International Journal of Computer Sciences and Engineering
Vol.**11**, Issue.**10**, pp.**37-44**, October **2023**
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

ISSN: 2347-2693 (E)

Research Paper

A Systematic Literature Review of Proof of Work and Proof of Activity: Privacy and Performance

Denis Wapukha Walumbe[1*], John Gichuki Ndia[2]

[1]School of Computing & Informatics, Gretsa University, Thika, Kenya
[2]School of Computing and Information Technology, Muranga University of Technology Muranga, Kenya

**Corresponding Author: dwapukha6@gmail.com*

Received: 02/Sept/2023; **Accepted**: 05/Oct/2023; **Published**: 31/Oct/2023. **DOI**: https://doi.org/10.26438/ijcse/v11i10.3744

Abstract: Censuses protocols is one of the blockchain framework architecture layer that is critical to the privacy of the technology. Therefore, any attempt to improve on privacy and Performance of blockchain technology will focus on the consensus layer. Understanding the consensus mechanism underly the layer is paramount. This paper focuses on two of the mainstream consensus mechanism; PoW and PoA with a comparison of the advantages and disadvantages of each of the consensus algorithm. The privacy of these algorithms has been evaluated based on the metrics selected from the existing literature. The paper used SLR research method. It consists of three activities: Planning, Execution, and reporting. The activities have several processes and steps that were undertaken. A total of 72 papers were selected for analysis and they were those published between 2019-2023. The review highlighted the wide range of application areas for PoW and PoA, including healthcare, IoT, and industry 4.0. However, PoW's popularity seemed to decline due to the introduction of faster and more secure blockchain algorithms. Privacy was a common theme, with decentralization, strong encryption, mutability, and scalability being key factors discussed in various studies. Overall, the systematic literature review Future Directions: Future research on PoW should focus on addressing concerns related to diminishing algorithm rewards and incentives for participants. Scholars should put effort in development of more hybrid algorithms that combine PoW with other blockchain algorithms to overcome challenges and gain benefits. In addition, the authors propose that more studies to focus on improving performance of PoA and explore on defining more decentralized algorithms.

Keywords: Proof of Work, Proof of Stake, Proof Action, Privacy, Blockchain, performance

1. Introduction

Censuses protocols is one of the blockchain framework architecture layer that is critical to the privacy of the technology. Therefore, any attempt to improve on privacy and Performance of blockchain technology will focus on the consensus layer. Understanding the consensus mechanism underly the layer is paramount[1]. There are four mainstream consensus algorithm: Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Proof of Activity (PoA). This paper focuses on two of the mainstream consensus mechanism; PoW and PoA [2]with a comparison of the advantages and disadvantages of each of the consensus algorithm. The privacy of these algorithms has been evaluated based on the metrics selected from the existing literature. The main contribution of the is privacy metrics, a review of the advantages and disadvantages of the two algorithms. This paper narrowed down the number of protocols in systematic literature review to two mainstream consensus algorithms: PoW and PoA. The paper has evaluated the advantages and disadvantages of these consensus algorithms[3]. Finally, the paper evaluated the privacy of these two techniques based on defined evaluation metrics.

2. Related Work

Consensus is a in blockchain is a process of giving guarantees all parties particular rules and regulations that should be observed by the participants on the network resulting to a trustless, secure and convenient blockchain technology[5]. There are several protocols used for different standards, it allows nodes in the network comply with the policies and regulations. Scholars such as Xiao et al. [3] provides a detailed review of the five components consensus protocol architecture and categorized the different levels of fault tolerance. The author explored the architecture on the basis of distributed systems and transaction processing with the blockchain technology[6]. The authors explained PoS classes of consensus algorithm.

Other scholars [7]–[9], in this paper they carried out survey research that offers detailed information on consensus protocols. The authors explored blockchain architecture by

dividing it into three groups. Blockchain was explored as a single layer and multi-layer-based architecture, interoperability-based architecture. After the analysis of the architecture, they pointed out the issues and possible solutions that Blockchain architecture faces. The article [1], [4]offered a description of consensus protocols PoW, PoS, DPoS, PBFT and Ripple. They looked at the characteristics and detailed some of the advantages of each protocol. The study by Mahmoud et al [10] described PBFT as the most popular consensus algorithm and discussed the need for large amount of resources by this algorithm. Wang and others came up with a new protocol called credit-delegated byzantine fault tolerance (CDBFT). It was a solution to the issues highlighted in the paper where credit was assigned on a new block[11]. The paper carried out simulations that lowered the overhead on communication and Performance improved.

The first reports of PoW were in early 1990s by Dwork and Naor but Nakamoto utilized this concept later in 2008 and gave it more breath in the blockchain technology [12]. The most used consensus algorithm is PoW. Financial institution and the application of cryptocurrencies is based on PoW where nodes on a network compete in creating a valid block by solving a puzzle. The puzzle forms a cryptographic contest among the nodes and one who solves first is rewarded. Nonce is a value assigned to all valid blocks. To protect the block, each miner should get a nonce value and all the block follows a specific threshold referred to as weight[13].

The miner that starts to solve the cryptographic puzzle gets the rights to build a new block. The process of mining is complex and it requires transaction fee that is computed by the service provider[14]. Apart from the transaction fee, there is a mining fee that is a reward given to the miner by the entire blockchain network. It is estimated that it takes ten minutes to create a block in Pow. To create a new block, too many processing and energy resources are used hence it is a challenge [15]. PoW suffers from several drawbacks as the paper will highlight at the end.

PoA (Proof of Activity) was designed to overcome challenges that PoW faced such as the lack of motivation to participate in mining after all the puzzles are solved. PoW becomes less relevant and attractive to miners when the mining fee is no longer offered but only transaction fees. The mining fee is very high and it is what makes miners work hard to solve the cryptographic puzzles[4], [16]. Miners will not be interested in participating in the process without the incentives equal to the resources used. The problem has been addressed by having PoW and PoS integrated[1]. The transaction fees is split between the miners and the validators and it promotes involvement of the nodes in the mining process. Therefore, PoA is as a result of the integration of PoW and PoS algorithms.

At the initial stages, PoA functions like ordinary PoW, where miners compete to solve the puzzle and get a unique number. A block is generated with all contents except for the payload[17]. The new created block is broadcasted to the network. The second stage is where a number of validators are selected. They are selected on the basis of the amount of cryptocurrency they have with the help of PoS algorithm. The blocks are validated and added to the blockchain by the stakeholder hence a valid block[18]. Once this is done, the block miners who mined the block and the validators referred to as stakeholder share the reward.

The paper is structured as follows. The next section presents a brief discussion on related literature on PoW and PoA[4]. Then SLR outline follows, an order of the activities for the SLR process, and discussion of the results and their implications. The threats to validity is discussed in the paper, the lessons gained in relation to carrying out the SLR and finally the future works.

3. Research Methods: SLR Outline

The paper used SLR research method. It consists of three activities: Planning, Execution, and reporting [5]. The activities have several processes and steps that were undertaken. The paper carried out planning that included allotting workload to different time period and relevant resources. It ensured that the researcher was able to interact and carry out review, come up with the procedure for review among others[19]. On the other hand, the execution activity had activities such as retrieving data, selection of the study, data extraction, data synthesis. The last activity was reporting that shows and makes sense of the results. The activities of SLR are described in details in the following section.

3.1 Planning the review

The activity of planning the review includes defining the research protocol, research questions and developing the search strategy, the criteria for inclusion and exclusion, and data extraction form.

3.2 Designing SLR Protocol

The protocol shows the steps taken in the process for the SLR study. The paper done in a pre-defined and structured manner that included the selection of the topic and asking questions for review, describing the population(s), intervention(s) of interest, comparisons and outcomes. The search criteria for the literature and the criteria for inclusion and exclusion. The paper has defined each of the protocol element in subsequent sections. The Protocol was designed as per the protocol developed by other SLR in the same area of consensus algorithm.

3.4 Research Question

the reasons for having the research questions was to determine the level of coverage of PoS and PoA algorithms research area. the motivation behind each question is tabulated below. The guided how the review was designed. There are three research questions that have motivated the study shown in table 1:

Table 1: Research Questions ad Motivations

Research questions	Motivation
RQ1: which type of characteristics of PoW and PoA are investigated by	To understand the different characteristics specific to each algorithm that have been researched

researchers?	
RQ2: which research methods are used in research on PoW and PoA?	To determine if the field has more basic or applied research to establish a gap for future research.
RQ3: Which metrics are used in research for PoW and PoA privacy and Performance?	To find out the metrics in research used in measuring PoW and PoA privacy and Performance.
RQ3: What are the suggestions for the future research PoW and PoA on privacy and Performance ?	To understand the research interests: which areas have been under-researched and which areas have been most researched. Aim is to advance the practices of research

3.5 Inclusion and Exclusion criteria

There are many collections of research studies to select from both electronic and library physical papers. The study search was limited to only electronic journals, conferences and workshops.

While there is rich content in additional materials in literature such as working papers, web pages, books, white papers, trade fair and magazine articles, these contents has not been included in the study and have not been subjected to review. The quality of these sources cannot be reliably established.

3.6 Search Engine Identification

The search engines used for the study were identified on the basis of the area of research and the research reputation of the publishers. There were four search engines identified.
IEEE Xplore www.ieeexplore.com
Google scholar www.scholar.google.com
Springer www.springerlink.com
Scopus www.scopus.com
String Refinement

Refinement of the string was to ensure that the results that generated by the search engines were relevant. One of the refinements was to ensure that the search results show popular papers and primary research papers. The following steps were used in refining the search terms

Defined the major terms
Identified alternative spellings, synonyms or related terms to the major terms
Looked for relevant keywords in selected papers
Used the Boolean OR to add alternative spellings, synonyms or related terms.
Used the Boolean AND to connect the major terms
The major terms for the search are “Proof of Activity” and “Proof of Work”. The alternative spelling, synonyms or terms related to the key terms are tabulated in table 2 below.

Table 2: Major Terms and alternative terms

Major terms	Alternative terms
Proof Stake	PoA or Proof of Activity
Proof of Work	PoW OR Proof of Work
Performance	Ability, adaptability, capability, competence · energy, expertise, productivity
Privacy	Privacy

The paper carried out several searches with Scopus database which helped in calibrating to fine tune the final search terms. The search was restricted to title and abstract in the relevant databases.

The specific search string used in the study was based on specific database being searched. The table 3 below shows the strings on scientific databases.

Table 3: Scholarly databases and search string definition

Database	Search String
Google Scholar	PoA AND PoW Performance and privacy -bitcoin [2019-2023]
Springer	[All: not bitcoin] AND [Publication Date: 01/01/2019 TO *)] PoA OR PoW AND privacy) AND Performance AND NOT bitcoin) within 2019-2023
IEEE Xplore Digital Library	((((PoW) OR PoA) AND privacy) AND Performance) NOT bitcoin Filters Applied: 2019-2023
Scopus	TITLE-ABS-KEY(“PoW” OR “PoA” AND “privacy” AND “Performance” AND NOT “bitcoin” AND PUBYEAR>2018 AND PUBYEAR<=2023

4. Research Procedure

The research carried out through use of the listed search engines for references and scientific publications. The main terms used were ‘Proof of Activity’, “Proof of Work” “Privacy” and “Performance”. The results for main term “Bitcoin”, and “cryptocurrency” were excluded. The paper applied paper restriction on basis of date of publication, limiting the existing articles since 2019.

There was increased publication of articles on the term “Proof of Work” and “blockchain” from 2019 which reached is maximum in 2020 December. The privacy and effectiveness dominated the search results in early 2020 to mid 2021 with the introduction of Proof of Activity. Although Proof of Stake was introduced way in 2012, it gained greater importance with the discussion of Performance and privacy issue in blockchain technology. The two terms PoA and PoW when combined gives more relevant information especially with the terms “privacy” and Performance” observed along.
The section presents screenshots of the search process.
The search for Google scholar, the filters, and the number of results shown.

4.1 Selection of Publications

We selected possibly pertinent journals that related to the main terms used in the searches. A sum of 120 journal articles were initially designated for inclusion in the systematic review. The journals and conferences where the journal were published was analyzed and extracted as show in below. This data is essential in knowing where most relevant publications are published hence knowing where to find additional scientific literature[17]. It also helps in knowing where previous scholars have published scientific work.

Table 4: Relevant Journals and publishers

Relevant Journals	Publishers
ACM computing Surveys	ACM
Computer & Security	Elsevier
Computer Networks	Elsevier
Future Generation Computer System	Elsevier
Procedia Computer Science	Elsevier
Sensors	MDPI
PLoS ONE	PLos ON
IEEE Access	IEEE

After the search was done, and initially the paper had a total of 124 publications that meet the search criteria used. Subsequently, the papers that had access for full reading were checked out of the selected papers. Those without full access were discarded. The next phase was to analyze each article with emphasizes on the title of the publication, the main terms and the abstract to ensure they meet the focus of the research in terms of privacy and Performances. There were some duplicate publications in the list (11) that were immediately excluded. Several databases was used to carry out bibliography hence the source of duplication in the document listing. Additionally, some paper got published as conference papers and then as an article hence duplication of the papers. Finally, the paper selected the publications that answered the research questions formulated in this study. The answers about the techniques used by PoA and PoW to improve on privacy and resistant to attacks through blockchain technology were considered. To end, a total of 72 publications are selected for information extraction, all articles were published from 2019.

4.2 Assess Studies

Concurrent process to that of data extraction is the quality assessment of the primary studies. The assessment is done as per contextualization, the relevance of the information offered and the link to the main terms of the study. This ensures that data extracted is quality and validated hence it serves as a reason for accepting or rejecting a publication.

4.3 Performance Snowballing

The snowballing phase [20] is the use of references from a publication or citations to find more publications, important in systematic literature search. Articles relating to the study were identified by looking at what current scholar with a relevant study cited or used in the reference list. A research paper in the collection had a link to others suggested by the tool hence they helped in looking into the articles.

4.4 Data extraction and Synthesis

Each paper was revised, for the abstract and the entire text, extracting information related to PoW and PoA techniques to implement privacy and Performances in each case. The papers selected were those discussing the techniques separately, both on same paper or those that had additional techniques not under investigation in this study. The information collected has been annotated for analysis later.
During the analysis of the information extracted, the focus was on privacy and Performance of PoW and PoA. on the other hand, the paper explored the characteristics of each mechanism to find how different elements of the techniques help in the privacy. Blockchain as a technology has wide range of application in real life. The paper took note of the real-life applications and focus on areas that require management o privacy and Performance.

The process of data extraction was designed to address the initial questions asked in the study (Q1-Q3). The aim was to understand studies that are looking into this aspects, current situation as well as offer conclusions of the work. The term privacy and Performance are related as shown in the fig. 2 below. Most of the studies analyzed explored both concepts. The other diagram fig.3 shows the relationship between PoW and PoA, it illustrates that the two terms are often considered together. However, there were some studies that explored the terms separately [1], [21]–[34]. We noted that most of the studies selected addressed the issues of privacy and Performance in both protocols.

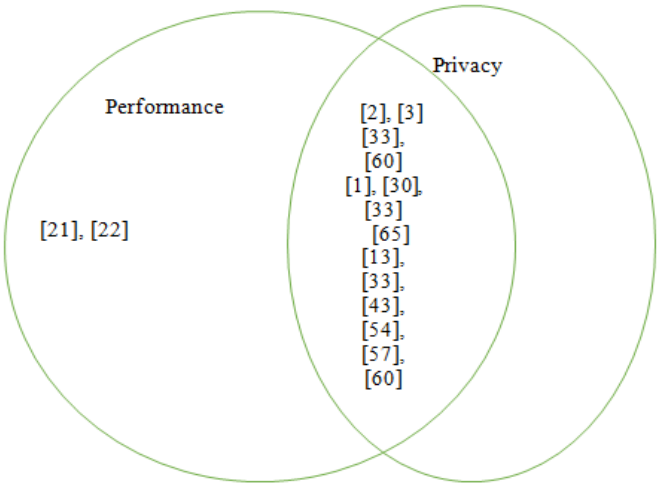

Figure 1 showing relationship between privacy and performance

5. Results and Discussion

The research findings are presented in this section. The aim of the review analysis is to address the research questions formulated. There were 124 found and 72 primary studies in the final selection. The selected studies were categorized as per the dimensions of the detailed scheme of the study.
Number of articles from databases

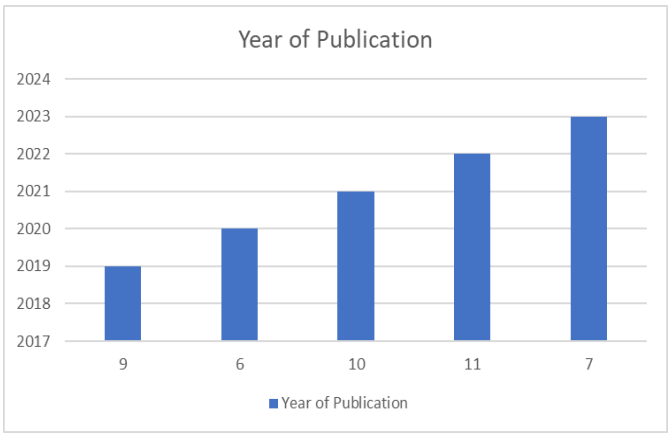

Chart 1 showing research papers selected per year of publication

Table 6 showing search results per each question

S. No	Database	Total results found			Primary selection	Final selection
		RQ1	RQ2	RQ3		
01	IEEE Xplore	13	14	9	36	23
02	Google scholar	16	12	8	36	15
03	Springer	9	8	7	21	19
04	Scopus	08	11	12	31	15
	TOTAL				124	72

Application domain
Proof of Work and Proof of activity are some of the popular algorithms used in blockchain technology. The first area was to look at the different areas of applications of the selected papers. The following are the results.

Healthcare: 38% of the articles selected focused on use of blockchain in health care systems. The main concepts were security and privacy of patient data. There were suggestions of the potential use of blockchain in small medical devices and remotely monitored medical devices [19], [22], [26], [27], [35]–[53].

IoT- the concept of Internet of Things was explored in many of the research papers. 20% of the work selected had application domain of IoT. Some of the articles that looked at healthcare also mentioned the IoT application[2], [8], [21], [28], [36], [43], [54]–[60].

Cryptocurrency – The main area of cryptocurrency is the use of PoW about 10%. There was an aspect of its application together with PoA in ensuring the system continues to be relevant beyond cryptocurrency system.
Industry 4.0- another set studies were specific in looking at how 5G network and the industry 5.0 technology[45], [61], [62].

RQ2: which research methods are used in research on PoW and PoA?
There were different research approach used in the primary researches. However, a high number of the research upto 80% of the primary study selected used simulation of the blockchain network to illustrate the concepts of privacy and Performance[1]–[3], [6], [12], [17], [19], [20], [30], [33], [45], [55], [56], [59], [63]. The work in [17] gives a more detail aspect of tools, language and platforms used to simulate the research.

Table 5 experiment tools used in primary studies

Platform	Algorithm	Programming language	Contributions
Eclipse	PoA, PoW	Java	Privacy and tolerance to attack
SimBlock	PoA	Python	Performance
Cooja Simulator	PoA and PoW	Solidity /JavaScript	Privacy
Etherueum	PoW	Solidity	Performance and privacy
Chainspace	PoA	Solidity	Privacy

RQ3: Which metrics are used in research for PoW and PoA privacy and Performance?
There were different metrics used to measure performance [11]. However, there was no specific tool for measuring privacy as it was described in terms of access, encryption, authentication and authorization [64]. The results show 70% of the articles that for PoW performance was measured as transaction per second, block size and number of nodes on a network. The same aspects of measure were used on PoA algorithm with large number of articles 80% using number of transactions per second as the main metrics for performance. Overall, Performance was assessed using different metrics, with transaction per second, block size, and number of nodes on a network being the primary measures for PoW's performance (70% of the articles). For PoA, the main performance metric used was the number of transactions per second, found in about 80% of the articles.

RQ3: What are the future of PoW and PoA privacy and performance.
There was a greater concern with the incentives required for the PoW to work. The concern was about the diminishing aspect the algorithm reward systems[64]. The reward is reduced at every math problem solved. To the end, there will be no reward hence no node would want to work. There are several proposal that scholars have suggested including hybrid the algorithm with other blockchain algorithm. The advantages of this algorithm can be used to gain benefit over other algorithm. In other words, PoW can be used to overcome the challenges of PoS when combined in a system.

On the aspect of decentralization and centralization, studies have suggested future work to see how more decentralized algorithms can be designed. The future work for PoA was mainly on its performance.

During the analysis of several studies, it has been established that different application areas have been explored in relation to PoW and PoA. They focused on different aspects of privacy and performance of the relevant algorithm. The areas of healthcare, IoT, industry 4.0, among others. It shows that blockchain technology has a wider areas of application. There were many publications in 2019-2021 on PoW then it started losing momentum. The trend can be associated with introduction of new blockchain algorithm that seemed to be faster and more secure.

Simulations studies were observed in the study at high number. It shows how performance is simulated and measured. However, different programming languages and platforms were used to run the simulations. The diversity of the tooling in simulation is important aspect to ensure that the researchers are not restricted to a specific tool and language. The experiments can be replicated in different environments.
Among the main terms analyzed in the studies are privacy and performance. The paper highlights that there was a common conclusion on privacy that blockchain technology offers privacy to data. The concept of decentralization, strong encryption, mutability and scalability were discussed in various studies as basis for privacy. The major aspects in comparison for the two protocols are in the table 6 below.

Table 6: Major comparison of PoW and PoA

	PoW	PoA
Type of blockchain	Public	Public
Accounting rights assignment	Computational power	Stake
Level of decentralization	High	High
Latency	10 min	1 min
Transaction per section TPS	>=7 TPS	>=300
Fault tolerance	49%	49%
Computing overhead	High	Medium
Security	Possible attacks 51%	Less prone 51% attack
References	[5,6,21,8,12]	[11,15,17,28]

6. Conclusion and future Works

The systematic literature review aimed to explore the application domains, research methods, metrics used, and future directions concerning Proof of Work (PoW) and Proof of Activity (PoA) algorithms in blockchain technology. The review covered selected papers and research articles on the subject, and the following key findings were observed:

1. Application Domain: The selected papers focused on various application domains of blockchain technology. Healthcare was the most prominent with 28% of articles discussing blockchain's use in health care systems, mainly concerning security and privacy of patient data. Internet of Things (IoT) was the next significant area with 20% of the work exploring its applications. Cryptocurrency was discussed in about 10% of the articles, mostly regarding PoW's application. Additionally, some studies examined Industry 4.0, specifically looking at the role of 5G networks and technology.
2. Research Methods: The primary research studies used various research approaches, with approximately 80% employing simulation of the blockchain network to illustrate privacy and performance concepts. Simulation tools like Eclipse, SimBlock, Cooja Simulator, Ethereum, and Chainspace were commonly used in these studies.
3. Performance was assessed using different metrics, with transaction per second, block size, and number of nodes on a network being the primary measures for PoW's performance (70% of the articles). For PoA, the main performance metric used was the number of transactions per second, found in about 80% of the articles.

In conclusion, the review highlighted the wide range of application areas for PoW and PoA, including healthcare, IoT, and industry 4.0. However, PoW's popularity seemed to decline due to the introduction of faster and more secure blockchain algorithms. Simulations played a crucial role in understanding and measuring performance, with diversity in tools and programming languages enabling better replication of experiments. Privacy was measured in terms of access, encryption, authentication, and authorization, but there was no specific tool dedicated to measuring privacy. Privacy was a common theme, with decentralization, strong encryption, mutability, and scalability being key factors discussed in various studies. Overall, the systematic literature review sheds light on the significance of PoW and PoA in blockchain technology, their applications, and the need for continued research to address challenges and explore new avenues for improvement.

Future Directions: Future Directions: Future research on PoW should focus on addressing concerns related to diminishing algorithm rewards and incentives for participants. Scholars should put effort in development of more hybrid algorithms that combine PoW with other blockchain algorithms to overcome challenges and gain benefits. In addition, the authors propose that more studies to focus on improving performance of PoA and explore on defining more decentralized algorithms.

Conflict of interest: None

Funding source: not funded

Authors Contribution: equal contribution

Acknowledgement
I would like to express my gratitude to God. I acknowledge the academic guidance of my supervisor Dr. John G. Ndia. I have learnt a great deal of PoW and PoA, and how to do systematic literature review. I would like to thank my family wife Bilha, Carlos, Princess and Adaiah for support during the research. I thank my Ph.D colleagues at Murang'a University of Technology for the good times during our studies and research presentations.

References

[1]. V. Neziri, I. Shabani, R. Dervishi, and B. Rexha, "Assuring Anonymity and Privacy in Electronic Voting with Distributed Technologies Based on Blockchain," Applied Sciences (Switzerland), Vol.**12**, No.**11, 2022**. doi: 10.3390/app12115477.

[2]. S. Wadhwa, S. Rani, Kavita, S. Verma, J. Shafi, and M. Wozniak, "Energy Efficient Consensus Approach of Blockchain for IoT Networks with Edge Computing," Sensors, Vol.**22**, No.**10**, **2022.** doi: 10.3390/s22103733.

[3]. S. Bouraga, "A taxonomy of blockchain consensus protocols: A survey and classification framework," Expert Syst Appl, Vol.**168**, **2021**. doi: 10.1016/j.eswa.2020.114384.

[4]. I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]," ACM SIGMETRICS Performance Evaluation Review, Vol.**42**, No.**3, 2014.**

[5]. B. Mi, Y. Weng, D. Huang, Y. Liu, and Y. Gan, "A novel PoW scheme implemented by probabilistic signature for blockchain," Computer Systems Science and Engineering, Vol.**39**, No.**2, 2021**. doi: 10.32604/csse.2021.017507.

[6]. C. Pu, A. Wall, I. Ahmed, and K. K. R. Choo, "SecureIoD: A Secure Data Collection and Storage Mechanism for Internet of Drones," in Proceedings - IEEE International Conference on Mobile Data Management, **2022**. doi: 10.1109/MDM55031.2022.00033.

[7]. [7] A. A. Laghari, A. A. Khan, R. Alkanhel, H. Elmannai, and S. Bourouis, "Lightweight-BIoV: Blockchain Distributed Ledger Technology (BDLT) for Internet of Vehicles (IoVs)," Electronics (Switzerland),Vol.12, No.**3, 2023**. doi:10.3390/electronics12030677.

[8]. C. W. Hsueh and C. T. Chin, "Toward Trusted IoT by General Proof-of-Work," Sensors, Vol.**23**, No.**1**, **2023.** doi: 10.3390/s23010015.

[9]. R. Xu and Y. Chen, "Fed-DDM: A Federated Ledgers based Framework for Hierarchical Decentralized Data Marketplaces," in Proceedings - International Conference on Computer Communications and Networks, ICCCN, **2021**. doi: 10.1109/ICCCN52240.2021.9522359.

[10]. H. H. M. Mahmoud, W. Wu, and Y. Wang, "Proof of learning: Two Novel Consensus mechanisms for data validation using Blockchain Technology in Water Distribution System," in 2022 27th International Conference on Automation and Computing: Smart Systems and Manufacturing, ICAC 2022, **2022**. doi: 10.1109/ICAC55051.2022.9911156.

[11]. K. Qian, Y. Liu, Y. Han, and K. Wang, "Performance Benchmarking and Optimization for IIoT-oriented Blockchain," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), **2021**. doi: 10.1007/978-3-030-68884-4_33.

[12]. S. Bouraga, "A taxonomy of blockchain consensus protocols: A survey and classification framework," Expert Syst Appl, Vol.**168**,

2021, doi: 10.1016/j.eswa.2020.114384.
[13]. T. Machacek, M. Biswal, and S. Misra, "Proof of X: Experimental insights on blockchain consensus algorithms in energy markets," in 2021 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference, ISGT 2021, **2021**. doi: 10.1109/ISGT49243.2021.9372194.
[14]. L. Shi, T. Wang, J. Li, S. Zhang, and S. Guo, "Pooling is Not Favorable: Decentralize Mining Power of PoW Blockchain Using Age-of-Work," IEEE Transactions on Cloud Computing, **2022**, doi: 10.1109/TCC.2022.3226496.
[15]. W. Lv, N. Wang, X. Xie, and Z. Hong, "A Classification-Based Blockchain Architecture for Smart Home with Hierarchical PoW Mechanism," Buildings, Vol.**12**, No.**9**, **2022**, doi: 10.3390/buildings12091321.
[16]. I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake," Cryptology ePrint Archive, Vol.**452**, No.**3**, **2014.**
[17]. X. Chen, K. Nguyen, and H. Sekiya, "On the Latency Performance in Private Blockchain Networks," IEEE Internet Things J, vol. 9, no. 19, 2022, doi: 10.1109/JIOT.2022.3165666.
[18]. A. Alrowaily, M. Alghamdi, I. Alkhazi, A. B. Hassanat, M. M. S. Arbab, and C. Z. Liu, "Modeling and Analysis of Proof-Based Strategies for Distributed Consensus in Blockchain-Based Peer-to-Peer Networks," Sustainability, vol. 15, no. 2, 2023, doi: 10.3390/su15021478.
[19]. S. Pandey, Vanshika, Anshul, and R. K. Dwivedi, "A Secure Design of Healthcare System with Blockchain and Internet of Things (IoT)," in IDCIoT 2023 - International Conference on Intelligent Data Communication Technologies and Internet of Things, Proceedings, 2023. doi: 10.1109/IDCIoT56793.2023.10053491.
[20]. S. Kaur, S. Chaturvedi, A. Sharma, and J. Kar, "A Research Survey on Applications of Consensus Protocols in Blockchain," Security and Communication Networks, vol. 2021. 2021. doi: 10.1155/2021/6693731.
[21]. [21] L. Xiong, T. Peng, F. Li, S. Zeng, and H. Wu, "Privacy-Preserving Authentication Scheme With Revocability for Multi-WSN in Industrial IoT," IEEE Syst J, vol. 17, no. 1, 2023, doi: 10.1109/JSYST.2022.3221959.
[22]. [22] H. Yang, J. Shen, J. Lu, T. Zhou, X. Xia, and S. Ji, "A Privacy-Preserving Data Transmission Scheme Based on Oblivious Transfer and Blockchain Technology in the Smart Healthcare," Security and Communication Networks, vol. 2021, 2021, doi: 10.1155/2021/5781354.
[23]. M. S. Jalali, A. Landman, and W. J. Gordon, "Telemedicine, privacy, and information security in the age of COVID-19," Journal of the American Medical Informatics Association, vol. 28, no. 3. Oxford University Press, pp.**671–672**, Mar. 01, **2021**. doi: 10.1093/jamia/ocaa310.
[24]. H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," Sustainable Cities and Society, Vol.**50**, **2019**. doi: 10.1016/j.scs.2019.101660.
[25]. N. Qamar, Y. Yang, A. Nadas, and Z. Liu, "Querying Medical Datasets while Preserving Privacy," in Procedia Computer Science, Elsevier B.V., pp.**324–331, 2016.** doi: 10.1016/j.procs.2016.09.049.
[26]. R. Seigel, S. T. Lashway, M. M. K. Stein, and C. J. Rundell, "Telehealth and digital health privacy regulations," in Diabetes Digital Health and Telehealth, **2022**. doi: 10.1016/B978-0-323-90557-2.00020-0.
[27]. M. AbdulRaheem, J. B. Awotunde, C. Chakraborty, E. A. Adeniyi, I. D. Oladipo, and A. K. Bhoi, "Security and privacy concerns in smart healthcare system," in Implementation of Smart Healthcare Systems using AI, IoT, and Blockchain, **2023**. doi: 10.1016/b978-0-323-91916-6.00002-3.
[28]. W. Liang and N. Ji, "Privacy challenges of IoT-based blockchain: a systematic review," Cluster Comput, Vol.**25**, No.**3**, **2022**, doi: 10.1007/s10586-021-03260-0.
[29]. E. R. Weitzman and M. Floyd, "Privacy and diabetes digital technologies and telehealth services," in Diabetes Digital Health and Telehealth, **2022**. doi: 10.1016/B978-0-323-90557-2.00011-X.
[30]. A. D. Dhass, S. Raj Anand, and R. Krishna, "Implementation of Blockchain-Based Security and Privacy in Energy Management," in Green Energy and Technology, **2021**. doi: 10.1007/978-3-030-64565-6_18.
[31]. W. Wang et al., "A privacy protection scheme for telemedicine diagnosis based on double blockchain," Journal of Information Security and Applications, Vol.**61**, **2021**. doi: 10.1016/j.jisa.2021.102845.
[32]. F. J. de Haro-Olmo, Á. J. Varela-Vaca, and J. A. Álvarez-Bermejo, "Blockchain from the perspective of privacy and anonymisation: A systematic literature review," Sensors (Switzerland), Vol.**20**, No.**24**, pp.**1–21**, Dec. **2020**, doi: 10.3390/s20247171.
[33]. A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K. K. R. Choo, "Blockchain-Enabled Authentication Handover with Efficient Privacy Protection in SDN-Based 5G Networks," IEEE Trans Netw Sci Eng, vol. 8, no. 2, 2021, doi: 10.1109/TNSE.2019.2937481.
[34]. H. A. Al Hamid, S. M. M. Rahman, M. Shamim Hossain, A. Almogren, and A. Alamri, "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility with Pairing-Based Cryptography," IEEE Access, vol. 5, 2017, doi: 10.1109/ACCESS.2017.2757844.
[35]. G. Capece and F. Lorenzi, "Blockchain and healthcare: Opportunities and prospects for the ehr," Sustainability (Switzerland), vol. 12, no. 22, 2020, doi: 10.3390/su12229693.
[36]. T. Frikha, A. Chaari, F. Chaabane, O. Cheikhrouhou, and A. Zaguia, "Healthcare and Fitness Data Management Using the IoT-Based Blockchain Platform," J Healthc Eng, vol. 2021, 2021, doi: 10.1155/2021/9978863.
[37]. D. T. Myran et al., "Physician Health Care Visits for Mental Health and Substance Use during the COVID-19 Pandemic in Ontario, Canada," JAMA Netw Open, vol. 5, no. 1, 2022, doi: 10.1001/jamanetworkopen.2021.43160.
[38]. K. Kumari and K. Saini, "Data handling & drug traceability: Blockchain meets healthcare to combat counterfeit drugs," International Journal of Scientific and Technology Research, vol. 9, no. 3, 2020.
[39]. S. Mbunya, C. Asirwa, and D. Felker, "Telemedicine: Bridging the Gap Between Rural and Urban Oncologic Healthcare in Kenya," J Glob Oncol, vol. 4, no. Supplement 2, 2018, doi: 10.1200/jgo.18.91500.
[40]. B. Yang and P. Y. Hsueh, "An socio-technical approach to securing health informatics," Eur J Epidemiol, vol. 31, 2016.
[41]. A. O. Almagrabi, R. Ali, D. Alghazzawi, A. AlBarakati, and T. Khurshaid, "Blockchain-as-a-Utility for Next-Generation Healthcare Internet of Things," Computers, Materials and Continua, vol. 68, no. 1, 2021, doi: 10.32604/cmc.2021.014753.
[42]. T. Ahmed, M. M. Al Aziz, and N. Mohammed, "De-identification of electronic health record using neural network," Sci Rep, vol. 10, no. 1, 2020, doi: 10.1038/s41598-020-75544-1.
[43]. K. Azbeg, O. Ouchetto, and S. Jai Andaloussi, "BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security," Egyptian Informatics Journal, vol. 23, no. 2, **2022**, doi: 10.1016/j.eij.2022.02.004.
[44]. P. Krebs and D. T. Duncan, "Health app use among US mobile phone owners: A national survey," JMIR mHealth and uHealth, Vol.**3**, No.**4, 2015**. doi: 10.2196/mhealth.4924.
[45]. S. Aggarwal, N. Kumar, M. Alhussein, and G. Muhammad, "Blockchain-Based UAV Path Planning for Healthcare 4.0: Current Challenges and the Way Ahead," IEEE Netw, Vol.**35**, No.**1**, **2021**, doi: 10.1109/MNET.011.2000069.
[46]. P. Esmaeilzadeh, "Use of AI-based tools for healthcare purposes: A survey study from consumers' perspectives," BMC Medical Informatics and Decision Making, Vol.**20**, No.**1**, **2020**. doi: 10.1186/s12911-020-01191-1.
[47]. K. Wac, A. T. van Halteren, R. G. A. Bults, and T. H. F. Broens, "Context-aware QoS provisioning in an m-health service platform," in International Journal of Internet Protocol Technology, **2007**. doi: 10.1504/IJIPT.2007.012373.

[48]. C. M. Chen, Z. Chen, S. Kumari, and M. C. Lin, "LAP-IoHT: A Lightweight Authentication Protocol for the Internet of Health Things," Sensors, Vol.**22**, No.**14**, **2022**. doi: 10.3390/s22145401.
[49]. C. G. Kamotho and F. Bukachi, "Telemedicine is an effective way to manage cardiovascular disease in rural Kenya and to achieve universal healthcare," Eur Heart J, Vol.**41**, no. Supplement_2, **2020**. doi: 10.1093/ehjci/ehaa946.3485.
[50]. S. Subha and P. Perumal, "An analysis of a secure communication for healthcare system using wearable devices based on elliptic curve cryptography," World Review of Science, Technology and Sustainable Development, Vol.**18**, No.**1**, **2022**. doi: 10.1504/wrstsd.2022.10042352.
[51]. P. Perumal and S. Subha, "An analysis of a secure communication for healthcare system using wearable devices based on elliptic curve cryptography," World Review of Science, Technology and Sustainable Development, Vol.**18**, No.**1**, **2022**, doi: 10.1504/WRSTSD.2022.119327.
[52]. K. Sowjanya, M. Dasgupta, and S. Ray, "An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems," in International Journal of Information Security, **2020**. doi: 10.1007/s10207-019-00464-9.
[53]. P. Esmaeilzadeh and T. Mirzaei, "Comparison of consumers' perspectives on different health information exchange (HIE) mechanisms: an experimental study," Int J Med Inform, Vol.**119**, **2018.** doi: 10.1016/j.ijmedinf.2018.08.007.
[54]. D. Puthal and S. P. Mohanty, "Proof of Authentication: IoT-Friendly Blockchains," IEEE Potentials, Vol.**38**, No.**1**, **2019**, doi: 10.1109/MPOT.2018.2850541.
[55]. Y. Su, K. Nguyen, and H. Sekiya, "Latency Evaluation in Ad-hoc IoT-Blockchain Network," in WSCE 2022 - 2022 5th World Symposium on Communication Engineering, **2022**. doi: 10.1109/WSCE56210.2022.9916023.
[56]. S. Alrubei, E. Ball, and J. Rigelsford, "Securing IoT-Blockchain Applications through Honesty-Based Distributed Proof of Authority Consensus Algorithm," in 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2021, **2021**. doi: 10.1109/CyberSA52016.2021.9478257.
[57]. A. Ali et al., "An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network," Sensors, Vol.**22**, No.**2**, **2022**, doi: 10.3390/s22020572.
[58]. G. Sagirlar, J. D. Sheehan, and E. Ragnoli, "On the design of co-operating blockchains for IoT," in Proceedings - 3rd International Conference on Information and Computer Technologies, ICICT 2020, **2020**. doi: 10.1109/ICICT50521.2020.00093.
[59]. S. M. Alrubei, E. Ball, and J. M. Rigelsford, "The Use of Blockchain to Support Distributed AI Implementation in IoT Systems," IEEE Internet Things J, Vol.**9**, No.**16**, **2022**, doi: 10.1109/JIOT.2021.3064176.
[60]. A. Hakiri and B. Dezfouli, "Towards a Blockchain-SDN Architecture for Secure and Trustworthy 5G Massive IoT Networks," in SDN-NFV Sec 2021 - Proceedings of the 2021 ACM International Workshop on Software Defined Networks and Network Function Virtualization Security, co-located with CODAYSPY 2021, **2021**. doi: 10.1145/3445968.3452090.
[61]. C. Rupa, D. Midhunchakkaravarthy, M. K. Hasan, H. Alhumyani, and R. A. Saeed, "Industry 5.0: Ethereum blockchain technology based DApp smart contract," Mathematical Biosciences and Engineering, Vol.**18**, No.**5**, **2021**, doi: 10.3934/MBE.2021349.
[62]. S. Shyam, S. J. Devaraj, K. Ezra, J. Delattre, and G. K. Lynus, "Design and implementation of UWB-based cyber-physical system for indoor localization in an industry environment," in Intelligent Edge Computing for Cyber Physical Applications, **2023**. doi: 10.1016/b978-0-323-99412-5.00010-1.
[63]. Z. Ullah, B. Raza, H. Shah, S. Khan, and A. Waheed, "Towards Blockchain-Based Secure Storage and Trusted Data Sharing Scheme for IoT Environment," IEEE Access, Vol.**10**, **2022**, doi: 10.1109/ACCESS.2022.3164081.
[64]. Y. Supreet, P. Vasudev, H. Pavitra, M. Naravani, and D. G. Narayan, "Performance Evaluation of Consensus Algorithms in Private Blockchain Networks," in Proceedings - 2020 International Conference on Advances in Computing, Communication and Materials, ICACCM 2020, **2020**. doi: 10.1109/ICACCM50413.2020.9213019.
[65]. N. Lasla, L. Al-Sahan, M. Abdallah, and M. Younis, "Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm," Computer Networks, Vol.**214**, **2022**, doi: 10.1016/j.comnet.2022.109118.

AUTHORS PROFILE

Mr. Denis Wapukha Walumbe-1 am a dedicated Computer Science Lecturer with over 13 years of experience in higher education. His expertise spans a wide range of technology and research domains, making him a versatile professional in the field. He is currently pursuing a Ph.D. in Information Technology at Murang'a University. With a Master of Science in Information Systems from Kisii University and a Bachelor of Science in Computer Science from Masinde Muliro University of Science and Technology, I have a strong academic foundation. I have not only an educator but also an active contributor to research. He has authored and co-authored papers published in international journals, addressing critical issues such as insider security system threats, Blockchain Technology and green IT.I have technical skills in programming languages, data modeling, data mining, and project management. He is a strong advocate for data-driven decision-making and is well-versed in various data science tools.

Dr. John Gichuki Ndia is a lecturer at Murang'a University of Technology, Kenya and the Dean of School of Computing and Information Technology. He has a PhD in Information Technology from Masinde Muliro University of Science and Technology, Kenya(2020). His Research interests include Software Engineering, and Computer Networks & Security. He is a Professional Member of Institute of Electrical and Electronics Engineers(IEEE) and the International Association of Engineers(IAENG).

