IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, May 2025
Impact Factor: 7.67

A Technology Review On Blockchain-Based E-Voting Systems

Sapana Sachin Baheti
Lecturer Computer Technology Dept.
Amrutvahini Polytechnic, Sangamner, Ahmednagar, India
sapanabaheti@gmail.com

Abstract: *Democratic voting is a crucial event in any country as the current voting scheme is through ballot paper or by use of EVM. These processes have many drawbacks such as transparency, low voter turn-out,tampering of votes, distrust in the election body, duplicating of voter id card, delay in giving out results and the most important is security issues. Security of digital voting is always the biggest concern when considering to implement a digital voting system. The security issues can be potentially solved through the use of blockchain technology. Blockchain technology offers infinite number of applications. Blockchain is a distributed ledger technology that allows digital assets to be transacted in a peer-to-peer decentralized network. A distributed ledger technology is an exciting advancement in this regard. Block is a collection of all the transactions. Blockchain possess salient features such as immutability, Decentralization, Security, Transparency and anonymity. Blockchain with smart contracts emerges as apromising candidate for building a safer, secure and transparent E-voting systems. In this paper I have tested a sample e-voting application as a smart contract for the Ethereum network using the blockchain technology through wallets and the Solidity language. Limited amount of token(gas) is given in the wallet which is exhausted when the user votes thus preventing duplicity of votes. This paper also highlights the pros and cons of using blockchain technology and also demonstrates a practical system implemented for voting and its limitations*

Keywords: Blockchain, E-voting, Smart-contracts, Ethereum

I. INTRODUCTION

Blockchain technology has been recognized as a solution for secure and transparent e-voting systems. By using the decentralization, immutability, and transparency of blockchain technology, e-voting systems can prevent fraud and manipulation, improve voter anonymity, and increase trust in the electoral process. Moreover, blockchain based e-voting systems can reduce the cost and time associated with traditional voting systems. Traditional voting mechanisms commonly rely on centralized entities, which can give the opportunity for susceptibility such as the electoral fraud. The decentralized and immutable features inherent in blockchain technology offer a promising solution to the susceptibilities related to traditional and other e-voting approaches. Blockchain technology has the ability to create a tamperproof and transparent platform for conducting e-voting. Blockchain based e-voting systems provide secure, verifiable and auditable voting procedures through the integration of cryptographic techniques and consensus protocols. The growing interest in blockchain based e-voting systems indicates the importance of a extensive and systematic evaluation of the current knowledge in this domain. One of the aims of this review is to identify the main benefits of e-voting systems based on blockchain technology through review of the previous research. These benefits include heightened security, transparency, decentralization, and privacy. Moreover, a comprehensive understanding of the technologies and implementations involved in blockchain based e-voting platforms is imperative in order to evaluate their feasibility and functionality. Furthermore, this systematic review provides technical insight into common blockchain frameworks, consensus algorithms, and security and privacy enhancing techniques used in these systems. Overall, the purpose of this

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, May 2025
Impact Factor: 7.67

review is to conduct an extensive review of the current state of the literature related to blockchain based e-voting systems. I look into the benefits,challenges, technological aspects, impacts, and potential research and development areas in the context of e-voting systems using blockchain technology. Additionally, I examine the technology implemented in these with respect to the already mentioned key concerns. The evaluation follows the PRISMA guidelines, which guarantee a rigorous and transparent methodology for the synthesis of available research data. The PRISMA protocol (Preferred Reporting Items for Systematic Review and Meta-Analysis Protocols) is a reporting guideline designed to aid researchers in the preparation and documentation of systematic review and meta-analysis protocols. **A** blockchain is a decentralized and distributed ledger made of a sequence of blocks linked to each other. Each block contains a list of transactions, and each transaction is a record of an event or action. The block header, which includes the previous block hash, timestamp, nonce, and Merkle root, identifies each block. The previous block hash links the current block to the previous one. The timestamp once, is a central part of the proof of work in the block**.** verifies the data in the block and assigns a time or date of creation for digital documents. The nonce, a number used only The Merkle root, a type of data structure frame for different blocks of data, stores all the transactions in a block by producing a digital fingerprint of the entire set of transactions. This structure provides assurance that once data are recorded in a block, they cannot be altered in the future without modifying all subsequently recorded blocks, making blockchain transactions immutable and secure.These blocks are broadcasted and replicated across a network of peers. This method is characterized by its robust security measures through cryptographic principles, which effectively mitigate the risks of manipulation and fraudulent activities. The decentralized nature of blockchain enables universal accessibility of the distributed database to all participants in the network,which is governed by a consensus algorithm. Therefore, blockchain data are immutable; it additionally traces and validates transactions based on their origins. This technique makes digital transactions transparent, secure, and tamper-proof. Considering these unique features, blockchain is an appropriate mechanism for integration with e-voting systems.

II. LITERATURE SURVEY

Studies exploring potential applications of blockchain technology in the domain of e-voting aim to evaluate its feasibility, security, and efficiency in enhancing the transparency and integrity of the election process.

Ta¸s and Tanrıöver [1] reviewed in 2020 the state of blockchain based voting research,identifying potential challenges and forecasting future directions. They presented a con-ceptual description of the desired blockchain based e-voting application and conducted a review of 63 research papers. The articles that were examined were categorized into five main categories: general, integrity, coin based, privacy, and consensus. They concluded that, whereas blockchain based voting systems can prevent data manipulation and integrity issues, the most frequently highlighted issues are scalability, cost-effectiveness,authentication, privacy, and security in blockchain based e-voting systems.

Jafar et al. [2] presented a conceptual description of a blockchain based e-voting application in addition to an introduction to the blockchain's fundamental structure and characteristics in relation to e-voting. They mentioned that whereas blockchain systems could help solve some of the issues that currently affect election systems, the authors con-clude that the most frequently mentioned issues in blockchain applications are scalability,user identity, transactional privacy, energy efficiency, immatureness, acceptableness, and political leaders' resistance.

In [3], Pawlak et al. indicated the remaining problems like security attacks, coercion,cost efficiency, and privacy that still need to be solved. The paper serves as a valuable resource for understanding the current trends and challenges in blockchain based electronic voting systems.

Huang et al. [4] in 2021 provided a comprehensive review of blockchain based voting systems, discussing their advantages, challenges, and technical innovations. They also provide a taxonomy of blockchain and identify key challenges in blockchain based voting systems such as authentication, anonymity, coercion-freeness, and auditability.

Jafar and Ab Aziz in [5] emphasized the benefits and challenges of blockchain based e-voting systems, providing useful details on probable future applications of this technology with regard to democratic processes. They demonstrated how

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, May 2025
Impact Factor: 7.67

blockchain technology offers security, transparency, and a reduced risk of fraud. However, they brought up issues with scalability, transactional privacy, and immaturity for these systems.

Devi and Bansal [6] provided a comprehensive review of the security requirements and potential threats in e-voting systems. They discuss various cryptographic techniques that can be used to secure these systems.

Benabdallah et al. [7] presented a comprehensive analysis of blockchain solutions for e-voting. They discussed the challenges faced by e-voting systems and how blockchain technology can address these issues. They also provide a comparison of several blockchain based e-voting solutions, identifying their strengths and weaknesses. The paper also addressed the limitations and issues raised by this technology, such as scalability, unpredictable attacks, weakness of the identification system, new issues raised using blockchain technology, efficiency and decentralization, the digital divide, and vulnerabilities in smart contracts.

Jafar et al. in their systematic literature review [8] discussed the challenges and solutions for scalable blockchain-based electronic voting systems, in addition to anticipating future developments. To evaluate cost and time, they identified well-known proposals, their implementations, verification methods, and various cryptographic solutions in previous research. They analyzed performance parameters, the primary benefits and limitations of different systems, and the most common approaches to blockchain scalability.

In [9], Vladucu et al. provided a thorough overview of blockchain based e-voting systems currently in use by various countries and companies, as well as those proposed for academic research. The authors discussed the challenges that blockchain e-voting systems face and identified areas for future research to improve their trustworthiness. Furthermore,they included a detailed explanation of the terminology used in blockchain based e-voting systems, such as consensus algorithms, cryptography, and system characteristics.

Implementations of Blockchain Based E-Voting Systems

In the following, several systems are presented that are presently being developed or have formerly enforced e-voting on blockchain.

• Luxoft Luxoft Holding Inc., a global IT service provider of technology results, is developing ane-voting structure that will enable the world's first exemplary vote on blockchain in Zug, Switzerland. Hyperledger Fabric was used to produce an authorized blockchain that included a network, operations, and algorithms. In order to allow choosers to cast their ballots, Zug's digital ID enrollment app grounded on Ethereum was authorized through uPort. Luxoft announces its intention to open source this technology and creates a Government Alliance Blockchain to encourage blockchain use in public institutions.

• Votem A company specializing in election operation, its main product is the CastIron platform. This platform is erected on blockchain technology and offers several distinctive features, including a distributed database, invariability, authorization- grounded access, and an inspection trail. Votem has successfully handled over 13 million choosers, serving both government choices and colorful associations in the United States and around the world. specially, their track record boasts zero cases of fraud, concession, attacks, or hacking, pressing the security and trustability of there systems.

• Voatz A blockchain- grounded mobile voting tool that was launched in 2018 in West Virginia for overseas military choosers sharing in the 2018 quiz choices in the United States. Voatz includes biometric confirmation, similar as fingerprints or retinal reviews, so that choosers validate their aspirants and themselves on the operation. A recent study set up Voatz has major security excrescencies that allow bushwhackers to cover votes and edit or block ballots in large quantities.

• POLYAS In the summer of 1996, Finland held the first POLYAS online election, with 30,000 choosers sharing in three languages. The company uses blockchain technology to offer an electronic voting system to the public and private sectors. Germany's Federal Office for Information Security granted the first online election instrument in 2016. The online voting system satisfies obscurity, delicacy, oddity, verifiability, and auditability. In Europe and the USA, several important companies employ POLYAS to manage their electronic voting systems.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, May 2025
Impact Factor: 7.67

• DecentraVote A blockchain grounded result for virtual meetings was firstly developed by a platoon at the iteratec position in Vienna. DecentraVote uses a public Ethereum network grounded on Proof of Authority agreement with permissioned validator nodes. The smart contract constructed a Merkle tree of all voting rights on- chain, and the Zero-Knowledge Succinct Non-Interactive Argument of Knowledge(zk- SNARK) generated a evidence for every voting right off- chain. DecentraVote doesnot address public political choices.

Benefits of Blockchain Based E-Voting Systems

Various studies recommend blockchain based e-voting systems due to their benefits. We compare here the benefits associated with blockchain based e-voting systems with those of traditional (e-)voting systems, in terms of the requirements listed above for e-voting. We categorize these benefits into major requirement categories, each further decomposed into several more detailed specific properties, if needed. In order to extract these benefit properties, we employed a hybrid strategy that includes both syntactic and semantic selection methods. These properties were identified as general benefits of blockchain technology and advantages offered by proposed blockchain based e-voting systems, as discussed in the related work sections of the respective literature in comparison to conventional election systems. We now list properties identified as benefits in the literature over traditional voting system types. We provide further comments on sources and explanations on each indicating how blockchains can achieve the benefits.

1. Security: a major benefit of blockchain based e-voting systems, where subcategories highlight a unique perspective:
• Integrity: holistic assurance of security aligned with the design .
• Immutability: once a vote is recorded, it cannot be altered, ensuring the voting process's finality .
• Durability: robust against data loss and ensures the permanency of stored data.
• Stability: Resistance to disruptions or manipulations like hacking. Stability is enhanced by strong encryption systems, often inherent in blockchain technology .
• Non-repudiation: a voter cannot dispute the validity of their cast vote .
2. Transparency: The blockchain based e-voting system's inherent design encourages open voting, recording, management, and counting procedures. It facilitates independent audits and ensures that all transactions (votes) on the blockchain are visible to all participants and can be independently verified.
3. Privacy: the ability of blockchain based e-voting systems to protect voters personal information and the confidentiality of their voting choices.
• Anonymity: protecting a voter's identity .
• Confidentiality (secrecy): the voters choices are private, and outcomes are not presented ahead of time .
• Untraceability: prevent the tracing of a vote back to its individual voter .
• Pseudoanonymity: voters' actual identities are masked, but their voting activities are linked to unique identifiers similar to pseudonyms or addresses .
4. Verifiability: the ability to confirm that votes have been cast as intended, stored and counted.
• Public verifiability: the ability of all to verify the entire election process .
• Individual verifiability: the ability for every voter to verify that their vote was precisely recorded and counted .
5. Auditability: ensure the voting process accuracy and truthfulness .
6. Accessibility: provide every eligible voter with an equal opportunity to participate in the voting process.
• Availability: blockchains generally ensure that voters are able to cast their votes anytime within the stipulated period without facing any issue.
• Broad turnout: technology allows substantial participation of eligible voters.
• Universal access: the ability of the system to be used effectively by all eligible voters.
7. Decentralization: Refers to the distribution of voting system authority, responsibility and operations across a network compared to a central entity. This property is fundamental to blockchain technology and is essential for enhancing confidence among citizens by minimizing control of a potentially corrupt third party .

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, May 2025
Impact Factor: 7.67

8. Usability: facilitate an extensive number of voters casting votes in accordance with their choices in an effective way while being satisfied with the process .
• Simplicity: how simple and straightforward the system is to operate.
• Understandability: clarity in system operation ensures that voters cast their votes as intended.
9. Efficiency: ability of an e-voting system to allow voters to cast votes in a swift and inexpensive manner.
• Cost efficiency: The system's capacity to carry out voting operations at a cost that is affordable. This can involve a lower-cost setup and maintenance, material distribution, and human expenses.
• Time efficiency: the system's ability to speed up voting and vote tallying.
• Performance efficiency: the ability to handle massive amounts of data (votes), process, and count votes accurately, securely, and swiftly.
10. Trustworthiness: Secure, transparent, and fair system that ensures the accurate tracking and integrity of each vote. It is a balance of rigorous security measures, prompt results, and scalability, all of which are critical to preserving trust in the voting process .
• Eligibility: only eligible voters can participate .
• Fairness: election results are not exposed before the voting process finalizes .
• Accountability: ability to determine whether or not the official vote record is inaccurate is facilitated by the blockchain
• Uniqueness: each eligible voter merits one and only one vote.
• Accuracy: each vote is precisely accounted for, ensuring there is no modification, omission, or unauthorized inclusion
• Reliability: the system's consistency in performance through time ensures accurate, error-free function and availability
11. Compatibility: ability of the e-voting system to operate in conjunction with various types of hardware, software, protocols, and legislation.
• Adaptability: ability of an e-voting system to alter or adjust in order to accommodate various circumstances or necessities that may emerge .
• Flexibility: ability to adapt to different frameworks, election types, voting methods, and voter interfaces.
12. Resistance to coercion: capacity of an e-voting system to shield voters from potential manipulations or coercions .

Challenges in Blockchain Based E-Voting Systems

Although blockchain technology brings several advantages to electronic voting, it is not universally suitable for all voting scenarios due to a range of limitations. Our goal is to examine the key challenges and limitations linked to implementing blockchain in e-voting systems, with a focus on identifying features present in conventional e-voting systems that are lacking or underdeveloped in blockchain-based approaches. As with previous sections, these challenges are grouped and ranked based on how frequently they appear in relevant studies and discussions.
1. Privacy: It encompasses efforts to protect the secrecy of everyone who casts a vote,keep sensitive voter information from leaking out, and minimize the risk of tracking individual voters. However, ensuring privacy in e-voting causes challenges due to the conflicting objectives of auditability and transparency with privacy .
2. Security: It is a crucial aspect of blockchain based e-voting systems, as it encompasses various measures to maintain the voting process's integrity, and availability. Defensive measures against cyber-attacks, Zero-Day exploits, and smart contract vulnerabilities are challenges for the blockchain security fundamental qualities. In [66], several types of attacks on blockchain such as hash-based attack, centralization attack, traffic attack, network level attack, injection attack, integrity attack, and private key leakage attack are discussed. It is necessary to mitigate such threats and prevent fraudulent use or disclosure of sensitive voter data without authorization .
3. Scalability: As voter participation and the volume of transactions grow, maintaining efficient performance and high throughput becomes increasingly important. Blockchain's core features—such as distributed consensus and permanent transaction recording—introduce inherent scalability limitations. The decentralized structure can result in slower transaction speeds and higher resource consumption. To make blockchain-based e-voting systems scalable, challenges

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, May 2025
Impact Factor: 7.67

related to transaction throughput, network capacity, and storage must be effectively managed. Addressing these issues is essential to support growing participation while preserving the security and decentralized benefits of blockchain technology.4. Technical aspects: various implementation challenges for blockchain based e-voting systems arise, encompassing algorithm restrictions, technical complexity of consensus algorithms, hardware platform compatibility, integration with existing systems, complexity of technology, interoperability (including protocol interoperability), technical limitations, transparency in certain implementations, implementation challenges, complexity of implementation, complex design requirements, automating configuration, and limitations of authentication schemes .

5. Efficiency and feasibility: This encompasses various factors, including computation resource efficiency, energy consumption, performance efficiency, cost efficiency, and feasibility. Computation resource efficiency includes minimizing computational overhead associated with the consensus protocol and effectively allocating resources to handle the increasing workload. For minimizing the operational costs of blockchain based e-voting systems, energy efficiency is crucial. The development of energy efficient protocols, algorithms, and hardware can help reduce energy consumption .

6. Acceptability and immaturity: It refers to the level of trust and confidence stakeholders have in blockchain based e-voting systems. To address this, it is necessary to achieve security, privacy, transparency, and reliability, thus building an environment that encourages the acceptance of blockchain based e-voting systems. The immaturity of blockchain technology in e-voting leads to a lack of real-world experiments, extensive testing, stakeholder engagement, and comprehensive evaluation .

7. Usability: it is necessary to achieve a balance between a user-friendly interface and the security and integrity of the voting process .

8. Coercion freeness: it refers to challenges to protect voters from external pressures or coercive influences that could compromise their right to vote freely .

9. Accuracy and Reliability: Maintaining accuracy is essential to ensure that every vote is correctly recorded and counted, free from errors or omissions. Blockchain offers a promising foundation for improving accuracy through its transparent and tamper-resistant ledger of voting activities. However, building a trustworthy and dependable e-voting system requires the development of fair protocols that eliminate double-voting and minimize dependence on centralized control. The integration of strong cryptographic methods, secure consensus protocols, and rigorous audit trails is key to enhancing the accuracy, reliability, and overall credibility of blockchain-based voting systems—ultimately safeguarding the integrity and fairness of the election process.

10. Accessibility: Access to voting opportunities is a fundamental principle. Limited internet access in certain locations presents a significant challenge to accessibility in blockchain based e-voting systems. Providing a method such as offline voting that is consistent with the overall system is complex .

11. Regulatory and Governance: Deploying blockchain-based e-voting systems necessitates compliance with existing laws and the ability to adapt to an ever-changing legal framework. Tackling legal and regulatory challenges involves navigating jurisdictional mandates, data protection laws, and election-specific regulations, all of which present significant complexities. Additionally, achieving interoperability among various e-voting solutions demands the development of unified standards and protocols to ensure smooth integration and cooperation between different stakeholders. Overcoming these governance and regulatory hurdles, including the creation of shared frameworks, remains a major obstacle for blockchain-enabled voting platforms.

12. Decentralization and Consensus Mechanisms: Decentralization in e-voting involves distributing authority, control, and decision-making responsibilities across all stages of the voting process—from voter registration to the final tally of results. Striking the right balance of decentralization is vital to enhance transparency, eliminate single points of failure, and foster trust in the system. A key factor in achieving this balance is the selection of an appropriate consensus mechanism that can validate and confirm transactions securely and efficiently. Consensus algorithms play a fundamental role in ensuring agreement among network participants and safeguarding against malicious activity.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, May 2025
Impact Factor: 7.67

Choosing the most suitable consensus method requires careful evaluation of factors like system scalability, security requirements, energy consumption, and the unique demands of the e-voting platform.

Technologies and Implementation of Blockchain Based E-Voting Systems

Blockchain-based e-voting systems incorporate a range of concepts and technologies to support secure, transparent, and reliable electoral processes. These technologies include blockchain platforms such as Ethereum and Hyperledger Fabric, consensus mechanisms like Proof of Work, Proof of Stake, and Practical Byzantine Fault Tolerance, as well as privacy-preserving tools such as homomorphic encryption and zero-knowledge proofs. In addition, robust authentication methods—such as biometric identification and digital identity management systems—are essential for verifying voter identity and upholding the system's integrity. In this section, we provide an overview of the technology landscape, organized into five main categories:

- Blockchain platforms
- Consensus algorithms
- Security and privacy techniques
- Authentication and identity verification techniques
- Other techniques (cryptography, development, testing).

Blockchain Platforms

The blockchain frameworks and technologies domain includes a variety of platforms and tools used in the design and implementation of blockchain based systems. Blockchain frameworks such as Ethereum, Hyperledger Fabric, Bitcoin, and Multichain provide the foundation required for developers to create decentralized apps. In all of the frameworks mentioned, Ethereum is the most popular choice, as evidenced by the 34.91% portion of utilized frameworks.

Consensus Algorithms

The consensus algorithms that were mentioned are illustrated in Table 5. Although a substantial number of papers do not explicitly mention the consensus algorithm used, it is reasonable to assume that for most proposed systems that use Ethereum as their framework,the consensus algorithm can be considered as Proof of Work (PoW). The following and most substantial protocol is referred to as "Proof of Work (PoW)", resulting in approximately 5.2% portion of used consensus algorithms. In the following, we provide a brief definition for each of these consensus algorithms:

1.Proof of Work (PoW): Commonly used consensus algorithm, including Bitcoin. It is a technique that requires members, known as miners, to solve computationally demanding puzzles in order to secure the network and validate transactions .

2. Proof of Stake (PoS): a consensus process in which block creators (validators) are selected depending on their wealth or stake in the network, and their possessions act as a guarantee, inciting honesty and network security .

3. Proof of Authority (PoA): A consensus approach used with authorized entities or individuals as block validators. Unlike other consensus methods, PoA is based on a predetermined set of reliable validators who proved their credibility in the network .

4. Byzantine Fault Tolerance (BFT): A technique that obtains agreement among participants even in the presence of malfunctioning or malicious nodes. BFT consensus algorithms are designed for dealing with Byzantine failures, in which nodes behave unexpectedly and inconsistently.

5. Practical Byzantine Fault Tolerance (PBFT): A specific algorithm that provides BFT in distributed systems. A leader node is selected to propose a block of transactions, which the other nodes, called replicas, validate and agree on .

6. Raft consensus algorithm: Developed for fault-tolerant log management to handle replicated logs. The Raft algorithm elects a leader to replicate logs across all nodes.The leader logs client requests and replicates them to cluster nodes. After a majority of nodes acknowledge log entries, the leader commits them and informs the followers .

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, May 2025
Impact Factor: 7.67

7. Delegated Proof of Stake (DPoS): A PoS consensus algorithm variant. DPoS relies on the PoS concept by delegating block creation and validation commitments to a selected number of trusted delegates elected through vote .
8. Crash Fault Tolerant (CFT): A type of consensus method established for distributed systems that can endure crash failures, in which nodes in the system stop responding or crash. In it, a simple majority voting method is frequently used, in which nodes vote on the proposed state or decision. The system considers a value or decision to be acceptable if a majority of nodes agree on it .
9. Stellar consensus protocol (SCP): It combines the principles of federated agreement and Byzantine agreement to offer the Stellar network with a decentralized and fault tolerant consensus mechanism. It enables nodes to agree on the state of the blockchain and keep the security and integrity of system transactions .
10. Hybrid (Proof of Credibility (PoC) combined with Proof of Stake (PoS): The weight of each vote in the consensus process is determined by the value of the tokens staked by validators through the Proof of Stake (PoS) mechanism. The method brings Proof of Credibility (PoC) to address the issue of coin collapse in the PoS consensus mechanism.This combination of PoS and PoC is a safe hybrid structure that ensures full security when deployed in e-voting systems .

Security and Privacy Techniques

The use of blockchain-based e-voting systems needs to take security and privacy into consideration. Since it is decentralized and transparent, blockchain offers the possibility to boost the trustworthiness and credibility of e-voting systems. The use of security and privacy techniques in blockchain-based e-voting systems could assist in alleviating concerns about vote tampering, manipulation, and privacy violations.
The zero-knowledge proofs (ZKPs) technique was referenced in a majority of studies. In addition, homomorphic encryption, blind signature, and ring signatures have been subject to a moderate degree of exploration. Several techniques, such as mix networks, time-lock encryption, machine learning, circle shuffle, and multi-signature schemes were briefly discussed in a few publications.

Authentication and Identity Verification Techniques

In blockchain based e-voting systems, reliable authentication and identity verification is important to protect the integrity and security of the voting process. Authentication and identity verification in blockchain-based e-voting systems play an essential duty in satisfying various important objectives, such as ensuring voter eligibility, preventing fraud,and maintaining vote secrecy .
1. Biometric authentication: This method uses an individual's unique characteristics to validate their authenticity. These qualities can include fingerprints, facial recognition,iris or retina patterns, and even voice.
2. OTP (One-Time Password): a password that can only be used for one login session or transaction, often used to give a higher level of protection to sensitive transactions or systems .
3. Aadhaar ID verification: the Unique Identification Authority of India (UIDAI) issues Indian residents a 12-digit Aadhaar number based on the resident's self-portrait, ten fingerprints, and two iris scans
4. Multifactor authentication: this is the safety mechanism that requires multiple authentication methods from different categories to validate a user's identity for a login or other transaction.
5. Multi-step authentication: a security procedure that requires a user to provide extra evidence of identification when an additional level of assurance is required.
6. PKI-based X.509: PKI-based X.509 is a widely adopted standard that outlines how public key certificates are structured .
7. Unique IDs based on hash values: this method entails creating a unique identifier by applying a hash function to the biometric data, name, and date of birth of the voters .

Other Concepts

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, May 2025
Impact Factor: 7.67

We identified several key concepts that deserve further consideration during the development and implementation of blockchain-based e-voting systems. These concepts address areas such as

- Cryptography techniques;
- Choice of development environments for smart contracts;
- Utilization of testing and benchmarking tools.

Category	Tool	Description
Smart Contract Development and Execution	Solidity	Programming language for writing smart contracts on various blockchain platforms.
	Remix	A popular web-based development environment and IDE (Integrated Development Environment)specifically designed for writing, testing, and deploying smart contracts on the Ethereum blockchain.
	RIDE language	A specific language used for developing decentralized applications (DApps) on the Waves blockchain.
Smart Contract Development and Execution	Chaincode	Smart contract code written in Hyperledger Fabric for executing transactions.
	Truffle	Development framework for Ethereum smart contracts,providing testing and deployment.
	Hyperledger Composer	Framework for building blockchain applications and smart contracts on Hyperledger.
Blockchain Development and Testing Tools	Ganache	Personal Ethereum blockchain for local development and testing of smart contracts.
	Hyperledger Caliper	Benchmarking tool for measuring the performance of blockchain systems.
Performance Testing	Gatling Performance tool	A load testing tool used to simulate and measure the performance of systems, including blockchain-based applications.
Monitoring and Visualization	Grafana Monitoring tool	A tool used for monitoring and visualizing various metrics and data from systems, including blockchain networks.
Blockchain Interaction	Metamask	A browser extension that allows users to interact with the Ethereum blockchain, manage wallets, and execute transactions.
Cryptography	SHA	A family of cryptographic hash functions used for data integrity verification and password hashing.
	Chameleon hash	A type of hash function that allows for the creation of"trapdoor" information, enabling efficient collision generation.
	Advanced Encryption	A widely-used symmetric encryption

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, May 2025
Impact Factor: 7.67

	Standard (AES)	algorithm. It operates on fixed-size blocks of data and supports key lengths of 128, 192, and 256 bits
	Paillier cryptosystem	An asymmetric encryption algorithm that allows for homomorphic operations, such as encrypted data manipulation.
	Cryptography over an elliptic curve	Encryption schemes based on elliptic curve mathematics,offering efficient and secure asymmetric encryption.
	RSA-based Public Key	A reference to the RSA encryption algorithm and key generation, which involves the use of a public key and a private key pair.
	RSA digital signature	A signature algorithm that utilizes the RSA encryption scheme for signing and verifying digital signatures.
	ECDSA(Elliptic Curve Digital Signature Algorithm)	A widely-used digital signature algorithm based on elliptic curve cryptography

III. CONCLUSION

This study is motivated by the need to comparatively assess benefits,challenges, and impacts and open future research in comparison to other types of voting systems. Furthermore, a discussion of technology aspects to address the required properties was lacking.The evolution of blockchain based e-voting systems from 2017 to 2023 has been marked by significant advancements, as evidenced by research papers from this period.Significant studies emerged, proposing a novel approach to utilizing blockchain technology for recording votes for different voting scenarios. These systems aimed to address common limitations in existing voting systems and involved a critical evaluation of popular blockchain frameworks suitable for e-voting applications. During the years, the primary research emphasis shifted towards enhancing security and developing robust frameworks for blockchain based e-voting systems. In recent years, the other aspects of e-voting systems,scalability and cost efficiency, have received more attention. Moreover, the importance of privacy-preserving protocols grew significantly, prompting the development of coercion resistant and privacy-preserving e-voting protocols.This study followed the PRISMA protocol, resulting in a selection of 252 papers. Five research questions centered on benefits, challenges, impacts, and open future research, as well as technology aspects, guided this study. To provide context, we supplemented this study of the literature with a comprehensive definition of voting system types as a framework, but also technology definitions, also extracted from the literature, in order to make the concerns better understood from an implementation perspective.The results show that blockchain technology has the potential to successfully implement e-voting systems. Transparency and auditability are seen as undisputed benefits.Security and privacy are, as would be expected for voting processes, the central properties.Here, the potential is seen in blockchain technology over other platform technologies, but whereas some specific aspects are acknowledged, both remain serious open problems,which their top rankings in the frequency lists for challenges and future directions show.An undisputed limitation of blockchains is their lack of scalability, which is the most serious non-security concern. Beyond core platform concerns, usability, verifiability, accessibility, reliability, and acceptability are properties of concern that in the wider voting systems implementation require more attention. Where evident from the studies considered, we supplemented these observations with concrete solution techniques.Therefore, this study effectively clarifies both the potential and the limitations of blockchain based e-voting systems. It achieves this by

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, May 2025
Impact Factor: 7.67

jointly integrating an analysis of fundamental properties with practical technological implementations and exploring a future roadmap, concluding in a comprehensive discussion that offers a holistic view of the topic.

REFERENCES

[1] Ta¸s, R.; Tanrıöver, Ö.Ö. A systematic review of challenges and opportunities of blockchain for E-voting. Symmetry 2020, 12, 1328. [CrossRef]
[2] Jafar, U.; Ab Aziz, M.J.; Shukur, Z. Blockchain for Electronic Voting System—Review and Open Research Challenges. Sensors 2021, 21, 5874. [CrossRef] [PubMed]
[3] Pawlak, M.; Poniszewska-Mara ´nda, A. Trends in blockchain-based electronic voting systems. Inf. Process. Manag. 2021, 58, 102595.[CrossRef]
[4] Huang, J.; He, D.; Obaidat, M.S.; Vijayakumar, P.; Luo, M.; Choo, K.-K.R. The application of the blockchain technology in voting systems: A review. ACM Comput. Surv. (CSUR) 2021, 54, 1–28. [CrossRef]
[5] Jafar, U.; Ab Aziz, M.J. A state of the art survey and research directions on blockchain based electronic voting system. In Proceedings of the Second International Conference, ACeS 2020, Penang, Malaysia, 8–9 December 2020; Revised Selected Papers2; Springer: Singapore, 2021.
[6] Devi, U.; Bansal, S. Secure e-Voting System—A Review. In Proceedings of the Hybrid Intelligent Systems, Olten, Switzerland; Porto, Portugal; Vilnius, Lithuania; Kochi, India, 12–14 December 2023; Springer Nature: Cham, Switzerland, 2023; pp. 1209–1224.
[7] Benabdallah, A.; Audras, A.; Coudert, L.; El Madhoun, N.; Badra, M. Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review. IEEE Access 2022, 10, 70746–70759. [CrossRef]
[8]Jafar, U.; Ab Aziz, M.J.; Shukur, Z.; Hussain, H.A. A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems. Sensors 2022, 22, 7585. [CrossRef]
[9] Vladucu, M.-V.; Dong, Z.; Medina, J.; Rojas-Cessa; R.Vladucu, M.-V.; Dong, Z.; Medina, J.; Rojas-Cessa, R. E-Voting Meets Blockchain: A Survey. IEEE Access 2023, 11, 23293–23308. [CrossRef]
[10] Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.;Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. Int. J. Surg. 2021, 88,105906. [CrossRef] [PubMed]
[11]Voting Technology. Available online: https://electionlab.mit.edu/research/voting-technology (accessed on 22 April 2023).
[12] Krimmer, R.; Volkamer, M. Bits or Paper? Comparing Remote Electronic Voting to Postal Voting. In Proceedings of the EGOV (Workshops and Posters), Copenhagen, Denmark, 22–26 August 2005; Citeseer: State College, PA, USA, 2005; pp. 225–232.
[13] Jones, D.W. The evaluation of voting technology. In Secure Electronic Voting; Springer: New York, NY, USA, 2003; pp. 3–16.
[14] Fischer, E.A.; Coleman, K.J. The Direct Recording Electronic Voting Machine (DRE) Controversy: FAQs and Misperceptions; Congres-sional Research Service, Library of Congress: Washington, DC, USA, 2007.
[15] Electoral Technology. Available online: https://aceproject.org/ace-en/topics/et/eta/default (accessed on 19 March 2023).
[16] Verified Voting–The Verifier. Available online: https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2024 (accessed on 19 March 2023).
[17] Oostveen, A.-M.; van den Besselaar, P. E-voting and media effects, an exploratory study. In Proceedings of the Conference on New Media, Technology and Everyday Life in Europe, Amsterdam, The Netherlands, 18–19 September 2003.
[18] Buchstein, H. Online democracy, is it viable? Is it desirable? Internet voting and normative democratic theory. In Electronic Voting and Democracy: A Comparative Analysis; Palgrave Macmillan UK: London, UK, 2004; pp. 39–58.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, May 2025
Impact Factor: 7.67

[19] Akbari, E.; Wu, Q.; Zhao, W.; Arabnia, H.R.; Yang, M.Q. From blockchain to internet-based voting. In Proceedings of the 2017 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 14–16 December 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 218–221.
[20]Kshetri, N.; Voas, J. Blockchain-enabled e-voting. IEEE Softw. 2018, 35, 95–99. [CrossRef]
[21] Tanwar, S.; Gupta, N.; Kumar, P.; Hu, Y.-C. Implementation of blockchain-based e-voting system. Multimed. Tools Appl. 2023, 1–32.[CrossRef]
[22] Gritzalis, D.A. Principles and requirements for a secure e-voting system. Comput. Secur. 2002, 21, 539–556. [CrossRef]
[23] Anane, R.; Freeland, R.; Theodoropoulos, G. E-voting requirements and implementation. In Proceedings of the the 9th IEEE International Conference on E-Commerce Technology and the 4th IEEE International Conference on Enterprise Computing,E-Commerce and E-Services (CEC-EEE 2007), Tokyo, Japan, 23–26 July 2007; IEEE: Piscataway, NJ, USA, 2007; pp. 382–392.
[24] Volkamer, M. Evaluation of Electronic Voting: Requirements and Evaluation Procedures to Support Responsible Election Authorities,1st ed.; Springer Science & Business Media: Berlin, Germany, 2009; Volume 30.
[25] Wolf, P.; Nackerdien, R.; Tuccinardi, D. Introducing Electronic Voting: Essential Considerations, 1st ed.; International Institute for Democracy and Electoral Assistance (International IDEA): Stockholm, Sweden, 2011