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

Novel Approach for Decentralized Voting System Using Blockchain

Dr. Umapathi G R[1], Saurav Gupta[2]

Department of Information Science and Engineering, Acharya Institute of Technology, Bangalore, India
E- Mail: *umapathigr93[at]gmail.com*

Abstract: ***Electronic voting, also known as e-voting, has been utilized in various forms since the 1970s and offers significant advantages compared to traditional paper-based systems, including improved efficiency and reduced errors. Nonetheless, the widespread adoption of e-voting systems still faces obstacles, particularly in enhancing their ability to withstand potential faults. The emergence of blockchain technology, which is currently revolutionizing various industries, holds the promise of enhancing the overall resilience of e-voting systems. This paper presents a dedicated endeavor to leverage the advantages of blockchain, such as cryptographic principles and transparency, to establish an effective e-voting scheme. The proposed scheme adheres to the essential requirements for e-voting systems and ensures end-to-end verifiability. This paper offers a comprehensive overview of the proposed e-voting scheme, including its implementation utilizing the Multichain platform. Furthermore, a thorough evaluation of the scheme is presented, demonstrating its efficacy in achieving a verifiable e-voting system from start to finish.***

Keywords: Blockchain, Multichain, Cryptography, e-voting, AccessControl, Security

1. Introduction

Elections are a crucial component of a democratic system, allowing individuals to express their opinions through voting. The transparency and reliability of the election process are vital to ensure public trust. As a result, voting methods have continuously evolved to prioritize security, verifiability, and transparency. Electronic voting, or e-voting, has played a significant role in this evolution. Since its introduction as punched-card ballots in the 1960s, e-voting systems have made substantial advancements, particularly with the integration of internet technologies. However, for e-voting to gain widespread acceptance, certain essential parameters must be met, including voter anonymity, vote integrity, and non-repudiation.

Blockchain technology, known for its strong cryptographic foundations, has emerged as a disruptive solution that can enhance the security of various applications. Blockchain operates as a distributed decentralized database, ensuring the secure and tamper-proof storage and sharing of transactional data. Users can connect to the network, verify transactions, and create new blocks. Each block is assigned a cryptographic hash that remains valid unless the data within the block is altered. Consequently, blockchain technology has found increasing use in mitigating unauthorized transactions across different domains.

While Bitcoin is the most well-known application of blockchain, researchers are exploring its potential in various domains, leveraging its benefits of non-repudiation, integrity, and anonymity. This paper focuses on using blockchain to facilitate e-voting applications that guarantee voter anonymity, vote integrity, and end-to-end verification. The fundamental features of blockchain, such as self-validating transaction structures through hashes and the public availability of a distributed ledger, can significantly benefit e-voting. The decentralized and publicly distributed nature of blockchain enables efficient prevention of issues like double voting and manipulation of result transparency.

This research aims to address key challenges in e-voting, including voter anonymity, vote confidentiality, and end-to-end verification. These challenges are essential for establishing an efficient voting system that maintains the integrity of the process. The paper explores the use of blockchain technology, specifically based on the Voter approach, and utilizes the open-source blockchain platform Multichain to develop the system. To ensure vote anonymity and integrity, the system generates strong cryptographic hashes for each vote transaction based on voter-specific information. These hashes are communicated to the voter through encrypted channels to facilitate verification. The proposed system aligns with the fundamental requirements of an e-voting system identified by previous studies.

The paper is organized as follows: the subsequent section outlines the requirements for an e-voting system as identified in prior research and explains how our system meets them. The following section provides an overview of the current state-of-the-art in e-voting and describes our contribution. The system design is then detailed, followed by the implementation using Multichain and the user interface. The evaluation of the system highlights its fulfillment of the requirements presented earlier. Finally, the paper concludes by summarizing the current progress and outlining future plans.

2. System Architecture

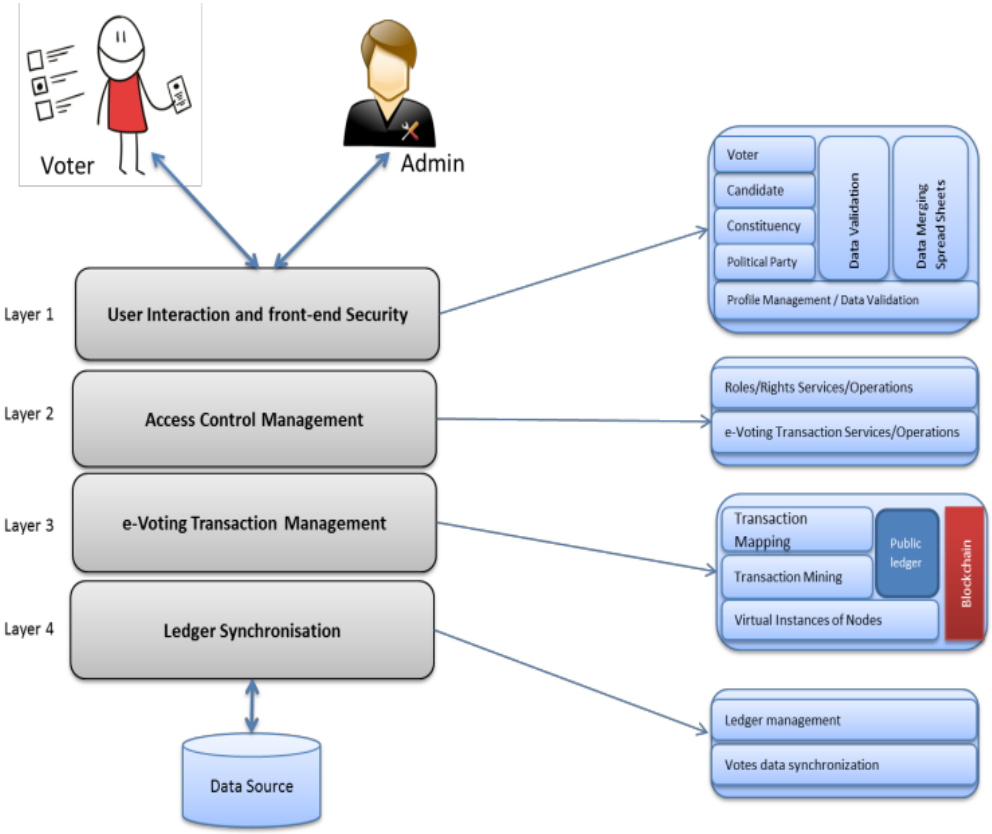


Figure 1: System Architecture

The proposed e-voting system architecture, illustrated in Figure 1, is designed with modularity in mind, consisting of multiple layers with distinct functions.

User Interaction and Front-end Security layer: This layer facilitates interaction with voters and administrators, ensuring authentication and authorization. It validates user credentials based on system-specific policies, employing methods like username/password or advanced techniques such as fingerprint or iris recognition.

Access Control Management layer: This layer supports the functions of layers 1 and 3 by providing services like defining roles, access control policies, and voting transaction definitions. Role management enables access control in layer 1, while voting transaction definitions assist blockchain-based transaction mapping and mining in layer 3.

e-Voting Transaction Management layer: This core layer maps the e-voting transaction constructed in the Role Management/Transactions layer to the blockchain transaction for mining. It incorporates voter credentials, like fingerprint data, to create a cryptographic hash that contributes to the transaction ID. Verification of credentials occurs in layer 1, and multiple virtual node instances participate in the mining process for the transaction to be added to the chain.

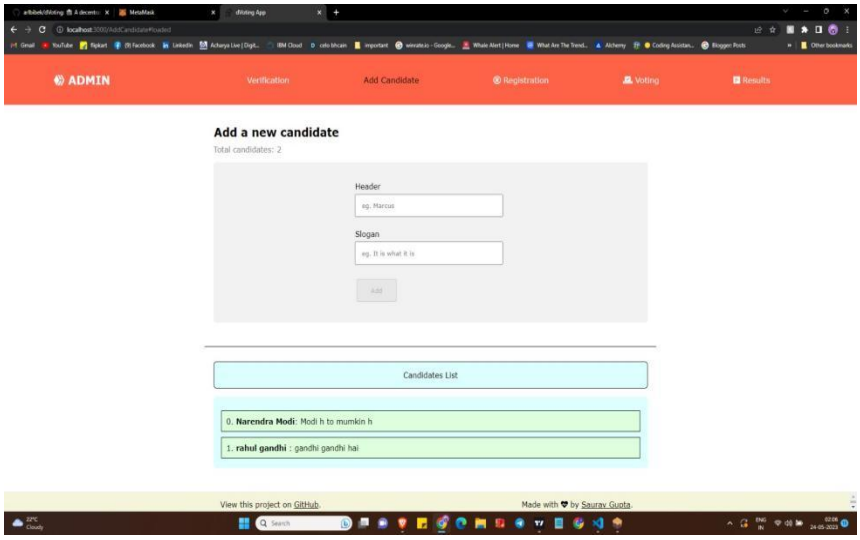
Ledger Synchronization layer: This layer synchronizes the Multichain ledger with the application-specific database using established database technologies. Votes cast are recorded in the database backend, and voters can track their votes using unique identifiers once they are mined and added to the blockchain ledger. Vote security relies on blockchain technology, utilizing cryptographic hashes for secure communication. Voting results are stored in the application's database for auditing and future operations.

3. Proposed System

The system has been meticulously designed to cater to the requirements of a real-world voting application, considering aspects such as privacy, eligibility, convenience, receipt-freeness, and verifiability. Its primary objective is to ensure secure digital voting while maintaining user-friendliness. To achieve this, the system utilizes a web-based interface that allows users to engage easily, incorporating measures like fingerprinting to prevent instances of double voting.

Recognizing the importance of managing voters, constituencies, and candidates, the system includes an administrator interface that is user-friendly and accessible. It ensures equal rights of participation for all voters and promotes fair competition among candidates while preserving voter anonymity. As a means of proof that their vote has been casted, voters receive an email containing the cryptographic hash of the transaction (ID). This enables them to track their vote even outside the premises of the constituency.

4. Voting Process



Let us now illustrate a typical user interaction with the proposed scheme based on our current system implementation. To begin, a voter logs into the system by providing their thumb impression. If a match is found, the voter is presented with a list of available candidates and the option to cast their vote. On the other hand, if no match is found, further access is denied. This authentication mechanism, in this case fingerprinting, and predefined role-based access control management enable this functionality. Additionally, voters are assigned to specific constituencies offline, and this information is used to generate the list of candidates for each voter. However, the assignment of voters to constituencies is beyond the scope of this research.

Once a vote is successfully cast, it undergoes validation by multiple miners. Valid and verified votes are then added to the public ledger using blockchain technology, employing cryptographic hashes for end-to-end verification and security. Each successful vote cast is considered a transaction within the voting application's blockchain. It is added as a new block to the blockchain after successful mining and is also recorded in the database's backend data tables. The system ensures the "one-person, one-vote" principle of democracy by leveraging the unique thumbprint of each voter, which is matched at the beginning of every voting attempt to prevent double voting. If a vote is identified as malicious during the validation process, it is rejected by the miners.

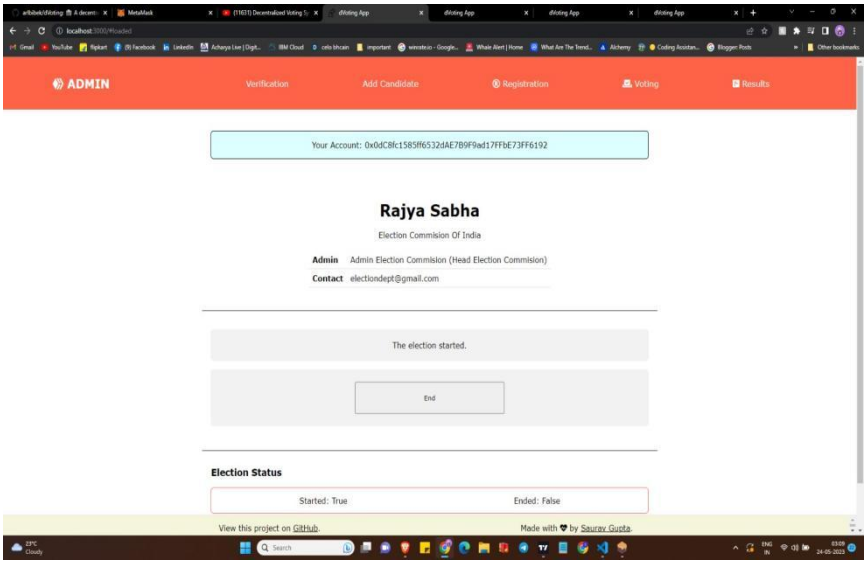
After the validation process, the system promptly sends a notification to the voter through a message or email, providing the transaction ID defined earlier. This allows the voter to track their vote in the ledger. It is important to note that this notification serves as confirmation to the voter, but it does not disclose any information about how a specific individual voted, ensuring the privacy of voters. The cryptographic hash assigned to each voter serves as their unique identifier in the blockchain, enabling verifiability of the overall voting process. Furthermore, this identifier remains hidden, even from the system operator, ensuring the privacy of individual voters.

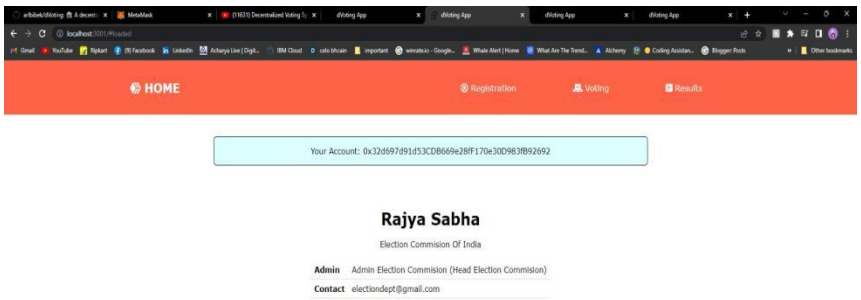
5. Implementation

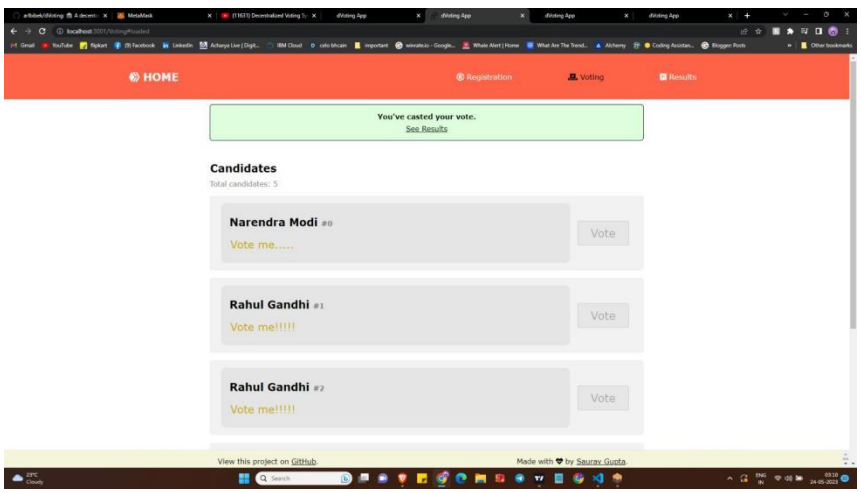
The implementation of the proposed system was conducted in a controlled environment, utilizing a web-based application as the user interface for seamless interaction. The application was developed using Java EE within the Netbeans platform, and the native Glassfish server was employed for hosting the application. The Glassfish server served as the server-side container for managing the application's Enterprise JavaBeans (EJBs) and data source. MySQL was selected as the backend database for storing application data, including voter details, constituency information, and data related to political parties participating in the election.

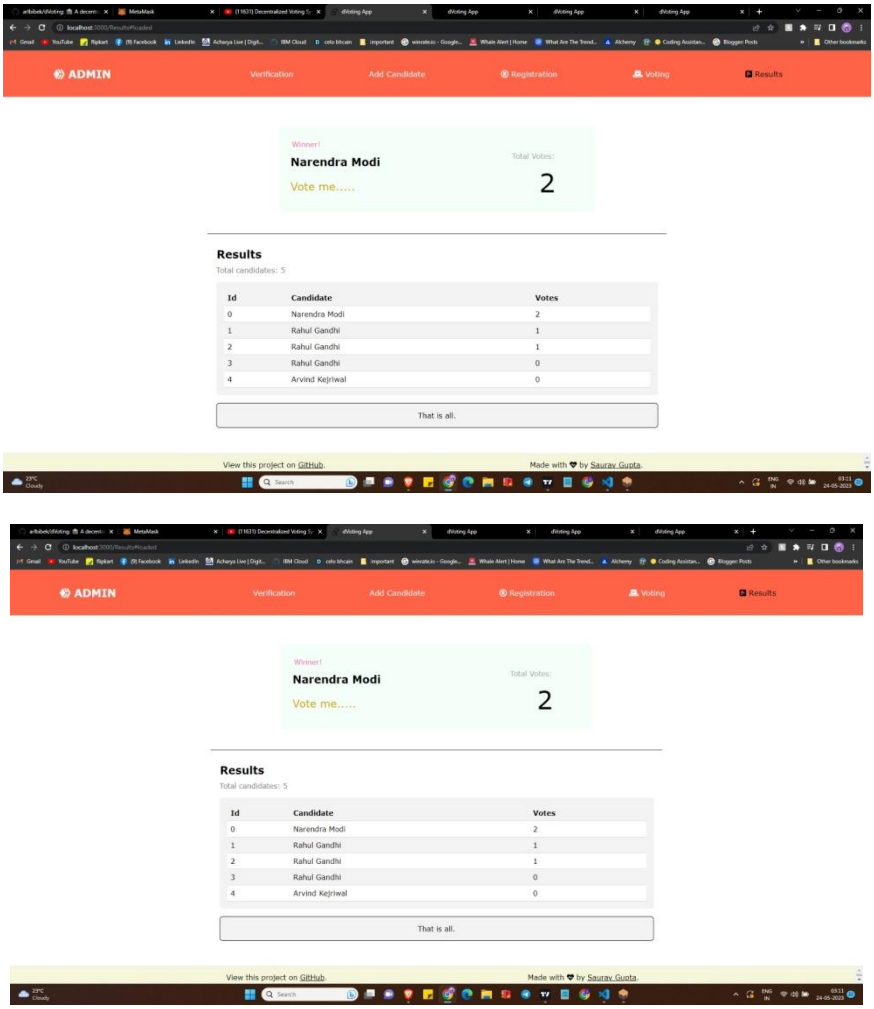
To incorporate the benefits of blockchain technology into the system, we adopted Multichain as the blockchain platform. This allowed us to create a private blockchain specifically for this application, dedicated to recording the voting transactions. The selection of Multichain was based on its user-friendly nature, which facilitated seamless integration into our proposed architecture.

6. Snap Shots









7. Evaluation and Experimentation

The evaluation of the system aimed to assess its performance based on the requirements outlined for an e-voting system and to identify any considerations for its real-world application. The evaluation process involved several steps, including conducting multiple transactions, verifying the transactions, mining them into the blockchain, reflecting the changes in the public ledger across all network nodes, and evaluating the usability of the system.

To perform transactions in Multichain, we first determined the address and balance of the node from which the asset (vote) would be sent. When sending the asset to the designated address, a transaction hash was generated to record the transfer of the vote. The balance of the receiving node was incremented by one vote (asset). This transaction was then added to the public ledger, indicating that it had been successfully mined.

It's important to note that our customized API for asset creation was designed to allow each address to have a maximum of only one vote (asset). This ensures that a voter cannot cast multiple votes unless the vote is received from a different address, which is only permissible in the case of a candidate.

8. Conclusion and Future Enhancement

Electronic voting has been utilized since the 1970s and offers advantages over traditional paper-based systems, including increased efficiency and reduced errors. The emergence of blockchain technology has prompted exploration into leveraging its capabilities for effective e-voting solutions. This paper presents an initiative that utilizes blockchain's cryptographic foundations and transparency to propose an effective e-voting solution. The implementation of this approach using Multichain is evaluated extensively, demonstrating its effectiveness in meeting the fundamental requirements of an e-voting scheme.

Building upon this work, our current focus is to enhance the resilience of blockchain technology against the "double spending" issue, which translates to "double voting" in the context of e-voting systems. While blockchain technology has made significant progress in detecting tampering with transactions, instances of successful demonstrations of such events motivate us to further investigate this challenge. Consequently, we believe that establishing a trustworthy provenance model for e-voting systems is crucial to achieve an end-to-end verifiable e-voting scheme. We are actively pursuing this objective by developing an additional provenance layer to complement the existing blockchain infrastructure.

References

[1] Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In 2016 IEEE Symposium on Security and Privacy (SP) (pp.839-858). IEEE.
[2] Teixeira, T., Fonseca, J., Ferreira, H. J., & Rodrigues, J. J. (2018). Blockchain-based secure and transparent electronic voting system. In 2018 Global Information Infrastructure and Networking Symposium (GIIS) (pp.1-6). IEEE.
[3] Zohrevand, A., & Clark, J. A. (2018). Blockchain-based voting protocol for low-power Internet of Things (IoT) devices. In 2018 IEEE International Conference on Internet of Things and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp.1023-1029). I
[4] Sturiale, D., Longo, F., &Orsini, V. (2020). Secure voting systems using blockchain. In 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp.251-254). IEEE.
[5] Rellermeyer, J. S., Schiavoni, V., &Traverso, G. (2020). Towards decentralized voting systems: A survey. ACM Computing Surveys (CSUR), 53 (4), 1-33.
[6] López-Pintado, O., &Román, P. L. (2020). Secure and private voting using blockchain technology. IEEE Internet Computing, 24 (5), 40-48.
[7] Roehrs, C., Bodendorf, F., & Manner, J. (2018). Trustworthy voting systems using blockchain technology. In 2018 51st Hawaii International Conference on System Sciences (HICSS) (pp.3523-3532). IEEE.
[8] McCorry, P., Shahandashti, S. F., &Hao, F. (2017). A smart contract for boardroom voting with maximum voter privacy. In 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp.25-33). IEEE.
[9] Weber, I., Xu, X., Riveret, R., Governatori, G., Ponomarev, A., &Mendling, J. (2016). Untrusted business process monitoring and execution using blockchain. In 2016 International Conference on Business Process Management (BPM) (pp.329-347). Springer. Decentralized Voting System Using Blockchain AIT/ISE/2022-23
[10] Sgantzos, K., Pimenidis, E., &Furnell, S. (2018). Decentralized voting system using blockchain and zero-knowledge proofs. In 2018 16th Annual Conference on Privacy, Security and Trust (PST) (pp.1-6). IEEE.
[11] Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2017). Proof of activity: Extending bitcoin's proof of work via proof of stake. ACM Transactions on Information and System Security (TISSEC), 20 (1), 1-34.
[12] Van Laerhoven, T., &Zibuschka, J. (2020). Towards secure and transparent voting systems using distributed ledgers. In 2020 IEEE 19th International Symposium