to new technologies like decentralized cryptocurrencies that is quickly making these old systems redundant. Like communication evolving from landlines to mobile phones, or post to email, money is now finally catching up with other information revolutions. virtual assets are enabling us to reimagine the financial system and to upgrade the world to something better. On the other hand, cases that involve the abuse of virtual assets for money laundering purposes or other criminal activities are already being seen around the world. Competent authorities in Zambia should prepare for these developments. The following recommendations should be considered by stakeholders in the AML/CFT regime;

- i. Government should develop a framework to ensure VASPs are registered or licensed and are subjected to effective AML/CFT systems for monitoring or supervision by a designated competent authority.
- ii. Policy response to virtual assets operations should 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 virtual assets which include financial integrity, consumer/investor protection, and tax evasion while leaving less immediate risks (for example, financial stability, monetary policy) to a later stage.
- iii. Effective policy coordination will be required at the national and international levels to allow local law enforcement agencies and the FIC to work closely with foreign counterparts in conducting investigations and inquiries, making arrests, and seizing criminal assets in cases involving digital asset activity. These partnerships should be encouraged to support multi-jurisdictional investigations and prosecutions, particularly those involving foreign-located persons, digital asset providers, and transnational criminal organizations.

- iv. While mutual legal assistance requests remain a key mechanism for enhancing cooperation authorities should develop policies for obtaining evidence and restraining assets located abroad through technological means, recognizing that digital assets and the associated transactional data and evidence may be stored or located via technological means and processes not contemplated by current legal methods and treaties.
- v. Virtual Assets Service Providers should identify and assess the money laundering or terrorist financing risks relating to virtual assets activities as required by the updated FATF Recommendations 2012 as updated in June 2019.
- vi. Information exchange between the public and private sector should form an integral part of a country's strategy for combating ML/TF in the context of cryptocurrency activities. Dialogue with the private sector is essential in understanding the technology underlying virtual assets, the different types of virtual assets and associated business models as well as the technological solutions that can be used to enhance AML/CFT compliance.

**Disclaimer:** *This article is published for information purposes only and is not intended to solicit readers to engage in virtual assets operations. Further, the article does not constitute legal advice and is not intended to replace the FIC Act or any other guidelines, directives or regulations issued by the FIC or any Supervisory Authority for the Reporting Entities.*

**Authored by the Financial Intelligence Centre  
Compliance and Prevention Department**

**For more information, kindly visit the fic website: [www.fic.gov.zm](http://www.fic.gov.zm) or call +26021120 238230**

---