IOSR Journal of Mobile Computing & Application (IOSR-JMCA)
e- ISSN: 2394-0050, P-ISSN: 2394-0042.Volume 11, Issue 5 (Sept. – Oct. 2024), PP 07-13
www.iosrjournals.org

Decentrailized E-Voting System Using Blockchain

Sarthak Burmi, Soumya Ranjan Barik, Deepanshi
School of Computer Applications Manav Rachna International Institute of Research And Studies MCA

Abstract
This research paper examines the implementation of an electronic voting application using blockchain technology, specifically employing Solidity and Ethereum smart contracts. It explores how blockchain can enhance election processes by ensuring security, immutability, and transparency in electronic voting systems.
Keywords: *Blockchain, Ethereum, Sepolia, Solidity, Flutter, and Dart.*

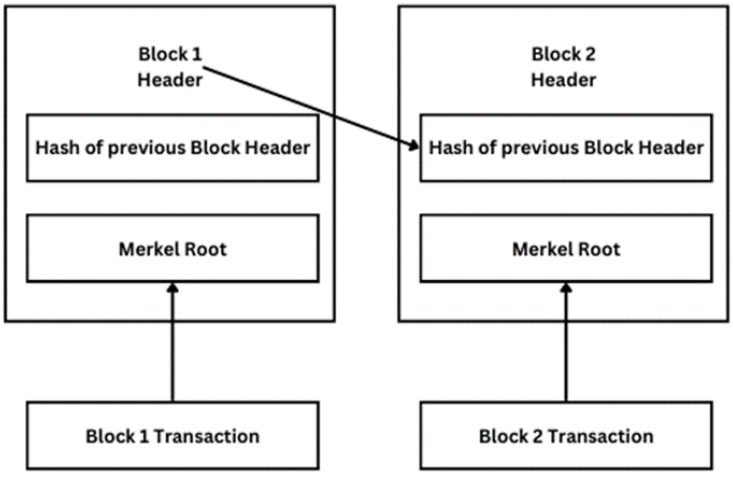
Date of Submission: 17-10-2024 Date of Acceptance: 27-10-2024

I. Introduction

Electronic voting systems have been the subject of numerous studies; however, due to inherent security flaws, widespread adoption of these systems has been impeded. Voters can cast their ballots using laptops and smartphones. Using strong security, voter anonymity, transparency, and dependability, blockchain technology is explored in this work as a means of improving electronic voting. Since vote legitimacy problems plagued the US Pentagon's online voting system in 2005, it is evident how difficult it is to create a secure electronic voting system. This highlights the potential of blockchain for decentralized data storage by showing how it can be used to create a voting application that is more resilient to hacking and stops data modifications.

Blockchain

Blockchain technology uses cryptographic hashing to create a distributed, decentralized ledger that tracks the origin of digital assets. This ensures security and transparency. It works in a similar way to how Google Docs allows multiple users to share documents in real-time, forming a decentralized chain where all users can see changes at the same time. Blockchain is more secure and sophisticated, though. It avoids the single points of failure common to centralized systems and keeps an expanding list of data records that are secure from alteration. Blockchain is made up of cryptographically connected blocks that provide improved fraud resistance, decreased uncertainty, and transparency.[5]



Blocks: A Merkle tree is created by hashing and encoding each transaction within a blockchain block. Blockchains are made up of blocks connected by cryptographic hashes. Every block has a cryptographic signature, key data, and a timestamp. Verification of transactions occurs when someone exchanges data using their private key. Three essential elements comprise a block: a data segment, a 32-bit value known as a nonce, and a 256-bit value called a hash. The nonce generates the cryptographic hash for each block in the SHA-256 algorithm, which uses hash encryption to secure the data.

Nodes: No single computer can possess the chain in blockchain development. With the aid of the chain's center points, it is dispersed in instep. Centers can take any form, like an electronic device that maintains copies and keeps the system operating.

E-voting using Blockchain

Voting is one of the many areas where blockchain has become essential. It is difficult to develop a secure electronic voting system because every detail needs to be done just right. Here are some benefits of e-voting on blockchain technology:

Greater Transparency: Open and distributed ledgers enhance visibility.
Inherent Anonymity: Voter identities are protected.
Security and Reliability: Increased resilience against denial-of-service attacks.
Immutability: Ensures strong integrity for the voting process and individual votes.

By dispersing voting data among multiple computers, blockchain technology eliminates the possibility of voter fraud and builds voter-government trust. Long lineups at polling places are eliminated when people vote using computers or cellphones. Blockchain technology doesn't require the government to reorganize already-in-place systems. Blockchain's ability to process only brief text strings that record transactions, however, is one of its main drawbacks. Blockchain is enhanced by the Interplanetary File System (IPFS), which provides the necessary infrastructure for decentralized data storage.[1]

Existing Model

Both the traditional paper-based voting method and the centralized digital voting system have limitations. Paper-based voting systems are prone to human error, voter fraud, and voting process delays. Due to their reliance on a single point of authority, centralized online voting systems, while convenient, present security risks due to the potential for hacking, data breaches, and manipulation. These models are opaque and weaken public trust because voters cannot verify that their votes were cast and counted correctly. Due to their vulnerability to fraud, corruption, and voter impersonation, these systems are less secure and reliable for large-scale elections.

II. Literature Review

Morocco recently implemented an electronic voting system based on blockchain technology to improve electoral security and transparency, one of the case studies of which is highlighted in the research. As demonstrated by plans for national elections utilizing blockchain technology, the results imply that this technology can greatly enhance the integrity and transparency of the electoral process.[23].

Due to their ability to increase electoral efficiency, lower costs, and increase voter turnout, electronic voting systems have grown in popularity. Traditional electronic voting systems, however, have issues with security, transparency, and scalability. [26].

The shortcomings of traditional electronic voting systems have been suggested to be addressed by blockchain technology. Blockchain-based voting ensures voting process integrity by providing improved security, immutability, and transparency. It also makes it difficult to tamper with or alter vote records. [25].

The integrity of the voting process is maintained while voter privacy and anonymity are protected by blockchain-based electronic voting systems that use cryptographic techniques.[21].

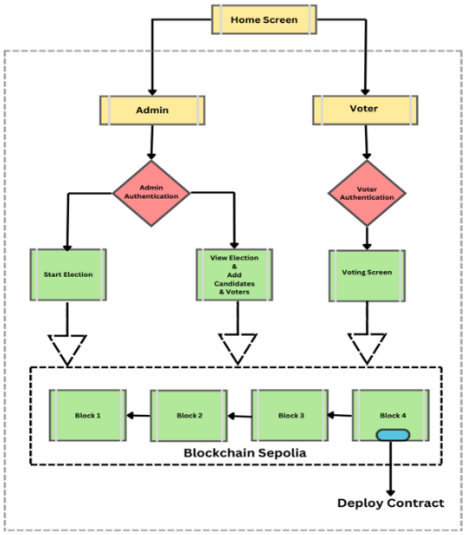
Furthermore, by offering a transparent and safe election process, blockchain technology can lower the possibility of fraud and manipulation [27].

There are potential benefits to blockchain-based electronic voting systems, but there are also a number of issues that need to be resolved. And the feasibility, effectiveness of these systems in practical environments needs to be further investigated. [24].

EVM Issue	Blockchain Solution	How Blockchain Resolves or Mitigates the Issue
Tampering & Hacking	- Decentralized ledger.	- Blockchain's decentralized nature makes it extremely difficult for a single entity to tamper with the system.
	- Cryptographic security.	- Transactions (votes) are cryptographically secured, preventing unauthorized access or manipulation.
Voter Verifiability	- Transparent and auditable records.	- Voters can verify their vote on the blockchain in real-time while maintaining anonymity.
	- Immutable voting record.	- Once recorded, votes cannot be altered or deleted, ensuring accuracy and trust.
Lack of Transparency	- Open-source and transparent network.	- Blockchain can operate on an open-source protocol where anyone can audit the system for transparency.
Storage & Transportation Risks	- No physical storage required.	- Blockchain eliminates the need for transporting physical machines, reducing the risk of tampering in transit.
Technical Failures	- Distributed ledger.	- Votes are stored on a distributed network, making it resistant to technical failures or power outages.
Digital Divide & Accessibility	- Remote voting access.	- Blockchain can allow secure voting from anywhere with internet access, reducing the need for tech literacy.
	- Mobile and web-based platforms.	- Accessible through mobile and web apps, reducing barriers for people with disabilities or limited mobility.
Delayed Counting with VVPAT	- Instant vote tallying.	- Blockchain can provide real-time vote tallying, reducing delays caused by manual verification processes.
Legal & Political Controversies	- Immutable, publicly verifiable ledger.	- Blockchain ensures every vote is accounted for and publicly verifiable, reducing disputes and controversies.
Vendor Dependency	- Open-source blockchain platforms.	- Reduces dependency on a specific vendor since blockchain solutions can be developed by multiple independent entities.
Insufficient Auditing	- Transparent audit trails.	- Blockchain provides a permanent and transparent record that can be audited at any time by independent parties.
Voter Travel Requirements	- Remote voting capability.	- Blockchain enables secure remote voting, eliminating the need for physical travel to polling stations.
Health Concerns (Indelible Ink)	- No physical ink required.	- Blockchain voting systems eliminate the need for physical interaction, thereby removing health risks associated with ink.
Election Day Challenges (Long Wait Times)	- Continuous and flexible voting periods.	- Blockchain can enable flexible, extended voting periods, reducing congestion and long waits at polling stations.

III. System Architecture

The system architecture is given in Figure 2.

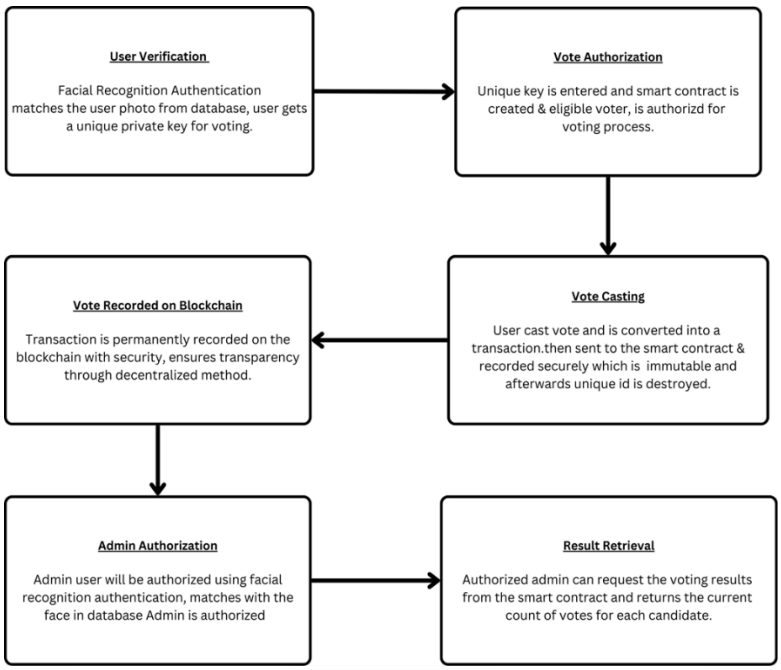


The most important part of our plan is the selection process, which includes validating administrators and voters. This is necessary to establish security within the system. [8]It is imperative to resolve any doubts regarding the propriety of someone's character, particularly in light of the fact that every vote counts. allowing voters to confirm and cast their ballots regardless of whether their information is listed in the database. Following that, the voter receives an exceptional hash address that he can use to cast a ballot. Every hash is provided along with others, allowing him to vote once. When a voter visits the app during voting day, they will see an affirmation handle. They can then cast a vote using the address that has been provided. They will also be able to view the live voting status.

IV. Proposed System

Using decentralized ledger technology on Ethereum, enhanced by Solidity smart contracts, the proposed blockchain-based voting model addresses the shortcomings of conventional and centralized systems. Voters can

verify their votes on an unchangeable public ledger, ensuring transparency. Additionally, the system uses cryptography techniques to ensure tamper-proof, secure voting. This prevents vote manipulation and fraud by doing away with the need for a central authority. The model also provides faster results with global accessibility and scalability and cost-effectiveness. The system guarantees a seamless voting experience across platforms; this increases voter engagement and trust thanks to its user-friendly interface, which was created with Flutter.



V. Implemented E-Voting System App -

Select user type Screen

Fig 1.1: Home page
Source: Author(s) Compilation

If admin is selected, enter the password

Fig 1.2: Admin Password Authentication
Source: Author(s) Compilation

Voter screen - Select the candidate you want to vote for.

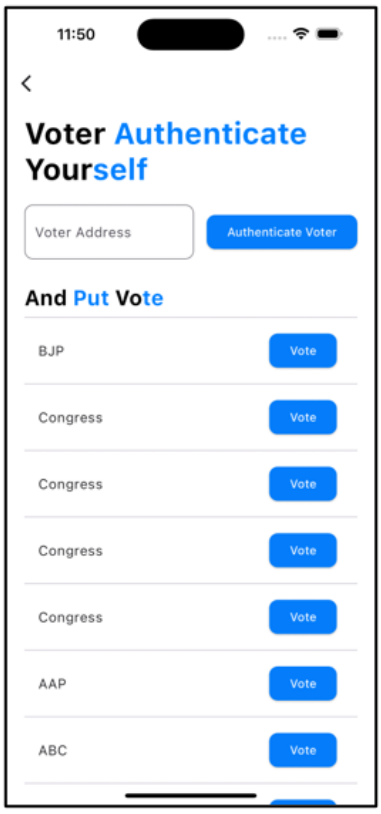


Fig 1.3: Voter authentication and vote
Source: Author(s) Compilation

This is admin screen where admin can start a new election.

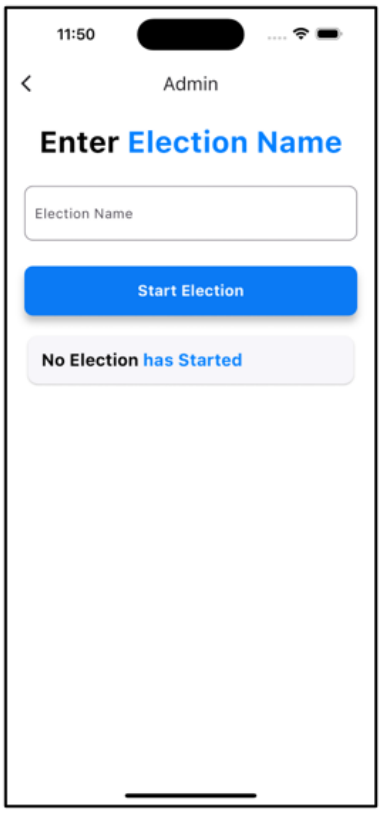


Fig 1.4: Admin to start the election
Source: Author(s) Compilation

Election Screen - see the started election details

Fig 1.5: Admin voting review panel
Source: Author(s) Compilation

Started election List - See all started elections here

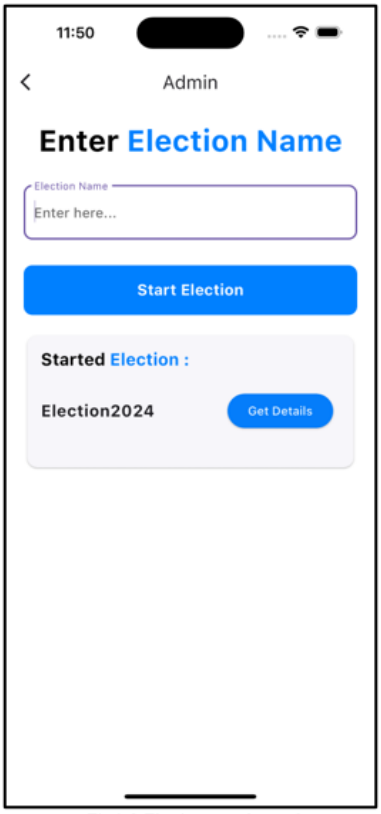


Fig 1.6: Election started pannel

VI. Representation Of The E-Voting System

We are developing a decentralized voting application using blockchain technology, which enhances security by making data nearly impossible to alter. Blockchain's decentralized nature ensures that information isn't stored in a single location, reducing the risk of hacking and ensuring data integrity[17].

I. To set up a blockchain development environment, it's essential to explore various frameworks, such as Ethereum and Multichain. [18] This project will utilize the Ethereum framework, which simplifies blockchain development, allowing developers to focus more on building applications rather than creating a complete blockchain from scratch.
II. To create a smart contract for an e-voting system, blockchain stores data in blocks, with each block containing various transactions. These transactions are verified by the smart contract before being added to the blockchain. If a transaction is not confirmed, it cannot be included in the block. The smart contract is written in a robust programming language, and Remix is a platform used to check for errors in the smart contract.[19]
III. Testing the smart contract on remix.
IV. The e-voting system will feature two modules: admin and voter. The admin interface, built with Dash and Firebase for authentication, will allow administrators to add new parties and display election results. This design ensures a secure and user-friendly experience for both administrators and voters.
V. The user interfaces for both the admin and voter modules have been developed. The admin module allows for adding member names and parties and displaying election results. The voter module displays party names and provides an option to vote, generating a transaction that adds and counts each vote.

Technology Used for E-Voting

Metamask: Metamask allows users to access the future distributed web directly from their browsers, enabling the use of Ethereum without needing to run a full Ethereum node. It includes a secure identity block, providing a user interface for managing identities across various websites and signing blockchain transactions.[20]

Flutter: Flutter, by Google, is an open-source UI toolkit for creating native apps on desktop, web, and mobile from one codebase. It uses Dart for flexible design, offers excellent performance, and supports real-time code updates.

Dart: Dart, developed by Google, is a programming language for desktop, mobile, and web apps. Known for its scalability and strong type system, it aids in error detection. Supporting both JIT and AOT compilation, Dart offers flexible deployment and integrates seamlessly with Flutter, making it ideal for high-performance cross-platform applications.

Sepolia: With a smooth transition from Proof of Work to Proof of Stake, Sepolia is a dependable Ethereum testnet that closely resembles the Ethereum mainnet. It offers a stable environment for Solidity smart contract deployment and testing to developers. To ensure that developers can use Sepolia ETH as gas for their decentralized apps on the testnet, Sepolia also provides an easy-to-use faucet service.[16]

VII. Conclusion

The study highlights the potential of blockchain technology to improve election processes' integrity, equity, and transparency. Electronic voting systems based on blockchain technology can uphold democratic principles by employing distributed consensus mechanisms, cryptographic security, and decentralization.

Important subjects covered include:

Transparency and Auditability: Voters' anonymity is protected while real-time auditing is made possible by blockchain technology, which securely stores votes. Blockchain technology enhances accessibility and inclusivity by enabling remote voting, which is especially beneficial for individuals who are unable to physically visit polling places.

Election Outcomes: Unchangeable ledgers encourage transparency and increase voter trust.

Security: By dealing with concerns like fraud, cost, scalability, and privacy, blockchain ensures voters' anonymity and the integrity of the voting process.

Additional research is required on scalability, usability, and accessibility. The study also highlights that user interface design, smart contract development, and system architecture are critical for successful implementation.

References

[1] E-Voting Using Blockchain Suraj Pratap Gupta1 And Ankur Mani Tripathi1 Paper Link
[2] A Review On E-Voting Based On Blockchain Models. (2022). Iraqi Journal Of Science, 63(3), 1362-1375. Paper Link
[3] Privacy And Verifiability Preserving E-Voting Based On Permissioned Blockchain. Sallal, M.; De Fréin, R.; Malik, A. Pvpbc:, 15, 121 Paper Link

[4] Blockchain Security: A Survey Of Techniques And Research Directions J. Leng, M. Zhou, J. L. Zhao, Y. Huang And Y. Bian In Ieee Transactions On Services Computing, Vol. 15, No. 4, Pp. 2490-2510, 1 July-Aug. 2022, Doi: 10.1109/Tsc.2020.3038641 Paper Link

[5] Implementation Of Decentralized Blockchain E-Voting Saad Moin Khan1, Aansa Arshad1, Gazala Mushtaq1,*, Aqeel Khalique1, Tarek Husein1 Paper Link

[6] A Systematic Review Of Challenges And Opportunities Of Blockchain For E-Voting. Taş, R.; Tanrıöver, Ö.Ö. Symmetry 2020, 12, 1328. Paper Link

[7] Evaluation Of Blockchain-Based Smart Contract E-Voting For National Elections. Informatics O.; Thebus, D. Architecture-Centric Paper Link

[8] Investigating Performance Constraints For Blockchain Based Secure E-Voting System Kashif Mehboob Khan , Junaid Arshad , Muhammad Mubashir Khan Paper Link

[9] A Scalable Decentralized Privacy-Preserving E-Voting System Based On Zero-Knowledge Off-Chain Computations Ashkan Emami A 1, Habib Yajam A 1, Mohammad Ali Akhaee A, Rahim Asghari Paper Link

[10] Blockchain-Based Electronic Voting Systems: A Case Study In Morocco Tarik Chafiq , Rida Azmi , Ouadoud Mohammed

[11] Improving Authentication And Transparency Of E-Voting System – Kosovo Case Blerim Rexha, Vehbi Neziri And Ramadan Dervishi Paper Link

[12] Transparent Voting System Using Blockchain V. Anitha A, Orlan Do Juan Marquez Caro B, R. Sudharsan A, S. Yoganandan A, M. Vimal Paper Link

[13] E-Voting Systems Using Blockchain: An Exploratory Literature Survey S.K. Vivek; R.S. Yashank; Yashas Prashanth; N. Yashas; M. Namratha Paper Link

[14] A Comprehensive Survey On Blockchain-Based Decentralized Storage Networks Muhammad Irfan Khalid; Ibtisam Ehsan; Ayman Khallel Al-Ani; Jawaid Iqbal; Saddam Hussain Paper Link

[15] Blockchain-Based Comparative Analysis Of E-Voting A Review Soubhagya Kumar Gochhi; Soumya Sahoo; Prabeer Kishore Samanta; Sanjeeb Kumar Panda Paper Link

[16] Electronic Voting Using Blockchain And Smart Contracts: Proof Of Concept Fáber D. Giraldo; Barbosa Milton C.; Carlos E. Gamboa Paper Link

[17] Design Of Blockchain-Based Secured Election Voting System Sumedh V. Chinchamalatpure; Smita R. Kapse; Aditya K. Balki; Vaishnavi A. Rahangdale; Vidisha K. Fulzele Paper Link

[18] Design And Development Of Smart Contract System For Blockchain Based Applications Kushwaha, Shivang, Paper Link

[19] Smart Contract Using Solidity (Remix -Ethereum Ide) Varun Tiwari, Santosh Kumar Singh, Vikas Rao Vadi Paper Link

[20] Implementation And Evaluation Of Blockchain Based E-Voting System With Ethereum And Metamask Deni Pramulia; Bayu Anggorojati Paper Link

[21] Ashkan, E., Habib, Y., & Mohammad, A. A. (2020).A Scalable Decentralized Privacy-Preserving E-Voting System Based On Zero-Knowledge Off-Chain Computations

[22] Gupta, S. P., & Tripathi, A. M. (2020). E-Voting Using Blockchain

[23] Informatics, O., & Thebus, D. (2020). Evaluation Of Blockchain-Based Smart Contract E-Voting For National Elections.

[24] Kashif, M. M., Junaid, A., & Muhammad, M. (2020). Investigating Performance Constraints For Blockchain Based Secure E-Voting System

[25] Leng, J., Zhou, M., Zhao, J. L., Huang, Y., & Bian, Y. (2022). Blockchain Security: A Survey Of Techniques And Research Directions.

[26] Sallal, M., De Fréin, R., & Malik, A. P. (2020). Privacy And Verifiability Preserving E-Voting Based On Permissioned Blockchain.

[27] Tarik, C., Rida, A., & Ouadoud, M. (2020). Blockchain-Based Electronic Voting Systems: A Case Study In Morocco.

[28] Taş, R., & Tanrıöver, Ö. Ö. (2020). A Systematic Review Of Challenges And Opportunities Of Blockchain For E-Voting