Grenze International Journal of Engineering and Technology, June Issue

Blockchain-Enabled Trust less and Transparent E-Voting using Smart Contracts and Consensus Mechanism

Mohit Singh Bisht[1], Sumit Pathak[2], Mohit Purohit[3] and Rosey Chauhan[4]
[1-4]Computer Science Engineering, Sharda University, Knowledge Park 3, Greater Noida, 201310, Uttar Pradesh, India
Email: mohitbisht13579@gmail.com

***Abstract*— The fundamental of democracy is voting. The process of voting must be open, safe and must be an embodiment of democracy. The development of technologies increases the need in safe and impeccable electoral systems. E.g. the paper ballot used to be subject to human error, logistic inconvenience or vote manipulation. The electronic voting machine itself is compromised on numerous occasions due to security concerns, such as cyberattacks, or insider manipulation, and questions its reliability.**

In order to maintain democracy, they need electoral systems to be updated with the technology and at the same time be reliable and trusted. The blockchain technology would present answers to the current questions regarding the integrity and reliability of the electoral process as it would offer an alternative which is more transparent, immutable and resilient and is technologically advanced.

The concept of blockchain is based on the principles of decentralization and cryptography that result in the reduction in the total dependence on central authority and the lack of the single point of failure phenomenon.

In this technology, every vote is recorded as a secure digital transaction which is stored in a common ledger and authenticated by consensus, and cannot be manipulated. It wins the confidence and loyalty of voter.

A blockchain-based smart contract-based voting system provides a system that carries out important functions automatically, such as ascertaining the eligibility of the voter, preventing or detecting fraud, and counting the votes in real-time. It is a system that has already been experimented with real elections in certain countries like Estonia, Sierra Leone and the UAE. These tests proved that blockchain will be capable of providing the voting process with increased transparency, increased security, and efficiency.

However, they also discovered several problems, including the impossibility to deal with a high number of voters, consider digital identity, and make it available to everyone and integrate it into the existing legislation.

In this chapter, the authors discuss the advantages and the disadvantages of the blockchain voting, and how it can be used to create more trust to the election process and more individuals participate in the democracy.

***Index Terms*— Blockchain Technology; Decentralization; Distributed Ledger; Cryptography; Smart Contracts; Consensus Mechanism; Transparency; Security; Digital Identity.**

Grenze ID: 01.GIJET.12.2.514_20

I. INTRODUCTION

A. Voting- A Democratic Foundation

Suffrage is an ancient, important feature of democracy. It is through it that citizens are given the first choice in which they elect their representatives, are given a chance to influence their policies to the masses, and keep the government responsible to them. Ideally, the voting process is an indicator of equality, inclusiveness, and free choice, where every individual is represented on the direction of the community. Still, although, the notion that the idea of the voting is regarded as one of the most important concepts, the adequate functioning of the voting systems is often not noticed.

The most common forms of voting systems are paper based systems that are popular in most regions of the world but have many drawbacks [1]. Not only are they time-consuming but also expensive to manage, but are prone to human errors, ballot manipulations, transportation delays and counting delays. The new solution to these problems in the United States, Brazil, and India, among others, was the electronic voting machines (EVMs). These systems were supposed to be more efficient and many new risks were also caused. This has made most people develop mistrust due to the lack of proper auditing, hacking, malfunctioning software and disputed election outcomes.

B. Issues in Traditional Voting Methods

On a more intense examination of the current systems, there are still areas of persistent issues that directly influence the backbone of democracy [2].

- Transparency-based: In paper-based and electronic voting systems, voters can have only a few methods of assessing whether their vote has been recorded and counted properly. This is not all verification, particularly when elections are in close contests, which leads to more questioning and distrust by voters.
- Security inquiry: The electronic voting machines and centralized systems have single points of failure. Any attack or failure of these systems may impact the entire election. Due to this, some countries, such as France and Germany, have minimized or halted the utilization of electronic and online voting.
- Verification difficulties: Although certain EVMs generate a paper record, elaborate audits are challenging to conduct, consume a large amount of resources, and usually create disagreements.
- Maintenance cost: EVMs are expensive to maintain, and their operating costs are high and demand frequent upgrades, whereas the management of paper ballots demands a big and complicated infrastructure.
- Remote voter concern: The citizens that live in remote areas, foreign citizens, and migrants usually lack proper methods of voting, thus leading to injustice in the democratic process.

They are not the only technical issues, and they lead to a lack of trust among the people. Failure by voters to be convinced that an election system is just and effective may undermine legitimacy of governments.

C. Blockchain - An Unsettling Alternative

The advent of the blockchain technology in the digital age has created a new and novel way of considering elections.

This is a technology that is referred to as blockchain that was first created in 2008 to support Bitcoin even though over time it has experienced numerous extensions to other industries such as finance, healthcare, government services and supply chain management [3]. Most simply, blockchain is described as a safe and unchangeable document system based on the digital world, and the data are stored in a huge number of computers.

The long-standing problems with the voting system may be tackled by blockchain by enhancing the security, transparency, and efficiency:

- Fixity: Once the votes have been counted, they are not able to be deleted or altered, and hence it is assured that they are really truthful.
- Subsidiarity: The absence of single points of failure occurs in the event that the power is spread across many nodes.
- Transparency: The tally can be checked by the public, and also there is a higher confidence when citizens check the tally of votes on their own.
- Cryptography: The privacy of the voter identity and the ability to verify ballots are offered by such techniques as homomorphic encryption and the zero-knowledge proofs.
- Smart Contracts: The polls are able to automatically add the votes, remove the possibility to vote the same way as well as make sure the rules are fulfilled without the human interference.

The preliminary experiment shows that blockchain has a high potential. The digital governance is founded on the application of blockchain in Estonia to protect the records of the citizens. In Sierra Leone, national elections were additionally conducted using blockchain to increase transparency [4].

D. This Chapter's Goals and Purpose

The next chapter attempts to provide a detailed discussion of the concept of blockchain-based voting systems and the way it is able to revolutionize democracy in the digital era. In particular, it will:

- Understand the basic blockchain technologies such as smart contracts, consensus mechanism, and cryptography, that are employed to run safe and transparent elections.
- Evaluate practical tests and examples of the international practice to get to know what is good and what is bad.
- Disclose the problems and the problems that have not been tackled, such as the usability, verifying the identity of a voter, scalability, preventing coercation and supporting legal frameworks.
- Provide an equal treatment on how blockchain would empower democratic involvement and social,
- ethical, and law issues.

II. The Technological Underpinnings of Blockchain Voting Systems

A blockchain-based voting system is based on robust technology and democracy. In comparison with the conventional electronic voting system, blockchain voting makes use of distributed ledgers, smart contracts, cryptography, and secured authentication to offer transparency, data integrity, and voter privacy [5].

A. Design Justification and Security Objectives

Blockchain voting would satisfy the most important election demands of voter eligibility, one person-one vote, ballot secrecy, end-to-end checking, accuracy, fairness, and availability of the system by eliminating single points of failure that are present in centralized electronic voting systems. This translates into:

- Robust authentication that ensures only registered voters can participate once.
- Ballots that are cryptographically protected to ensure that choices are kept secret.
- Tamper-evident storage and public auditability of the count path.
- Transparent rules encoded in smart contracts.

B. System Basic Buildup Model (A Four-Unit Model)

The majority of designs divide the election process into four collaborative units that are held together by the blockchain ledger:

- Unit of Registration: The candidates and the voters are registered by the officials of the election. Only privacy-preserving
- The chain is touched with references, and the eligibility is usually stored in off-chain registries. proofs and PII.
- Unit of Authentication: In the system, a one-time authorization to vote during the polling time is issued. checking the given qualifications.
- Voting Unit: The process of voting is on-chained. The contract is enforced by one of the qualified.
- voter, one counted ballot.'
- Tallying and Publication Unit: The outcomes of the election are also published at the conclusion of the election with the help of authorised tally keys.

C. Blockchain Layer Platform

Etherium has an elegant model of smart-contracts (Solidity + EVM) that natively represents election rules as a verifiable, deterministic, and executable byte-code and includes a full developer stack, which it is the focus of most prototype systems [6]. Even though public networks offer the benefit of decentralization at the cost of gas and privacy, private test nets (Ganache/Geth) can be used when repeating an evaluation.

D. Smart Contracts

Election Factory/Registry that is normally included in the family of the ballot contracts. The elections are indexed, and the metadata is developed and saved.

- Oracle of Voter Roll: Ensures that a derived token of or address has not done so but is eligible to vote.
- Ballot Contract: Re-submission of blocks, and Audits in progress, and accepts one ballot of every qualified voter.

- Tally/Result Agreement: Produces a canonical record which is uncountable in-contract votes and external tally.

E. Using Cryptography for Verifiability and Privacy

Ballots are public key-encrypted using the election authority key: the tally holders decrypt the ballots once the polls have ended[7]. Additively homomorphic schemes of prototypes have a low cost in an attempt to achieve end-to-end verifiable trust. Blind signatures are used to make the eligibility.

F. The Developer, Middleware, and Client Stack

Modern App/ Web stacks are better to use in a prototype:
- Front-end React/JS constructs the connections to provide communication with the node providers and a wallet to manage key management.
- Local chain and wallet: Ganache has a local chain which it can be used in deterministic testing, Truffle has control, migrations Metamark sign.
- Off-chain services: Metadata and records of registration that are not sensitive and stored by RDBMS. (MySQL/PostgreSQL).

H. A Technical Reference Blueprint

A voting machine based on blockchain has six important steps:
- Prewar political - The contract concerning the election was concluded, the list of candidates was announced and tacked up by the organizers' voter roll.
- Voter sign-in – Each voter proves who they are using their digital wallet (and maybe biometrics).
- Casting a ballot – The voter's choice is encrypted and sent to the blockchain as a transaction.
- Securing the record – The blockchain locks in all ballots permanently using its consensus process.
- Counting votes – When polls close, authorized parties decrypt or compute the totals.
- Checking the results – Anyone can audit the process: totals match the on-chain ballots.

III. E-VOTING: AN EVOLVING PARADIGM

E-Voting system is basically based on voting system in which we use electronic devices to cast, record or count votes.
Electronic Voting can be defined as the voting that is supported by any electronic hardware and software [9]. E-voting system contains three aspects: registration authorities, voters, tallying authorities.

A. Types Of E-Voting Systems

- Punch-card: Developed in the 1960s, voters are given a punch card with small dots then punches hole in front of their respective candidate.
- Direct Recording Electronic (DRE): Voters cast their votes directly into computer memory. Voters interact through DREs using push buttons, touchscreens, or dials.
- Optical scanning systems: Voters mark their votes on machine-readable ballots then it is scanned by an optical reader which counts the votes.
- Ballot-Marking Devices (BMDs): Presents ballots electronically where voters can cast votes then it produces a human readable paper.
- Internet Voting: Qualified voters cast their votes through internet voting from anyplace remotely from a protected online portal.

B. Requirements of E-Voting Systems

Functional Requirements
- Voter Authentication: The system must check that only the registered and verified voters can cast a vote.
- Vote Casting: The System must allow the voters to select their preferred candidate.
- Vote Recording: Each vote must be logged securely without change or loss.
- Vote Communication: Votes must be communicated securely using encoding.
- Vote Counting: The system must count the votes and give the result timely.

Security Requirements
- Secrecy: The actual vote should not be connected with the personality of the person who casts it.
- Integrity: The cast votes should be unaltered.

- Authentication: only the registered voters are allowed to cast the vote, and only one person is allowed to cast a vote.
- Verifiability: The voter can confirm his vote that no one is cheating on it.

Legal and Regulatory Requirements
- Compliance: The system must be compliant with the provision and regulations of the election commission.
- Transparency: The system will be subjected to a third party testing and certification.
- Accountability: Working on the design, implementation and maintenance should be evident.

Usability Requirements
- Accessibility: It has to be accessible to all forms of voters such as the old and the physically challenged.
- Convenience: The voting must be convenient and easy to use.
- Multilingual Support: The interface should be offered on many languages.

C. Process of Electronic Voting
- Voter Registration: The citizens are registered in the voter database through Aadhaar or biometric verification.
- Checks and Log in: Voter has to identify himself or herself by fingerprint verification or retina scan.
- Ballot Casting: The voter is provided with an online ballot of the list of contenders.
- Vote Encryption: Votes are encrypted directly with the help of cryptography to achieve confidentiality.
- Vote Counting: The system is the one that counts the votes without the identification of the voter.
- Result Declaration: Results have been presented in a verifiable way.

IV. PROOF OF CONCEPT (POC)

In order to validate the feasibility of the proposed blockchain-based electronic voting system framework, a proof of concept (PoC) has been implemented based on the Ethereum blockchain and smart contracts. The PoC essentially showcases the potential of the proposed system by integrating the blockchain infrastructure and the associated consensus and authentication protocols. The primary objective of the proposed PoC is to validate the feasibility of the proposed system by showcasing the potential of the proposed system for the execution of the entire election process by employing smart contracts while ensuring the integrity and transparency of the entire system and the trust of voters.

In the proposed system, the voting and result computation processes are carried out by the authority. In the proposed system, the entire voting and result computation processes are carried out by the authority.

The proposed system has been implemented by integrating the client application and the blockchain-based smart contracts.

A. Components of System Architecture

The architecture of the proposed system for proof of concept follows a layered model that connects user interaction components with blockchain infrastructure. As shown in Fig. 1, the system's architecture is comprised of four main components: the user layer, the client-side application layer, the smart contract layer, and the distributed ledger layer.
- User Layer: This layer comprises individuals using the voting system, such as administrators and voters. Administrators manage activities such as initializing election campaigns, managing candidate information, and governing the election process. Voters, on the other hand, take part in the voting process by accessing the voting interface. All user activities are authenticated using blockchain wallet credentials, where each transaction is digitally signed using cryptographic keys. This ensures that all activities submitted to the blockchain network are securely verified, thus preventing unauthorized activities while providing accountability and traceability.
- Client-Side Application Layer: This offers a platform through which users can interact with the blockchain technology-based voting system. For this purpose, in the context of the proposed proof of concept, this layer has been developed through the use of the Next.js framework, which offers a responsive user interface through a web application. Moreover, this application has been integrated with a digital wallet known as MetaMask to manage user identities as well as securely sign blockchain transactions. For this purpose, the application has been developed through the use of the Ethers.js library to communicate with the blockchain network.

- Smart Contract Layer: The smart contract layer is the core component of the voting system, and it is here that the voting process is controlled. In the proposed system, there are two smart contracts that are implemented: the Factory Contract and the Campaign Contract. The Factory Contract is a registry that manages the deployment of the election instances. This means that administrators of the system will be able to create new elections. Each election will have a separate contract referred to as the Campaign Contract. The contract will manage the details of the candidates and the voters. It will also prevent voters from voting more than once.
- Distributed Ledger Layer: This is the layer that can be stated as the blockchain of Ethereum, in which all the voting transactions are recorded. are recorded. Anytime a voter makes a vote, it has become a transaction that has to make through. a validation mechanism through consensus mechanism, and by the time it is added to a block. After that, the transaction cannot be altered and deleted. This decentralized form of a ledger provides transparency, reliability, and responsibility, so that the observers can confirm the. election and the voting procedure via blockchain.

The entire communication between the user layer, client-side program, the smart contracts, and the Ethereum blockchain constitutes the entire decentralized voting architecture. The interaction and data exchange between these parts is depicted in Fig. 1, which creates the visual connection of how users are interacting with the web interface, ushered together by blockchain wallets and transmitting to smart contracts running on Ethereum net blockchain.

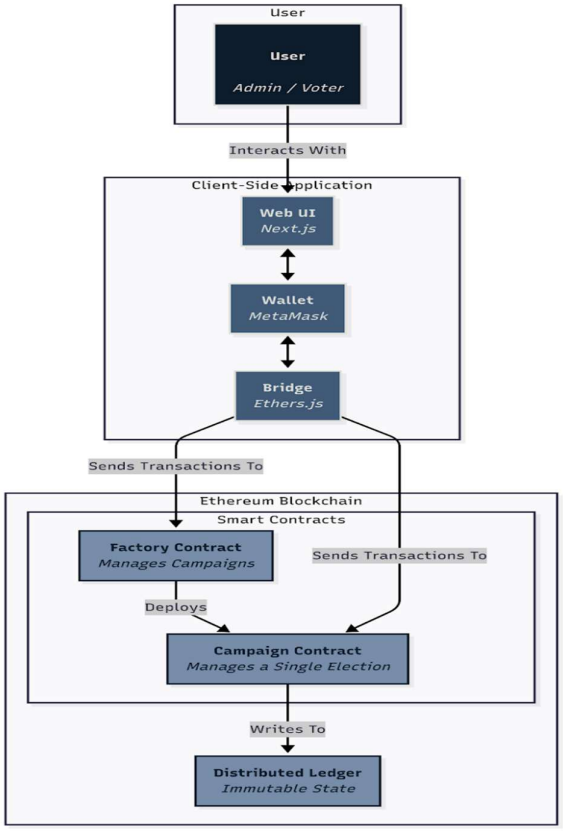

Fig. 1. System Architecture Diagram

B. Workflow and Interactions

The follow-up flow of the intended blockchain-based voting system consists of different sequential interactions among users, client machine-based applications, smart contracts, and the Ethereum blockchain system. Since this workflow allows the execution of all the phases of the voting process, including the initiation, the counting of votes, etc., to be conducted in a secure, transparent, and verifiable manner. The voting process has three major stages: election deployment, voting, and finalization of results.

- "Phase I: (Election Deployment): Phase I is the first phase in the election process, and the administrator initiates it by launching the deployment through the client interface. The web application interface enables the administrator to establish the rules of the election, such as the information about the candidates. After a configuration is made, a transaction involving a blockchain is formed by the client interface and calls the createCampaign() command of the Factory Contract. The blockchain wallet of the administrator is used to include a digital signature of the transaction provided through the MetaMask interface and forwarded to the Ethereum blockchain with the help of the Ethers.js communication bridge. After the transaction has been authenticated on the blockchain, the Factory Contract forms a new Campaign Contract, which is the instance of the election. The address of the new instance of the election is recorded in the registry on the blockchain, which can never be changed.
- Phase II (Voting Process): It is a process where the voters engage the system via the voting interface that the web based system provides. The client application presents the voter with a ballot upon which the voter selects the choice of candidate. When the client application is validated, a transaction is created which executes the vote () method of the Campaign Contract. The voter then signs this transaction digitally through the MetaMask wallet, which authenticates that the voter is in possession of a unique address on the blockchain. Lastly, the signed transaction is sent to Ethereum network as the smart contract verifies the vote by determining whether the voter has already cast a vote in the vote. In case the voter is authentic and has never voted previously, the smart contract documents their vote, and it increases the corresponding vote tally of the candidate they elected. Lastly, a consensus algorithm is used to verify this transaction, and it ensures a permanent recording of the vote in the distributed ledger, such that they cannot be changed or deleted.
- Phase III (Result Finalization): Once the voting process ends the result finalization phase is achieved in which the outcome of the election is calculated. Activating the client interface, the administrator initiates a procedure named tallyVotes which is a procedure of the Campaign Contract. This operation will determine the number of votes each of the candidates got based on the votes cast on them as per the voting record stored in the smart contract. Finally, these results are written to the blockchain as part of a confirmed transaction, thus creating a permanent record of the results of the election. These results are then retrieved by the client application, which then presents them to users through a web interface. Since the computation of votes is done within the smart contract, there is no scope for manipulation of votes.

The sequence of interactions between users, the client application, the Ethereum blockchain, and smart contracts is illustrated in Fig. 2, which depicts the step-by-step electoral workflow and the communication flow between the system components during election deployment, vote casting, and result computation.

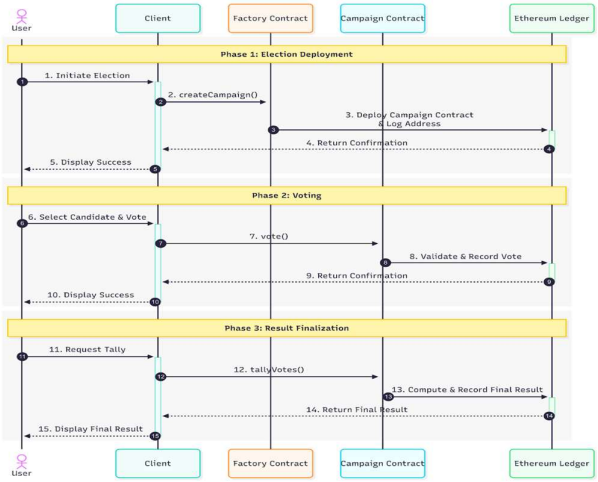

Fig. 2. Electoral Workflow Diagram

V. Recent Advancements

Luo et al. [13] suggested a blockchain-based voting system based on proxy multi-signatures, which reduces storage and provides more scalability of the system. On the review by Ohammah et al. [14], blockchain was considered as a cheaper and safer means of voting. Kaveri et al. [15] invented a biometric blockchain system of

voting, which allows individuals to authenticate their identities with the help of Aadhaar. Abdulah et al. [16] developed an Ethereum based voting system in smart contracts. Singh et al. [17] offered a blockchain-based methodology of voting at online with Ethereum smart contracts. Joni et al. [18] proposed a hierarchical blockchain, HAC-Bchain, which is a shard-based blockchain. Gnanapriya et al. [19] suggested an e-voting system based on Ethereum smart contracts. Rahi et al. [20] gave an overview on a computer security viewpoint. The model that was suggested by Shadab et al. [21] is an Indian-centered model that incorporates Aadhaar card authentication. O et al. [22] proposed an insecure e-voting platform based on Next.js and Solidity on the Polygon blockchain. Shakir et al. [23] developed a blockchain voting system integrating biometric authentication. Singh et al. [24] reviewed various blockchain e-voting frameworks. Prasad et al. [25] explored a private Ethereum-based e-voting system. Mahalakshmi et al. [26] advanced the field by proposing a decentralized Ethereum smart contract system. S et al. [27] implemented 'Snap Vote,' an Ethereum blockchain application. Pachorkar et al. [28] reviewed blockchain's decentralization, immutability, and auditability as key features. The recent advancements have been summarized in Table I.

TABLE I. SUMMARY OF RECENT ADVANCEMENTS

Author	Year	Contributions
Luo et al.[13]	2021	Proposed proxy multi-signature scheme to reduce storage overhead and improve efficiency in blockchain voting.
Ohammah et al.[14]	2022	Survey analyzing blockchain voting models, highlighting trust, transparency, and security challenges in Africa.
Kaveri et al.[15]	2022	Suggested a biometric blockchain e-voting framework enabling secure vote casting, voter verification via Aadhaar, and transparency.
Abdulah et al.[16]	2023	Designed Ethereum-based voting using smart contracts ensuring transparency and cost analysis.
Singh et al.[17]	2023	Proposed decentralized voting using Ethereum smart contracts with end-to-end verifiability.
Joni et al.[18]	2023	Introduced HAC-Bchain using hybrid consensus and category-based sharding for scalable e-voting.
Gnanapriya et al.[19]	2023	Proposed Ethereum-based e-voting system using smart contracts for secure, transparent elections.
Rahi et al.[20]	2023	Overview of blockchain in e-voting showing how Ethereum enhances transparency and authentication.
Shadab et al.[21]	2023	Proposed blockchain-based e-voting for India integrating Aadhaar card authentication.
O et al.[22]	2024	Developed secure e-voting for Nigeria using Next.js + Solidity on Polygon blockchain.
Shakir et al.[23]	2024	Built blockchain e-voting with biometric authentication and proof-of-work.
Singh et al.[24]	2024	Reviewed blockchain-based e-voting systems, highlighting strengths and noting scalability issues.
Prasad et al.[25]	2024	Developed private Ethereum-based e-voting with Proof-of-Authority consensus.
Mahalakshmi et al.[26]	2024	Introduced decentralized blockchain voting using Ethereum smart contracts.
S et al.[27]	2025	Implemented Ethereum-based 'Snap Vote' with smart contracts.
Pachorkar et al.[28]	2025	Review analyzing blockchain's role in e-voting with focus on decentralization.

VI. CONCLUSION AND FUTURE DIRECTIONS

In this paper, we analyse about the blockchain-based electronic voting system and suggest an efficient workflow and structure of an e-voting system using blockchain. E-voting system using blockchain is the future. E-voting system using blockchain provides efficiency and a less tamper-proof environment. By the help of e-voting system every person can vote by sitting in their homes using internet. It helps the people with disabilities to vote without going to the vote station. Blockchain in e-voting provides immutability and transparency that add to security and reliability in voter registration. Blockchain with e-voting provides efficiency, scalability and rightful use of resources. E-voting system gives more efficiency and lower error rates. In this paper we suggest a decentralized blockchain based voting system. We suggest an architecture with a hybrid model designed to balance the robust security of on-chain logic with the usability of an off-chain client. We also give our architecture workflow where we suggest three phases. E-voting using blockchain technology is the hope of the future for a better and secured voting environment. In regard to future direction, there is also scope of improvement by the integration of Zero-Knowledge Proofs (ZKPs) which allows for advanced, privacy-preserving attribute verification without revealing personal data. We can also implement a migration to Layer-2 scaling solutions and a cross-chain oracle network to use it as an authenticator of identity across multiple ecosystems, ensuring scalability and sustainable governance through a DAO.

REFERENCES

[1] S. T. Alvi, M. N. Uddin, L. Islam, and S. Ahamed, "A privacy-aware digital voting system employing blockchain and smart contracts," 2020 IEEE CSDE, pp. 1–6, 2020.

[2] N. B. Al Barghuthi et al., "An analytical view on political voting system using blockchain technology," 2019 Sixth HCT ITT, pp. 132–137, 2019.
[3] D. Arora, Ruchi, and V. Wasson, "Blockchain based voting decentralized application," 2023 14th ICCCNT, pp. 1–6, 2023.
[4] N. S. Varma Indukuri et al., "Blockchain-based voting system in a democratic environment," 2023 ICAISS, pp. 1312–1316, 2023.
[5] H. Dudeja, J. Kaushik, and Shalu, "Cloud based voting system using Blockchain technology," 2023 ICAC3N, pp. 1392–1396, 2023.
[6] A. M. Al-madani et al., "Decentralized e-voting system based on smart contract," 2020 ICSIDEMPC, pp. 176–180, 2020.
[7] S. Joseph et al., "Ether vote: Revolutionizing elections with blockchain-powered electronic voting system," 2023 SMART GENCON, pp. 1–7, 2023.
[8] E. Chovancová et al., "Online voting management system based on Blockchain," 2023 IEEE INES, pp. 000169–000174, 2023.
[9] A. A. Othman et al., "Online voting system based on IOT and Ethereum Blockchain," 2021 ICTSA, pp. 1–6, 2021.
[10] G. Pranitha et al., "Utilization of blockchain in e-voting system," 2022 CONIT, 2022.
[11] M. Hajian Berenjestanaki et al., "Blockchain-based e-voting systems: A technology review," Electronics, vol. 13, 2023.
[12] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[13] G. Luo et al., "A blockchain-based voting system with proxy multi-signature," 2021 IEEE Int. Conf. on Blockchain, pp. 1–6, 2021.
[14] O. Ohammah et al., "Blockchain voting models: A survey," 2022 Int. Conf. on Cyber Security, 2022.
[15] K. Kaveri et al., "Biometric blockchain e-voting framework," 2022 Int. Conf. on Computing Technologies, 2022.
[16] A. Abdulah et al., "Ethereum-based voting using smart contracts," 2023 Int. Conf. on Blockchain Applications, 2023.
[17] R. Singh et al., "Blockchain-enabled online voting methodology," 2023 Int. Conf. on Smart Technologies, 2023.
[18] J. Joni et al., "HAC-Bchain: A shard-based blockchain with hierarchical consensus," 2023 Int. Conf. on Distributed Systems, 2023.
[19] C. Gnanapriya et al., "Ethereum smart contract–driven e-voting system," 2023 Int. Conf. on Smart Computing, 2023.
[20] P. Rahi et al., "Blockchain in e-voting: A computer security perspective," 2023 Int. Conf. on Cybersecurity, 2023.
[21] M. Shadab et al., "Blockchain-based e-voting for India with Aadhaar authentication," 2023 Int. Conf. on Emerging Technologies, 2023.
[22] O. O et al., "Secure e-voting using Next.js and Solidity on Polygon," 2024 Int. Conf. on Blockchain Technology, 2024.
[23] S. Shakir et al., "Blockchain voting with biometric authentication," 2024 Int. Conf. on Digital Identity, 2024.
[24] P. Singh et al., "Review of blockchain e-voting frameworks," 2024 Int. Conf. on Electronic Voting, 2024.
[25] S. V. Prasad et al., "Building voting systems for a fairer future," 2024 IEEE ICBDS, pp. 1–7, 2024.
[26] M. Mahalakshmi et al., "Decentralizing voting: Blockchain based e-voting using Ethereum Smart Contracts," 2024 ISCS, pp. 1–7, 2024.
[27] M. G. S et al., "Design and implementation of a blockchain-based secure electronic voting system," 2025 ICICI, pp. 584–590, 2025.
[28] P. R. Pachorkar and S. Ponnusamy, "Exploring blockchain technology for Secure Electronic Voting Systems," 2025 ICCSAI, pp. 1321–1330, 2025.