THE POINT

INSIDE

There exist numerous discussions as pertains to the usage, uptake, and the regulatory framework in place to govern cryptocurrencies in Kenya. Firstly, the basic information as to what cryptocurrencies are is an issue that needs more public education. Secondly, how it is used and how it has been embraced by users both in Kenya, across the region and worldwide should be brought to the fore, and thirdly, what kind of framework the regulator – the Central Bank of Kenya (CBK), has put in place to govern these types of currencies, and what it portends for its users in the country and beyond.

In this view, the Institute of Economic Affairs held a Public forum on 'Cryptocurrencies in Kenya', at which members from the academic fraternity, members of the public, civil society organization representatives, and practitioners in the crypto space in Kenya, were in attendance. Mr. John Walubengo, a member of the National Taskforce on Blockchain & AI made a presentation on the 'Fundamentals of Cryptos – Opportunities and Risks', while Mr. Jared Osoro, the Head of Research & Policy at Kenya Bankers Association presented on 'Opportunities for the Financial Sector'. Other presentations were on 'Digital Identity as an Integral Part of Cryptocurrency Regulation by Djibril Wachiye of Belfrics Kenya Limited, and 'Opportunities for Mining Bitcoins in Kenya' by Joseph Nyagari and Eric Michubu, both Bitcoin Entreprenuers.

This bulletin covers the key issues presented during the forum, as well as the ensuing plenary session queries and feedback from the panelists and participants in attendance.

Cryptocurrencies in Kenya

By Stephen Jairo

Introduction

In the olden days, the exchange of goods and services was done through barter trade; exchange of a good for a good, or a service for a service, or an interchange of these. However, in recent past, this kind of exchange has been facilitated by use of money as a medium of exchange. With developments on the technological front however, new ways of exchange have arisen. Use of credit cards and online money transfers are some of the most notable ones.

Further to the above, a focus on the technological platforms have brought to the fore a whole new world of doing business not only between individuals, but amongst business organizations at a global level. The advent of the online platform has led to the rise of virtual currencies that is gaining traction as medium of exchange across the globe, and this is what is referred to broadly as cryptocurrency.

A cryptocurrency is a subset of digital currencies that uses cryptography for security making it extremely difficult to counterfeit. A defining feature of cryptocurrencies is the fact they are not issued by any central authority (not controlled by a central bank like fiat currency) – it is fully decentralized. It is a medium of exchange like government issued currencies, developed by Satoshi Nakamoto[1] in 2009, but one that uses cryptography to secure the exchange of digital information and to

control the creation of new currency units. It has been touted as a mode that solves the problems that initially existed in the decentralized system. In a centralized system, the regulator oversees all the transactions and can take preventive measures to curb double spending which was the major impediment on the digital platform.

It is imperative therefore to differentiate between what 'fiat currency', and what 'digital currency' (electronic money) is. Fiat Currency refers to government issued currency that is designated as legal tender in its country of issuance through government decree, regulation, or law. Digital currency, also known as electronic money, refers to a digital representation of Fiat Currency used to electronically transfer value denominated in Fiat Currency.

Cryptocurrency therefore is a digital representation of value that can be digitally traded and used to functions as; 1) a medium of exchange; and/or, (2) a unit of account; and/or (3) a store of value, but does not have legal tender status in any jurisdiction. It is neither issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the Cryptocurrency.

Other classifications of digital assets are in the following categories; Non-security tokens, Security tokens, and Derivatives or funds.

Non-Securitized Tokens are also known as "Utility Tokens" or "Non-Security Tokens". They are Virtual tokens that do not exhibit the features and characteristics of a regulated investment or traditional asset. They are comparable to Bonga-points, Supermarket Loyalty Points, Hotel Lunch Vouchers or Frequent Flyer Miles points award schemes. In effect, they are meant to give certain specific benefits to its users within a given business community.

Securitized Tokens are virtual tokens that have features and characteristics of a Security under the traditional capital market regulations. They digitally represent a traditional asset such as Land title, Shares, and Stocks, and are also known as Asset-backed Tokens; the cryptocurrency version of a traditional asset.

In the business world, the token can be defined as *'A unit of value that an organization creates to self-govern its business model, and empower its users to interact with its products, while facilitating the distribution and sharing of rewards and benefits to all of its stakeholders.'*

The Token Utility

When evaluating a given token-based organization, the more advantages one can attain as pertains to the role a particular token can play would yield more advantages. The role of tokens is like nails – every person requires more than a one to hold firmly in place and in the same vein also guarantee safety and sustainability both in the medium and in the long run. This is where entrepreneur's creativity has been shining, as they invent and create the many ways that a token can be put to use at the operational level. Notably, if the token usage is obscure, not well explained, or not defensible, there is weakness in that model. the token utility has key roles as below;

As a Right: Owning a token bestows a right that results in product usage, a governance action, a given contribution, voting, or plain access to the product or market. In some cases, tokens will grant real ownership to a given product/service.

As a Value of Exchange: The token is also a small unit of value exchange within a particular market or application which results in the creation of a transactional economy between various buyers and sellers. This consists of features that allow users to earn value and to spend it on services that are internal to the inherent ecosystem. They can earn it by doing active work (real work and actions), or passive work (e.g. sharing data). The creation of such an internal economy is arguably one of the most important outcomes, and one that must be sustained over time.

As a Toll: Just like paying a toll to use a freeway, the token can be the pay-per-use rail for getting on the block chain infrastructure or for using the product. This also ensures that users have skin in the game. It can include running smart contracts to perform a specific function, paying for a security deposit, or plain usage fees in the form of transaction fees or other metered metric, e.g. Ethereum and Bitcoin.

As a Function: The token can also be used as a lever to enrich the user experience, including basic actions like joining a network, or connecting with users. It can also be used as an incentive, if it is given in return to begin usage or for on-boarding.

A Currency: The token is a very efficient payment method and transaction engine of choice. This is key for enabling frictionless transactions inside these closed environments. For the first time, companies can be their own payment processors without the cumbersome or costly aspects of traditional financial settlement options. Tokens offer a much lower barrier for processing end-to-end transactions inside a given market.

As Earnings: An equitable redistribution of the resulting increased value is part of what blockchain-based models can enable. Whether it is profit sharing, benefits sharing or other benefits (such as from inflation), sharing the upside with all the stakeholders is expected.

How the Bitcoin Works

Being the market leader so far, the how pertaining to operationalization of cryptocurrencies will heavily borrow from the Bitcoin platform which has a free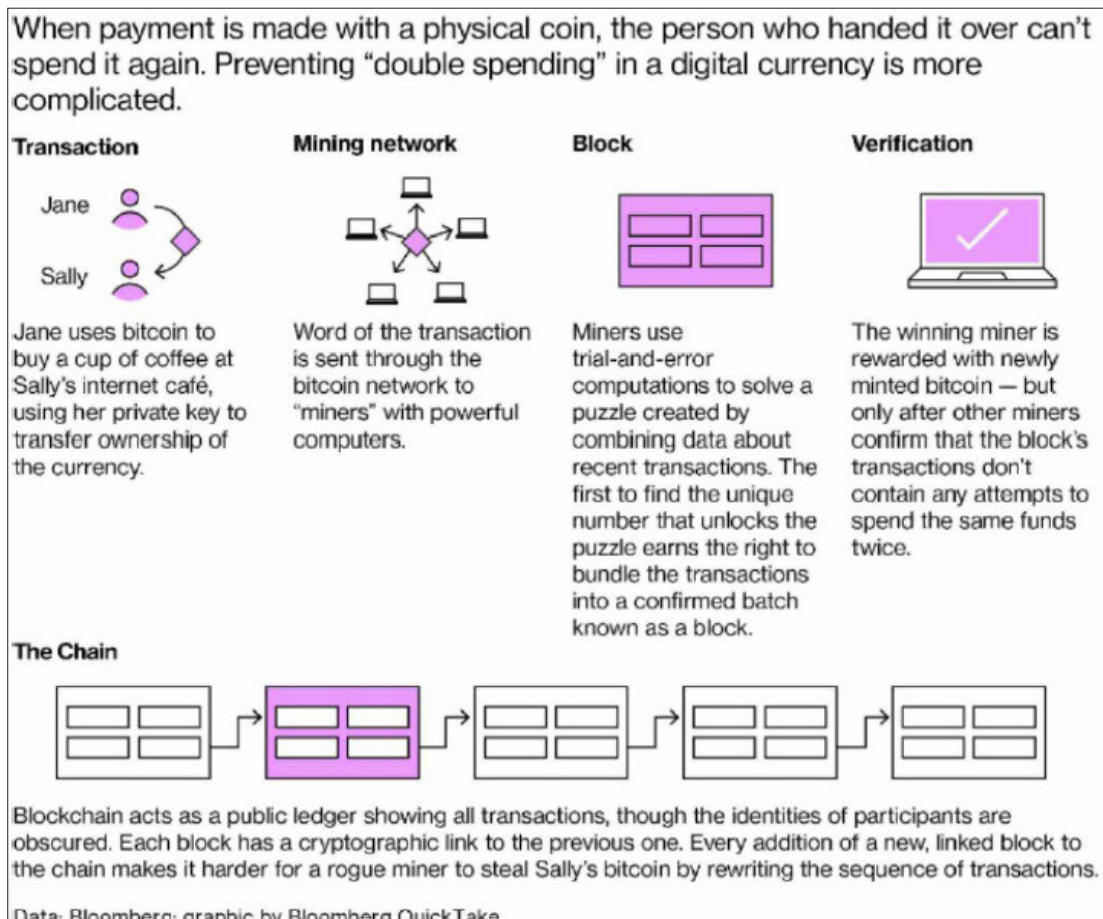 and open source code for its functionality. Other cryptocurrencies have been developed using code written and shared by Satoshi, with their own enhancements and additional features.

As the name suggest, cryptocurrencies use cryptography to enhance and operationalize the system. It provides a mechanism for securely encoding the rules of a cryptocurrency system within the system itself. It can be used to prevent tampering and ambiguousness, as well as to encode the rules for creation of new units of the currency into a mathematical protocol.

Within the Bitcoin blockchain network, bitcoins are spent to pay for monetary transmission, and to pay miners or block creators for maintaining the network. To convert the digital currency, for instance Bitcoin, to Fiat currency, one needs to have a Crypto Wallet. Various wallets exist for the various cryptocurrencies in the market.

Bitcoin uses SHA-256, which is a set of cryptographic hash functions designed by the U.S National Security Agency, and is based on the proof-of-work system.

Figure 1: How Blockchain works for Bitcoin

When payment is made with a physical coin, the person who handed it over can't spend it again. Preventing "double spending" in a digital currency is more complicated.

Transaction
Jane
Sally
Jane uses bitcoin to buy a cup of coffee at Sally's internet café, using her private key to transfer ownership of the currency.

Mining network
Word of the transaction is sent through the bitcoin network to "miners" with powerful computers.

Block
Miners use trial-and-error computations to solve a puzzle created by combining data about recent transactions. The first to find the unique number that unlocks the puzzle earns the right to bundle the transactions into a confirmed batch known as a block.

Verification
The winning miner is rewarded with newly minted bitcoin — but only after other miners confirm that the block's transactions don't contain any attempts to spend the same funds twice.

The Chain
Blockchain acts as a public ledger showing all transactions, though the identities of participants are obscured. Each block has a cryptographic link to the previous one. Every addition of a new, linked block to the chain makes it harder for a rogue miner to steal Sally's bitcoin by rewriting the sequence of transactions.

Data: Bloomberg; graphic by Bloomberg QuickTake

Source: Presentation by John Walubengo during the Public Forum on Cryptocurrencies held on September 6th 2018 at The Stanley Hotel, Nairobi.

The main problem that made uptake and use of cryptocurrencies slow in the early years of its rollout was the issue of 'double spend', which meant that the system was not tamper proof as opposed to use of fiat currency. As a consequence, one unit could be used by two or more different persons at the same time thereby meaning one party was cheating. However, with technological advancements, advanced coding has curbed this shortcoming thus ensuring this problem is non-existent.

In the Bitcoin scenario, once a purchase is made, or one individual makes payment via bitcoins, there is a complex system that is deployed to ensure verification of the transaction. This is done by high end computers and groups upon groups of miners who ensure the authenticity of the transaction and that only the intended end user acquires the bitcoin in the end. The process entails creation of chains of blocks of computerized puzzles and computations that lead to a confirmed batch – hence the term blockchain. The figure above demonstrates this process which leads to the recipient being the validly selected winner of the bitcoin, and eliminates the double spend problem too. A transaction occurs when data is sent to and from one (bitcoin) address to another.

Just like in a normal financial transaction where one sends money from one person to another, for bitcoin, you do the same thing but by sending data (bitcoins) to each other. Bitcoins have value because it's based on the properties of mathematics, rather than relying on physical properties (like gold and silver) or trust in central authorities, like fiat currencies. In enterprise environments, the transactions could be property, land, educational/birth certificates, etc.

Issues on Cryptocurrencies Vs Money (Fiat)

Some of the issues that have come to the fore in so far as uptake and usage of cryptocurrencies all over the world has to do with comparison with fiat currency. Some key issues are below;

1. *Safety of the cryptocurrencies:* Episodes of hacking, stealing of bitcoin, and even bankruptcy of exchanges and wallet providers have occurred. However, there is notable decline in such episodes with the evolving technology which continues to make systems that are tamper proof.¬
2. *Volatility of cryptocurrencies:* As has been noted, cryptocurrencies can be, and indeed are, very volatile. At one point they are highly priced yet at another, prices dip down.
3. *As an Investment Option:* One of the questions that sets cryptocurrencies apart from fiat currency is the aspect of using them as form of investment. Clearly, it is not an option that is backed by the Central Bank of Kenya thus leaves individuals and organizations to bear the risk on their own.¬
4. *Usage as a payment system:* Notably, technological advancements have enhanced payment models and which are much cheaper than many conventional options for remittances or money transfers. They are also convenient for instance for smartphone payments within and across borders.¬
5. *Purchase of the digital currency:* There are many exchanges that sell and buy cryptocurrency. There are also a growing number of physical automated teller machines, or ATMs, that will convert hard currency into digital currency.¬ In Kenya, the first Bitcoin machine has been installed in Westlands, Nairobi.
6. *As a medium of Storage:* Unlike fiat currency, digital currencies are stored in digital formats with the most known method being use of digital wallets which one can download onto their smartphones for free, online. It acts lust alike a normal wallet allowing one to make payments for large or small amounts, as is necessary. However, one has to take precautions to protect their funds from hacking; using strong passwords, or even just having an offline wallet.
7. *Uptake and Usage:* Acceptance is still limited but is gradually increasing. In the Kenyan scenario, some retailers accept bitcoins for goods and/services that they offer, with many tech savvy Kenyans joining the fray for various reasons; to make a kill as investors, or just to be part of the bitcoin family.

Note: There are many types of cryptocurrencies with various names in the market. Notably, it is Bitcoin that dominates with the rest slowly picking pace, gaining acceptance and usage with time.

Cryptocurrencies and the financial sector

The question that many people ask as pertains to cryptocurrency relates to how it affects the Kenyan financial landscape as it is. Notable however is the fact that the Central bank issued a circular that states their displeasure to embrace the digital technology in the

financial sector. This notwithstanding, there has been advantages that relate to usage of the cryptocurrency and which will tilt the landscape as is, and requires some sort of urgent policy direction by the regulator and the financial sector as a whole.

One of the issues of concern is the fact that digital technology has reduced the settlement time for transaction of securities. This has made it possible for much faster trading across borders which is beneficial to parties involved in a transaction. As a consequence, less money needs to be set aside to cover credit and settlement risks—just as collateral is not needed for a cash transaction.

In case of carrying out a transaction such as property purchase or sale, a blockchain could provide digital, unforgeable proof of ownership along with a complete record of the chain of possession. This has endeared it to many early adopters, especially tech savvy individuals and organizations both in the mainstream technology and even many business persons.

Advantages of Cryptocurrencies

1. **Reduces Transaction Settlement Time**: Payments and remittance settlement can happen rapidly allowing people to access their capital when they need it. Time and cost efficiencies could support large amounts of small transactions or micro transactions within the trusted network

2. **"Trusted" Third Party Elimination:** Storing transactions in an automatically shared, tamperproof database eliminates the need for complicated procedures and clearing houses and ensure that banks have their records in sync; jut in case the banking fraternity adopts this system.

3. **Eliminates Error Handling**: Since there is a large pool of independent individuals in the system, cryptocurrency provides for real-time tracking of transactions in a decentralized manner with no double spending or double-transactions, thus helping to eliminate errors.

4. **Support Smart Transactions:** Blockchain supports smart contracts, transactions that include multiple assets, transactions that include multiple parties and two-way transactions. In the long term, this will allow the unbanked not only access to paperless bank accounts, but also access to global capital markets as the connections are both local and global.

5. **Reduction in Transaction Costs:** Blockchain can cut operational costs which banks are targeting, giving real benefits while reaching out to the real customers and not just those with physical bank accounts.

6. **Ensures Secure Transaction-Ledger Database**: Since the system is checked by a community of connected computers within a distributed network, it has a secure transaction ledger database which has been checked and verified by all as being authentic and true reflection of a given transaction. This is an advantage that accrues to the users within the community.

Risks associated with Cryptocurrencies

Digital currencies have gained traction across the globe. However, some outstanding issues that have come to the fore include the following;

a) Money Laundering/Terrorists taking advantage of its anonymity; The use of cryptocurrencies has been said to be a conduit for money laundering or use by terrorist groups and/or organizations to fund their illegal activities since a key attribute of the currency is anonymity. However, it is not impossible to trace the origin of a bitcoin, and its ultimate recipient, though it is a tall order.

b) Users getting conned; Instances have occurred where some unscrupulous individuals or organizations create fake Crypto Assets/Currencies, Cyrpto-Exchanges & Initial Coin Offers (ICOs) and use these to con unsuspecting persons. In countries where this space is not regulated, losses are reported to be huge.

c) Safety of digital wallets is an issue; Blockchain based solution requires and puts more responsibility on users as pertains to the safety of their crypto-assets (Wallet Pins and Passwords). Instances of hacking have occurred where one manages to make through and steal bitcoins from individuals or organizations. Notably, it has been noted that 51% attacks on Blockchain based systems that assume majority of the participants (nodes) are honest (mining pools are growing).

Opportunities for Mining Digital Currencies

Mining, or processing, keeps the Bitcoin process secure by chronologically adding new transactions (or blocks) to the chain and keeping them in the queue. Blocks are chopped off as each transaction is finalized, codes

decoded, and bitcoins passed or exchanged. In the end, one individual will be given a reward in terms of tokens.

Conclusion

The digital landscape in the country has, and will continue to witness growth buoyed by the dynamics in the technological field. In terms of the effect to the financial sector, it becomes important that the status quo be checked so that benefits that may accrue are not left to chance, but rules and regulations put in place to govern this going forward.

The regulatory space for cryptocurrencies in Kenya currently is non-existent with only a warning from the regulator for individuals and organizations to steer clear to transact through the digital currencies platform. However, it is important to note that, and realize the fact that Tokens/Cryptocurrencies are with us to stay. Suggestions have been fronted as to how the sector can be regulated to ensure benefits accrue both to the user and the government. Noting this fact therefore, the Kenyan government set up a task force in April to look into ways of gaining a better understanding of, and thereby regulating this ecosystem. One of the approaches proposed is to have a 'Sandbox' Regulation to host emerging technologies in a controlled environment before rolling out to the general public. This ensures that there is a balance between embracing and enhancing new technological advancements while in the same vein protecting consumer interests.

The Point

The Institute of Economic Affairs (IEA-Kenya is a Public Policy Think Tank and a civic forum that seeks to promote pluralism of ideas through open, active and informed public debates on key policy issues.

The Institute provides research back-up to policy makers, including members of parliament through research and advocacy, and is independent of political parties, pressure groups, lobbies and any other partisan interests.

The Point is a publication by the Economic Regulation and Competition Policy (ERCP) Programme.