A Secured Election through Distributed Ledger

Pragya Vaishnav[1*],
Assistant Professor,
Department of Computer Applications,
Manipal University Jaipur,
Jaipur, Rajasthan, India

,

Aswin Rajendiren[2]
DSP Explorer,
MS – Oracle – DBA,
Leeds, UK

Abstract : **The field of distributed ledger technology and blockchain has experience significant growth in popularity in the last several years. The assurance of an entirely safe environment for data storage has piqued the imagination of individuals and organizations alike. Consequently, companies have begun to allocate substantial resources towards pertinent research and system development, particularly in the domains of banking and cryptocurrencies. In this work, we concentrate on systems that go beyond these subjects in an effort to address the problem of vote-tallying tampering in elections worldwide. Author has created a tamper-proof technique that implement a distributed ledger system and a permissioned consensus process to offer a safe and secure voting environment for proposed system, BWI.**

Keywords: *Blockchain, Distributed Ledger, Voting System, BWI.*

1. Introduction

Blockchain technologies, also known as distributed ledger technologies, or DLTs, are fundamentally changing how we think about data security and cryptography.

A blockchain is a distributed ledger of transactions kept on numerous nodes, all of are required to continuously maintain an accurate and up-to-date copy of the record without the need for a single node to oversee or manage the process. By using consensus techniques and cryptographic protocols, nodes can verify the veracity of the data they possess without requiring the assistance of a third party.

Although the original objective of this technology was to safeguard financial transactions, interest is currently being directed towards uses other than money transfers. The goal of this research is to address a significant issue with data security and integrity related to elections worldwide by leveraging the enormous possibilities of this technology. The majority of nations in the globe still conduct elections and vote in the conventional manner. On a sheet of paper, voters would write down the candidate's name they wanted to win and place it in a voting box. This is a government-secured method that relies solely on public confidence in the election commission that is in charge of gathering and organizing the votes. The trust model is not without problems, as evidenced by the numerous instances of ballot boxes being stolen, tampered with, or even demolished that have been reported around the globe. Furthermore, there have been multiple instances of a significant number of fictitious and fraudulent votes being tabulated, which invariably resulted in the incorrect individuals holding pivotal positions. Making decisions on a large scale, like a whole country, is a difficult and important activity that needs a safe environment where all stakeholders are happy. Everyone's rights would be upheld, and prosperity should follow.

Data security will be guaranteed without a third party's assistance thanks to blockchain technology. In order to ensure nodes' privacy, it can be accomplished by making the data public after it has been mathematically encrypted (among the permissioned nodes). This way without the ability to alter any of the data and, if necessary, without knowing the identity of the person who entered it,

each concerned node can confirm it. This suggests that since human error cannot affect the system, all that is required is trust.

2. Background

A quick summary of related technologies is given in this section.

2.1. Computer Cryptography Overview:

An extra input for the cryptographic system is a key. Keys are used in common computer cryptography methods to encrypt data using specific methods. In order to shape the encrypted result transformed into a specific and unique format that can be decrypted with either the same key or a different key.

A symmetric key is one that may be used to both decrypt and encrypt data. Conversely, asymmetric key pairs are those in which, in the event that one data is encrypted and additional key can be locked., and vice versa. As a result, one of the keys dubbed the "private key" should remain a secret from its proprietor. The other is known to as the "public key" and is well known to all. As a result, communications sent to separate parties are encrypted using that party's public key, and only that party's private key may be used to decrypt the message.

A symmetric key that is transferred across nodes via their asymmetric keys is called a session key. This key is only good for a short span of time. For distinct connections, and occasionally even for distinct messages sent over the same connection, various session keys are utilized. Another degree of security for message exchange is added by session keys. With challenge-response authentication, a question is posed to those requesting to be authenticated by an authenticator; only those who meet the eligibility requirements can correctly respond. Passwords are the most popular example of this.

2.2. Evidence of Passed Time

A consensus occurs in a blockchain when nodes decide whether to append newly suggested data to the ledger that is records.

These days, there are several ways to reach a consensus. Intel developed an one popular method which is the evidence of passed time, which is an open-source method created by Intel.

The main notion is that when a decision needs to be made unanimously, the nodes are designed to set random timers. Even though the new data is allowed into the ledger or not is decided during the consensus session by the first node whose timer expires. It's important to note that this method is applicable only to permissioned and private ledgers, where only nodes with attributes are allowed to join the network. This differs from permissionless and public ledgers, where anyone can take part in the process

3. Literature Review

Numerous solutions were put up to address particular problems with electronic voting and provide clarification on certain technological constraints. The platform dependence of the majority of blockchains is one of the topics that has been studied [1]. Scholars contend that performance and security problems arise from a reliance on a certain platform. A few academics attempted to leverage the public blockchains now in use, including Etheruem [2, 3, 4]. Additionally, several commercial alternatives were put up, such as Agora [5], an end-to-end verifiable voting solution designed for use by institutions and governments. Additionally, models have been developed to optimize voter information security

and privacy, as noted in Blockchain-Based E-Voting System [2], the authors of which have created a custom model. Their research indicates that two other recently suggested models are A Smart Contract for Digital Voting Using Blockchain Technology [1] and Boardroom Voting with Maximum Voter Privacy [8].

By creating a permissioned ledger—a system in which only users with permission can participate—the model put forward in this study seeks to circumvent the issue of open ledgers and offer a more effective consensus mechanism for voting.

4. Proposed Work

The proposed BWI system comprises three primary components: the blockchain network, a web user application, and an intermediary authentication server that handles the connections between the client application and the blockchain. The process begins with the server, where an administrator initiates a new election for the BWI by inputting candidate information into the database and providing essential details about the election, including start and end dates, times, and other relevant information.

At this point, however, the server initializes the election data on the blockchain nodes. Here, it's crucial to remember that the nodes are computer programs that can only be managed by the server not by an administrator or user who is human.

Data manipulation on the chain is restricted to what is permitted by the blockchain's consensus mechanism and transaction logic, which are unchangeable. It's also crucial to note that the admin's data entered into the server is open to the public, so there's no need to worry about it being altered or manipulated.

The server comes equipped by default with a database that holds data on every person who is entitled to vote. In a real-world application, this server may be a blockchain created by the approved organization to safely store the data of its members from the moment they join the community in order to achieve the highest level of security.

Since we are more interested in the activities that take place within the blockchain network, we will assume for the purposes of this research that this server is secure. As we previously indicated, the administrator's only responsibility is to enter certain public data; they should not, under any circumstances, be able to alter any other data. This requirement might only apply to a blockchain-based server and not to our situation since we are showcasing our network utilizing a basic MySQL database.

Via a web page, the user establishes a connection with the server and provides the necessary details to verify their identity. After that, the server verifies if the user is authorized to access the network by comparing these details with its database. The server then adds a new user to the blockchain if the requirements are met. In response, the blockchain network issues a token. This token serves as a key that enables the user to conduct network transactions, such as voting. After giving the users their tokens, the server sends them to a website where they can cast ballots.

The token is a one-time token, meaning that the user can only use it for the specified set of candidates and for one transaction, which is voting, in accordance with the guidelines established by the governing body. Candidates who are eligible to vote and who meet the same requirements as ordinary users may access the network. They may vote once, either for themselves or another candidate. Once a user has cast a ballot, they are not allowed to do so again.

The results of the dynamic voting will remain secret from the public during the election process. The results won't be available until the procedure is complete. The blockchain allows for their public publication. As an alternative, anyone

can inquire and view the outcome. This is done in order to prevent prejudice of any type, as people have a propensity to follow the crowd, which could compromise the process's integrity.

A vote in the blockchain is referred to as an asset. The value that will be traded between the participants is an asset. The blockchain is made up of several nodes. A machine that runs the blockchain code is called a node. A PoET consensus session is started when a node broadcasts its vote to all other nodes. Once a vote is agreed upon, all nodes record it to their ledgers, ensuring that the recorded vote is unchangeable. For the suggested system model, see Figure 1.

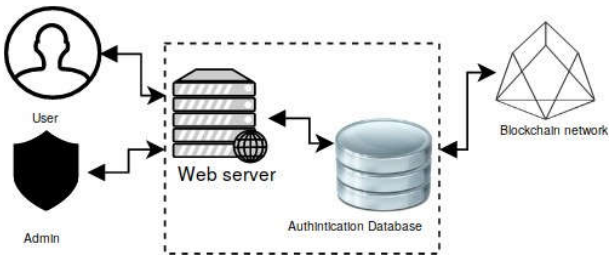

Fig. 1. BWI.

5. System Architecture

Three primary components make up the proposed system: the Blockchain network, a server, and clients.

This system has two different kinds of clients: users and administrators. The admin, a dependable member of the host institution, is in charge of giving the system the data it needs to set up the election. This data is condensed into a particular structure.

The user is a person with voting rights. The database that the system administrator supplied should contain the user's identity. Before creating an account to be used for voting, the user must authenticate themselves to the system. There is a communication unit between the authentication server and the web server.

Every node in the peer-to-peer blockchain network is a computer programme that needs to be set up by a reliable party beforehand. The challenge response mutual authentication mechanism was used in the architecture of the permissioned blockchain to require mutual authentication between nodes and the web server. Nodes are in charge of finding one another and coordinating communication amongst themselves; this synchronization was achieved by using a condensed version of the evidence of passed time consensus process.

The nodes are in charge of recording the votes in the secure ledgers and include information on every account that has been formed, including a special random identity known as the "account hidden id" that corresponds to the user's chosen token. The workflow of the system is shown in Figure 2.

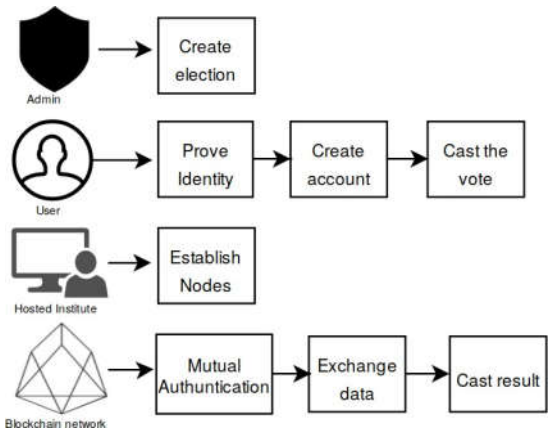

Fig: 2 Workflow of the BWI

6. Implementation

6.1 Validator Nodes

The nodes that make up the blockchain network are divided into two categories: participant nodes, or standard blockchain nodes, and validator nodes. A node with a specific function, known as a validator, is in charge of overseeing and verifying the authenticity of the participating nodes. The other nodes are aware of the IP address and port number of the validator. A shared key representing the new network must be given to the validator node, which is the first node to be created. In order to get verified and take part in the blockchain, every other node connects to the validator with this key.

For the demonstration network, we have one validator node and several participant nodes, with the validator's address preconfigured on the nodes. To guarantee optimal efficiency, the network needs a large number of validators, and depending on the network's current status, nodes can always connect to a different validator. The management of the validators' addresses also requires a DNS server or some other mechanism, but this is outside the purview of our study. The network ID is provided by the shared key. This key belongs to the network if the node possesses it. The first validator on the network determines the shared key, which is required for all other nodes, including the web server, to join the network. To guarantee that you are utilizing a powerful key, there are a few specific limitations.

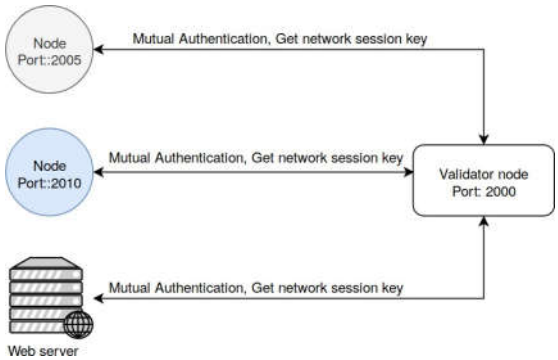

Fig. 3 Communication of nodes with the validator

6.2 Mutual Authentication and Node Discovery

The validator bides its time for more nodes to connect to the network after it has been formed. The validator node should receive an authentication request from any new nodes wishing to connect to the network. The time duration that the node needs to encrypt with the shared network key in order to respond to the validator is called a challenge. The server waits for the challenge response; The validator notifies the node that it has succeeded if the result matches the expected value; if not, it sends a message indicating failure. The node authenticates itself to the validator in the same way. Replay attacks, where a malicious node uses a previously sent message between a node and a validator to impersonate itself, are prevented through the use of timestamps. A non-double-used value is called a timestamp. Additionally, the web server and validator need to mutually authenticate.

Following mutual authentication, the validator gives the addresses of every active node on the network to the new node and gives the addresses of every inactive node to every active node.

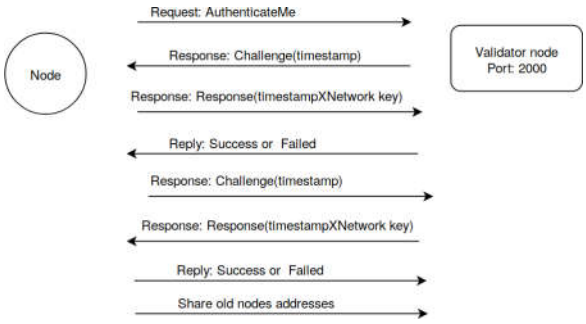

Fig. 4. Mutual Authentication

6.3 Creating user Account

Upon registering to take part in the election process, a new user's data is processed through a cryptographic function to produce a digest value. This value is then checked to the data on the authentication server, confirming the user's eligibility to vote. The creation of a new user profile on the blockchain is then accomplished by sending this value to a randomly selected node. The cryptographic digest functions as the user's anonymous network identity.

The digest is sent to a node in the form of a transaction signed with the server's private key as adding a user to the blockchain is considered a transaction. The user profile is created on the chain and shared with other nodes in compliance with consensus standards once the node has validated the signature. The new user receives one token on the network, which gives him or her the right to one vote.

6.4 Transaction and Handling Votes

The two sorts of transactions on the blockchain are voting and user creation; we covered the former in the last section. The web server sends the user to a webpage where they can select their favorite candidate when they're ready to cast their ballot. Subsequently, the web server transmits the selection to a node for inclusion in the blockchain in the form of a transaction.

The transaction message includes the sender and recipient's public keys, the transaction type, and the payload—which could be a vote or a user. The signature is attached to the message and is part of the message itself.

Upon receiving a vote transaction, a node verifies that the voting user is active on the network and has a token. If all the requirements are met, a consensus meeting is convened to add the vote to the chain and create a new block. The hashes of the previous and current blocks, a timestamp, the vote, and the Merkle root—which is the hash of all previous hashes in the chain—are all included in this block.

The concept of chaining is created by combining all of the hash values. The vote is not accepted if any of the requirements are not met. Every token that is awarded to a user is tracked by the node. To make sure that every node has the most recent version of the blockchain, we developed our own streamlined software version of the PoET consensus process.

The blockchain stops accepting transactions at the conclusion of the election process and is prepared to reveal the results. Until now, the outcomes remain unknown. To send the findings to the web server, a random node is selected. To guarantee that no data is kept on the web server and that all information is safe on the blockchain, this is done dynamically each time a user requests to view the results.

7 System Testing

We made a fake database and submitted it to the authentication server in order to test the system. registered as participants in the network, and attempted to cast votes for fictitious candidates. Votes were successfully counted by the system. The votes were seamlessly and irreversibly transmitted between the nodes; the data was encrypted and chained together in the form of blocks, meaning that no node could ever recover the stored information. The system accurately displayed the fact that tokens are lost the instant they are cast, so that no participant was allowed to cast a second vote. The web server and blockchain nodes were all operated on the same local network, and customers could access the web application using any standard web browser. We also tested mobile web browsers, and the web application worked flawlessly with all user-friendly browsers.

The author also attempted to run several nodes concurrently; we were able to run as many nodes as author wanted, and the system remained stable. The validator could handle the addition of new nodes and the exchange of addresses amongst all the nodes.

The author is able to operate our system through a Linux terminal; as a result, we could execute commands and view log files, which made it simple for us to monitor system activities. Overall, our technology has the potential to be an effective tool for securely storing data, and when combined with other blockchain systems, it will offer a safe substitute ecosystem for database systems.

8 Result and Recommendation

Our study has shown that blockchain technologies can be extremely effective tools for replacing conventional database systems. There is a great deal of promise for using blockchain technologies outside of the finance industry, such as with Bitcoin and other blockchains. We advise organizations to begin thinking about the advantages of endorsing blockchain systems, as the more organizations that do so, the more robust blockchain systems will become. As we developed our system, we realized that, in most cases, one would want a strong infrastructure in order to create a blockchain application that is capable of fully securing data. We envision a fully functional blockchain supersystem,

with subsystems that collaborate and are assigned distinct responsibilities. This is what we believe blockchain technology offers. Further research should be done on both integrating various blockchain systems and establishing guidelines for their cooperation.

Our system demonstration demonstrated stability and demonstrated that the objectives we set out to accomplish could be met with a blockchain system; however, as we have already indicated, the system may not function as well without robust infrastructure. The system functioned flawlessly when we ran a fictitious, straightforward election procedure on it, handling vote counting and security.

9 Conclusion

In contemporary countries, where voting is a means of electing deserving individuals to positions of official power, reliable, secure voting systems that are impervious to manipulation have become essential. This study suggests a novel blockchain-based safe voting system concept. The suggested model BWI has a good chance of being an effective tool to address the issues with the current voting system, according to the results of preliminary small-scale testing.

The suggested system has not yet been put into practice or tested in a large-scale voting environment in real life.

References

[1] Khan, Kashif Mehboob, Junaid Arshad, and Muhammad Mubashir Khan. "Secure digital voting system based on blockchain technology." International Journal of Electronic Government Research (IJEGR) 14.1 (2018): 53-62.

[2] “Agora,” Available at https://goo.gl/SyjpK8

[3] Yu, Bin, et al. "Platform-independent secure blockchain-based voting system." Information Security: 21st International Conference, ISC 2018, Guildford, UK, September 9–12, 2018, Proceedings 21. Springer International Publishing, 2018.

[4] “Developer guide-bitcoin.”Available at https://bitcoin.org/en/developer-guide.

[5] Yavuz, Emre, et al. "Towards secure e-voting using ethereum blockchain." 2018 6th International Symposium on Digital Forensic and Security (ISDFS). IEEE, 2018.

[6] Navroop, S., et al. "Blockchain for Business-An Introduction to Hyperledger Technologies." Tillgänglig online: https://courses. edx. org/courses/course-v1: LinuxFoundationX+ LFS171x+ 3T2017/course/[Hämtad 2018-04-06] (2018).

[7] Hjálmarsson, Friðrik Þ., et al. "Blockchain-based e-voting system." 2018 IEEE 11th international conference on cloud computing (CLOUD). IEEE, 2018.

[8] Dagher, Gaby G., et al. "Broncovote: Secure voting system using ethereum’s blockchain." (2018)..

[9] Alexander, Jonathan, Steven Landers, and Ben Howerton. "Netvote: A decentralized voting network." Netvote-White-Paper-v7. pdf (2018).

[10] Yli-Huumo, Jesse, et al. "Where is current research on blockchain technology?—a systematic review." PloS one 11.10 (2016): e0163477.

[11] Kshetri, Nir, and Jeffrey Voas. "Blockchain-enabled e-voting." Ieee Software 35.4 (2018): 95-99.

[12] McCorry, Patrick, Siamak F. Shahandashti, and Feng Hao. "A smart contract for boardroom voting with maximum voter privacy." Financial Cryptography and Data Security: 21st International Conference, FC 2017, Sliema, Malta, April 3-7, 2017, Revised Selected Papers 21. Springer International Publishing, 2017.

[13] Singh, Vijander, et al. "Prediction of COVID-19 corona virus pandemic based on time series data using Support Vector Machine." Journal of Discrete Mathematical Sciences and Cryptography 23.8 (2020): 1583-1597.

[14] Bitcoin, Nakamoto S. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[15] Vaishnav, Pragya, Manju Kaushik, and Linesh Raja. "Behavioral biometric authentication on smartphone using keystroke dynamics.".