Lightweight Proof-of-Stake Models for Privacy-Preserving Telemedicine Systems: A Systematic Review

Denis Wapukha Walumbe
Department of Information Technology,
Murang'a University of Technology
Murang'a, Kenya
Email: dwapukha6 [AT] gmail.com

Gabriel Kamau
Department of Information Technology,
Murang'a University of Technology
Murang'a, Kenya
Email: gkamau [AT] mut.ace.ke

Jane Wanjiru Njuki
Department of Information Technology,
Murang'a University of Technology
Murang'a, Kenya
Email: jnjuki [AT] mut.ac.ke

Abstract---- **Proof of Stake (PoS) models are energy-efficient and require limited computational power. These features are critical in telemedicine environments, where resource-constrained devices must handle sensitive data securely. The growing need for auditable and privacy-preserving data storage in telemedicine underscores the importance of PoS models optimized for lightweight devices while complying with strict regulatory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA).This study was guided by two research questions: (i) Which PoS models are lightweight and suitable for telemedicine? and (ii) What features make lightweight PoS models effective for privacy and efficiency in telemedicine? To address these questions, a systematic literature review (SLR) guided by the PICOC framework was conducted to investigate lightweight PoS models that can enhance privacy in telemedicine systems. Out of 2,394 papers studies screened, 55 were included in the analysis. The findings identified Algorand, Ouroboros Praos, Tendermint, Nxt, and Casper CBC as promising candidates. Key enabling features included lightweight voting mechanisms, such as Byzantine Agreement protocols and Verifiable Random Functions, as well as cryptographic techniques like symmetric encryption and multiparty computation. Performance metrics evaluated included latency, throughput, energy efficiency, and battery consumption, with Grey Relational Analysis ranking Algorand highest due to its low latency, high throughput, and minimal energy consumption.**

Keywords-- Proof of Stake (PoS), Telemedicine Systems, Lightweight Models, Data Privacy, Voting Mechanisms, Data Encryption

I. INTRODUCTION

Privacy in the processing of patient data has been emphasized by several regulators including General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA). These regulations emphasize enforcement of privacy and data protection in health information systems[1]. Ensuring privacy in telemedicine, however, presents unique challenges due to the reliance on small, resource-constrained devices with limited storage and computational power. telemedicine requires solutions that provide comparable privacy on resource-constrained devices [2].

Proof of Stake (PoS), first introduced in 2011 by blockchain researchers seeking to improve the efficiency of digital currency systems offers potential in this context. Developed as an improvement over the Bitcoin Proof of Work (PoW) protocol, PoS reduces the computational overhead and energy waste inherent in PoW [3], [4]. Since its introduction, PoS has expanded beyond cryptocurrency into diverse fields such as finance, healthcare, administration, and agriculture [5]. In telemedicine, however, the direct application of PoS remains challenging because most protocols were designed for high-capacity systems and remain too computationally demanding for low-power devices. Extant literature indicates Byzantine Agreement protocol and verifiable random functions to achieve efficient consensus, while others leverage multiparty computation and symmetric key cryptography to enhance data security under constrained conditions [6] , [7], [8].

Recent studies propose lightweight PoS models for low-powered telemedicine devices, incorporating voting and encryption mechanisms to ensure confidentiality and verifiability [9], [10]. Scholars have focused on features of PoS models that make them suitable for lightweight environments[11]. Voting mechanisms, which determine how validators are elected, are crucial features explored. Algorand's Byzantine Agreement mechanism [12] offers low computational requirements while ensuring privacy and decentralization. Another property explored is verifiable random functions (VRF) for validator selection and Ouroboros Praos that helps in balancing fairness and efficiency [13].

Nevertheless, several challenges remain, including consensus throughput, resource consumption, transaction latency, and block storage efficiency. Moreover, literature lacks a systematic analysis of PoS models tailored to the specific privacy and efficiency requirements of telemedicine environments. This paper reviews lightweight Proof of Stake (PoS) models for enhancing privacy in telemedicine, focusing on suitability for resource-constrained devices. It highlights key mechanisms, evaluation metrics, and research gaps, offering directions for optimizing PoS in telemedicine applications. The study was guided by two research questions:

i.) Which PoS models are considered lightweight and suitable for telemedicine?
ii.) What features make lightweight PoS models effective for privacy and efficiency in telemedicine**?**

II. METHODS

The study used the PICOC framework. The protocol shows the steps taken in carrying out the study. PICOC was adopted because it explicitly incorporates **C**ontext, which is essential for analyzing lightweight PoS mechanisms within telemedicine systems running on resource-constrained devices indicated in Table 1 and Figure 1.

Table 1: PICOC framework

P (Population/Problem)	Blockchain-based telemedicine systems.
I (Intervention)	Lightweight PoS models suited for resource-constrained devices**.**
C (Comparison)	Lightweight models versus traditional PoS mechanisms.
O (Outcome)	Effectiveness measured by privacy, energy efficiency, and system performance.
C (Context)	Privacy-preserving telemedicine within regulated healthcare environments.

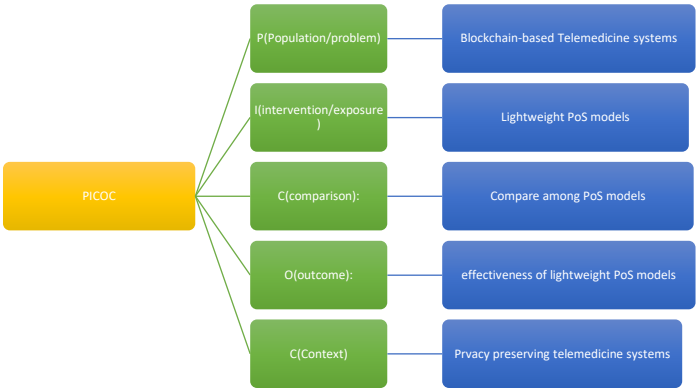


Figure 1: PICOC Framework in relation to Lightweight PoS models

The method consists of three main activities: Planning, Execution, and reporting. [15], [16]. Each activity has several processes and steps that were carried out. At planning, tasks were scheduled and relevant resources were assigned. The activities and procedures carried out in this section were documented to ensure the validity of the study. The execution activity had several processes; retrieving data, selection of the study, data extraction, and data synthesis. Reporting of the results is the last activity. It answers the research questions and presents findings from the entire process. [16]. The following are the search steps used in SLR.

2.1 Planning the Review

The study carried out this activity by defining the research protocol, and the research questions that guided the study objective, and developing the research strategy. Afterward, the study defined the criteria for inclusion and exclusion as well as how data was extracted.

2.1.1 Information Sources

Peer reviewed journal databases were used in sourcing published papers. The information sources included:

a. Scopus (www.scopus.com)
b. IEEE Xplore
c. ScienceDirect
d. PubMed

2.1.2 Inclusion and exclusion criteria

There is an increasing interest in the area of blockchain technology as well as telemedicine systems. Out of the many

publications, some were not relevant to the study. It was possible to identify relevant publications through inclusion and exclusion criteria. Only primary studies relating to the thesis were included.[15]. Therefore, this study was limited to electronic journals, conference and workshop papers.
On the exclusion criteria, journal articles that were based on secondary data were excluded. Although books, web pages, working papers, trade fairs, and magazine articles offer rich content, they were excluded from this thesis. The studies have not been subjected to peer review hence the validity of the content cannot be verified. Therefore, the quality of the sources and authority of the paper cannot be reliably established.

2.2 Data extraction and synthesis
The process of data extraction and synthesis is important for SLR. This section presents how it was carried out.
2.2.1 Defined Keywords
The keywords were extracted from the research questions. They are listed below:

1. Data Privacy
2. Telemedicine Systems
3. Privacy Issues/Challenges
4. PoS Models (Proof of Stake Models)
5. Enhancing Data Privacy

2.2.2 Search engine identification

The search engines were identified based on specific areas of research, and the reputation of the publishers. They included:

a. Scopus (www.scopus.com)
b. IEEE Xplore
c. ScienceDirect
d. PubMed

2.2.3 Defining search string
The keywords were used to form a search string using the OR and AND connectors. Words were concatenated with the defined synonyms with the connectors. The following shows how the search strings were defined for different search engines.
(Information Privacy OR Data Protection OR Confidentiality of Information OR Privacy of Personal Data OR Data Confidentiality OR Personal Data Protection) AND (Staking Models OR Stake-Based Consensus Models OR Proof of Stake Algorithms OR Staking Consensus Protocols OR Stake Validation Systems) AND (Telehealth Systems OR Remote Healthcare Systems OR Telemedical Platforms OR E-Health Systems OR Digital Health Systems OR Virtual Care Systems OR Telecare Platforms OR Remote Patient Monitoring Systems).

2.2.3.1 String Refinement

String refinement was carried out on various databases to ensure that the results generated were relevant. The filters on the selected search engines were used to ensure that the search results were recent, relevant to the study area and they were primary research studies. The refinement of the string was done on a case-by-case basis where some keywords or abstract were analyzed on relevance.
2.2.3.2 Search String Execution
Once the process of search string was defined, it was used on each of the search engines. The search strings used were kept in the research note document to ensure consistency in all the searches. The search findings were exported to the Mendeley reference management tool.
2.3 Download and store search results.
The following section shows several search results carried out from different databases.
The search in the PubMed database for instance as shown in Figures 2 , 3, and 4



Figure 2: PubMed first search results

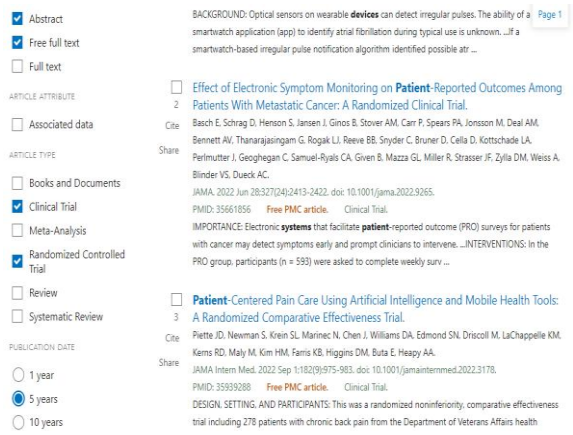


Figure 3 PubMed refined the search with inclusion criteria

Initial search is depicted in Figure 4 depict the initial search that applied to papers under year of 5 years, abstract and full text should be available and they should be primary studies.

2.3.1 IEEE Xplore search

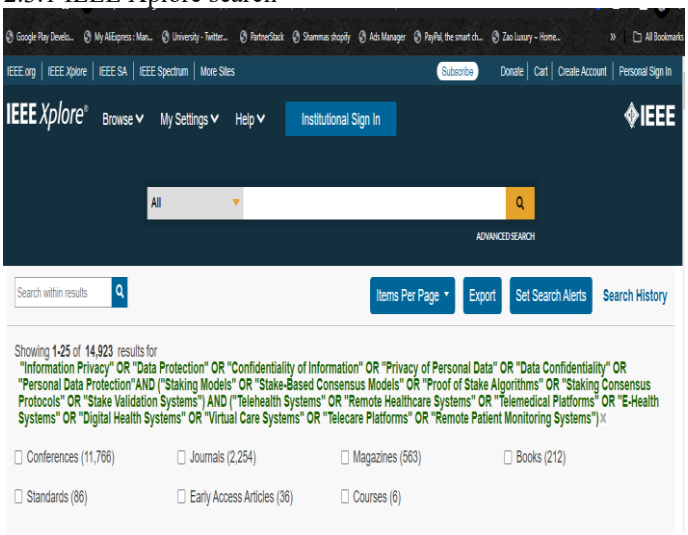


Figure 4: initial IEEE Xplore search results

The search with the search strings defined gave an output of 14,923 files that included books, courses, magazines, and conference papers. Since they were part of the exclusion criteria, the searchers were excluded. More filters were applied to the data as indicated in Figure 5.

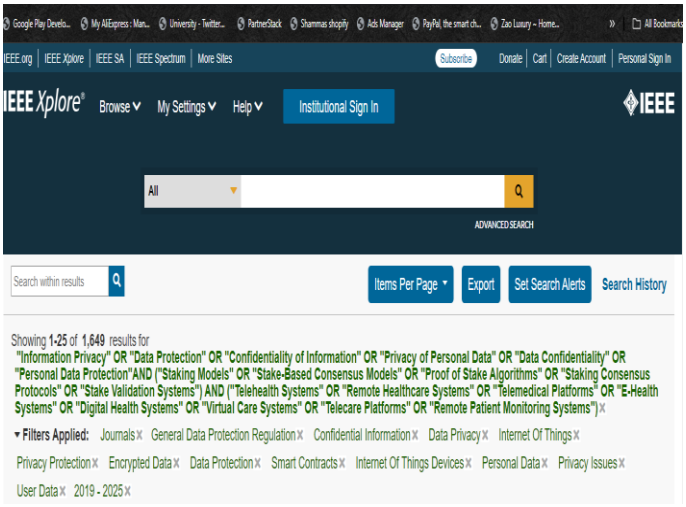


Figure 5: IEEE Xplore filtered search

After applying the filters for publications within 5 years and other filters such as keywords, the search total was 1,649. The files were downloaded in Excel. The download included the abstract for further screening.

2.2.2 Snowball search

To expand on the search of the papers, research keywords were used to look for graphs of related papers. Research Rabbit tool was used to graph map the research articles as indicated in Figure 6.

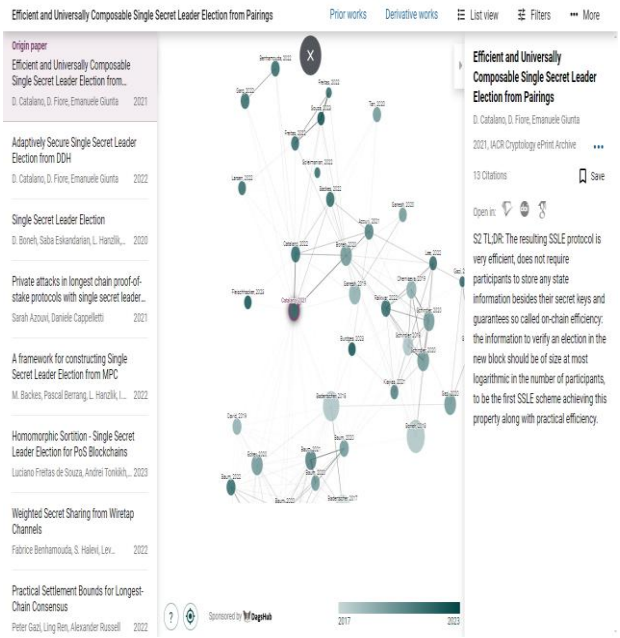


Figure 6: Snowballing on related studies for more refined results

2.2.3 Checking for Duplicates

The Mendeley research tool was used to detect and remove duplicate in exhibited in Figure 7 and Figure 8

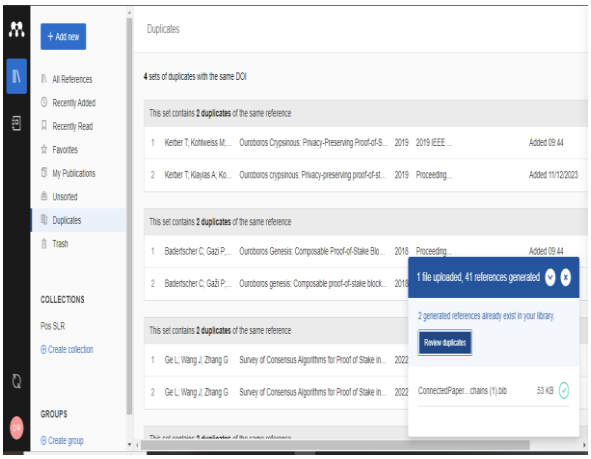


Figure 7: Mendeley research tool for the detection of duplicates

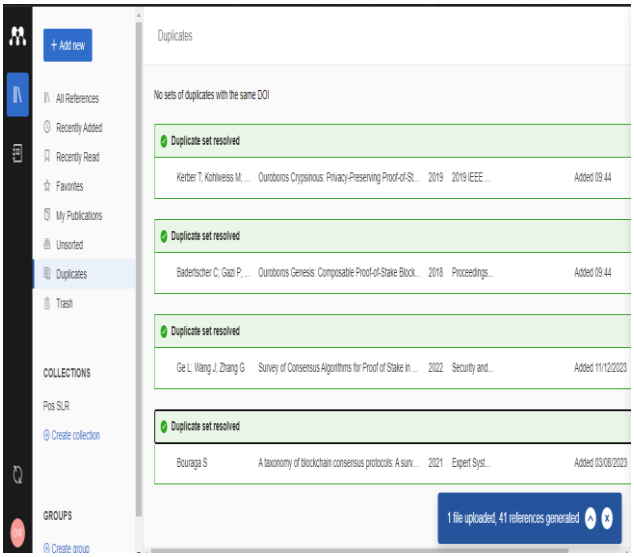


Figure 8 removed duplicates in research references

2.4 Selection of papers

The process of paper section is outlined below.

2.4.1 Selection of the papers- first stage [by title and abstract]

The research objective was to classify proof of Stake (PoS) models used in telemedicine. At this first stage, the papers selected were based on their titles and abstracts to ensure that they were relevant to the research objective. The titles and abstracts were examined to identify studies that discussed PoS, telemedicine systems, and data privacy mechanisms in healthcare. The criteria for inclusion of the papers were:

- Research articles that explicitly mentioned proof of stake models.
- Research studies that focused on telemedicine or healthcare technology
- Related studies on data privacy in telemedicine systems.
- Papers that were published between 2019 to 2024 in peer-reviewed journals as per defined criteria

During the initial search, the following results were realized:

Table 2: Initial Search Results

Search Engine	**Results**
- Scopus	- 400 papers
- IEEE Xplore	- 1649 papers
- ScienceDirect	- 100 papers
- PubMed	- 245
Total papers on initial[refined] Search	- **2,394**

Out of the 2,394 in Table 2 research papers in the initial search results, those that did not align with the scope of the study or explored other blockchain models such as Proof of Work were excluded. In the end, the number of studies was narrowed. The studies that were irrelevant based on title and abstract alone were filtered at this stage. The outcome are exhibited in Table 3:

Table 3: Stage One Selection Results

Search Engine	**Included papers after stage one**
- Scopus	- 120
- IEEE Xplore	- 300
- ScienceDirect	- 40
- PubMed	- 60
Total Papers after Stage One	- **526**

2.4.2 Selection of papers -second stage [by introduction and conclusion]

In the second stage, papers selected in the first stage were further examined by reading the introduction and conclusion sections of 520 papers. The objective was to confirm the relevance of the studies to the focus of the research on the classification of PoS models in telemedicine systems. The researcher examined the introduction section to establish

whether the research problem, objectives, and background were related to PoS and telemedicine. The conclusion was assessed on its contributions and findings, to ensure that they offer insights into the adoption, design, implementation, or improvement of PoS models in healthcare systems. Studies were excluded if:

- The research did not address the context of PoS in a healthcare environment
- The conclusions did not offer significant findings that relate to telemedicine
- The paper focused on generic blockchain models without specific relevance to PoS

The goal of this section was to ensure that at this stage, the remaining papers offered substantial and relevant discussions that aligned with the research objectives. The outcome results are in Table 4.

Table 4: Selected papers after stage two

Search Engine	Included papers after stage two
- Scopus	- 40
- IEEE Xplore	- 90
- ScienceDirect	- 25
- PubMed	- 20
Total Papers after Stage Two	- **175**

2.4.3 Selection of papers third stage- [complete reading and quality checklist]
At this stage, 175 papers remained for the final stage review. The remaining papers were fully interrogated and evaluated for their quality and depth. Based on the study-defined inclusion criteria, the papers were assessed whether they met the methodological and context requirements needed for inclusion. The activities in this stage included assessing the paper on:
- *Relevance*: Does the paper specifically address PoS models in telemedicine systems?

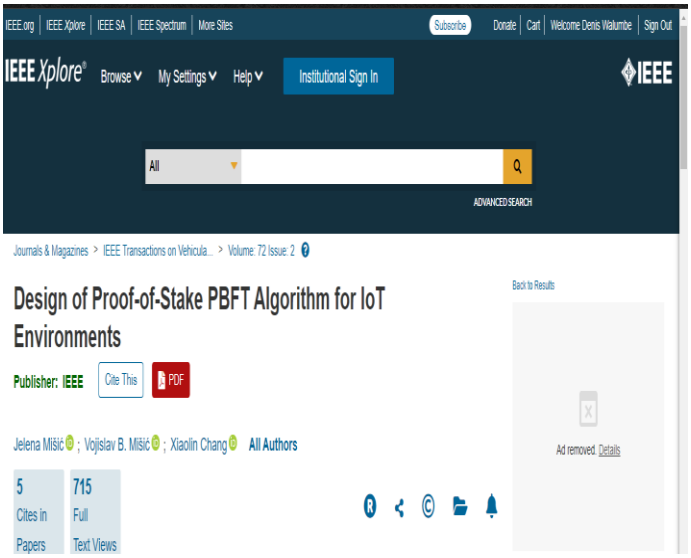


Figure 9: Checking for relevance and context of papers

- *Methodology*: does the study clearly define research methodology and apply it appropriately?
- *Findings*: does the paper give significant contributions to understanding the role of PoS models in enhancing data privacy in telemedicine?
- *Clarity*: is the study well-written, with appropriate definitions, objectives, and results?
- Peer-reviewed: is the paper published in reputable research database, peer-reviewed journals? This is shown in Table 5.

Table 5 Selected Papers after Stage Three

Search Engine	Included papers after stage three
- Scopus	- 15
- IEEE Xplore	- 25
- ScienceDirect	- 10
- PubMed	- 5
Total Papers	- **55**

Papers that did not meet the research inclusion criteria were excluded at this stage. The remaining studies consisted of high-quality, relevant research offering meaningful insights into PoS models in telemedicine systems. **Figure 10** shows a flow diagram summarizing the selection process, which included identification of records, removal of duplicates, screening

based on inclusion criteria, and final selection of high-quality, relevant studies.

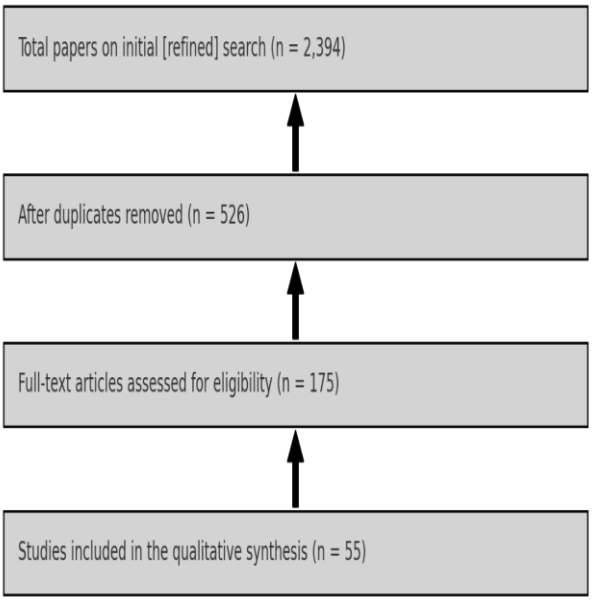


Figure 10 Summary of Search Process

III. RESULTS AND DISCUSSION

This section presents and discusses the results for PoS models for enhancing data privacy in telemedicine systems organized by the research questions: RQ1, the voting mechanisms that make PoS models lightweight; and RQ2, the data encryption techniques used in PoS models.

3.1 RQ1: *What PoS models are considered lightweight?*

The literature identifies Algorand, Ouroboros Praos, Tendermint, NXT, and CBC (Chain-based Consensus) as the main PoS models considered lightweight. Among these, Algorand (42%), Ouroboros Praos (26%), and NXT (14%) were the most frequently studied. Scholars focused mainly on voting mechanisms and data encryption techniques as lightweight features, while aspects such as storage and architecture were mentioned less often and generally within the broader blockchain context. Notably, Algorand's Byzantine Agreement and Ouroboros's Verifiable Random Functions (VRFs) were frequently highlighted for their efficiency on low-power devices.

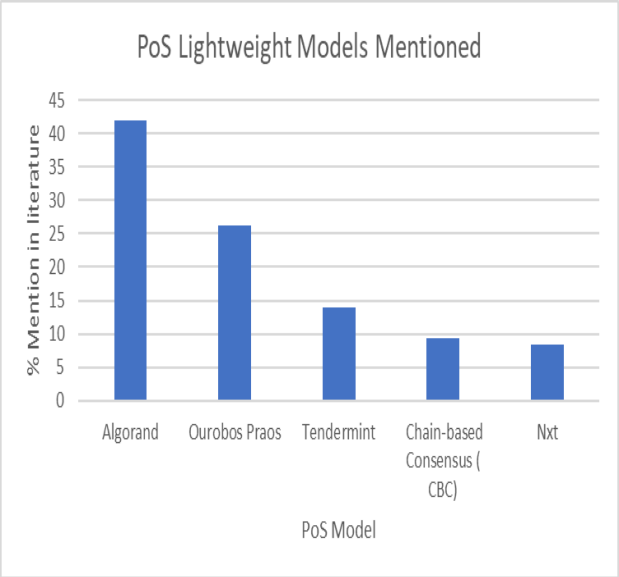


Figure 11 PoS models considered Lightweight

Lightweight PoS models were commonly described in terms of low computational demand, reduced network delays, high throughput capacity, and low energy consumption. Some studies also examined battery drain and transaction costs per

block as additional indicators of suitability for resource-constrained telemedicine systems.

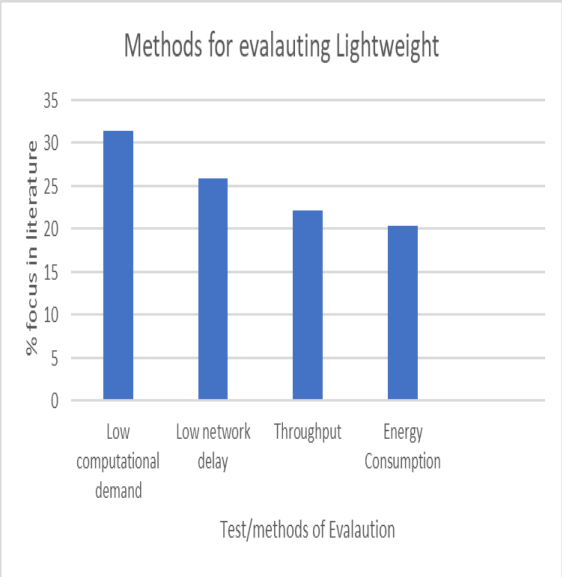


Figure 12: How Lightweight is Evaluated

There were 34 authors that used the term low computation demand in describing a lightweight PoS model. Low network delays were mentioned by 28 authors. There were 24 authors mentioning the throughput capacity of the model in consideration of lightweight. Only 22 authors mentioned energy consumption.

Majority of the literature published in the PoS models used processing time (PT) of a block, latency L, block creation rate (BCR), transactions per second (TPS), energy efficiency (EE) and battery drain time (BDT) for performance of lightweight PoS models[17]. From the selected literature, the average of the performance metrics for different PoS models is presented in Table 6. The values depend on the network conditions, and configurations.

Table 6 Performance Measures for PoS Models

Metric	**Algorand**	**Ouroboros Praos**	**Tendermint**	**Nxt**	**CBC (Chain-based Consensus)**
Processing Time	~4-5	~20-30 second	~1-2 seconds	~10-20 second	~15-30 seconds
Latency	~1-2 seconds	~5-10 seconds	~1 second	~5-10 seconds	~5-10 seconds
Block Creation Rate	~5 blocks per second	~1 block every 20-30 seconds	~1 block per second	~1 block every 10-20 seconds	~1 block every 15-30 seconds
Transactions Per Second (TPS)	~1,000-5,000 TPS	~100-500 TPS	~1,000 TPS	~50-100 TPS	~100-500 TPS
Energy Efficiency	~0.5-1 kWh per block	~1-2 kWh per block	~1-1.5 kWh per block	~1-2 kWh per block	~1-2 kWh per block
Battery Drain Test	~Low (<5% per hour)	~Moderate (5-10% per hour)	~Moderate (<5% per hour)	~Moderate (5-10% per hour)	~Moderate (5-10% per hour)

From Table 6, the following inferences are made:

Algorand performs well with high throughput of approximately 5 blocks per second, it is optimized for low latency. It has a competitive processing time and TPS.

Ouroboros Praos has high latency and processing times

Tendermint offers low latency and high TPS with fast finality

Nxt has moderate TPS and latency but simple and suitable for less demanding application.

These outcomes present each PoS model with the potential of being used in telemedicine systems. It presents a challenge on selecting which is the most suitable approach to implement. There is need to find an approach that will help in selecting or recommending the most suitable lightweight PoS model for use in telemedicine systems.

3.2 RQ2: *What are the features of lightweight PoS Models?*
The lightweight nature of PoS models arises from four main features: storage approach, architecture, consensus algorithm (voting mechanism), and cryptography technique. These features represent functional characteristics that determine how efficiently a PoS model operates under resource-constrained environments. Scholars consistently discussed these four as the core functional units of lightweight PoS models.

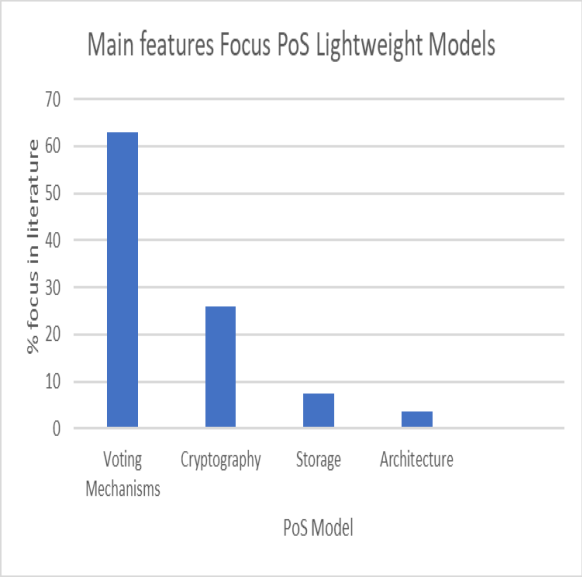


Figure 12: Main Features of Lightweight PoS models

There was a 63% focus on voting mechanisms and 26% of the studies explored data encryption within the literature. Studies using simulation were predominant (60%), highlighting the need for more real-world testing in lightweight telemedicine applications[19], [20]. Consensus algorithm is mainly about voting mechanisms, time and trust in selecting the validators and blocks added to the chain. For this paper, the focus was on storage, architecture, voting mechanism and cryptography approach used in lightweight PoS model.

3.2.1 Storage

The storage is an important feature for lightweight PoS models because telemedicine systems do not have large storage facilities. The scholars focused on the size of the ledgers and the amount of data that each node retains[21]. Other aspects that were explored include pruning, data compression and shading. Understanding storage management in devices with limited storage helps with how much data can be stored on the devices.

3.2.2 Architecture

Architecture, according to the authors, referred to the design of the blockchain system in relation to node layout [21]. Scholars did not give a lot of attention to this concept with assumption of portability of the protocol across architecture.

3.2.3 Voting Mechanisms

This section presents the results on voting mechanisms of some of the PoS models identified from the literature about lightweight devices. Overall Table 7 shows features from the five models were explored.

The comparison of voting mechanisms across PoS models is summarized in Table 7.

Table 7: Voting Mechanisms, Measures, and Limitations

Model	**Voting Mechanism**	**Key Features**	**Limitations/Remarks**	**Sources**
Algorand	Randomized Byzantine Agreement	Designed for speed and energy efficiency, suitable for low-power devices like telemedicine systems	None specified	[16]
Ouroboros Praos	Cardano blockchain	Uses Cardano blockchain, provides secure and verifiable voting mechanisms	None specified	[17], [27]
Tendermint	Round-Robin Validation Rotation	Focused on speed and efficiency; requires further	Limited information on achieving lightweight optimizations	[17], [27]

		exploration to make the mechanism lightweight		
Casper CBC	Validator Rotation	Enhances scalability while preserving resource efficiency	Proposed protocol, limited real-world deployment details	[29]
NXT	Randomized Block Creator Selection	Early PoS variant; designed for environments with limited computational and storage capacity	Suitable for minimal resource use but lacks advanced modern optimizations	[31], [32], [33]

The selection of participating nodes and validators comprises the voting mechanism. It is a key factor in achieving computational efficiency, and hence suitability of PoS models for lightweight devices such as telemedicine systems. The consensus mechanism must strike a balance between data privacy and resource requirements. The balance is critical when it comes to devices with limited processing power and energy.

Although there are other novel proposed PoS models for lightweight, the study focused on generic PoS lightweight models. It is because they have not been tested with real world data but at simulation level only. Algorand was the most mentioned PoS lightweight model among the scholars[14]. Other PoS lightweight models found in literature were; Ouroboros Praos, Tendermint, Nxt and CBC (Chain-based Consensus). Therefore, the focus was on these models in terms of their features and how they are measured in relation to PoS lightweight models.

Algorand uses the Byzantine Agreement (BA) election mechanism as a voting mechanism. The mechanism selects validators at random, demanding minimal computational power and time from each node. The aspect of randomness is used to achieve fairness, and reduce energy consumption, consequently making Algorand well-suited for light for lightweight systems. However, as discussed by [12], although the model is efficient, its reliance on all nodes for consensus presents a challenge in a telemedicine system where some nodes might be occasionally disconnected.

3.2.4 Cryptography

Cryptography is a critical feature for ensuring data integrity, confidentiality, and efficiency in lightweight PoS models. As shown in Table 8, secure but computationally simple methods are preferred to minimize energy use and storage overhead. A desirable lightweight approach is one that balances security with minimal computational complexity. For example, Algorand employs Pure PoS cryptography, enabling quick consensus and reduced resource consumption. However, because several components of this method are patented, adoption, modification, and further improvement by the broader research community are limited.

Table 8: Encryption Methods, Features, and Limitations

Model	**Encryption Method**	**Key Features**	**Limitations**
Algorand	Pure PoS cryptography	Quick consensus, reduced computational resources	Patented, limiting adoption, modification, and improvement
Ouroboros Praos	Secure Multiparty Computation (SMPC)	Focuses on secure data sharing in decentralized systems	Increased communication overhead. Because of the command-line programming usability is difficult
Tendermint (Ignite Consensus)	Station-to-station protocol Symmetric Key	Efficient, secure, quick consensus, and reduced	Vulnerable to a Man-In-The-Middle attack. Limited

	Cryptography	resource consumption; suitable for limited networks	scalability compared to other solutions such as Algorand
Casper CBC	Hash-Based Encryption (Block hashing Merkle trees)	Potential for lightweight computational systems	No known deployment or application in telemedicine Encryption is not primary focus
Nxt	Advanced Encryption Standard (AES)	Open-source licenses available for academic purposes	Restricted to academic use only

HIPAA and GDPR provide guidelines on data minimizing, data integrity and confidentiality, accountability and transparency. One of the features of a lightweight system is ability to collect and transmit minimal data; that only which is required[10]. Secure voting mechanisms and encryption data among different PoS models as discussed presents data integrity and confidentiality. On the aspect of accountability, PoS models are inherently transparent with transaction logs that provides accountability at each level.

3.4 PoS Features and Metrics

The features and metrics of lightweight PoS models present an association. Latency is a measure of speed of block finality and consensus agreement which measures voting mechanism of the model. Block creation is an indicator of frequency of proposed block in consensus, it impacts the architecture on throughput and scalability. Block creation rates also indicate how storage needs will be handled in a network. Cryptography influences storage, architecture and data privacy. The privacy of messages on the network depends on the type of cryptography used. The summarized table for the metrics and features is shown in Table 9.

Table 9 Features and Metrics of Lightweight PoS Model

Features of lightweight PoS model	**Metrics**
Voting mechanism	Processing time, latency, block creation rates, TPS, energy efficiency, battery drain
Cryptography	Cryptographic proof of sizes
Architecture	Processing time, latency, energy efficiency, block creation rate
Storage	Block creation rate, TPS

From table 9, focusing on voting mechanism, and cryptography is sufficient in addressing the key aspects of lightweight features and privacy without need to explore storage and architecture. Voting mechanism directly determines the computational and network efficiency of PoS models. Therefore, low computational demand, low network delays and energy efficiency are concepts that voting mechanism addresses. The concepts are also measured in relation to architecture.

Whereas lightweight PoS models focuses on minimizing resource usage, privacy cannot be compromised hence the need for cryptography that ensures the balance. Efficient cryptographic techniques are desired for lightweight models in securing privacy during transactions and communication between nodes[22], [23]. Additionally, an efficient cryptographic system size of signatures and proof hence minimizing storage requirements. There is minimal data overhead in transaction validation for some cryptographic techniques[24]. Privacy and reducing computation and communication overheads is the priority of lightweight PoS models. These priorities can be achieved independently of particular architecture.

3.5 Validation of the Results

The method used for validation of the results is referred to as Grey Relational Analysis (GRA) for algorithm ranking. It is a multi-objective optimization technique applied in decision making problems that are complex with various factors to consider.

The following steps as proposed by proposed by Professor Deng Julong in 1982[33], [34] were followed in computing GRA:

- Extra matric by generating data as per average literature PoS model performance
- Grey normalization

- Determine grey relational coefficient
- Calculating grey relational grade (GRG)

Step 1 generation of data

The data in Table 10 are extracted using equation (1) as X_{data}

$$X_{data} = \begin{matrix} x_{11} & x_{12} & \cdot & x_{1n} \\ x_{22} & x_{22} & \cdot & x_{2n} \\ x_{m1} & x_{m2} & \cdot & x_{mn} \end{matrix} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Where *m* is type of PoS model and *n* is the performance measures

Table 10 Grey Relational Analysis Results

Metric	Algorand	Ouroboros Praos	Tendermint	Nxt	CBC
Processing Time (s)	4.5	25	1.5	15	22.5
Latency (s)	1.5	7.5	1	7.5	7.5
Block Creation Rate (blocks per second)	5	0.04	1	0.07	0.04
Transactions Per Second TPS	3000	300	1000	75	300
Energy Efficiency (kWh)	0.75	1.5	1.25	1.5	1.5
Battery Drain Test (%per hour)	4	7.5	4	7.5	7.5

Step 2: Normalize data

The data set is normalized as X_i (j) where (0≤x_i (j) by using the following equation (2) to reduce the variability.

$$X_i(j) = \frac{x_{(j)} - min\, x_{i(j)}}{max\, x_{(j)}(j) - min\, x_{(j)}(j)} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

where, i=1,2,….m; j=1,2…n.

the inverted matrix is used where lower values are better such as battery drain, processing time, and latency

Step 3 Calculating grey relational coefficients. The results are shown in Tables 11, 12 and Figure 13.

Table 11: Calculating Grey Relational Coefficients

PoS Model	GRG
Algorand	0.9439
Tendermint	0.7055
Nxt	0.3557
CBC (Chain-based Consensus)	0.3406
Ouroboros Praos	0.3363

Table 12 presents the Grey Relational Grades (GRG) and corresponding rankings of the evaluated lightweight Proof of Stake (PoS) models, summarizing their relative performance based on selected metrics such as latency, throughput, energy efficiency, and battery drain

Table 12: Grey Relational Grades and Ranking of PoS Models

Metric	Algorand	Ouroboros Praos	Tendermint	Nxt	CBC
Processing Time (GRC)	0.789	0.333	1.000	0.530	0.360
Latency (GRC)	0.714	0.333	1.000	0.333	0.333
Block Creation Rate (GRC)	1.000	0.333	0.385	0.335	0.333
TPS (GRC)	1.000	0.358	0.412	0.333	0.358
Energy Efficiency (GRC)	1.000	0.333	0.385	0.333	0.333
Battery Drain Test (GRC)	1.000	0.333	1.000	0.333	0.333
Average GRG	0.917	0.337	0.697	0.366	0.342

Factors such as high number of blocks generated per second and low battery drain can be attributed to Algorand being ranked highest.

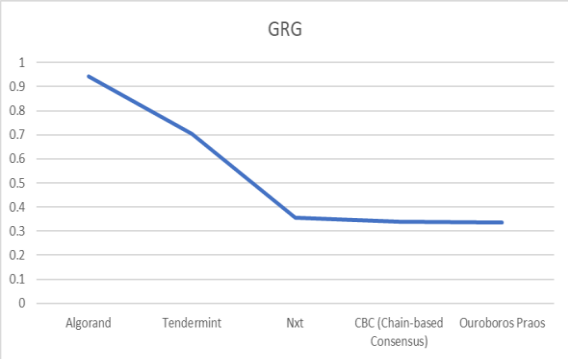


Figure 13 GRG Value for PoS Performance Measures

The GRA results (Table 11, Figure 14) show that Algorand ranks highest (GRG = 0.9439) due to its low latency, minimal battery drain, and high throughput, making it the most suitable for lightweight telemedicine systems. Tendermint performs moderately well, while NXT, CBC, and Ouroboros Praos rank lower because of higher energy demands and slower performance. This validates Algorand as the most efficient lightweight PoS option for privacy-preserving telemedicine applications.

IV. CONCLUSION

This study analyzed lightweight Proof of Stake (PoS) models and their suitability for telemedicine systems. The findings show that Algorand and NXT are the most suitable models, as they balance efficient voting mechanisms and encryption with relatively low computational cost. In contrast, CBC Casper and Ouroboros Praos introduce stronger privacy measures but at the expense of higher computational overhead, making them less practical for ultra-lightweight telemedicine devices.

In reviewing the features of Proof of Stake (PoS) models, reducing computational demands and privacy are the priority for lightweight models. There is need to find a balance between two aspects. Looking at the four features; voting mechanism, architecture, cryptography and storage, two carries more weight because they address the priority areas for lightweight PoS models. Voting mechanism and cryptography are the areas that more weight should be put in realizing a better lightweight PoS model as per the validation results. Therefore, the question is what could be done to improve on algorand's Byzantine agreement protocol and its data encryption technique to make it more suitable for telemedicine systems.

4.1 Validity

To ensure content validity, the study used established framework PICOC framework for conducting systematic literature review. The framework validates that the review covers the scope by following recognized protocols. Construct validity was strengthened through triangulation, drawing on multiple independent sources to confirm consistency of themes and conclusions.

4.2 Recommendations

i. Incorporate lightweight voting mechanism: use byzantine agreement protocol PoS algorithm with asynchronous communication that reduces latency and improves efficiency in telemedicine systems where network conditions may vary.
ii. Utilizing privacy-preserving encryption: privacy-preserving encryption techniques such as Cryptographic sortition and zero-knowledge proofs could be explored and incorporated in PoS models for systems that require high level of privacy like healthcare.
iii. Lightweight consensus for telemedicine: future work should explore optimizing PoS models for lightweight devices, for energy efficiency, reduced computational load, and low communication overheard, critical for telemedicine systems.

The recommendations above suggest that future PoS-based systems for telemedicine should adopt lightweight and fair voting mechanisms combined with vigorous encryption to balance between privacy, and performance.

4.3 Future Work

Future research will focus on developing a lightweight PoS model that combines Byzantine Agreement (BA) protocol with cryptographic sortition to improve privacy and efficiency in telemedicine systems. Special attention will be given to optimizing reward redistribution to reduce energy consumption and enhance finality.

While BA and cryptographic sortition show strong potential, challenges remain in minimizing latency during validation and managing computational overhead. Addressing these issues through simulations and prototype implementations will help refine the mechanisms for lightweight telemedicine devices. Moreso, BA and Cryptographic sortition provide promising solution, practical implementation in telemedicine systems demands addressing challenges like lowering latency during validation and managing computational overhead. The next phase of the research would be to refine these mechanisms through simulations to ensure they are efficient for lightweight devices without compromising on data privacy, and system performance.

Eventually, the proposed approach can significantly improve blockchain applications in healthcare by contributing to privacy-preserving and efficient consensus mechanisms for telemedicine systems. Beyond telemedicine, the contribution may also inspire blockchain adoption in other resource-constrained sectors, such as agriculture and IoT.

V. REFERENCES

[1] C. Baum, B. David, and T. Frederiksen, "P2DEX: Privacy-Preserving Decentralized Cryptocurrency Exchange," *IACR Cryptol. ePrint Arch.*, vol. 2021, p. 283, 2021, doi: 10.1007/978-3-030-78372-3_7.

[2] L. Freitas *et al.*, "Homomorphic Sortition – Secret Leader Election for PoS Blockchains," 2022, [Online]. Available: https://www.semanticscholar.org/paper/3c770a39032f597c01ac543fa97199da47681e10

[3] X. Li, W. Wu, and T. Chen, "Blockchain-Driven Privacy-Preserving Contact-Tracing Framework in Pandemics," *IEEE Trans Comput Soc Syst*, vol. 11, no. 3, 2024, doi: 10.1109/TCSS.2024.3351191.

[4] 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.

[5] S. Siddiqui and S. Gujar, "QuickSync: A Quickly Synchronizing PoS-Based Blockchain Protocol," *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, vol. null, pp. 1–2, 2020, doi: 10.1109/ICBC56567.2023.10174928.

[6] M. Kaur, M. Z. Khan, S. Gupta, A. Noorwali, C. Chakraborty, and S. K. Pani, "MBCP: Performance Analysis of Large Scale Mainstream Blockchain Consensus Protocols," *IEEE Access*, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3085187.

[7] A. Kiayias, C. Moore, S. Quader, and A. Russell, "Efficient Random Beacons with Adaptive Security for Ungrindable Blockchains," *IACR Cryptol. ePrint Arch.*, vol. 2021, p. 1698, 2021, [Online]. Available: https://www.semanticscholar.org/paper/876f595f6384ef813408592e1118dd87d2c8a7d1

[8] P. Schindler, A. Judmayer, N. Stifter, and E. Weippl, "HydRand: Practical Continuous Distributed Randomness," *IACR Cryptol. ePrint Arch.*, vol. 2018, p. 319, 2018, [Online]. Available: https://www.semanticscholar.org/paper/b837abafc6b45978533072913a79a93fb246408e

[9] F. Valovich, "Investcoin: A System for Privacy-Preserving Investments," *ArXiv*, vol. abs/1703.01284, p. null, 2017, [Online]. Available: https://www.semanticscholar.org/paper/ddadf1858de6a15ba52d837a8562f3b39a328f08

[10] C. Ganesh, C. Orlandi, and D. Tschudi, "Proof-of-Stake Protocols for Privacy-Aware Blockchains," *IACR Cryptol. ePrint Arch.*, vol. 2018, p. 1105, 2019, doi: 10.1007/978-3-030-17653-2_23.

[11] F. Valovich, "Investcoin: A System for Privacy-Preserving Investments," *ArXiv*, vol. abs/1703.01284, p. null, 2017, [Online]. Available: https://www.semanticscholar.org/paper/ddadf1858de6a15ba52d837a8562f3b39a328f08

[12] M. Conti, A. Gangwal, and M. Todero, "Blockchain Trilemma Solver Algorand has Dilemma over Undecidable Messages," *Proceedings of the 14th International Conference on Availability, Reliability and Security*, vol. null, p. null, 2019, doi: 10.1145/3339252.3339255.

[13] O. Adeniyi, A. S. Sadiq, P. Pillai, M. A. Taheir, and O. Kaiwartya, "Proactive Self-Healing Approaches in Mobile Edge Computing: A Systematic Literature Review," 2023. doi: 10.3390/computers12030063.

[14] 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.

[15] A. Carrera-Rivera, W. Ochoa, F. Larrinaga, and G. Lasa, "How-to conduct a systematic literature review: A quick guide for computer science research," *MethodsX*, vol. 9, 2022, doi: 10.1016/j.mex.2022.101895.

[16] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering - A systematic literature review," 2009. doi: 10.1016/j.infsof.2008.09.009.

[17] P. Hegde and P. K. R. Maddikunta, "Secure PBFT Consensus-Based Lightweight Blockchain for Healthcare Application," *Applied Sciences (Switzerland)*, vol. 13, no. 6, 2023, doi: 10.3390/app13063757.

[18] J. Wang, X. Lin, Y. Wu, and J. Wu, "Blockchain-Enabled Lightweight Fine-Grained Searchable Knowledge Sharing for Intelligent IoT," *IEEE Internet Things J*, vol. 10, no. 24, 2023, doi: 10.1109/JIOT.2023.3306606.

[19] H. U. Kumar and R. Prasad, "Algorand: A Better Distributed Ledger," in *1st IEEE International Conference on Advances in Information Technology, ICAIT 2019 - Proceedings*, 2019. doi: 10.1109/ICAIT47043.2019.8987305.

[20] L. Spadafora *et al.*, "Blockchain technology in Cardiovascular Medicine: a glance to the future? results from a social media survey and future perspectives," *Minerva Cardiology and Angiology*, vol. 72, no. 1, 2024, doi: 10.23736/S2724-5683.23.06457-8.

[21] A. G. Chandini and P. I. Basarkod, "A Robust Blockchain Architecture for Electronic Health Data using Efficient Lightweight Encryption Model with Re-Encryption

Scheme," in *IEEE International Conference on Data Science and Information System, ICDSIS 2022*, 2022. doi: 10.1109/ICDSIS55133.2022.9915902.

[22] T. Kerber, M. Kohlweiss, A. Kiayias, and V. Zikas, "Ouroboros Crypsinous: Privacy-Preserving Proof-of-Stake," *2019 IEEE Symposium on Security and Privacy (SP)*, vol. null, pp. 157–174, 2019, doi: 10.1109/SP.2019.00063.

[23] 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," 2019. doi: 10.1016/j.scs.2019.101660.

[24] K. Qian, J. Liu, and F. Tsui, "Decoupling metrics for services composition," in *Proceedings - 5th IEEE/ACIS Int. Conf. on Comput. and Info. Sci., ICIS 2006. In conjunction with 1st IEEE/ACIS, Int. Workshop Component-Based Software Eng., Softw. Archi. and Reuse, COMSAR 2006*, 2006. doi: 10.1109/ICIS-COMSAR.2006.30.

[25] I. M. Al-Joboury and E. H. Al-Hemiary, "CONSENSUS ALGORITHMS BASED BLOCKCHAIN OF THINGS FOR DISTRIBUTED HEALTHCARE," *Iraqi Journal of Information & Communications Technology*, vol. 3, no. 4, 2020, doi: 10.31987/ijict.3.4.116.

[26] C. Badertscher, P. Gazi, A. Kiayias, A. Russell, and V. Zikas, "Ouroboros Genesis: Composable Proof-of-Stake Blockchains with Dynamic Availability," *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, vol. null, p. null, 2018, doi: 10.1145/3243734.3243848.

[27] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol," 2017, doi: 10.1007/978-3-319-63688-7_12.

[28] L. Beltrando, M. Potop-Butucaru, and J. Alfaro, "TenderTee: Increasing the Resilience of Tendermint by using Trusted Environments," in *ACM International Conference Proceeding Series*, 2023. doi: 10.1145/3571306.3571394.

[29] R. Nakamura, T. Jimba, and D. Harz, "Refinement and verification of CBC casper," in *Proceedings - 2019 Crypto Valley Conference on Blockchain Technology, CVCBT 2019*, 2019. doi: 10.1109/CVCBT.2019.00008.

[30] E. Li, T. Serbanuta, D. Diaconescu, V. Zamfir, and G. Rosu, "Formalizing Correct-by-Construction Casper in Coq," in *IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2020*, 2020. doi: 10.1109/ICBC48266.2020.9169468.

[31] I. E. Mazurok, Y. Y. Leonchyk, and T. Y. Kornylova, "PROOF-OF-GREED APPROACH IN THE NXT CONSENSUS," *Applied Aspects of Information Technology*, vol. 2, no. 2, 2019, doi: 10.15276/aait.02.2019.6.

[32] W. Zhao, "On Nxt Proof of Stake Algorithm: A Simulation Study," *IEEE Trans Dependable Secure Comput*, vol. 20, no. 4, 2023, doi: 10.1109/TDSC.2022.3193092.

[33] Y. Kuo, T. Yang, and G. W. Huang, "The use of grey relational analysis in solving multiple attribute decision-making problems," *Comput Ind Eng*, vol. 55, no. 1, 2008, doi: 10.1016/j.cie.2007.12.002.

[34] D. Deng, T. Li, Z. Huang, H. Jiang, S. Yang, and Y. Zhang, "Multi-response optimization of laser cladding for TiC particle reinforced Fe matrix composite based on Taguchi method and grey relational analysis," *Opt Laser Technol*, vol. 153, 2022, doi: 10.1016/j.optlastec.2022.108259.