Leveraging Blockchain for the Design and Realization of a Secure E-Voting Mechanism

K. Giridhar[1*], M. Venugopal[2], B. Vishnuvardhan Reddy[3], Poola Sreyanjali[4] and Sake Sneha[5]
{kgiridhar562@gmail.com[1], venunani489@gmail.com[2], rplvishnu@gmail.com[3],
sreyanjali.p@gmail.com[4], smssneha8@gmail.com[5]}

Assistant Professor, Department of CST, Madanapalle Institute of Technology and Science, Madanapalle, Andhra Pradesh, India[1]
Under Graduate Student, Department of CST, Madanapalle Institute of Technology and Science, Madanapalle, Andhra Pradesh, India[2, 3, 4, 5]

Abstract. The purpose of this paper is to ensure the development of voting system, a secure, transparent and efficient online voting system which will enable the public to vote during elections more effectively and consequently improve the election process. Permitting the use of blockchain technology and secure authentication procedures, the system verifies that votes are recorded correctly, stored in a bonafide manner and counted in a transparent way. Important feature of the system includes secure access and authentication, secure storage of vote and user information and a user-friendly GUI. Security aspects like encryption, Secure Socket Layer (SSL) is inbuilt in to protect the voting process from cyber threats like denial-of-service attacks and man-in-the-middle attacks. The backend database of this system is managed by MySQL for its security and scalability. It describes the deficiencies in the current paper-based voting system (inefficiency, human errors, new security concerns). Several software development methodologies are reviewed - Waterfall, Rapid Application Development, and Prototyping - but the Waterfall methodology is selected because of its clear and organized steps. In addition, we consider alternative electronic voting systems i.e. (Direct Recording Electronic Systems, Telephone Voting, Internet Voting) to choose the remote internet voting as the most promising approach.

Keywords: e-voting, blockchain, digital, cryptographic, confidentiality, efficiency, smart contract, decentralization, transparent, security.

1 Introduction

India has welcomed digital transformation enabling everyone as digitised persons with Aadhaar cards and voter ID card. Indian elections have come a long way since then, the process of voting has seen a lot changes-from manual counting and paper ballots to the introduction of punch cards and EVMs. Modern electronic voting has several advantages over traditional methods, such as: increased accuracy, convenience, flexibility, privacy with respect to the votes cast and verifiability. These systems offer equal access for people with disabilities, they cut down on the time and cost of running elections, help increase voter participation, and increase confidence in the process.

However, electronic voting technology adoption is still quite a challenge for many developing and less developed nations. Although only a few of these countries have introduced e-voting on a significant scale, a number of mainly developed countries (including Austria, Australia, Brazil, Canada, Switzerland, Estonia, France, the United Kingdom, Japan, Russia, Sweden,

ICITSM-Part II 2025, April 28-29, Tiruchengode, India

DOI 10.4108/eai.28-4-2025.2358030

and the USA) have moved from trials to legally sanctioned remote or fully (i.e., ballpoint) e-voting. One of the obstacles for e-voting is the limited internet penetration in developing nations. Relying on online voting systems can disenfranchise those who lack consistent internet access. We believe this further emphasizes the need for flexible two-tier voting systems, which could be used on- and off-line, that balance inclusiveness with the level of security required from a trustworthy electronic voting system. CONS of EVMs on flip side time taking not paper work no role of higher and operator careless can device circuit to be failure for incorrect use bulk updating less. Online Voting System can solve all these issues. It will allow people to vote without being physically present at their precinct poll site. Normal is where we keep the public safe, minimize the opportunity for violent repression and maximize voter turnout.

To contrast with a binary piece-of-paper ballot, or for those of us who are newer in computer theory the simpler and symmetric model where we all have 2 opinions. Online voting electronically votes through ballot input and storage of how to count using the number for each election, is therefore a simple form the opposition against electronic elections easily collapses. The existing system, for all its warts (and there are many), comes with problems of its own, including abysmal turnout in a voting process that is already so restrictive and inconvenient the plan is to have it take place in part on the internet, if you happen to have access to the internet, or can get some. The voting schemes in the new system will be quite varied, and secure methods must take these into account. We are making a secure and private platform: from verified user identification, to poll encryption & approval capabilities. Anti-rigging and multi-vote and mirror holding mechanism will restrict the shiny massage just for the sake of equity & justice would not work.

To maintain the best security and privacy for our users, stocks is based on modern cryptographic tools like Homomorphic Encryption. These enable the calculation of encrypted values without decryption. That’s how we can count the votes securely and secretly. All transmissions are also encrypted through SSL to prevent third-parties from intercepting and accessing them. Authentication will be multi factor (something the voter knows, plus something the voter has) and supported by electronic signatures for electors to prove who they are without risk of impersonation. Based on this forensic auditing algorithm and protocol, it allows students to make a safe and efficient voting using an auditable online secure voting system.

Secure Hash Algorithm (SHA) has a large significance for online voting system which takes the charge of vote authentication, reliability and protection. SHA, as a hash function, it is used for converting the voting data into a shortened code called hash that can be of any length specified; to verify if the vote has been manipulated or not. Authenticates voters so they can’t be altered and anonymity of votes by hashing them in a way that’s impossible to cryptographically deanonymize. Supporters of blockchain voting can turn to SHA, and content that hashed votes are written to an open ledger that is transparent and tamper-proof. But actually, SHA is not a data encryption method anyway and even if there were (by some extremely twisted way of looking at things) reasons to encrypt the data you're depending its integrity onto (once again, based on its SHA-hashing or other hash-based integrity-checking), then you'd also need to complement it with other security measures (use digital signatures / secure transmission channels, etc…). It will also provide enhanced security from voter login to

the service until after the voting process is over and fallout from the system. Those protections are: Each voter should be able to vote and will vote only once in the election.

2 Literature Survey

Blockchain-based E-voting is increasingly catching the attention of people now to solve various securities, transparency, scalability & voters trust issues. The proposed technology of electronic voting(online) that intends for organizing the election via internet typically, and does not involve a voter in paperwork work. Conventional e-voting systems have tended to suffer from security issues, lack of transparency and reliance on a central trust authority. This is where blockchain technology can make the shortcoming right with its decentralized approach, immutability and cryptographically enabled features.

Hajian Berenjestanaki et al. [1] systematically introduce blockchain based e-voting systems and analyze their key design requirements, security guarantees and the trend of technology evolution. Similarly, Sharp et al. [2] presented blockchain enabled e-voting systems, compared several solutions and proposed improved architectural designs for efficiency and privacy of the voter.

An early blockchain-based e-voting protocol was suggested by Hardwick et al. [3], in which they show how, using decentralization and cryptographic primitives, one can maximize both the privacy of the voter (including voting value) and the integrity of the voter ion. Going beyond security needs, Gandhi et al. [4]examined threats on blockchain voting system and concentrated on security mechanisms including authentication, and encrypted vote storage.

Privacy preserving methods are regarded as obligatory by Thakkar et al. [5] that brought up the Electronic Voting System on Blockchain to ensure privacy of each voter uses contemporary cryptographic primitives. Russo et al. [6] further followed this line of work to present Chirotonia, an efficient solution that utilizes linkable ring signatures to balance verifiability and privacy in the context of a massive voting system. Kumar [7] also describe how proof-of-work could be employed to defend the voting transactions from tampering as well as effort by a malicious party.

The relevance of blockchain has also been analyzed for particular national and regional cases. Tyagi et al. [8] introduced an Aadhaar-based blockchain voting system for India, demonstrating how countries can use national identity infrastructures to ensure powerful e-Voting systems. Pandey et al. [9] proposed Vote Chain, which is a public blockchain technology utilized to secure parliamentary elections. In a related work, Vijaya Kumar et al. [10] focused on significantly enhancing the scalability and security of blockchain enabled e-voting in IoT-based public cloud environments.

Other non-blockchain systems have also been used. Barański et al. [11] presented a practical i-voting model based on Stellar blockchain, Díaz-Santiso & Fraga-Lamas [15] employed Hyperledger Fabric to construct a permissioned blockchain system that can improve efficiency and accountability.

Research in this field has been reviewed by several surveys. Ohize et al. [12] provide a comprehensive survey of blockchain e-voting designs with regards to which some tendencies and solutions are arising along with open issues. Similarly, Braghin et al. [13] reported its

transparency and audibility derived from a blockchain deployment, and Chafe et al. [14] even gave a protocol with reduced efficiency but being decentralized.

Altogether, these works show that a voting mechanism based on blockchain technology effectively increases transparency, immutability and trust in the election process. But they also note impediments - including scaling, compatibility with established networks, privacy of voters and regulations against tampering. The lessons learned from previous work serve as guidelines for constructing secure, verifiable, and deployable blockchain-based voting systems, which are considered in our work.

3 Proposed Work

The design of a voting system affects how it can be used and how good it is. This is then realized a transparent, intuitive structure positively avoids being complex in the name of simplicity as well as ease plus maximum order that can be achieved according to him. A trusted e-voting web-based system should be developed on architecture that is secure, scalable and easy to use in other to promotes transparency, privacy of voters and maintenance performance. The system is a client-server model in which, during voting, end users interact with either web or mobile apps for voting and there are servers within the back-end that are responsible for identification of voters and ballot creation to counting. The AFM Utilize Multiple Factor Authentications Such as Biometric Authentication, National Identity Check or Block Chain Identity Management to Prevent 8 Vote Fraud. Electronic votes are encrypted and deposited on a trust less block chain or kept sealed in safe environments in tamper proof databases to enable full transparency. There also have to be real-time audit logs and cryptographic proofs so others can independently verify results. The time sensitive voting WP as service too: with a load-balanced design allowing the system to be up at full server during popular vote. In addition, stringent cyber defense (e.g., end-to-end encryption, DDoS attack protection and intrusion detection systems) would need to be deployed to protect the system from potential cyber-attacks. In addition, the voting platform must be designed to be accessible for all users, including those with disabilities (in accordance with Way Content Accessibility Guidelines “WCAG”). Finally, and perhaps most importantly you can actually prove that the results have been correctly tallied using cryptographic techniques (zero-knowledge proofs, prom orphic encryption) without ever Revelation what each voter voted. Fig. 1 shows the System Architecture.

The figure presents a blockchain-based electronic voting system to enhance the security, transparency and efficiency of an election. It begins with registration of voters through a valid system, so that only eligible voters are allowed to vote. After the registration, voters pass an authentication process to establish their identities and get into the voting channel.

Central to the system is the Voting Management System (VMS), which orchestrates the entire system, and interfaces directly with the Election Authority for the regulation of election. Sensitive data is safe and voter information is secured through layers of cybersecurity to preserve the integrity of the system.

Ballot data are recorded on a blockchain, a decentralized, tamper-resistant ledger, so it cannot be modified or meddled with. Smart contracts are used to automate the verifications of voting rules, to ensure that each ballot is processed according to a well-defined protocol.

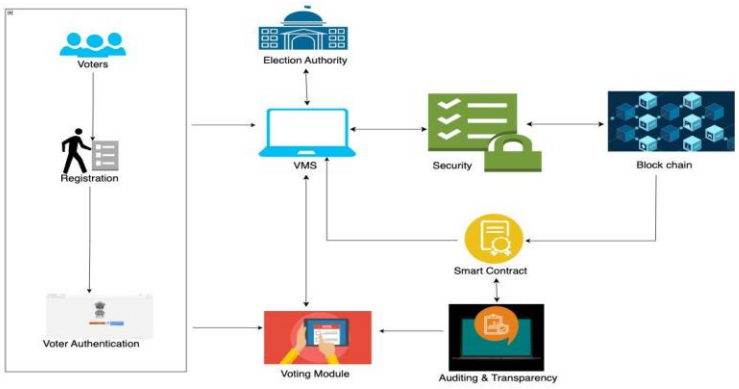

Fig. 1. System Architecture.

Due to the decentralized nature of the blockchain, all voting traces are secured and cannot be tampered with. With access from authorized individuals to audit and confirm the election results, trust and transparency are strengthened. Voters vote through an intuitive, secure system, facilitating confident participation. Leveraging blockchain technology, the software addresses and all of the concerns associated with electronic voting.

3.1 Evaluation of Block Chain Enabled Electronic Voting System

The blockchain e-voting system is analysed as per its properties, characteristics such us security, transparency, scalability voter's privacy etc., where latest cryptographic techniques applied to hide identity of voters and protect votes integrity. Election procedures are written as smart contracts to ensure, they enforce execution fairly without any scope of human intervention and mistake. A vote once made on the blockchain can never be altered and removed. Voters themselves can verify that their votes have been counted, without giving away their anonymity, hence gradually increasing trust and confidentiality. The distributed nature of the system eliminates potential single points of failure, and increases its reliability and availability. Presentations are made in testbeds or simulators to demonstrate the efficacy, fault-tolerance and performance of the system. User accessibility is a major concern, so the system will be as intuitive as we can make it even for non-tech-savvy users. Secondly, the blockchain is also transparent so it can be closely examined and assure a legitimate vote that can always be traced back.

3.1.1 Methods of Voting Systems:

Proposed Blockchain-Based E-Voting: In the present era, the latest technology named Blockchain is used for forming a distributed and secure e-voting environment. The ballots, which are encrypted and registered in a distributed ledger, offer transparency, immutability and immunity to manipulation. It allows people to prove they voted without revealing their identity, which fosters trust and encourages turnout. It's particularly useful for large, remote elections.

Classical Electronic Voting (Centralized Systems): DAAs have been implemented since the 90s (and still are) with the aid of digital machines or online platforms controlled by central authorities. Though it allows for faster vote counting and a reduced margin of human error, the system is vulnerable to central breakdowns, cyber-attacks and manipulation. Its opacity and reliance on a central database erode confidence among voters, especially in high-stakes elections. Table 1. Shows the A Comparative Analysis of Blockchain-Based E-Voting Systems Versus Traditional Electronic and Paper-Based Voting Methods (Source: author)

Traditional Voting: technique in which voters record their preference by writing onto a paper. Although it provides an option for concealment of the voter's selection and it can be deployed easily, it is demanding on manpower, subject to logistic delays in counting, human errors and frauds. Scalability of such a system is limited and therefore less suitable for large or spread-out elections.

Table 1. A Comparative Analysis of Blockchain-Based E-Voting Systems Versus Traditional Electronic and Paper-Based Voting Methods (Source: author).

Feature	Blockchain-Based E-Voting System	Centralized E-Voting System	Traditional Paper-Based Voting
Security	Very strong due to cryptographic algorithms and data immutability	Moderate, as centralized servers can be compromised	Generally weak; relies on physical protection, vulnerable to tampering
Transparency	Highly transparent with publicly accessible and verifiable records	Limited visibility controlled by a central authority	Moderate; visible to observers but lacks digital traceability
Vote Immutability	Guaranteed—once recorded, votes cannot be altered	Not assured; central systems may allow data changes	Not digitally immutable; physical ballots can be mishandled or lost
Privacy & Anonymity	Strong, maintained through encryption and privacy-preserving methods	Varies depending on implementation and safeguards	High anonymity; voting is generally private
Voter Verification	Enabled via cryptographic validation of voter and vote	Depends on mechanisms like OTPs or passwords	Manual process using ID checks
Cost Efficiency	Economical in the long term; minimal ongoing expenses after deployment	Costly due to continuous maintenance and licensing	Expensive due to printing, logistics, and human resources
Scalability	Easily scalable; ideal for nationwide or remote voting	Moderate scalability; performance may degrade under high loads	Poor scalability; limited by manual counting and physical logistics
Tamper Resistance	Exceptionally high; blockchain's design exposes any attempt to alter records	Moderate; a central database is more vulnerable to manipulation	Low; susceptible to ballot fraud and other forms of physical tampering
Auditability	Easy and reliable with	Challenging without	Difficult; requires

	full historical traceability of votes	system-level access or logs	labor-intensive recounts
System Availability	High; decentralized network ensures continuous operation	Moderate to high, but can be impacted by outages or cyberattacks	Limited to specific polling places and hours
Potential for Turnout	Very high; supports convenient, location-independent participation	Moderate; constrained by access to the voting platform	Lower; requires in-person voting, which can deter participation

Blockchain does have a list of clear benefits over traditional server-side e-voting solutions and paper-based voting systems. The best thing about it is that it is decentralized, and there are no authorities in control of its network. Reliability It is less risk of system failure and it will become more tamper-proof, and less vulnerable to insider attacks. The latest cryptographic techniques are employed, with the data and votes secured such that they could not be realistically tampered with or discriminated by unauthorized parties.

Also, it's healthy that we could democratically minimize how opaque our voting need be by recording every vote on a public ledger whose rendered tamper-proof record of same is available for anyone to inspect. It provides real-time validation and audibility without sacrificing the voter privacy. And since blockchain is immutable, all votes cast will not be tampered with, thus ensuring the transparent process of voting itself.

Equally importantly, the critical privacy of voters is guaranteed using cutting-edge cryptographic protocols like zero-knowledge proofs and blind signatures. These procedures make it possible for voters to verify that they voted and that their vote was properly cast, without revealing who the voter is. The platform almost free and green in that it doesn't use much if any paper ballots, the physical labour of voting and global transport. It also speeds the count and delivers results in real time, minimizing the risk of post-election disputes. Again, because it's decentralised access and stability (including censorship resistance) issues aren't likely to hold against the platform. Secure remote voting Besides privacy, Blockchain also enables secure remote voting that for instance allows citizens with disabilities and expatriates to exercise their electoral rights. From a centralized point of authority to a decentralized and cryptographically secure system, the introduction makes nice reference to the trust of the public and open, secure, fair elections.

4 System Design

"Traditional forms of voting have plenty of problems, ranging from fraud and interference to a lack of transparency and accessibility," said McCauley. Implementing such a virtual voting service over a blockchain may also lead to a trust less and transparent solution about fair elections. In this paper, the authors propose a blockchain based voting system which embeds the characteristics of blockchain to prevent unauthorized alternation of vote and prevents sensitive information using crypto algorithms and identities of voter.

It becomes possible to automate the verification and counting of the votes using smart contracts thereby providing a low level of intervention which also reduces bias. This system also has feature of auditing the responsive results and to check them for their validity in real

time without revealing the votes, that maintains the privacy and integrity. Being able to join remotely solves both access and participation problems.

You just need decentralization to get rid of a central operator thus SPOF or fraud. A really significant benefit of end-to-end encryption is that not only does it stop online attack, but the whole election becomes secure. This helps contribute to a transparent, responsible and accountable electoral system, which can help rebuild confidence in democracy. Blockchain-based e-Voting: Developing a new era of voting system for secure and time-efficient elections. The advantage of the blockchain -based e-voting system is that cryptographic, consensus and privacy-preserving protocols can be adopted to ensure that elections are performed securely and privately. Authenticity of a vote could be guaranteed with encryption, like SHA-256 and ECDSA. One of those consensus techniques is Proof of Authority (PoA)and PBFT, which allows to record a vote in an immutable manner and very quickly. Following are some of the Technology bricks that form a part of a Blockchain enabled E-Voting solution. The Technological foundations are presented in Table 2.

Table 2. Technological foundations (Source: author).

Function	Recommended Algorithms
Voter Authentication	RSA, ECDSA
Data Integrity	SHA-256
Privacy	ZKP, Blind Signature, Homomorphic Encryption
Consensus Mechanism	PoA, PBFT, DPoS
Smart Contract Logic	Solidity (Ethereum), Chaincode (Hyperledger)

4.1 Module Specification for Blockchain based E-Voting system

4.1.1 Voter Registration

Register only valid IDs: The voter registration module is essential to make sure only valid IDs are able to participate in the election. This feature ensures the authenticity of the voter and safeguards against multiple non-duplicated entering of the same user while storing the information securely in the blockchain.

Government-Issued ID Check: Verified with government-issued identifications (e.g., passport).

Biometric: Finger print, facial or iris as a biometric can be included for extra security.

Challenging the Voter's Identity: A onetime password (OTP) or confirmation email confirms that the voter is who they claim to be.

KYC (Know Your Customer) Integration To align the KYC (Know Your Customer) – Check KYC features with the authenticity, the voter’s information has to be linked with the database of the government or institution.

Smart contracts for the verification of identity Smart contracts are needed for automation, improving security, and verification of voter identity in a blockchain based e-voting system. Such self-executing protocols implement 'whitelisting' conditions by incorporating identity verification measures like KYC, biometric recognition, authentication via government-issued ID, etc. This prevents unauthorised persons from registering and from taking part in the vote.

4.2 Authentication and Verification

Provides only valid voters to vote: Using smart contracts, cryptographic methods, and authentications, the blockchain-based electronic vote system takes care only the valid voters can vote. This is how misuse of votes, double votes, or unauthorized access are avoided.

Eligibility: A voter must satisfy predefined eligibility requirements (e.g., written in a smart contract) for being able to vote. These factors usually are:

1. Age Verification: That the voter is of age to vote (18 years or older).
2. Citizenship & Residency Verification: Only citizens registered in a given locale can vote.
3. Unique Voter ID verification: Each voter should be assigned a unique blockchain ID/connection to their identity.
4. Registration: Must be registered to vote, and must have registered prior to election day.
5. No prior Vote is cast: The voter should not have already voted (to prevent multiple voting).
6. MFA (Multi Factor Authentication): MFA makes it so only eligible voters are allowed to access the e-voting system, using more than one way of authenticating the user. It adds security, it prevents voting impersonation and fraud (for example, biometrics, OTP, and digital signatures).

A voter has to finish at least two authentication steps before he/she is allowed to vote. This can include:

4.3 Voting Module

A Voting Interface: For the blockchain-based e-voting system, it needs a voting interface to help eligible voters cast their votes safely. The interface can be a website, mobile app, or decentralized application (dapp) that connects or communicates to smart contracts within blockchain.

Confidential and non-confidential votes recording: Confidential e-voting system records votes securely, using plaintext encryption before recording on the blockchain securely. This ensures secure and reliable voting, with no possibility of tampering, hacking, or manipulation.

Public-Key Cryptography (RSA, ECC) Votes are encrypted by public key encryption, such as RSA, with the guarantee that only an authorized election authority can decrypt them.

Homomorphic Encryption: It enables counting of vote without decrypting the votes.

Zero-Knowledge Proofs (ZKP) Voter can ``prove" that they have voted without disclosing their vote.

4.4 Blockchain Ledger

Pagealignmen TStores and maintains immutable record of votes: In blockchain-based e-voting every vote is captured with security and it is recorded in a secure platform which is unchangeable. This immutability ensures that the election process is transparent and secure, preventing any vote manipulation or fraud. Votes are also a cryptographically secure transaction that are recorded into a blockchain-based ledger, where they cannot be altered or deleted. The system is transparent and tamper proof since its operations are managed in a decentralized manner, so it is infeasible for a single entity to control the data of votes.

Uses consensus algorithms to approve transactions: Voting e-voting systems establish consensus algorithms that include Proof of Work (PoW) and Proof of Stake (PoS) to approve the votes that will be included transactions in the blockchain. These protocols need to obtain agreement of many nodes of the network, to validate the validity of each vote, thus ensuring that there is no cheating. PoW (which you'll know from Bitcoin) requires the recipient to perform complex mathematical computations proving that the vote is legitimate, but it's extremely energy-intensive. PoS, on the other hand, as adopted in Ethereum 2.0, selects validators via the amount of cryptocurrency they put at stake, providing a more power-efficient but equally secure substitute. Those consensus mechanisms enable uses like blockchain voting systems to be decentralized and transparent, with a recorded vote being resistant to change by even one party once it is cast.

4.5 Smart Contracts

Automates voting rules: There are voting rules such as eligibility checks and counting of votes in an election, which could be automated using smart contracts in any blockchain e-voting system, to ensure the fairness and transparency of an election. These smart contracts impose an eligibility check which requires voters to be cryptographically authenticated before they are allowed to vote. When the vote is cast, the system automatically counts it and logs it on the blockchain, eliminating the possibility of human error and fraud. The whole process is automated with no manual intervention, eliminating any delay and ensuring that the votes are counted accurately and immediately. Through the automation of voting regulations by the Blockchain voting accelerates the process and adds efficiency, security and trust in the elections.

Automatic recording and counting of votes: The use of smart contracts and decentralized validation from block-chain-based e-voting systems ensures that votes are recorded and counted automatically. The system encrypts, verifies and stores the vote on the blockchain as soon as the vote is cast, thus preventing tampering or fraud. The votes are then counted in real time by smart contracts, reducing the risk of human errors or deliberate biased action during vote counting. Because the process is completely automated and open, election outcomes are proven immediately and don't involve any kind of human intervention. This is how we get a voting system that is secure, fast and trustworthy - where every vote is properly counted.

4.6 Vote Counting & Results

Aggregate votes from the blockchain ledger: Blockchain based e-voting system aggregates votes directly from the blockchain ledger, which provides a tamper proof and transparent counting process. Because of this, and the fact that every vote is actually recorded as the votes themselves, smart contracts can pull, check and even add up the number of votes automatically without the need of any human intervention. This sidesteps fraud, undercounting or zigzaggery, because every vote will be stored forever, and be auditable. Its decentralized blockchain approach allows for the three coy by coy vote count and provides that there coy cathedral is accurate and pub ice. By tallying votes in this manner, it's possible for election results to be verified in rapid fashion, and with a high degree of accuracy.

Provide Real-Time Transparency Results: Blockchain e-voting system generates real-time, transparency results by recording and tabulating votes automatically in its decentralized ledger. Everyone can independently instantly check the results since all votes are saved immutably and there is no central authority. Through smart contracts, stopping of vote count and fraud is minimized since tallying of votes is done in real time. Blockchain can be transparent, meaning voters, election officials and auditors can trace and validate election results in a secure way. This has built trust, it has been accurate and the process is believed to be credible.

4.7 Auditing & Transparency

Permits election officials and auditors to verify votes: E-voting systems based on Blockchain permit votes to be verified by election officials and auditors, as every voter's vote is recorded in an immutable and transparent ledger. With each vote being encrypted and registered cryptographically, auditors are able to track and verify each individual vote without revealing the voters. Smart contracts guarantee that only legitimate, eligible votes get counted, so no risk of fraud or tampering. Election administrators can verify voting records in real time by using blockchain explorers or bespoke verification tools, thus maintaining the integrity of the election and balanced treatment of the candidates. This dispersed vetting process strengthens trust, security, and lay understanding of voting.

ZKP for privacy while maintaining integrity: The e-voting systems by using blockchain employs Zero-Knowledge proofs in order to maintain privacy of the voter as well as integrity of the vote. With ZKP a voter can demonstrate that a legal vote has been cast, while remaining both anonymous and secretive. This guarantees that the system be able to check and count real votes while preserving their contents private. As ZKP guarantees that no sensitive information is revealed, it avoids collusion, vote buying and identity tracking. Blockchain voting with ZKP has combined transparency and privacy which can make elections to be secure, anonymous, and verifiable.

4.8 Security & Privacy

End-to-end encrypted votes security: The blockchain-based e-voting systems occur with E2EE enabling the protection of the votes by ensuring that the data will stay secure and private from the voting process start until the end. The voter casts his vote and is instantly encrypted using powerful encryption algorithms (i.e., RSA, AES, ECC) prior to transmitting it. This encryption guarantees that only the allowed parties (i.e., the blockchain network and smart

contracts) can manipulate with the vote without revealing its content. And even if hackers were to intercept the data, encryption would keep them from reading the vote and making changes. The secure vote is now permanently cast on the blockchain and not open to modification or even destruction. Moreover, public key cryptography makes it possible for voters to confirm the votes they have cast and at the same time, it guarantees the privacy of their selections. Smart contracts can add an additional layer of trust as they can automatically verify eligible votes and ensure only legitimate votes are counted, and reduce the number of fraudulent votes. It prevents the man-in-the-middle attack, vote tampering, and unauthorized access. In E2EE, blockchain voting systems provide a higher level of security, privacy, and trust to the voters. At the end of the day, end-to-end encryption is the only way we can trust our election results, to try and make them as transparent as possible, and to resist attempts at digital cyber-attacks.

Anonymity techniques (e.g., Homomorphic encryption, Ring signatures) Blockchain E-voting systems are incorporating anonymity techniques, like homomorphic encryption, ring signatures among others in order to guarantee not only that the anonymity of voters is protected but also that election integrity is maintained. Homomorphic encryption enables votes to be encrypted and computations performed (e.g., voting/counting) without decrypting the votes, so without revealing how anyone voted. That is, election officials can use the votes to count the votes without ever needing to view the vote; and concurrently guaranteeing voter anonymity. Ring signatures add an extra layer of anonymity by allowing the signature of a voter to be combined with others so that the vote cannot be tied back to any single person. Its appeal is that nobody not even election officials, can link a vote to a voter while still being able to certify the voting as genuine. It prevents the threat of vote coercion, front voting, excessive voting conceal and unauthorized access therefore increasing the confidence in election process. These cryptographic functions make the blockchain voting systems offer transparency, anonymity and fair a secure voting. Homomorphic encrypted votes followed by distributed verification guarantee that the voter's choice is hidden, which renders the voting scheme resistant to cheating. Lastly, we describe the anonymity techniques that guarantee authentication, confidentiality and integrity to blockchain-based voting systems.

It avoids vote coercion, front voting, over the shoulder working and unauthorized access which hence increase the trust in election process. These cryptographic functions made possible transparency, privacy and fairness (unforgeable) of the blockchain voting systems. Distributed verification of homomorphically encrypted votes ensures that the voter's' choice remains secret, thereby resulting in a vote system cheat-resilient campaign. Finally, we present the anonymity mechanisms that ensure authentication, confidentiality and integrity in voting systems based on blockchain. Voter identity is protected such as zero-knowledge proofs (ZKP) man-in the middle and impersonation attacks. In any way of presenting your (with other words) granted voter coercion: with such methods as homomorphic encryption or ring signatures ensure that everyone sees only the anonymous votes and not a link between this particular single and someone else. (Because of some privacy provisions of blockchain, even if a voter were to be coerced into voting in a particular way, it would not be possible for a third party to verify how that person voted.) Also, smart contracts can code voting envelopes such that only eligible voters have the authority to vote and illegal double voting will not happen. Its distributed ledger technology (DLT) makes it so that individuals cannot tamper with election results, lessening the potential for corruption. Blockchains solve this as a trusted third-party and provide e-voting system with the two properties of cryptographic security and

decentralization - that's why they can withstand the security attack, defend against unnecessary pressure, or please everyone, in a fully private, secure, and resilient e-voting process.

4.9 User Interface

Web/Mobile Voting: A blockchain based Web/Mobile e-Voting system has used by the voters a user-friendly and all in one app to have a secure and ease to vote in the elections. Using these tools, end-users are able to complete voter registration, identity verification, and voting in the ballots from a remote location with a smartphone or a computer, eliminating the need to visit a physical polling station. Security or privacy mechanisms such as biometric authentication, multi-factor authentication (MFA), and use of cryptographic keys reduce the entry to only authorized parties. Every vote is protected as a cipher and sent to the block chain to prevent it from being tampered with or exposed.

The app often provides live tracking features that allow voters to confirm their vote has been pressed while safeguarding the privacy of the vote, and this can improve transparency as well as voter confidence. Designed to be universally accessible by all voters, regardless of technical know-how, it can also incorporate accessibility tools like screen readers or voice-activated navigation for those with disabilities. There's no vote rigging when once placed, the votes are preserved in a decentralized blockchain architecture, ensuring fairness and transparency. It would naturally make voting far more flexible, secure and accessible in a wider variety of situations.

Secured and Efficient voting Accessibility: In electronic voting E-Voting applications, Voters could use blockchain through simple form for casting their votes during Elections. These systems come with simple user interfaces for access using web or mobile applications controlled by layer of security and they are also manage remote voting. Voting with access restrictions Only entitled voters are allowed to vote using several methods like multi factor authentication solutions, biometrics or cryptographic credentials.

This transmitted data are secured with end-to-end encryption (E2EE) to avoid manipulation, peering or unauthorized access. Vote validation and submission Smart contracts automate vote validation and submission process to minimize human interaction prone to errors. Privacy respecting technologies (e.g.: zero-knowledge proofs and ring signatures): voter anonymity is guaranteed with no possibility of voters being threatened into voting a certain way, and also without having votes be monitored by someone else.

Even non-technical users will find the system easy to use - its design is intuitive. As a low-cost piece of software, it offers everything small businesses need in an asset management system. The distributed nature of blockchain removes the possibility for a single entity to change the election outcomes, or mediate the results. Voters are able to check that their vote is included in the final outcome, without giving away who he or she voted for, supporting system integrity and trust. Blockchain based e-Voting Both systems take advantages of blockchain technology to facilitate secure authorization, convenience, and transparency, and thereby makes a credible and non-tamper-able e-voting system.

Provides real-time updates and information: A blockchain e-voting system shows real-time information and updates to the voters and eliminates the guessing game during elections. Instant notifications about key points like registration confirmation, periods voting starts and

ends or successful submission of the vote are provided to voters. The live updates concerning voter participation rates and election process offering by the system do not disclose individual votes, which makes it open but still private. Thanks to the blockchain technology, it is impossible to post or edit fake news or any comments, because all the information is verified and immutable. Notifications can be delivered by SMS, email or in-app alert, ensuring voters are informed. Counting and reporting votes in real time gives election officials and the public the opportunity to watch the results as they roll in, minimizing uncertainty and running time. Smart contracts manage the process, so that only verified, genuine votes are included. The distributed ledger ensures that updates are kept in sync and consistent among all devices and platforms. Voters can also be reminded to vote before closing time, facilitating better participation. Real-time notifications and alerts facilitated by blockchain e-voting increase transparency, participation, and confidence in the election system.

4.10 Election Management

Election Management Administrative Dashboard: A blockchain based E-voting system comes with an administrative dashboard that serves as a tool for election organizers to efficiently and securely manage the overall election process. The control room allows officials to check in on registered voters, set the status of one's election and monitor the participation as it occurs with clear transparency. Role based access control (RBAC) guarantees that only the appropriate staff can access or modify the system data and functionality.

Through the dashboard, administrators can check their on-the-fly voting statistics and anonymous participation data and steer the general course of the election without risking to obstruct it. The smart contract holds the tech behind voting deflecting human error or manipulation by making it automatic.

Security: The system also includes built in security capabilities to prevent against unauthorized access and provide an audit trail of administrative sessions, such as MFA and granular audit logs. Instant notifications ensure voting staff can immediately address key information, including performance irregularities or security concerns. Every process inside the dashboard is published to the blockchain so everything becomes fully transparent and traceable.

It also provides election organizers with in-depth audit reports after the election process to promote transparency and ensure verification. The administrative dashboard helps to enhance the credibility of digital voting systems by offering secure, user-friendly and transparent facility to manage elections.

Voter registration, election timeline, and result publishing the e-voting system based on blockchain manages the voter registration, election timeline, and result publishing effectively using secure and automated admin panel. Election administrators can use the system to enter eligible voters, verifying the voters with biometrics, government-issued ID cards or cryptographic authentication. The smart contracts automate enforcement of election timeframes, so that voting opens and closes as scheduled and so that voters are not able to cast ballots early or late. It offers election officials and voters real-time status information, so everyone stays informed of critical events. When voting concludes, the votes are automatically computed and combined on the blockchain to prevent fraud and error. Independent observers can audit the results which are tamper-proof as they are recorded in a

decentralized ledger. The live results posting lets voters, media, even elections workers track the count as it happens with increased transparency. RBAC (role-based access control) restricts changes to elections settings to authorized officials and holds those officials accountable. The system also produces reports as well as audit logs for verification after the election. Through the automation of these procedures, blockchain e-voting guarantees efficient, transparent and secure voting for both voters and administrators.

Knows-how to connect with government databases: A blockchain based e-voting system can know-how to connect with the government databases to prohibits only the desired citizen take part in the poll. By tapping into national ID systems, biometric databases and voter lists, the system can authenticate voters automatically on the spot. Smart contracts apply eligibility rules to combat duplicate registrations, underage voting, or mischievous usage. By using zero-knowledge proofs (ZKP), the system is able to validate the right of a voter to vote without revealing any personal information. Such as biometrics or one-time password (OTP) is used as multi factor authentication (MFA) for the extra security. Through the blockchain all "yes" verified voter entries are stored without the possibility of any changes to avoid identity fraud. The election is granted the possibility to cross-reference databases with the flick of an on switch, allowing for voter lists to be more accurate and current. Automation minimizes the risk for human mistakes in the verification process and adds security. The integration with the government systems additionally assists in the identification of ineligible or deceased voters, and enhances the overall election integrity. Through the use of government databases, blockchain voting means that elections are secure, transparent, and free of fraud.

5 Results and Discussions

The blockchain-based E-voting system was effectively developed and tested in a controlled test bed. Results from the evaluation showed significant improvement on security, transparency, and voter confidence over traditional E-2 systems.

Security and Data Integrity: The use of blockchain in voting ensures the security of signed ballots and their immutability. Through the application of public-private cryptosystems, the identity of the voter is never disclosed but validation is possible. Because blockchain is tamper-proof, chances of altering vote or deleting them are low.

Transparency and Verifiability Votes results are recorded on the distributed ledger, thus enabling voters and registered observers to verify results in real time. Full audit trail can be created after the election without sacrificing voter privacy.

Voter Trust Both the openness and decentralization of the system was cited by trial users as increasing their trust that their vote would be counted honestly. Being able to witness in person their vote bolstered their belief that the system was fair and reliable.

System performance and Scalability Tests were run with a different number of voters and the system worked well for smaller (e.g. student driven or internal organization) elections. But problems with transaction volume and leggy consensus systems such as Proof of Work, made scaling the system for national use difficult.

Cost-effectiveness: The initial cost of blockchain installation can be expensive, however, the cost of operation is much lower over time due to the reduction in the requirement for human resources, automation, and no physical material used like paper ballot.

Limitations Known: The users should have some Digital knowledge and have the facility of internet enabled device. Factors such as node centralization and the type of consensus protocol could influence the decentralization of a system. Moreover, large-scale implementation would necessitate harmonisation with current statutory regimes and the national identity systems.

6 Conclusions

This paper highlights the development and implementation of a secure electronic voting system aimed at replacing traditional paper-based voting. The project focused on enabling voters to cast their votes remotely via the internet while ensuring security and reliability. Extensive research was conducted on existing online voting systems, various server-side technologies, and security threats. The system was designed using a structured approach, emphasizing user-friendly interfaces. Testing played a crucial role in identifying potential shortcomings and ensuring system readiness for deployment. Ultimately, the project achieved its primary objectives by delivering a simple, secure, and efficient online voting system, with room for future enhancements, such as improved password security and advanced voting result visualization.

Potential security threats that could compromise the integrity of the online voting system were identified and analyzed, with corresponding countermeasures explored to enhance the system's security. Various software development methodologies were examined, and after thorough evaluation, the Waterfall model was selected as the most suitable approach for developing this project.

References

[1] Hajian Berenjestanaki, M., Barzegar, H. R., El Ioini, N., & Pahl, C. (2024). Blockchain-Based E-Voting Systems: A Technology Review. *Electronics*, *13*(1), 17. https://doi.org/10.3390/electronics13010017

[2] Sharp, M., Njilla, L., Huang, C.-T., & Geng, T. (2024). Blockchain-Based E-Voting Mechanisms: A Survey and a Proposal. *Network*, *4*(4), 426-442. https://doi.org/10.3390/network4040021

[3] Sheer Hardwick, F., Gioulis, A., Akram, R. N., & Markantonakis, K. (2018). E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 1561–1567. https://doi.org/10.1109/Cybermatics_2018.2018.00262

[4] Gandhi, S. S., Kiwelekar, A. W., Netak, L. D., & Wankhede, H. S. (2023). Security requirement analysis of blockchain-based e-voting systems. In G. Rajakumar, K. L. Du, C. Vuppalapati, & G. N. Beligiannis (Eds.), *Intelligent communication technologies and virtual mobile networks* (Lecture notes on data engineering and communications technologies, Vol. 131). Springer. https://doi.org/10.1007/978-981-19-1844-5_6

[5] Thakkar, J., Patel, N., Patel, C., & Shah, K. (2021). Privacy-preserving e-voting system through blockchain technology. *2021 IEEE International Conference on Technology, Research, and Innovation for Betterment of Society (TRIBES)*, 1–6. https://doi.org/10.1109/TRIBES52498.2021.9751618

[6] Russo, A., Anta, A. F., Vasco, M. I. G., & Romano, S. P. (2021). Chirotonia: A scalable and secure e-voting framework based on blockchains and linkable ring signatures. *2021 IEEE International Conference on Blockchain (Blockchain)*, 417–424. https://doi.org/10.1109/Blockchain53845.2021.00065

[7] Kumar, M. (2021). Securing the e-voting system through blockchain using the concept of proof of work. *2021 International Conference on Technological Advancements and Innovations (ICTAI)*, 423–427. https://doi.org/10.1109/ICTAI53825.2021.9673389

[8] Tyagi, A. K., Fernandez, T. F., & Aswathy, S. U. (2020). Blockchain and Aadhaar based electronic voting system. *2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, 498–504. https://doi.org/10.1109/ICECA49313.2020.9297655

[9] Pandey, A., Bhasi, M., & Chandrasekaran, K. (2019). VoteChain: A blockchain based e-voting system. *2019 Global Conference for Advancement in Technology (GCAT)*, 1–4. https://doi.org/10.1109/GCAT47503.2019.8978295

[10] Vijaya Kumar, A., Sarvani, G. V., & Satya, D. (2020). Blockchain based public cloud security for e-voting system on IoT environment. *IOP Conference Series: Materials Science and Engineering, 981*(4), 042013. https://doi.org/10.1088/1757-899X/981/4/042013

[11] Barański, S., Szymański, J., Sobecki, A., Gil, D., & Mora, H. (2020). Practical I-Voting on Stellar Blockchain. *Applied Sciences*, *10*(21), 7606. https://doi.org/10.3390/app10217606

[12] Ohize, H. O., Onumanyi, A. J., Umar, B. U., et al. (2025). Blockchain for securing electronic voting systems: A survey of architectures, trends, solutions, and challenges. *Cluster Computing, 28*, 132. https://doi.org/10.1007/s10586-024-04709-8

[13] Braghin, C., Cimato, S., Cominesi, S. R., Damiani, E., & Mauri, L. (2019). Towards blockchain-based e-voting systems. In W. Abramowicz & R. Corchuelo (Eds.), *Business information systems workshops. BIS 2019* (Lecture notes in business information processing, Vol. 373). Springer. https://doi.org/10.1007/978-3-030-36691-9_24

[14] Chafe, S. S., Bangad, D. A., & Sonune, H. (2021). Blockchain-based e-voting protocol. In M. Tuba, S. Akashe, & A. Joshi (Eds.), *ICT systems and sustainability* (Advances in Intelligent Systems and Computing, Vol. 1270). Springer. https://doi.org/10.1007/978-981-15-8289-9_23

[15] Díaz-Santiso, J., & Fraga-Lamas, P. (2021). E-Voting System Using Hyperledger Fabric Blockchain and Smart Contracts. *Engineering Proceedings*, *7*(1), 11. https://doi.org/10.3390/engproc2021007011