http://dx.doi.org/10.5455/sf.XXXXX

Science Forum (Journal of Pure and Applied Sciences)

journal homepage: www.atbuscienceforum.com

An overview on the impact of bitcoin on monetary activities in Nigeria

Ameena Almakura Ahmed[1], Samaila Musa[2*]

[1.] *Department of Computer Science, Nasarawa State University, Keffi, Nigeria*

[2.] *Department of Computer Science, Federal University Gusau, Gusau, Nigeria*

ABSTRACT

Electronic cash or cyber cash and virtual currency are all forms of digital currencies. Indeed, computers on the bitcoin network check for unauthorized attempts to alter transactional records. The importance cannot be overstated, as virtually every human civilization, every bank, council, and local library is based on a centralized or decentralized organizational structure. Bitcoin is a digital currency that is referred to as cryptocurrency because it is a form of electronic currency that relies on cryptographic techniques, the science of making and breaking codes, to prove identity and authenticity and to enforce read and write access to the bitcoin network. This paper examines the features of bitcoin, the stakeholders in it, the mining process, and the position of Central Bank of Nigeria. This paper will help new researchers to work on bitcoin and its integration challenges in the financial system.

ARTICLE INFO

Article history:
Received 01 November 2021
Received in revised form
09 November 2021
Accepted 10 November 2021
Published 27 April 2022
Available online 27 April 2022

KEYWORDS

Bitcoin
Electronic cash
Bitcoin network
Cryptocurrency
Nigeria economy and Internet

1. Introduction

The global economic system is amazingly complicated. At its fabric, this superficially complex system disintegrates into a set of few rules that sum up how humans trade their notions of value. The Internet has changed the entire game for age-old systems, so it is no surprise that it has caused immense disruption to the financial system too. It does not seem like technology is going to stop disrupting the financial systems anytime soon. Digital currency is an Internet-based medium of exchange which is dissimilar in terms of physicality compared to real currency. Digital currency exhibits similar possessions to real currencies and allows for prompt and borderless transfer of ownership (Tasca, 2018).

Mazikana (2019) refers to blockchain as a ledger that is updated constantly and maintained by computers. It is a distributed ledger technology which bundles transactions into groups called "blocks," cryptographically chains those blocks together, and then broadcasts them to the nodes of a peer-to-peer (P2P) network. The essence is to create an immutable, distributed database of those transactions. This technology is developed in order to create a database that is consensually shared and synchronized across the network spread across multiple sites, institutions, or geographies. Blockchain eliminates the traditional role of a middleman which is required in financial institutions like banks that are supervised by authorities. An important feature of blockchain is that it is public; everyone can see it because it acts as a public ledger which is updated after every transaction. Every transaction becomes a block, which is then checked by others' computer and approved. These verifiers are what people call miners (Dwyer, 2014). After it

* **Corresponding author** Ameena Almakura Ahmed ✉ Samaila Musa samailaagp@gmail.com ✉ Department of Computer Science, Federal University Gusau, Gusau, Nigeria.

is approved, the transaction is added to the chain of blocks, the blockchain, and goes through. Every transaction is public and if someone tries to corrupt it, the mathematics behind it would flag it and prevent a consensus among all the ledgers, thus basically preventing fraudulent transactions.

Blockchain technology can transform a business process with a strategic, operational model. It has the potential to replace the current infrastructure by adopting the distributed ledger process that is focused on the improving operational process. A dedicated team must be approved to learn the new technologies, explore their potential, and evaluate the positive results it can yield upon implementation. The government must prioritize their immediate pain points by studying the feasibility of transforming processes that can create an edge. Initially, when Satoshi Nakamoto invented bitcoin in the year 2008 as a decentralized network of digital money exchange, the number of Bitcoin (BTC) users and miners were few in number; thus, simple computer processors were enough to handle the BTC mining process. However, due to the current popularity of BTC and the spike it showed in 2017 reaching to a high price of up to 20,000 USD, BTC network has hugely grown in size and magnitude. In its core, BTC functions as a P2P network of miners trying to solve a mathematical problem to validate a complete block of transactions. This mathematical puzzle gets harder to crack with the increasing number of miners. Moreover, a group of miners solving the puzzle quickest gets the reward; however, this eagerness might in turn increase the overall energy consumption. Recently, BTC has gone through swear criticism over its energy usage being labeled as "*Bitcoin is killing the planet*" or "*BTC energy usage is huge - we can't afford to ignore it*" by the Guardian. However, before reaching any conclusion, it is very important to go through all the important details about BTC's working, examining in detail the factors contributing to BTC's high energy consumption, and highlighting any initiatives which may add up to bring green energy usage for BTC transactions. To the best of our knowledge, the current academic research lacks any such work highlighting the aforementioned points; therefore, this paper is just an effort to fill up this research gap.

2. Features of Bitcoin

Bitcoin is a digital currency that is referred to as cryptocurrency because it is a form of electronic currency that relies on cryptographic techniques, the science of making and breaking codes, to prove identity and authenticity and to enforce read and write access to the bitcoin network. It follows the ideas set out in a whitepaper by an anonymous entity (Rogojanu and Badea, 2014) and pseudonymous Satoshi Nakamoto. In the paper, Satoshi Nakamoto proposed bitcoin as a decentralized network that is:

- Functional 24 hours a day without dependence on any external entity.
- Works across geographical borders.
- Bitcoin does not have a central authority.
- There is no central server; the bitcoin network is P2P.
- There is no central storage; the bitcoin ledger is distributed.
- The ledger is public, anybody can store it on their computer.
- There is no single administrator; the ledger is maintained by a network of equally privileged miners.
- Anybody can become a miner.
- The additions to the ledger are maintained through competition. Until a new block is added to the ledger, it is not known which miner will create the block.
- The issuance of bitcoins is decentralized. They are issued as a reward for the creation of a new block.
- Anybody can create a new bitcoin address (a bitcoin counterpart of a bank account) without needing any approval.
- Anybody can send a transaction to the network without needing any approval; the network merely confirms that the transaction is legitimate.

Issued in 2009, bitcoin technology has become a leader in P2P cryptocurrency, allowing secure transfer and exchange of digital tokens in a distributed and decentralized manner (Nakamoto, 2008). Over the last few years, bitcoin has been labeled in many different ways. It has been called everything from electronic cash to digital gold. While bitcoin's definition may change, depending on who you ask, it holds certain universal properties which give the bitcoin value. Bitcoin can be traded for other national fiat currencies at the agreed market rate (CoinDesk, 2019) through online marketplaces into a digital wallet. In addition to money, the exchange can also be done for goods and services, or use the bitcoins to buy goods or properties. Consequently, many people regard it as a better alternative to traditional fiat currencies and other physical assets such as gold or silver.

In the bitcoin network, money is not printed, but mined through widely distributed P2P network computing power in a controlled way by the miners running a dedicated program in their computer system (Bradbury, 2013). The miners' job is to run the program to record the bitcoins transactions from one user to another user. Those transactions will be recorded in a publicly distributed ledger called blockchain (Swan, 2015a, 2015b). In a blockchain ledger, the set of bitcoins' transactions are publicly distributed throughout the P2P nodes across the network. The uniqueness of this underlying technology for bitcoin is it allows for secure and transparent transactions while protecting the identity of transaction's parties (Nakamoto, 2008). Transactions are considered pseudo-anonymous because although the transactions are publicly archived under an individual's bitcoin address, the identity of the owner's address remains undisclosed. These processes in bitcoin network are decentralized and supported by multiple stakeholders.

Figure 1 shows the difference between the centralized networks (i.e., the traditional monetary system) and the decentralized bitcoin network.

2.1. Bitcoin stakeholders

Bitcoin is managed and applied by a community. Shcherbak (2014) grouped bitcoin stakeholders in four categories: users, miners, exchanges, and merchants.

2.1.1. Bitcoin users

Bitcoin users are people who own the bitcoins in their bitcoin wallets. The bitcoin users use bitcoins either to buy goods and services from the bitcoin merchants or to buy and sell bitcoins for other national fiat currencies such as USD and Pound Sterling (Shcherbak, 2014) or other types of cryptocurrencies, such as Ether and Nem, from the bitcoin exchanges (Agarwal, 2018).

2.1.2. Bitcoin miners

Bitcoin miners are those who own the miner machine that is used to process bitcoin transactions; they are in charge of processing the transactions on the blockchain and running complex computer rigs to solve complicated puzzles in an effort to confirm groups of transactions called blocks; upon success, these blocks are added to the blockchain record, and in return, the miner will be rewarded with bitcoins for each new block of bitcoin transactions recorded in the blockchain ledger (Eyal and Sirer, 2014). The miner's machines range from the CPU of an ordinary personal computer to an ASIC bitcoin miner, which is a machine that consists of an integrated circuit that is designed specifically for bitcoin mining (Martindale, 2018a, 2018b).

These miners can be thought of as the decentralized authority enforcing the credibility of the bitcoin network. New bitcoin is released to the miners at a fixed, but periodically declining rate. There are only 21 million bitcoins that can be mined in total, in other words, Nakamoto set a monetary policy based on artificial scarcity at bitcoin's inception that the total number of bitcoins could never exceed 21 million. As of January 30, 2021, there are approximately 18,614,806 bitcoin

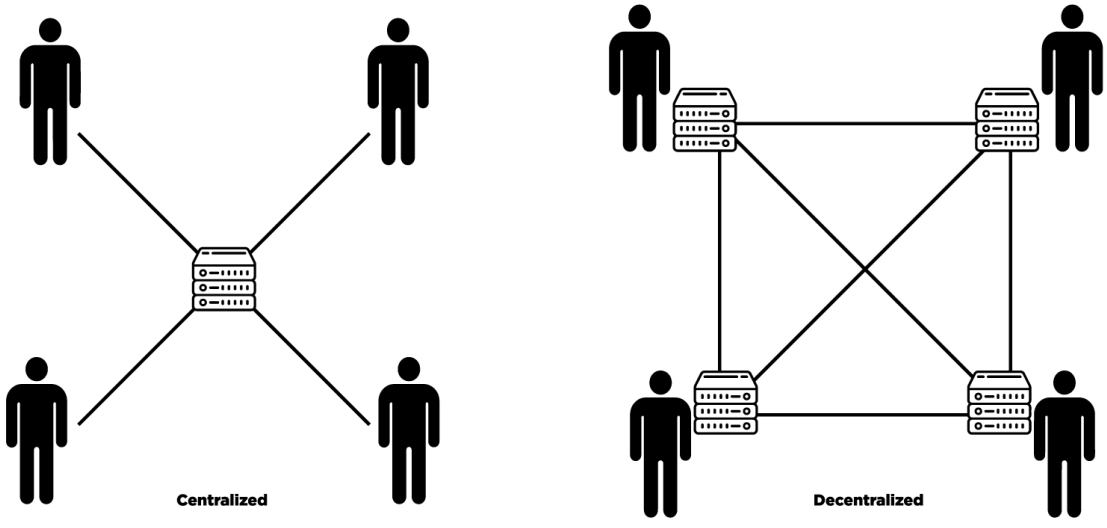

Figure 1. Comparison between centralized and decentralized network.

in existence and 2,385,193 bitcoins are left to be mined. New bitcoins are created roughly every 10 minutes and the rate at which they are generated drops by half about every 4 years until all will be in circulation.

2.1.3. Bitcoin merchants

Bitcoin merchants are businesses which accept bitcoins as a medium of exchange for goods and services. The merchants can be either an online business or a physical store. For example, one of the famous franchises Kentucky Fried Chicken in Canada does accept bitcoins in their branches and Microsoft accepts bitcoins in their online stores.

2.1.4. Bitcoins exchanges

Bitcoin exchanges are companies that provide the online trading platform for bitcoins to be exchanged with fiat money or other types of cryptocurrencies. The bitcoin exchanges act as a third party between the bitcoin seller and buyer. However, users are required to register and de-anonymize themselves to the exchange company. In addition, for each bitcoin transaction, there are also additional fees to be paid to the company.

2.2. How bitcoin works

2.2.1. Traditional money exchange versus crypto/ digital currency

Figure 2 differentiates between traditional and cryptocurrency transfers, respectively. As per the scope of this paper, BTC is considered to be the chosen cryptocurrency. For simplicity, the figure shows a scenario of a customer who wants to pay for shopping at a supermarket. It is assumed that the customer does not have any cash amount to make this payment. Clearly, the traditional transaction (via credit card) has to pass through several steps before the amount is transferred to the supermarket's registered bank account (Mir, 2020). This involves verification by the customer's bank and the credit card company, both charging buyer and seller with a fee for this transaction. The BTC transaction, on the other hand, looks quite simple and short. The customer uses her BTC wallet to pay which gets verified by the blockchain network. The payment is then made to the supermarket's wallet with a fee, despite having simplicity and pseudonymity of transactions (Mir, 2020),

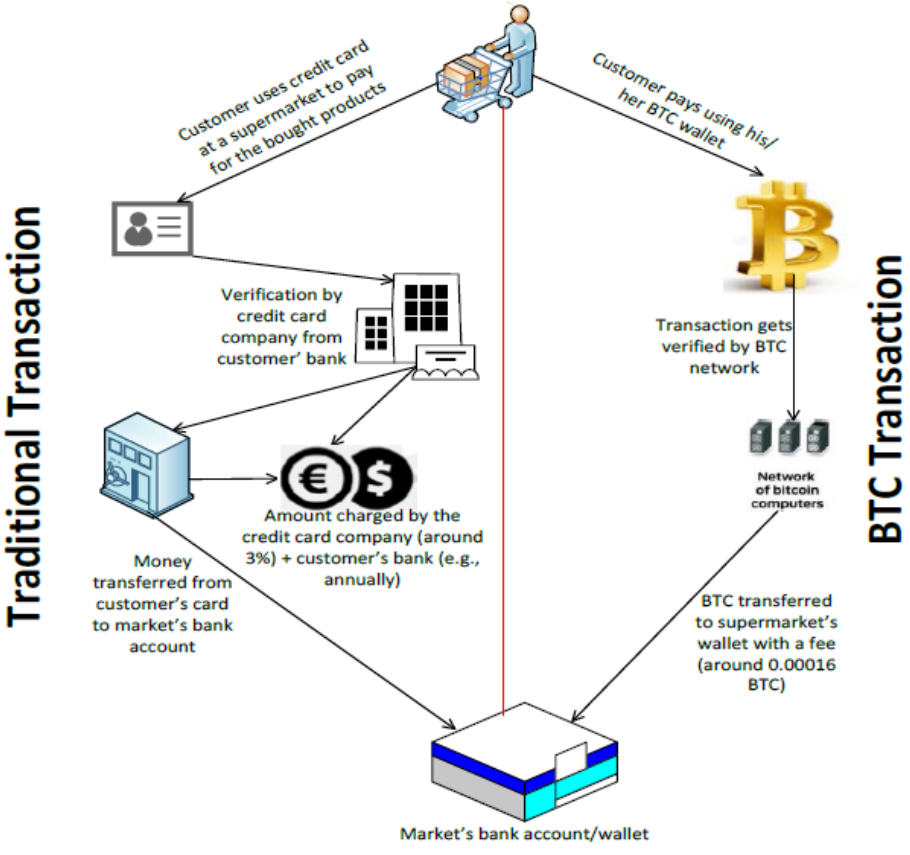

Figure2. Fiat exchange versus BTC transfer (Mir, 2020).

2.2.2. A transaction in the blockchain

The agents who process transactions in the bitcoin network use a set of bitcoin addresses called wallet (Dwyer, 2014), which is a set of bitcoin addresses that belong to a single person/entity. Each transaction record includes one or more sending addresses (inputs) and one or more receiving addresses (outputs), as well as the information about how much each of these addresses sent and received. An example of a typical transaction is shown in the Figure 3.

In the example, Almakura sends to Samaila an amount of 8 BTC. This transactions has two inputs (2 and 7 BTC) and two outputs (8 and 1 BTC), where the transaction involving 1 BTC can be considered essentially as the change of the transaction, which is returned back to Almakura. Since each transaction can have multiple sending addresses and receiving addresses, it is often impossible to link a specific sending address to a specific receiving address. The consequence of this is that you cannot assign a serial number to a specific bitcoin and trace its path in the bitcoin network.

Transaction processing in the bitcoin network is based on mechanisms which ensure that (a) the verification of each transaction is distributed among several network members; (b) the record of each transaction is discrete with respect to time, i.e., the transactions are linearly ordered with successive time stamps; (c) the particustomer identification proceduresants in the payment network compete and are rewarded for the recording of the transactions in a (bitcoin network) block; and (d) multiple nodes cross check each recorded transaction.

2.2.3. Starting a transaction

Suppose Almakura wants to send Samaila 1 bitcoin using the bitcoin network. To do this, Almakura and Samaila must have a bitcoin address. Let us call them ID Almakura and ID Samaila. Then, Almakura needs to send and certify digitally the authenticity of the message, such as "ID Almakura sends ID Samaila 1 bitcoin."

After Almakura signs a transaction message with her private key and sends it, the particustomer identification proceduresants in the bitcoin networks can verify that Almakura sent the message, and the message has not been altered. In addition, as we discussed before, digital signatures guaranteed that no one else could sign the message, so Almakura cannot deny that she did not sign the message.

2.2.4. Checking a transaction

Before executing transactions, the bitcoin protocol must verify two aspects of communication: first, whether Almakura sent a message. The digital signature schemes ensures that only the owner of the private key for that address can sign a message; second, to check whether there is enough funds in the address to ensure the complement of the transaction.

Although transaction records and verification are the main features of the electronic payment system, these functions are usually carried out through private registries, supported by trusted third parties. Decentralized systems such as bitcoin replace the third-party intermediaries and store transaction records in the public ledger, which are managed by a distributed information systems.

2.2.5. Updating the blockchain

After the initial check of the transaction signed messages, the validation node on the bitcoin network begins to compete for the opportunity to record transactions in the blockchain. First, in the transaction block, the competitive node begins to unite the transaction, which is executed since the last record

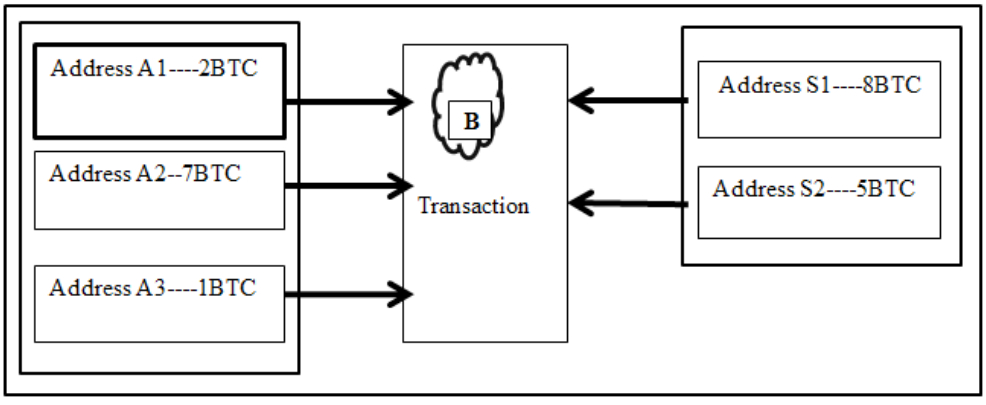

Figure 3. A typical transaction in the bitcoin network.

in the blockchain. Then, blocks are used to determine complex computing tasks. The node that first solves this task proceeds to record the transactions on the blockchain and collects a reward. The task which the competitive nodes try to solve is based on one of the encryption schemes described above—the hash function.

First, the newly broadcasted transactions are again used as input for a cryptographic hash function to obtain a hash called digest. This digest, along with a one-time random number code *nounce* (i.e., alphanumeric string) and the hash from the previous block is used in another hash function that produces a hash of the blockchain for the new block. The problem that must be solved by the node includes finding such a random code, so the hash of the new blockchain has certain properties (in this case, it has a number of initial zeros). The first of the competing nodes, which will find the right random code, transfers this information to other particustomer identification proceduresants in the network, and the blockchain is updated. The implementation of this scheme is called Hashcash—a proof that the system operates correctly [proof of work (PoW)], and whose purpose is to ensure that the computer uses a certain amount of computing power to carry out the task.

Nodes that carry out the process of the PoW in the bitcoin network are called miners. These miners use their computing resources in this process with the aim of getting reward offered by the bitcoin protocol. Usually, the reward is a predetermined number of newly created bitcoins. The rest of the reward (which is currently much smaller) is a voluntary transaction fee paid by those who carry out the transactions to the miners for the transaction processing. The initial idea is that this voluntary contribution will replace a predetermined compensation of the newly created bitcoin when this amount will tend to zero from time to time and new incentives will be needed to stimulate miners to process transactions in the bitcoin network (Nakamoto, 2009).

2.3. Bitcoin mining process

Bitcoin is designed with a hard limit of 21 million bitcoins, which is expected to be created by 2040. For now, this bitcoin is produced through mining, where miners, who are bitcoin users, run software on special hardware, process transactions, and are rewarded with new bitcoins for contributing their computer power to maintain the network. The importance of mining is not only for the creation of new bitcoin but also because it is a process needed for transactions to be added to the blockchain and then subsequently confirmed. The verification process is a computational intensive process that ensures that only legitimate transactions are verified and recorded in the blockchain. This is a network that provides computing power for transactions to be carried out and for transactions to be recorded. What happens during mining is actually a mathematical process. A real-life analogy to bitcoin mining will be a search for prime numbers: while it is easy to find a small one, it becomes increasingly difficult to find a larger number, leading researchers to use a special high-performance computer to find it.

Mining is a computational intensive task that requires miners to find a solution to predetermined math problems to create a new block. This is a mathematical PoW. Mining is difficult because in addition to ensuring that transactions are valid, miners must match the data in a certain way to add it to the blockchain. Miners must guess and look for data sequences of data that produce the required patterns. Chances are you hear the "bitcoin mining" phrase and your mind starts to wander the western fantasy of pickaxes, dirt, and striking it rich. Apparently, the analogy is not too far away. Bitcoin mining is carried out by a high-powered computer that solves complex computing math problems; these problems are very complex that they cannot be solved by hand and are quite complicated enough to task even a very strong computer. The results of bitcoin mining are discussed.

First, when the computer resolves this complex math problem on the bitcoin network, they produce new bitcoin (unlike when the mining operation extracts gold from the ground). And second, by solving computational math problems, bitcoin miners create a bitcoin payment network to be trusted and secure by verifying transaction information. When someone sends bitcoin anywhere, it is called a transaction. The transactions made in stores or online are documented by banks, point-of-sale systems, and physical acceptance. Bitcoin miners achieve the same thing by clumping transactions in "blocks" and adding it to public records called "blockchain." The node then maintains the records from the block so that they can be verified into the future.

When the bitcoin miner adds a new transaction block to the blockchain, part of their work is to ensure that the transaction is accurate. Each new block that is successfully added onto the blockchain references the previous block, making it exponentially difficult to reverse the previous transaction in the previous block. Because changing blocks on the blockchain will require a recalculation of the PoW of all the subsequent block

(bitcoin project), it becomes more and more infeasible for an adversary to manipulate blocks after more blocks are added, and the bitcoin protocol is accordingly designed to prefer longer chains. Therefore, miners do vital tasks because they verify transactions and ensure that blockchains cannot be tampered with. In particular, miners ensure that bitcoin is not duplicated, a unique quirk of digital currency called "double-spending." With printed currency, forgery is always a problem. But in general, once you spend $20 in the store, the bill is in the hands of the clerk. However, with digital currency, this is a different story. Digital information can be reproduced relatively easy, so with bitcoin and other digital currencies, there is a risk that spenders can make copies of their bitcoin and send them to other parties while still holding onto the original.

While bitcoin transfers are broadcasted instantly over the network, there is, in practice, a 10-minute delay for a transaction to be confirmed. This is the result of a 10-minute delay for the block to be created and added to the blockchain. Having confirmation ensures that the network (miners) has verified that bitcoin is valid and has not been spent. Usually, most users wait for six confirmations, that is, 1 hour, before considering the transaction to be "confirmed," but every user has the freedom to decide how long they want to wait before they consider their transaction confirmed.

To ensure progressive growth in new bitcoin, the reward for solving blocks is split in two automatically every 4 years, and the difficulty of solving increases over time. Over time, the rate at which bitcoins are produced will be similar to the level of commodity production such as gold. There will be a point in the future when the hard boundary bitcoin will be reached and incentives for miners will be a transaction fee. Arbitrary numbers chosen to be the limit in number of bitcoin is 21 million. Once the last bitcoin, or to be specific, the very last Satoshi—0.00000001 of a bitcoin—is produced through mining, miners who continue to contribute their computing power to verify transactions will be rewarded with transaction fees. This may be a less desirable situation for people and businesses that rely on bitcoin payments, which have to pay transaction fees, but it ensures that miners will still have incentives to keep the network up and running even after the last bitcoin is mined.

2.4. Double-spending

Until the invention of bitcoin, it was impossible for two parties to transact electronically without employing a trusted third-party intermediary. The reason was a conundrum known to computer scientists as the "double-spending problem," which has plagued attempts to create electronic cash since the dawn of the Internet. The double-spending is the analog concept to counterfeiting on physical money, but for digital currencies, it is necessary to verify, whenever you receive a unit of money, if that same unity, represented by a hash, was used by the same person on a different transaction. Specifically, even if someone knows a valid hash, it is necessary to verify the real owner of the hash. Only the PoW is not enough to enforce the correct transaction flow on cryptocurrencies. Cryptocurrencies can solve this problem with two approaches: centralized or decentralized. Each currency implements its own solution to the problem.

On bitcoins, the double-spending is avoided by verifying the public ledger, which is a bookkeeping of the transactions made with bitcoins since its creation. According to Nakamoto (2011), bitcoins use a decentralized methodology. Each transaction is recorded, and it is propagated by the P2P network. This shows that some specific node has significant importance in the process of exchanging bitcoins. Therefore, all the transactions with a given bitcoin can be traced back to the moment of its creation. Obviously, this is implied on the problem of defrauding the blockchain itself. Some malicious agents can modify the blockchain for their own benefit. Again, the solution to this problem is act decentralized, which is a central idea on the concept of bitcoins. The first thing that bitcoin does to secure the ledger is decentralize it. There is no huge spreadsheet being stored on a server somewhere. There is no master document at all.

Actually, the ledger is split in two parts. Each block contains the activity of transactions from until 10 minutes ago. King et al. (2013) says that "the ledger is broken up into blocks: discrete transaction logs that contain 10 minutes worth of bitcoin activity apiece. Every block includes a reference to the block that came before it, and you can follow the links backward from the most recent block to the very first block, when bitcoin creator Satoshi Nakamoto conjured the first bitcoins into existence." Also, it is necessary to digitally sign the transactions, which means that there must be a hash algorithm validating the transaction, and then it is added to the block and distributed on the P2P network, and therefore, the other miners (24) will know the existence and attest or not the validity of the transaction. If there is an attempt of inserting an invalid transaction on the block, it will be refused by the other network nodes. Hence, most of the nodes

must adhere to a new protocol in order to be accepted as a valid change. This shows how important the concept of decentralizing on bitcoins concept is.

2.5. Proof of work

PoW describes a system that requires a not insignificant but feasible amount of effort in order to deter frivolous or malicious uses of computing power, such as sending spam emails or launching denial of service attacks. PoW is a key concept to bitcoins and cryptographic currencies in a broad sense, since it prevents indiscriminate issuing of the currency, which would turn it into an impractical idea. The concept was subsequently adapted to securing digital money by Hal Finney in 2004 through the idea of "reusable proof of work" using the SHA-256 hashing algorithm. This concept is analogous to what happens on the file sharing network known as "bit torrent": if someone connects to it with a different protocol version, it would not be able to transfer files, unless that there exist more people using that same protocol. Ultimately, what this means is that the rules behind the generation of bitcoins is community-driven.

Following its introduction in 2009, bitcoins became the first widely adopted application of Finney's PoW idea (Finney was also the recustomer identification proceduresant of the first bitcoin transaction). PoW forms the basis of many other cryptocurrencies as well, allowing for secure, decentralized consensus.

2.5.1. Understanding PoW

Bitcoin is a digital currency that is underpinned by a kind of distributed ledger known as a "blockchain." This ledger contains a record of all bitcoin transactions, arranged in sequential "blocks," so that no user is allowed to spend any of their holdings twice. In order to prevent tampering, the ledger is public or "distributed"; an altered version would quickly be rejected by other users.

The way that users detect tampering in practice is through hashes, long strings of numbers that serve as PoW. Put a given set of data through a hash function (bitcoin uses SHA-256), and it will only ever generate one hash. Due to the "avalanche effect," however, even a tiny change to any portion of the original data will result in a totally unrecognizable hash. Whatever the size of the original dataset, the hash generated by a given function will be the same length. The hash is a one-way function: it cannot be used to obtain the original data, only to check that the data that generated the hash matches the original data.

Generating just any hash for a set of bitcoin transactions would be trivial for a modern computer, so in order to turn the process into "work," the bitcoin network sets a certain level of "difficulty." This setting is adjusted so that a new block is "mined"—added to the blockchain by generating a valid hash—approximately every 10 minutes. Setting difficulty is accomplished by establishing a "target" for the hash: the lower the target, the smaller the set of valid hashes, and the harder it is to generate one. In practice, this means a hash that starts with a very long string of zeros.

The PoW on bitcoins is given by creating a digest produced by an algorithm created by the National Security Agency (NSA) known as SHA-256C.26 This algorithm receives a string (objects that represent sequences of characters) with an arbitrary size, and returns a string with 64 characters. For instance, the string "bitcoins" generates the following digest:

a a 0 9 2 1 d 2 4 d 0 9 5 d f 0 3 8 a 0 c 0 a 3 2 e b 0 d - 644f1882e3a0a3d8814175c4e1cebbf84fb

While the string "cryptocurrencies" generates the following digest:

471a97f90b5df17b2f4a79d40f5d5d73fd6c46d-f96b34d2334c68aea90a8494b

The digests generated by this algorithm are on the hexadecimal format. On the bitcoins protocol, there is a rule that is necessary in order to generate a valid hash: it must possess a certain amount of leading zeros. The actual amount of zeros determines the difficulty level: the bigger the number of leading zeros needed, the harder is to find a valid result. This difficult is automatically adjusted by the network itself, according to the mining rate. Therefore, none of the previous hashes is actual bitcoins: the first one starts with "aa0" and the second one starts with "471." If the difficulty is low, then a low number of leading zeros is needed to compose a valid bitcoin.

For instance, the difficulty can be in finding only one leading zero, then any string on the format "0…" is valid, whereas if the protocol only authorizes two zeros, then a valid hash should follow the pattern "00..." Since the string size is fixed on 64 characters, each additional leading zero diminishes the total number of possibilities, therefore making the mining process more difficult.

This is the general concept, but in practice, it works slightly different. The input string is the previous transaction block, to which is added a random number with the intention of changing the resulting hash. This number is called nounce. The idea behind the nounce is to generate a completely different hash.

As seen before, any minor change on the input string would result in a very different hash. For instance, let "Hello World!0" be our input string. Applying the SHA-256 algorithm to this string, the following hash will be yielded:

1 3 1 2 a f 1 7 8 c 2 5 3 f 8 4 0 2 8 d 4 8 0 a 6 a d c 1 e 2 5 e - 81caa44c749ec81976192e2ec934c64

If there is a minor change on the end of the string, replacing the "0" with "1," the new string will be

"Hello World!1."

This new string will result in the following hash:

e 9 a f c 4 2 4 b 7 9 e 4 f 6 a b 4 2 d 9 9 c - 81156d3a17228d6e1eef4139be78e948a9332a7d8

None of those hashes is valid as bitcoins because they do not start with zeros.

Let x be the ending number. If we keep increasing x by 1, we will eventually find a valid bitcoin.

Suppose that the difficult is set to three leading zeros. Then, we are looking for a hash such as

H = SHA256 ("Hello World!" + x) j H = "000…"

Starting with x = 1, the following hashes will be yielded:

Hello, World!1) 1312af…
Hello, World!2) e9afc4…
Hello, World!3) ae3734…
Hello, World!4248) 6e110d…
Hello, World!4249) c00419…
Hello, World!4250) 0000c3…

So, the nounce 4250 outputs a valid bitcoin. An interesting fact about this is that the previous nounce, 4249, generates what one can perceive as an "almost" valid bitcoin, because its leading pattern is "c00." This does not mean that this number is actually "closer" to a valid bitcoin than any other nonvalid nounce. Each additional attempt of mining a valid bitcoin does not leaves one "closer" to get a valid hash. This is analogous to rolling a 6-faced dice n−1 times without getting a 3, and expect to have a greater chance of rolling a 3 in the next throw. This is a fallacy known as "Gambler's Fallacy." This is a very simplified explanation of how the PoW is operated on bitcoins. In reality, the protocol is more complex than that, and the blocks have a predefined format, which is part of bitcoins protocol.

2.6. Buying and storing bitcoins

Against this technical backdrop, bitcoins are often used simply as payment in exchange for goods and services (Kaplanov, 2012). While the numbers of brick-and-mortar merchants who accept payments in bitcoins remain low, there are many more online merchants who accept bitcoins for both digital and physical goods and services. The price of these goods and services is usually based on the exchange rate between bitcoin and a real-world currency, which can be found easily online exchange (XE).

Typically, a user who wishes to spend bitcoins obtains it by exchanging real-world currency for bitcoins. This can be achieved by purchasing bitcoins from a vending machine, from an exchange, or simply from another person. Bitcoin vending machines, often called "ATMs," are the most convenient way to buy bitcoins, because one can easily insert cash into a machine to obtain bitcoins instantly (Ulm, 2014). Bitcoin exchanges are also a popular means to obtain bitcoins, but users often face a time delay while waiting for bank transfers to clear (Ulm, 2014). Trading real-world cash for bitcoins is also a possibility, but it is inconvenient if bitcoins are needed on the spot. However, marketplace websites like LocalBitcoins have sprouted up to connect people interested in buying and selling bitcoins to enable them to do so privately, whether in person or online (LocalBitcoins). This option is more likely to be used in countries with restricted or no access to bitcoin vending machines or exchanges.

Bitcoins are typically stored in a wallet, so a user needs to have a wallet available to buy and sell bitcoins. Specifically, it is the private keys that are stored in a wallet (CoinDesk, 2014). These keys are used to access the bitcoin addresses and sign transactions, and therefore, must be kept securely. There are various types of bitcoin wallets, including desktop, mobile, webs, and hardware wallets. Users who choose to install a desktop wallet on their computer can create and keep wallets on their computer. The original bitcoin client software, known as Bitcoin Core, which is still in use today, includes the functionality of creating a bitcoin address to send and receive bitcoins and to store the corresponding private key for that address. There are many other wallet software in which users may select to install on their computer, like the cross-platform MultiBit and the security-conscious armory (Bitcoin.org). The different wallet software have varying additional features, although the most basic function of a wallet in storing the private keys for corresponding bitcoin addresses remains the same. While the user maintains control of his desktop wallet at all times, such wallets, like any other computer file, are vulnerable to theft by malicious users or software.

Desktop wallets are not the be-all and end-all kind of wallets, even if they were the first. When transacting at a physical store, a mobile wallet is often the most convenient way to spend some bitcoins. Mobile wallets are simply applications that provide for bitcoin wallet

functionality in a mobile phone. There are apps like the Mycelium Bitcoin Wallet that only exists on the mobile platform, while some desktop wallets like Blockchain.info also have mobile versions (Bitcoin.org). However, in the early 2014, Apple removed bitcoin wallet apps like Blockchain.info from its App Store (Southurst, 2014), although unofficial versions and mobile browser-based wallets continue to exist.

Another convenient type of wallet is the online wallet, which is generally accessible from anywhere through a browser with an Internet connection, regardless of the device used (CoinDesk, 2014). The private keys for a user's bitcoin addresses are kept and stored by the service provider of the online wallet, which may present a risk of the service provider or a third party absconding with the bitcoins, if security was not implemented properly. Blockchain.info also has a popular web-based online wallet and some online wallets offer extra encryption and two-factor authentication for additional security. Finally, there is small but growing interest in hardware wallets, which are specialized devices that can hold keys electronically and are also able to send and receive bitcoins. An example of a dedicated bitcoin device is the Trezor, a single-purpose token-sized device for making secure bitcoin transactions (SatoshiLabs).

Assets are distinguished from fiat currency and E-money meaning that there is a fundamental difference between cryptoassets and cryptocurrency under the Nigerian regulatory landscape.

Furthermore, The Securities and Exchange Commission (SEC) characterized virtual assets into the below four categories.

2.6.1. Cryptoassets

The statement provides that cryptoassets will be treated as commodities If they are traded on a recognized investment exchange and issued as an investment pursuant to part E of the SEC Rules and Regulations 2013 (the "Regulations") and any other relevant rules that will be issued in the future.

2.6.2. Utility tokens

Utility Tokens have functionalities that can be used to access a product or service built on a blockchain and can be exchanged with the use of the virtual currency native to the blockchain. Utility tokens will be treated as commodities as well, but spot trading (over the counter) of utility tokens will not fall under the scope of SEC unless It is conducted on a recognized investment exchange compliant with part E of the regulations.

2.6.3. Security tokens

These are tokens with functionalities similar to securities such as shares. They are used to represent underlying assets and even an ownership stake in the issuing entity. They also bring in dividends or Interest payments for holders. The commission according to the statement will treat such cryptoassets as securities pursuant to Section 315 of the ISA.

2.6.4. Derivatives and collective investment funds of cryptoassets, security, and utility tokens

Derivatives are usually contracts between parties backed by an underlying asset; in this situation, the underlying asset would be cryptoassets. Collective investment funds, on the other hand, are pools of investments being managed for investors. Section 153 of ISA defines collective investment schemes as a scheme in whatever form, including an open-ended investment company, in pursuance of which members of the public are invited or permitted to invest money or other assets in a portfolio. The collective investment funds envisaged by the SEC statement would be schemes used to pool money to invest in cryptoassets.

According to the statement, derivatives and collective investment funds involving cryptoassets would be regulated as specified investments under the ISA and the regulations. Capital market operators dealing with the aforementioned need to be approved by the commission.

2.6.4.1. What will be regulated? The statement sets out the position of SEC regarding virtual assets. The commission will now treat cryptoassets as securities unless the issuer or sponsor of the virtual asset proves otherwise.

This burden of proof will only be satisfied if the issuer or sponsor makes an initial assessment filing with the SEC to determine whether the assets are under its regulatory purview, where the findings of the commission is that the virtual assets are indeed securities and the sponsor must register the assets as securities. The effect of this is that all virtual assets will now be registered by the commission with any of the following approaches:

Option 1: An initial assessment filing to determine whether the assets are securities and to satisfy the burden of proof on the sponsor. Where the commission believes the cryptoasset is under the regulatory scope of SEC and is a security, a subsequent filing will be carried out by the issuer to comply with the SEC rules.

Option 2: The issuer can directly register the virtual assets with SEC without the initial assessment filing. Also, all digital assets token offerings ("DATOs"), initial coin offerings ("ICOs"), security token ICOs, and any offering of digital assets on a blockchain

— within Nigeria or;
— by Nigerian issuers or;
— foreign issuers targeting Nigerians;

will be regulated by the commission. Existing offerings or ICOs currently ongoing have 3 months to either submit their initial assessment filing or documents for registration.

2.6.4.2. Who will be regulated? Any person (individual or corporate) whose activities involve any aspect of blockchain related and virtual asset services must be registered by the commission and as such will be subject to the regulatory guidelines. The services envisaged by the commission that will have to comply with the guidelines are:

— Reception;
— Transmission;
— Execution of orders for cryptoassets on behalf of potential investors;
— Dealers in cryptoassets;
— Portfolio management with cryptoassets making up the portfolio;
— Investment advice regarding cryptoassets; and
— Custodians or nominees involved with virtual assets.

The services to be regulated by the commission are not limited to the ones aforementioned. Issuers will also be regulated by the commission and SEC may require a foreign or nonresidential issuer to establish an office in Nigeria. However, if there is a reciprocity agreement in place, foreign issuers need not establish an office and they will be recognized by the commission. A recognition status will also be given, where the foreign issuer is a member of the International Organization of Securities Commissions ("IOSCO").

3. The Current Position of the Central Bank of Nigeria

Nigerian authorities have been debating how to regulate the use of private cryptocurrency in the country. Earlier in the year (2021), Central Bank of Nigeria (CBN) ordered all local banks to seek and shut down accounts tied to cryptocurrency platforms, although the CBN governor later clarified that cryptocurrency trading is not banned in the country. Meanwhile, cryptocurrency usage as a store of value and remittance tool is and has continued to soar in Nigeria. According to a Central Bank official, Rakiya Mohammed, an Information Technologist Specialist at the Central Bank of Nigeria on the 10th of June, 2021, said that the entity had been exploring a possible Central Bank Digital Currency (CBDC) for over 2 years. Mohammed said one reason for the CBDC would be to make it easier to transfer remittances into the country. Before the pandemic hit and caused a dip in remittance worldwide, Nigeria received more than $5 billion in remittance quarterly. The specialist further said that before the end of the year the central bank would be making a special announcement about the possibility of launching a pilot scheme in order to be able to provide this kind of currency to the populace and that the entity will explore different technology options, engage various industry players, and test the digital currency. Mohammed reportedly said that the CBDC would complement cash, and that the CBN has looked at the architecture, accessibility, and privacy issues of a digital currency.

Unlike bitcoin, which are decentralized blockchains and entirely dependent on market forces, a CBDC is an instrument that replaces a physical banknote with a digital token or record. It is available exclusively in digital form and can only be issued by banks, as well as selected financial institutions. central Bank can record and verify all CBDC transactions. Meanwhile, there is no gold or other commodity reserve to back it. However, unveiling a CBDC is an extremely complex undertaking that requires years of planning, testing, and scaling. China leads the race currently and its pilot program is already active in a few cities. However, smaller countries like El Salvador cannot justify creating a new monetary policy out of scratch, and hence choose to embrace existing cryptocurrencies.

4. Conclusion

At the moment, CBDC is one of the hottest issues under debate, involving not only academics from different fields of knowledge, such as economics, finance, computer science, data analysts, and law, but also regulators, monetary authorities, and practitioners from all over the world. The recognized merits of bitcoin as a disruptive technology and the success of it and other cryptocurrencies paved the way for central banks to rethink new venues for the issuance and management of fiat money. For many, bitcoin and other cryptocurrencies do not, by themselves, threaten the pivotal role of central banks in existing payment systems, as they are conceptualized as more a market-based

speculative asset than a new kind of money, or due to the narrowness of its influence. However, other structural changes are taking place, such as the significant reduction in the demand for cash happening in some countries and, most notably, the increasing importance of new players.

References

Agarwal S. Blockchain technology in supply chain and logistics. Doctoral dissertation, Massachusetts Institute of Technology, Cambridge, MA, 2018.

Bradbury D. The problem with bitcoin. Comput Fraud Secur 2013; 2013(11):5–8.

CoinDesk. (2014). CoinDesk Bitcoin price index. Retrieved May 2017, from http://www.coindesk.com/price/

Dwyer GP. The economics of bitcoin and similar private digital currencies. J Financ Stab 2014; 17:81–91.

Eyal I, Sirer EG. Majority is not enough: bitcoin mining is vulnerable. In International Conference on Financial Cryptography and Data Security, 2014 Mar, Springer, Berlin, Heidelberg, pp 436–54, 2014.

Kaplanov N. Nerdy money: bitcoin, the private digital currency, and the case against its regulation. Loy Consumer L Rev 2012; 25:111.

King, R. S., Williams, S., & Yanofsky, D. (2013, Dec. 17). By reading this article, you're mining bitcoins. Retrieved from http://qz.com/154877/by-reading-this-page-you-are-mining-bitcoins

Martindale JR. Merging developing and developed worlds: the blockchain revolution's impact on collective global growth. New Visions Public Affairs 2018a; 10:39–47.

Martindale J. Nvidia speaks out against rising price of GPUs due to cryptocurrency mining. Digital Trends, 2018b.

Mazikana AT. The impact of cryptocurrencies in Zimbabwe: an analysis of bitcoins. 2019. Available via https://www.researchgate.net/publication/332292; doi: 10.13140/Rg.2.2.17100.26243

Mir U. Bitcoin and its energy usage: existing approaches, important opinions, current trends, and future challenges. KSII Trans Internet Inf Syst (TIIS) 2020; 14(8):3243–56.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Www.Bitcoin.Org, http://doi.org/10.1007/s10838-008-9062-0

Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. 2009. Available via http://bitcoin.org/bitcoin.pdf

Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. Technical Report, 2011. Available via www.bitcoin.org; http://bitcoin.org/bitcoin.pdf

Rogojanu A, Badea L. The issue of competing currencies. 2014. Volume XXI (2014), No. 1(590), pp. 103-114/

Shcherbak S. How should bitcoin be regulated? Eur J Legal Stud 2014; 7(1):46–1.

Southurst J. ATM Industry Association publishes report on bitcoin ATMs. CoinDesk, 2014. http://www.coindesk.com/apple-removes-blockchain-bitcoin-wallet-from-app-stores/ (accessed 06.02.21).

Swan M. Blockchain thinking: the brain as a decentralized autonomous corporation [Commentary]. IEEE Technol Soci Mag 2015a; 34(4):41–52.

Swan M. Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.". 2015b.

Tasca P, Hayes A, Liu S. The evolution of the bitcoin economy: extracting and analyzing the network of payment relationships. J Risk Finance 2018; 19:94–126.

Ulm B. Bitcoin ATMs boom: new locations. CoinTelegraph, 2014.