International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

E-Voting using Blockchain: Moving Away from the Ballot Paper

Irvine Mutandiwa[1], Calvin P Mugauri[2], Maronge Musara[3]

[1] MTech Cloud Computing, H. I. T, Zimbabwe

[2]MTech IT - Networking, V. I. T, India

[3]MTech Cyber Security and Forensics, SRM IST, India

Abstract: ***The technology of blockchain can solve the issues that arise with conventional voting systems. It introduces decentralization, transparency, and resistance to manipulation in e - voting. Each vote is securely recorded on the blockchain, allowing for independent verification. Blockchain - based e - voting systems also offer benefits such as remote participation and anonymous yet verifiable voting. To ensure its feasibility, scalability, and security, additional research and collaboration are needed. Challenges like network resilience and user - friendly interfaces need to be addressed. Overall, blockchain - based e - voting can enhance the democratic process, improve efficiency, and restore trust in electoral outcomes.***

Keywords: Blockchain Technology, Network resilience

1. Introduction

In recent years, electronic voting (e - voting) has gained popularity but concerns about security and integrity persist. The technology of blockchain has emerged as a potential solution for the secure and transparent electronic voting. [1]By utilizing blockchain, an e - voting system can offer benefits such as easy registration and verification of voters, Counting votes in real - time., and the protection of voter privacy through the use of Linkable ring signatures. [2] This paper explores developing a blockchain - based voting system to ensure secure, trustworthy elections.

Problem Definition

The current voting systems used in many countries are frequently plagued with disputes such as voter fraud, lack of transparency, and difficulties in verifying the authenticity of votes. Concerns about the legitimacy of election results have been raised due to issues leading to a loss of trust in the electoral process. [5]

To ensure the integrity of the electoral process, a secure and transparent voting system is necessary to overcome current challenges Blockchain technology is gaining attention as a potential solution due to its tamper - proof and decentralized nature, which makes it suitable for securely recording transactions. [8], [10]

Several challenges need to be addressed in existing blockchain - based voting systems.12]For instance, many of these systems do not provide an easy way for voters to register and verify their identities. Additionally, some systems do not allow for real - time vote counting, which can delay the announcement of election results.

Furthermore, privacy concerns remain a major issue in electronic voting systems. Without adequate measures to protect voter privacy, individuals may hesitate to participate in the electoral process due to fears that their personal information could be compromised.

To address these challenges, developing a blockchain - based voting system that effectively tackles the identified issues and ensures secure and transparent e - voting processes is crucial. This can be achieved by implementing an easy registration and verification process for voters and real - time vote - counting capabilities. [13], [16] Additionally, this system should incorporate measures such as Linkable ring signatures to defend voter privacy and ensure verification of authenticity while preserving the anonymity of the signer.

2. Background

Conventional voting systems have long been inundated by challenges such as deceptive activities, mistiness in the process, and operational inefficiencies. Paper - based ballots are vulnerable to manipulation, miscounting, and disputes, while centralized electronic voting systems give rise to concerns regarding security and privacy. In recent times, the advent of blockchain technology and smart contracts has offered a potential solution to these challenges, paving for the development of e - voting methods that are protected, transparent, and efficient.

Blockchain technology, popularized by cryptocurrencies like Bitcoin, is a dispersed and distributed ledger system. [1] In a blockchain, transactions are recorded in a chronological and incontrovertible manner across a network of computers. Each transaction, or vote in the case of e - voting, is confirmed by multiple contributors, or nodes, in the association via a consent mechanism, such as proof - of - work or proof - of - stake. [1] [2] Once authenticated, the transaction is appended to a block and interconnected with the preceding blocks, creating a sequence of interconnected blocks, hence the term "blockchain. " This decentralized and immutable characteristic of the blockchain renders it a well - suited platform for securely recording and preserving votes.

Smart contracts are essential for blockchain e - voting systems, as they eliminate intermediaries and ensure

Licensed Under Creative Commons Attribution CC BY

transparency and security. They perform functions such as voter authentication, vote casting, counting, and result declaration through automated execution based on pre - defined conditions. This guarantees fairness and accuracy, making the voting process more trustworthy. [6] [8] [12]

The combination of blockchain technology and smart contracts in e - voting systems offers numerous advantages, including transparent and verifiable voting records, reduced risk of manipulation, decentralization, redundancy, and fault tolerance through participant consensus, and streamlined processes with automated vote counting and result tabulation, enhancing the veracity, efficiency, and trustworthiness of the voting progression. [5] [6] [7]

The enactment of e - voting systems that leverage blockchain and smart contracts presents various challenges. These include technical considerations like scalability, privacy, and energy consumption. Additionally, establishing legal and regulatory frameworks that align with election laws is crucial. Furthermore, cultivating acceptance and trust among the public, politicians, and stakeholders is essential to promote the widespread adoption of such systems. [2] [11] [12] The diagram below shows the basic operation of a linkable ring signature.

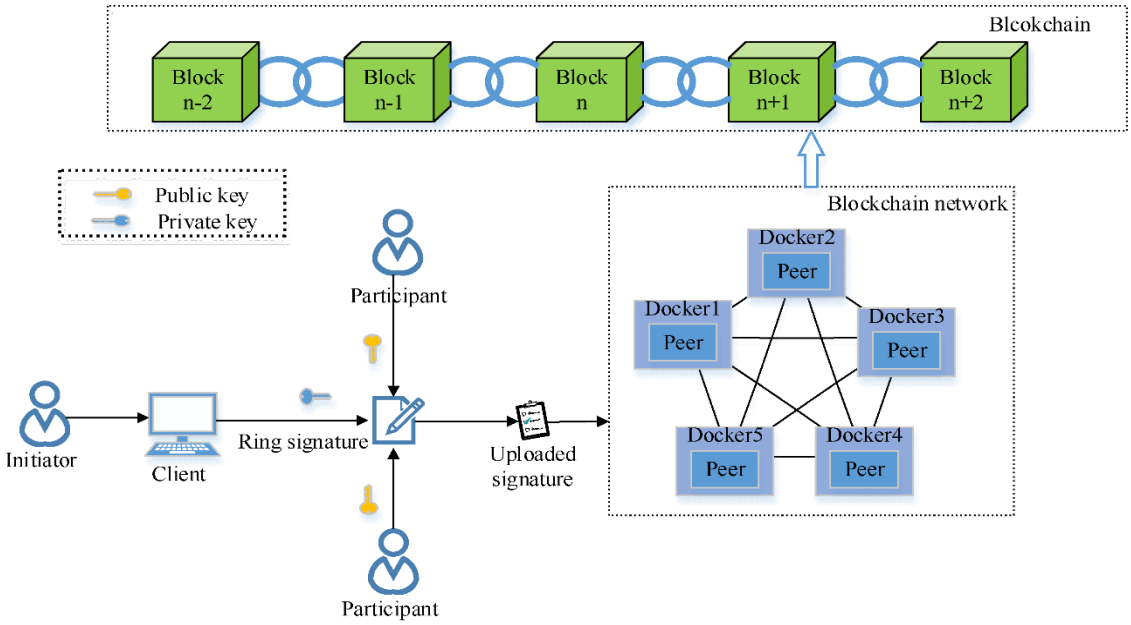

Figure 1.1: Ring signature basic operation flow [15]

Integrating blockchain technology and smart contracts into e - voting systems can overcome the limitations of traditional voting. This integration has the potential to augment clarity, security, and efficiency, thereby strengthening trust in the electoral process and reinforcing democratic governance. [6] [8] Understanding the full potential of blockchain - based e - voting systems requires careful planning, testing, and collaboration among technology experts, policymakers, and society. Successful implementation hinges on the collective effort to address technical, legal, and social considerations. [14] [15]

3. Related Work

The use of blockchain technology in voting systems has garnered significant attention due to its potential to enhance transparency, security, and efficiency. [7] Blockchain has been extensively studied as a potential solution for the challenges faced by traditional voting systems including voter fraud, vote manipulation, and lack of transparency. [11] [13]

The authors Bingsheng Zhang, Xiaohui Liang, and Hao Wang allude to a blockchain - based e - voting system that harnesses the immutability and decentralization characteristics of blockchain technology. [1]The study presents significant findings, including the creation of a protected and private e - voting system that guarantees transparency, immutability, and decentralization. The proposed system automates voting with smart contracts for eligible voters. Furthermore, the authors developed a proof - of - stake (PoS) consensus mechanism to safeguard against double - spending attacks. [1] Asif et al. (2019) support the use of smart contracts in e - voting systems, emphasizing their ability to enforce voter eligibility, preserve anonymity, prevent tampering with voting records, and guarantee accurate election results. [2] In many research studies, each focuses on a specific aspect, such as immutability and decentralization, and its associated drawbacks. However, other researchers have highlighted the importance of a blockchain system that ensures voter privacy, prevents double voting, and safeguards the integrity of election results by incorporating privacy - enhancing features like zero - knowledge proofs and ring signatures to protect voter anonymity. [3] Numerous studies on blockchain e - voting systems have suggested various measures to enhance the security and privacy of voting data. Cryptographic techniques are utilized to maintain the confidentiality, integrity, and availability of data, thus improving security and privacy. The system also includes features such as multi - factor authentication, voter anonymity, and tamper - proof audit trails, which collectively reinforce the system's security and privacy aspects. [4]

Licensed Under Creative Commons Attribution CC BY

In their article, Safavi et al. (2023) present a blockchain - based e - voting system that leverages ring signatures to enhance privacy. The authors simulated the system's performance to evaluate security, privacy, and efficiency. The results indicate that the proposed system effectively withstands attacks such as double - spending, Sybil attacks, and vote buying. Furthermore, the system offers robust privacy protections by preventing the tracing of individual votes back to specific voters. [5] Perera et al. (2022) provide an overview of group signatures and ring signatures, highlighting their ability to enable anonymous authentication and signing of messages. The paper explores the characteristics of cryptographic techniques, such as anonymity, untraceability, unlinkability, and revocation, and delves into practical considerations like signature size and efficiency. Tas et al. (2020) present a review paper that explores how blockchain technology can address challenges in e - voting by offering a secure, transparent, and decentralized platform. The study discusses numerous blockchain - based e - voting systems and protocols, encompassing permissioned/permissionless blockchains, smart contracts, and cryptographic techniques like zero - knowledge proofs. [7]

Authors have proposed modifications to the proof - of - work consensus algorithm in blockchain systems to prevent double - spending and fraud in e - voting. These modifications involve integrating multi - factor authentication, encryption, and other precautions measures to strengthen the veracity and confidentiality of the e - voting process. [8] Consensus algorithms like proof - of - work, proof - of - stake, and Byzantine fault tolerance have the potential to enhance network security. These algorithms are valued for their ability to promote system reliability and integrity. [9] Panja and Roy (2021) presented an end - to - end verifiable e - voting system that combines blockchain and cloud servers to ensure the integrity and transparency of the voting process. Every vote is recorded on the blockchain as a transaction by the system, while the cloud servers provide additional storage and computational resources for verification. The paper includes encryption, digital signatures, multi - factor authentication, and a mechanism for anonymous yet verifiable voting. [10]

The paper outlines challenges and research questions for blockchain e - voting, including scalability, interoperability, and usability. It concludes by discussing the opportunities and potential benefits of blockchain - based e - voting, such as increased voter participation and improved trust in the integrity of the electoral process. After reviewing multiple studies on techniques for using blockchain in e - voting, several critical factors need to be considered when selecting a suitable model for implementation:

When selecting a model for executing e - voting employing blockchain, it is imperative to consider the following factors:

To ensure a secure and effective blockchain - based e - voting system, stakeholders should consider the following factors:

1) Security: The system should be resilient against various attacks and protect against unauthorized access.
2) Transparency: The voting process, including counting and tabulation, should be transparent and easily auditable.
3) Verifiability: Voters should have the ability to authenticate that their votes have been accurately verified and held.
4) Privacy: The system must safeguard the privacy and anonymity of voters.
5) Usability: The system should be user - friendly and accessible to all eligible voters.
6) Scalability: It ought to be capable of operating a large number of transactions and voters without compromising security or performance.
7) Interoperability: The system should integrate smoothly with other electoral technologies.
8) Governance: Clear roles and responsibilities should be defined for all stakeholders involved in the e - voting process.
9) Standardization: Adherence to standardized protocols and best practices ensures consistency and interoperability.

By considering these factors, stakeholders can select a blockchain - based e - voting model that meets their specific needs and requirements, while providing a secure, transparent, and verifiable electoral process. To address irregularities in e - voting systems, Farooq et al. (2022) propose a framework that utilizes blockchain technology to enhance transparency. The framework comprises four main components: the voter client, the blockchain network, the election authority, and the results aggregator. Each component has a specific role, with the voter client casting votes, the blockchain network logging and verifying votes, the election authority managing the voting process, and the results aggregator tabulating and reporting the results. The authors conduct a thorough analysis of the system's enactment and security, including a simulation in a real - world election scenario. The results show that the voting process is transparent, confidential, and accurate. [11], [12]

Blockchain - based e - voting systems offer potential benefits in transparency, security, and efficiency. Proposed mechanisms include smart contracts, proof - of - stake consensus, cryptographic proceduresexample zero - knowledge proofs and linkable ring signatures, and group signatures to address traditional voting system challenges. These include voter fraud, vote manipulation, lack of transparency, and seclusion concerns. Blockchain e - voting systems offer secure and private voting experiences by ensuring admissibility, preventing attacks, and maintaining result integrity. However, practical considerations and trade - offs remain for implementation.

4. Contributions

- The proposed framework aims to address gaps in e - voting systems using blockchain.
- Offers a segmental approach for building dispersed, stable, certifiable, and mountable e - voting systems.
- Provides instruments for customization and flexibility in different e - voting scenarios.
- Incorporates linkable ring signatures to ensure privacy and verifiability in voting.

Licensed Under Creative Commons Attribution CC BY

- Formal security analysis supports the use of linkable ring signatures.
- Linkable ring signatures enable anonymous yet auditable voting.

Blockchain - Based E - Voting Systems: Benefits and Limitations

1) Blockchain technology in e - voting provides tamper - resistance and immutability. When a vote is registered on the blockchain, it is permanently recorded and cannot be altered or deleted. The blockchain's distributed nature ensures secure voting by requiring most of the network computing power to change a vote, making it highly unlikely and economically unfeasible. [13]
2) Distributed consensus mechanisms, like Proof of Work (PoW) or Proof of Stake (PoS), are essential to electronic voting systems. They validate and authenticate votes, ensuring agreement among network participants and safeguarding against manipulation. Any attempts to tamper with votes are quickly detected, thereby upholding the integrity of the election process.12]
3) Blockchain e - voting systems provide transparency and auditability by recording all voting transactions on a decentralized ledger. This ledger is accessible to all participants, allowing for public scrutiny and verification of the voting process. As a result, trust and confidence in the fairness and accuracy of the system are enhanced. [11]
4) Blockchain technology employs cryptographical techniques to bolster security in e - voting, safeguarding voter privacy, maintaining anonymity, and ensuring the integrity of the voting process. Through cryptographic algorithms, voters can be authenticated without divulging personal information, and the authenticity of votes can be verified using cryptographic signatures. [2]
5) E - voting systems based on blockchain technology eliminate the possibility of a single point of failure by removing the need for central authorities. The decentralized nature of the blockchain, which is governed by predefined rules and smart contracts, helps to mitigate the risks associated with relying on a single entity and reduces the chance of manipulation or bias. [8]
6) Blockchain - based e - voting systems provide an immutable audit trail that allows for the tracing and verification of all transactions. This ensures transparency and integrity by easily detecting any attempts to manipulate or alter voting results. [5]
7) Blockchain technology resists cyber - attacks, including DDoS attacks and data breaches. Its distributed nature and cryptographic security measures make it highly resilient against hacking attempts. The consensus mechanism ensures operational continuity even if some nodes are compromised. [4]
8) Blockchain - based e - voting systems build trust by offering transparency, tamper - resistance, and auditability. Participants can trust the security and accuracy of their votes, fostering confidence in the democratic process and addressing concerns about electoral fraud. This promotes wider participation and strengthens democracy. [10]

It is essential to integrate voter registration, authentication, voting, and tallying into electronic voting systems.

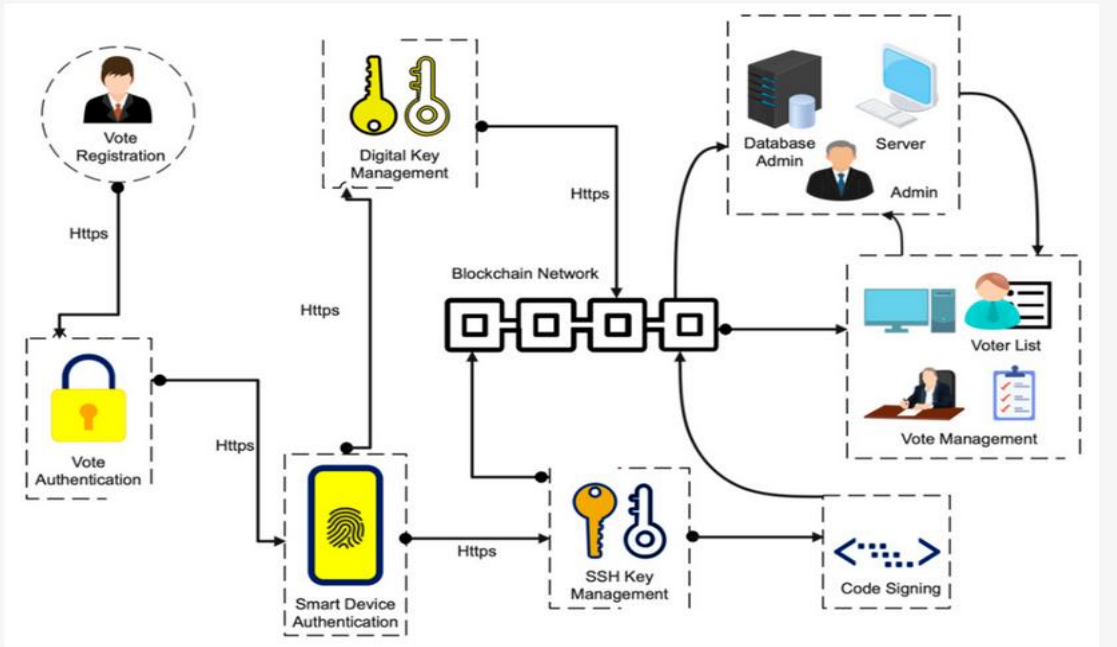

Figure 1.2: E - voting System Architecture [16]

E- voting System Architecture

1) Blockchain Network: The blockchain's distributed nodes combine to form a shared ledger. Platform and consensus mechanisms are chosen based on scalability, security, and performance needs.
2) Smart contracts: govern e - voting, ensuring transparency and automation. .
3) Voter Interface: allows voters to authenticate, access, and cast their votes securely and intuitively.
4) Identity Management: Systems verify and authenticate voter identities, employing digital signatures or multi - factor authentication for security and integrity.
5) Ballot Creation and Distribution: Secure the creation and distribution of digital ballots, maintaining

Licensed Under Creative Commons Attribution CC BY

confidentiality and integrity through encryption techniques.

6) Vote Recording and Validation: Votes are securely recorded on the blockchain using digital signatures or zero - knowledge proofs, ensuring vote integrity and validity.
7) Consensus Mechanism: Ensures secure and decentralized agreement among blockchain nodes for validating and adding votes to the blockchain.
8) Auditing and Verification: Independent auditing and verification through access to the blockchain ledger, supporting the validation of election integrity and generating audit trails.
9) Robust measures, including encryption, access control, and cryptographic protocols, protect against unauthorized access, tampering, and manipulation of votes and voter data, ensuring confidentiality, integrity, and privacy.

Development tools used (programming languages used):

1) Laravel

An open - source PHP web framework that follows the MVC pattern. It offers a streamlined approach to building web applications and APIs, with an expressive syntax, powerful tools, and a vast ecosystem of packages and libraries.

Laravel include:

- Routing: Laravel offers a straightforward and elegant routing system to define application routes.
- ORM (Object - Relational Mapping): Laravel's Eloquent ORM simplifies database interaction with an intuitive syntax for querying and manipulating data.
- Template Engine: Laravel utilizes the powerful and flexible Blade template engine, enabling developers to create clean and reusable views.
- Middleware: Laravel's middleware feature filters incoming HTTP requests, making it convenient to handle tasks like authentication and session management.
- Authentication and Authorization: Laravel offers a comprehensive authentication system with user registration, login, password reset, and more. It also provides robust authorization features for defining roles and permissions in your application.
- Caching: Laravel supports multiple caching systems, such as file - based and database caching, which can greatly enhance application performance.
- Testing: Laravel offers a testing framework for writing and executing unit tests, ensuring code stability and quality.

Laravel is a popular PHP framework known for its developer - friendly syntax, robust features, and modern development practices. It has a large and active community that provides abundant resources, tutorials, and packages to assist developers in getting started and solving common issues.

2) Solidity is a specialized programming language specifically designed for creating smart contracts on blockchain platforms, particularly Ethereum. It is commonly used in the development of various applications, including e - voting systems**.**

- Solidity is a programming language that facilitates the development of smart contracts for e - voting systems. These contracts define the rules and logic governing processes like voter registration, ballot creation, vote casting, tallying, and result auditing.
- Data Storage: Solidity provides data structures and syntax for defining and storing data on the blockchain. You can use variables, structs, and arrays to store voter details, ballot information, and voting results. Solidity also supports mapping data structures that allow efficient key - value storage.
- Security and Access Control: Solidity provides security and access control features for e - voting systems. Modifiers and access control keywords allow restricting functions or data to authorized individuals or roles, preventing unauthorized access and ensuring only eligible voters can cast their votes.
- Event Emission: Solidity allows you to emit events within smart contracts to notify the external world about specific occurrences or changes in the contract state. In the context of e - voting, you can emit events for actions like new ballot creation, vote casting, or the declaration of election results. These events can be listened to by the front end or other smart contracts to trigger appropriate actions.
- Integration with External Contracts: Solidity supports the interaction of smart contracts with other contracts on the blockchain. This can be useful for integrating with additional functionalities, such as identity verification systems, external voting registries, or result auditing contracts.
- Testing and Deployment: Solidity provides testing frameworks like Truffle and tools like Ganache for testing and simulating blockchain environments. You can write trial cases to ensure the correctness and robustness of your smart contracts. Once tested, the contracts can be compiled and deployed to the blockchain network using tools like Remix, Truffle, or web3. js.
- Security Considerations: Building secure e - voting systems with Solidity requires careful attention to potential vulnerabilities. It's crucial to follow best practices, such as avoiding re - entrance issues, preventing integer overflow/underflow, and conducting thorough security audits.

Creating protected and decentralized e - voting systems on blockchain platforms is made possible by Solidity. However, it is crucial to have expertise in Solidity programming and blockchain security. Consulting with blockchain development and security experts is highly recommended to safeguard the integrity and privacy of the e - voting system.

Required Tools:

1) Laravel
   Laravel is a robust PHP web framework for building e - voting systems on the blockchain. It integrates with smart contracts for vote recording and validation, provides secure backend functionality, and offers user - friendly interfaces. With authentication and authorization features, Laravel ensures secure

Licensed Under Creative Commons Attribution CC BY

participation and leverages blockchain benefits for transparency.

2) Git
Git can improve e - voting transparency, auditability, and immutability via blockchain integration. Security measures, access controls, and validation mechanisms are crucial to protect the voting process. Consulting Git and blockchain experts ensures a secure implementation.
3) VSCode
VSCode is an IDE for efficient development of blockchain e - voting systems, offering comprehensive features for writing, debugging, testing, and collaborating on smart contracts.
4) MetaMask Chrome Extension (install on any Chrome - based browser eg Chromium, Google Chrome, etc)
MetaMask is a browser extension for user - friendly interaction with blockchain networks like Ethereum, suitable for blockchain e - voting systems. However, ensuring security requires measures like secure smart contracts, data handling, encryption, and thorough security audits. Protecting user identities and voting process integrity is crucial.
5) Ganache CLI
Ganache CLI is a command - line tool for local Ethereum development and testing. It simulates a blockchain environment for deploying and interacting with smart contracts. However, deploying an e - voting system on a real Ethereum network requires additional considerations like security audits and validation before production deployment.
6) Truffle
Truffle is a popular Ethereum development framework that simplifies building and deploying smart contracts for e - voting systems. It provides a structured framework, testing utilities, deployment management, and debugging capabilities, streamlining the workflow and enhancing security and reliability.

System Components and Interactions

Components and their interactions:

- Voters: Eligible voters use electronic devices to cast votes with unique digital identities and cryptographic keys.
- Candidate Registration: Candidates register on the blockchain through a smart contract for proper recording and verification.
- Smart Contracts: Handle voter registration, verification, vote tallying, ensuring transparency and auditability.
- Blockchain Network: Stores transactions and smart contracts, can be public or private/consortium for decentralization and access control.
- Consensus Mechanism: Validates transactions, achieves agreement on the blockchain state (e. g., PoS, PBFT).
- Encryption and Privacy: Protects voter privacy with techniques like linkable ring signatures and secure vote transmission.
- Voter Interface: A user - friendly interface for voters to interact with the e - voting system through apps or web portals.

Linkable Ring signatures

Linkable ring signatures provide anonymous signing while linking signatures in a ring. They detect double - spending or double - voting without revealing identity or message. Steps:

Step 1: Key Generation:

- Each potential signer generates a distinctive key pair, consisting of a private key and its own public key.

Step 2: Ring Creation:

- A ring is formed by selecting a group of potential signers. The public keys of these signers are included in the ring.

Step 3: Signature Generation:
Create a linkable ring signature for a specific message, the signer follows these steps:

- Choose a public key from the ring, at random, to serve as the actual signer's public key. Generate a signature on the message using the real signer's private key.
- To create decoy signatures, the remaining public keys in the ring, excluding the actual signer's public key, are used. A random selection of potential signers is made, and their private keys are utilized to sign the message.
- Combine the real signer's signature and the set of decoy signatures to form the linkable ring signature.

Step 4: Verification:

- To verify a linkable ring signature, anyone can perform the following steps:
- Verify the individual signatures within the ring using the corresponding public keys.
- Check if any of the signatures in the ring match the real signer's signature. If a match is found, the signature is considered valid and linked to a previous signature.
- Confirm that the linkable ring signature is correctly formed and satisfies the desired properties.

Step 5: Linkability:

- The linkability property of the ring signature allows the detection of double - spending or double - voting. By comparing the unique identifiers of the linked signatures, it is possible to identify if a signer has participated in multiple signatures.

Select a secure and well - vetted linkable ring signature scheme for e - voting systems, considering variations in details, algorithms, properties, security assumptions, and efficiency.

5. Methodology

In an e - voting system utilizing blockchain technology, user interaction for voting is facilitated. Smart contracts are essential components that automate contractual obligations and actions, eliminating the need for manual intervention. By operating on a decentralized network, these smart contracts enhance security, reduce errors, and foster trust in the voting process. [1]

Smart contracts automatically enforce encoded terms and conditions, eliminating manual enforcement and reliance on

Licensed Under Creative Commons Attribution CC BY

intermediaries. When predefined conditions are met, they execute agreed - upon actions without further intervention. Programmable in blockchain - specific languages like Solidity, they provide a flexible framework for defining complex logic and rules in decentralized applications (DApps). [3]

Proposed Framework for a Secure and Transparent E - Voting System

Voters: Eligible voters securely register with unique digital identities and cryptographic keys.

Candidate Registration: Candidates register on the blockchain to ensure proper recording and verification.

Implement a robust voter registration process where eligible voters can securely register their identities. Each voter would be assigned a unique digital identity and cryptographic keys.

The voting process isuser - friendly while ensuring security and privacy. Here's how it is achieved:

- Voters cast their votes using a secure electronic device such as a computer or smartphone.
- The system should use robust encryption to protect the confidentiality of votes during transmission.
- Implement strong authentication devices to ensure that only authorised voters can participate.
- Provide accessibility options for voters with disabilities.
- Generate a cryptographic receipt for each vote cast, allowing voters to verify their votes later.

Develop smart contracts on a blockchain platform (such as Ethereum) to manage the voting process. The smart contracts contain the following functionalities:

- Candidate registration: Candidates register their candidacy through the smart contract.
- Vote recording: The smart contract records each vote on the blockchain in an immutable manner.
- Verification: Enable electorates to independently verify that their votes were correctly taped and counted.
- Vote tallying: Implement an algorithm within the smart contract to accurately count the votes and determine the winner.

6. Conclusion

The combination of blockchain and linkable ring signatures in e - voting is an area of ongoing research. Agora and Voatz are exploring blockchain - based e - voting systems, while Monero uses linkable ring signatures in cryptocurrency. Future studies can focus on integrating both technologies for improved privacy, verifiability, and security in e - voting systems, considering factors like scalability, legal compliance, and usability.

References

[1] Bingsheng Zhang, Xiaohui Liang, and Hao Wang. "A Blockchain - Based E - Voting System with Improved Security and Privacy. " IEEE Transactions on Information Forensics and Security 14, no.5 (2019)
[2] Muhammad Asif, Muhammad Imran Tariq, and Muhammad Ali Imran. "Blockchain - Based E - Voting System for Secure and Transparent Elections. " IEEE Access 7 (2019)
[3] Yassine Maleh, Abderrahim Beni - Hssane, and Abdellah Ezzati. "A Secure Blockchain - Based E - Voting System with Enhanced Privacy. " Journal of Information Security and Applications 50 (2020): 102424.
[4] Ayesha Khalid, Muhammad Awais Shibli, and Syed Ali Hassan. "A Blockchain - Based E - Voting System with Improved Security and Privacy. " Future Generation Computer Systems 105 (2020)
[5] Seyed Mohammadreza Safavi, Amir Masoud Rahmani, and Amir Hossein Jahangir. "A Blockchain - Based E - Voting System with Enhanced Privacy Using Ring Signatures. " Journal of Ambient Intelligence and Humanized Computing (2023)
[6] A survey on Group signatures and Ring Signatures: traceability vs. Anonymity by Maharage Nisansala Sevwandi Perera, Toru Nakamura, Masayuki Hashimoto, Hiroyuki Yokoyama, Chen - Mou Cheng and Kouichi Sakurai, MDPI, 2022
[7] A systematic review of challenges and opportunities of Blockchain for E - Voting by Ruhi Tas and Ömer Özgür Tanrıöver, MDPI, 2020
[8] Trustworthy Electronic Voting using Adjusted Blockchain Technology by Basit Shahzad, IEEE Access, 2019
[9] E - Voting Meets Blockchain: A survey by Maria - Victoria Vladucu; Ziqian Dong; Jorge Medina; Roberto Rojas - Cessa, IEEE Access, 2023
[10] A secure end - to - end verifiable e - voting system using blockchain and cloud server by Somnath Panja, Bimal Roy, Science, 2021
[11] A framework to Make Voting System Transparent Using Blockchain Technology by Muhammad Shoaib Farooq; Usman Iftikhar; Adel Khelifi, IEEE Access, 2022
[12] Distributed and Anonymous E - Voting Using Blockchain and Ring Signatures by Nishay Madhani, Vikrant Gajria& Pratik Kanani, Springer Link, 2021
[13] Griggs, K., & Mahoney, W. (2019). Blockchain Technology in the Public Sector: Opportunities, Challenges, and Future Directions. Government Information Quarterly, 36 (4), 101385.
[14] Chirotonia: A Scalable and Secure e - Voting Framework based on Blockchains and Linkable Ring Signatures by Antonio Russo, Antonio Fern´andez Anta, Mar´ıa Isabel Gonz´alez Vasco and Simon Pietro Romano (2021)
[15] Representative ring signature algorithms based on smart contracts, Quide Li Eta. . lhttps: //www.mdpi. com/1424 - 8220/22/18/6805 (2022)
[16] Blockchain for the electronic voting system – review and open research challenges by Uzmar Jafar, Mohd Juzaiddin Ab Aziz, Zarina Shukur, MDPI, 2021

Licensed Under Creative Commons Attribution CC BY