Review on Blockchain Voting Systems

Saksham Gupta

April 2024

[1]School of Computing Science Engineering, VIT University, Bhopal, India
[a)]Corresponding author: *saksham.gupta@vitbhopal.ac.in*

1 Abstract

Creating an electronic voting system that is secure, fair, and private while also being transparent and flexible has been a difficult challenge. This work-in-progress paper explores the use of blockchain technology as a service to develop a distributed electronic voting system. The paper proposes a new e-voting system that overcomes the limitations of existing systems and evaluates various blockchain frameworks for constructing it. The potential of distributed ledger technologies is analyzed through a case study of a national election process, where a blockchain-based application is implemented to enhance security and reduce costs.

Index Terms: blockchain-based electronic voting; blockchain technology; electronic voting; privacy; security; trust; voting.

2 Literature survey

Elections must use lawful, accurate, safe, and convenient electronic voting technology. But potential issues with electronic voting methods might prevent widespread implementation. Due to the benefits of end-to-end verification, blockchain technology was developed to address these problems. It provides decentralised nodes for electronic voting and is utilised to create electronic voting systems. [**?**]

Kashif Mehboob Khan1 et.al in offered a method for utilising the transparency and cryptographic underpinnings of the blockchain to build an efficient voting process. The suggested system achieves end-to-end verifiability and complies with the key criteria for e-voting schemes. The planned electronic voting system was described in full, along with how it would be implemented using the Multichain platform. The study provided a thorough analysis of the system, effectively demonstrating its ability to produce an end-to-end verifiable e-voting system. [**?**]

An outline of blockchain-based electronic voting systems was provided by Uzma Jafar et al in 2021. The analysis's main objective was to assess the state of online voting systems and blockchain-based voting re-

search, as well as any connected challenges, in order to forecast future advances. This study included an introduction to the basic structure and properties of the blockchain in relation to electronic voting as well as a conceptual description of the anticipated blockchain-based electronic voting application. The study led to the discovery that some of the problems now plaguing election systems may be resolved by blockchain technologies. [**?**]

Prof Mrunal Pathak et.al explored using a blockchain technology to record election results from all locations. The thesis presented a mechanism based on a predefined turn on the system for each node in the built-of blockchain, in contrast to Bitcoin's Proof of Work. [**?**]

3 Problem statement

As discussed, creating a voting system that is secure, robust, fair and private has been a really difficult challenge. Along with this we must alos make sure that the system is flexible and transparent. Block chain technology provides us with such an platform which can be used to make the voting system more secure, private and fair while also maintaining the transparency of the transactions (votes) and flexible. [**?**]

In order to have the close to perfect model of a voting system, we must first take into consideration certain requierments. These requierments can be listed down as:

(i) Coerced voting shouldn't be possible in an election system. (ii) A voting system ought to support a technique for safe authentication using an identity verification service. (iii) A voting system shouldn't permit linking of votes to specific voters. [**?**] (iv) An election system should promote openness by giving each voter the verifiable confidence that their vote was counted fairly and without jeopardising their right to privacy. (v) A voting mechanism ought to make it impossible for outsiders to meddle with any votes. [**?**] (vi) The ability to tally votes and choose the winner of an election should not be granted to a single body by an electoral system. (vii) A voting mechanism should only permit those who are eligible to do so. [**?**]

4 Introduction

Electronic voting systems have been actively studied for decades with the goal of minimizing the cost of operating elections while ensuring voter integrity while meeting security, privacy, and compliance requirements. [1]. Replacing the traditional pen-and-paper system with a new electoral system can limit fraud and at the same time make the electoral process traceable and controllable. [2] Blockchain is a decentralized, immutable, indisputable public ledger. This new technology has three main functions: [**?**] (i) Immutability: Each "new block" proposed for the ledger must refer to a previous version of the ledger. This creates an immutable chain, from which the blockchain gets its name, and prevents the integrity of previous records from being altered. (ii) Verifiability: The ledger is decentralized, duplicated, and divided into several places. This provides high availability (ie eliminates a single point of failure) and provides third-party assurance because all nodes maintain a consensus ver-

sion of the ledger. (iii) Decentralized Consensus: A decentralized consensus protocol determines who can add the following new transaction to the ledger. Most network nodes must reach a consensus before a new proposed entry block becomes a permanent part of the ledger. These features are partly achieved through an advanced encryption technology that provides greater security than any previously known protocol system. Therefore, blockchain technology is considered by many [3], including us, to have significant potential to implement a new modern electoral process. [**?**]

5 Previous methodology

Several techniques for blockchain electronic voting systems have been presented in the past. One popular method is to utilize a public blockchain to store voting data, with each vote recorded as a transaction on the blockchain. Voters are recognized in this system via digital signatures, and the blockchain assures that each vote is immutable and transparent. [**?**] Another alternative is to utilize a private or consortium blockchain, which restricts access to the blockchain to authorized parties. Voters are identifiable in this system via digital certificates, and the blockchain assures that each vote is tamper-proof and auditable. [**?**]

A hybrid blockchain is utilized in a third solution, where a public blockchain is used for transparent vote counting and a private or consortium blockchain is used for secure voter identification and authentication.

Regardless of technique, all blockchain electronic voting systems strive to provide a safe and transparent method of conducting elections by exploiting blockchain technology's qualities such as decentralization, immutability, and transparency. However, such systems may be challenging to install, and various technological and regulatory hurdles must be addressed to ensure their effective adoption. [**?**]

Scalability difficulties plague currently existing blockchain-based voting systems. These systems are suitable for usage on a modest scale. Nonetheless, such systems are inefficient for handling millions of transactions at the national level since they leverage contemporary blockchain frameworks such as Bitcoin, Ethereum, Hyperledger Fabric, and others. [**?**] Because of the scalability issue with blockchain value suggestions, changing blockchain settings is difficult. It is inadequate to raise block size or reduce block time by reducing hash difficulty to scale a blockchain. Each technique reaches a limit before it can handle the volume of transactions required to compete with firms like Visa, which handles an average of 150 million transactions each day. [**?**] According to Tata Communications research published in 2018, 44 % of organizations employed blockchain in their study which alludes to broad difficulties coming from the usage of new technologies. Unresolved scalability issues emerge as an architectural impediment to blockchain acceptance and practical applications. According to Deloitte Insights, "Blockchain-based systems are comparatively slow." The slow transaction speed of blockchain is a key worry for organizations that rely on

high-performance traditional transaction processing technologies." [**?**]

6 Proposed Methodology/Algorithm

The suggested system is divided into three phases along with the following three elements:
1. The phase of beginning.
2. The voting process.
3. The counting and verifying process.
The first stage involves setting up the hardware and software tools that will be used to authenticate and authorise the elected officials, the corresponding electoral districts, and the usage of VIT (Vote Identification Token) numbers to identify and authenticate the votes. during which each voter authenticates themselves at their voting place. A random envelope holding the VIT number is then selected by the voter. In order to complete the process, the voting location enters the VIT. Once the vote has been cast, the vote is posted to the blockchain if the authorisation is approved. Voting is further protected by the generation of a printout known as the VVPAT (Voter-Verified Paper Audit Trail), which acts as confirmation of the procedure. The third stage demonstrates the counting and auditing of the vote process once the election is over. The super-node chain and trustworthy nodes are used to tally the votes. The outcomes are then contrasted to ensure validity. The two chains are then contrasted to look for any apparent abnormalities. To ensure that the chains are accurate, the votes cast through VVPAT are tallied. The election results are released if this step is successful. For the ABVS system, they have introduced the usage of a multi-agent system; the fundamental justification for doing so is the need to address issues of a distributional or computationally challenging type. Decentralisation may be accomplished by using a system like this since each agent can contribute to a variety of rules that set up and prepare the system. The system deals with two different types of phases. The first one is the authorization-configuration agent, which handles authorization and configures the voting system. The second one deals with the voter by handling a voting card and sending a vote to the nodes along with all the necessary vote metadata, such as a timestamp, a VIT number, information about the polling place, etc.

7 Module Description

This module creates a system that can be used to conduct fair and transparent voting system using blockchain technology. It does so by the use of a decentralized network of nodes which are used to verify the authenticity of the votes and store them in a blockchain. Doing this ensures the fact that the results recorded ensure that the election process cannot be tampered with or manipulated.

This module comprises of the following components:

1: Voter registration and Authentication: Voters can use the system to securely and independently register their identification and eligibility to vote.

2: Vote Casting: Voters use an online or mobile application to cast their ballots. To save and verify the vote, it

is encrypted and sent to the blockchain network.

3: Vote Counting: The vote counting is done automatically, and the results are generated and stored on the blockchain.

4: Result Verification: By checking the blockchain record, voters may confirm that their vote was tallied and that the election results are valid.

5: Audit Trail: The module creates a thorough audit record of the voting procedure, including all of the blockchain network's transactions.

6: Administration: For handling the election process, including voter registration, ballot production, and result generation, the system offers an administration interface.

8 Proposed Design/Architecture

The well-known Prêt à Voter e-voting method described in (Ryan, 2008) serves as the foundation for the proposed electronic voting system. A voting application has been supported by the system in the real-world setting while taking into account certain needs like privacy, eligibility, convenience, receiptlessness, and verifiability. With the suggested approach, safe digital voting is achieved without sacrificing usability. In this regard, the system is created with a web-based interface to simplify user interaction with security features like finger printing to prevent double voting. A user-friendly administrator interface is designed to facilitate ease of access because there is an obvious need to administer the voters, constituencies, and candidates for constituencies. The system also creates a fair and healthy competition by giving all voters the same rights to participate. Additionally, the system maintains voter anonymity while granting all voters equal participation rights and encouraging fair and healthy competition among all the candidates. The voter receives an email containing the transaction's cryptographic hash (ID) as confirmation that their vote was cast. This hash can then be used to monitor the voter's vote outside the boundaries of the constituency.

The suggested architecture for the electronic voting system is shown in Fig. 1, and it has been separated into a number of levels to accomplish modular design. below is a description of these layers; Front-end interaction with users The security layer is in charge of communicating with the voter (to facilitate voting operations) and the administrator (to assist election administration duties). It combines two essential tasks, namely user authentication and authorization (for voters and administrators), to guarantee that only authorised users have access to the system in accordance with established access control regulations. This function can be accomplished using a variety of techniques, from straightforward username/password authentication to more sophisticated techniques like fingerprint or iris recognition.

As a result, they become customised for each installation. As a result, they become unique to each implementation of the suggested architecture. In general, this layer acts as the first point of contact with users and is in charge of verifying user credentials in accordance with the rules set

forth by the system. By offering the services necessary for layer 1 and layer 3 to perform as expected, the access control management layer is intended to facilitate these layers. Roles definition, the corresponding access control rules, and voting transaction definitions are all included in these services. The layer 1 access control functions are fundamentally supported by role definition and maintenance, whereas layer 3 mining and transaction mapping on a blockchain are supported by voting transaction definitions. Overall, by providing the support needed by other layers, this layer enables the proposed system to work coherently. The transaction for evoting created at the Role Management / Transactions layer is mapped onto the blockchain transaction that needs to be mined at the e-Voting Transaction Management layer, which is the fundamental layer of the design. The authentication credentials supplied by a voter at layer 1 are also included in this mapped transaction. The voter's fingerprint is one example of this data. The transaction ID is then generated using this data, which is also used to generate the cryptographic hash. The User Interaction and Front-end Security layer (layer 1) is where it is intended to be possible to verify such credentials. To finally add this transaction to the chain, mining is being done by a number of virtual instances of nodes. Using one of the current database technologies, the Ledger Synchronisation layer synchronises the Multichain ledger with the local application-specific database. The data tables at the database's backend keep track of votes cast. As soon as a vote is mined and uploaded to the blockchain ledger, voters are given a unique identification that allows them to track their votes. Voting security is built on block-chain technology, which secures end-to-end communication using cryptographic hashes. In order to enable audits and any subsequent procedures, voting results are also recorded in the application's database.

9 Implementation Detail

According to the specified voting requirements and blockchain as a service, a new electronic voting system is suggested in this section. We describe the blockchain's setup, the smart contract for electronic voting that will be used on it, and how the suggested system complies with the expected voting criteria. A. Blockchain setup First voters must cast their ballots in a controlled setting in order to meet the privacy and security standards for electronic voting and to guarantee that compelled voting is not possible. In order to accomplish these objectives, we put up a Go-Ethereum [7][9] permissioned Proof-of-Authority (POA) blockchain in our work. A consensus technique based on identification as a stake is used by POA to deliver transactions very quickly. In section C, a justification for employing Go-Ethereum for the blockchain infrastructure is given. Figure 1 shows the organisation of the blockchain, which primarily comprises of two different kinds of nodes. (i) District node: Comprised of each electoral district. There is a software agent on each district node that independently communicates with the "bootnode" and controls the smart contract life cycle on

that node. A ballot smart contract is issued and installed onto the associated district node when the election administrator initiates an election (see the section on smart contracts for more information). Each of the related district nodes is given access to communicate with their corresponding contract when the ballot smart contracts are formed. The vote data is validated by the majority of the associated district nodes when each voter casts a vote from their corresponding smart contract, and each vote that they concur upon is added to the blockchain. (ii) Bootnode: Each institution that has been granted access to the network is required to host a bootnode. A bootnode is a coordination and discovery service that aids with district node discovery and communication. In order to let district nodes locate their neighbours more quickly, the bootnode operates on a static IP and does not maintain any state of the blockchain [6]. The next stage is to develop and implement a smart contract that reflects the e-voting process on the blockchain infrastructure after creating a secure and private blockchain. B. Selecting to become a smart contract There are three components to defining a smart contract: Identifying the roles engaged in the agreement, in this case the election agreement, as well as the election process and the transactions employed in the smart contract are the first two steps in any agreement. Election-related roles: The parties required for participation in the agreement are among the roles in a smart contract. Following are some responsibilities in the electoral process: Election lifecycle management is the responsibility of the election administrator (i). This function may enlist several reliable organisations and businesses. Election administrators are in charge of creating elections, registering voters, determining how long they will last, and allocating permissioned nodes. B. Selection as a smart contract Three components make up the definition of a smart contract: (1) identifying the roles that are involved in the agreement (in our example, the election agreement); (2) the agreement process (i.e., election process); and (3) the transactions (i.e., voting transaction) utilised in the smart contract. 1) Election-related roles The parties required to take part in the agreement are among the roles in a smart contract. The following roles are involved in the election process: (i) Election administrator: To oversee the whole election lifecycle. This duty may be taken up by several reliable organisations and businesses. The election administrators designate the election, register voters, select the election's duration, and assign permissioned nodes. Voter registration is (ii). The election administrators are in charge of voter registration. The election administrators must specify a deterministic list of eligible voters when an election is formed. For a government identity verification service to securely authenticate and authorise qualified persons, this could require a component. To satisfy the necessity for secure authentication, which is not by default ensured when utilising a blockchain infrastructure, one must use such a service. In our approach, a matching identification wallet would be established for each qualified voter. For each election in which a voter is entitled to cast a ballot, an individual wallet is created. (iii)Results tallying: In the smart contracts, the election re-

sults are calculated instantly. Each voting smart contract keeps track of the results for its respective location in its own storage. (iv)Verifying votes: Each voter obtains a transaction ID for his vote during the voting process. In our electronic voting system, voters may use this transaction ID to find the transaction with the associated transaction ID on the blockchain at an official election site (or authority) after verifying themselves with their electronic identification. Voters may thus check that their votes were listed and counted accurately by viewing their votes on the blockchain. While prohibiting vote tracing, this kind of verification meets the transparency requirements. 3) Voting transaction: Every voter engages with a smart contract for the ballot that corresponds to her voting district. The district node that corresponds to this smart contract communicates with the blockchain and adds the vote to it. The transaction ID for each voter's vote is given to them individually for verification reasons. Each vote that has the support of the majority of the district nodes in question is recorded as a transaction and added to the blockchain.

10 Simulation Setup and Environment

As dicussed in [**?**] in order to maintain the requierments for privacy, security and transparency for the e-voting system as well as to ensure that the e-voting system should not be allowed to to record coerced voting, in this model, we set-up our model on a private (permissioned) blockchain as the infrastructure where the smart contracts will be deployed. For our model, we use three different blockchain network frameworks for implementing and deploying the elction smart contracts.

11 Comparative analysis of techniqual findings

These are the same frameworks used in [**?**], Exonum, Quorum and Geth. More information on these are given below:

1: Exonum: The Rust programming language was used throughout the Exonum blockchain's whole development, ensuring its durability end-to-end. Built for private blockchains is Exonum. It uses a customised version of the Byzantine algorithm to reach network consensus. Up to 5000 transactions per second are supported by Exonum. The framework's unfortunate limitation—Rust being the sole language supported in the present version—limits developers to the constructs offered by that language. In order to make Exonum more developer-friendly, Exonum plans to provide Java bindings and platform-independent interface description in the near future.

2: Quorum: A distributed ledger technology built on Ethereum with novel consensus processes, transaction/contract privacy, and transaction security. As a Geth fork, it is updated in accordance with Geth updates. The consensus method has been modified by Quorum, which now favours consortium chain-based consensus algorithms. It can accommodate hundreds of transactions per second by using

this consensus.

3: Geth: One of the three initial implementations of the Ethereum protocol is Go-Ethereum, often known as Geth. It executes smart contract applications precisely as intended, free from the risk of downtime, censorship, fraud, or outside influence [7][9]. This framework is the most developer-friendly of those we reviewed and enables development beyond the Geth protocol. Whether a public or private network is used to construct the blockchain will affect the transaction rate. Geth was the framework we selected to base our work on because of these features, however any comparable blockchain framework with the same capabilities as Geth might be taken into consideration for such systems. // The comparison between the different frameworks is shown below in Table 1:

	Exonum	Quorum	Go-Ethereum
Consensus	Custom-built BFT algorithm	QuorumChain, IBFT and Raft-based consensus	PoW, PoS and PoA
Transactions p/s	up to 5000 transactions p/s	Dozens to hundreds	Depends
Private	support	Yes	Yes
Smart Contract Language	Rust	Solidity	Solidity
Programming Language	Rust	Go, C, JavaScript	Go, C, Javascript

Table 1: Comparison between different frameworks

12 Conclusion

In this paper, recent research on blockchain-based voting systems will be reviewed and evaluated. The study in the article uses blockchain technology to offer a systematic mapping analysis that compiles the most recent e-voting research. The blockchain idea and its applications are provided before information on existing e-voting methods. Then, a number of flaws in the current e-voting systems, opportunities presented by the blockchain concept to enhance e-voting, existing blockchain-based e-voting system solutions, and prospective future research areas are noted and explored. The blockchain can serve as an appropriate mechanism for a decentralised e-voting system, according to many academics. Additionally, all voters and outside observers can see the voting records kept in these proposed systems. On the other hand, we discovered that the majority of articles on blockchain-based electronic voting acknowledged and addressed related issues. Five categories were used to classify these problems: general, integrity, coin-based, privacy, and consensus. Future study on e-voting has to take into consideration a number of research gaps that have emerged. Attacks on scalability, a lack of transparency, the use of unreliable systems, and coercive resistance may have additional drawbacks that need to be addressed. We are not entirely aware of all the concerns connected with the security and scalability of such systems since the blockchain-based e-voting systems still need more testing. Voting procedures based on blockchains may introduce unidentified security concerns and vulnerabilities. Blockchain technologies demand increasingly sophisticated software architecture and man-

agerial abilities. Using the prior knowledge, these important concerns should be explored in greater depth during actual voting procedures. Due to this, e-voting systems should be implemented in limited pilot locations first before being expanded. There are still significant security flaws in both voting machines and the internet. Significant security improvements will be needed in order to conduct electronic voting over a trustworthy and secure internet. Despite appearing to be the ideal answer, it was determined that the blockchain system's flaws prevented it from properly resolving the voting system's issues. This study demonstrated that blockchain systems had flaws that required further attention and that there are still a lot of technical challenges. It is crucial to understand that an e-voting system based on blockchain technology is still in its infancy.

References

13 Authors

First Author - Saksham Gupta, B.Tech 4th Year, Vellore Institute of Technology, Bhopal, saksham.gupta@vitbhopal.ac.in