Evaluating the Feasibility of Blockchain Technology for Secure Voting System: A Systematic Mapping

Dijesh Shrestha, Shishir Poudel
Beacom College of Computer and Cyber Sciences
Dakota State University
Madison, United States
dijesh.shrestha@trojans.dsu.edu, shishir.poudel@trojans.dsu.edu

Abstract—**Blockchain technology is a peer-to-peer, immutable, and secure ledger system that has emerged as a possible solution to address the problems of centralized ballot and online voting systems, which are prone to risks regarding electoral integrity. This research evaluates the feasibility of blockchain-based voting technologies, analyzing their benefits and security assessments. Adopting a systematic mapping methodology, we extracted and analyzed relevant academic papers from multiple scientific databases that focus on blockchain frameworks applied to voting systems. Our evaluation is guided by three critical questions concerning the overall architecture, scalability, and security of blockchain-based voting systems. We aim to categorize and describe gaps and trends in existing literature, identifying areas that may require further research. Overall, the study identifies the benefits and limitations of blockchain voting technology from a robust democratic perspective.**

Keywords—blockchain, e-voting, blockchain voting, consensus mechanism

I. Introduction

Voting has been an integral part of human civilization to arrive on a unanimous decision, especially when electing a leader for society. However, people have trust issues in conventional voting approaches, namely ballot voting, due to frequent election manipulation, voter fraud, and rigging with illegal involvement with election process [1]. Moreover, ballot-based voting systems have the risk of records being destroyed by natural and human factors. Traditional ballot voting is still in practice in the majority of the elections worldwide, with a fairly new introduction of electronic voting (e-voting) systems in few countries. Amplified research demonstrates that implementing e-voting systems can improve security concerns associated with voter turnout, ensures ease of operation, and makes the overall election process. Although it an improvement on the ballot-based voting system on many aspects, security of the e-voting system is still an underlying issue. According to [2], electronic voting has challenges with data integrity, transparency, uneducated voters, secrecy of ballot, and consequences of system breakdown. Vladucu et al. [3] also states that citizens have expressed concerns over the security, privacy, authenticity, however, with the major issue being in control of a central authority or ballot-based voting [2]. While being more scalable and efficient, it addresses challenges such as voter accessibility, increases manipulation by unauthorized parties. With centralization, the question of electoral integrity is always at risk. Blockchain comes into this space with its decentralized public ledger and immutability. Blockchain is a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions [4]. Blockchain is the foundation for the development of cryptocurrencies such as Bitcoin and Ethereum. The integration of e-voting and blockchain seems to provide many solutions to voting systems such as decentralization, transparency, and immutability [5] . Although blockchain voting systems provide several advantages over e-voting and ballot-based voting, it is still in its early phases of development. The major problems of blockchain e-voting systems are regarding scalability and its security risks. To evaluate the prevalent issues and assess the strength of blockchain voting models, we have used systematic mapping process to review the current literature on this topic, selecting papers based on their relevancy and scrutinizing their scalability and security factor.

II. Blockchain Concept and Terminologies

A. Overview of Blockchain

Blockchain is a peer-to-peer, immutable, and secure ledger system that records transactions across multiple computers so that any involved transaction cannot be altered without altering all subsequent blocks [4]. Blockchain is a data structure on its own. In the paper, Nakamoto described it as a long chain of blocks containing several records, a timestamp, and a cryptographic hash of the previous block. Because of the way the chain and consensus mechanism are implemented, the chain, once recorded, is immutable to alterations by malicious parties [4].

In simple words, whenever a transaction is recorded, it is broadcast over the network, where predefined rules and protocols verify it. After verification, the transaction is recorded on the current block, which is then validated by the network through consensus mechanisms. Next, the block is added to the existing chain in a linear, chronological order. The consensus mechanism process makes the chain secure and decentralizes control—no single entity can change the data already stored in the system[2].

Following Bitcoin, several other technologies have evolved significantly over the years. While Bitcoin's scope was limited to peer-to-peer electronic cash, other technologies expanded the scope of blockchain beyond simple financial transactions. Platforms like Ethereum introduced programmable smart contracts that utilize blockchain's immutable and distributed consensus characteristics [6].

Smart contracts, in themselves, are just written pieces of logic in code. However, they can act as unconditionally trusted third parties because of their immutable properties. The application of smart contracts enabled Dapps to operate autonomously without intermediaries. In essence, what began as a solution for financial transactions has evolved into a dynamic technology, reshaping how trust and security are implemented in a wide range of industries [6].

B. *Fundamental Characteristics of Blockchain*

Blockchain architecture has several key characteristics that provide unique features across various sectors incorporating blockchain. Below is a list of some common characteristics of blockchain:

- Decentralization: The distributed ledger is managed and accessed by all nodes/participants in the network. Every node in the blockchain network maintains a backup of all transactions. Thus, the failure or unavailability of one node does not impact the entire network. This characteristic makes blockchain-based voting systems more robust [7].
- Immutability: Once transactions are verified and added to the ledger, data cannot be modified. This ensures that any malicious entity cannot benefit from data [3].
- Transparency: Transaction details are visible to all participants, while confidential information can be protected through various cryptographic methods. This also ensures that no single entity can alter the ledger without detection, as all participants can verify the integrity of the records [6, 8].
- Provenance: Every previous transaction/vote can be traced back in the blockchain ledger through the chain [6].
- Anonymity/Privacy: Various implementations of blockchain prioritize user privacy. Blockchain architecture primarily operates with cryptographic addresses rather than direct user identification. Depending on the implementation, users can be either pseudonymous or anonymous [7].

C. *Components of Blockchain Architecture*

Blockchain consists of several fundamental components and core parts:

- Nodes: Users or individual computers (peers) on the network that maintain a copy of the ledger [6].
- Transaction: Data recorded on the blocks (e.g., a vote or monetary transfer) is later broadcast to the network [8].
- Block: A container of transactions typically consists of a block header and body. The block header includes the previous block hash, Merkle root, timestamp, nonce, and difficulty target, while the block body contains the actual transactions [8].
- Chain: A sequence of blocks in a particular order, linked through cryptographic hashes [8].
- Distributed Ledger: A database of all transactions replicated across multiple nodes. Every node maintains an updated copy of the ledger [9].
- Consensus Mechanism: A collection of rules and protocols that nodes follow to reach an agreement on the validity of transactions and mining of new blocks (elaborated in Section 2.6) [6].
- Smart Contracts: Pieces of code that execute automatically when predefined conditions are met [5].

D. *Types of Blockchain*

Based on the set of rules defined for privacy, access control, and permission, Blockchain architecture can be classified based on privacy, access control, and permission models. From a privacy perspective, blockchains can be categorized into three main types: public, private, and consortium (hybrid) blockchains.

A public blockchain is fully decentralized and open to anyone to read or append data on the network. Examples of popular public blockchains include Bitcoin and Ethereum. A private blockchain, however, uses an entity to grant read/append permissions to users or allow them to join the network. Examples of private blockchains include Ripple and Eris. Private blockchains often adopt different methods to implement a semi-centralized structure. This allows the entity to control certain functions, such as throughput and transaction delay, while still maintaining some decentralized properties. A private blockchain is similar to traditional business models where central authority and control are essential [3].

A consortium blockchain is similar to a private blockchain, but instead of a single entity, multiple pre-selected nodes manage the network, making it partially decentralized. This model is often adopted in business environments where transparency and privacy are important. Hyperledger Fabric is a well-known example of a consortium blockchain [2, 3].

Blockchain architecture can also be classified as permission or permissionless. Public blockchains follow a permissionless model, where all nodes are allowed to join the network and read/append/validate blocks. They are fully decentralized, with most information available to the public. However, privacy preservation is often an issue in permissionless blockchains, as most information is accessible to all participating nodes in the network [3].

Private and hybrid blockchains fall under permissioned blockchain models. These typically require authorization from an entity or a majority of nodes to join the network or validate blocks [1].

E. *Cryptographic Techniques Relevant to E-Voting*

This section discusses different cryptographic techniques relevant to blockchain-based voting systems.

1) *Hash Function / Secure Hashing Algorithm*

A hash function is a mathematical function that maps a variable-sized input into a fixed-sized string output that is illegible to unintended receivers. The United States has published a group of cryptographic hash functions known as Secure Hashing Algorithms (SHA). There are multiple versions of SHA, one of which is SHA-256. SHA-256 takes an input of any length and converts it into a 256-bit hash value [3].

2) *Merkle Tree*

A Merkle tree is a tree-like structure in which leaf nodes are labeled with the hash of a data block, and non-leaf nodes (also known as nodes, branches, or inner nodes) are labeled with the hash of their child nodes [3]. The Merkle root is a single hash that represents all transactions within a block, making it easier to verify the entire set of records in a block [4].

3) *Blind Signature*

A blind signature is a digital signature used to verify the authenticity of digital messages without revealing the original content before signing. The authenticity of encrypted content can later be verified after signing the content, ensuring privacy while maintaining data integrity [3].

4) *Zero-Knowledge Proof (ZKP)*

ZKP is a cryptographic mechanism that involves three entities: the Prover, the Verifier, and the Secret. The prover can prove a given statement is true without revealing additional information to the verifier. This mechanism helps anonymize privacy-sensitive decisions or secrets without disclosing any information during the proving process. The prover does not need to reveal any details beyond confirming the statement's validity. ZKP enhances transparency while maintaining privacy in systems like blockchain-based e-voting [3] [5].

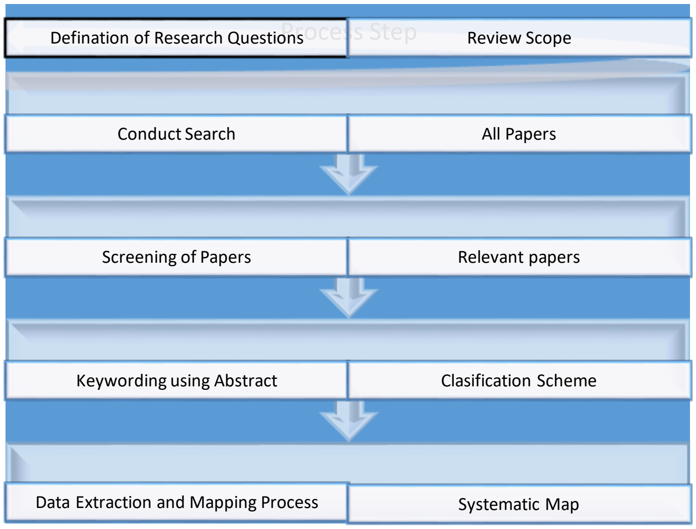
5) *Homomorphic Encryption*

(*Can be used to tally votes without decryption*). Homomorphic encryption allows computations to be performed on encrypted data without requiring decryption during processing. When the encrypted result is finally decrypted, it produces the same outcome as if the computations had been performed directly on plaintext data. With homomorphic encryption, data remains private and secure throughout the computation process, making it particularly useful for secure vote tallying in e-voting systems [5].s

III. Methodology

We started our paper by following the methodology presented in the paper [10] by Peterson. Our mapping process and outcome of each steps is shown in Figure 1 . According to [10] systematic mapping studies are broader in scope and are designed to provide an overview of a research area. They categorize and describe existing literature without necessarily evaluating the quality of each study in detail. This approach helps identify gaps in research, trends, and areas that may require further investigation .

Figure 1 . The Systematic Mapping Process



We started by defining the research questions. We carried out search of relevant keywords in multiple databases and screened the papers. We classified our paper based on keyword and abstract. Finally we summarized and synthesized the data extracted data from each paper.

A. *Research Questions*

We started our search by identifying scopes of blockchain voting systems that were relevant for our research. Our study is guided by three questions on blockchain based voting systems, each of which is discussed in ~~on~~ detail in section 4.

RQ.1. Issues in traditional voting system and can blockchain be a solution to it?

RQ.2. What are the current solutions and trends in blockchain based voting?

RQ.3. . What are the challenges and security risks faced by blockchain based voting system?

B. *Screening Process and Data Collection*

We focused on literature specifically addressing blockchain technology applied to voting systems or national elections. To this end, we employed targeted search queries using keywords such as “Blockchain voting,” “Secure blockchain voting,” and “blockchain e-voting.”

Our focus was majorly on blockchain technology applied to voting systems. For this, we organized targeted search queries on three data sources using keywords such as “Blockchain voting,” “Secure blockchain voting,” and “blockchain e-voting.”

Data Sources:

1) *IEEE Xplore*
2) *ACM Digital Library*
3) *Web of Science*

Below are tables summarizing the raw results and the numbers after applying exclusion criteria (e.g., excluding magazines and books, and applying publication date filters for 2020–2024 and relevant article types). Additional search filter using keywords such as “electoral system,” “electronic voting,” and “consensus mechanism” were applied in IEEE Xplore and Web of Science. The filters could not be applied in ACM Digital Library.

1. IEEE Xplore

Search Query	Raw Results	After Exclusions
Blockchain Voting	1208	609
Secure Blockchain Voting	483	297
Blockchain e-voting	524	340

2. ACM Digital Library

Search Query	Raw Results	After Exclusions
Blockchain Voting	2112	1615
Secure Blockchain Voting	2033	1550
Blockchain e-voting	1535	1160

3. Web of Science

Search Query	Raw Results	After Exclusions
Blockchain Voting	986	538
Secure Blockchain Voting	332	178
Blockchain e-voting	392	201

C. *Articles merging and filtering*

We merged the results from the different queries that were duplicates using Python and performed several filtering steps:

We further refined the datasets by ensuring that only articles with keywords containing “blockchain,” “e voting,” or “voting” (case-insensitive) were kept. This step resulted in:

IEEE Xplore	492 articles
Web of Science	424 articles
ACM Digital Library	NA (Filters could not be applied)

Additional criteria were applied to select articles with a minimum citation count **(⩾ 5)** and to ensure that titles explicitly mentioned both “**blockchain**” and “**voting.**”

This final filtering resulted:

IEEE Xplore	63 articles
Web of Science	51 articles
ACM Digital Library	19 articles

D. *Final refining and skimming*

Ensuring the quality and relevancy of our review, we applied an extra filter based on journal impact. We included paper from journal with rating equal to or **greater than 3**. This step helped us to reduce the overall set from 131 to 94 articles.

Beyond above filtering, we screened all papers and selected 31 papers based on their abstract, introduction and conclusion. Furthermore, we included paper [2],[4],[5],[6],[34],[37],[38] based on their relevance discovered through citation tracking.

In the end, after integrating our systematic filtering with manual screening and handpicking, we read a total of 38 papers related to blockchain and blockchain-based voting systems.

IV. Research questions and findings

A. *R.Q1. Issues in traditional voting system and can blockchain be a solution to it?*

In the present context, the ballot voting system suffers from a lack of transparency and the potential for manipulation. It becomes more and more difficult for the government to gain voters' trust. Verification of votes after the vote is still a prevailing issue, as any method to disclose the votes will jeopardize the voter's privacy [11]. Ballot-based voting systems often have a central authority that makes it easier to change or modify the decisions, impacting the final decision. Total reliance on a central authority leads to distrust in the system, reducing voter turnover. Reduction in turnover often results in polarizing outcomes, which begs us to raise questions about the process's validity [12]. Managing the ballot-based voting system on a larger scale comes with a price. It requires significant resources and money for infrastructure, staff, and security to manage the voting process. In addition, polling stations' location becomes a major hurdle for people living in rural and challenging landscapes. As for people who are living abroad and who have a disability, it is difficult for both these people and the voting commission to efficiently count their votes [13].The Revolution of computers and IoT devices has benefited human lives in many aspects, including electronic and online voting. The online voting system seems much more cost-effective and fast. The online voting systems might look like an upgrade from traditional ballot-based voting. However, it suffers from authentication, privacy, and data integrity issues. The storage of voter information in a database makes it more susceptible to hacking and changes by unauthorized parties and the central authority itself [6]. Blockchain-based voting systems present a good solution to the problems posed by centralized voting systems.

Below is a list of advantages of blockchain-based voting systems over conventional centralized voting systems

1. Blockchain technology maintains a higher level of transparency and reliability, which ultimately increases voters' trust in the system. Since the anonymity of voters' identities is crucial in any voting system, different mechanisms and proxies help hide voter identities. It also allows for data to be publicly verified, allowing voters to audit the data instead of one central authority [12].

2. Implementation of consensus mechanisms and security layers like hashing, immutable data structure, and encrypted ledger improves the security of e-voting systems on aspects where e-voting could fail otherwise. The property of an immutable data structure doesn't allow for any data modification or deletion after data is verified on the network [6]. Cryptographic hash and consensus mechanisms prevent the system from collision attacks or any other attacks, ensuring the data integrity of the network [2].

3. Blockchain-based systems are accessible to people with disabilities, old age, or anyone living abroad. While increasing voter turnover, some blockchain systems tally the data on the fly, where every node computes the data separately, saving costs associated with manpower and resources [12] [2].

One of the major advantages of a blockchain-based system over a conventional system is the elimination of the need for a *trusted third party or central authority*. The network can be managed by the network participants using consensus algorithms and smart contracts [5].

However, blockchain-based voting systems and platforms also faces many unresolved challenges, including finding the balance between scalability, security and decentralization (explained in section 4.3).

Studies suggest that maintaining high throughput comes with the cost of diluting the network's security, and high security lowers the network's scalability. It is still a challenge to conduct large-scale voting like national-level elections while maintaining security [6].

Although different solutions have been presented, it is a complex challenge to fully implement voter privacy while maintaining transparency in the process. Anything electronic connected to the internet makes it difficult to truly conceal network participant identity and is susceptible to malware attacks [2].

Managing blockchain networks requires expertise in multiple domains, which makes it difficult for blockchain network architects to maintain the highest level of system performance from a security perspective. Moreover, Blockchain technology increases the use of technologies, which is directly proportional to an increase in attack surface, resulting in the network's susceptibility to large-scale attacks and data manipulation [2].

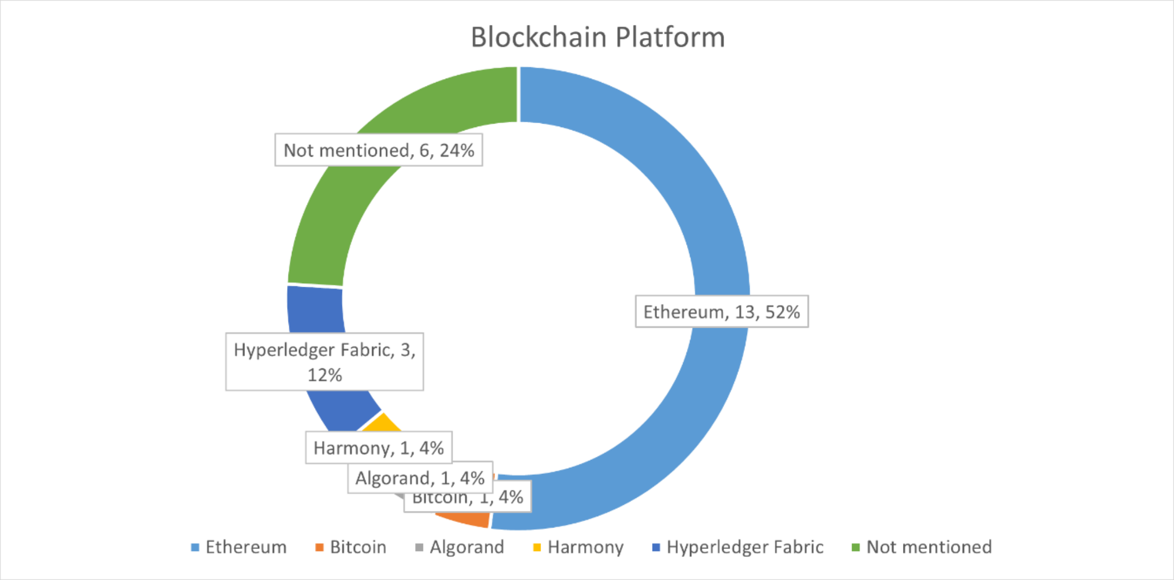
Besides the system, external factors like denial of unknown technology from public and political leaders drag the field to advance further with research and studies. Furthermore, people in powerful positions resist blockchain-based voting because it will shift away from central authorities [6].

B. R.Q2. What are the current solutions and trends in blockchain based voting?

In this section, we will summarize and categorize the state-of-the-art blockchain-based voting solutions according to their key features and problems they aim to solve. According to [5] and [3], a robust voting system should cover features such as eligibility/authentication, anonymity/privacy, auditability/reliability/transparency and security, but is not constrained to these. We further try to classify and analyze the proposed solutions based on the blockchain platform, cryptographic techniques, consensus mechanism and scalability, decentralization, coercion resistance and other key features.

After going through all the papers, we came across different voting-models that address specific aspects of a robust voting system. Among the types, one type points out a general solution that the use of blockchain and smart contracts instead of a centralized server could enable a decentralized voting environment that provides better privacy, security, and transparency.

According to [14], the foremost challenges of integrating blockchain technology and voting are speed and scalability. However, their model fails to address both issues. They explicitly do not mention what kind of blockchain platform they are using and hint at using the public Bitcoin network with proof-of-work as the consensus algorithm. This consensus protocol is energy intensive and provides a very low throughput, in turn providing very low transaction speed, *Figure 2 2.Blockchain Platform used by evaluated models*



making the proposal ineffective for scalable elections. They have stated the use of smart contracts in verification of voter, creation of block for casted vote, miner selection, and vote counting. They claim their proposed mechanism provides anonymity, integrity, privacy, security, verifiability, decentralization, singularity, and authentication. Their claim for privacy is highly doubtful because they have not used any encryption technique to not disclose the link between a voter and their vote. Also, they have implemented this system online, introducing lots of security and coercion risks.

A. Fatrah et al. [13] proposes a proof-of-concept blockchain-based voting system. Their name is misleading, as we might mistake proof-of-concept as their consensus algorithm. However, they use Proof of Authority (POA) in a permissioned private blockchain. Unlike Proof-of-Work (PoW), POA does not depend on nodes solving difficult mathematical problems. Instead, it relies on pre-selected nodes, known as validators, to validate transactions and run the consensus mechanism [citation]. This solves the problem of speed, scalability, and cost. However, electing certain on-authority nodes to validate transactions is against the very idea of decentralization and integrity. In [14], they have zero-knowledge set membership (ZKSMP) to validate ballots without revealing their content, which provides privacy. They concluded public adoption remains slow due to lack of awareness about blockchain technology.

Zhu, Hongyu et el. [15] presents, BCvoteMDE, a blockchain-based voting scheme for multi-district elections. They have implemented two-layer blockchain architecture to improve scalability and efficiency for large scale elections inspired by US electoral college system. Layer 1, known as the district blockchain, runs independently in each district with its own local blockchain. It uses lightweight consensus mechanism for fast processing of transactions to accommodate high voting participation. It uses a security algorithm called Verifiable Random Function (VRF) to randomly allocate consensus nodes to the electoral district. The second layer, the global blockchain, gathers and records the final vote counts from all district blockchains. It uses a more robust consensus method to ensure that the election results are secure, unchangeable, and protected from tampering.

Alvi, Syada Tasmia et al. [16] makes use of sidechain technology to solve the computational and storage problems. Use of sidechain reduces costs and brings scalability while maintaining Ethereum security. The proposed system uses three blockchains: a Registration Chain, a Voting Chain, and a Vote Management Chain, where the Registration Chain and Voting Chain act as sidechains to reduce the cost. Similarly, Singh, Saurabh et al. [17] proposes a theoretical implementation of a website based voting mechanism that utilizes Ethereum blockchain and smart contracts. They give a diagram of how their system's computational time is less than the existing model till now which is unverifiable since they do not tell how they assessed this computational time of different voting models. On top of that, they haven't provided assessments about the security risks associated with web-based servers.

The d-BAME: Distributed Blockchain-Based Anonymous Mobile Electronic Voting [18] scheme is designed to run large-scale elections, and aims at improving voter turnout by allowing use of smart phones and desktop applications. Their model is resistant against double voting, coercion ballot linkability, provides anonymity to voters and prevents vote manipulation. With a 4096-bit key size, casting a vote takes approximately 0.11 seconds on a desktop and less than a minute on a smartphone. It estimates that running an election for 150 million voters using d-BAME over Ethereum 2.0 could complete the casting votes phase in approximately 25

Table 4. Features of Evaluated Voting Models

Paper	Authorization/Eligibilty	Auditability/Verifiability	Anonymity/Privacy	Coercion Resistant	Scalability
[14]	Yes	Yes	No	No	No
[13]	Yes	Yes	Yes	No	No
[15]	Yes	Yes	Yes	Not mentioned	Yes
[16]	Yes	Not mentioned	Yes	Not mentioned	Yes
[17]	Yes	Yes	Yes	Not mentioned	No
[18]	Yes	Yes	Yes	Yes	Yes
[19]	Yes	Yes	Yes	Yes	Yes
[20]	Yes	Yes	Yes	Not mentioned	Yes
[11]	Yes	Yes	Not mentioned	Not mentioned	Yes
[21]	Yes	Yes	Yes	Not mentioned	No
[22]	Yes	Yes	Yes	No	Yes
[23]	No	Yes	Yes	Not mentioned	Yes
[24]	Yes	Yes	Yes	Not mentioned	Yes
[25]	Yes	Yes	Yes	Not mentioned	Yes
[26]	Yes	Yes	Yes	No	No
[12]	Yes	Yes	Yes	Not mentioned	Yes
[27]	Yes	Yes	Yes	Not mentioned	Yes
[28]	Yes	Yes	Yes	Not mentioned	Not mentioned
[29]	Yes	Yes	Yes	No	No
[9]	Yes	Yes	Yes	Not mentioned	Yes
[30]	Yes	Yes	Yes	Yes	Yes
[31]	Yes	Yes	Yes	Not mentioned	Not mentioned
[32]	Yes	Yes	Yes	Not mentioned	Yes
[33]	Yes	Yes	Yes	Not mentioned	Not mentioned

minutes. Universal verifiability allows all voters to verify that their votes have been counted properly and prevents the registrar from issuing unassigned ballots. However, it provides weak coercion resistance, as coercers can find out whether coerced votes are counted. They provide a flexible approach where an election can either prioritize full transparency and verifiability at the cost of potential coercion or prioritize voter privacy and coercion resistance at the cost of limiting individual and universal verification capabilities. Overall, this proposal seems to be robust with room for minimal changes.

Huang Jen et al. [19] proposes a self-tallying voting system with maximum voter-privacy. According to them, they have succeeded in addressing issues found in existing blockchain-based voting systems, such as limited participants, weak fault tolerance, and inadequate privacy protection. The paper introduces a method using threshold secret sharing to address the abstention problem in self-tallying voting systems. This ensures the system tallying process remains consistent regardless of voter abstention, and correct results are calculated if the number of participants exceeds a specified threshold. The system does not give receipt to the voter after they cast their ballot, preventing coercive voting and vote buying. The maximum weight on the voting system doesn't change much as we increase the number of voters proving this model effective for huge scale elections as well.
Similarly, Li Yannan et al. [20] also proposes a self tallying voting model in Decentralized Internet of things (IOT) environment. The protocol aims to satisfy four security requirements:

◦Maximal ballot secrecy: Access to partial tallies requires collusion of all remaining voters.

◦Self-tallying: Anyone can compute voting results with all ballots after voters cast them.

◦Fairness: No one has priority access to partial tallies, addressing abortive (users refusing to reveal votes) and adaptive (last voter knowing results in advance) issues.

◦Dispute-freeness: Anyone can check if voters follow the protocol.

The paper provides detailed proof for the zero-knowledge proof in the Commit phase (ZKPoK2), and notes that proofs for the other zero-knowledge proofs follow a similar structure. Experiments show that the time consumption of all algorithms is linear with the number of voters. The gas costs for online phases (Register, Commit, Vote, Tally) are also evaluated, with costs for each phase remaining below 1 USD. The time-consumption of each algorithm is tested on a laptop, mobile phone and Raspberry Pi. They aim to implement the protocol in the future on a universal scale.

The paper [11] describes an auditable blockchain voting system (ABVS) and details the application of a multi-agent system to enhance its security. Intelligent agents are computer programs that make autonomous decisions to achieve goals, interact with other agents, and react to environmental changes. Multi-agent systems consist of multiple interacting agents that cooperate to solve complex problems.
Types of Agents in ABVS:

- Authorization-Configuration Agent: Responsible for authorizing and configuring voting applications at polling stations and managing transactions between client applications and trusted nodes. It also delivers voting ballots in the form of voting agents.
- Voting Agent: Receives voters' votes and transmits them to the trusted nodes

Finally, it suggests that smart contracts could be used to implement the described intelligent agents which just means the use of smart contracts to automate the manual voting process is the intelligent agent.

Cheema Mohammad et al. [21] merges blockchain's cryptographic security with ML's intrusion detection to counter both internal (e.g., data tampering) and external (e.g., DDoS) threats. Accuracy and Area Under the Curve (AUC) were measured to evaluate the models. The results showed that both models were effective at detecting attacks. Similarly, Xu, Dongliang et al. [22] proposes a multi candidate voting model based on Hyperledger Fabric-based electronic voting model that integrates smart contracts and elliptic curve encryption for enhanced security. However, this model is better suited for small to medium sized elections as it has disadvantages in its throughput rate.

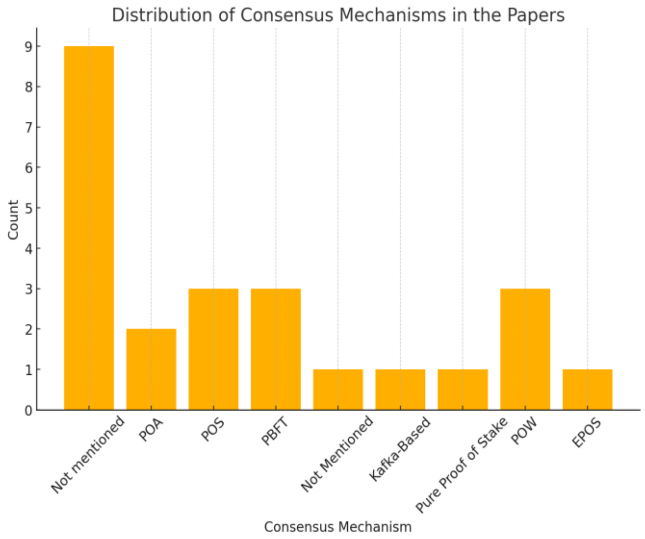
The model proposed by Luo Tianyuan [23] employs a novel proxy multi-signature scheme, based on Schnorr signatures, delegated by certificate which helps save storage space and improve efficiency. Proxy multi-signature allows a trusted proxy (like a representative) to vote on behalf of a group, but only if they're authorized by a minimum number of voters. The multi-signature scheme generates standard Schnorr signature values, making it highly compatible with blockchain systems using elliptic curves.

Christian Esposito and Chang Choi [24] uses Algorand blockchain for its scalability and security. They claim to solve the following problems in the traditional blockchain:

-No Forking: Unlike other blockchains, Algorand has near-zero probability of forking.
- Fast Consensus: Transactions are processed in less than
- Energy Efficiency: Uses Pure Proof-of-Stake (PPoS) instead of energy-intensive Proof-of-Work.

The election model is governed by Algorand smart contracts ensuring Automated verification and validation of vote. Out of 26 requirements that they listed, they have been successful in achieving 23 completely with the remaining requirement of scalability and instant auto-tallying partially achieved. The scalability factor cannot be proved until applied in a real

Figure 3. Consensus Mechanism used by evaluated models



World setting and auto tallying features might face performance issues in large scale due to API limitations. One of the additional requirements for this system is AddRQ4 "ABI implementation," which is marked as "Incomplete" in the qualitative assessment of the solution.

The scalable anonymous voting scheme over ethereum blockchain [25] has been formulated on the Ethereum blockchain towards three big bottlenecks in terms of division overflow in encryption, the time-taking tallying process, and tally failures due to "no votes" scenarios. In solving these problems, the system replaces division entirely with multiplication, removes time complexity, and allows remaining voters to cooperate with one another and recover their tally values. The system enhances scalability and saves gas compared to previous systems. Still, it faces common challenges for ballot secrecy, denial-of-service attack prevention, and even key management. This scheme extends from small-scale blockchain voting systems into the middle category.

Killer Christian et al.[26] proposes Provotom, a End-to-End Verifiable, fully decentralized, blockchain based voting system. Provotum provides E2E-V, including Cast-as-Intended, Recorded-as-Cast, and Tallied-as-Recorded verifiability. Provotum uses various cryptographic techniques to ensure the verifiability and security of its blockchain-based remote electronic voting (REV) system:

1. Homomorphic Encryption (HE), specifically the ElGamal cryptosystem, enables tallying encrypted votes without decryption
2. Distributed Key Generation (DKG) mitigates the risk of a single point of failure
3. Cooperative Decryption (CD) distributes trust in the decryption process
4. Zero-Knowledge Proofs (ZKP), including Schnorr and Chaum-Pedersen proofs, prove ciphertext validity without revealing content
5. Non-Interactive Zero-Knowledge Proofs (NIZKP), like Disjunctive Chaum-Pedersen proofs, prove that encrypted votes contain a yes or no answer without revealing the actual vote

However, this protocol does not yet offer any Coercion-Resistance or Receipt-Freeness and does not yet provide large scale scalability as Ethereum is the underlying blockchain.

Muhammad Shoaib et al. [12] provides a unique approach to the scene. They introduce plug-and-play consensus algorithms, with Proof of Work (PoW) as the default. Other consensus algorithms like Ripple, Proof of Vote, Proof of Trust, and Proof of Stake can be implemented. The framework is flexible enough to incorporate changes in consensus algorithms at run time, which helps to keep the blockchain secure and the voting activity undisrupted.

Kohal, Hemlata et al. [27] introduces a multiobjective genetic algorithm-based side-chain creation to improve the scalability and performance of blockchain-based e-voting systems. Sharding is used as a database partitioning technique to manage data faster and more efficiently by splitting it into different parts and storing it on different servers. The proposed model shows superiority when compared to a low number of e-voters, and performance increases as the number of voters increases. Similarly Yang, Xuechao et al. [28] have proposed a protocol that promises security and privacy above all. Intel SGX is CPU-based technology that protects the applications, even when the operating system has been compromised while hypervisor or BIOS is not functional. After a voter submits their encrypted vote to Intel SGX, it computes a "fingerprint" (hash value) of the encrypted vote3. This fingerprint, instead of the actual vote, is published on the public blockchain via a smart contract. Votes will never be modified because the fingerprints of the votes are kept on the blockchain. Immutability of the blockchain guarantees that these fingerprints will not change. After the election time limit when the actual encrypted votes are available, anybody could ensure if the released votes match the fingerprints kept on the blockchain.

Patrick Mccoryy et al [29] discusses a decentralized voting for a small-scale boardroom election, implementing the Open Vote Network (OV-net) protocol over Ethereum as a smart contract. The total election cost for 40 participants is $31.98, which averages $0.73 per voter. Gas measures the computation required to execute operations on the Ethereum blockchain. However, what should be noticed is this assessment was done in 2021 with Ethereum Network's gas fee being comparatively very low than now. So, the cost analysis is not valid today. Furthermore, this model is not coercion-resistant and scalable for large-scale elections.

Ivana Stančíková and Ivan Homoliak's [9] approach is suitable for privacy-preserving self-tallying large-scale e-voting. SBvote maintains the properties of decentralized e-voting, including public verifiability, perfect ballot secrecy, and fault tolerance. Gnosis and Harmony were selected as the smart contract platforms for evaluation due to their low costs and high throughput. Their evaluation determined the trade-off between the number of voters and the number of candidates, considering the platform's throughput and the cost of vote-casting transactions6. With two candidates, the system can accommodate approximately 1.5 million voters over a 2-day voting period on the Harmony blockchain. With the maximum number of 38 candidates on Harmony, maximally 216,000 voters can participate within a 5-day voting period. Furthermore, this model achieves both individual and universal verifiability. Voters can verify their vote has been recorded, and any interested party can verify the booth tally. Overall, this model is one of the most robust and complete voting systems out of all the models we have evaluated.

Tassos Dimitriou's [30] proposal focuses on Coercion Resistance and Receipt-Freeness along with the quintessential features of a voting model. Achieved through a randomizer token, a tamper-resistant source of randomness that acts as a black box in constructing the ballot. The voter does not need to take any special action or be strategic. The voter simply has no way to prove how they voted. "*All a voter has to do is vote*" is the proposal's motto. The system is practical and can be used in large-scale elections because it does not require any heavy computational power on behalf of the talliers. However, it does not consider Denial-of-Service (DoS) attacks, assuming that erroneous data can be easily filtered.

C. R.Q3. What are the challenges and security risks faced by blockchain based voting system?

Blockchain systems face an explicit trade-off between scalability, security, and decentralization[34]. To balance the performance and suitability of different consensus mechanisms and blockchain architectures is the fundamental challenge of Blockchain design [35].

Improving scalability can sometimes compromise security. For example, increasing block size to accommodate more transactions can lead to network centralization because fewer participants will have the resources to store the increased data volume [34]. Traditional Proof-of-Work (PoW) consensus protocols require decentralized consensus to be made throughout the entire network, but this limits the throughput of transactions[36] . Meanwhile, shifting to faster, more efficient consensus mechanism can lay off the very idea of decentralization of blockchain or diminish security assurances.

This trilemma in real example would be: Bitcoin prioritizes security and decentralization but has limited scalability, with a low transaction processing speed [34]. Delegated Proof-of-Stake (DPoS) systems like EOS aim for higher scalability by reducing the number of nodes involved in transaction validation, but this can lead to concerns about centralization and potential takeovers and Practical Byzantine Fault Tolerance (PBFT) improves system efficiency by having

Ceyhun Onun and Arda Yurdakul [32] proposes, ElectAnon, an anonymous ranked-choice voting protocol that focuses on anonymity, robustness, and scalability. The protocol flows fully autonomously once the election authority starts the election manually. This is achieved through timed-state machines. The election concludes with the result obtained after tallying committed votes, even if some voters fail to fulfill their required duties. ElectAnon offers solutions for scalability, including making the ranked-choice ballot independent of the number of candidates. Merkle trees are stored in batches to scale the system indefinitely with increased transactions, and zk-SNARK proofs are used for their lower computation and storage requirements. Experiments showed ElectAnon is compatible with the Avalanche network, with significantly reduced election costs due to lower gas prices. Their evaluation showed it offers an 83% to 89% decrease in total election gas consumption compared to other systems tested with 40 voters and 10 candidates. Overall, this is a very robust proposal.

According to [33], the current blockchain-based systems, including online voting platforms, are vulnerable to attacks from quantum computers because they rely on pre-quantum cryptography. The project aims to use post-quantum cryptography to neutralize potential quantum attacks on blockchain-based voting systems. It uses cryptographic algorithms that are believed to be secure against attacks by both classical and quantum computers.

only one master node responsible for generating new blocks, but its fault tolerance rate is only one third and its security needs to be improved [35]. Achieving an efficient e-voting solution via blockchain requires careful consideration of factors like block generation rate, transaction speed, and block size, which have a profound role in determining the overall performance of the solution.According to [35] if the rate of incoming transactions to the unconfirmed pool does not match the rate of confirmation of transactions to the blocks by the miners, it can result in significant performance overhead as well as delays in transaction confirmation time.

1) Problems and vulnerabilities in top of electronic voting.

"Democracy-- and the consent of the governed cannot be contigent on whether some uncheckable software correctly recorded voters' choices", Sunno Park et al. [37] strongly argues that blockchain technology, while offering potential benefits, doesn't inherently resolve the issues already present in electronic voting systems and can, in fact, introduce new security concerns. Any blockchain e-voting system still suffers from the vulnerabilities associated with electronic voting because they still have to use vulnerable devices such as mobile phones, and network infrastructures [37]. According to [37], blockchain alone do not guarantee software independence for vote casting, and along software dependence comes the threat that an undetected change or error in software could disrupt the whole election outcome without even being noticed. Security also hinges on key management. If a user loses their private key, they can no longer vote, and if an attacker obtains a user’s private key they can now undetectably vote as that user. We further encourage reader to go through paper [37] for thorough security assessments of blockchain voting models.

*2) Types of Threats according to “**Going from bad to worse: from Internet voting to blockchain voting” and “The Disruptive Blockchain Security Threats and Threat Categorization”***

a) Blockchain runtime environment threats consist of operating system threats, language threats and runtime endpoint threats. Although they are not directly related to blockchain mechanism, they are essential for online voting. Any threats to these system compromise the security of the blockchain platform. Some examples are stack buffer overflow, DNS manipulations, operating system, hardware vulnerabilities, insecure device drivers, infected systems, fork vulnerabilities, bug in smart contracts etc. [38]. Adversarial modification of a computer’s hardware, software, or equipment allows attackers to gain access to information and change the system’s operation. Polling-place electronic-only voting devices are vulnerable, even without direct connection to the Internet. Internet-connected electronic voting has also been shown to be vulnerable. Election systems have been targeted by foreign adversaries, such as the Russian government infiltrating voter registration databases [37]. Flaws might be introduced by the voting software vendor, the hardware vendor, the manufacturer, or any third party that maintains or supplies code [37]. Once a system is compromised, malware can also be injected that may prevent casting votes, deceive voters, expose voters’ choices, or degrade the experience to discourage participation.

b) Communication Protocol threats can be organized into network level threats and protocol threats. Since, its essential for node in the network to be connected with other nodes at certain interval of time. Attacks like eclipse attack, routing attack, ddos attack, sybil attack etc can be performed if security on the network layer is not implemented properly. Protocol threats consist of transaction malleabilty, refund attacks, transaction privacy leakage [38]. Online systems are susceptible to "scalable" attacks, where a single point of compromise can affect a large number of votes. These attacks can be far more dangerous than "retail" attacks affecting only a few votes. [37].

c) Consensus protocol threat deals with security of the consensus protocol module. The essence of blockchain platform is in its lack of dependency on one authority and hence, it is self operation. The self operation property of blockchain is build on top of consensus mechanism of the platform. Any threat to the consensus protocol could result in severe attacks like race attack, finney attack, vector76 attack, selfish mining, block withholding attack etc [38].

d) The second revolution of blockchain technology brought Smart Contract as a feature which proportionally increased the threats categorized as Smart Contract vulnerabilities. Vulnerabilities in contracts source code and smart contracts state comes under this category. Immutable bug, stack overflow, unpredictable state, reentrancy vulnerability are some of the vulnerabilities associated with it [38]. If an attacker can alter the election outcome without detection by voters, election officials, or auditors, the attack becomes impossible to prevent or mitigate [37].

e) Cryptographic threats consist of all the threats linked with cryptography aspect of the blockchain. With the emergence of quantum computing, certain time complexity math problems will not take that long time un securing the cryptography of the system. Any algorithmic fault or any exception cases based on mathematics give rises to algorithmic vulnerabilities. Flawed key generation, weak private, hash keys also comes under cryptographic threats [38].

f) Even if cryptography is secured, it does not prevent most systems bugs from being exploitable, and systems flaws may enable breaking cryptographic guarantees [37]. Any threats related to service, authentication, authorization, access control comes under blockchain service threat. Most of the attacks are started in the service layer. On platforms that dont rely on trusted third party, it can be challenging to implement authentication. In addition to that, there are threats related to APIs related to blockchain service layer [38].

Blockchain architecture when implemented on top of online voting system consists of many layers vulnerable to different attacks. The more technology we add to the system, the more it becomes susceptible to different attacks. Although most of the layers can be secured to some extent, online systems are never guaranteed to be 100% secured. Furthermore, implementing security on an event on the scale of national level election is harder because of all the open ends.

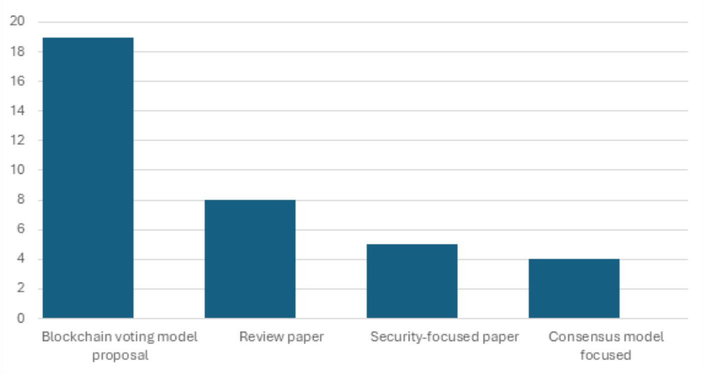


Figure 4. Paper Categorization

V. CONCLUSION

We found only a few papers that dive into consensus mechanisms and security in blockchain voting. Many studies just offered broad e-voting solutions instead. We might have missed some research since we only reviewed around 50 papers. From what we analyzed, we concluded that blockchain-based voting works best for small boardroom scenarios, atleast for now. It seems risky for significant elections where failure is not an option. We did find a few models that are close to addressing the serious security needs of voting systems. Overall, blockchain technology holds promises for improving the security and transparency of e-voting systems, but careful consideration must be given to address existing challenges and vulnerabilities. Despite the gaps, we hope to try to build our blockchain voting solution in the future that comprises all the robust and secure features.

REFERENCES

[1] M. J. H. Faruk *et al.*, "Development of Blockchain-based e-Voting System: Requirements, Design and Security Perspective," 2022.

[2] R. Taş and Ö. Ö. Tanrıöver, "A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting," *Symmetry,* vol. 12, no. 8, p. 1328, 2020. [Online]. Available: https://www.mdpi.com/2073-8994/12/8/1328.

[3] M.-V. Vladucu, Z. Dong, J. Medina, and R. Rojas-Cessa, "E-Voting Meets Blockchain: A Survey," *IEEE Access,* vol. 11, pp. 23293-23308, 2023, doi: 10.1109/ACCESS.2023.3253682.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Satoshi Nakamoto,* 2008.

[5] J. Huang, D. He, M. S. Obaidat, P. Vijayakumar, M. Luo, and K.-K. R. Choo, "The application of the blockchain technology in voting systems: A review," *ACM Computing Surveys (CSUR),* vol. 54, no. 3, pp. 1-28, 2021.

[6] 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. [Online]. Available: https://www.mdpi.com/1424-8220/21/17/5874 https://pmc.ncbi.nlm.nih.gov/articles/PMC8434614/pdf/sensors-21-05874.pdf.

[7] S. T. Alvi, M. N. Uddin, L. Islam, and S. Ahamed, "From Conventional Voting to Blockchain Voting: Categorization of Different Voting Mechanisms," 2020.

[8] S. Al-Maaitah, M. Qatawneh, and A. Quzmar, "E-Voting System Based on Blockchain Technology: A Survey," 2021.

[9] Stan\v\'kov, "SBvote: Scalable Self-Tallying Blockchain-Based Voting," presented at the Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing, 2023. [Online]. Available: https://doi.org/10.1145/3555776.3578603.

[10] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic mapping studies in software engineering," presented at the Proceedings of the 12th international conference on Evaluation and Assessment in Software Engineering, Italy, 2008.

[11] M. Pawlak and A. Poniszewska-Maranda, "Blockchain e-voting system with the use of intelligent agent approach," 12, 2019.

[12] M. S. Farooq, U. Iftikhar, and A. Khelifi, "A Framework to Make Voting System Transparent Using Blockchain Technology," *IEEE Access,* vol. 10, pp. 59959-59969, 2022, doi: 10.1109/ACCESS.2022.3180168.

[13] A. Fatrah, S. E. Kafhali, A. Haqiq, and K. Salah, "Proof of Concept Blockchain-based Voting System," presented at the Proceedings of the 4th International Conference on Big Data and Internet of Things, Rabat, Morocco, 2020. [Online]. Available: https://doi.org/10.1145/3372938.3372969.

[14] S. T. Alvi, M. N. Uddin, and L. Islam, "Digital Voting: A Blockchain-based E-Voting System using Biohash and Smart Contract," 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9214250/.

[15] H. Zhu, L. Feng, J. Luo, Y. Sun, B. Yu, and S. Yao, "BCvoteMDE: A Blockchain-based E-Voting Scheme for Multi-District Elections," 2022.

[16] S. T. Alvi, M. N. Uddin, L. Islam, and S. Ahamed, "A Blockchain based Cost effective Digital Voting System using SideChain and Smart Contracts," 2020.

[17] S. Singh, A. Singh, S. Verma, and R. K. Dwivedi, "Designing a Blockchain-Enabled Methodology for Secure Online Voting System," Jan ,, 2023.

[18] E. Zaghloul, T. Li, and J. Ren, "d-BAME: Distributed Blockchain-Based Anonymous Mobile Electronic Voting," *IEEE Internet of Things Journal,* vol. 8, no. 22, pp. 16585-16597, 2021, doi: 10.1109/JIOT.2021.3074877.

[19] J. Huang, D. He, Y. Chen, M. K. Khan, and M. Luo, "A Blockchain-Based Self-Tallying Voting Protocol With Maximum Voter Privacy," *IEEE Transactions on Network Science and Engineering,* vol. 9, no. 5, pp. 3808-3820, 2022, doi: 10.1109/TNSE.2022.3190909.

[20] Y. Li *et al.*, "A Blockchain-Based Self-Tallying Voting Protocol in Decentralized IoT," *IEEE Transactions on Dependable and Secure Computing,* vol. 19, no. 1, pp. 119-130, 2022, doi: 10.1109/TDSC.2020.2979856.

[21] M. A. Cheema, N. Ashraf, A. Aftab, H. K. Qureshi, M. Kazim, and A. T. Azar, "Machine Learning with Blockchain for Secure E-voting System," 2020.

[22] D. Xu, W. Shi, W. Zhai, and Z. Tian, "Multi-Candidate Voting Model Based on Blockchain," *IEEE/CAA Journal of Automatica Sinica,* vol. 8, no. 12, pp. 1891-1900, 2021, doi: 10.1109/JAS.2021.1004207.

[23] T. Luo, "An Efficient Blockchain Based Electronic Voting System Using Proxy Multi-signature," 2021.

[24] C. Esposito and C. Choi, "Design and Implementation of a Blockchain-based e-Voting system by using the Algorand platform," presented at the Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing, Tallinn, Estonia, 2023. [Online]. Available: https://doi.org/10.1145/3555776.3577750.

[25] J. G. Song, S. J. Moon, and J. W. Jang, "A Scalable Implementation of Anonymous Voting over Ethereum Blockchain," (in eng), *Sensors (Basel),* vol. 21, no. 12, Jun 8 2021, doi: 10.3390/s21123958.

[26] C. Killer *et al.*, "Provotum: A Blockchain-based and End-to-end Verifiable Remote Electronic Voting System," 2020.

[27] H. Kohad, S. Kumar, and D. A. Ambhaikar, "Scalability of Blockchain based E-voting system using Multiobjective Genetic Algorithm with Sharding," 02, 2022.

[28] X. Yang, X. Yi, and A. Kelarev, "Secure Ranked Choice Online Voting System via Intel SGX and Blockchain," 2021.

[29] P. Mccorry, M. Mehrnezhad, E. Toreini, S. F. Shahandashti, and F. Hao, "On Secure E-Voting over Blockchain," *Digital Threats,* vol. 2, no. 4, p. Article 33, 2021, doi: 10.1145/3461461.

[30] T. Dimitriou, "Efficient, Coercion-free and Universally Verifiable Blockchain-based Voting," *Computer Networks,* vol. 174, p. 1, doi: 10.1016/j.comnet.2020.107234.

[31] 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, doi: 10.1109/ACCESS.2021.3061411.

[32] C. Onur and A. Yurdakul, "ElectAnon: A Blockchain-based, Anonymous, Robust, and Scalable Ranked-choice Voting Protocol," *Distrib. Ledger Technol.,* vol. 2, no. 3, p. Article 19, 2023, doi: 10.1145/3598302.

[33] S. Gupta, K. K. Gupta, P. K. Shukla, and M. K. Shrivas, "Blockchain-based Voting System Powered by Post-Quantum Cryptography (BBVSP-PQC)," 2022.

[34] K. Kashif Mehboob, A. Junaid, and K. Muhammad Mubashir, "Investigating performance constraints for blockchain based secure e-voting system," *Future Generation Computer Systems,* vol. 105, pp. 13-26, 2020, doi: https://doi.org/10.1016/j.future.2019.11.005.

[35] C. Zhang, C. Wu, and X. Wang, "Overview of Blockchain Consensus Mechanism," presented at the Proceedings of the 2020 2nd International Conference on Big Data Engineering, Shanghai, China, 2020. [Online]. Available: https://doi.org/10.1145/3404512.3404522.

[36] C. Li, B. Palanisamy, R. Xu, L. Duan, J. Liu, and W. Wang, "How Hard is Takeover in DPoS Blockchains? Understanding the Security of Coin-based Voting Governance," presented at the Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, Copenhagen, Denmark, 2023. [Online]. Available: https://doi.org/10.1145/3576915.3623171.

[37] S. Park, M. Specter, N. Narula, and R. L. Rivest, "Going from bad to worse: from Internet voting to blockchain voting," *Journal of Cybersecurity,* vol. 7, no. 1, 2021, doi: 10.1093/cybsec/tyaa025.

[38] M. K. Shrivas, T. Y. Dean, and S. S. Brunda, "The Disruptive Blockchain Security Threats and Threat Categorization," 2020.