



Examining the role of blockchain technology against fraud in SMEs

Victor Amadin Idehen ^(a) Ewere Mayor ^(b)

^(a) Lecturer II, Department of Entrepreneurship, Faculty of Management Sciences, University of Benin, Edo State, Nigeria

^(b) Assistant lecturer, Department of Entrepreneurship, Faculty of Management Sciences, University of Benin, Edo State, Nigeria



ARTICLE INFO

Article history:

Received 13 June 2021

Received in rev. form 14 July 2021

Accepted 17 July 2021

Keywords:

Small and Medium enterprises,
Business, Blockchain, Technology,
Fraud

JEL Classification:

Q55

ABSTRACT

The study examined the use of blockchain technology for the prevention of fraud in small and medium enterprises. Fraud in businesses is a significant problem that stifles the growth of businesses. The methodology used is a review of relevant and extant literature, after which a conclusion was made. The transparency, security, and traceability of blockchain enhance its credibility as the most valuable technology to stem fraud in a business organization. The study contributed to knowledge by evaluating how blockchain can be adopted to stem the tide of fraud in businesses in Nigeria.

© 2021 by the authors. Licensee SSBFNET, Istanbul, Turkey. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

Introduction

Most businesses in Nigeria suffered greatly or close shop as a result of fraudulent activities by members of staff who have a conflicting interest to that of the organization. Fraud stifles growth and liquidate many businesses in Nigeria through loss of profits and depletion of shareholders fund. Unethical practices perpetuated by staff include manipulation and misrepresentation in terms of falsification, alteration, concealment and misappropriation of funds, fraudulent manipulation of accounting information, forging of cheques and documents, funds diversion, secret commission, bribery, false invoicing, theft of inventory assets. Fraudulent activities therefore involve the use of deceit and tricks to change the truth so as to deprive another person of his right. Despite the effort of most organizations to put mechanism in place to check the excess of their staff, it is always circumvented. In a guide to reduce employee fraud; CPA, 2009 (as in Olanrewaju and Johnson-Rokosu, 2019) emphasizes that misplaced trust, inadequate living and supervision policies and failure to implement strong internal control create an environment that is ripe for employee to commit fraud.

Factors responsible for the occurrence of fraud are situational pressures, existence of lapses for fraud to flourish and personal characteristics. This tend to be prevalent particularly where there is job dissatisfaction, personal financial difficulties, pressure from fellow employees, friends and relations, which subject the individual(s) to financial pressure and susceptibility to fraud (Olanrewaju & Johnson-Rokosu, 2019). There is need to stem the tide by deploying a technology that could check fraud in business organization. Blockchain is at the forefront of digital disruption and innovation. Blockchain technology can help fraud detection because it enables the sharing of information in real time and all participants in a blockchain have visibility over transactions. A blockchain network can track orders, payments accounts, production and virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

* Corresponding author. ORCID ID0000-0003-1005-1562:

© 2021by the authors. Hosting by SSBFNET. Peer review under responsibility of Center for Strategic Studies in Business and Finance.

<https://doi.org/10.20525/ijrbs.v10i5.1311>

Is in the light of the above, the study attempts to review relevant literature on blockchain as well as its potential business application as an effective tool to checking fraud in an organization. The paucity of academic journal that discuss the functional technology that underlay blockchain create a research gap the research wish to address. Such exploration will give business organizations in Nigeria insights as to its workability and possible usage to stem fraud. The research question is how blockchain can assist in checking fraud in business organization in Nigeria. To achieve our goal, the work is structured into introduction, literature review; which provide detailed understanding of the concept and conclusion.

Literature Review

Conceptual Background

A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains a number of transactions that are linked together using cryptography and every time a new transaction occurs in the blockchain, a record of that transaction is added to every participant's ledger. For clarity, each block contains a cryptographic hash of the previous block, a time stamp and transaction data. The time stamp proves that the transaction data existed when the block was published in order to get into its hash. As block, each contains information about the block previous to it. They form a chain with each additional block reinforcing the ones before it. The decentralized database managed by multiple participants is known as Distributed Ledger Technology (DLT). Such decentralization makes blockchain to be resistant to modification of their data because once recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks. Blockchain is a type of DLT in which transactions are recorded with an immutable cryptographic signature called a hash.

Blockchain technology can help fraud detection because it enables the sharing of information in real time and all participants in a blockchain have visibility over transactions. Therefore, errors and complexity are thwarted, fake data, errors in approval, double purchases, are prevented within the linked blockchain process. Fraudulent data cannot be inserted into the blockchain. Blockchain help to foster trust, accountability and transparency in business relationship. Blockchain can help to reduce and prevent fraud through greater transparency and improved traceability of products. It's very difficult to manipulate blockchain; which is an immutable record that can only be updated and validated through consensus among network participants. If a product is digitized on blockchain, it can easily be traced to its origin because the information is on share distributed ledger and changes can only be possible through consensus of the majority to do so.

Components of Blockchain

Node application

Every computer connected to the internet, needs a node application specific to the blockchain ecosystem that it wants to participate in.

Distributed ledger (database)

The distributed ledger means the share contents and databases available to the participants of a particular blockchain ecosystem.

Consensus Algorithm

The consensus algorithm provides permanence and security to the data in the blockchain

Key element of blockchain

Distributed ledger technology

All network participants have access to the distributed ledger and its immutable record of transactions. With this shared ledger, transactions are recorded only once.

Immutable records

No participant can change or tamper with a transaction after it's been recorded to the shared ledger. If a transaction record includes an error, a new transaction must be added to reverse the error and both transactions are then visible.

Smart contract

To speed transactions, a set of rules called a smart contract is stored on the blockchain and executed automatically. A smart contract can define conditions for corporate bond transfer.

Types of Blockchain

Public Blockchain

A platform where every participant would be able to read on and write to.

Private Blockchain

A platform where only the owner of the blockchain has the right to making any changes in rule or other terms.

Consortium Blockchain

This platform is partially like the private blockchain. Instead of allowing anyone person/company to have full control and participate in the verification of transactions process, some specific number of nodes are selected in a predetermined manner and the control is vested on them.

Importance of Blockchain

Nakamoto 2008 (as in Oyebanjo et al.,2021) posit that blockchain is a technology used as a distributed ledger that rides on a point-to-point network, enabling trust between unknown parties within the system and enabling seamless payment without human intervention. It help keep history of transaction because it is not subject to alteration, manipulation, once verified through mutual agreement by the various peers (nodes) involved in the transaction. Security of data and the transaction is achieved through cryptography, thus enabling secure transaction, integrity and privacy (Baranwal,2020 as in Oyebanjo et al., 2021). Unlike traditional systems of managing funds and contracts, blockchain can make fund management and the contracting process more transparent and secure and ensure accountability and efficiency of process, in a way not possible through the conventional system (Kumar, 2017 as in Oyebanjo et al., 2021). Thus the main stakeholders can verify transactions within the system to confirm its validity and legitimacy.

Blockchain Architecture

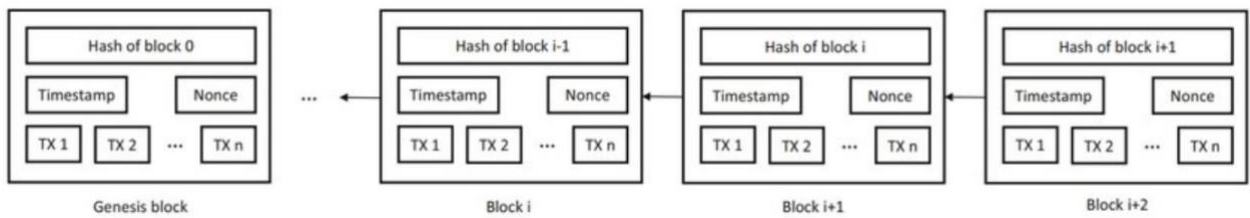


Figure 1: An example of blockchain which consists of a continuous sequence of blocks.

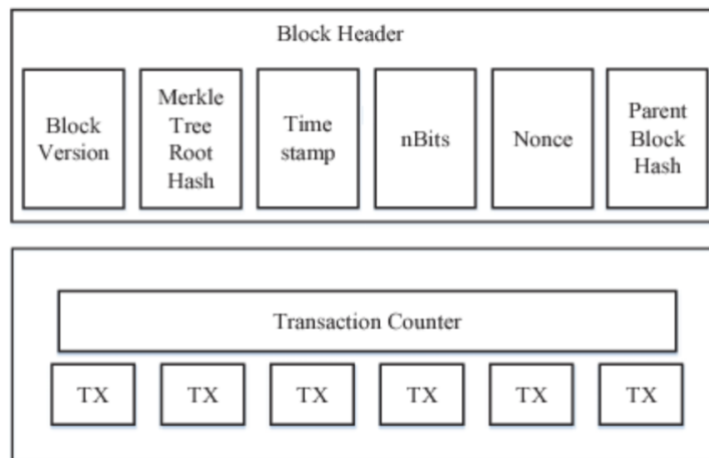


Figure 2: Block Structure; **Source:** Zheng et al (2017)

Zheng et al. (2017) posits that Block chain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger. Figure 1 illustrate an example of a blockchain with a previous has only one parent block. The first block of a blockchain is called genesis block which has no parent block.

The internals of Blockchain

Block

A block consists of the block header and the block body as shown in figure 2, in particular, the block header includes: (i) Block version. Indicates which set of block validation rules follow:

- i. Merkle tree root hash: the hash value of all the transactions in the block
- ii. Time stamp: current time as second in universal time
- iii. nBits: target threshold of a valid block hash

- iv. Nonce: an 4-byte field. Which usually starts with 0 and increases for every hash calculation
- v. Parent block hash: a 256-bit has value that points to the previous block.

The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions. Digital signature based on asymmetric cryptography is used in an untrustworthy environment

Digital signature

Each user owns a pair of private key and public key. The private key that shall be kept in confidentiality is used to sign the transactions. The digital signed transactions are broadcasted throughout the whole network. The typical digital signature is involved with two phases; signing phase and verification phase. The typical digital signature algorithm used in blockchain is the elliptic curve digital signature algorithm (ECDSA)

Key Characteristics of Blockchain

- i. Decentralization: in conventional centralized transaction systems, each transaction needs to be validated through the central trusted agency. In contrasts to the centralized mode, third party is no longer needed in blockchain. Consensus algorithms in blockchain are used to maintain data consistency in distributed network.
- ii. Persistency: transactions can be validated quickly and invalid transactions would not be admitted by honest miners. It is nearly impossible to delete or rollback transactions once they are included in the blockchain. Blocks that contain invalid transactions could be discovered immediately.
- iii. Anonymity: Each user can interact with the blockchain with a generated address, which does not reveal the real identity of the user. Noted that blockchain cannot guarantee the perfect privacy preservation due to the intrinsic constraint
- iv. Audibility: Bitcoin blockchain stores data about user balances based on the unspent Transaction output(UTXO) . Any transaction has to refer to some previous unspent transactions once the current transaction is recorded into the blockchain, the state of those referred unspent transactions switch from unspent to spent. So transactions could be easily verified and tracked.
- v. Taxonomy of blockchain systems: current blockchain systems are categorized roughly into three types: public blockchain, private blockchain and consortium blockchain. In public blockchain, all records are visible to the public and everyone could take part in the consensus process. Differently, only a group of pre-selected nodes would participate in the consensus process of a consortium blockchain. As for private blockchain, only those nodes that come from one specific organization would be allowed to join the consensus process.

A private blockchain is regarded as a centralized network since it is fully controlled by one organization. The consortium blockchain constructed by several organizations is partially decentralized since only a small portion of nodes would be selected to determine the consensus.

- i. Consensus determination: in public blockchain, each node could take part in the consensus process. And only a selected set of nodes are responsible for validating the block in consortium blockchain. As for private chain, it is fully controlled by one organization and the organization could determine the final consensus.
- ii. Real permission: Transaction in a public blockchain are visible to the public while it depends, when it comes to a private blockchain or a consortium blockchain
- iii. Immutability: since records are stored on a large number of participants, it is nearly impossible to tamper transactions in a public chain. Differently, transactions in a private blockchain or a consortium blockchain could be tampered easily as there are only limited numbers of participants.
- iv. Efficiency : it takes plenty of time to propagate transactions and blocks as there are a large number of nodes on public chain network. As a result, transaction through put is limited and the latency is high with fewer validations, consortium blockchain and private blockchain could be more efficient.
- v. Centralized: The main difference among the three types of blockchains is that public blockchain is decentralized, consortium blockchian is partially centralized and private blockchain is fully centralized as it is controlled by a single group
- vi. Consensus process: Everyone in the world could join the consensus process of the public blockchian. Different from public blockchian, both consortium blockchian and private blockchian are permissioned. Since public blockchian is open to the world , it can attract many usres and communities are active. Many public blockchians emerge day to day. As for consortium blockchian, it could be applied into many business applications.

Approaches to consensus

POW (proof of work) is a consensus strategy used in the Bitcoin network. In a decentralized network, someone has to be selected to record the transactions. The easiest way is random selection. However, random selection is vulnerable to attacks. So if a node wants

to publish a block of transactions, a lot of work has to be done to prove that the node is not likely to attack the network. Generally, the work means computer calculations. In POW, each node of the network is calculation a hash value of the block header. The block header contains a nonce and miners would change the nonce frequently to get different hash values. The consensus requires that the calculated value must be equal to or smaller than a certain given value. When one node reaches the target value, it would broadcast the block to other nodes and all other nodes must mutually confirm the correctness of the hash value. If the block is validated, other miners would append this new block to their own blockchains. Nodes that calculate the hash values are called miners and the POW procedure is called mining in Bitcoin.

In the decentralized network, valid blocks might be generated simultaneously when multiple nodes find the suitable nonce nearly at the same time. As a result, branches may be generated. However it is unlikely that two competing forks will generate next block simultaneously. In POW protocol, a chain that becomes longer is judged as the authentic one. Consider two forks created by simultaneously validated block U4 and B4. Miners keep mining their block until a longer branch is found. B4, B5 forms a longer chain, so the miners on U4 would switch to the longer branch. Miner have to do a lot of computer calculation in POW, yet this work waste too much resources to mitigate the loss, some POW protocols in which work could have some side applications have been designed.

POS (Proof of stake) is an energy saving alternative to POW. Miners in POS have to prove the ownership of the amount of currency. It is believed that people with more currencies would be less likely to attack the network. The selection based on account balance is quite unfair because the single richest person is bound to be dominant in the network. As a result, many solutions are proposed with the combination of the stake size to decide which one to forge the next block. In particular, blockchain uses randomization to predict the next generation. It uses formular that looks for the lowest hash value in combination with the size of the stake. Peercoin favour coin age-based selection. In peercoin, older and larger set of coin have a greater probability of mining the next block. Compared to POW, POS saves more energy and is more effective. Unfortunately, as the mining cost is nearly zero, attacks might come as a consequence. Many blockchains adopt POW at the beginning and transform to POS gradually.

Challenges of Blockchain

Scalability: with the amount of transactions increasing day by day, the blockchain becomes bulky. Each node has to store all transaction to validate them on the blockchain because they have to check if the source of the current transaction is unspent or not. Beside, due to the original restriction of block size and the time interval used to generate a new block, the Bitcoin Blockchain can only process nearly 7 transactions per second, which cannot fulfill the requirement of processing millions of transactions in real time fashion. Meanwhile as the capacity of block is very small, many small transactions might be delayed since miners prefer those transactions with high transaction fee.

Privacy leakage: Blockchain can preserve a certain amount of privacy through a public key and private key. Users transact with their private key and public key without any real identity exposure. Blockchain cannot guarantee the transaction privacy since the values of all transaction and balances for each public key are publicly visible.

Selfish mining: Blockchain is susceptible to attacks of colluding selfish miners. In selfish mining strategy, selfish miners keep their mined block without broadcasting and the private branch would be revealed to the public only if some requirements are satisfied. As the private branch is longer than the current public chain, it would be admitted by all miners. Before the private blockchain publish, honest miners are wasting their resources on useless branch while selfish miners are mining their private chain without competitors. So, selfish miners tend to get more revenue.

Blockchain in business application

Sarmah (2018) posits that Bank and payment systems have stated using blockchain to make their operations smoother, efficient and secure. Funds can be efficiently and safely transferred with the decentralization technology. Blockchain become increasingly popular in healthcare industries as it is able to restore the lost trust between the customers and health care providers. With the help of blockchain, authorization and identification of people have become easier and fraud and records loss can be avoided. Due to blockchain ability to store and verify documents efficiently, businesses have started using blockchain to verify records and document securely. Blockchain can significantly reduce the court cases and battle by providing an authentic medium to verify and confirm truthfulness of legal document.

Rigging of election result can be avoided with an effective use of blockchain. Voter registration and validation can be done using blockchain and ensure the legitimacy of votes by creating a publicly available ledger of recorded votes. Industries such as insurance, education, private transport and ride sharing, government and public benefits, retail, real estate etc have started implementing blockchain to reduce cost, to increase transparency and to build trust.

Benefits of Blockchain

- i. Reduced cost- Time savings
- ii. Transparency-information is available to all stakeholders and easily accessible in various locations
- iii. Real –time information: updates automatically and is replicated across all nodes

- iv. Innovative- reduced time to handle reporting and meetings because processes are automated
- v. Contract management
- vi. Enhanced security-Data protection is sure and lost transaction and storage is cloud based
- vii. Verification is independent
- viii. Assets are controlled by the owner
- ix. Less fraud

Disadvantage of Blockchain

- i. Not suitable where data has to be deleted.
- ii. Blockchain are expensive and resource intensive as every node in the blockchain repeats a task to reach consensus.
- iii. Blockchain is characterized with complexity and complicity to understand.

Empirical Review

Risius and Spohrer (2017) studied the applicability of blockchain technology and where it has mentionable practical effects. The study adapts an established research frame work to structure the insights of the current body of research on blockchain technology. The frame work differentiates three groups of activities (design and features, measurement and value, management and organization) at four level of analysis (users and society, intermediaries platforms, firms and industry). The review shows that research has predominantly focused on technological questions of design and features while neglecting application, value creation and governance. Olaniyi (2018) investigate the relationship between blockchain technology and financial market. The US and China are used as case studies for the 2008-2016 period using fully modified least square and Toda- Yamamoto causality technique. The estimates show that blockchain technology has positive and significant relationship with the financial market in US and China. In other words, the higher the levels of blockchain innovation in these countries, the more developed the financial market. Liu and Ye (2021) studied the relationship between trust and user acceptance. 254 questionnaires about blockchain applications were collected and analyzed with smart PL3.0. The results show that trust and information quality has positive effects on the users' behaviour intentions, except in terms of output quality.

Oseiweh (2018) studied how frauds have affected the banking sector financial performance in Nigeria. Data spanning 1993 to 2016 was used. The method of data analysis was co-integration and error correction mechanism. The finding from the estimation revealed that a three period lag of number of fraud cases has negative effect on the banking sector financial performance and was statistically significant. Ijeoma and Aronu (2013) studied the impact of fraud management on organizational survival. The objective of the study is to determine if business organization or companies adopt holistic approach to fraud management. A sample size of forty four (44) staff was used to evaluate the chi-square test statistics. It was observed that adoption of holistic approach to fraud management do not help companies in preventing fraud in Nigeria. Omokaro and Ikpere(2019) did a study on the impact of fraud management activities on organizational survival in Nigeria. The study used structured questionnaire which was administered to 270 respondents. The Wilcoxon test was used to analyze the data obtained in the study. The study revealed that the major measures of fraud management in Nigeria are deterrence measures, analysis measures, investigation measures and prosecution measures. The result implies that effective implementation of fraud management activities does not significantly impact on fraud management in organizations. Surjandari and Martaningtyas (2015) studied the effect of performance incentives, internal control system, organizational culture, on fraud of Indonesia government officer. They made use of questionnaire, stratified random sampling and structural equation modeling. Two results were opposite with previous studies. (a) The performance incentive did not affect the fraud because the incentive was not based on performance. Most of the fraud was done by those with below 5years working period. (b) Internal control system did not affect the fraud because application on internal control did not confirm with PP number 60, year 2008 as a good guidance and most fraud was done because of opportunity presence. The organization culture, only one in line with previous studies had effected the fraud, because of success in punishment socialization, officer trainings , transparency and accountability.

Archambeault and Webber (2018) examined the survival of nonprofit organizations after the discovering of fraud. An analysis of 115 nonprofit organizations experiencing a fraud shows that over one fourth of these organizations did not survive at least 3years beyond the publication of the fraud, a rate considerably higher than the typical nonprofit failure rate. Frazer (2012) determined whether internal control system influenced restaurant managers' perceptions of undesirable behaviours also known as deviation in restaurant. Deviation in this study was defined as fraud, waste and errors. A random sample of restaurants doing business in Nassau country in the state of New York was selected. The data was analyzed using multiple regression and descriptive statistics. The result from the study indicated that there was a statistically significant relationship between internal control and deviation (that is errors, fraud and waste). Enofe et al.(2017) did a study on bank fraud and preventive measures in Nigeria. Primary data were used for this study. This study was carried out by collecting data from 15 quoted commercial banks in Nigeria as at 31st December, 2015. The study utilized ordinary least square regression model. It was observed that strong internal control system, good corporate governance and compliance with banking ethics have positive and significant influence in fraud prevention in banking industry. Micheni (2016) did a study on the effectiveness of internal control on detection and prevention of fraud on commercial bank listed in Nairobi.

Questionnaires were administered to solicit information from respondents. Data collected were analyzed descriptively using figures and tables and inferentially using Microsoft office spread sheet program (EXCEL). The finding of the study revealed a strong positive association between internal controls instituted by organization.

Conclusion

Blockchain with its characteristics of decentralization, immutable records, persistency, anonymity, security, auditability, transparency, accuracy, verifiability and sharing of information has the potential of transforming business organization in Nigeria. Blockchain peer-to-peer connections help to identify fraud activities in the network and distributed consensus. No doubt blockchain can help fraud detection because it enabled the sharing of information in realtime and all participants in a blockchain have visibility over transaction. Its traceability can help keep staff at bay and enhanced the profitability of the firm. Blockchain record keeping attribute helps the various stake holders to confirm validity and legitimacy. Blockchain has strong connectivity to business survivals, businesses in Nigeria must move from the conventional method of fraud control to a more digitized method which is more efficient and effective and could be more durable method to solve fraudulent activities of staff that undermines the growth of business organization and deplete shareholder funds. Adequate understanding on how and why people commit fraud will help to deploy the necessary technological tools to stem the tides. Payment processing, contract management, supply processing, money transfer and account recording can be better protected with blockchain. It almost impossible to invade the network as attacker can impart the network only when they have majority control of the node.

We suggest a multidisciplinary collaboration in the use of blockchain technology for wider acceptance and trust because of its impact on business survival. Accordingly, further research focus, should be on simplified application and value creation of blockchain technology.

References

- Archambeault, D.S. & Webber, S (2018). Fraud survival in nonprofit organizations: Empirical evidence. *Nonprofit Management and Leadership*, 29(1), 29-46. <https://doi.org/10.1002/nml.21313>
- Enofe, A.O., Abilogun, T.O., Omoolorun, A.J & Elaiho, E.M.(2017). Bank fraud and preventive measure in Nigeria. An Empirical Review. *International Journal of Academic Research in Business and Social Sciences*,7(7), 40-51. <https://doi.org/10.6007/IJARBS/V7.17/3076>
- Frazer,L.(2012). An empirical analysis on the effects of internal control on deviation in small restaurants. *Journal of Business & Economics Research*, 10(6),361-374. <https://doi.org/10.19030/ijber.v10i6.7027>
- Ijeoma, N. & Aronu, C.O.(2013). The impact of fraud management on organizational survival in Nigeria. *American Journal of Economics*, 3(6), 268-272. <https://doi.org/10.5923/j.economics.20130306.04>
- Liu, N.& Ye, Z. (2021). Empirical research on the blockchain adoption- based on TAM. *Applied Economics*, 53 (37), 4263-4275. <https://doi.org/10.1080/00036846.2021.1898535>
- Micheni, S.N. (2016). Effectiveness of internal control on detection and prevention of fraud on commercial Banks listed in Nairobi security exchange. A research project submitted in partial fulfillment of the requirement for the award of Master of Science, finance, University of Nairobi
- Olaniyi, E. (2018). Blockchain technology and Finance market: An Empirical Analysis. *Actual Problems of the Economy*, 211 (12 october,2019), 82-101
- Olanrewaju, R.A. & Johnson-Rokosu, S. (2019). Impact of employee fraud on business entities in Nigeria. *International Journal of Research and innovation in social science*, III(XI), 41-50
- Omokaro, B.E. & Ikpere, O.C.(2019). The impact of fraud management activities on organization survival in Nigeria. *International Journal of Research and Innovation in Applied Science*, IV(IV),20-24
- Oseiweh, O.S.(2018). Empirical assessment of frauds on the financial performance of banking sector in Nigeria. *International Journal of Research studies in Management*, 7(1), 75-84. <https://doi.org/10.5861/ijrsm.2018.3007>
- Oyebanjo, G.O., Olabode, H.O. & Robertson, K.T. (2021). Blockchain technology as a panacea for procurement corruption in digital era. *International Journal of Research in Business & Social Science*(2147-4478), 10(4), 311-20. <https://doi.org/10.20525/ijrbs.v10i4.122>
- Risius ,M. & Spohrer, K. (2017). Blockchain Research Framework: What we (don't) know, where we go from here and how we will get there. *Business & Information Systems Engineering*,59(6), 385-409. <https://doi.org/10.1007/512599-017-0506-0>
- Sarmah, S.S (2018). Understanding Blockchain Technology. *Computer Science and Engineerin*,8(2),23-29. <https://doi.org/10.523/j.computer.2018.08802.07>

- Surjandari, D.A & Martaningtyas, I. (2015). An Empirical Study: The effect of performance incentives, internal control system, organizational culture, on fraud of Indonesia government officer. *Mediterranean Journal of Social Sciences*, 6(5S5),71. D <https://doi.org/10.5901/mjss.2015.v6n555,71>
- Zheng, Z., Xie, S., Dia, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus and Future Trends. 6TH IEEE International Congress on Big Data. <https://doi.org/10.1109/Big Data on grass.2017.85>

Publisher's Note: SSBFNET stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



© 2021 by the authors. Licensee SSBFNET, Istanbul, Turkey. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

International Journal of Research in Business and Social Science (2147-4478) by SSBFNET is licensed under a Creative Commons Attribution 4.0 International License.