Economic Risk, Cyber Threats and Privacy Issues of Blockchain Technology in Nigeria

Musa Ahmed Zayyad

Department of Computer Studies, Hassan Usman Katsina Polytechnic, P.M.B. 2052, Katsina State, Nigeria

***Abstract*: Blockchain technology and cryptocurrency are continuously becoming more popular all over the world, especially with the rapid popularity of access to the internet. It appears to be one of the most significant trends of the modern era. It is difficult nowadays to spend a whole day without coming across issues of cryptocurrency in the news, or social networking sites, broadcasts channels and even legislations made by various governments. The debate surrounding the subject is highly polarized, with strong feelings on all sides of the multifaceted cryptocurrency. Some call it a bubble, while others believe it has the potential to destabilize the economy of the world. Blockchain technology, which is the heart of cryptocurrency, has been described as a major disruptor of the global business process. Many entrepreneurs have jumped on the initial coin offering (ICO) bandwagon, selling tokens to the general public and raising hundreds of millions of dollars. Therefore, the aim of this article is to investigate the impact of cryptocurrency on the global economy risk and cyber threats and privacy issues with particular emphasis on a developing country like Nigeria.**

Keywords: **Bitcoin, blockchain, cryptocurrency, internet, technology**

I. INTRODUCTION

Blockchain is a collection of records or transactions that are organized into blocks that define a portion of a ledger. The ledger is distributed among peers, who rely on it as a trusted authority to determine whether or not records are valid. Each block in the ledger is linked to the block after it, forming a chain, hence the name blockchain. Anyone can determine the status of an address by looking at the most recent blocks and their "parent" blocks. In the case of cryptocurrencies, we can calculate the worth of an address and track every transaction that leads to the creation of each contributing coin. It is critical to validate the transactions. Each node can independently validate the accuracy of each chain [1].

There are two types of Blockchain technology, which are known as permissionless and permissioned blockchain. Permissionless blockchains allow any party to participate in the network without any vetting, while permissioned blockchain is formed by an administrator or consortiums who evaluate an entity's participation in the blockchain framework [2].

The business logic is encoded using smart contracts, regardless of the type of blockchain. Smart contracts are self-executing code on the blockchain framework, whichenable straight-through processing, which does not require manual intervention to execute transactions. They rely on data from third-party entities known as "oracles" and can act on information associated with any public address or another smart contract on the blockchain,

While blockchain technology has the potential to increase efficiency and reduce costs, it also has some potential risks. In order to reap the benefits of this technology, businesses must first understand the risks and the appropriate safeguards. Furthermore, it is critical to comprehend the evolution of regulatory guidance and its implications [3]. Blockchain technology provides countless benefits to the progress of information technology. However, in orderto utilize blockchain efficiently, it is essential to consider privacy and security concerns. Although it has a solid backbone of cryptography which ensures the data protection, however, security vulnerabilities are still the part of this system and they are continuously emerging [4].

This study is aimed at exploring the deep analysis of several blockchain applications and digital currency, related security concerns and weaknesses, known as vulnerabilities, future trend and possible solutions, which could provide the reliability of this technology.

A. Security Risk in Blockchain Technology

Any new technology's adoption and operation is reliant on the proper management of the risks related with that technology. This is particularly true when the technology is more than just an application and is integrated into the organization's core infrastructure. In the near future, Distributed Ledger Technologies (DLT) have the potential to be the backbone of many core platforms [5].

Security concerns such as fraud and theft of personal information by cyber criminals when users make online transactions, has increased the popularity of blockchain technology and cryptocurrencies such as "Bitcoins". Reference [6] in their studystated that the averse usage of online banking by the users was as a result of hacking and cyber fraud. They further stated that deceitful behaviour such as phishing, in which sensitive information including passwords and credit card information are obtained illegally from users, led to them feeling more susceptible when transacting online. Security and privacy concerns such as

these make cryptocurrencies a more feasible and protected option.

According to [7], security risks in blockchain technology can be categorized into three classifications, which include:

i. Standard risks: blockchain technologies expose institutions to risks that are similar to those associated with current business processes but introduce nuances for which entities need to account.
ii. Value transfer risks: blockchain technology enables peer-to-peer transfer of value without the need for a central intermediary. The value transferred could be assets, identity, or information. This new business model exposes the interacting parties to new risks that were previously managed by central intermediaries.
iii. Smart contract risks: smart contracts can potentially encode complex business, financial, and legal arrangements on the blockchain, and could result in the risk associated with the one-to-one mapping of these arrangements from the physical to the digital framework.

The blockchain peer-to-peer technologyprovide the prospect of transforming current business activities by disintermediating central processes or entities, increasing efficiencies, and producing an absolute audit trail of transactions. This offers the prospect to reduce costs, lower interaction or settlement times, and increase transparency for all events. This transformational framework could change the method in which financial institutions conduct businesses, since majority of the transactions are peer-to-peer in nature[1].

Even though the benefits are clear, there are potential risks that may be enforced by this emerging technology. Studying of security and privacy issues associated with blockchain may change and advance as the technology continued to develop. Therefore, it is important for all organizations to continue to study the development of this technology and its application to various use cases.Blockchain technology will transform business models from a human-based trust model, which might expose firms to risks that they may have not encountered before. In order to respond to such risks, firms should consider establishing a robust risk management strategy, governance, and controls framework[8].

B. Cyber Threats in Blockchain Technology

Hackers and cyber criminals device various techniques that enables them to steal cryptocurrencies. These techniqueswere designed to penetrate users and their wallets, exchanges or major custodial services, and other fundamental networks or protocols supporting cryptocurrencies. FireEyeCybersecurity Company that specialized in detecting and preventing major cyber-attacks has observed successful attacks that steal from users and cryptocurrency exchanges over the past several years. Even though less frequent, attacks targeting cryptocurrency networks and protocols have also been observed. It is believed that cryptocurrency exchanges or main custodial services are, and will continue to be attractive targets for malicious operations due to the potentially large profits, their often-lax physical and network security, and the lack of regulation and oversight [9].

C. Cyber Threats of Blockchain Technology in Nigeria

The adoption of blockchain by using bitcoin by some sophisticated criminal gangs in Nigeria ranging from internet fraudsters to high profile and smart kidnappers that uses bitcoin cryptocurrency in asking for ransom payment of their victims, brings additional dilemma and much difficulties to security agencies in identifying and tracing the perpetrators of these heinous crimes, once the payment is made, it will be much difficult to trace the transactions.

Kidnapping in Nigeria has never been this bad, especially when it comes to making use of bitcoin as a means of collecting ransom from families and friends of the victims. Kidnappers who often patronize the rich, middle-class earners, and the poor have shown their level of desperateness in gaining money from the abduction of individuals who go about their normal businesses, unaware of their devious schemes.

On one Saturday, a lady was kidnapped in the country's capital, Abuja FCT. The lady is a daughter of a famous politician in the country. On that same day, sources recorded that about five people in Abuja were kidnapped. However, the police made the public understand that they were briefed of just two kidnappings aside that of the young lady.

The lady was freed after her father paid the ransom of $15,000 dollars in bitcoin, which was about N5,000,000 million naira. It was a shocking discovery that kidnappers now use bitcoin to collect ransom. This discovery has opened the mind of many Nigerians to the fact cryptocurrency is now a new means of collecting ransom. Nigerians now understood that these criminals will go to any length in ensuring that they collect the required money from the family and friends of the abducted individuals [10].

Blockchain technology provides abundant benefits to the development of information technology. However, in orderto deploy blockchain technologysuccessfully, it is essential to consider securityand privacy issues.Even though it has a robust backbone of cryptography thatsafeguards the data protection, however, security concerns are still the part of this system and they are continuously developing. This studyis aimed at exploring the deep analysis of numerous blockchain applications and digital currency, related security threats and vulnerabilities, future trend and possible solutions, which could ensure the reliability of this technology**[**11].

D. Threats of Bitcoin to Nigerian Economy

Bitcoins are considered as an example of digital currency that were developed in the year 2009 by an anonymous group of developers under the pseudonym "Satoshi Nakamoto" [14].

Bitcoins as a form of digital currency make payments based on cryptographic proof, as opposed to traditional payment systems which are based on trust. According to [12], [13], cryptographic proof is when two willing parties make transaction with each other, without the need of a trusted third-party. In this type of transaction, there is no need for a bank account, or credit card or to provide personal data or information when making a transaction using bitcoins. Bitcoins are decentralized, which means they are not controlled centrally or regulated by any authority or register keeper [14].

Using bitcoin to bypass trade hurdling is another major issue. Many Nigerian traders and international importers are now using bitcoin to do their transaction with countries like China for importation of their goods and services. These types of transactions evade taxes and other potential economic benefits to the country. This shows that digital currency has to be secure so as to be accepted by the normal day business people, but this had not been fully the case in terms of bitcoins because in June 12, 2013 bitcoin got hacked and USD$375 000 worth of Bitcoins were lost and no coins were ever recovered. This led to people losing their trust in bitcoins. Stealing of bitcoins have been documented on several occasions. On other occasions, bitcoin transactions have shut down, taking their clients' bitcoins with them [11]. "A Wired study published April 2013 showed that 45 percent of bitcoin exchanges end up closing."

Bitcoins can be exchanged from one person to another without the need for a third-party to perform the transaction, which lowers costs that could have been attracted if using a third party to conduct the transactions [15]. The transaction records of these cryptocurrencies are stored in a digital ledger known as a blockchain, which keeps records of all transactions ever made on the bitcoin network. Unlike traditional banking systems where the currency is governed by a central bank which is backed by the government [16]. Bitcoins are not restricted to one country or a single user, but are worth the same value everywhere no matter what country a person is in [15].

According to Mbadiwe, O. Eze & Ikerionwu (2020), in their study on regulation of blockchain technology in Nigeria, the need and risk mitigation towards industry highlighted the importance of the blockchain technology in the modern era. They also stress the need for the government to regulate the blockchain technology due to the risk of illegal usage and unpleasant practices. The importance and challenges inherent in the blockchain technology necessitated the need for government to regulate the blockchain technology to reduce adoption risks by deriving an adoption framework that is consumer based and providing guidelines for service providers. The authors emphasized the need to regulate the blockchain technology due to the security risks in the adoption and implementation of the technology. The societal and industrial concerns require protection. The regulation and standardization of blockchain are now necessary and apt to reduce some unwanted wholesome practices of individuals by developing policies to guard customers and service providers [18].

E. Privacy Issues of Blockchain

Blockchain has some essential privacy issues by virtue of its design. Particularly, the distributed feature of a blockchain means that each full node that processes transactions and builds the blockchain necessarily has access to the blockchain transaction data itself. In a cryptocurrency like bitcoin, this means that the blockchain is publicly available and every transaction can be traced back to the first genesis block. Bitcoin is said to be "pseudonymous", which means that it has data points that are not directly associated with a specific individual but where multiple appearances of a person can be linked together [6].

A recent study by the New York Times described how enough pseudonymous location data can make identification of the individual insignificant. This is a big issue for blockchain for a few reasons. Unlike application data cited in the Times article, blockchain data is open for scrutiny by everyone – including every malevolent criminal looking to exploit information for financial gains. Also, the immutable record of the blockchain exacerbates this problem. Once attributed to an individual through any means, a lifetime of pseudonymous transactions will be permanently exposed as linked to that person.

The public nature of the blockchain enables opportunities for identification. According to [17] in their study on systematic literature review of blockchain cyber security to monitor the communications between nodes on the blockchain, which can associate transactions and internet protocol addresses. Applications have been developed to perform these types of analyses on public blockchains. In addition, although not public, cryptocurrency wallet software can be forensically analysed even without the passphrases or keys that are needed to use the wallet.

The most high-profile use of these techniques was the arrest of Ross Ulbricht for operating the deep website "Silk Road", which was a market place for illegal drugs among other things. The techniques allowed law enforcement agents to identify Ulbricht as the operator of Silk Road. More interestingly, an IRS special agent was also able to track bitcoin transactions to determine that a US Drug Enforcement Administration agent involved in the investigation, Carl Force, was laundering bitcoin related to Silk Road.

II. CONCLUSION

In conclusion, this article has identified that both bitcoin and blockchain technologies provides very slight privacy protection. Apart from the public scrutiny, individuals that rely on intermediaries such as an exchange like Coinbase are subject to having their identities exposed by the exchange,

such as when the IRS demanded that Coinbase turn over certain records involving cryptocurrency transactions. Although, privacy is often focus when weaknesses of blockchain are discussed, the technology has some comparably problematic security issues as well.

REFERENCES

[1] Casino, F., Dasaklis, T. K., &Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and informatics*, *36*, 55-81.

[2] Solat, S., Calvez, P., &Naït-Abdesselam, F. (2021). Permissioned vs. Permissionless Blockchain: How and Why There Is Only One Right Choice. *Journal of Software*, *16*(3), 95-106.

[3] Polasik, M., Piotrowska, A., Wisniewski, T.P., Kotkowski, R., and Lightfoot, G. (2015). Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry. *International Journal of Electronic Commerce*, 20(1), 9-49.

[4] Johnson, F.T., Akande A. F., Akinsanya P.A (2019). Leveraging digital currency for national development. International Journal of Advanced Research (IJAR) http://dx.doi.org/10.21474/IJAR01/xxxx

[5] Gilbert, S., & Loi, H. (2018). Digital currency risk. *International Journal of Economics and Finance*, *10*(2), 108-123.

[6] Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys & Tutorials*, *20*(4), 3416-3452.

[7] Deloitte. (2017). Blockchain Risk Management: Risk Functions Need to Play An Active Role in Shaping Blockchain Strategy.

[8] Grover, P., Kar, A. K., &Ilavarasan, P. V. (2018). Blockchain for businesses: A systematic literature review. In *Conference on e-Business, e-Services and e-Society* (pp. 325-336). Springer, Cham.

[9] ElMamy, S. B., Mrabet, H., Gharbi, H., Jemai, A., &Trentesaux, D. (2020). A survey on the usage of blockchain technology for cyber-threats in the context of industry 4.0. *Sustainability*, *12*(21), 9179.

[10] Akinpelu, O. (2019, September 16). *Crypto-Ransoms! Nigeria has just recorded its first known kidnap-for-bitcoin case and it could get worse.*https://technext.ng/2019/09/16/crypto-ransoms-nigeria-has-just-recorded-its-first-kidnap-for-bitcoin-case-and-it-could-get-worse/

[11] Rosenfeld, M. (2011). Analysis of bitcoin pooled mining reward systems. *arXiv preprint arXiv:1112.4980*.

[12] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.

[13] Wright, A., & De Filippi, P. (2015). Decentralized blockchain technology and the rise of lexcryptographia. *Available at SSRN 2580664*.

[14] Böhme, R., Christin, N., Edelman, B. and Moore, T., 2015. Bitcoin: Economics, technology, and governance. *The Journal of Economic Perspectives*, 29 (2), pp.213-238.

[15] Portmann, E. (2018). Rezension „Blockchain: Blueprint for a New Economy ".

[16] Brito, J. and Castillo, A., 2013. *Bitcoin: A primer for policymakers.* MercatusCenter at George Mason University.

[17] Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., &Choo, K. K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, *6*(2), 147-156.

[18] Mbadiwe, O. N., Eze, U. F. &Ikerionwu, C. O. (2020). Regulation of blockchain technology in Nigeria: need and risks mitigation towards industry 4.0. 15thInternational Conference on Emerging Applications and Technologies for Industry 4.0, EATI. 229 – 237.