iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** XI **Month of publication:** November 2021

DOI: https://doi.org/10.22214/ijraset.2021.38948

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XI Nov 2021- Available at www.ijraset.com

Exploratory Review: Decentralized Voting System Using Blockchain

Hitesh Potdukhe[1], Durgesh Sakhardande[2], Avi Savla[3], Shivani Tiwari[4], Vivek Ramakrishnan[5]
[1, 2, 3, 4] *B.E. Student, Dept. of Electronics and Telecommunication, Atharva College of Engineering, Mumbai, India*
[5]*Professor, Dept. of Electronics and Telecommunication, Atharva College of Engineering, Mumbai, India*

Abstract: ***Electronic voting, often known as e-voting, has been utilized in various forms since the 1970s, with basic advantages over paper-based systems such as improved efficiency and lower error rates. However, achieving widespread acceptance of such systems remains a problem, particularly in terms of strengthening their resistance to possible failures. Blockchain is a modern-day disruptive technology that promises to enhance the overall robustness of electronic voting systems. This article describes an effort to use blockchain's features, such as cryptographic underpinnings and transparency, to create an effective e-voting mechanism. The suggested method meets the basic requirements for electronic voting systems and provides end-to-end verifiability. The proposed e-voting method is described in depth, as well as its implementation on the Multichain platform. The article provides an in-depth analysis of the scheme, demonstrating its efficacy in achieving an end-to-end verifiable e-voting system. Electronic trust services are becoming an integral part of the information space. With the reliable implementation of basic services as an electronic signature and electronic authentication, it is possible to build more complex systems that rely on them, particularly the electronic voting system. In the paper, the new concept for developing a decentralized electronic voting system using blockchain technology is proposed. The two-level architecture provides a secure voting process without redundancy of existing (not based on blockchain) systems. The presented blockchain-based voting protocol ensures all requirements that are put forward to such types of protocols including voting transparency and anonymity. This project is aimed to design a decentralized e-voting system. The core idea is to combine the blockchain technology with secret sharing scheme and homomorphic encryption to realize the decentralized e-voting application without a trusted third party. It provides a public and transparent voting process while protecting the anonymity of voter's identity, the privacy of data transmission and verifiability of ballots during the billing phase.***

Keywords: Blockchain, Multichain, authentication, decentralized, anonymity.

I. INTRODUCTION

Elections are a crucial component of a democratic society because they allow the general people to express their opinions through voting. Because of their importance to our society, elections should be open and dependable in order to assure participants of their legitimacy. The method to voting has been an ever-evolving domain in this setting. The attempts to make the system safe, verifiable, and transparent are driving this progress. Because of its importance, ongoing attempts have been undertaken to enhance the voting system's overall efficiency and robustness. Electronic voting, often known as e-voting, plays a significant part in this. Since 1960, when it was initially used as punched-card ballots. With the use of internet technology, e-voting systems have made significant development. However, in order for e-voting systems to be widely used, they must comply to specified benchmark requirements.

These characteristics include, among others, the voter's anonymity, the vote's integrity, and non-repudiation. Blockchain is an emerging technology with strong cryptographic underpinnings, allowing applications to take advantage of these capabilities to build secure security solutions. A Blockchain is a data structure that records and distributes all of the transactions that have occurred since its inception. It's essentially a distributed, decentralized database that keeps track of an ever-growing list of data records that are protected from unwanted manipulation, tampering, and alteration. Although Bitcoin is the most well-known blockchain application, academics are eager to investigate how blockchain technology may be used to support applications in a variety of fields, utilizing features such as non-repudiation, integrity, and anonymity. In this article, we look at how blockchain may help with e-voting applications by ensuring voter anonymity, vote integrity, and end-to-end verification. We think that core blockchain properties like self-cryptographic validation structure among transactions (through hashes) and public availability of distributed ledger of records may be used for e-voting. The blockchain technology has the potential to be very useful in this field.

Due to the intrinsic nature of maintaining anonymity and maintaining a decentralized and publicly distributed record of transactions across all nodes, electronic voting is becoming more popular. As a result, blockchain technology is particularly effective at dealing with the risk of using a voting token multiple times and attempts to sway the outcome's transparency.

Our investigation will focus on critical concerns such as voter anonymity, vote secrecy, and end-to-end verification. These difficulties are the bedrock of an effective voting system that maintains the integrity of the electoral process. We share our attempts to investigate the usage of blockchain technology to find answers to these problems in this article. Our solution is built on the Prêt à Voter method and employs an open source blockchain platform, Multichain, as the underlying technology. To protect the anonymity and integrity of a vote, the system generates strong cryptographic hash for each vote transaction based on information specific to a voter. This hash is also communicated to the voter using encrypted channels to facilitate verification.

II. BASICS OF DIFFERENT VOTING SYSTEMS

Around the world different types of voting systems are used for different applications including elections, plebiscite, board decisions, etc. Some of the methods used for voting are:

1) *EVM Based System:* Electronic Voting System is the one in which we use a machine to handle the process of voting in India. EVM consists of two units namely control unit and ballot unit which are connected by a cable. The polling officer is in charge of the control unit. The ballot unit is for the voters to cast their votes. These units are sealed and directly opened on the vote counting day. Major criticism faced by EVMs is that these systems use microprocessors internally which can be subjected to tampering.
2) *Paper Ballot based System:* Here, voters are provided a paper ballot (usually a piece of paper) which consists of names of all candidates. These paper ballots are provided at the polling station. The major disadvantages of such a system are the high duration required to calculate votes, manpower, wastage of paper, ease in manipulation, etc.
3) *Head Count Method:* This approach is more popularly used in the Upper and Lower House of Indian Parliament when you need to get the count of members in support of a proposition and vice versa. Here we have a leader who instantiates the voting and declares the result. It is a trust and authority model. Here the speaker is trusted by the members and given authority by the constitution to conduct voting declare results.
4) *Database Approach:* Here, we have a centralized database managed by an authority which has the right to manipulate the database. The database consists of rows and columns. Each time a voter votes, the corresponding candidate's count gets incremented by one. Backtracking of votes is possible in this approach.

III. LITERATURE REVIEW

The Blockchain Technology- Blockchain is so-called, as it consists of a chain of blocks, that is, interconnected nodes that have their copy of the distributed ledger that contains the history of all transactions. Data is processed and put in a block through a process called mining. Every block contains a hash of the previous block and hence it forms a chain of blocks, with the first block known as the genesis block. Hence, it forms a linked list kind of structure.

Blockchain has several ledgers where data can only be appended but not deleted or tampered. Consequently, it is immutable. Blockchain can either be public, where anyone can read or write data onto the blockchain, or private, in which case only a few restricted individuals can read or write data.

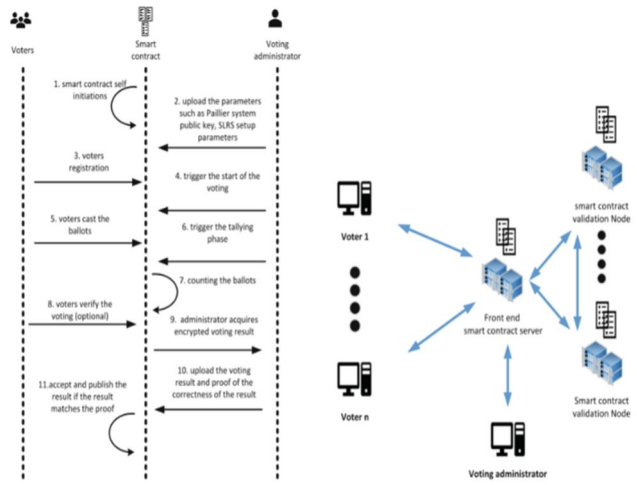
Existing E-Voting Systems and Betterment using Blockchain- Estonia has been using electronic voting (I-voting system) since 2005. The basis of this system is a national ID card given to all its citizens. These cards are encrypted files, which uniquely identify the owner and can be used for signing documents, banking services, and so on. For the voter to cast his/ her vote, the voter must insert their card into a card reader, after which the voter will be granted access to the voting website. Translating this process to the blockchain network to improve reliability and resolve concerns of manipulation from the client system, a system can be proposed consisting of two blockchains the vote blockchain and voter blockchain. This involves a registration process of voters followed by the voting process. In the registration process, the voter fills a form with all his/her personal details. This is a transaction and is added to the voter blockchain. In this process, the miner analyses the transaction and awards the user with a vote token, obtained from a pool of infinite vote tokens. Following this, a ballot paper and a password are sent to the voter, using which the voter can cast his/her vote. The user is now authenticated with the following three pieces of evidence: identification number, the password generated during registration and the ballot paper. As a result, following the authorization step of verifying the user's right to vote, another transaction is created in the same voter blockchain, which is the transaction containing the user's vote token, indicating the availability of the user's vote. Once the user votes, this transaction containing the user's vote is removed from the voter blockchain.

To simplify and scale the design, the system can be designed to have a 3-tier architecture: National, Constituency and Local. The local tier consists of all polling stations and is associated with a constituency node.

The constituency tier contains all nodes in the constituency level. The national nodes are responsible for mining transactions and adding blocks to the vote blockchain. As part of the design, there exists an encryption method based on public and private keys and a structure where the data is segregated and isolated logically. This segregation has been achieved by getting the different constituency level nodes to generate distinct key pairs. The public key of a constituency node will then be distributed to the polling station nodes connected to that particular constituency node, which use the public key to encrypt any vote made at those polling stations. The vote and voter data from all constituency nodes are then stored in an encrypted format within the blockchain and are propagated out to the entire network. Therefore, even if a hacker manages to get hold of a constituency private key, he/she would only be able to decrypt a part of the blockchain, that is, the votes originating from that constituency node.
Consequently, this design makes the system more independent and secure. However, this system is not effectively manageable for large-scale implementation due to large overhead in encrypting all the votes.
Blockchain Methodology for E-Voting System- Any blockchain-based e-voting system will consist of the following entities:

1) Smart Contract Admin
2) Voting Process Admin/ Authorization Organization.
3) Smart Contract
4) Voters

The architecture can be summarized as follows:



(a) The voting protocol diagram.(b) The blockchain evoting system.

IV. DISCUSSION

During the election time the admin will initiate the election. When the election is initiated the candidate, list is sent to the front end of the portal (which is setup at govt. authorized locations). The front end can display useful information on the candidate and can aid in their decision making (display promises, proposals etc.). The encrypted vote along with the user information is sent to the initiate vote method at the backend. This initiate vote method calls the account validation method which validates the user using the Aadhaar details and make sure that the user has not voted yet. If the user validation is successful then the vote cast method is called, which sends the vote as a contract to the Blockchain Service.

NOTE: At the end of the election, the candidate with the most votes is elected.

First the user come's to the interface of the website, where he will find that the election will be started soon, as the admin give's permission for the public to vote the user will be allowed to put his email id as well as 12 digit Aadhar number then he will be directed to other page where he will have to give the OTP sent to him, later he puts the OTP he will be given access to the voting page then after he votes a hash value is generated to that id and its stored in the blockchain, later even if he tries to vote again the system will not permit him to access the voting system unless and until the admin allows him to do so.

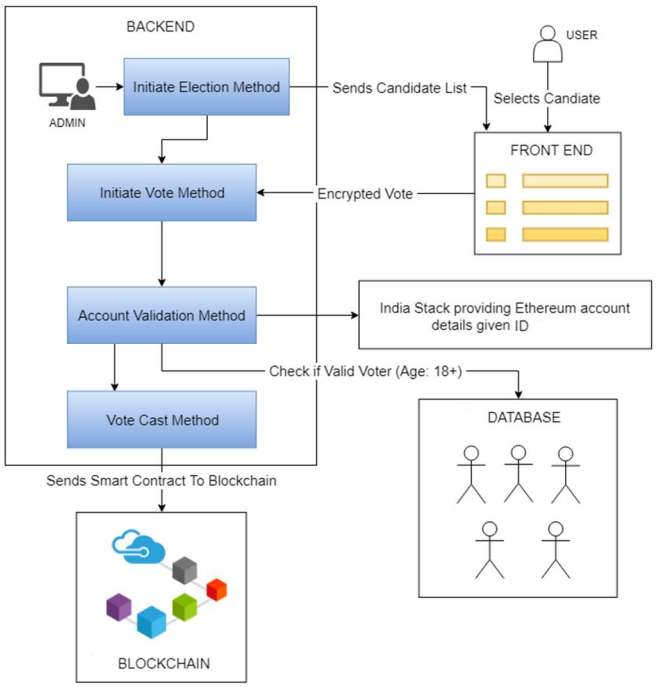


Figure: Workflow chart of the voting system

In continuation of this work, we are focused at improving the resistance of blockchain technology to 'double spending' problem which will translate as 'double voting' for e-voting systems. Although blockchain technology achieves significant success in detection of malleable change in a transaction however successful demonstration of such events has been achieved which motivates us to investigate it further. To this end, we believe an effective model to establish trustworthy provenance for e-voting systems will be crucial to achieve an end-to-end verifiable e-voting scheme. The work to achieve this is underway in the form of an additional provenance layer to aid the existing blockchain based infrastructure.

V. CONCLUSION

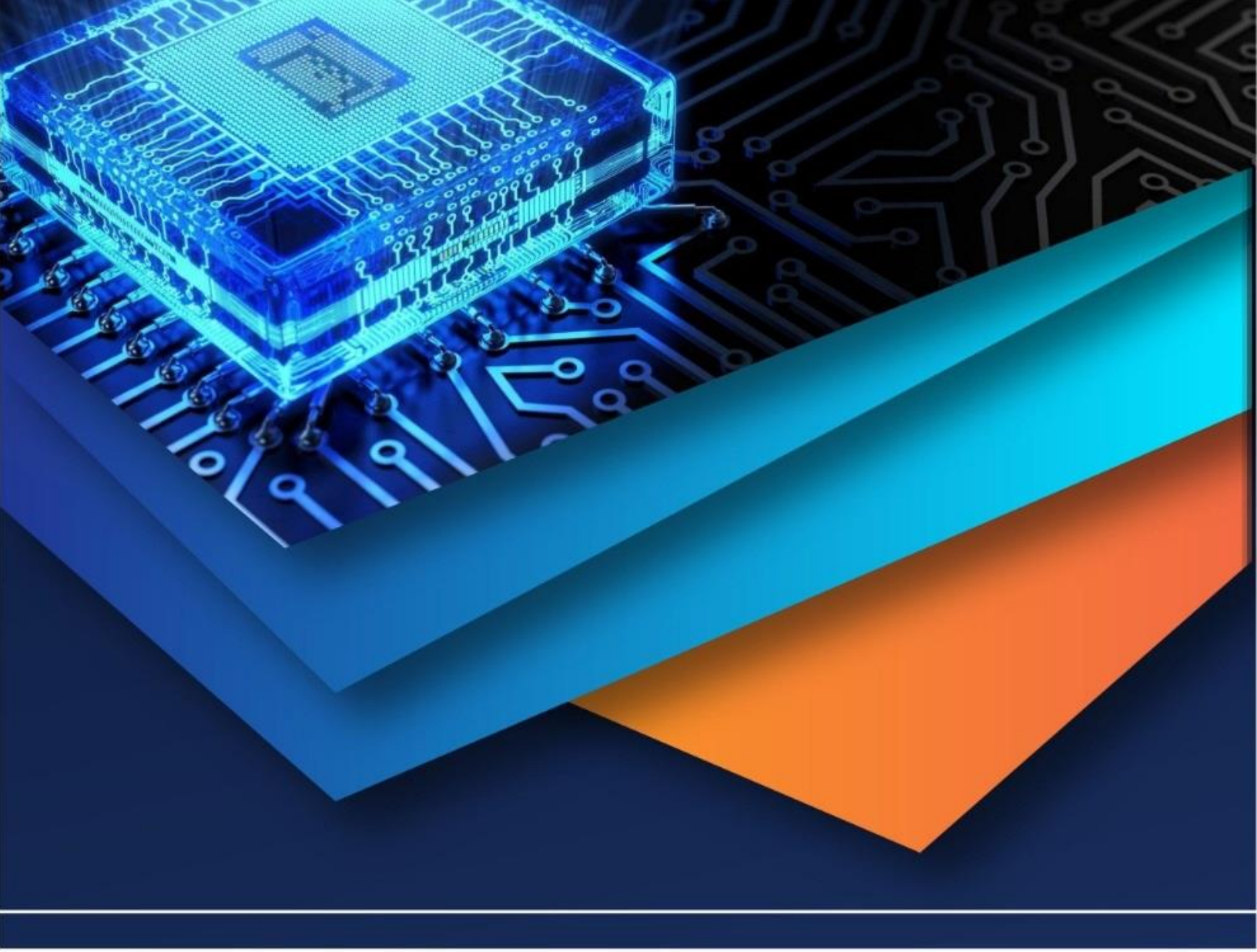
Our system takes advantage of the transparency of smart contract to allow all voters to participate in both the recording and verification of ballots. It enhances the voters' confidence and reduces the waste of election resource

Electronic voting has been used in varying forms since 1970s with fundamental benefits over paper-based systems such as increased efficiency and reduced errors. With the extraordinary growth in the use of blockchain technologies, a number of initiatives have been made to explore the feasibility of using blockchain to aid an effective solution to e-voting. This project has presented one such effort which leverages benefits of blockchain such as cryptographic foundations and transparency to achieve an effective solution to e-voting. The proposed approach has been implemented with Multichain and in-depth evaluation of approach highlights its effectiveness with respect to achieving fundamental requirements for an e-voting scheme

REFERENCES

[1] Abhishek Kaudare; Milan Hazra; Anurag Shelar; Manoj Sabnis, "Implementing Electronic Voting System with Blockchain Technology", 2020 International Conference for Emerging Technology (INCET)
[2] Kriti Patidar; Dr. Swapnil Jain, "Decentralized E-Voting Portal Using Blockchain",2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)
[3] R. Aroul Canessane, N.Srinivasan, Abinash Beuria, Ashwini Singh, B. Muthu Kumar,"Decentralised Applications Using EthereumBlockchain", 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)
[4] Jiazhuo Lyu; Zoe L. Jiang; Xuan Wang; Zhenhao Nong; Man Ho Au; Junbin Fang,"A Secure Decentralized Trustless E-Voting System Based on Smart Contract", 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)
[5] Vysakh Anilkumar; Joseph Antony Joji; Asif Afzal; Reshma Sheik1, "A Secure Decentralized Trustless E-Voting System Based on Smart Contract", 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)
[6] David Khoury; Elie F. Kfoury; Ali Kassem; Hamza Harb, "Decentralized Voting Platform Based on Ethereum Blockchain",2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)

[7] T.M. Roopak; R Sumathi, "Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology", 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)
[8] S.K. Vivek; R.S. Yashank; Yashas Prashanth; N. Yashas; M. Namratha, "E-Voting Systems using Blockchain: An Exploratory Literature Survey", 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)
[9] K Teja; MB Shravani; Chintarlapallireddy Yaswanth Simha; Manjunath R Kounte, "Secured voting through blockchain technology", 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)
[10] Using Blockchain Data Security Management for E voting system, "Using Blockchain Data Security Management for E voting system", 2020 8th International Conference on Cyber and IT Service Management (CITSM)
[11] Mario Navarrete; Rudel Huancas; Paúl DÍaz; Mauro Rivadeneira, "Blockchain electronic vote system", 2019 IEEE CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)
[12] Ravi Rahman; Kevin Liu; Lalana Kagal, "From Legal Agreements to Blockchain Smart Contracts", 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)
[13] Philipp Frauenthaler; Marten Sigwart; Christof Spanring; Michael Sober; Stefan Schulte, "ETH Relay: A Cost-efficient Relay for Ethereum-based Blockchains", 2020 IEEE International Conference on Blockchain (Blockchain)
[14] Tara Salman; Raj Jain; Lav Gupta, "A Reputation Management Framework for Knowledge-Based and Probabilistic Blockchains", 2019 IEEE International Conference on Blockchain (Blockchain)
[15] Harsh Desai; Murat Kantarcioglu; Lalana Kagal, "A Hybrid Blockchain Architecture for Privacy-Enabled and Accountable Auctions", 2019 IEEE International Conference on Blockchain (Blockchain)
[16] Paige Rodeghero; Collin McMillan; Abigail Shirey, "API Usage in Descriptions of Source Code Functionality", 2017 IEEE/ACM 1st International Workshop on API Usage and Evolution (WAPI)



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY