Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 17 No. 23 (2023) | OPEN ACCESS

https://doi.org/10.3991/ijim.v17i23.45257

PAPER

A Review of Blockchain-Based E-Voting Systems: Comparative Analysis and Findings

Rabia Fatih(✉), Sara Arezki, Taoufiq Gadi

Faculty of Sciences and Techniques, Mathematics, Computer Science and Engineering Sciences Laboratory, Hassan first University of Settat, Settat, Morocco

r.fatih@uhp.ac.ma

ABSTRACT

The emergence of blockchain has ushered in a significant transformation in information systems research. Blockchain's key pillars such as decentralization, immutability, and transparency have paved the path for extensive exploration in various research domains. This particular study is focused on electronic voting, aiming to improve voting procedures by making better use of the benefits offered by blockchain technology. Through a comprehensive review of existing literature, we highlight the potential benefits of blockchain-based electronic voting systems such as transparency, security, and efficiency. However, several challenges, such as scalability, personal data confidentiality, and ensuring robust identity verification, persist. Addressing these issues is necessary to unlock the full potential of blockchain-based electronic voting systems, thereby fostering the development of trustworthy election systems in the future.

KEYWORDS

blockchain, e-voting, decentralization, electronic voting, consensus

1 INTRODUCTION

As technology continues to revolutionize every facet of human existence, electronic voting methods have become the subject of many extensive study and debate in recent years. There have been several problems with the conventional ways of voting and tallying results, including security breaches, a lack of transparency, and logistical inefficiencies [1]. A promising solution lies in the incorporation of blockchain technology in electronic voting systems. The decentralized and transparent nature of blockchain has the potential to significantly transform the voting process, leading to more reliable voting systems.

In today's technologically dependent world, reliable and efficient electronic voting methods are more important than ever. Researchers, legislators, and technologists

Fatih, R., Arezki, S., Gadi, T. (2023). A Review of Blockchain-Based E-Voting Systems: Comparative Analysis and Findings. *International Journal of Interactive Mobile Technologies (iJIM)*, 17(23), pp. 49–67. https://doi.org/10.3991/ijim.v17i23.45257

Article submitted 2023-09-05. Revision uploaded 2023-10-05. Final acceptance 2023-10-05.

© 2023 by the authors of this article. Published under CC-BY.

have paid close attention to blockchain-based electronic voting systems because of their intrinsic qualities that overcome the drawbacks of conventional voting methods. These features include cryptographic security, decentralization, immutability, and transparency [2]. However, before blockchain-based electronic voting systems can be widely used, they need to be thoroughly analyzed and evaluated to determine their benefits, drawbacks, and real-world consequences.

The purpose of this article is to do a thorough investigation of blockchain-based electronic voting systems and to compare and contrast them. Through a review of related works, we want to add to the expanding body of information and understanding around this developing technology. This review provides researchers, policymakers, and practitioners with valuable insights into the current state of research and the potential implications for real-world implementation of blockchain-based electronic voting systems by systematically analyzing the strengths, limitations, and challenges associated with such systems.

The motive of this review paper is to analyze the current research on blockchain-based electronic voting systems and synthesize the results in order to spot patterns, gaps, and potential directions for further study. To achieve this goal, we set out to fill the void of a recent and thorough study by conducting a detailed comparison of various approaches, methods, and results in the area. Our goal is to add to the conversation about the future of secure and transparent voting mechanisms by compiling and analyzing existing knowledge about the benefits and drawbacks of using blockchain technology in electronic voting systems.

The remainder of the paper will start with an introduction to the topic under consideration, followed by an exploration of blockchain technology. The third section will elaborate on the literature review methodology, while the fourth part will delve into the presentation of the findings, then the discussion in the fifth part. Finally, the concluding section will provide an overarching summary and conclusion of the paper.

2 BLOCKCHAIN BACKGROUND

A blockchain is a distributed ledger that is shared by all the nodes of a computer network. It serves as a digital database for the storage of data [3].

The blockchain is constituted of blocks that are added to the chain in a linear order at systematic intervals. However, the timestamp, transaction, and hash are present in all blockchain implementations. The data in the blocks varies on the blockchain network. The cryptographic hash of the preceding block is contained in each new block. Since every piece of information in a hash is generated automatically, it is impossible to alter any of its components. Each new block in this situation strengthens the security of the entire blockchain and the verification of the previous block. The blockchain becomes more secure and dependable as there are more blocks added to the chain as Figure 1 shows.

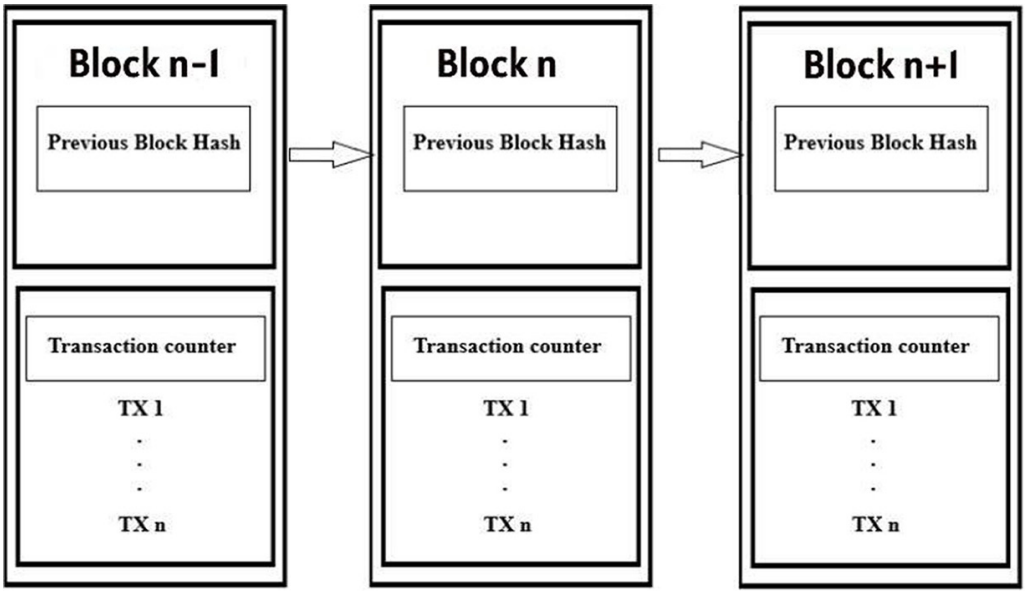

Fig. 1. Blockchain structure

2.1 Blockchain network types

The option of whether to use public, private, or consortium blockchain is critical since it has a direct impact on the governance and operation of a blockchain-based system. Depending on the level of transparency and control sought, businesses can use a public blockchain for open participation, a private blockchain for controlled access, or a consortium blockchain for a hybrid of the two. This classification emphasizes blockchain technology's adaptability, allowing for bespoke solutions across a wide range of industries. Table 1 effectively summarizes the fundamental distinctions between the three types of blockchains: public, private, and consortium in terms of management, consensus, participant access, immutability, transaction speed, and efficiency [4], [5].

Table 1. Blockchain types

Property	Public	Private	Consortium
Management	Decentralized management	One organization	Multiple organization
Consensus determination	All miners	Organization participating	Selected miners
Participants	Permissionless	Permissioned	Permissioned
Immutability	Almost impossible to tamper	Controlled and could be tampered	Could be tampered
Transaction duration	Long	Short	Short
Efficiency	Low	High	High

1. Public Blockchain: A completely decentralized, power-free blockchain, public blockchain has no central authority. The blockchain's secondary components may be updated by anyone, and anyone can take part in the approval or publication of new blocks. Its content is available to all subscribers. Publishing new blocks on the public blockchain necessitates doing several calculations to solve difficulties or keeping one's own coin for an extended period of time. Each transaction in the block is accompanied by a transaction fee as a reward to the node for releasing the new block. This might motivate nodes to take part in consensus. At the

same time, it can effectively stop hackers from attacking the public blockchain due to the higher cost of altering with transaction information.

2. Private Blockchain: Every node in a private blockchain is a known member of an organization, in contrast to public blockchain. A private blockchain is a database set aside by one institution to regulate the sharing of information between various divisions or people. Both cryptocurrencies and transaction fees are not necessary.
3. Consortium Blockchain: Also called a federated blockchain, it incorporates features of both private and public blockchains, making it similar to a hybrid blockchain. The ways in which many people inside an organization use a decentralized network together, however, are not uniform. The risks associated with having a single party run the network on a private blockchain are eliminated with a consortium blockchain, which mostly functions as a private blockchain with restricted access to a certain group.

In a consortium blockchain, consensus procedures are managed by nodes that have already been established. A validator node is responsible for initiating, receiving, and validating transactions. Transactions can be sent to and received from any member node.

2.2 Pillars of blockchain technology

1. Decentralization: While we are aware of the weaknesses of a condensed system, which is employed in a conventional financed transfer system, we can only comprehend the need for a decentralized system [6]. The client-server paradigm and banks are two instances of centralized systems where the bank acts similar to the primary authority and manages all aspects of transaction processing. In order to overcome these restrictions, the concept of a separate system is put out, in which information is used to store, record, and synchronize transactions at multiple nodes. Every node in a separate system is able to carry out data-related transactions. Administered networks, digital signatures, and encryption/decryption methods based on the security field all helped to build blockchain technology. Peer-to-peer networks, where each node might possess a duplicate of the whole information in the chain of blocks, are used in decentralized systems.
2. Transparency: Blockchain activities are typically not encrypted. The hash of the preceding block is stored in the current block. Blockchain uses the encryption method, which in the end secures the data. As a result, this feature authorizes blockchain technology to preserve transparency and privacy across all peer connection nodes in the network. A node's identity is concealed by using complicated cryptographic characters that are both unique and alphanumeric, and it is often only represented by its public address.
3. Immutability: Immutability is a core component of blockchain technology, guaranteeing that once data is uploaded to the chain, it remains permanent and resistant to any adjustments. Cryptographic hash functions, which produce one-of-a-kind strings of a certain length from the given input data, provide this crucial functionality. As a consequence, the hash value would change drastically if the original data was altered in any way, providing an obvious red flag to consumers about possible data manipulation. In the context of electronic voting, immutability guarantees that votes cannot be changed or erased after being recorded on the blockchain. It is nearly difficult to alter the content of a vote without altering the whole succeeding chain of blocks since each vote is securely tied to a unique cryptographic hash. Voters are reassured that their ballots will not be tampered with thanks to this feature, increasing faith in the voting process.

3 RESEARCH METHODOLOGY

In this study, a systematic literature review (SLR) is conducted to determine how blockchain technology can be used to cast ballots. Its goal is to locate pertinent research articles so that it can utilize them to compare various blockchain-based voting solutions.

3.1 Overview systematic literature review

A systematic literature review (SLR) is a technique for carrying out derivative research that makes use of a prearranged approach to pinpoint, evaluate, as well as interpret existing study pertinent to a given subject, issue, or phenomenon [7]. There are three phases to the process: organizing the review, carrying it out, and reporting it.

Instituting research questions and determining a review process are two objectives of the organization and review stage. In essence, that stage introduces the study's whole breadth. Generating a search plan, using it to gather as many pertinent main researches as you can, besides evaluating them, are the central tasks involved in executing the review phase. A selection of pertinent articles that can be analyzed and utilized to address the study questions is produced as a consequence of this phase. The reporting part of the review phase, on the other hand, requires writing up the results in a chosen presenting pattern. In this stage, a research paper is the desired form for the final study report.

3.2 Research questions

This systematic literature review aims to shed light on the most significant advancements in blockchain-based electronic voting solutions that are presently shaping the electoral landscape in the rapidly evolving landscape of electronic voting systems. Blockchain technology has emerged as a promising solution for addressing security, transparency, and trust concerns in electronic voting systems. Table 2 outlines the research questions that will guide our investigation and serve as the foundation of this study. In the following pages, we will delve into these central questions, using a comprehensive analysis of the existing literature to provide valuable insights into the current state of blockchain-based electronic voting.

Table 2. Research questions

Id Question	Questions	Description
RQ1	Which implementation of blockchain-based electronic voting solutions are the most well-known?	This query attempts to highlight the most popular blockchain implementations that serve as the framework for electronic voting systems. It enables a comparison of several blockchains and their characteristics.
RQ2	Can the blockchain concept enhance systems for electronic voting?	This query seeks to demonstrate How well can blockchain be used to administer electronic voting?
RQ3	What models of blockchain consensus are used?	This question aims to identify the different consensus used in blockchain.
RQ4	Does the solution comply with any law or standards?	This inquiry tries to ascertain if electronic voting systems are governed by any laws or regulations.
RQ5	What various cryptographic techniques were employed in the studies?	Solutions for electronic voting make use of numerous cryptographic primitives and techniques. This inquiry seeks to identify them so that they can be included in other answers.

3.3 Primary study

Particular keywords were grouped to form a journal or search engine search tool to emphasize the value of primary research. The keywords were chosen to make it easier to find research findings that would help to address the research questions. Additionally, the only operators employed to restrict this research were "AND" and "OR".

3.4 Inclusion and exclusion criteria

An exhaustive set of inclusion (IC) and exclusion (EC) criteria has been meticulously defined to ensure the accuracy and relevance of our systematic literature review. These criteria form the basis for filtering the database search results. Please refer to Table 3 for inclusion criteria and Table 4 for exclusion criteria for a detailed breakdown of the specific criteria that govern our selection procedure. These tables provide a comprehensive and transparent list of the criteria we've established to ensure that the articles chosen for review closely correlate with the research objectives and questions posed in this study.

Table 3. Inclusion criteria

Id Inclusion	Criteria
Inclusion Criteria 1	Studies published in the last five years (01.01.2018–10.12.2022).
Inclusion Criteria 2	Studies that answer a research question or present a practical solution.
Inclusion Criteria 3	Studies that cover blockchain-based electronic voting.
Inclusion Criteria 4	The papers are published in peer-reviewed journals/conference journals.
Inclusion Criteria 5	The papers should only be in English language.

Table 4. Exclusion criteria

Id Exclusion	Criteria
Exclusion Criteria 1	The papers that are not written in English language.
Exclusion Criteria 2	Studies that appeared before (01.01.2018) and after (10.12.2022).
Exclusion Criteria 3	Studies that are not relevant since they don't address the study's research questions.
Exclusion Criteria 4	Duplicated research.
Exclusion Criteria 5	The articles have not been published in peer-reviewed journals or conference proceedings

3.5 Strategy search

Information was gathered from three databases—IEEE Digital Library, Scopus, and web of Science were used as part of the search approach. The PICOC criteria were utilized in the review methodology to frame the following research questions:

1. Population: We looked at articles describing electronic voting systems centered on blockchain for big to small elections.
2. Intervention: Gather data on electronic voting systems based on blockchain networks.

3. Comparison: The studies that were gathered will not be compared.
4. Outcomes: Understanding the scalability of blockchain-based electronic voting systems, their use in real-world settings, their benefits and drawbacks, and how they make use of cryptographic solutions.
5. Context: Electronic voting, e-voting and blockchain.

In light of this, after many attempts, the following search term was eventually produced for searching the selected databases: ("e-voting blockchain" OR "electronic voting blockchain").

3.6 Selection procedure

A total of 692 documents were found after running the search string through the databases: 279 from Web of Science, 281 from Scopus, and 132 from the IEEE Digital Library as presented in Figure 2. The four stages of filtering the collected papers were as follows: First comes the starting search, where the principal body of texts was assembled; second, duplicate removal, where duplicates must be omitted; third, selection based on a title and abstract reading, in which the inclusion and exclusion standards were applied to titles and abstracts; and then selection based on a full reading, in which the inclusion and exclusion standards were applied to entire papers. The procedure resulted in a total of 120 papers where 70 are conference papers and 50 articles. we will depend on conference paper besides journal paper for analysis since conference paper provides clear and detailed samples of voting systems as well.

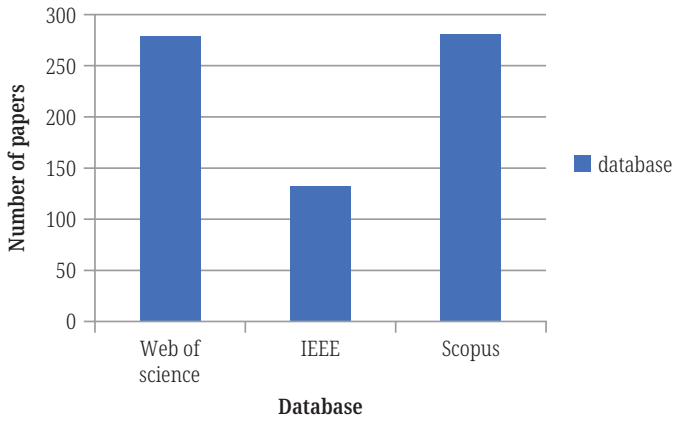

Fig. 2. Number of papers per database

3.7 Publication year

Figure 3 displays the distribution of selected articles and conference papers in publications for analysis, organized by year of publication. It is apparent that the term is merely five years even though no restrictions were placed (2018–2022).

Between 2018 and 2020, both the research paper and the conference paper have rising slope curves. From 2020 to 2021, the slope of the article curve begins to take on a linear shape, then drops from 2021 to 2022. While the slope of the curve decreases from 2020 to 2021, whereas the slope of the conference paper curve increases from 2021 to 2022.

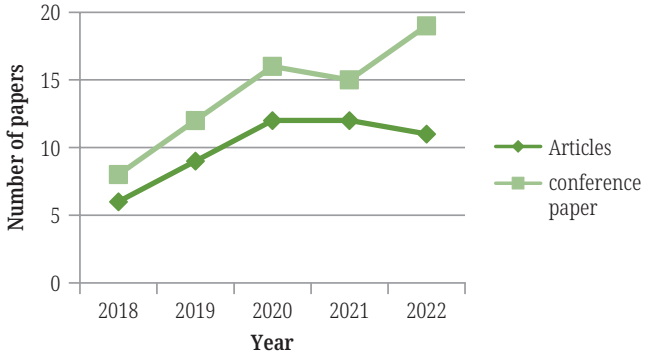

Fig. 3. Researches selected for analysis per year

3.8 Conferences papers vs journals

According to the pie chart below Figure 4, conference papers make up 59% of all publications while journal papers make up just 41%. The visual isolation of this point from the chart emphasizes it very strongly.

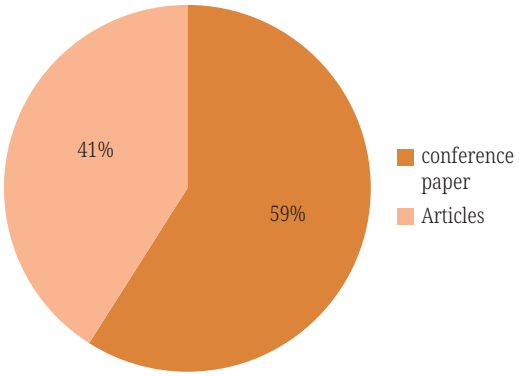

Fig. 4. Percentage of selected articles and conference papers

4 RESEARCH RESULT

4.1 RQ1: Which implementation of blockchain-based electronic voting solutions are the most well-known?

In the beginning section of the study, we looked for existing studies on using blockchain technology to set up a safe electronic voting system. A wide variety of e-voting strategies are put forth in the context of blockchain-based e-voting. We looked at a lot of research papers for this study, and we will only discuss about a few of them.

A blockchain-based electronic voting system is suggested by [8]. This system maintains transparency by providing the voter with transaction IDs. On the election site, voters can use a blockchain explorer to authenticate themselves utilizing their electronic identification. They can then pinpoint the corresponding transaction ID using the transaction ID they were given to show their vote. The system is verifiable since the voter can check to make sure that their vote was recorded and counted appropriately.

According to [9], the blockchain-based electronic voting system is secure from duplication. Only eligible voters are allowed to cast ballots under their proposed system, and each eligible voter is only permitted to obtain one voting token. Once a vote has been cast using one of these tokens, the other nodes in the network will reject any more votes from being sent to the blockchain.

The Blockchain-based e-voting Scheme (BES), developed by Yi [10], established methods for utilizing blockchain technologies to upgrade the security of e-voting in Peer-to-Peer (P2P) networks. Voting forgery can be avoided by using a distributed ledger-based BES. On Linux platforms in the P2P network, the system testing was planned and demonstrated. Attacks using countermeasures pose a serious issue for this method. This method requires reliable outside parties and is not well suited to being used centrally in a system context with various agents. A distributed (decentralized) strategy, i.e., the use of safe multipart computers, can be used to solve this. However, in the latter scenario, computing expenses are higher and may become restrictive if the computation function is compound and there are a very large number of parties.

Anti-Quantum EV Protocol in Blockchain with Audit Function has been proposed by Gao and Zheng [11]. Voter registration, verification, voting, counting, agreement, auditing, and announcement of the election results are the first steps in the process. To fend off quantum attacks, they modified the code-based Niederreiter method. Even if they use Ring Signature to preserve the anonymity of voters, managing and organizing various signatory organizations can be difficult. The benefits of efficiency and security are excellent for a small-scale election, but when there are more voters, argues, better security is attained by sacrificing some efficiency. Gao claims that privacy, anonymity, audit, and fairness were the main focuses of this blockchain-based electronic voting system.

The BSJC Proof of Completeness is an authentic electronic voting system that Shahzad and Crowcroft presented [12]. The SHA-256 hashing technique is used in this scheme to create and seal the blocks utilizing a configurable PoW (proof of work) blockchain algorithm which is a consensus method to validate and record new transactions on the blockchain. More security is needed for electronic voting, such as verifiability, scalability, security, and quantum assaults, which were disregarded by the author. Another problem with involving a third party is the high likelihood of information tampering, leakage, and biased outcomes that might affect end-to-end verification. The PoW is a vast, mathematically challenging undertaking that demands a huge amount of energy to complete.

The creation and sealing of the block can cause a significant polling delay due to the PoW's high energy consumption. The basic result is that for common data sizes, SHA-256 takes 50% longer to compute than SHA-512. It was primarily centered on anonymity, audit, and the legitimacy of the procedure and attempted to address anonymity, privacy, and security issues in the election on a small scale. An examination of their plan, however, leads us to the conclusion that, if the electorate is small, the security and efficiency benefits are substantial for the election on a small scale. Greater security is achieved when the number is large by lowering some of the efficiency.

Through a variety of scenarios including voting population, block size, block production rate, and block transaction speed, Khan, Arshad [13] rigorously experimented with permissioned and permissionless blockchain designs. In relation to their plan, the election procedure requires the creation of voter and candidate addresses. Votes from voters are afterwards sent to candidates at these addresses. Until a miner updates the central ledger, the vote status is not established. At the polling place, the vote is afterwards cast using the voting machine. This model does have some drawbacks, such

as the absence of a regulating body to prevent ineligible voters from voting. They did not worry about the integrity of the voter, their model is inaccurate, and it is insecure from quantum attach. Only in small and medium-sized voting situations is their technique effective. They have employed the multichain substructure and a private Bitcoin-based blockchain, that are inappropriate for use in a national election process.

Additionally, Table 5 below displays other research that employ various blockchain frameworks to create the e-voting system.

Table 5. Some of blockchain framework used in e-voting

Framework	Year Release	Power Consumption	Scalability	Papers
Bitcoin	2008	Very high	Very low	[10],[11],[14],[15], [16],[17],[18]
Ethereum	2015	High	Low	[8],[19],[20],[21],[22],[23], [24],[25],[26],[27], [28],[29],[30],[31]
Hyperledger Fabric	2015	Very low	Good	[22],[32],[33],[34], [35],[36],[37],[38]

4.2 RQ2: Can the blockchain concept enhance systems for electronic voting?

The blockchain protocol is a distributed, transparent method of logging and verifying records. Votes are typically logged, handled, counted, and verified by a central authority. By enabling voters to keep a copy of the voting record, electronic voting based on blockchain would give them the power to do these responsibilities independently [39]. Because other voters would notice that the record is different from theirs, the historic record could not thereafter be altered. Because other voters could check to see if the votes were legal and in accordance with the rules, unauthorized votes could not be added (possibly because they have previously been counted or because they are not linked to a legitimate voter register) [27]. Blockchain-based electronic voting would displace authority and trust from centralized actors, including electoral officials, and promote the growth of a tech-enabled community consensus. Making a brand-new, custom system that is made to reflect the unique characteristics of the election and electorate is one method of establishing blockchain-based systems for electronic voting. Moreover, taking the idea a step further, e-voting systems might be linked with smart contracts to execute predetermined actions automatically [40]. For example, under this case, election results may automatically conduct manifesto commitments, financial decisions, or other organizational decisions.

4.3 RQ3: What models of blockchain consensus are used?

In order to add a block of arrangements to the peer-to-peer distributed ledger, the nodes initiate a consensus method. The consensus mechanism on the blockchain ensures the legitimacy and authenticity of all transactions, in addition to ensuring that every node in the network has a copy of the ledger. There are a wide variety of consensus algorithms available.

To achieve consensus, blockchain networks typically use either a Proof-of-Work (PoW) or Proof-of-Stake (PoS) architecture. POW [41] is a method that permits impartial and reliable validation of the transactions. The fee is entirely discretionary

and can be traded between the transaction's parties so that it can be forwarded to users for verification. It could be necessary in some other contexts, such as bitcoin. In exchange for verifying a block of transactions and receiving a transaction fee, the network rewards participants with bitcoin. Initiated by a user, this procedure is called as "mining," and it effectively represents a transaction that resolves an issue. The results of this method are straightforward to verify but extremely difficult to replicate. One disadvantage of POW is that it is expensive and takes a long time to implement. The wasteful consumption of electricity is another problem.

While the Proof of Stake (PoS) chains produce and confirm new blocks through staking, PoS [42] is a system that employs mining to confirm new blocks. Instead of highly computation-intensive competition for the next block, PoS validators are picked depending on the amount of coins they choose to stake. This network uses pre-created currency, and therefore, unlike PoW, there is no need for a mining operation to produce them. As a result, energy costs are reduced because no intricate problem-solving transaction is required, and PoW processing times are greatly accelerated. There are many other widely used consensus methods that rely on different ideas like the Delegated Proof of Stake (DPOS) and the Practical Byzantine Fault Tolerance (PBFT). A DPOS [43] is a voting-based algorithm in which a select group of delegates casts the majority of the stakeholder votes. In return, these delegates' duty is to protect the network. When producing and certifying new blocks, the delegates—also known as witnesses—are in charge of coming to an agreement. Every user's total quantity of coins must equal their total number of votes.

Furthermore, the Practical Byzantine Fault Tolerance [44] is a technique utilized in permissioned blockchains, where network members are familiar with one another. The leader and backup nodes of the PBFT are different types of nodes. Even if malicious users disregard the rules, this method can guarantee that agreements between nodes may be reached. The systems using the PBFT method can operate up to (N-1/3) malfunctioning nodes, where N is the total figure of nodes, to stop unscrupulous users from making poor decisions.

In conclusion, blockchain's consensus process ensures that all participating nodes reach a unanimous decision and that only legitimate blocks are added to the distributed ledger. Different consensus methods are used in this procedure, and they all have their own quirks and applications. The most popular consensus algorithms in blockchain are shown in the following Table 6.

Table 6. Types of blockchain consensus

Property	Proof of Work	PBFT	Proof of Stake	DPOS
Management	Open	Permissioned	Open	Open
Energy efficiency	No	Yes	Partial	Partial
Adversary tolerance	51%	33%	51%	51%
Scalability	Good	Bad	Good	Good
Application Type	Public blockchain	Permissioned Blockchain	Public blockchain	Public blockchain

4.4 RQ4: Does the solution comply with any law or standards?

The standard includes a list of standards and requirements for testing voting systems, such as fundamental operation, accessibility, and security capabilities. None of

the standards, laws, or regulations that apply to what was stated in the publications were mentioned.

On the basis of general knowledge or other publications, there are various prerequisites for electronic voting systems that are mentioned.

These prerequisites consist of the features we have in the following Table 7.

Table 7. Features e-voting blockchain

Features	Description
Voter confidentiality	Only voters must be aware of their ballot choices.
Eligibility	Only persons who are lawful, authenticated, and authorized may vote.
Fairness	Entails that the results of an election are impossible to be influenced whatsoever.
Accuracy	Necessitates that every vote be accurately counted in the final total and that the voting process be impenetrable.
Receipt freeness	The absence of receipts that may be used to connect voters to their ballots.
Integrity	Votes must not be changed after they have been cast.
Coercion	Needs that it be impossible to initiate that a vote was cast under coercion.
Verifiability	Necessitates that the election procedure be open and auditable.

4.5 RQ5: What various cryptographic techniques were employed in the studies?

This inquiry sought to discover the cryptographic techniques that are currently being used more frequently in research on electronic voting. The results that link individual academic publications to cryptographic solutions are displayed in Table 8.

Table 8. Cryptographic techniques used in voting

Cryptography Solution	Papers
Homomorphic Encryption	[20],[37],[45],[46],[47],[48],[49],[50],[51],[52]
Blind Signature and ring Signature	[9],[20],[26],[36],[37],[51],[53]
Secure Hashing Algorithm (SHA)	[10],[12]
Zero-knowledge proof	[15],[28],[46],[47],[49],[50],[54]

1. Homomorphic Encryption: Is a type of cryptographic solution that enables calculations to happen on ciphertext with the same outcome as if the calculations had been made on plaintext [37]. Symmetric-key encryption is the name given to this sort of encryption. ElGamal and Paillier cryptosystems were the two homomorphic encryption techniques that were most frequently utilized in the chosen papers [45],[46]. To ensure privacy and fairness, votes are encrypted using homomorphic encryption.
2. Digital blind and ring signatures: Are public-key cryptographic techniques used for authentication and permission. The privacy and anonymity of the signer are greatly enhanced by digital, blind, and ring signatures. Without disclosing the owner of the ballot, voting systems use blind signatures to persuade the tallying center that the ballot shape a legitimate voter [9]. The person approving the ballot is unaware of the voter's choices at the same time. The two, voters and

the tallying center should believe the signer in a blind signing. The signature scheme could stop working if the signer is compromised. Linkable ring signature, as opposed to blind signing, is suggested to prevent unauthorized signers. It is a cryptographic procedure that enables someone to secretly electronically sign their vote. Other users selected by the signer—the person who created the signature—are involved in this system, though they are not always made aware of how they contributed to the formation of the electronic signature. To make his signature distinct from other voters' signatures, the voter must add their public keys when signing the ballot [37]. The authority can quickly determine whether a voter has already cast a ballot by matching the linkability tag. However, for these methods to be trustworthy, anonymous channels and reputable signing institutions are needed.

3. Secure hashing algorithm (SHA): SHA, a more recent iteration of MD5, is used to hash data and verify certificates. By utilizing binary operations, modular additions, and compression functions, a hashing algorithm reduces the input information into a smaller shape that is impossible to comprehend. It is not possible to "decrypt" a hash for getting back the utility of the plaintext that it was encrypted from; as a result, the principal function of the hash in the blockchain is to keep the blocks reliable and unchangeable. Also, this is achieved by the outcome of blocks in which every block includes the hash of the latter block. Consequently, the odds of an attacker altering the contents of a block are zero since doing so would require altering all subsequent blocks in the chain rather than just one. More than that, the hash is also used to obtain the Merkle root, which is obtained by hashing every transaction in a block. This makes a digital fingerprint of every operation, enabling the user to examine if the block contains a transaction that ensures the integrity of the data [10],[12].
4. Zero-knowledge-proof: Is a cryptographic method that allows one party to reveal to another party that a given assertion is true without disclosing any other information. In a voting system, the voter should persuade the authority that his ballot is authentic by demonstrating that it merely contains one genuine candidate without disclosing his vote [28],[47].

5 DISCUSSION

Whether to use a public or permissioned blockchain is a crucial question for blockchain-based electronic voting systems. While public blockchains have the advantages of openness and decentralization, they may have difficulty scaling to handle high transaction volumes. Permissioned blockchains, on the other hand, provide for more oversight and privacy at the expense of some decentralization. To reduce the possibility of voter impersonation, permissioned blockchains may use more stringent identity management and authentication techniques.

Electronic voting systems rely heavily on consensus procedures to guarantee their reliability and safety. The throughput, energy efficiency, and attack resistance of a network may all be affected in different ways by the consensus method used. The costs and benefits of various consensus methods have been uncovered via comparative research. Examples include Proof of Work (PoW), which provides high security but uses a lot of energy, and Practical Byzantine Fault Tolerance (PBFT), which has greater throughput but needs a set of trustworthy nodes to be established ahead of time.

It is still difficult to provide voter anonymity in electronic voting systems without compromising on overall verifiability. Although blockchain technology increases openness, finding a happy medium between privacy and openness is difficult. To overcome this obstacle and safeguard voter anonymity without compromising the honesty of the vote, novel cryptographic approaches like zero-knowledge proofs or homomorphic encryption may be investigated.

Blockchain-based electronic voting systems need careful attention to identity management and verification. Voter impersonation may be avoided and the integrity of the electoral process can be protected by the use of a number of different methods of authentication, including digital signatures, biometrics, and multi-factor authentication.

Blockchain-based electronic voting systems also confront the problem of scalability. With more people casting ballots and doing business, the system must be able to process massive amounts of data quickly and reliably. Some solutions to the scalability problem have been offered, such as the use of sharding to divide the blockchain into smaller, more manageable pieces.

The widespread use of electronic voting systems relies heavily on their ease of use and accessibility. The adoption and use of blockchain-based electronic voting systems may be boosted by making the interface and voting process easier to understand and use. Prioritizing accessible design and user-friendliness in the development of such systems is essential.

While this body of work gives useful information, further study is required to fill in the remaining gaps and problems. To evaluate the viability, performance, and acceptability of blockchain-based e-voting systems in real-world voting situations, their installation and assessment are crucial. The safety and efficacy of these technologies can only be determined by real-world testing, hence pilot studies and field trials are necessary.

In conclusion, blockchain technology shows great promise for addressing concerns about credibility, safety, and accountability in online voting. The relative benefits of public and permissioned blockchains, consensus methods, privacy and identity protection, identity management, scalability solutions, usability, and practical application are all important questions that need more research. These issues, if resolved, could improve the credibility and openness of blockchain-based electronic voting systems.

6 CONCLUSION

This article has compared and contrasted many distinct blockchain-based e-voting systems to highlight their respective advantages and disadvantages. This research demonstrates the potential benefits of blockchain technology for increasing the trustworthiness, safety, and efficacy of electronic voting. The gaps and the need for more research in this area, however, must not be overlooked.

The difficulty of scaling is a major obstacle for us. Despite its inherent security and tamper-resistant qualities, blockchain technology has struggled to date to manage the number of transactions required for large-scale elections. Managing a big number of voters in a short amount of time requires further study to develop efficient, secure, and trustworthy solutions.

Another difficulty with blockchain-based electronic voting systems is the question of how to ensure the privacy of voters' personal information. Finding a happy medium between protecting voters' right to remain anonymous and making sure elections may be observed by anybody can still be challenging. Future research

should explore innovative methods of overcoming privacy issues to ensure that the voting results can be independently confirmed and audited.

Furthermore, it is crucial to provide reliable methods for verifying voter's identities. Maintaining trust in the electoral process necessitates robust identity verification while preserving individual's privacy. The identity verification process might be strengthened by the investigation of new cryptographic methods and safe identification protocols.

In conclusion, blockchain-based electronic voting systems hold significant promise, but there are persistent challenges that must be addressed to rectify current shortcoming. Important issues that need to be tackled include scalability, privacy, and identity verification techniques. Researchers can help in creating more secure, transparent, and trustworthy elections in the future by tackling these issues and paving the road for the actual deployment of blockchain-based e-voting systems.

7 REFERENCES

[1] E. Zaghloul, T. Li, and J. Ren, "d -BAME: Distributed blockchain-based anonymous mobile electronic voting," *IEEE Internet Things J.*, vol. 8, no. 22, pp. 16585–16597, 2021. https://doi.org/10.1109/JIOT.2021.3074877

[2] U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system—review and open research challenges," *Sensors*, vol. 21, no. 17, p. 5874, 2021. https://doi.org/10.3390/s21175874

[3] S. A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," *International Journal of Research in Engineering and Technology*, vol. 5, no. 9, pp. 1–10, 2016. https://doi.org/10.15623/ijret.2016.0509001

[4] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, 2017. https://doi.org/10.6633/IJNS.201709.19(5).01

[5] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019. https://doi.org/10.1109/ACCESS.2019.2936094

[6] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018. https://doi.org/10.1504/IJWGS.2018.10016848

[7] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," 2007.

[8] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtỳsson, "Blockchain-based e-voting system," in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, IEEE, 2018, pp. 983–986. https://doi.org/10.1109/CLOUD.2018.00151

[9] F. Sheer Hardwick, A. Gioulis, R. Naeem Akram, and K. Markantonakis, "E-voting with Blockchain: An e-voting protocol with decentralisation and voter privacy," *arXiv e-prints*, arXiv-1805, 2018. https://doi.org/10.1109/Cybermatics_2018.2018.00262

[10] H. Yi, "Securing e-voting based on blockchain in P2P network," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–9, 2019. https://doi.org/10.1186/s13638-019-1473-6

[11] S. Gao, D. Zheng, R. Guo, C. Jing, and C. Hu, "An anti-quantum e-voting protocol in blockchain with audit function," *IEEE Access*, vol. 7, pp. 115304–115316, 2019. https://doi.org/10.1109/ACCESS.2019.2935895

[12] B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," *IEEE Access*, vol. 7, pp. 24477–24488, 2019. https://doi.org/10.1109/ACCESS.2019.2895670

[13] K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system," *Future Generation Computer Systems*, vol. 105, pp. 13–26, 2020. https://doi.org/10.1016/j.future.2019.11.005

[14] C. K. Adiputra, R. Hjort, and H. Sato, "A proposal of blockchain-based electronic voting system," in *2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, IEEE, 2018, pp. 22–27. https://doi.org/10.1109/WorldS4.2018.8611593

[15] T. Dimitriou, "Efficient, coercion-free and universally verifiable blockchain-based voting," *Computer Networks*, vol. 174, p. 107234, 2020. https://doi.org/10.1016/j.comnet.2020.107234

[16] S. Bistarelli, I. Mercanti, P. Santancini, and F. Santini, "End-to-end voting with non-permissioned and permissioned ledgers," *Journal of Grid Computing*, vol. 17, no. 1, pp. 97–118, 2019. https://doi.org/10.1007/s10723-019-09478-y

[17] X. Sun, Q. Wang, P. Kulicki, and M. Sopek, "A simple voting protocol on quantum blockchain," *International Journal of Theoretical Physics*, vol. 58, no. 1, pp. 275–281, 2019. https://doi.org/10.1007/s10773-018-3929-6

[18] S. Bartolucci, P. Bernat, and D. Joseph, "SHARVOT: Secret SHARe-based VOTing on the blockchain," in *Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain*, 2018, pp. 30–34. https://doi.org/10.1145/3194113.3194118

[19] D. Pawade, A. Sakhapara, A. Badgujar, D. Adepu, and M. Andrade, "Secure online voting system using biometric and blockchain," in *Data Management, Analytics and Innovation*, N. Sharma, A. Chakrabarti, and V. E. Balas, Eds., in Advances in Intelligent Systems and Computing, vol. 1042. Singapore: Springer Singapore, 2020, pp. 93–110. https://doi.org/10.1007/978-981-32-9949-8_7

[20] Y. Zhang, Y. Li, L. Fang, P. Chen, and X. Dong, "Privacy-protected electronic voting system based on blockchain and trusted execution environment," in *2019 IEEE 5th International Conference on Computer and Communications (ICCC)*, IEEE, 2019, pp. 1252–1257. https://doi.org/10.1109/ICCC47050.2019.9064387

[21] C. Braghin, S. Cimato, S. R. Cominesi, E. Damiani, and L. Mauri, "Towards blockchain-based E-voting systems," in *International Conference on Business Information Systems*, Springer, 2019, pp. 274–286. https://doi.org/10.1007/978-3-030-36691-9_24

[22] M. Soud, S. Helgason, G. Hjálmtỳsson, and M. Hamdaqa, "TrustVote: On elections we trust with distributed ledgers and smart contracts," in *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, IEEE, 2020, pp. 176–183. https://doi.org/10.1109/BRAINS49436.2020.9223306

[23] M. Pawlak, A. Poniszewska-Marańda, and N. Kryvinska, "Towards the intelligent agents for blockchain e-voting system," *Procedia Computer Science*, vol. 141, pp. 239–246, 2018. https://doi.org/10.1016/j.procs.2018.10.177

[24] Y. Abuidris, R. Kumar, T. Yang, and J. Onginjo, "Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding," *Etri Journal*, vol. 43, no. 2, pp. 357–370, 2021. https://doi.org/10.4218/etrij.2019-0362

[25] G. Rathee, R. Iqbal, O. Waqar, and A. K. Bashir, "On the design and implementation of a blockchain enabled e-voting application within IoT-oriented smart cities," *IEEE Access*, vol. 9, pp. 34165–34176, 2021. https://doi.org/10.1109/ACCESS.2021.3061411

[26] S. T. Alvi, M. N. Uddin, and L. Islam, "Digital voting: A blockchain-based e-voting system using biohash and smart contract," in *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, IEEE, 2020, pp. 228–233. https://doi.org/10.1109/ICSSIT48917.2020.9214250

[27] A. M. Al-Madani, A. T. Gaikwad, V. Mahale, and Z. A. Ahmed, "Decentralized E-voting system based on smart contract by using blockchain technology," in *2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC)*, IEEE, 2020, pp. 176–180. https://doi.org/10.1109/ICSIDEMPC49020.2020.9299581

[28] R. Bosri, A. R. Uzzal, A. Al Omar, A. T. Hasan, and M. Z. A. Bhuiyan, "Towards a privacy-preserving voting system through blockchain technologies," in *2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, IEEE, 2019, pp. 602–608. https://doi.org/10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00116

[29] A. J. Perez and E. N. Ceesay, "Improving end-to-end verifiable voting systems with blockchain technologies," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, IEEE, 2018, pp. 1108–1115. https://doi.org/10.1109/Cybermatics_2018.2018.00202

[30] E. Yavuz, A. K. Koç, U. C. Çabuk, and G. Dalkılıç, "Towards secure e-voting using ethereum blockchain," in *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, IEEE, 2018, pp. 1–7. https://doi.org/10.1109/ISDFS.2018.8355340

[31] D. Khoury, E. F. Kfoury, A. Kassem, and H. Harb, "Decentralized voting platform based on ethereum blockchain," in *2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)*, IEEE, 2018, pp. 1–6. https://doi.org/10.1109/IMCET.2018.8603050

[32] M. B. Verwer, I. Dionysiou, and H. Gjermundrød, "TrustedEVoting (TeV) a secure, anonymous and verifiable blockchain-based e-voting framework," in *International Conference on e-Democracy*, Springer, 2019, pp. 129–143. https://doi.org/10.1007/978-3-030-37545-4_9

[33] O. Daramola and D. Thebus, "Architecture-centric evaluation of blockchain-based smart contract e-voting for national elections," in *Informatics*, MDPI, 2020, p. 16. https://doi.org/10.3390/informatics7020016

[34] Y. Zhou, Y. Liu, C. Jiang, and S. Wang, "An improved FOO voting scheme using blockchain," *International Journal of Information Security*, vol. 19, no. 3, pp. 303–310, 2020. https://doi.org/10.1007/s10207-019-00457-8

[35] S. Chaisawat and C. Vorakulpipat, "Fault-tolerant architecture design for blockchain-based electronics voting system," in *2020 17th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, IEEE, 2020, pp. 116–121. https://doi.org/10.1109/JCSSE49651.2020.9268264

[36] D. Kirillov, V. Korkhov, V. Petrunin, M. Makarov, I. M. Khamitov, and V. Dostov, "Implementation of an e-voting scheme using hyperledger fabric permissioned blockchain," in *International Conference on Computational Science and Its Applications*, Springer, 2019, pp. 509–521. https://doi.org/10.1007/978-3-030-24296-1_40

[37] W. Zhang et al., "A privacy-preserving voting protocol on blockchain," in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, IEEE, 2018, pp. 401–408. https://doi.org/10.1109/CLOUD.2018.00057

[38] C. Denis González, D. Frias Mena, A. Massó Muñoz, O. Rojas, and G. Sosa-Gómez, "Electronic voting system using an enterprise blockchain," *Applied Sciences*, vol. 12, no. 2, p. 531, 2022. https://doi.org/10.3390/app12020531

[39] M. Chaieb, S. Yousfi, P. Lafourcade, and R. Robbana, "Verify-your-vote: A verifiable blockchain-based online voting protocol," in *European, Mediterranean, and Middle Eastern Conference on Information Systems*, Springer, 2019, pp. 16–30. https://doi.org/10.1007/978-3-030-11395-7_2

[40] S. T. Alvi, M. N. Uddin, L. Islam, and S. Ahamed, "DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 9, pp. 6855–6871, 2022. https://doi.org/10.1016/j.jksuci.2022.06.014

[41] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*, IEEE, 2017, pp. 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

[42] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain," *Journal of Information Processing Systems*, vol. 14, no. 1, pp. 101–128, 2018.

[43] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, "Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism," *IEEE Access*, vol. 7, pp. 118541–118555, 2019. https://doi.org/10.1109/ACCESS.2019.2935149

[44] M. Castro and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems (TOCS)*, vol. 20, no. 4, pp. 398–461, 2002. https://doi.org/10.1145/571637.571640

[45] M. Chaieb and S. Yousfi, "LOKI Vote: A blockchain-based coercion resistant E-voting protocol," in *European, Mediterranean, and Middle Eastern Conference on Information Systems*, Springer, 2020, pp. 151–168. https://doi.org/10.1007/978-3-030-63396-7_11

[46] X. Yang, X. Yi, S. Nepal, A. Kelarev, and F. Han, "Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities," *Future Generation Computer Systems*, vol. 112, pp. 859–874, 2020. https://doi.org/10.1016/j.future.2020.06.051

[47] C. Killer et al., "Provotum: A blockchain-based and end-to-end verifiable remote electronic voting system," in *2020 IEEE 45th Conference on Local Computer Networks (LCN)*, IEEE, 2020, pp. 172–183. https://doi.org/10.1109/LCN48667.2020.9314815

[48] R. Taş and Ö. Ö. Tanrıöver, "A manipulation prevention model for blockchain-based e-voting systems," *Security and Communication Networks*, vol. 2021, 2021. https://doi.org/10.1155/2021/6673691

[49] H. Li, Y. Li, Y. Yu, B. Wang, and K. Chen, "A blockchain-based traceable self-tallying E-voting protocol in AI era," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1019–1032, 2020. https://doi.org/10.1109/TNSE.2020.3011928

[50] Y. Li et al., "A blockchain-based self-tallying voting protocol in decentralized IoT," *IEEE Transactions on Dependable and Secure Computing*, 2020. https://doi.org/10.1109/TDSC.2020.2979856

[51] S. Zhang, L. Wang, and H. Xiong, "Chaintegrity: Blockchain-enabled large-scale e-voting system with robustness and universal verifiability," *International Journal of Information Security*, vol. 19, no. 3, pp. 323–341, 2020. https://doi.org/10.1007/s10207-019-00465-8

[52] S. A.-B. Salman, S. Al-Janabi, and A. M. Sagheer, "Valid blockchain-based e-voting using elliptic curve and homomorphic encryption," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 16, no. 20, pp. 79–97, 2022. https://doi.org/10.3991/ijim.v16i20.33173

[53] T. M. Roopak and R. Sumathi, "Electronic voting based on virtual id of aadhar using blockchain technology," in *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, IEEE, 2020, pp. 71–75. https://doi.org/10.1109/ICIMIA48430.2020.9074942

[54] P. Li and J. Lai, "LaT-Voting: Traceable anonymous E-voting on blockchain," in *International Conference on Network and System Security*, Springer, 2019, pp. 234–254. https://doi.org/10.1007/978-3-030-36938-5_14

8 AUTHORS

Rabia Fatih is currently pursuing his PhD degree with the Mathematics, Computer Science and Engineering Sciences Laboratory, Hassan first University of Settat, Faculty of Sciences and Techniques, Settat, Morocco. His current research interests include blockchain. He received his master's degree in Application Design and Development Engineering from Hassan first University of Settat, Faculty of Sciences and Techniques, Settat, Morocco, in 2018 (E-mail: r.fatih@uhp.ac.ma).

Sara Arezki is an Associate Professor, PhD, in University Hassan First and visiting professor in several Moroccan universities and schools. She is also computer science engineer from University Mohamad V – National School of Informatics and System Analysis in Rabat. She started her professional career as an IT project manager in the finance sector and then in several others sectors (EDtech, Fintech, etc). She is an expert in implementing quality projects using referentials and norms (CobiT, CMMI, ITIL and ISO 27001, etc) in public and private sectors. She has served and continues to serve on technical program and organizing committees of several conferences and events. Pr. Arezki leads several projects related to smart cities such as smart citizen, smart parking and smart waste management. Her main research topics are Digital Transformation, Smart Cities, Quality Assurance, Disruptive technologies. She has published over 15 papers (book chapters, international journals, and conferences/workshops). Pr. Arezki is also a startup coach and mentor (E-mail: sara.arezki@gmail.com).

Taoufiq Gadi has been the Director of the Informatics, Imaging, and Modeling of Complex Systems Laboratory, since 2014. He is currently a professor of computer science with the Faculty of Science and Technologies, Hassan First University, Settat, Morocco. He has conducted more than twenty PhD theses and has written seventy scientific articles in the domain of model driving architecture, data mining and database analysis, 3D models analysis, modeling of complex systems, and machine learning (E-mail: gtaoufiq@yahoo.fr).