An Efficient and Secure Voting Mechanism Build on Blockchain

JayaPrakash C[1], Raja J[2] and Vignesh Perumal K[3]
{ drrajaj@veltech.edu.in[2], Vtp4209@veltech.edu.in[3]}

Associate Professor, Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai-600062, Tamil Nadu, India[1, 2]
PG Student, Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology,Chennai-600062, Tamil Nadu, India[3]

Abstract. Elections are a vital aspect of democratic states, and their integrity is a fundamental element in guaranteeing the democratic process's equity. Since the development of the blockchain technology, potential solutions to secure, transparent voting has emerged. Alternate voting systems offered by previous public blockchain voting systems however suffer scalability, privacy and access problems. In this paper, we propose a hybrid blockchain voting system that utilizes the strengths of public and private blockchains. We make our scheme scalable, secure and transparent, with the privacy and availability of voters being preserved. In order to ensure the security and scalability of the system, a hybrid consensus mechanism based on proof of work and proof of stake is adopted. In addition, we use an original zero-knowledge proof technique to ensure voter privacy, whilst maintaining security in the voting. Additionally, we provide two user-friendly interfaces to facilitate the accessibility and participation of voters and two One Time Passwords, one for voter login and one for vote verification. The recommended system could reshape voting and be a model for secure and reliable democratic voting operations.

Keywords: Blockchain, Distributed ledger, Transparency, Security, Immutability, Scalability, Voter privacy, Hybrid Blockchain.

1 Introduction

Voting is the foundation of democracy and it should have some integrity around it in order to maintain credibility in the way our government is elected. Conversely, the classical voting mechanisms are fraught with a multitude of problems such as anonymity concerns, secure voting access, and ensure the fairness of election. The invention of blockchain has created an opportunity to build a secure and transparent system of voting. In this article, we propose a blockchain-powered voting system that leverages on advantages of DLT to solve certain problems of traditional voting systems.

There are multiple benefits to using blockchains in voting systems – increased transparency, security, and irreversibility. The distributed ledger can ensure the correct voting process to maintain credibility, so that it would be challenging for the attacker to forge or modify the outcome. Also, backed by blockchain, a system can promote transparency and let anyone know and check the election results. In addition, the risk of fraud and security may decrease

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

DOI 10.4108/eai.28-4-2025.2358103

when blockchain-based system encrypt the sensitive data using strong encryption algorithms.

Yet there are a number of hurdles that they face for public blockchain voting systems to be a feasible reality. There are many challenges, and scaling is a big one since public blockchains can handle only so many transactions. Another problem is privacy, as public blockchains are inherently transparent, leaving no room for voter privacy. These limitations may prove significant impediments to the implementation of BVS in practice. In this paper, we propose a hybrid blockchain based voting system which enjoys advantages of both public and private blockchain in order to overcome these challenges. The proposed system is designed to be scalable, secure, and transparent, while ensuring voter privacy. To achieve this, Bcgame adopts a hybrid consensus mechanism that combines Proof of Work (PoW) and Proof of Stake (PoS), enhancing both security and scalability. Additionally, we introduce a novel zero-knowledge proof scheme to preserve voter privacy and maintain the integrity of the voting process. Our system is designed to be easy to use and available to most voters. We include easy-to-use interfaces that you can access from your cell phone or computer to vote from anywhere. We also offer various models to verify the voter as a valid voter or not.

One of the major advantages of our proposed work is its scalability. We can achieve such a system while maintaining voters' privacy by employing a hybrid model using public and private blockchains. Furthermore, our model provides enhanced transparency as well as systems security, both of which are essential toward a fair and democratic election.

1.1 AIM

The aim of a blockchain-based voting system is to offer a secure, transparent and convenient voting process that ensures the integrity, accuracy and accessibility. Among its targets are to enhance confidence in the electoral process, reduce costs and administrative exigencies, and foster democracy and participation.

2 Objective

The aim of a platform that benefits from a BVI model would be to provide a tamper-proof, decentralised backend that is capable of guaranteeing the integrity and accuracy of election results, while also preserving voter privacy and suffrage. The system aims at having an easy to use and convenient system for voters since they can vote easily and securely from anywhere in the world. It is also designed to enhance transparency and auditability of votes by storing all the ballots on an immutable, tamper-resistant distributed ledger. Additionally, the method aims to improve voting efficiency and expediency while reducing cost and administrative process. The end goal is to keep democracy alive, and to build trust in the electoral process.

3 Scope

Effectiveness: An enormous potential of the blockchain- based voting system is due to its capability of secure, transparent, and efficient platform for carrying out multiple types of elections, referendums, and polls. It is able to increase confidence in elections by verifying the honesty of voting results. Blockchain-based voting solutions could also lower the amount of admin and cost that goes into previous voting systems, making it easier and cheaper to vote for constituents. In general, the jurisdictions of the blockchain-based E-VS are beyond the electoral elections as they could be used in corporative, academic and community elections, and they would have the potential to impact the electoral process greatly.

4 Literature Survey

In [1], a biometrics-based voting system was proposed to address the shortcomings of current voting systems using fingerprint input verification. The received biophysiological data was compared with the database record, and only an authorized user was allowed to cast votes. The system was connected to the IoT and provided real-time results with automatic counting.

This work was extended in [2], where the authors compared various i-voting schemes with respect to voter anonymity and safeguards against manipulation. The paper offered a retrospective of major research outcomes and described methods to tackle pressing concerns in e-voting and online voting.

An online voting system based on a cloud platform was discussed in [3], where limitations of manual voting such as collusion and malpractice were highlighted. The system design utilized cloud technologies to ensure secure and equitable access to voting facilities.

A secure voting system with two-factor biometric authentication was proposed in [4], in which face recognition and fingerprint scanning were combined to avoid duplicate and false votes. This mechanism enhanced the security, efficiency, and user-friendliness of the voting system.

A smart application of electronic voting using blockchain technology was proposed in [5]. In this model, the blockchain served as a storage space for votes, with the implementation programmed using web technologies. Despite its advantages, the system remained susceptible to issues such as DoS attacks, single-node failures, and falsified record modifications.

Challenges and solutions based on blockchain techniques were discussed in [6], which also explored hybrid secure voting systems using public and private blockchains for scalability and privacy. Reference [7] presented a decentralized e-voting system with hybrid consensus for secure, scalable, and efficient elections. Similarly, [8] emphasized privacy and transparency enhancements when using blockchain for secure voting solutions.

In [9], a blockchain-based hybrid voting architecture was introduced, combined with zero-knowledge proof techniques to ensure voter confidentiality and vote integrity. The authors in [10] provided an overview of blockchain e-voting solutions, highlighting privacy-preserving approaches and identifying optimization opportunities for future digital voting systems.

5 Related Works

There is several blockchain-based voting systems avails-able, including Follow My Vote, Voatz, and Agora, which pro- vide secure and transparent voting mechanisms to prevent fraud voting, and the cost of the voting system is extremely low when compared to other e-voting and ballot voting systems. These systems employ sophisticated encryption algorithms to keep votes and data secure while remaining transparent. Some blockchain-based voting systems use

Ethereum as their fundamental platform, necessitating the use of Ethereum cryptocurrency for each and every transaction, and some will be distributed as an incentive to miners. One disadvantage of this Ethereum-based blockchain voting system is that it is a public blockchain, which means that everything, regardless of the identity of the voter or details, is available to all participants in the network. Furthermore, the Ethereum blockchain was not intended for use in a voting system because it is not scalable and cannot keep all voting data in the blockchain. Some voting systems were constructed using antiquated encryption methods such as DES. (Data Encryption Standard).

6 Proposed System

The system is based on a hybrid blockchain mechanism, which is a combination of public and private blockchains that is secured with high-security voter authentication and verification without compromising the higher degree of transparency. The system employs AES (Advanced Encryption Standard) for encrypting voter information and the RSA encryption technique for voter authentication and the voting procedure. And SHA-256 (Secure Hash Algorithm) for hashing the voters' identities to attain pseudo-anonymity while increasing vote privacy. To increase security, the system employs a hybrid consensus mechanism with smart contracts that will be per- formed on top of the blockchain, and everything is immutable according to the append only principle. The proposed system has the benefit of using a hybrid blockchain method, as sensitive information such as the voter's name, location, pincode, date of birth, email-id, and photo will be stored in the private blockchain, also known as the permissioned blockchain. Other information, such as the vote tally, result, and blockchain record, will also be kept in the public blockchain, also known as the permission less blockchain. This will aid in achieving voter anonymity, which will strengthen the system's security. To improve network security, strong security and encryption techniques have been adopted. The database we used can hold a large amount of data without sorting or running out of memory.

6.1 Architecture Diagram

- Fig. 1 depicts the design schematic of the hybrid blockchain-based voting system. The system is made up of three major parts: the blockchain, the election system, and the database. The blockchain is the system's central component, storing and managing all polling data.
- The voting mechanism is made up of voters, candidates, and administrators. The voter must fill out a form that includes the voter's name, date of birth, pincode, email address, location, and a photo, and then submit the request to the admin or the election commission.
- The admin will verify all of the information received from the voter and update the details in the database; additionally, the candidate must upload the specific logo for their party.
- The database is used to keep voter information as well as other information. The architecture of the system is intended to guarantee that the voting process is secure, transparent, and accessible.
- On voting day, the portal will be available to all, but only the voters in the

database will be able to participate in the voting process.

- The voter must input their unique id, and their identity will be verified using a one-time password. Following that, a private key will be created to ensure that the voter remains the original voter.
- After effectively casting a vote, the mining process will be completed, and the mined votes will be added to the blockchain record, which is transparent because anyone in the world can verify the record. The verified document will update the count to the respective candidate and cannot be deleted or updated, ensuring immutability.

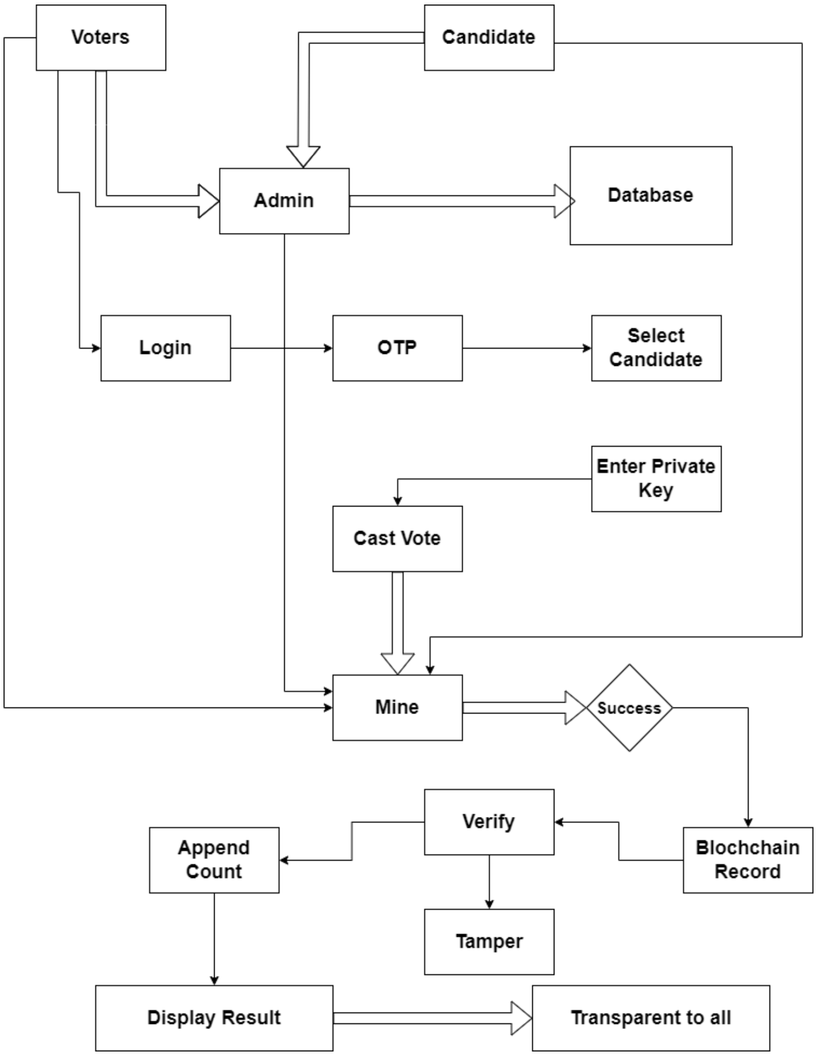


Fig. 1. Architecture Diagram.

7 Use Case Diagram

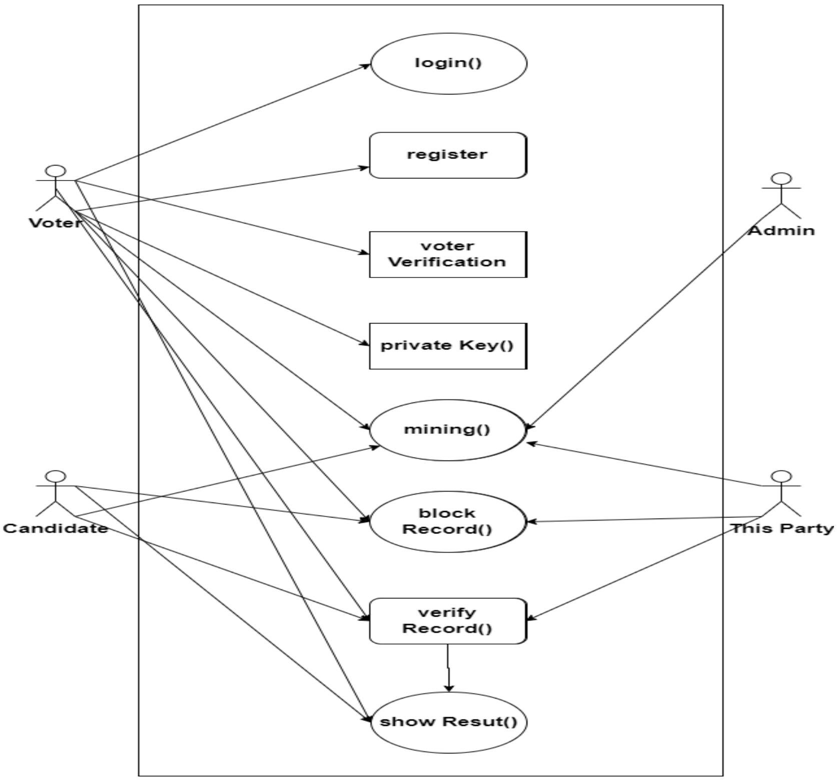


Fig. 2. Use Case Diagram.

- Fig 2 depicts the use case schematic for the hybrid blockchain-based voting system. The system is comprised of four major players.

- The primary actor in the system is the voter, who is in charge of casting votes. The infrastructure and database are managed by the administrator.

- The third party is a regular visitor from around the globe. Because the blockchain adheres to the transparent concept, all records will be visible to anyone in the world. A third party can also mine, verify records, and examine vote counts and results. The candidate is in charge of campaigning and gathering ballots.

- The use case diagram for the system is intended to guarantee that the voting process is secure, transparent, and accessible.

7.1 List of Modules

- Data Preparation.
- Identity verification.
- Mine the Votes
- Blockchain Records
- Display the Result

Data Preparation: Evidence collection in a blockchain-supported voting scheme is an indispensable part which guarantees the correctness and integrity of the voting process. The process includes signing up eligible voters and giving them a unique digital identity on the blockchain. The next step is to implement a digital ballot and voting on a digital platform. Prior to tallying votes and producing final results, the blockchain protocol authenticates the correctness and security of a vote by way of cryptographic algorithms. Block-chain based voting systems provide the solutions for these issues and limitations of traditional voting systems by incorporating cryptographic and secure storage technologies.

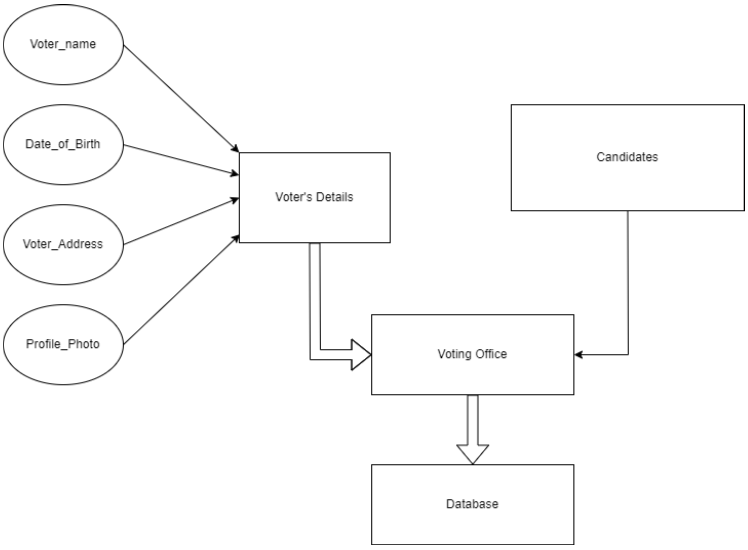


Fig. 3. Data Collection Module Diagram.

Fig 3. The above Data Collection module diagram shows a Blockchain-Based Voting System that depicts how data is collected in a blockchain-based voting system and how it is stored in a database with admin permission.

Identity Verification: In a hybrid blockchain voting system, identity verification is an essential part. It ensures that only individuals meeting eligibility requirements are voting, and that each counted vote comes from a unique person. The hybrid system checks voters' identities with both online and offline tools, including government ID, biometrics and multifactor authentication. In the proposed system, voters use a secure one-time password to login, and a secure cryptographical key to decrypt the encrypted vote. The system can maintain a tamper proof log of verified identities and securely link them to the voting data with the help of blockchain's immutable ledger. This increases the integrity of the election process and decreases the opportunity for fraud, abuse, and meddling. Identity Verification in a Hybrid Blockchain-Based Voting System 1.2 1.2 displayed in Fig 4, the verification process is done in blocks; one is at the time of logging in when the voter logs in with unique credentials and the other is when the voter selects preferred party and verified with his private key, this private key is sent along with the user credentials.

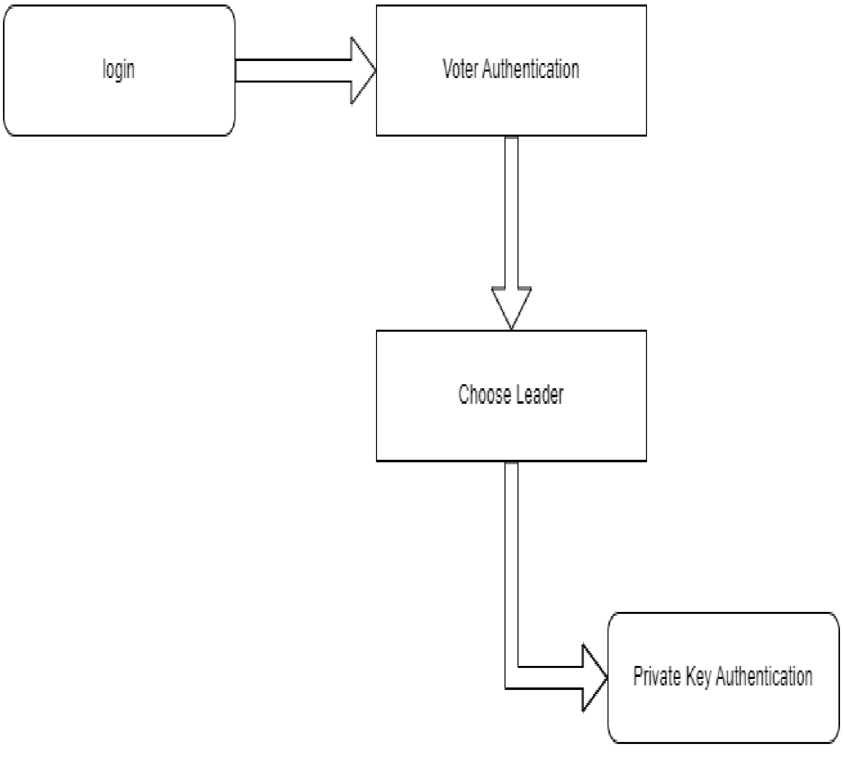


Fig. 4. Voter Authentication Diagram.

Mine the Votes: After successfully verifying the voters' identities, the voters or anyone from the network or third parties may begin the mining procedure to mine the block. After the mining process is finished, the block will be added to the blockchain with full voter information and votes in hashed values. Nobody in the network or third parties was able to determine the participants' true identities. Fig 5 The mining of votes depicts the mining procedure that takes place after the voter's identity has been verified. When a vote request is received, it is added to the network and awaits miners to mine the vote. If the mining was successful, the block will be added to the blockchain; otherwise, an error message will be presented.

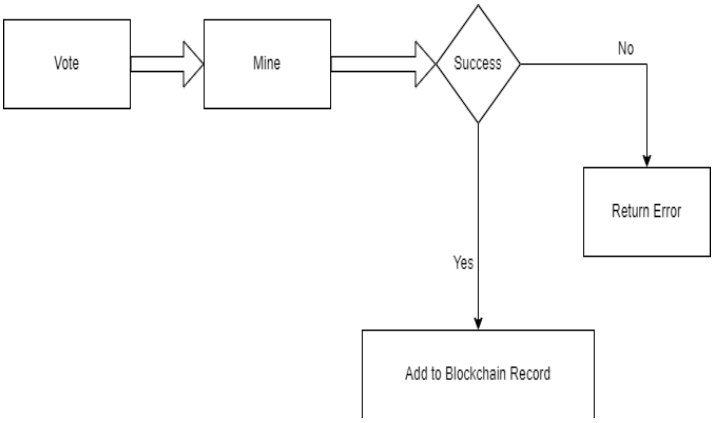


Fig. 5. Mining the Vote.

Blockchain Records: The blockchain is a publicly accessible record that anyone in the network can view. This transparency enables voters to confirm the integrity of the voting process and ensure that their votes were properly counted. The transparency of the blockchain also enables third parties to verify the integrity of the voting process and ensure that the election was fair and free of fraud. The blockchain is an immutable ledger that adheres to the append only principle, which means that data added to the blockchain cannot be altered or deleted. This feature guarantees the integrity of the voting procedure and the accuracy of the results. Fig 6 Blockchain Record depicts the complete record of events that occurred in the voting system, complete with an accurate time stamp that includes the data and time in 24-hour format. The blockchain record is made up of the genesis hash, the merkle hash, the block hash, and the timestamp, as well as the verification button, which is used to check the block. The next block includes the same information as the previous one except for the genesis hash, which is replaced by the previous block hash. This procedure will be repeated until the final block is reached. This allows the votes to be verified, and the verified record is denoted by the green sign, while the unverified record is denoted by the red sign, which includes a tampered block message.

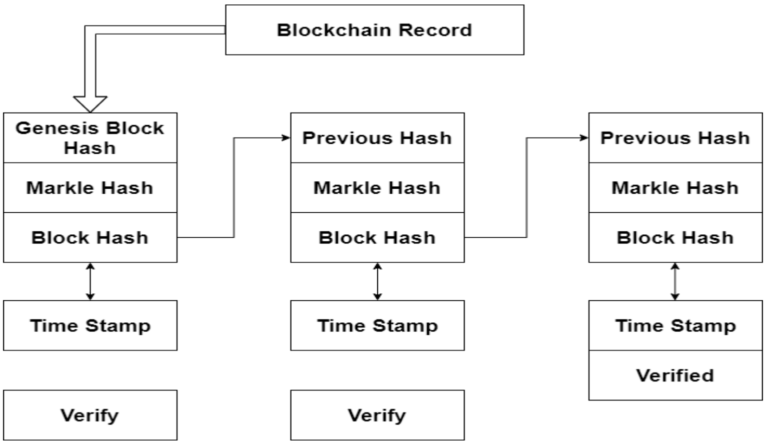


Fig. 6. Blockchain Record Module.

Display the Result: The election results are displayed on the screen once all of the verification and authorization processes, including vote mining and blockchain verification, have been finished. Every record was discovered in the blockchain, replete with log details such as the time and date of the voting process, the voters' identities, the votes, and the hash values of the votes. Anyone can verify and check the results, resulting in high confidence and the prevention of illegal activities.

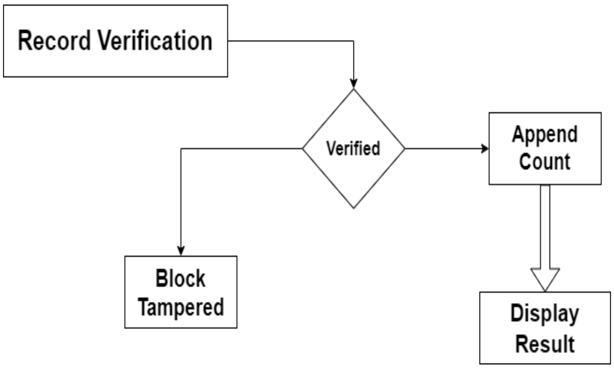
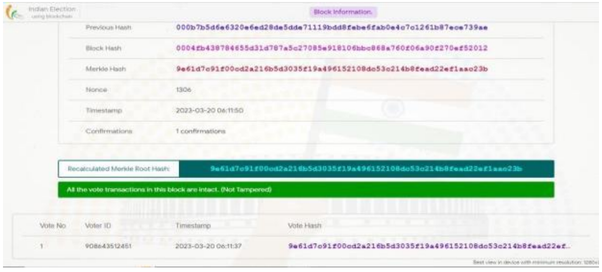


Fig. 7. Result Module.

Fig 7 Result Page is used to announce the result to the rest of the globe. The vote will be authenticated and the count to the corresponding party or candidate will be increased once the record is verified; if the record is not verified, the count will not be appended. Because it is an immutable ledger, once the count is appended to the network, it is difficult to update or delete the count, providing super security because no one can hack the ballot and change the count.

8 Sample Input and Output

Sample Input: Fig 8 depicts the voter's profile screen. Once all of the information has been saved in the database, and during the voting period, the voting portal will be available to all, and users will need to login using their unique credentials and verify their identity. Following that, the voting page, where the voter must select the candidate and press the vote button. After clicking the vote button, the voter needs to input their respective private key which was encrypted and sent to their credentials. The voter can vote after satisfactory verification.



Previous Hash	000b7b5d6e6320e6ed28de5dde71119bdd8febe6fab0e4c7c1261b87ece739ae
Block Hash	0004fb438784655d31d787a5c27085e918106bbc868a760f06a90f270ef52012
Merkle Hash	9e61d7c91f00cd2a216b5d3035f19a496152108dc53c214b8fead22ef1aac23b
Nonce	1306
Timestamp	2023-03-20 06:11:50
Confirmations	1 confirmations

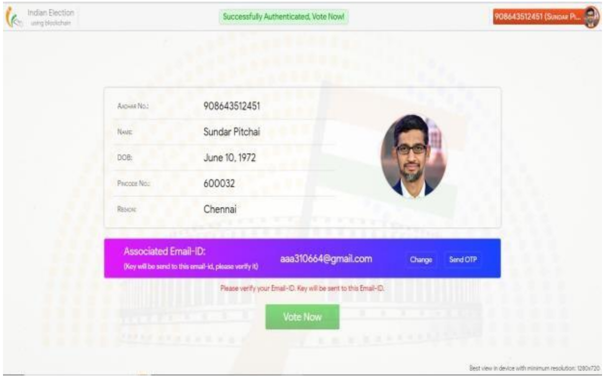
Recalculated Merkle Root Hash: 9e61d7c91f00cd2a216b5d3035f19a496152108dc53c214b8fead22ef1aac23b

All the vote transactions in this block are intact. (Not Tampered)

Vote No	Voter ID	Timestamp	Vote Hash
1	908643512451	2023-03-20 06:11:37	9e61d7c91f00cd2a216b5d3035f19a496152108dc53c214b8fead22ef...

Best view in device with minimum resolution: 1280x

Fig. 8. Sample Input.



Successfully Authenticated, Vote Now!

908643512451 (Sundar Pi...

Aadhar No.:	908643512451
Name:	Sundar Pitchai
DOB:	June 10, 1972
Pincode No.:	600032
Region:	Chennai

Associated Email-ID:
(Key will be send to this email-id, please verify it)
aaa310664@gmail.com

Please verify your Email-ID. Key will be sent to this Email-ID.

Best view in device with minimum resolution: 1280x720

Fig. 9. Blockchain Record Page.

Sample Output: Fig 9 depicts the voting system's blockchain log. The blockchain record is made up of the genesis hash, the merkle hash, the block hash, and the timestamp, as well as the verification button, which is used to check the block. The starting hash is the genesis block hash, and the merkle hash is used to guarantee the integrity of the transactions in a block. A Merkle root, which is a hash of all the events in the block, is contained in each block of a blockchain. This enables anyone to check the Merkle root against the hash value stored in the previous block to ensure that the block has not been tampered with. The block hash is determined by the information contained within the block, which includes the transaction data, timestamp, and hash of the preceding block in the chain. a, as a slug of the slug. In the blockchain, block hashes fulfil several functions. They facilitate the identification and verification of particular blocks in the chain, contribute to the integrity and immutability of the blockchain, and are used in the mining process to secure the network and validate transactions.

9 Conclusion

Finally, a hybrid blockchain-based voting system is well-positioned to address many of the limitations and problems with the existing voting systems and mechanisms. Hybrid system can secure the integrity, confidentiality and availability of the vote process and, voting system in general, by taking all the advantages of two kinds of voting while excluding their main limitations: online and offline. Since the system operates in a decentralized order, no one will have the opportunity to falsify or change the voice results. In addition, the block- chain-based system can "maintain" the process of voting providing constant review to the vote process and subsequent publication. This system can support a distance ride, which opens the doors to voting for all categories of people, not just those who have no opportunity to come and vote for their physical handicap. However, hybrid blockchain-based voting system has its issues, such as high cybersecurity risks, voter electronic marketing effectiveness, and political actors and society acceptance, and other ones. Adoption of a hybrid blockchain based voting system, is an essential step in creating more democratic transparency and a more secure voting system.

References

[1] Rahat, R., Joni, S. A., Tasnin, N., & Gaur, L. (2025). Towards secure democracy: A hybrid blockchain-enabled secure and scalable e-voting system with sharding and post-quantum cryptography. *International Journal of System Assurance Engineering and Management*. Advance online publication. https://doi.org/10.1007/s13198-025-02927-w

[2] Ohize, H. O., Onumanyi, A. J., Umar, B. U., Ajao, L. A., Isah, R. O., Dogo, E. M., Nuhu, B. K., Olaniyi, O. M., Ambafi, J. G., Sheidu, V. B., & Ibrahim, M. M. (2025). Blockchain for securing electronic voting systems: A survey of architectures, trends, solutions, and challenges. *Cluster Computing, 28*, Article 132. https://doi.org/10.1007/s10586-024-04709-8

[3] Bhavani, D. D., Gayathri, R., Bhagavanthu, M., Sheeba, A., Sampoornam, M. M., & Bhuvaneshwari, P. (2025). Blockchain-based voting systems enhancing transparency and security in electoral processes. *ITM Web of Conferences, 76*, 02004. https://doi.org/10.1051/itmconf/20257602004

[4] Miao, Y. (2023). Secure and privacy-preserving voting system using zero-knowledge proofs. *Applied and Computational Engineering, 8*, 328–333. https://doi.org/10.54254/2755-2721/8/20230181

[5] Vladucu, M. V., Dong, Z., Medina, J., & Rojas-Cessa, R. (2023). E-voting meets blockchain: A survey. *IEEE Access, 11*, 23293–23308. https://doi.org/10.1109/ACCESS.2023.3253682

[6] Taş, R., & Tanrıöver, Ö. Ö. (2020). A systematic review of challenges and opportunities of blockchain for e-voting. *Symmetry, 12*(8), 1328. https://doi.org/10.3390/sym12081328

[7] 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

[8] Wang, B., Guo, F., Liu, Y., Li, B., & Yuan, Y. (2024). An efficient and versatile e-voting scheme on blockchain. *Cybersecurity, 7*, 62. https://doi.org/10.1186/s42400-024-00226-8

[9] 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

[10] Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain for electronic voting system—Review and open research challenges. *Sensors, 21*(17), 5874. https://doi.org/10.3390/s21175874