Research Article / Review Article FUPRE JOURNAL 8(3): 136-147(2024)

FUPRE Journal

of

Scientific and Industrial Research

ISSN: 2579-1184(Print) ISSN: 2578-1129 (Online)

http://fupre.edu.ng/journal

Exploring Biometric Gait with Blockchain Cryptocurrencies Framework

MATTHEW, J. O. [1,*], ***ALLENOTOR, D.*** [2]

[1,2]*Department of Computer Science, College of Science, Federal University of Petroleum*

ARTICLE INFO

Received: 10/12/2023

Accepted: 05/05/2024

Keywords

Biometric,
Blockchain,
Cryptocurrencies
Facial recognition,
Machine learning,

ABSTRACT

The blockchain has continued to showcase myriads of promises as a breakthrough tech and highly adapted in manifold sectors. Its adoption is accompanied by a range of issues that make implementation complicated. To aid successful implementation, a variety of frameworks have been developed. But, selecting the appropriate framework based on the conformity of its features with the financial sector is a challenge for decision-makers. This study seeks to provide solution to the challenge of synchronizing entire blockchain in a minimum possible time, and create a Blockchain Technology Framework for pricing and Evaluating Financial Markets and also simulate the cryptocurrency market data using a neural network based application to generate the optimal prediction and predicting the future of investment by fusing the facial recognition system with the framework.

1. INTRODUCTION

Businesses saw substantial changes with Industrial revolution and ledgers used grew complicated as factories and huge businesses proliferated, requiring better management (Pinna & Ibba, 2017; Polge et al., 2021). First used by business owners, ledgers were used records transactions and its entries measured a quantity of possessed or owed prior to the invention of fiat money managed by financial institutions (Ojugo & Ekurume, 2021a). Ledgers record business transacts between individuals such as sales credits/debits, assets and expenditures. Thus, value is assigned for goods (Saberi et al., 2019). The imposition of taxes for non-payment by central authorities like banks and government – allowed for the creation of fiat money, which increased its demand in time. The more a people accept a currency, its value rises as a powerful effect of its network. Ledgers have also evolved as for tracking and tracing of person's assets and liabilities (Ojugo & Ekurume, 2021b; Tian, 2017; Torky & Hassanein, 2020).

The birth of informatics and computing and the subsequent development of software revolutionized ledger systems. In the mid-20th century, businesses began transitioning from manual ledger entries to computerized systems. Initially, mainframe computers were used to process and store financial data, but with the advent of personal computers, ledger software became more accessible (Ojugo et al., 2021b, 2021a). A ledger is a modern day database of records/transactions. Traditional databases have long been used to store and manage data in a centralized manner. In this model, a central authority maintains control over the database and validates and verifies transactions (Ibor et al., 2023). While this approach has its benefits of simplicity and ease of use, it also suffers from vulnerabilities like points of failure and data manipulation risks (Ojugo, Odiakaose, & Emordi, 2023;

*Corresponding author, e-mail:sammydestiny@live.com
DIO

Ojugo, Odiakaose, Emordi, et al., 2023).

The birth of peer-to-peer (P2P) networks as alternative to centralized system – consists of distributed peers or nodes that are both clients and servers. P2P networks allow direct communication and data sharing between participants without need for intermediaries. This decentralized strategy decentralizes power while boosting privacy and resilience. P2P networks, however, cannot solve the issue of consensus and participant trust on their own. If a peer is sharing a confidential file on the network, it may be challenging to confirm that they have right authorizations to do so given number of nodes.

Ledgers have been used and dates back to ancient civilizations when humans started deploying means to record/track economic transactions (Baralla et al., 2019). Sumerians and Babylonians recorded such transactions on clay tablets (Ojugo, Ejeh, Odiakaose, et al., 2023) and Mesopotamia (i.e Iraq) recorded quantities over 5000years ago, partitioned into rows and columns where each cell has a picture of the type of item (pictograms) using cuneiform script to indicate the quantity of it (Bedoui & Robbana, 2019). Each item had its graphic representation making the ledger language an earliest form of writing we have discovered (Aghware et al., 2023a, 2023b; Akazue et al., 2023; Kabir Bako et al., 2019; Ojugo, Eboka, et al., 2015b).

Evidence abounds that Indians and kings of old, used skilled accountants to administer and oversee their financial concerns (Caro et al., 2018; Damoska & Erceg, 2022). Double-entry book-keeping is widely used during a certain era and was credited to Luca Pacioli with his birthing of debits and credits to keep track of financial transactions. Businesses were able to retain accurate financial records via double-entry bookkeeping. Double-entry book-keeping was used in Italy, which used a ledger to record both debits and credits. It was widely adopted and has evolved in time rather than via purposeful search. Ledgers have played a crucial role in accounting over time, evolving from primitive methods to sophisticated digital systems (Lewis, 2015; Quamara & Singh, 2023; Tian, 2016).

1.1. Blockchain Evolution as Ledger

Distributed ledger has gain prominence with the birth of blockchain. Distributed ledger is duplicated and distributed across a network with each node having a copy of the entire record of transactions on the network. Each node can supplement the data in the network but cannot alter any data without the consensus of majority of the nodes of the network. It can be viewed as a decentralized database managed and authenticated by multiple participants of the network. Features of digital currencies can include anonymity, consensus, distributed, immutable, secure and caries a time stamp on all transactions as in figure 1.

Figure 1: Evolution of Money

Blockchain ledger was built on the concept of Distributed ledger technology and it practical use was introduced in 2008 with the creation of Bitcoin (Nakamoto, 2008), which combines cryptographic techniques, decentralized consensus, and a data structure called a blocks and yield transparent, tamper-proof, and decentralized ledger transactions. Blockchain offer various merits such as better security, transparency, immutability without need for a central authority. It eliminates the need for a central authority by providing a decentralized, transparent, and secure ledger that is maintained by a network of nodes. In addition to financial applications, blockchain ledgers are being explored for use in other industries, such as healthcare, real estate, and government. Ledgers have evolved over time to meet the changing needs of society (Saberi et al., 2019).

1.2. Economic Impact of Cryptos

Cryptocurrency is digital money that does not require financial institution to verify transactions and can be used for purchases or as an investment. Cryptos are digital or virtual currencies that leverage cryptographic techniques to secure transactions and control the creation of new units. Cryptocurrency as the name given to a system that uses cryptography to allow the secure transfer and exchange of digital tokens in a distributed and decentralized manner. These tokens can be traded at market rates for fiat currencies. Bitcoin as the first cryptocurrency, started trading in January 2009 (Kamble et al., 2019; Kim & Laskowski, 2018).

Studies have examined various aspects of cryptos adoption, market dynamics, and economic implications. Factors that influence adoption and rise of cryptos in financial systems includes its price formation, market efficiency, and its trading behaviour. The rise in applications and adoption of electronic transactions in the financial sector by various organization have played a major role in cryptocurrency adoption across the globe. The increase in companies using informatics and finance (i.e. FinTech) has eased adoption of these techs, predicted to revolutionize the financial ecosystem (Allenotor et al., 2015; Allenotor & Ojugo, 2017; Eboka & Ojugo, 2020; Malasowe et al., 2023). The potential impact of digital currencies can be seen as in figure 2.

Breakthroughs like peer-to-peer lending, mobile payments, digital banking, and other high-tech advancements, the need for digital currencies to support seamless and rapid financial transactions has lately surged (Brezo, 2012). Financial institutions have a history of advancing financial breakthroughs. However, things have evolved with the dawn of FinTech business in this internet-age. With the introduction of the first crypto currency by Nakamoto, there has been an exponential growth in its us. Cryptos are not only used as a currency; But, is now adopted as assets to store value because of crypto price formation, and market behaviour ensures volatility (Gasco-Hernandez et al., 2018; Holmberg, 2018; Iyoboyi & Musa-Pedro, 2020; Ojugo & Eboka, 2018, 2019a, 2019b).

Figure 2: Potentials of digital currencies

It has presented various opportunities as people buy crypto currencies before they lunch at a very cheap price with the hopes of the coin increasing in price when it lunches. This alone will motivate a lot of adoption because of the possibility to make money. They noted that volatilities in its asset market can be explained by the direction of causality from conventional to Bitcoin markets and not vice-versa (Ojugo, Allenotor, et al., 2015; Ojugo & Eboka, 2014). Thus, price or value of a crypto is determined by its asset market (Ojugo, Eboka, Yerokun, et al., 2013; Ojugo, Eboka, et al., 2015a; Ojugo & Eboka, 2021). Some cryptocurrencies focus on privacy and anonymity features, aiming to provide enhanced confidentiality for users. Privacy-centric cryptocurrencies employ techniques like zero-knowledge proofs, ring signatures, or stealth addresses to obfuscate transaction details and protect user privacy (Kodali & Yerroju, 2017; Rakhra et al., 2022).

1.3. Biometric Gaits

Biometrics deals with measurement and analysis of biological data via authentication technologies. It seeks to extract body features and characteristics of a person such as voice and facial patterns, eye retinas, finger prints, DNA, eye irises and hand, and explore them for information purposes (Kamble et al., 2019; Kim & Laskowski, 2018). It also portends a means of identification via the characteristics or features (Abernathy, 2021; Ayyappan & Matilda, 2020; Edirisooriya & Jayatunga, 2021). It is simply a way to identify a person as in figure 3.

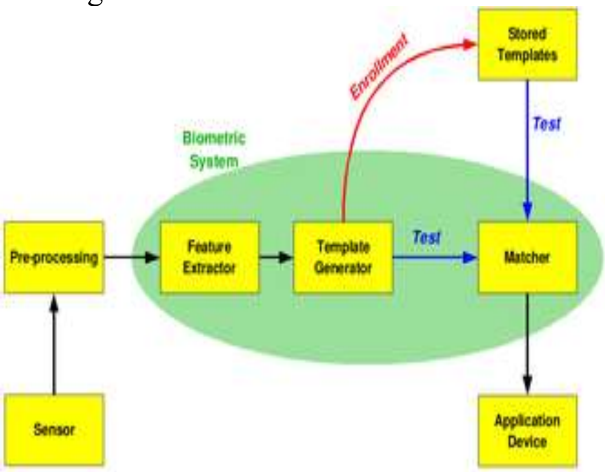

Figure 3. Logic block of Biometric system

Biometrics are often grouped into physiological (identification via DNA, iris scan, fingerprint, iris, hand, palm vein, face), and behavioural (identification via voice, typical rhythm, keystroke, gait recognition, and signatures. While, rarely used due to its accuracy – it is costly, and unsuited in many applications due to security requirements. Also, user reluctance is another factor as this is considered intrusive, inconveniencing and has privacy concerns.

Biometric authentication presents more potential. As it evolves, its accuracy and the convenience for users are likely to increase, and biometric devices may take the natural and well-deserved lead as user authentication credentials (Ojugo, Abere, Orhionkpaiyo, et al., 2013; Ojugo et al., 2015; Ojugo, Akazue, Ejeh, Ashioba, et al., 2023; Ojugo, Akazue, Ejeh, Odiakaose, et al., 2023).

This study is motivated as thus:

1. **Security:** Existing system incorporates security measures to protect the integrity and data confidentiality via: (a) the use of encryption techniques to safeguard data, ensure nonrepudiation and confidentiality with data transfer. It prevent unauthorized access to sensitive information, (b) access control helps to regulate user permissions and restrict unauthorized access to data. It ensures only authorized users can view or modify data, and (c) utilize the consensus mechanism such as proof-of-work (PoW) or proof-of-stake (PoS) for immutability of data stored in the chain, and maintains system integrity (Avinadav, 2020; Cao & Guo, 2017; Ojugo & Otakore, 2018b, 2020a; Oyemade & Ojugo, 2020).
2. **Decentralization** helps system achieve an effective data management via use of: (a) distributed network of nodes, where each node stores a copy of the blockchain. It prevents a single points of failure and enhances system's resilience, (b) use of a consensus algorithm to ensure agreement among nodes on validity of transactions. This enhances system reliability and trust, and (c) P2P enable direct communication between participants and removes the need for intermediaries. It also promotes decentralization and reduces reliance on centralized entities (Arias-Oliva et al., 2019; Bodó et al., 2018; Cha et al., 2018; Ojugo, Yoro, Okonta, et al., 2013).
3. **Privacy** seeks to preserve the privacy of sensitive data via: (a) uses pseudonymity identifiers to associate transactions with users, thereby protecting their real-world identities. It maintain user privacy while ensuring the traceability of transactions, and (b) it emplys user private transactions technique such as zero-knowledge proofs or ring signatures, to hide transaction details from unauthorized parties. This enhances transactional privacy within the system (Okonta et al., 2013, 2014; Tarafdar & Zhang, 2005).

Study aims to improved security feature in the blockchain currency using a machine-learning-based gaits detection ensemble to help provide a more personalized and secure ecosystem that enables users perform transactions, and not compromise security and anonymity.

2. MATERIALS AND METHODS

2.1. Existing Ensemble

The existing system is based on Prasanth and Hacket (2021) noted that trust between users and the banks were rapidly decreasing due to the increased costs of mediations and basic transactions. This propelled Nakamoto (2008) to proffer a secure method of payment for consumers that would embody the four objectives of cryptography and enable them to feel more secure. This new payment mode (i.e. bitcoin) used the secure hash algorithm (SHA256) cryptographic proof and built on the P2P network framework (Dwivedi et al., 2019; Kakarlapudi & Mahmoud, 2021).

Societies has transitioned from barter to use of money as a exchange medium, and people have devised means to allow rational mode of exchange value. In relation to goods and services, Aristotle posited 4-criteria to dictate what is considered to be 'good money' (Lee, 2009): It must be durable, portable, divisible and intrinsic value**.** The preferred medium of exchange was gold, and it fulfilled all criteria. As nations grew, this demand for exchange medium increased. Governments were forced to create a more acceptable one that could be controlled and regulated. This birthed fiat currency, and adopted globally with its range of complications that include authentication (Abdullah & Mohd Nor, 2018; Jameaba, 2020; Rakhra et al., 2022).

In order to help fix some of these issues, cryptocurrencies began to emerge in 2009, leveraging a disruptive technology called blockchain. A crypto is a digital currency that uses cryptography (Ojugo, Ugboh, Onochie, et al., 2013; Ojugo, Allenotor, et al., 2015; Ojugo & Yoro, 2020b)- to specifically deal with how data is structured and allows for the existence of decentralized ledger that is able to impact a transaction (Hackett, 2016). To be able to automate pay-out function normally, it requires a wallet. Wallets are controlled via APIs and receive orders to authenticate all outgoing transactions to pay clients wishing to withdraw their funds. Because you need to be able to automate these wallets, the keys must be live, and are therefore at risk.

To address these, a detailed description structure of the blockchain to ensure secure storage, share of sensitive data and privacy of users (Joshi et al., 2021; Ojugo & Yoro, 2020b; Pradeepa & Parveen, 2020). Its many benefits includes (Ojugo & Eboka, 2021).

2.2. Proposed Biometric Blockchain Model

The proposed system uses the advanced encryption standard algorithm to extend the works of (Nicholas, 2016) on Cryptocurrency (Ojugo et al., 2015; Ojugo & Eboka, 2014; Ojugo & Otakore, 2018a; Okobah & Ojugo, 2018). It fuses a facial recognition into the cryptocurrency system in other to secured the platform so that invalid transaction via third party or an invader/intruder cannot longer take place within the system as in figure 3.

The facial recognition to be used is also an improvement on Delac 2007, whose work is based on JPEG, we will further worked on Delac work so that the security issue can be solved once and for all. In addition to these, we will used JPEG 2000 to secure the facial recognition process in other for the image to be sharp and viable for correct recognition of the registered users (Patil et al., 2020; Philipp et al., 2019).

Proposed system resolves 2-problems as thus:

1. First, the facial recognition module in a bid to authenticate transcations, captures user image which is converted using the JPEG2000 format.
2. Second, the cryptocurrency platform uses adaptive scaling for cryptocurrencies with a number of measures to ensure that they will work well in both large and small scales. Bitcoin is programmed to allow for one transaction block to be mined every ten minutes. The algorithm adjusts after every 2016 blocks (theoretically, that's every two weeks) to get easier or harder based on how long it actually took for those 2016 blocks to be mined. So if it only took 13 days for

the network to mine 2016 blocks that means it's too easy to mine, so the difficulty increases. However, if it takes 15 days for the network to mine 2016 blocks that shows that it's too hard to mind, so the difficulty decreases. A number of other measures are included in digital coins to allow for adaptive scaling including limiting the supply overtime (to create scarcity) and reducing the reward for mining as more total coins are mined.

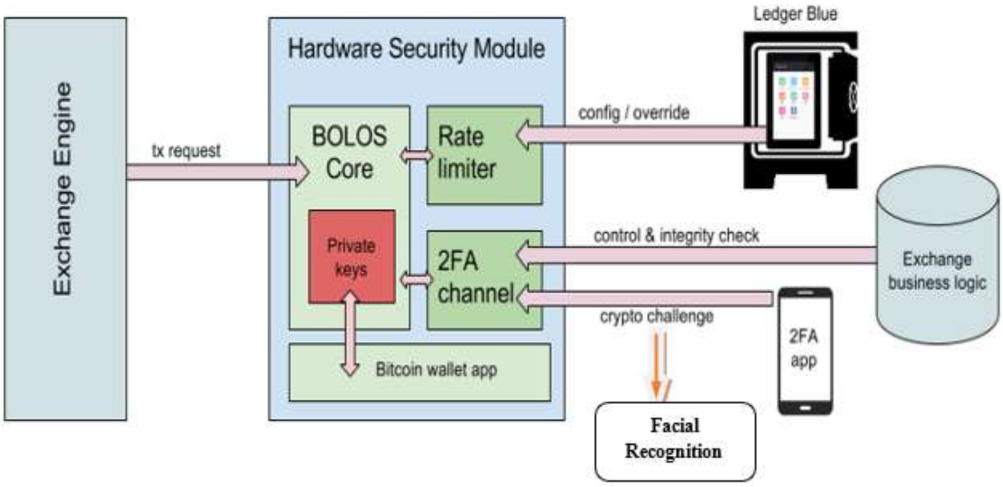

Figure 4: Architecture of Proposed System as supported by (Akazue et al., 2023; Jameaba, 2020; Kabir Bako et al., 2019; Zubaidi & Abdullah, 2017)

2.3. Experimental Testbeds Set-Up

The proposed system evaluates security, data decentralization, and privacy-preserving capabilities as compared to existing system (Ojugo et al., 2015; Ojugo & Eboka, 2014; Ojugo & Otakore, 2018a; Okobah & Ojugo, 2018) as in figure 2:

3. **Security:** We provision security features as thus: (a) encryption and Data Security: Our proposed system will incorporate robust encryption techniques to ensure the confidentiality and integrity of data. it implements secure protocols for data transmission and storage, protecting user information from unauthorized access (Yoro & Ojugo, 2019b, 2019a), (b) it uses smart contract to help system prioritize security via best practices code audits, and through the use of vulnerability tools (Omar et al., 2021). It ensures resilience against known attack/threat and potential exploits (Okuyama et al., 2014; Omar et al., 2020; Ometov et al., 2021), and (c) it uses the consensus mechanism to balance security and scalability. It prevent double-spend attack, maintains immutability, and ensures overall security of system (Castro & Liskov, 2002; Ojugo & Eboka, 2019c).
4. **Decentralization:** System provides these feat via: (a) node distribution and network resilience to mitigate the risks associated with single points of failure and enhances the system's resilience against attacks (Christidis & Devetsikiotis, 2016; De Giovanni, 2020), (b) governance with the consensus model will system establish a robust ensemble to ensure fair decision-making and consensus between various participants. Using transparent rules and mechanisms to aid dispute resolution, our system aims to maintain a decentralized governance structure that reflects the interests of ecosystem participants (Debe et al., 2020; Dourado & Brito, 2014), and (c) scalability and performance with feats such as sharding or layer-2 solutions, to help us address transaction throughput limitations and access time. It helps us handle increased user and data volume without degreded performance (Esposito et al., 2018; Fan et al., 2020; Finck, 2018).

5. **Privacy Analysis:** Proposed system will provide: (a) pseudonymity/anonymity via the unique identifiers that do not directly link users to their real-world identities. It maintain user privacy and traceability (Kakarlapudi & Mahmoud, 2021; Köhler & Pizzol, 2019), (b) privacy-preserving cryptos with advanced features, such as zero-knowledge proofs or ring signatures. This ensure that transactions conducted on our platform remain private and unlink able to specific individuals (De Giovanni, 2020), and (c) Data Minimization and Confidentiality: Our system follows the principle of data minimization, storing only essential information required for transaction validation. Also, this helps to maintain data confidentiality, preventing unintended data exposure (Lu et al., 2020; Madarasz & Santos, 2018; Malasowe et al., 2023; Monrat et al., 2019; Nguyen et al., 2021).

3. RESULT FINDINGS AND DISCUSSION

3.1. System Throughput

Throughput measures a system capacity for the actual transfer rate of data within the system over some time. Here, we measure the number of transactions per second on the proposed chain. The number of transactions per second was obtained from figure 3 as agrees with (Ojugo, Allenotor, et al., 2015; Ojugo & Eboka, 2019b; Yoro & Ojugo, 2019a). The transactions per second for other blockchains models were found to be less than 30. A feature attributed to their proof of work (PoW) adaptation, as a consensus mechanism that helps each user on the chain to effectively and efficiently, compute the posed task during its mining. The nature of each task requires loads of computational power vis-a-vis processing time. Our model uses a permissionless chain. Thus, the transaction per second of our experimental framework is about 1,101 (Ojugo, Abere, Orhionkpaiyo, et al., 2013; Ojugo, Yoro, Oyemade, et al., 2013; Ojugo & Otakore, 2020b; Ojugo & Yoro, 2020a). Figure 5 shows weighted face input for the captured image for the crypto.

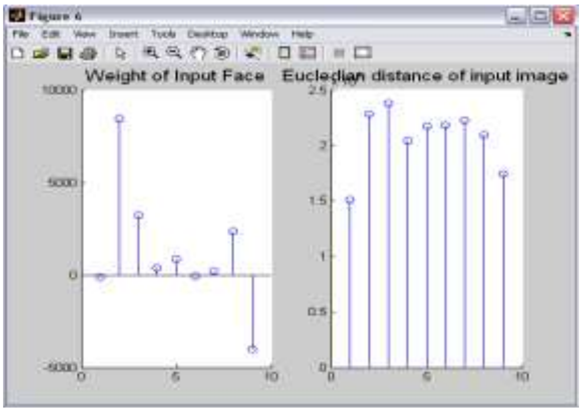

Figure 5. The throughput weighted face

3.2. Discussion of Findings

Our performance metric determines the time interval between a user's request and application response time for feedback to the user. We achieve this by measuring the response time from a query on the https page. Querying data means reading such data via the world-state as stored in the blockchain's hyper-fabric ledger. Data records are stored as a generated key-value pair. Thus, we can query and retrieve data directly as current key-value(s) of a record sought, without it traversing the whole ledger. This, in turn, improves the efficiency and effectiveness of the traceability system. Thus, for the first scenario with a population of 2,500-users, response time was about 0.21 s for queries and 0.28 s for https pages retrieval. While for scenario 2–we experienced a longer response time of about 0.32 s and 0.38 s respectively for both the queries and https pages retrieval. This agrees with (Ojugo, Abere, Orhionkpaiyo, et al., 2013; Ojugo, Yoro, Oyemade, et al., 2013; Ojugo & Otakore, 2020b; Ojugo & Yoro, 2020a).

4. CONCLUSION

We add facial recognition to a crypto-platform to acquire the image, and used the illumination normalization under varying lighting conditions on both training and test database. The description of this database is given in the next subsection. In illumination normalization, histogram equalization is used on the input images for contrast stretching. When the light source is not in front of the subject, the image captured in this condition has illumination variation. As the image has large illumination variation, i.e. the light source is more inclined, the image has lower contrast. On the output, DCT is applied to switch into the frequency domain from space domain. The variation is compensated for by scaling down a low frequency coefficient.

The inverse DCT is applied to generate the illumination normalized images. These images are fed to the classifier engine. We have adopted the k-NNC and NMC. The distance metrics are correlation coefficient and Euclidean distance. The calculation of correlation coefficient is done in two-ways. The Euclidean distance is the distance metric for the analysis. W is generated for training images using eigenvectors of scatter matrix S. After generating Eigen space W, all images, the training as well as the test images are projected on W to generate the set of weights. Euclidean distances are calculated between weights corresponding to the unknown face (test set) and known faces (training set).

Conflict of Interest

The authors declare that there is no conflict of interest.

References

Aghware, F. O., Yoro, R. E., Ejeh, P. O., Odiakaose, C. C., Emordi, F. U., & Ojugo, A. A. (2023a). DeLClustE: Protecting Users from Credit-Card Fraud Transaction via Deep-Learning Cluster Ensemble. *International Journal of Advanced Computer Science and Applications*, *14*(6), 94–100. doi: 10.14569/IJACSA.2023.0140610

Aghware, F. O., Yoro, R. E., Ejeh, P. O., Odiakaose, C. C., Emordi, F. U., & Ojugo, A. A. (2023b). Sentiment analysis in detecting sophistication and degradation cues in malicious web contents. *Kongzhi Yu Juece/Control and Decision*, *38*(01), 653.

Akazue, M. I., Yoro, R. E., Malasowe, B. O., Nwankwo, O., & Ojugo, A. A. (2023). Improved services traceability and management of a food value chain using block-chain network : a case of Nigeria. *Indonesian Journal of Electrical Engineering and Computer Science*, *29*(3), 1623–1633. doi: 10.11591/ijeecs.v29.i3.pp1623-1633

Allenotor, D., & Ojugo, A. A. (2017). A Financial Option Based Price and Risk Management Model for Pricing Electrical Energy in Nigeria. *Advances in Multidisciplinary & Scientific Research Journal*, *3*(2), 79–90.

Allenotor, D., Oyemade, D. A., & Ojugo, A. A. (2015). A Financial Option Model for Pricing Cloud Computational Resources Based on Cloud Trace Characterization. *African Journal of Computing & ICT*, *8*(2), 83–92. www.ajocict.net

Arias-Oliva, M., Pelegrín-Borondo, J., & Matías-Clavero, G. (2019). Variables Influencing Cryptocurrency Use: A Technology Acceptance Model in Spain. *Frontiers in Psychology*, *10*. https://doi.org/10.3389/fpsyg.2019.00475

Avinadav, T. (2020). The effect of decision rights allocation on a supply chain of perishable products under a revenue-sharing contract. *International Journal of Production Economics*, *225*, 107587. https://doi.org/10.1016/j.ijpe.2019.107587

Ayyappan, S., & Matilda, S. (2020). Criminals and Missing Children Identification Using Face Recognition and Web Scrapping. *2020 International Conference on System, Computation, Automation and Networking*, doi: 10.1109/ICSCAN49426.2020.9262390

Baralla, G., Ibba, S., Marchesi, M., Tonelli, R., & Missineo, S. (2019). *A Blockchain Based System to Ensure Transparency and Reliability in Food Supply Chain* (pp. 379–391). https://doi.org/10.1007/978-3-030-10549-5_30

Bedoui, H. eddine, & Robbana, A. (2019). Islamic Social Financing Through Cryptocurrency. In *Halal Cryptocurrency Management* (pp. 259–274). Springer International Publishing. https://doi.org/10.1007/978-3-030-10749-9_16

Bodó, B., Gervais, D., & Quintais, J. P. (2018). Blockchain and smart contracts: the missing link in copyright licensing? *International Journal of Law and Information Technology*, *26*(4), 311–336. doi: 10.1093/ijlit/eay014

Caro, M. P., Ali, M. S., Vecchio, M., & Giaffreda, R. (2018). Blockchain-based traceability in Agri-Food supply chain management: A practical implementation. *2018 IoT Vertical and Topical Summit on Agriculture - Tuscany (IOT Tuscany)*, 1–4. https://doi.org/10.1109/IOT-TUSCANY.2018.8373021

Cha, S.-C., Chen, J.-F., Su, C., & Yeh, K.-H. (2018). A Blockchain Connected Gateway for BLE-Based Devices in the Internet of Things. *IEEE Access*, *6*, 24639–24649. https://doi.org/10.1109/ACCESS.2018.2799942

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, *4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

Damoska, S. J., & Erceg, A. (2022). Blockchain

Technology toward Creating a Smart Local Food Supply Chain. *Computers*, *11*(6), 95. https://doi.org/10.3390/computers11060095

Debe, M., Salah, K., Ur Rehman, M. H., & Svetinovic, D. (2020). Monetization of Services Provided by Public Fog Nodes Using Blockchain and Smart Contracts. *IEEE Access*, *8*, 20118. doi: 10.1109/ACCESS.2020.2968573

Dourado, E., & Brito, J. (2014). Cryptocurrency. In *The New Palgrave Dictionary of Economics* (pp. 1–9). Palgrave Macmillan UK. doi: 10.1057/978-1-349-95121-5_2895-1

Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors*, *19*(2), 1–17. https://doi.org/10.3390/s19020326

Eboka, A. O., & Ojugo, A. A. (2020). Mitigating technical challenges via redesigning campus network for greater efficiency, scalability and robustness: a logical view. *International Journal of Modern Education and Computer Science*, *12*(6), 29–45. https://doi.org/10.5815/ijmecs.2020.06.03

Edirisooriya, T., & Jayatunga, E. (2021). Comparative Study of Face Detection Methods for Robust Face Recognition Systems. *5th SLAAI - International Conference on Artificial Intelligence and 17th Annual Sessions*, doi: 10.1109/SLAAI-ICAI54477.2021.9664689

Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K.-K. R. (2018). Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Computing*, *5*(1), 31–37. https://doi.org/10.1109/MCC.2018.011791712

Fan, K., Bao, Z., Liu, M., Vasilakos, A. V., & Shi, W. (2020). Dredas: Decentralized, reliable and efficient remote outsourced data auditing scheme with blockchain smart contract for industrial IoT. *Future Generation Computer Systems*, *110*, 665–674. https://doi.org/10.1016/j.future.2019.10.014

Ibor, A. E., Edim, E. B., & Ojugo, A. A. (2023). Secure Health Information System with Blockchain Technology. *Journal of the Nigerian Society of Physical Sciences*, *5*(992), 1–8. https://doi.org/10.46481/jnsps.2022.992

Jameaba, M. (2020). Digitization, FinTech Disruption, and Financial Stability: The Case of the Indonesian Banking Sector. *SSRN Electronic Journal*, *34*, 1–44. https://doi.org/10.2139/ssrn.3529924

Joshi, C., Aliaga, J. R., & Insua, D. R. (2021). Insider Threat Modeling: An Adversarial Risk Analysis Approach. *IEEE Transactions on Information Forensics and Security*, *16*, 1131–1142. https://doi.org/10.1109/TIFS.2020.3029898

Kabir Bako, H., Abba Dandago, M., & Shamsudeen Nassarawa, S. (2019). Food Traceability System: Current State and Future Needs of the Nigerian Poultry and Poultry Product Supply Chain. *Chemical and Biomolecular Engineering*, *4*(3), 40. https://doi.org/10.11648/j.cbe.20190403.11

Kakarlapudi, P. V., & Mahmoud, Q. H. (2021). Design and Development of a Blockchain-Based System for Private Data Management. *Electronics*, *10*(24), 3131. https://doi.org/10.3390/electronics10243131

Kamble, S., Gunasekaran, A., & Arha, H. (2019). Understanding the Blockchain technology adoption in supply chains-Indian context. *International Journal of Production Research*, *57*(7), 2009–2033. doi: 10.1080/00207543.2018.1518610

Kim, H. M., & Laskowski, M. (2018). Toward an ontology-driven blockchain design for supply-chain provenance. *Intelligent Systems in Accounting, Finance and Management*, *25*(1), 18–27. https://doi.org/10.1002/isaf.1424

Kodali, R. K., & Yerroju, S. (2017). IoT based smart emergency response system for fire hazards. *2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology (ICATccT)*, 194–199. doi: 10.1109/ICATCCT.2017.8389132

Köhler, S., & Pizzol, M. (2019). Life Cycle Assessment of Bitcoin Mining. *Environmental Science & Technology*, *53*(23), 13598–13606. https://doi.org/10.1021/acs.est.9b05687

Lewis, A. (2015). Blockchain Technology Explained. *Blockchain Technologies*, 1–27. http://www.blockchaintechnologies.com/blockchain-definition

Li, T., & Li, N. (2008). Towards optimal k-anonymization. *Data & Knowledge Engineering*, *65*(1), 22–39. https://doi.org/10.1016/j.datak.2007.06.015

Linoy, S., Stakhanova, N., & Ray, S. (2021). De-anonymizing Ethereum blockchain smart contracts through code attribution. *International Journal of Network Management*, *31*(1). doi: 10.1002/nem.2130

Lu, Y., Huang, X., Dai, Y., Maharjan, S., & Zhang, Y. (2020). Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT. *IEEE Transactions on Industrial Informatics*, *16*(6), 4177–4186. https://doi.org/10.1109/TII.2019.2942190

Madarasz, N. R., & Santos, D. P. (2018). The concept of human nature in Noam Chomsky. *Veritas (Porto Alegre)*, *63*(3), 1092–1126. doi:10.15448/1984-6746.2018.3.32564

Malasowe, B. O., Akazue, M. I., Okpako, E. A., Aghware, F. O., Ojie, D. V., & Ojugo, A. A. (2023). Adaptive Learner-CBT with Secured Fault-Tolerant and Resumption Capability for Nigerian Universities. *International Journal of Advanced Computer Science and Applications*, *14*(8), 135–142. doi:

10.14569/IJACSA.2023.0140816

Monrat, A. A., Schelen, O., & Andersson, K. (2019). A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities. *IEEE Access*, *7*, 117134–117151. https://doi.org/10.1109/ACCESS.2019.2936094

Nguyen, D. C., Ding, M., Pham, Q.-V., Pathirana, P. N., Le, L. B., Seneviratne, A., Li, J., Niyato, D., & Poor, H. V. (2021). Federated Learning Meets Blockchain in Edge Computing: Opportunities and Challenges. *IEEE Internet of Things Journal*, *8*(16), 12806–12825. https://doi.org/10.1109/JIOT.2021.3072611

Ojugo, A. A., Abere, R. A., Orhionkpaiyo, B. C., Yoro, R. E., & Eboka, A. O. (2013). Technical Issues for IP-Based Telephony in Nigeria. *International Journal of Wireless Communications and Mobile Computing*, *1*(2), 58. doi.org/10.11648/j.wcmc.20130102.11

Ojugo, A. A., Aghware, F. O., Yoro, R. E., Yerokun, M. O., Eboka, A. O., Anujeonye, C. N., & Efozia, F. N. (2015). Dependable Community-Cloud Framework for Smartphones. *American Journal of Networks and Communications*, *4*(4), 95. doi: 10.11648/j.ajnc.20150404.13

Ojugo, A. A., Akazue, M. I., Ejeh, P. O., Ashioba, N. C., Odiakaose, C. C., Ako, R. E., & Emordi, F. U. (2023). Forging a User-Trust Memetic Modular Neural Network Card Fraud Detection Ensemble: A Pilot Study. *Journal of Computing Theories and Applications*, *1*(2), 1–11. https://doi.org/10.33633/jcta.v1i2.9259

Ojugo, A. A., Akazue, M. I., Ejeh, P. O., Odiakaose, C., & Emordi, F. U. (2023). DeGATraMoNN: Deep Learning Memetic Ensemble to Detect Spam Threats via a Content-Based Processing. *Kongzhi Yu Juece/Control and Decision*, *38*(01), 667–678.

Ojugo, A. A., Allenotor, D., Oyemade, D. A., Yoro, R. E., & Anujeonye, C. N. (2015). Immunization Model for Ebola Virus in Rural Sierra-Leone. *African Journal of Computing & ICT*, *8*(1), 1–10. www.ajocict.net

Ojugo, A. A., & Eboka, A. O. (2014). A Social Engineering Detection Model for the Mobile Smartphone Clients. *African Journal of Computing & ICT*, *7*(3). www.ajocict.net

Ojugo, A. A., & Eboka, A. O. (2018). Modeling the Computational Solution of Market Basket Associative Rule Mining Approaches Using Deep Neural Network. *Digital Technologies*, *3*(1), 1–8. https://doi.org/10.12691/dt-3-1-1

Ojugo, A. A., & Eboka, A. O. (2019a). Extending Campus Network Via Intranet and IP-Telephony For Better Performance and Service Delivery: Meeting Organizational Goals. *Journal of Applied Science, Engineering, Technology, and Education*, *1*(2), 94–104. https://doi.org/10.35877/454ri.asci12100

Ojugo, A. A., & Eboka, A. O. (2019b). Inventory prediction and management in Nigeria using market basket analysis associative rule mining: memetic algorithm based approach. *International Journal of Informatics and Communication Technology (IJ-ICT)*, *8*(3), 128. https://doi.org/10.11591/ijict.v8i3.pp128-138

Ojugo, A. A., & Eboka, A. O. (2019c). Signature-based malware detection using approximate Boyer Moore string matching algorithm. *International Journal of Mathematical Sciences and Computing*, *5*(3), 49–62. https://doi.org/10.5815/ijmsc.2019.03.05

Ojugo, A. A., & Eboka, A. O. (2021). Modeling Behavioural Evolution as Social Predictor for the Coronavirus Contagion and Immunization in Nigeria. *Journal of Applied Science, Engineering, Technology, and Education*, *3*(2), 135–144. doi: 10.35877/454RI.asci130

Ojugo, A. A., Eboka, A. O., Yerokun, M. O., Iyawa, I. J., & Yoro, R. E. (2013). Cryptography: Salvaging Exploitations against Data Integrity. *American Journal of Networks and Communications*, *2*(2), 47. doi: 10.11648/j.ajnc.20130202.14

Ojugo, A. A., Eboka, A. O., Yoro, R. E., Yerokun, M. O., & Efozia, F. N. (2015a). Framework design for statistical fraud detection. *Mathematics and Computers in Science and Engineering Series*, *50*, 176–182.

Ojugo, A. A., Eboka, A. O., Yoro, R. E., Yerokun, M. O., & Efozia, F. N. (2015b). Hybrid model for early diabetes diagnosis. *2015 Second International Conference on Mathematics and Computers in Sciences and in Industry (MCSI)*, 55–65. https://doi.org/10.1109/MCSI.2015.35

Ojugo, A. A., Ejeh, P. O., Odiakaose, C. C., Eboka, A. O., & Emordi, F. U. (2023). Improved distribution and food safety for beef processing and management using a blockchain-tracer support framework. *International Journal of Informatics and Communication Technology*, *12*(3), 205. doi: 10.11591/ijict.v12i3.pp205-213

Ojugo, A. A., & Ekurume, E. O. (2021a). Deep Learning Network Anomaly-Based Intrusion Detection Ensemble For Predictive Intelligence To Curb Malicious Connections: An Empirical Evidence. *International Journal of Advanced Trends in Computer Science and Engineering*, *10*(3), 2090–2102. doi: 10.30534/ijatcse/2021/851032021

Ojugo, A. A., & Ekurume, E. O. (2021b). Predictive Intelligent Decision Support Model in Forecasting of the Diabetes Pandemic Using a Reinforcement Deep Learning Approach. *International Journal of Education and Management Engineering*, *11*(2), 40–48. https://doi.org/10.5815/ijeme.2021.02.05

Ojugo, A. A., Obruche, C. O., & Eboka, A. O. (2021a).

Empirical Evaluation for Intelligent Predictive Models in Prediction of Potential Cancer Problematic Cases In Nigeria. *ARRUS Journal of Mathematics and Applied Science*, *1*(2), 110–120. doi: 10.35877/mathscience614

Ojugo, A. A., Obruche, C. O., & Eboka, A. O. (2021b). Quest For Convergence Solution Using Hybrid Genetic Algorithm Trained Neural Network Model For Metamorphic Malware Detection. *ARRUS Journal of Engineering and Technology*, *2*(1), 12–23. https://doi.org/10.35877/jetech613

Ojugo, A. A., Odiakaose, C. C., & Emordi, F. U. (2023). Evidence of Students ' Academic Performance at the Federal College of Education Asaba Nigeria: Mining Education Data. *Knowledge Engineering and Data Science*, *6*(2), 145–156. doi: 10.17977/um018v6i22023p145-156

Ojugo, A. A., Odiakaose, C. C., Emordi, F. U., Ejeh, P. O., Adigwe, W., Anazia, K. E., & Nwozor, B. (2023). Forging a learner-centric blended-learning framework via an adaptive content-based architecture. *Science in Information Technology Letters*, *4*(1), 40–53. https://doi.org/10.31763/sitech.v4i1.1186

Ojugo, A. A., & Otakore, D. O. (2018a). Redesigning Academic Website for Better Visibility and Footprint: A Case of the Federal University of Petroleum Resources Effurun Website. *Network and Communication Technologies*, *3*(1), 33. https://doi.org/10.5539/nct.v3n1p33

Ojugo, A. A., & Otakore, O. D. (2018b). Improved Early Detection of Gestational Diabetes via Intelligent Classification Models: A Case of the Niger Delta Region in Nigeria. *Journal of Computer Sciences and Applications*, *6*(2), 82–90. https://doi.org/10.12691/jcsa-6-2-5

Ojugo, A. A., & Otakore, O. D. (2020a). Computational solution of networks versus cluster grouping for social network contact recommender system. *International Journal of Informatics and Communication Technology*, *9*(3), 185. doi: 10.11591/ijict.v9i3.pp185-194

Ojugo, A. A., & Otakore, O. D. (2020b). Investigating The Unexpected Price Plummet And Volatility Rise In Energy Market: A Comparative Study of Machine Learning Approaches. *Quantitative Economics and Management Studies*, *1*(3), 219–229. https://doi.org/10.35877/454ri.qems12119

Ojugo, A. A., Ugboh, E., Onochie, C. C., Eboka, A. O., Yerokun, M. O., & Iyawa, I. J. B. (2013). Effects of Formative Test and Attitudinal Types on Students' Achievement in Mathematics in Nigeria. *African Educational Research Journal*, *1*(2), 113–117. http://search.ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ1216962&site=ehost-live

Ojugo, A. A., & Yoro, R. E. (2020a). Empirical Solution For An Optimized Machine Learning Framework For Anomaly-Based Network Intrusion Detection. *Technology Report of Kansai University*, *62*(08), 6353–6364.

Ojugo, A. A., & Yoro, R. E. (2020b). Forging A Smart Dependable Data Integrity And Protection System Through Hybrid-Integration Honeypot In Web and Database Server. *Technology Report of Kansai University*, *62*(08), 5933–5947.

Ojugo, A. A., Yoro, R. E., Okonta, E. O., & Eboka, A. O. (2013). A Hybrid Artificial Neural Network Gravitational Search Algorithm for Rainfall Runoffs Modeling and Simulation in Hydrology. *Progress in Intelligent Computing and Applications*, *2*(1), 22–34. https://doi.org/10.4156/pica.vol2.issue1.2

Ojugo, A. A., Yoro, R. E., Oyemade, D. A., Eboka, A. O., Ugboh, E., & Aghware, F. O. (2013). Robust Cellular Network for Rural Telephony in Southern Nigeria. *American Journal of Networks and Communications*, *2*(5), 125. https://doi.org/10.11648/j.ajnc.20130205.12

Okobah, I. P., & Ojugo, A. A. (2018). Evolutionary Memetic Models for Malware Intrusion Detection: A Comparative Quest for Computational Solution and Convergence. *International Journal of Computer Applications*, *179*(39), 34–43. https://doi.org/10.5120/ijca2018916586

Okonta, E. O., Ojugo, A. A., Wemembu, U. R., & Ajani, D. (2013). Embedding Quality Function Deployment In Software Development: A Novel Approach. *West African Journal of Industrial & Academic Research*, *6*(1), 50–64.

Okonta, E. O., Wemembu, U. R., Ojugo, A. A., & Ajani, D. (2014). Deploying Java Platform to Design A Framework of Protective Shield for Anti– Reversing Engineering. *West African Journal of Industrial & Academic Research*, *10*(1), 50–64.

Okuyama, S., Tsuruoka, S., Kawanaka, H., & Takase, H. (2014). Interactive Learning Support User Interface for Lecture Scenes Indexed with Extracted Keyword from Blackboard. *Australian Journal of Basic and Applied Sciences*, *8*(4), 319–324.

Omar, I. A., Jayaraman, R., Debe, M. S., Salah, K., Yaqoob, I., & Omar, M. (2021). Automating Procurement Contracts in the Healthcare Supply Chain Using Blockchain Smart Contracts. *IEEE Access*, *9*, 37397–37409. https://doi.org/10.1109/ACCESS.2021.3062471

Omar, I. A., Jayaraman, R., Salah, K., Simsekler, M. C. E., Yaqoob, I., & Ellahham, S. (2020). Ensuring protocol compliance and data transparency in clinical trials using Blockchain smart contracts. *BMC Medical Research Methodology*, *20*(1), 224. https://doi.org/10.1186/s12874-020-01109-5

Oyemade, D. A., & Ojugo, A. A. (2020). A Property

Oriented Pandemic Surviving Trading Model. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(5), 7397. doi: 10.30534/ijatcse/2020/71952020

Patil, A. S., Hamza, R., Hassan, A., Jiang, N., Yan, H., & Li, J. (2020). Efficient privacy-preserving protocol using blockchain smart contracts. *Computers & Security*, *97*, 101958. doi: 10.1016/j.cose.2020.101958

Philipp, R., Prause, G., & Gerlitz, L. (2019). Blockchain and Smart Contracts for Entrepreneurial Collaboration in Maritime Supply Chains. *Transport and Telecommunication Journal*, *20*(4), 365–378. https://doi.org/10.2478/ttj-2019-0030

Pinna, A., & Ibba, S. (2017). *A blockchain-based Decentralized System for proper handling of temporary Employment contracts*. https://doi.org/1711.09758

Polge, J., Robert, J., & Le Traon, Y. (2021). Permissioned blockchain frameworks in the industry: A comparison. *ICT Express*, *7*(2), 229–233. doi: 10.1016/j.icte.2020.09.002

Pradeepa, K., & Parveen, M. (2020). Solid State Technology 8060 A Survey on Routing Protocols With Security in Internet of Things A Survey on Routing Protocols With Security in Internet of Things. *International Virtual Conference on Emerging Trends in Computing*, *63*(4), 38–111.

Rajput, A. R., Li, Q., Taleby Ahvanooey, M., & Masood, I. (2019). EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain. *IEEE Access*, *7*, 84304–84317. https://doi.org/10.1109/ACCESS.2019.2917976

Rantos, K., Drosatos, G., Kritsas, A., Ilioudis, C., Papanikolaou, A., & Filippidis, A. P. (2019). A Blockchain-Based Platform for Consent Management of Personal Data Processing in the IoT Ecosystem. *Security and Communication Networks*, *2019*, 1–15. https://doi.org/10.1155/2019/1431578

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, *57*(7), 2117–2135. doi: 10.1080/00207543.2018.1533261

Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The Energy Consumption of Blockchain Technology: Beyond Myth. *Business & Information Systems Engineering*, *62*(6), 599–608. https://doi.org/10.1007/s12599-020-00656-x

Sun, Y., & Gu, L. (2021). Attention-based Machine Learning Model for Smart Contract Vulnerability Detection. *Journal of Physics: Conference Series*, *1820*(1), 012004. https://doi.org/10.1088/1742-6596/1820/1/012004

Tarafdar, M., & Zhang, J. (2005). Analyzing the influence of Web site design parameters on Web site usability. *Information Resources Management Journal*, *18*(4), 62–80. https://doi.org/10.4018/irmj.2005100104

Torky, M., & Hassanein, A. E. (2020). Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges. *Computers and Electronics in Agriculture*, *178*, 105476. https://doi.org/10.1016/j.compag.2020.105476

Unal, D., Hammoudeh, M., & Kiraz, M. S. (2020). Policy specification and verification for blockchain and smart contracts in 5G networks. *ICT Express*, *6*(1), 43–47. https://doi.org/10.1016/j.icte.2019.07.002

Wang, H., Qin, H., Zhao, M., Wei, X., Shen, H., & Susilo, W. (2020). Blockchain-based fair payment smart contract for public cloud storage auditing. *Information Sciences*, *519*, 348–362. https://doi.org/10.1016/j.ins.2020.01.051

Yoro, R. E., & Ojugo, A. A. (2019a). An Intelligent Model Using Relationship in Weather Conditions to Predict Livestock-Fish Farming Yield and Production in Nigeria. *American Journal of Modeling and Optimization*, *7*(2), 35–41. https://doi.org/10.12691/ajmo-7-2-1

Yoro, R. E., & Ojugo, A. A. (2019b). Quest for Prevalence Rate of Hepatitis-B Virus Infection in the Nigeria: Comparative Study of Supervised Versus Unsupervised Models. *American Journal of Modeling and Optimization*, *7*(2), 42–48. https://doi.org/10.12691/ajmo-7-2-2

Zubaidi, I. B., & Abdullah, A. (2017). Developing a Digital Currency from an Islamic Perspective: Case of Blockchain Technology. *International Business Research*, *10*(11), 79. https://doi.org/10.5539/ibr.v10n11p79