Decentralised Voting System Using Blockchain

[1] K Dhanush Bhat, [2] Nandana S Bhat,[3] Prashanth R, [4] T Sagar, [5] Dr. Vrinda Shetty

[1]8th Sem Student,[2]8th Sem Student, [3]8th Sem Student, [4]8th Sem Student, [5]Professor & HOD
Department of Information Science and Engineering,
Sai Vidya Institute of Technology, Bengaluru, India

Abstract - The aim of this paper is to provide a voting system which is secure, transparent and convenient and utilizes the features of Blockchain and smart contracts. The proposed system would attempt to build trust between the voter and the government by maintaining the integrity and security of the votes cast. The system also aims to be more convenient by minimizing the time needed for voters to travel to polling stations and wait in queues as in the traditional voting system. This is achieved by employing a web application for the voting system that voters can use from anywhere across the world. The paper also mentions the challenges that such a Blockchain-based voting system would have to face.

Index Terms - Node, Transaction, Block, Chain, Miners.

I. INTRODUCTION

As the pillar of democracy, elections play a vital role in shaping the course of a nation's future. It is essentially a process that determines the future. The voting system that is used for such an important process should reflect and uphold the appropriate values. But, the current systems are intransparent and are very inconvenient for the voters as in many cases they have to travel long distances and wait in long queues to cast their vote which many of the new voters find tedious. They also require a significant amount of financial resources and manpower. Therefore, systems that are safe, transparent and secure are required. The systems should also aim to achieve these goals in an efficient manner.

There have been a number of systems that have been implemented as an alternative to the physical ballot paper voting systems. Countries such as India, Brazil and Belgium have adopted Electronic Voting Machines to varying extents. But the high cost of procuring, maintaining and transporting these EVMs along with the inherent security risks have limited their use in other countries. Mobile voting and postal voting have also been piloted in many countries such as the United States and the United Kingdom. But the lack of secrecy and logistical challenges in Postal voting and the accessibility challenges and concerns about transparency and integrity has led to significant concerns and opposition from both the public and the experts.

Blockchain technology is seen as a possible solution for such a system. Blockchain is a distributed ledger technology that stores information across different nodes of a network in a decentralized and transparent manner using blocks linked together with cryptographic techniques. Smart contracts are digital agreements that automatically execute according to predetermined conditions established during creation. They eliminate the need for a third party. The potential of using blockchain and smart contracts to create a decentralised voting system is immense. By leveraging the power of distributed ledger technology and automatically executing smart contracts, it is possible to create a secure and transparent voting system that can be used to ensure accurate and tamper-proof results. Blockchains' inherent nature of being decentralized and non-modifiable provides a solid base to develop a Voting system. Such a system would not only reduce the risk of voter fraud but also increases trust and confidence in the system and the government. Additionally, the proposed system, being a web application, can be accessed from any location which is very convenient for the voters.

II. LITERATURE SURVEY

Nir Kshetri and Jeffrey Voas[1] in their paper introduced various Internet voting systems already deployed at community, city and national levels in countries such as Russia, South Korea, Estonia and Sierra Leone. They compared these solutions and presented their features and shortcomings. They also provided a list of opportunities and challenges in developing a blockchain-based e-voting system on a large scale.

Sunny Pahlajani, Avinash Kshirsagar et al.[2] in their paper presented the theory and data for choosing a suitable consensus algorithm. The paper elucidated the various consensus algorithms and their properties such as the proof-based consensus algorithms, byzantine consensus algorithm, raft consensus algorithm and crash consensus algorithm. In this way, the paper also aimed to help future research works in practically implementing and researching these consensus algorithms.

Seoyoung Kim and Atulya Sarin[3] in their paper introduced blockchain and related concepts such as consensus algorithms, ledger design, block size and the working of a blockchain application. They also discussed its current potential and use cases like currency exchange, healthcare, etc. It also provided a business-oriented framework for implementing blockchain applications.

Muhammad Shoaib Farooq, Usman Iftikhar et. al.[4] in their paper proposed a layered structure for the voting framework. The proposed system utilised the national ID of the voters for registration and used OTPs communicated through SMS for verification. A unique concept of a voting coin as a digital currency to cast a vote is used which is exhausted after the voter has cast his vote. Along with the voting coin, a chain security algorithm and a flexible consensus algorithm were employed in the blockchain architecture. The system ensured vote authenticity by creating a hash with respect to the voter's national ID. The paper also mentioned how the system attempts to defend against a few of the popular cyber attacks.

Syada Tasmia Alvi, Mohammed Nasir Uddin et. al.[5] in their paper, proposed a mobile application based on blockchain where the voters register themselves with the central authority which generates a private key unique for the voter which is sent through SMS. They also proposed a biohash based solution where the hash is generated on the voters' biometric information. A Merkle tree structure is used for the Blockchain. The main properties they aimed to include were anonymity, integrity privacy, security and verifiability.

Basit Shahzad and Jon Crowcroft[6] in their paper presented Block sealing as a concept of sealing each block of a blockchain to make it more secure. They also proposed a similar solution with block sealing and a proof of completeness consensus algorithm in their solution. A Merkle tree representation of the blockchain is adopted for the proposed system. The paper also mentioned the limitations of the proposed system which need to be solved.

Cosmas Krisna Adiputra, Rikard Hjort et. al.[7] this paper proposed a solution that uses the voter's public key for hashing. The voters have to register with the central authority to receive their public key. The proposed system also uses a double envelope, the vote being encrypted with the election's public key and then signed by the voter's private key for enhanced security. They then compared it to Estonia's digital voting system and stated their solution's advantages along with the system's performance analysis.

Jian Yang and Hong Shen[8] in this paper presented the use cases of the various consensus algorithms along with their advantages and disadvantages. The paper proposed a new consensus algorithm for permissioned networks which is based on consistent hashing. It also proposed a new design of the hash ring for blockchain systems. The algorithmic steps of the proposed algorithm are listed and its use cases are discussed. Lastly, the security features and performance of the algorithm are discussed.

III. ARCHITECTURE

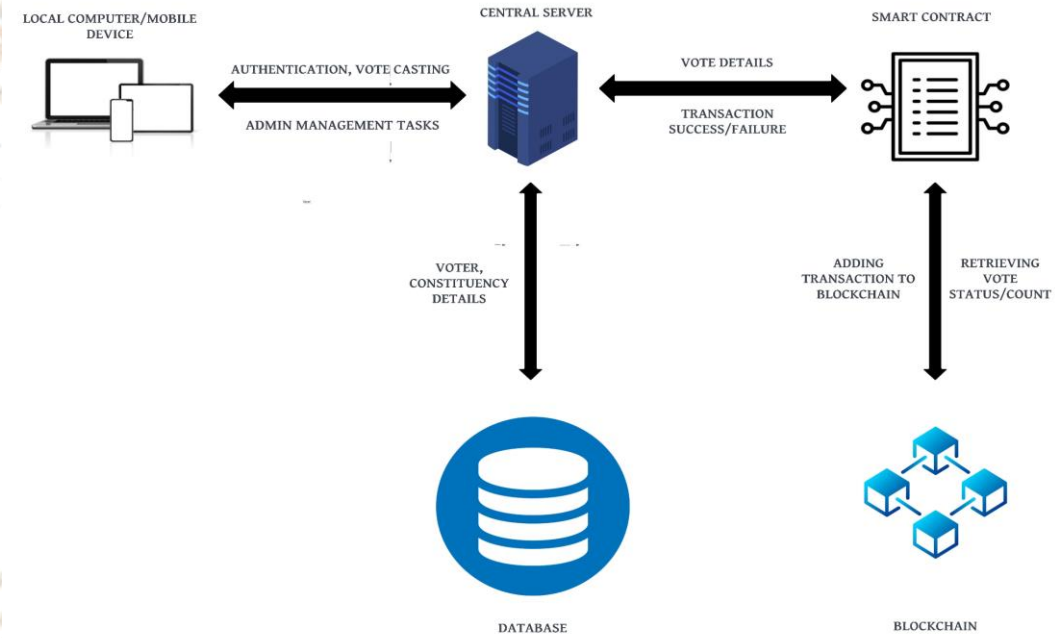

Fig 1. System Architecture

The architecture includes the following components:

1) Local computer/mobile phone: As the system is a web application, it can be used by voters on their local devices without the need to attend physical voting stations.

2) Central Server: The system contains a central server that the web application will communicate for authentication, registration and login purposes. It also communicates with smart contracts to add the vote to the blockchain

3) Central Database: The voters' ID numbers and biometric information available through the national ID are stored in the central database. The central server communicates with the central database for voter-related information.

4) Smart Contracts: Once the voter has cast his vote at the web application, the same will be sent to the server. The server will verify the details initially and forward the same to smart contracts. If all the information in the transaction is legit, the smart contracts execute and add the transaction to the blockchain.

5) Blockchain: The blockchain is the final storage area of the votes in the form of transactions. These transactions will be cryptographically hashed to maintain security.

IV. PROPOSED SYSTEM

The proposed system is a web application that aims to make use of Blockchain with Smart contracts to overcome the drawbacks of the existing voting system.

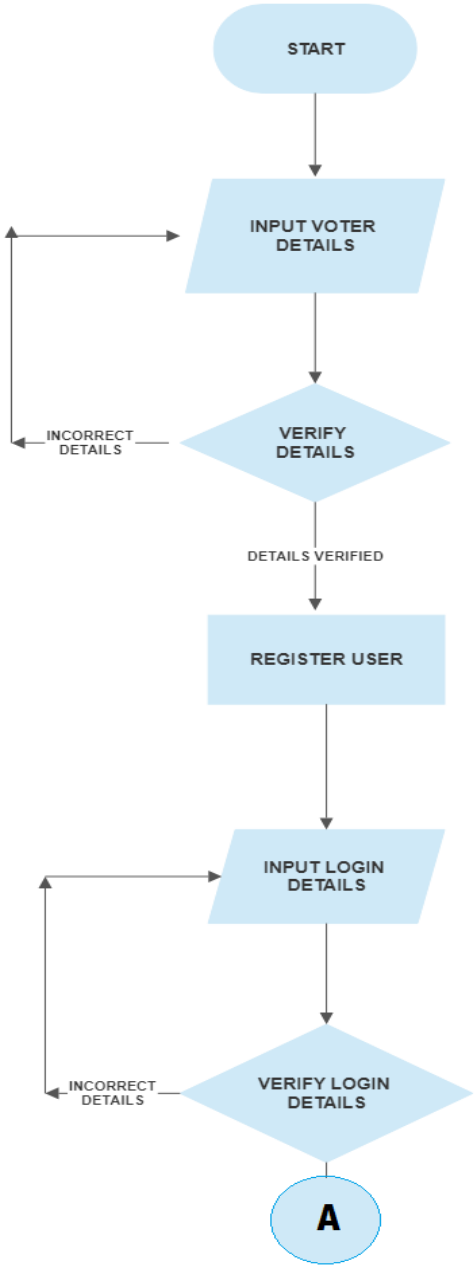

Fig 2. Voter Verification & Login Process

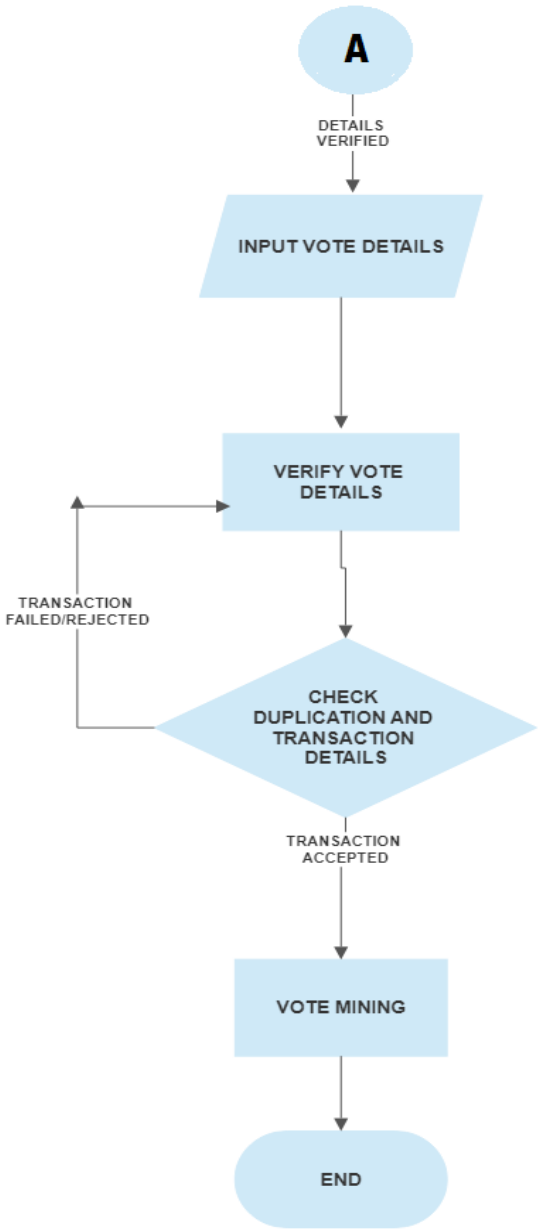

Fig 3. Post Verification & Voting Process

The user will first register themselves with the application using their Voter ID, biometric information and various other details such as their phone number, email, age, gender, etc. The voter will then be able to set a password for his account. The user can then be able to login to his system with his Voter ID and registered password at any time either to check his constituency details, to cast his vote or to verify his vote post-voting. As the voting window opens, the registered voters would be able to cast their vote which will first be verified on the server. If the vote is valid, the vote is then checked if it's a duplicate or not by the smart contracts, if not it is then added to the blockchain. Finally, the results of the election are declared to the head admin according to the constituencies which he then can announce to the public.

The admins would be able to manage the whole process of voting. The admins are divided into various hierarchy levels to distribute the responsibilities among themselves. The admins will be able to perform functions such as setting election details, managing constituency details, managing candidate details, etc. The level of access that an admin will have will depend on the level of the admin in the hierarchy.

V. IMPLEMENTATION

This section will explain how the Voting system is implemented and deployed on the blockchain. It is built with the Indian voting process in mind.

1) User-Interface:
The front-end user interface of the web application is implemented with the ReactJS library. ReactJS is a library that can be used to develop front-end applications. It is built on the javascript programming language. The application also uses the Bootstrap CSS framework to add styling to the web application and Redux data store to manage the data in the front-end part of the application.

2) Backend/Server:
The server for the web application is implemented in NodeJS along with the ExpressJS framework. The choice for using ExpressJS was to simplify the process of writing API scripts. MongoDB is used for storage at the backend. The various collections are used to store information related to the voters, constituencies, candidates, etc.

3) Smart Contracts and Blockchain:
The smart contracts for the application were written in the Solidity language which is the most popular smart contract language in use. The contract was first written and tested on the Remix IDE. The contract was then deployed in a local Ethereum blockchain using ganache. Ganache is a blockchain environment that helps developers emulate the Ethereum blockchain privately so as to test and interact with the smart contracts in their own private blockchain. Web3JS was used for communicating with smart contracts.

4) Voter Functionalities:
The voter will mainly be able to perform four functions:
   a) Register: The voter can register themselves with the voting system using their unique Voter ID and biometric information.
   b) Login: The voter can be able to login into the system using their Voter ID and the password set during the registration phase.
   c) Cast Vote: The voter will be able to cast their vote for the candidate of their choice once the voting window has opened.
   d) Verify Vote: The voter will also be able to verify their vote by logging back into the system.

5) Admin Functionalities:
The Admins are divided into 4 levels. New admins need to register themselves with the application. These new admins are then assigned roles and administrative areas as required. The 4 main levels are:
   a) Constituency Admins: The constituency admins can manage their individual constituencies. They can view the status of voting and manage the candidates that are contesting from their respective constituencies.
   b) District Admins: The district admins can manage their respective districts. They can assign constituencies to admins and manage the constituencies in their districts.
   c) State Admins: The state admins can oversee the voting in the constituencies present in their states. They can also manage the lower-level admins(district and constituency admins)
   d) Head Admin: The head admin can oversee the whole voting process. They can assign state admins or dismiss admins of any level if required. They can pause the election process and resume if necessary.

VI. RESULT

The implemented system provides various advantages both to the voter and to the election authority. Some of these advantages are: Transparency: The system provides better transparency than the traditional voting system as the voter will be able to verify their vote whenever required. This builds a sense of trust between the voter and the authorities.

1) Convenience: As the system is a web application, it can be accessed by any registered voter from any location required. This saves a lot of time and effort for the voter.

2) Security: The system has improved security capabilities with the adoption of blockchain into its architecture. The inherent property of blockchain to be immutable facilitates this.

3) Control: The system provides the authority with increased control to maintain the whole election process and also makes it more convenient for the authorities to do the same.

4) Resource Efficiency: The voting system being a web application is very resource efficient. The system saves a lot of money that otherwise would be required for the procurement and maintenance of the EVMs and setting up of voting booths.

VII. CONCLUSIONS

The purpose of proposing a blockchain-based solution for the voting system was to foster faith between the election authorities and the voters to assure them that their vote's integrity is preserved and maintained. Transparency and Trust in the voting system are enhanced and a lot of financial and other resources are saved when compared to the traditional voting system. The convenience of the users is also enhanced as it eliminates the need to travel and wait in queues. The overall speed of the process is increased as the counting of votes can be done almost instantly.

VIII. REFERENCES

[1] Nir Kshetri and Jeffrey Voas, "Blockchain-Enabled E-Voting", July/August 2018, DOI:10.1109/MS.2018.2801546.

[2] Sunny Pahlajani, Avinash Kshirsagar, Vinod Pachghare, "Survey on Private Blockchain Consensus Algorithms".

[3] Seoyoung Kim, Atulya Sarin, "Distributed Ledger and Blockchain Technology: Framework and Use Cases ", JEL Classification: G0; G2; N2, O0, April 2018.

[4] Muhammad Shoaib Farooq, Usman Iftikhar, Adel Khelifi, "A Framework to Make Voting System Transparent Using Blockchain Technology", DOI: 10.1109/ACCESS.2022.3180168, Vol.10, June 2022.

[5] Syada Tasmia Alvi, Mohammed Nasir Uddin, "Digital Voting: A Blockchain-based E-Voting System using Biohash and Smart Contract", Proceedings of the Third International Conference on Smart Systems and Inventive Technology (ICSSIT 2020).

[6] Basit Shahzad, Jon Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology", DOI: 10.1109/ACCESS.2019.2895670, Vol.7, February 2019.

[7] Cosmas Krisna Adiputra, Rikard Hjort, and Hiroyuki Sato, "A Proposal of Blockchain-based Electronic Voting System", The University of Tokyo, Tokyo, Japan, schukog@satolab.itc.u-tokyo.ac.jp.

[8] Jian Yang, Hong Shen, " Blockchain Consensus Algorithm Design Based on Consistent Hash Algorithm", DOI 10.1109/PDCAT.2019.00090, 2019 20th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT).