

# Secure E-voting System using Block-Chain

Prof. P. A. Dhakate<sup>1</sup>, Sakshee Haral<sup>2</sup>, Shubham Tambade<sup>3</sup>, Anish Teli<sup>4</sup>, Kartik Watile<sup>5</sup>

Faculty, Department of Information Technology<sup>1</sup>

Students, Department of Information Technology<sup>2,3,4,5</sup>

Sinhgad Institute of Technology, Lonavala, Maharashtra, India

pankajdhakate11@gmail.com<sup>1</sup>, haralsakshee@gmail.com<sup>2</sup>, shunhamstambad@gmail.com<sup>3</sup>,

anishteli238@gmail.com<sup>4</sup>, kwatile8@gmail.com<sup>5</sup>

**Abstract:** Block-chain is a peer-to-peer version which allows e-commerce payments, the building of smart cities, data sharing, copyright and royalty protection, etc. It is a decentralized system where there is no central node or server. We have built an e-voting system to overcome the problems such as low voter turnout in several states/ areas. To address this problem, we have designed a voting system where every person could vote by simply logging online either through their mobile phones or their nearest available computer. Block-chain technology when being used with the e-voting system makes the voting process more secure and reliable. The traditional voting system leads to many frauds and forgery. The E-voting system overcomes all the problems that we face in the traditional system. In information security study the online voting system is viewed as an interesting subject. The electronic voting system provides the people to elect their preferred candidate and express their opinions on how they are to be governed. The security community has declared the electronic machines as a flawed system based primarily on physical safety concerns.

**Keywords:** Block-chain

## I. INTRODUCTION

Block-chain is a peer-to-peer version which allows e-commerce payments, the building of smart cities, data sharing, copyright and royalty protection, etc. It is a decentralized system where there is no central node or server. We have built an e-voting system to overcome the problems such as low voter turnout in several states/ areas. To address this problem, we have designed a voting system where every person could vote by simply logging online either through their mobile phones or their nearest available computer. Block-chain technology when being used with the e-voting system makes the voting process more secure and reliable. The traditional voting system leads to many frauds and forgery. The E-voting system overcomes all the problems that we face in the traditional system. In information security study the online voting system is viewed as an interesting subject. The electronic voting system provides the people to elect their preferred candidate and express their opinions on how they are to be governed. The security community has declared the electronic machines as a flawed system based primarily on physical safety concerns

### 1.1 Proposed work

Our proposed system includes the following modules. Various authentication and security methods which can be applied are:

Elliptical Curve Cryptography: This consists of two steps:

#### Initialization:

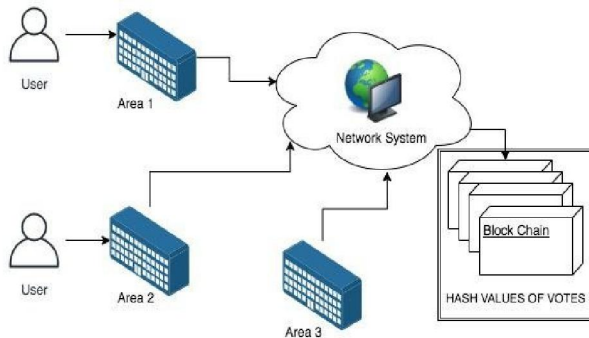
- Each voter generates private key
- Each voter generates public key from the private key (Identity element O, elliptical curve base point G, integer n such that  $nXG = O$ , then create private key Da)- public key  $Qa = DaXG$
- The private key is not shared by voters
- Public keys are sent securely by voters to the centralized database called the Public Key Infrastructure (PKI)
- Miners are randomly elected
- First block (genesis block) is generated

**Voting**

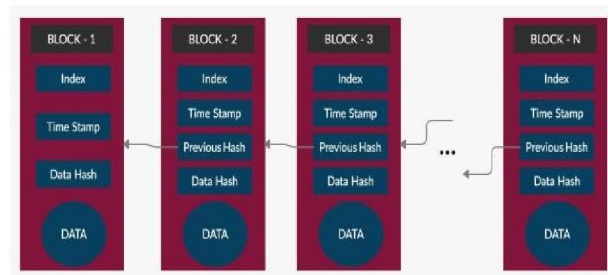
- SHA 256 to generate the hash value of the vote.  $H = \text{Hash}(\text{ID} + \text{vote} + \text{timestamp})$
- Voter's private key to generate signature  $S$  of hash value  $H$
- Voter sends ID, vote, timestamp,  $S$  to the miner
- The miner obtains voter's public key from a centralized database called the Public Key Infrastructure (PKI) using voter's unique voter ID
- Miner uses SHA 256 to generate hash value using  $H = \text{Hash}(\text{ID} + \text{vote} + \text{timestamp})$
- Miner uses the public key to verify  $S$  and get  $H'$
- If  $H$  and  $H'$  are the same, signature  $S$  is accepted
- Miner queries and verifies that voter has right to vote
- Miner generates a new block by including the previous block's hash value and information of the current vote.

**II. BLOCK STRUCTURE**

Block Structure for our system is described in the Fig A block structure used in our proposed system contains components such as given below:



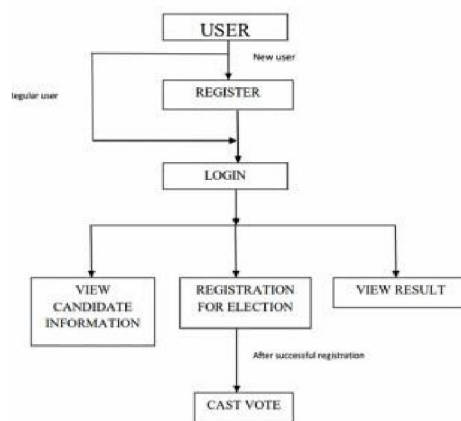
**Figure 1: Our Proposed System**



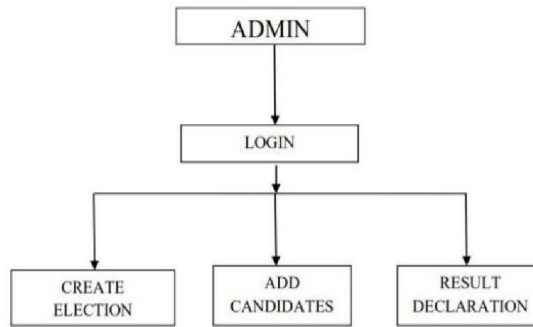
**Figure 2: Block-Chain Structure**

**III. UML DIAGRAMS**

**FLOW DIAGRAM**

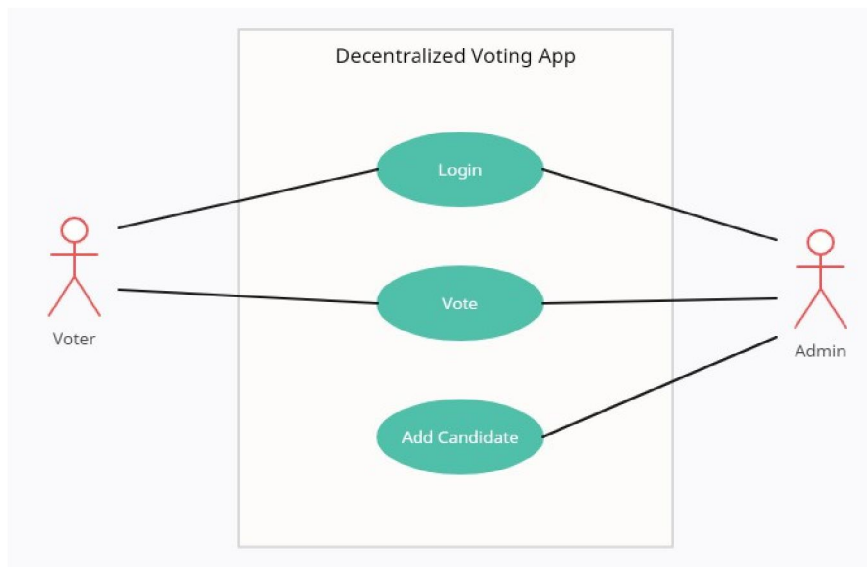


**Figure 3: User side flow diagram**



**Figure 4:** Admin side flow Diagram

**USE CASE DIAGRAM**



**Figure 5** Use Case Diagram

**IV. HARDWARE AND SOFTWARE REQUIREMENTS**

**Hardware Requirements**

- Processor – 2 GHz or more
- RAM – 4 GB or more
- Disk Space – Based on device

**Software Requirements**

- Node.js (version – 18.14.0)
- Web3.js (version – 1.8.2)
- Truffle (version – 5.7.6)
- Solidity (version – 0.5.16)
- Ganache (version – 7.7.3)
- Metamask
- Python (version – 3.9)
- FastAPI
- MySQL Database (port – 3306)

#### V. APPLICATIONS

- To register and complain a report against any crime taken place.

#### VI. FUTURE SCOPE

In future iterations, the decentralized voting system can be enhanced by implementing additional features such as real-time vote counting, secure voter identification mechanisms, advanced data analytics for voter insights, and integration with emerging technologies like artificial intelligence and biometrics.

These enhancements will further enhance the efficiency, security, and accessibility of the voting process, making it more inclusive and trustworthy.

#### VII. CONCLUSION

Decentralized Voting with Ethereum Blockchain offers a robust and transparent solution for secure elections. By leveraging blockchain technology, it ensures the integrity of votes and provides a tamper-proof platform. With continued enhancements, including improved user experience, scalability, and integration with other cutting-edge technologies, it has the potential to revolutionize the democratic process and empower citizens to participate in a trusted and efficient voting system. It represents a significant step towards building a more democratic and accountable society.

#### REFERENCES

- [1]. Liu Y., Wang Q. An E-voting Protocol Based on Blockchain. IACR Cryptol. Eprint Arch. 2017;2017:1043. [Google Scholar]
- [2]. Yaga D., Mell P., Roby N., Scarfone K. Blockchain technology overview. arXiv. 20191906.11078 [Google Scholar]
- [3]. The Economist EIU Democracy Index. [(accessed on 18 January 2020)];2017 Available online: <https://infographics.economist.com/2018/DemocracyIndex/>
- [4]. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. [(accessed on 28 July 2020)]; Available online: <https://bitcoin.org/bitcoin.pdf>.
- [5]. Garg K., Saraswat P., Bisht S., Aggarwal S.K., Kothuri S.K., Gupta S. A Comparative Analysis on E-Voting System Using Blockchain; Proceedings of the 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU); Ghaziabad, India. 18–19 April 2019. [Google Scholar]

#### BIOGRAPHY

- Sakshee S. Haral - An Undergraduate Scholar pursuing Bachelors of Engineering in Information Technology from Sinhgad Institute of Technology. She is working under the guidance of Prof. P.A. Dhakate
- Shubham S. Tambade - An Undergraduate Scholar pursuing Bachelors of Engineering in Information Technology from Sinhgad Institute of Technology. He is working under the guidance of Prof. P.A. Dhakate
- Anish D. Teli - An Undergraduate Scholar pursuing Bachelors of Engineering in Information Technology from Sinhgad Institute of Technology. He is working under the guidance of Prof. P.A. Dhakate
- Kartik S. Watile - An Undergraduate Scholar pursuing Bachelors of Engineering in Information Technology from Sinhgad Institute of Technology. He is working under the guidance of Prof. P.A. Dhakate