

## SECURING E-VOTING THROUGH BLOCKCHAIN

Adneya Khatate<sup>1</sup>, Yash Garibe<sup>2</sup>, Sahil Dere<sup>3</sup>, Ritesh Dere<sup>4</sup>, Jadhav V. V<sup>5</sup>

<sup>1,2,3,4,5</sup>Computer Department Jaihind Polytechnic, Kuran, India.

### ABSTRACT

One of the most significant and vital realizations that is being used more and more in democratic nations worldwide is the voting or election process. These days, the majority of the countries that are based on monarchies and dictatorships also have elections in one form or another. Elections are also held in the corporate world, in city municipalities, and in other legal jurisdictions. This explains why voting is the foundation of the majority of practical and effective techniques for implementing public opinion. Voting guarantees that the public's voice is heard and that they have a say in the numerous policies that impact them. However, the voting procedure has not changed in millennia, despite numerous advances in a variety of fields and annual technological improvements. The most prevalent problem with updating the voting mechanism is the insecurity of the post-voting data; thus, in order to address this shortcoming, this study presents a practical and efficient method for the post-voting data security using the distributed ledger system known as blockchain. A stand-alone voting application has been developed that preserves the data integrity through blockchain, and the performance of the system has been measured through experimentation.

**Keywords-** E-Voting, blockchain, Block heads, Terminal Key, Key Evaluation.

### 1. INTRODUCTION

Using voting to make decisions is an example of political and organizational democracy. With the development of networking technology, electronic voting has been included into various decision-making situations because to its affordability, speed, accessibility, and ease of use. Before that, researchers unveiled the first electronic voting method that fulfilled the requirements of an electronic election by incorporating features like confidentiality, tamper resistance, non-repeatable, and constitutionality. In contrast, the current electronic voting processes have a single administrator in charge of the whole election process. This alternative would lead to a rigged election because of the management's deceit, and there aren't any easy fixes as of yet. The decentralized blockchain can be utilized as a ground-breaking electronic voting platform to get around the centralized authorities. This is a reaction that is adaptable enough to fulfill regular duties. The blockchain is a decentralized distributed ledger system made up of multiple interconnected servers that form a decentralized network. Furthermore, each node in the system has a public blockchain of its own, which is used to store transaction data that has already been validated by the blockchain. The information in this ledger can be accessed remotely by someone. As a result, every node inside the blockchain technology keeps an eye on and maintains this chain. When most nodes reach consensus, the transaction is identified and recorded in each node's distributed ledger, so it cannot be altered in a transparent and inclusive manner. Since the data is kept on the blockchain, all authorized nodes have had the ability to review the information gathered throughout the voting process and the outcomes. To ensure voting is more accessible and equal, all parties involved collaborate to keep an eye on the electronic voting system. Blockchain comes in three flavours: alliance channels, private channels, and public networks. The strategy can be used to situations involving small-scale campaigns, hence it is made to be implemented on the private blockchain. Every transaction creates a new block and is subject to a voting process. This tactic ensures objectivity and transparency during the electoral process as well as regarding the outcome of the election. Furthermore, node confidentiality is another feature of the blockchain architecture that can be used in electronic voting to allow anonymous voting. Rui P. Pinto stated that the main objective was to determine whether it was feasible to implement a platform that combined distributed ledger technology and m-health promoting accountability regarding electronic health records while upholding confidentiality and enabling the advancement of health data management. The procedures and tools that combine public ledgers with mobile platforms or attempt to maximize. To meet the requirements, block chain technology-enabled electronic health records were examined. This evaluation made it sufficiently clear that a repository component needed to be included in the intended technique in order to store off-chain data that is not feasible to incorporate in the block chain technology.

### 2. LITERATURE REVIEW

A. Hao Guo describes how proper protocols must constantly be put in place to care for autonomous vehicles, which are becoming more and more essential parts of our everyday lives, in order to demonstrate guilt from failures, defects, or possibly even purposeful assaults. This study offers a novel approach to develop a repeatable and tamper-proof event record management system for crash investigations involving self-driving cars, one of the most important autonomous technologies of the modern era. Blockchain serves as the method's inspiration. They

- conduct numerical studies based on a state-of-the-art Proof-of-Event approach with a prompt leadership voting process. They also develop a model for a blockchain-influenced car network using Hyperledger Fabric.
- B. Wei She claims that most of the time, centralized verdict is utilized in today's WSNs to identify rogue nodes. This method has a number of shortcomings, such as the inability to trace the information's sources, the difficulty of duplicating and verifying the identification process, and the challenge of preventing errors and faked data. This project uses WS parallelogram measurements and block chain intelligence contracts to localize the identification of damaging networks in three-dimensional space. The voting results of the agreement mechanism are also recorded. The modelling findings show that the algorithm can reliably provide process accountability and precisely identify problematic activities in WSNs.
  - C. Yuhao Bai introduced a ground-breaking collaborative blockchain platform for stakeholder engagement that enables people to actively participate in the decision-making process while also monitoring all administrative procedures in real-time, with the goal of maintaining facilities. In order to fulfil the goal of including a subset of verifiers in the safe authentication that is randomly and proactively selected from the larger population, a compounded blockchain architecture was created. We have also created a novel agreement technique for such participatory planning decentralized network, which is consistent with adding a periodically extra verifier subgroup to the blockchain.
  - D. Ledger has shown to be a useful tool in real-world scenarios because of its decentralized structure and resilience to data tampering, but Quang Nhat Tran points out that there are still some unresolved issues around participant anonymity and data accessibility. While developing the potential of blockchain technology, measures to maintain confidentiality should be taken into consideration at the expense of privacy. In this paper, researchers have discussed the current challenges with data privacy while utilizing blockchain in numerous businesses. Based on that, researchers examined several noteworthy developments in a number of blockchain's applications before categorizing the different types of anonymity in line with those findings, offering two levels of classification for private information blockchain technology.

### 3. PROPOSED METHODOLOGY

#### A. Problem Statement

To design and develop Secured system to enrich the security of the post voting data using Blockchain technology.

#### B. Motivation

Creating a safe electronic voting system with blockchain technology is a direct result of the urgent need to fix the flaws and vulnerabilities in the current voting systems. Through the utilization of blockchain technology's intrinsic qualities, including immutability, transparency, and decentralization, this initiative seeks to improve the voting process's credibility and integrity.

Implementing a blockchain-based electronic voting system offers a viable way to protect democracy from election fraud, tampering, and cyberattacks. It ensures accurate, transparent, and impenetrable elections while encouraging voter engagement.

#### C. System Overview Diagram

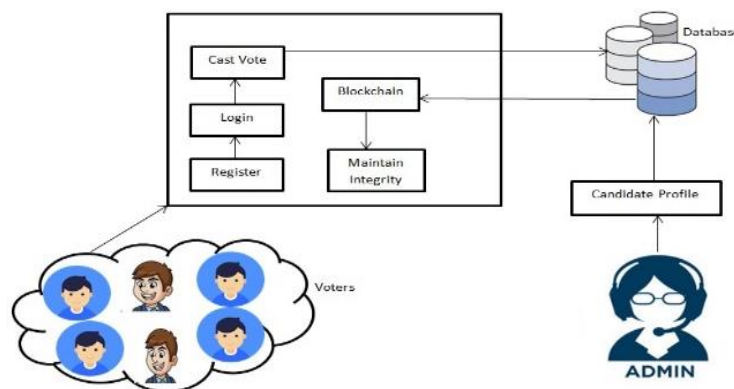


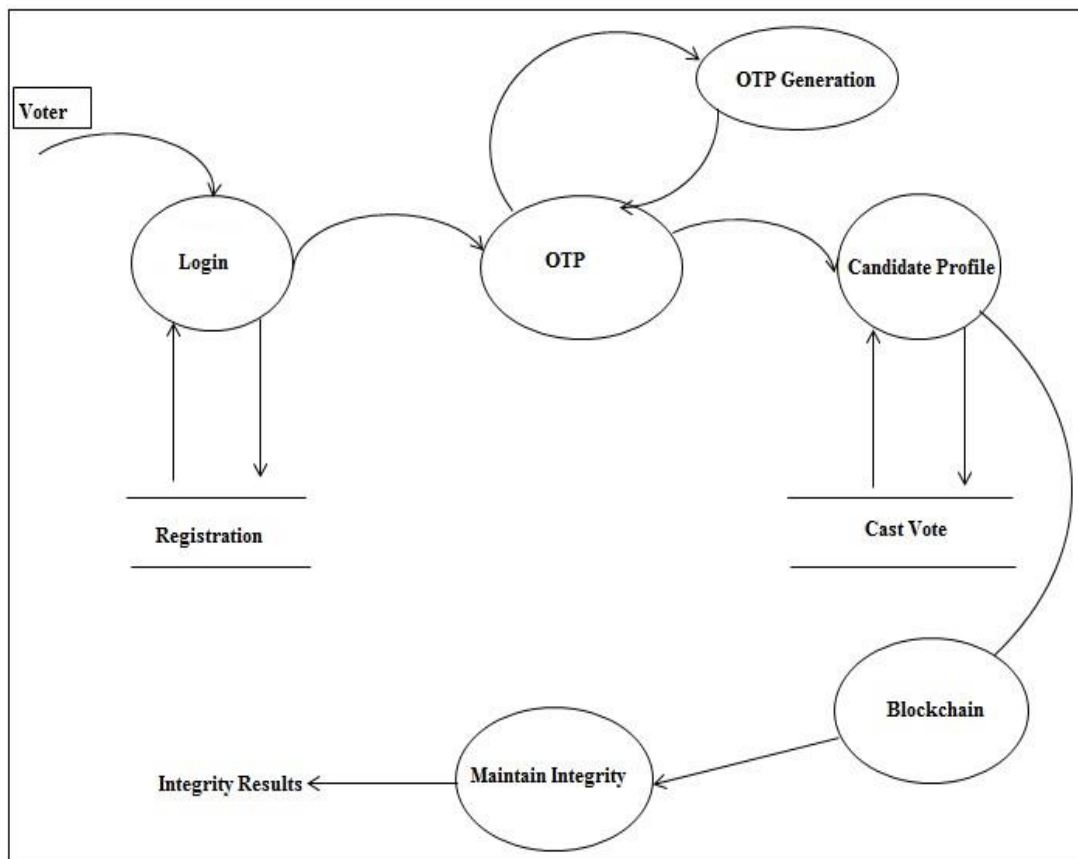
Fig. 1 System Overview Design

An overview of the system is given by the system overview diagram, which shows the key modules as blocks. Voters must first register, then log in with their details. If all of their credentials are accurate, they can then cast their ballot for the desired party. Following that, the vote will be saved in an encrypted database, and the administrator will count the results after receiving the final voter hash key.

D. Module Description

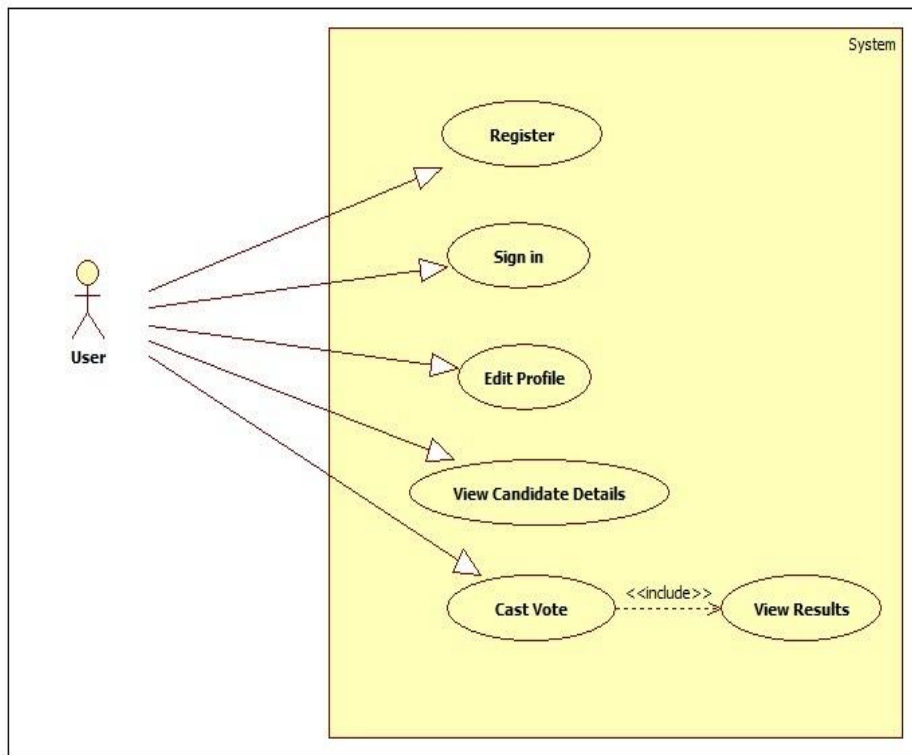
- 1) **Module A:** Reverse Circle Cipher
  - Block Formation
  - Character Rotation
  - Mod Function
  - Character Replacement
- 2) **Module B:** Block Formation
  - Encrypted String
  - Hash Key Generation
  - Random Character Selection
  - Body head and Body Formation
- 3) **Module C:** Linear Pairing
  - Number Of Blocks
  - Partition Of Blocks
  - Paring Decision
  - Hash Key Enhancement
- 4) **Module D:** Integrity Evaluation
  - Hash Key for Block Division
  - Previous Division Hash Key
  - Current Division Hash Key
  - Integrity Report for Securing E-voting

E. System Related Diagrams



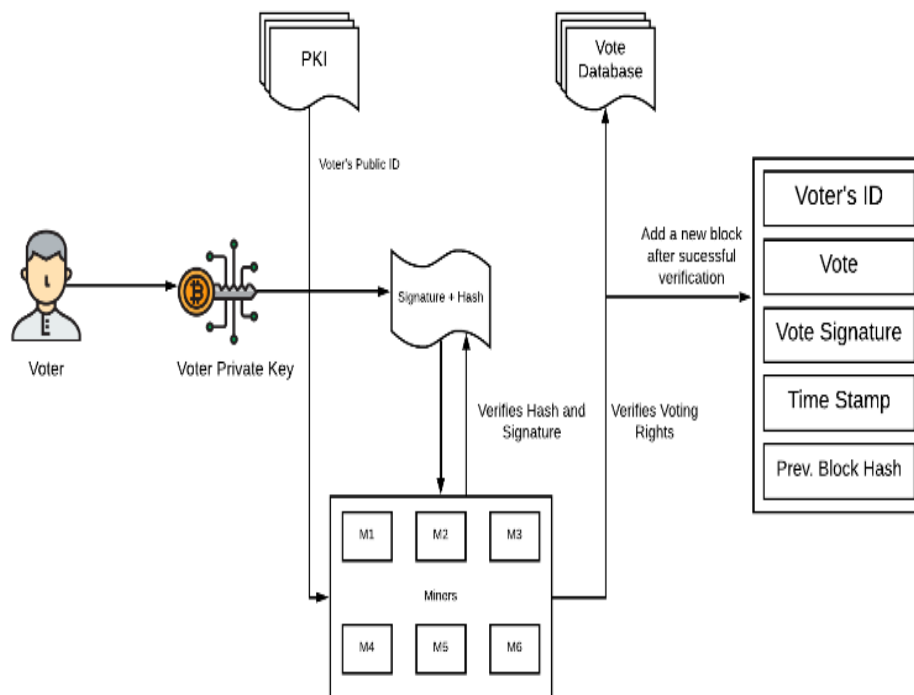
**Fig. 2** DFD Level 2

The most complete diagram is the DFD 2 one, which shows how voters join in to the system after registering, produce an OTP, submit it to a candidate's profile, and then cast their ballots. The blockchain is created, integrity is maintained, and integrity results.



**Fig. 3** Usecase Diagram

The several use cases that the user performs in the suggested model are shown in the use case diagram. User registration, sign-in, profile editing, viewing candidate details, and casting votes with result viewing are among the use cases.

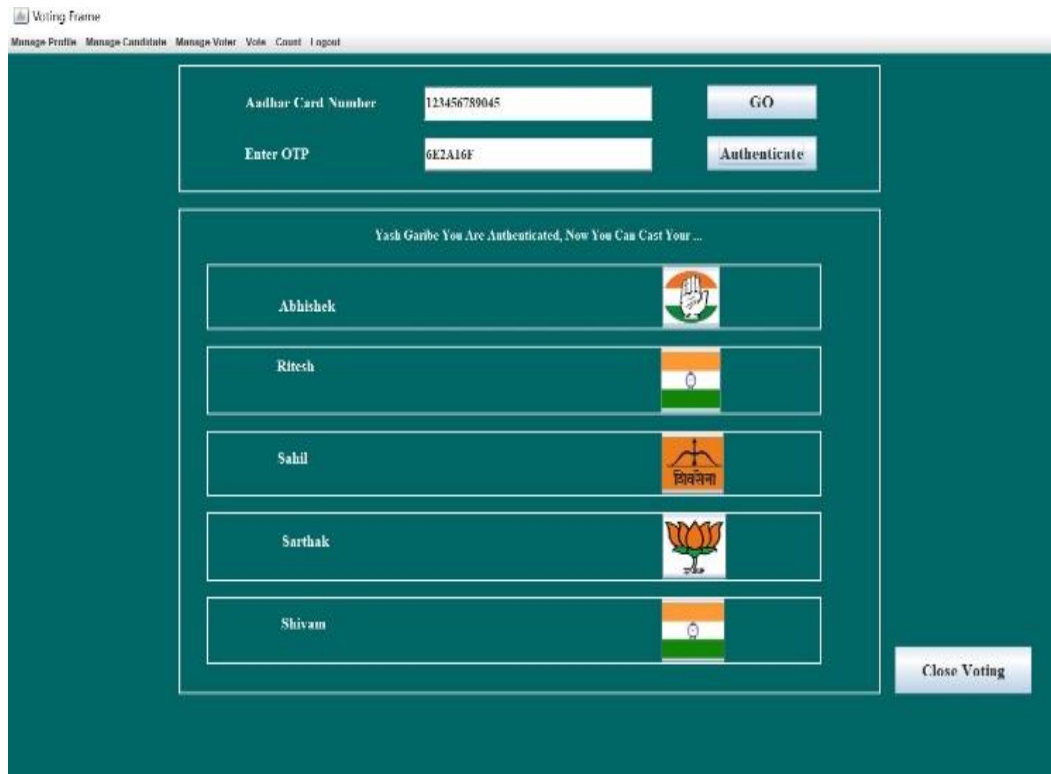


**Fig.4** Hash Key Generation Diagram

Each voter's hash key in a blockchain-based secure electronic voting system is created in this way: Voter registration first gathers personal identity data. Next, preprocessing is done on the gathered data to ensure consistency. The secure hashing algorithm of choice is SHA-256. A distinct hash key is generated by concatenating and hashing the data. This key is safely kept on the blockchain ledger together with the voter's data. The identical hashing procedure is repeated during verification, and identity validation is performed by comparing the resulting hash key with the stored one.

#### 4. RESULT

##### 1) Voting Page:



##### 2) View Vote Page:

Sr_no	Aadharcard_No	Voter_name	Constituency	Candidate_name	Party_name	Date_Time	Hash_key
3	123456789012	Adneya Khatate	Viman Nagar	Sarthak	BJP	16-02-2024, 10:47:33 AM	89c67b
5	123456789045	Yash Garibe	Viman Nagar	Sahil	ShivSena	28-02-2024, 7:27:13 PM	45a721
1	098765432221	Ram	Viman Nagar	Ritesh	NCP	16-02-2024, 10:37:12 AM	8ad19d
2	123454324523	Sarvesh	Viman Nagar	Ritesh	NCP	16-02-2024, 10:45:12 AM	d1d2d2
4	23456789:34	cCtpg(c'Mjrcvg	Viman Nagar	Abhishek	Congress	16-02-2024, 10:47:41 AM	af770c

#### 5. CONCLUSIONS

The voting or election process is one of the most important and crucial realizations that has been applied more regularly in democratic nations worldwide. These days, most of these countries still have elections in one way or another, and dictatorships and monarchies are comparatively uncommon. Elections are also held in the corporate sector, in municipalities throughout cities, and in other bodies.

This explains why the majority of practical and effective methods for expressing public opinion are based on voting. Voting ensures that the people have a say in the policies that affect them and that their opinion is heard. But unlike anything that has happened to science or technology over the ages, voting has remained the same since the beginning of time.

The most common issue with voting system upgrades is the lack of protection for post-vote data. As a result, this study uses blockchain, a distributed ledger technology, to provide an effective and workable solution for the post-vote data security. Blockchain technology has been used in a standalone voting application to guarantee the integrity of the data. Experiments have also been conducted to evaluate this system's effectiveness, and the results are covered in greater detail in the sections that follow.



## 6. REFERENCES

- [1] R. P. Pinto, B. M. C. Silva and P. R. M. In'acio, "A System for the Promotion of Traceability and Ownership of Health Data Using Blockchain," in IEEE Access, vol. 10, pp. 92760-92773, 2022, doi:10.1109/ACCESS.2022.3203193.
- [2] I. Malakhov, A. Marin, S. Rossi and D. Smuseva, "On the Use of Proof-ofWork in Permissioned Blockchains: Security and Fairness," in IEEE Access, vol. 10, pp. 1305-1316, 2022, doi:10.1109/ACCESS.2021.3138528.
- [3] C. Santiago, S. Ren, C. Lee and M. Ryu, "Concordia: A Streamlined Consensus Protocol for Blockchain Networks," in IEEE Access, vol. 9, pp. 13173- 13185, 2021, doi:10.1109/ACCESS.2021.3051796.
- [4] H. Guo, W. Li, M. Nejad and C. -C. Shen, "Proof-of-Event Recording System for Autonomous Vehicles: A Blockchain-Based Solution," in IEEE Access, vol. 8, pp. 182776-182786, 2020, doi:10.1109/ACCESS.2020.3029512.
- [5] W. She, Q. Liu, Z. Tian, J. -S. Chen, B. Wang and W. Liu, "Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks," in IEEE Access, vol. 7, pp. 38947-38956, 2019, doi:10.1109/ACCESS.2019.2902811.
- [6] Y. Bai, Q. Hu, S. -H. Seo, K. Kang and J. J. Lee, "Public Participation Consortium Blockchain for Smart City Governance," in IEEE Internet of Things Journal, vol. 9, no. 3, pp. 2094-2108, 1 Feb.1,2022,doi:10.1109/JIOT.2021.3091151.
- [7] Q. N. Tran, B. P. Turnbull, H. -T. Wu, A. J. S. de Silva, K. Kormusheva and J. Hu, "A Survey on Privacy-Preserving Blockchain Systems (PPBS) and a Novel PPBS-Based Framework for Smart Agriculture," in IEEE Open Journal of the Computer Society, vol. 2, pp. 72-84, 2021, doi:10.1109/OJCS.2021.3053032.
- [8] K. Agrawal, M. Aggarwal, S. Tanwar, G. Sharma, P. N. Bokoro and R. Sharma, "An Extensive Blockchain Based Applications Survey: Tools, Frameworks, Opportunities, Challenges and Solutions," in IEEE Access, vol. 10, pp. 116858-116906, 2022, doi: 10.1109/ACCESS.2022.3219160.
- [9] S. Gao, D. Zheng, R. Guo, C. Jing and C. Hu, "An Anti-Quantum E-Voting Protocol in Blockchain With Audit Function," in IEEE Access, vol. 7, pp. 115304-115316, 2019, doi:10.1109/ACCESS.2019.2935895.
- [10] A. Benabdallah, A. Audras, L. Coudert, N. El Madhoun and M. Badra, "Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review," in IEEE Access, vol. 10, pp. 70746-70759,2022, doi:10.1109/ACCESS.2022.3187688.
- [11] G. Rathee, R. Iqbal, O. Waqar and A. K. Bashir, "On the Design and Implementation of a Blockchain Enabled E-Voting Application Within IoT Oriented Smart Cities," in IEEE Access, vol. 9,pp. 34165-34176, 2021, doi: 10.1109/ACCESS.2021.3061411.
- [12] B. Shahzad and J. Crowcroft, "Trustworthy Electronic Voting Using Adjusted BlockchainTechnology," in IEEE Access, vol. 7, pp.24477-24488,2019,doi:10.1109/ACCESS.2019.2895670.
- [13] M. S. Farooq, U. Iftikhar and A. Khelifi, "A Framework to Make Voting System Transparent Using Blockchain Technology," in IEEE Access, vol. 10, pp 59959-59969, 2022, doi:10.1109/ACCESS.2022.3180168