Journal of Information Systems Engineering and Management
2025, 10(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Decentralized E-Voting and Governance System Using Blockchain

Dr. Thanga Revathi S[1], Dr.A.Gayathri[2], Dr.A.Sathya[3]

[1]*Dept. of Networking and Communication, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India. thangarevathi84@gmail.com*

[2]*Department of CSE, Saveetha School of Engineering Tamil Nadu, India. gaybalahari@gmail.com*

[3]*Department of Artificial Intelligence and Data Analytics, Sri Ramachandra Institute of Higher Education and Research, TamilNadu, India*

ARTICLE INFO

Received: 01 Oct 2024
Revised: 30 Nov 2024
Accepted: 10 Dec 2024

ABSTRACT

A democratic form of governance is the fairest and most effective system of authority in the human society. A key feature of any democratic authority is free and fair elections. However ensuring free and fair elections is an arduous task due to corrupt political practices, irresponsible management and human error. Using modern technologies like blockchain, can be an effective approach to reduce any intentional or unintentional attempt to sabotage the voting process. In this paper we lay out an overview of the methodology we propose for an efficient execution of the blockchain based voting system.

Keywords: blockchain-based voting, electronic voting systems, voter privacy, security, id verification, remote, trust, modern technology

INTRODUCTION

Blockchain technology, renowned for its decentralized and immutable nature, stands as a transformative solution in revolutionizing the conventional voting landscape. By leveraging blockchain in electronic voting systems, a paradigm shift emerges, addressing fundamental concerns plaguing traditional methods. Blockchain's decentralized ledger serves as an incorruptible record of votes, ensuring transparency and immutability throughout the process. Each vote, cryptographically sealed and time-stamped, finds its place in a chain of blocks, rendering alterations practically impossible. This not only fortifies vote integrity but also instills trust by enabling a transparent tally-keeping mechanism.

The essence of voter anonymity finds its stronghold in the integration of Zero-Knowledge Proofs (ZKPs) within blockchain-based voting systems. This cryptographic technique allows a voter to authenticate their eligibility and cast a valid vote without revealing the specifics of their choice. It grants the ability to prove the possession of certain information (the right to vote) without disclosing the content itself, ensuring absolute privacy while preserving the vote's legitimacy. ZKPs, thus, empower individuals to participate in the electoral process confidently, knowing their identities remain shielded while contributing to the tally.

Moreover, the inherent attributes of blockchain technology bolster the overall integrity of the voting process. The decentralized nature of the network and its consensus mechanisms deter any attempts at tampering or manipulation. With each transaction (vote) linked in a chain and encrypted, altering historical records necessitates consensus among the network's majority, a near-impossible feat. This immutability guarantees that once a vote is cast and recorded, it remains unchangeable, reinforcing the sanctity of the electoral outcomes.

Tally keeping, a cornerstone in election credibility, undergoes a profound transformation with blockchain. The distributed ledger system ensures that all nodes within the network possess an identical copy of the vote ledger. This redundancy safeguards against data loss or centralized manipulation. The cryptographic hashes, serving as digital fingerprints, further fortify the integrity of each vote, making the entire process resilient to unauthorized modifications.

The integration of Aaadhaar credentials within a blockchain-based voting system offers a unique avenue to combine identity verification with the inherent security of blockchain.

Aaadhaar, being a biometric-based identification system in India, can potentially enhance the authentication process while maintaining voter anonymity through a careful application of the technology.

In this hybrid approach, Aaadhaar credentials could be utilized during the initial voter registration process, allowing for the verification of a citizen's eligibility to vote. Once verified, a cryptographic key or unique identifier, detached from personal information, can be generated and linked securely with the individual's vote. This linkage ensures that a vote can be traced back to a legitimate voter without revealing the voter's identity or choice. The combination of Aaadhaar with blockchain enhances the trust and transparency of the voting process. However, it's crucial to implement this hybrid system while addressing privacy concerns and ensuring that the Aaadhaar information remains segregated from the actual vote cast. Utilizing cryptographic techniques, such as hashing or encryption, can help anonymize voter data while enabling traceability for auditing purposes.

Furthermore, employing a permissioned blockchain network could offer an additional layer of control over who can access the information associated with Aaadhaar credentials, ensuring that only authorized entities, such as election authorities or auditors, have the necessary permissions to trace votes back to specific voters, if required for verification or auditing purposes.

This hybrid model, merging Aaadhaar credentials with blockchain technology, holds the potential to reinforce the authentication process, provide traceability, and maintain the secrecy of votes in an electronic voting system. It could offer a nuanced balance between identity verification and voter anonymity, thereby contributing to a more robust and accountable electoral framework. However, the implementation of such a system would need to navigate legal, ethical, and technological challenges to ensure compliance with privacy regulations and uphold the sanctity of the voting process.

BACKGROUND KNOWLEDGE OF DECENTRALISATION

Blockchain technology, the cornerstone of decentralized ledgers, represents a monumental shift in recording and validating transactions across a distributed network. Comprehending its relevance in voting systems necessitates an exploration of blockchain's foundational principles and mechanisms. At its core, blockchain operates as a decentralized, immutable ledger comprised of interconnected blocks, each containing timestamped transactions. Decentralization stands as a pivotal concept, diverging from conventional centralized databases by distributing control among network nodes, fostering enhanced security and transparency. Consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), authenticate and add transactions to the chain while ensuring the network's integrity. The immutability of blockchain, reinforced by cryptographic hashing, fortifies data against retroactive alterations, fostering an environment of trust and accountability.

Proof of Work (PoW) and Proof of Stake (PoS) stand as two prominent consensus mechanisms within blockchain networks, each offering distinct approaches to validating and adding new blocks of transactions to the chain.

Proof of Work (PoW): This mechanism, popularized by Bitcoin, requires network participants, known as miners, to solve complex mathematical puzzles to validate transactions and create new blocks. Miners compete against each other by expending computational power in a race to find a solution to the cryptographic puzzle. The first miner to solve it gets the right to add a new block to the chain and receives a reward. PoW's security stems from the computational work needed to solve these puzzles, making it resource-intensive and time-consuming. However, this process also consumes significant energy due to the computational power required, leading to concerns about environmental impact.

Proof of Stake (PoS): PoS operates on a different principle, where validators are chosen to create new blocks based on the number of cryptocurrency tokens they hold and "stake" as collateral. Unlike PoW, PoS does not rely on mining or solving complex puzzles. Instead, validators are selected to create new blocks and validate transactions based on their stake in the network. The more tokens a validator holds and stakes, the higher the chance of being chosen to create a block. PoS is considered more energy-efficient compared to PoW since it doesn't require massive computational power. It incentivizes validators to act honestly, as they have a stake in the network.

Both mechanisms aim to achieve consensus in a decentralized network, ensuring that transactions are legitimate and adding new blocks to the chain. While PoW has been historically proven effective and secure, its energy-intensive nature has led to exploration of alternative methods like PoS, which offers potential energy savings and

scalability advantages. PoS also encourages coin holders to participate in the network's governance, aligning incentives toward maintaining its security and stability.

Each consensus mechanism has its strengths and limitations, and the choice between PoW and PoS often depends on factors like network goals, scalability needs, energy efficiency, and the cryptocurrency's specific design. Both mechanisms continue to evolve as blockchain technology progresses, aiming to address challenges while maintaining the integrity and security of decentralized systems.

When integrated into electronic voting systems, blockchain offers a myriad of advantages. Its decentralized nature bolsters security by dispersing the voting database across multiple nodes, mitigating risks associated with centralized vulnerabilities. Each vote, treated as a transaction, is securely recorded and linked, rendering tampering virtually impossible. Furthermore, blockchain's transparency empowers voters to verify the accuracy of their recorded votes without compromising their identities. This transparency cultivates trust in the electoral process while the technology's auditability enables comprehensive post-election analysis. However, while blockchain promises enhanced security and transparency in voting, challenges pertaining to scalability, privacy preservation, and user accessibility demand adept navigation for its full potential to be realized in revolutionizing democratic practices.

METHODOLOGY

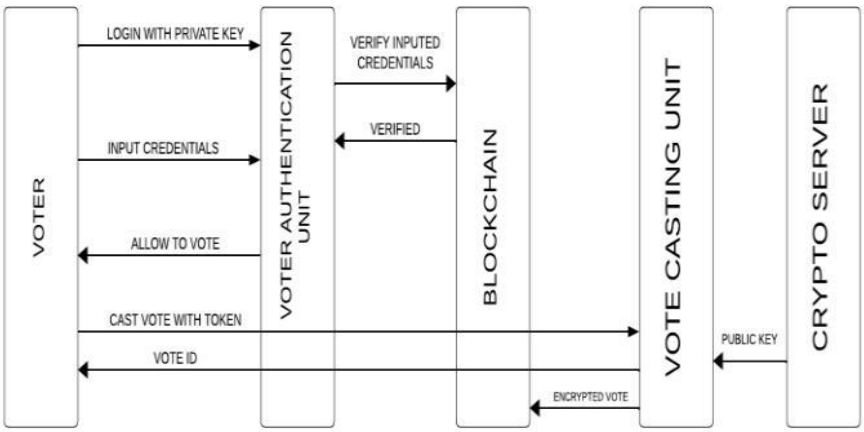

Figure 1: System model

In our proposed work, before we delve into the exact definition of the architecture, it is important to define a few terms:

Voter: Refers to the user entity casting the vote. To enroll as a voter the system will assign a unique identifier or token against which vote can be cast. Aadhaar details can be used to generate a unique digital token for every user. A voter's identity can be traced back to him by obtaining his fingerprint during the time of vote casting and then matching against the fingerprint data stored in the aadhaar. The generated digital token or unique identifier is securely stored on the blockchain along with the voter's details. Smart contracts or specific data fields on the blockchain record this association between the voter, Aadhaar, and the digital token.

Candidate: Refers to the entity standing in election. To enroll as a candidate a unique identifier can be allotted against which votes can be registered.

EC: Election commission is responsible for conducting the elections. EC will oversee the voting process. The members of the EC can be selected as validators of the chain who will be responsible for counting the votes and ensuring only valid votes are registered on the block.

Blockchain nodes: The network of computers, servers, or entities maintaining the chain. The nodes are responsible for validating transactions, reaching consensus and storing the record. Consensus is important to validate the correctness and authenticity of the votes.

Consensus can be reached by POS (proof of stake) - where validators are chosen based on the amount of tokens they hold, or by POW (proof of work) - where participants in a network solve complex mathematical transactions to validate transactions and create new blocks.

Soul Bound Token: Soulbound tokens are digital or physical assets, often in blockchain based ecosystems, intricately linked to a specific individual, preventing their transfer or use by anyone else, thereby ensuring uniqueness and ownership authenticity.

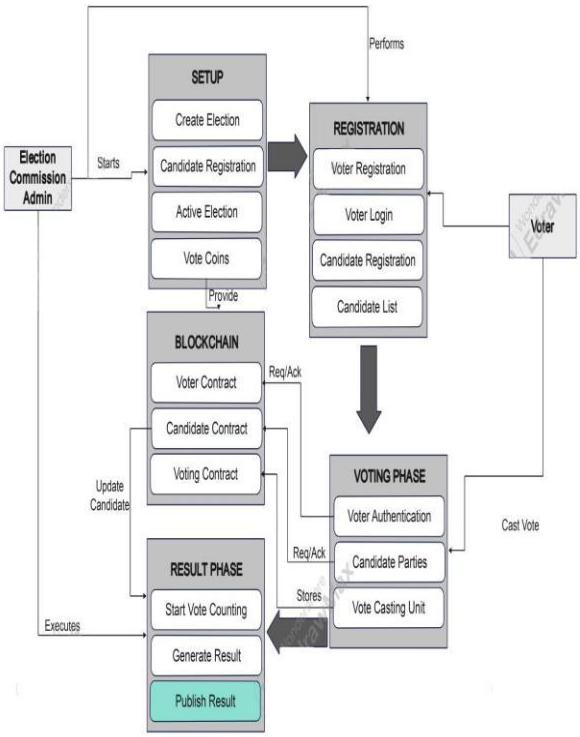

Figure 2: Architecture Diagram

The process as defined by our decentralized voting system can be divided up into 4 steps:

- ☐ Voter / candidate registration
- ☐ Pre-electoral stage
- ☐ Voting stage
- ☐ Post electoral stage

Voter / candidate registration:

If the person is a voter, then the registration process would involve gathering his biometric details and voter id details along with his constituency for which he wishes to cast his vote.

The basic details such as name, name of father, voter constituency and unique voter identification number can be obtained from the voter id of the individual. Next the biometrics of the person needs to be acquired. This can be done using the aadhaar details of the individual. Once the unique biometric details has been obtained which includes the fingerprint and iris scan of the individual, it needs to be linked to the voter id account of the individual. Any vote cast from this individual's account will be traced back to him.If the person is a candidate, since he is also a voter, the same procedures will be followed for him, along with that, his party that he is standing for, the criminal record of the person and authorised clearance of the EC needs to be registered alongside his id.

The voter's decentralised wallet address has to be provided during registration which he would need to access during the casting of the vote. If the person doesn't have a wallet, a public wallet issued by the EC can be made accessible to the people.

Pre electoral stage:

In this stage, the user's vote caste status will be checked and if he hasn't voted already then only he will be allowed to caste a vote. For this, his aaadhaar details will be collected, to verify his identity, then his real time biometrics will be collected to match against the aaadhaar value. If it is a match, then a certain amount of coin will be transferred to his wallet for the transaction gas fee along with a public key generated against his voter id. This public key will be used to encrypt his vote and then register the transaction on the blockchain. The resulting value stored in the block is a hash value which can be decrypted only using the private key with the EC. This will result in anonymous usage by the voter.

Authentication of the voter - The voter's identity is verified by comparing the hashes generated during voter registration and the generated hash of the biometric values obtained during the casting of the vote. The fingerprint scan obtained can be converted into a hash value as studied in **A Study on Fingerprint Hash Code Generation Using Euclidean Distance for Identifying a User Krishna Prasad K. #1 & P. S. Aithal*2.**

Once the hashes match, a certain amount of crypto tokens will be debited into the wallet of the voter, to serve as transaction fee. The public key of the EC generated for encrypting the vote will also be debited to the wallet.

Voting stage:

This is the actual vote casting phase. Votes can be cast in the privacy of the voter's house using his own electronic devices or can be cast physically at designated booths as well. In the voting stage, the person can cast his vote for his desired candidate / party. While voting, his live facial video feed will be captured along with his finger biometrics. The verification contract will match the recorded feed with photographic record on the voter's id [1]. Alongside his recorded fingerprint during the time of vote casting will also be recorded and matched with the recorded aadhaar biometric. Once both of the values match, the vote will be validated, encrypted with the public key in the user's wallet and recorded on the blockchain.

Post electoral stage:

In this stage the actual vote counting process shall begin. For this the vote will be decrypted using the private key generated against the vote by the election commission. To tally the vote, one unit of cryptocurrency can be debited against the wallet address of the candidate for which the vote is casted. At the end, the amount of credits in the wallet of the candidate will determine the number of votes received by the candidate. Once the votes are added to the block, it forms a part of the immutable ledger and cant be tampered with. This makes the electoral process secure.

For the entire process, we can define a few smart contracts which will help in executing the various functionalities of the voting process.

Initially, during the registration process, the voter contract stores the hash value of the voter's information in order to secure the voter's information and grant them anonymity. These hash values are also used to authenticate voters during vote casting. Information for each candidate in the chain is contained in the candidate contract. Voters use a vote currency to cast their ballots after completing the voter verification procedure and selecting a candidate from the list supplied by the candidate contract. In this case, the voter's voting status is represented by the vote coin. The voter abstains from casting a ballot if the vote coin balance is 1.

IMPLEMENTATION AND RESULTS

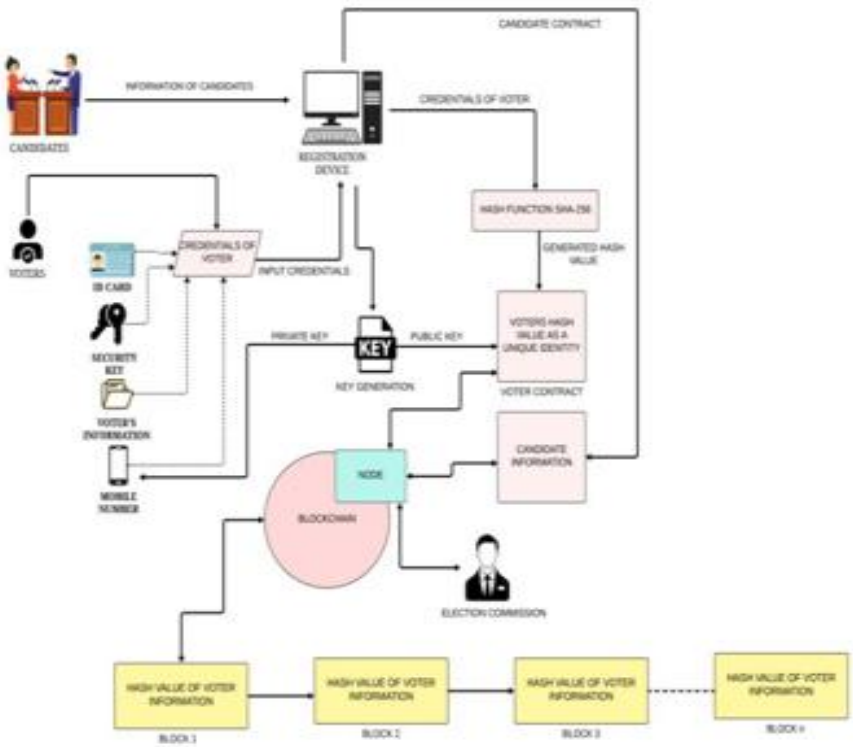

Figure 3: Implementation system

A. Implementation details:

The demo system can consist of two aspects – the client side and server side.

On the server side we will have a blockchain network running. The blockchain network will be composed of the following components – Truffle, solidity, ganache, node server / any alternative.

Truffle - Truffle stands as a comprehensive development framework within the Ethereum ecosystem, streamlining the creation, deployment, and testing of decentralized applications (dApps) and smart contracts. With a suite of tools, Truffle simplifies project management, enabling easy smart contract compilation and deployment to various Ethereum networks. Offering automated testing functionalities, a built-in console for interaction, and seamless integration with Ganache for local testing, Truffle supports developers in efficiently navigating the complexities of Ethereum development, making it a preferred choice for those building on the Ethereum blockchain.

Solidity - Solidity serves as a high-level, contract-oriented programming language specifically designed for writing smart contracts on various blockchain platforms, predominantly Ethereum. It enables developers to create and deploy self-executing contracts with predefined conditions, facilitating decentralized applications (dApps) and automated transactions on the blockchain. Solidity draws syntax and structure influences from JavaScript, Python, and C++, offering a familiar development environment for coders. It provides features like data structures, libraries, and inheritance while focusing on security, as smartcontracts are immutable and execute as programmed. Solidity's role in the Ethereum ecosystem is fundamental, empowering developers to build complex decentralized solutions, although it demands thorough consideration of security best practices to prevent vulnerabilities and potential exploits within smart contracts.

Ganache - Ganache stands as a popular personal blockchain development tool, serving as a local Ethereum test network for developers building decentralized applications (dApps) and smart contracts. It offers a user-friendly environment where developers can simulate blockchain behavior without interacting with the main Ethereum network. Ganache provides a personal Ethereum blockchain that operates entirely locally, allowing rapid development, testing, and debugging of smart contracts and dApps in a controlled environment. It offers features such as quick blockchain creation, predefined accounts with test Ether, on-demand mining, and detailed transaction logs, enabling developers to simulate various scenarios and interactions that occur on the Ethereum network. Ganache, with its ease of use and powerful testing capabilities, remains an essential tool in the Ethereum

development toolkit, aiding developers in ensuring the reliability and functionality of their blockchain-based projects before deployment to the live Ethereum network.

In the client side the demo web app/ mobile app can be built using Reactjs / Flutter along with Web3 libraries for javascript like web3.js. For decentralized wallet, metamask can be used.

LITERATURE REVIEW

In Khan et al. (2020) [2], a blockchain-based solution is proposed to address the issues with traditional elections. The goal of this thesis is to create a voting mechanism that is easily accessible and ensures the security of voter identity, data transfer, and verification, while also establishing a decentralized electronic voting technique through the use of blockchain technology. The suggested solution makes use of a number of technologies, such as metamask, truffle framework, and ganache. This technique has two drawbacks: it does not allow voters to remain anonymous and the cast vote is visible at the time of voting. A blockchain-based democratic procedure centered on the Ethereum network was proposed by Boshri et al. (Bosri et al., 2019) [3]. Using this method, the election commission created an Ethereum account to store voter data. Voters may cast their ballots at a polling place if they do not have access to a smartphone. Before they may cast their vote, they must finish a biometric verification process. Despite using blockchain technology, this approach involves a lot of third parties. A third party adds the chain, to which just the cast vote is recorded (Kumari et al., 2020) [4]. A bogus vote might be cast in this instance. They suggest a blockchain-based smart contract e-voting system in Jorge Lopes (2019)

[5]. The director, the developer, and the voter are the three groups of persons who can interact with the software. There are three contracts: Record, Creator, and Election. Voter registration data must be stored by record contracts in order to confirm authenticity. Following authentication, money is sent via the API to the Creator Contract, which is in charge of creating a new Election Contract.

To cast a vote, an Election contract is formed and its address is sent to the Creator contract. The ballot is encrypted using homomorphic encryption, a type of symmetric encryption, prior to being uploaded to the blockchain. The paradigm presented in Shahzad et al. (2019) [6] suggested a better method of blockchain-based electronic voting. This proof of completeness method addresses the creation of blocks, their locking, information management, and blockchain architecture, particularly with regard to the voting machine network. In the event that a block is formed, the elector's unique identity and biometric verification must be confirmed by the presiding officer (PO). After the voter casts his ballot, the computer generates a SHA-256 hash and forwards the information to the presiding officer so that a block may be created. The main drawback of this approach is that it needs further privacy, security, and transparency before it can be regarded as a completely reliable voting mechanism (Toapanta et al., 2019) [7]. In order to maintain an open, secure, and economical voting process, Dagher et al. (2018) [8] created BroncoVote, a blockchain-based voting platform that improves transparency and protects voter anonymity. With BroncoVote, university environments may now have auditable election outcomes and election management through the use of blockchain, smart contracts, and Ethereum. This system makes use of three contracts: the Registrar, the Creator, and the Voting Contract. This system's insufficient voter authentication and inadequately secured registration process are its drawbacks.

There are also privacy problems with the technique. AMVchain, an effective and scalable voting system that combines blockchain technology with smart contracts to enable transparent and decentralized voting, was designed and constructed by (Li et al. in 2021) [9]. They start by looking at the shortcomings and challenges with current blockchain-based voting systems, after which they assess important studies to deal with these problems. according to the requirements for a trustworthy and effective electronic voting system. In order to maintain voter anonymity and sever the connection between individuals and votes, linkable ring signatures are employed during the voting process. Alvi et al. (2020) [10] proposed a digital voting architecture using a smart contract to address issues with singularity, integrity, mobility, autonomy, transparency, accuracy, and privacy that arise when using blockchain technology for voting. The data provided by the voters will be used to create and store a hash in their system's chain.

CONCLUSION

In order to overcome the drawbacks of conventional voting procedures, this study proposes the adoption of a blockchain-based voting system. By using Zero-Knowledge Proofs to provide voter privacy and tamper-proof records, the decentralised and transparent nature of blockchain technology improves election integrity. While protecting voter privacy, the inclusion of Aadhaar credentials enhances identification verification even more. The

suggested hybrid model helps create an electoral framework that is more reliable and responsible by navigating ethical, legal, and technological issues.

FUTURE PLANS

The suggested blockchain-based voting mechanism will be put into practice and tested in the coming stages. The architecture and methods are well-defined, and technologies such as Truffle, Solidity, and Ganache will be employed in the development of the system. Voter authentication, secure voter registration, and vote counting will all be made possible via smart contracts, which are built to perform a variety of functions. To verify the implementation's effectiveness, security, and functionality, a local blockchain network will be used for testing. Future studies might concentrate on resolving issues with user accessibility, privacy protection, and scalability to facilitate broad adoption. In addition, navigating legal and regulatory considerations for practical implementation will require cooperation with pertinent authorities and parties.

ACKNOWLEDGMENT

I would like to express my deepest appreciation to Dr. Thanga Revathi S, who played a pivotal role in the successful completion of my mini project. Their unwavering guidance, expertise, and support were instrumental throughout this journey. She provided invaluable insights, direction, and constructive feedback that significantly enhanced the quality and depth of my project. Their dedication and commitment to mentorship went above and beyond my expectations, and I am truly grateful for their contributions. I would also like to extend my gratitude to my peers and all those who supported me along the way. Their encouragement and assistance were essential in making this project a reality.

REFERENCES

[1] Blockchain based E-Voting system with Facial Recognition Proceedings of the International Conference on Inventive Computation Technologies (ICICT 2023) IEEE Xplore Part Number: CFP23F70-ART; N Prathyusha, P Pooja, Dr. A Vijay Vasanth

[2] R. Bosri, A.R. Uzzal, A.A. Omar, A.S.M.T. Hasan, M.Z.A. Bhuiya Towards a privacy-preserving voting system through blockchain technologies 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech) (2019), pp. 602-608

[3] Pooja Kumari, Bhagia Sheri, Isma Siddiqui, Khubaib Khatri Conventional vs blockchain-based e-vote system (2020)

[4] José Luís Pereira Jorge Lopes. Blockchain based e-voting system: A proposal. In Twenty-fifth Americas Conference on Information Systems, Cancun, 2019, 2019.

[5] B. Shahzad, J. Crowcroft Trustworthy electronic voting using adjusted blockchain technology, IEEE Access, 7 (2019), pp. 24477-24488

[6] S.M.T. Toapanta, Marjorie Isanoa Sinche, and L. Gallegos. A cyber environment approach to mitigate vulnerabilities and threats in an electoral process in ecuador. In ICETM 2019, 2019.

[7] Gaby Dagher, Praneeth Marella, Matea Milojkovic, and Jordan Mohler. Broncovote: Secure voting system using ethereum's blockchain. pages 96–107, 01 2018.

[8] Chenchen Li, Jiang Xiao, Xiaohai Dai, and Hai Jin. Amvchain: authority management mechanism on blockchain-based voting systems. Peer-to-peer Networking and Applications, pages 1–12, 2021.

[9] Syada Tasmia Alvi, Mohammed Nasir Uddin, Linta Islam Digital voting: A blockchain-based e-voting system using biohash and smart contract 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT) (2020), pp. 228-233