International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

A Framework to Make Voting System Transparent Using Blockchain Technology

Ms. Rajaprabha.C. E[1], Prem K[2], Prakash Raja P[3], Manikandan M[4]

[1]Department of Computer Science and Engineering, Hindusthan Institute of Technology, Coimbatore
[2,3,4]Department of Computer Science and Engineering, Hindusthan Institute of Technology

Abstract
Generally, governments release schemes or plans like roadways or industries to some area as different projects. During this process, different types of peoples will be there as supportive or opponent for the schemes. In this project, we presented a secure and transparent framework for government schemes using blockchain. Blockchain is used as a secure and immutable data structure to store the government records that are highly susceptible to tampering. Here, we aim to address these issues to build a transparent and secure edge computing infrastructure for the allocation of government schemes which not only eliminates the need for human supervision or intervention but also makes it easy for the government to keep track and update its policies as time progresses. To solve this issue, we propose the framework to use blockchain technology for creating a decentralized system to perform government scheme processes with ease, transparent, auditable, and immutable.
The proposed model consists of a decentralized consortium architecture that combines both the security and privacy of a Permissioned Blockchain and the openness and transparency of a Permission-less Blockchain. The target of the model is to efficiently handle the government tender process securely. The system mainly consists of three types of entities: government officials, citizens and schemes.

Keywords - Blockchain, Blockchain Enabled E-voting, I voting, SHA(256).

INTRODUCTION

1.1 Blockchain

Blockchain seems complicated, and it definitely can be, but its core concept is really quite simple. A blockchain is a type of database. To be able to understand blockchain, it helps to first understand what a database actually is.
A database is a collection of information that is stored electronically on a computer system. Information, or data, in databases is typically structured in table format to allow for easier searching and filtering for specific information. What is the difference between someone using a spreadsheet to store information rather than a database?
Spreadsheets are designed for one person, or a small group of people, to store and access limited amounts of information. In contrast, a database is designed to house significantly larger amounts of information that can be accessed, filtered, and manipulated quickly and easily by any number of users at once.
Large databases achieve this by housing data on servers that are made of powerful computers. These servers can sometimes be built using hundreds or thousands of computers in order to have the

computational power and storage capacity necessary for many users to access the database simultaneously. While a spreadsheet or database may be accessible to any number of people, it is often owned by a business and managed by an appointed individual that has complete control over how it works and the data within it.

1.2 Storage Structure

One key difference between a typical database and a blockchain is the way the data is structured. A blockchain collects information together in groups, also known as blocks, that hold sets of information. Blocks have certain storage capacities and, when filled, are chained onto the previously filled block, forming a chain of data known as the "blockchain." All new information that follows that freshly added block is compiled into a newly formed block that will then also be added to the chain once filled.

A database structures its data into tables whereas a blockchain, like its name implies, structures its data into chunks (blocks) that are chained together. This makes it so that all blockchains are databases but not all databases are blockchains. This system also inherently makes an irreversible timeline of data when implemented in a decentralized nature. When a block is filled it is set in stone and becomes a part of this timeline. Each block in the chain is given an exact timestamp when it is added to the chain.

1.3 Decentralization

For the purpose of understanding blockchain, it is instructive to view it in the context of how it has been implemented by Bitcoin. Like a database, Bitcoin needs a collection of computers to store its blockchain. For Bitcoin, this blockchain is just a specific type of database that stores every Bitcoin transaction ever made. In Bitcoin's case, and unlike most databases, these computers are not all under one roof, and each computer or group of computers is operated by a unique individual or group of individuals.

Imagine that a company owns a server comprised of 10,000 computers with a database holding all of its client's account information. This company has a warehouse containing all of these computers under one roof and has full control of each of these computers and all the information contained within them. Similarly, Bitcoin consists of thousands of computers, but each computer or group of computers that hold its blockchain is in a different geographic location and they are all operated by separate individuals or groups of people. These computers that makeup Bitcoin's network are called nodes.
In this model, Bitcoin's blockchain is used in a decentralized way. However, private, centralized blockchains, where the computers that make up its network are owned and operated by a single entity, do exist.

In a blockchain, each node has a full record of the data that has been stored on the blockchain since its inception. For Bitcoin, the data is the entire history of all Bitcoin transactions. If one node has an error in its data it can use the thousands of other nodes as a reference point to correct itself. This way, no one node within the network can alter information held within it. Because of this, the history of transactions in each block that make up Bitcoin's blockchain is irreversible. If one user tampers with Bitcoin's record of transactions, all other nodes would cross-reference each other and easily pinpoint the node with the incorrect information. This system helps to establish an exact and transparent order of events. For Bitcoin,

this information is a list of transactions, but it also is possible for a blockchain to hold a variety of information like legal contracts, state identifications, or a company's product inventory.

In order to change how that system works, or the information stored within it, a majority of the decentralized network's computing power would need to agree on said changes. This ensures that whatever changes do occur are inthe best interests of the majority.

1.4 Transparency

Because of the decentralized nature of Bitcoin's blockchain, all transactions can be transparently viewed by either having a personal node or by using blockchain explorers that allow anyone to see transactions occurring live. Each node has its own copy of the chain that gets updated as fresh blocks are confirmed and added. This means that if you wanted to, you could track Bitcoin wherever it goes.

For example, exchanges have been hacked in the past where those who held Bitcoin on the exchange lost everything. While the hacker may be entirely anonymous, the Bitcoins that they extracted are easily traceable. If the Bitcoins that were stolen in some of these hacks were to be moved or spent somewhere, it would be known.

Bitcoin vs. Blockchain

The goal of blockchain is to allow digital information to be recorded and distributed, but not edited. Blockchain technology was first outlined in 1991 by Stuart Haber and W. Scott Stornetta, two researchers who wanted to implement a system where document timestamps could not be tampered with. But it wasn't until almost two decades later, with the launch of Bitcoin in January 2009, that blockchain had its first real-world application.

The Bitcoin protocol is built on a blockchain. In a research paper introducing the digital currency, Bitcoin's pseudonymous creator, Satoshi Nakamoto, referred to it as "a new electronic cash system that's fully peer-to-peer, with no trusted third party."

2.Literature survey

2.1 Author:Abhishek Subhash Yadav, Yash Vandesh Urade, Ashish Uttamrao Thombare.
Year: 2020
Title: E-Voting using Blockchain Technology
Methodology: Ethereum network using the blockchain
technology through wallets and the Solidity language.
Advantage: provide the security and
privacy features of a traditional election or have serious usability and scalability issues
Disadvantage: iits require lot more research and currently
might not reach till its full potential. improve its support for more complex applications.

2.2 Author: P. Raghava, P. Uday Kiran, Vimali. J.S
Year: 2020
Title: Trustworthy Electronic Voting using Adjusted Blockchain Technology
Methodology: utilizing the dynamic block chain

approach to hash the utility of algorithms
Advantage: is simple to download, is reliable, easy to manage, highly effective and versatile. reducing or removing human mistakes.
Disadvantage: Blockchain replica, it is much more difficult to restore the blocks. When the Chain becomes high, it is costly process.

2.3 Author: Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan
Year: 2018
Title: Secure Digital Voting System based on Blockchain Technology
Methodology: e-voting scheme along with its implementation using Multichain platform.
Advantage: successfully demonstrates its effectiveness to achieve an end-to-end verifiable e-voting scheme.
Disadvantage: however successful demonstration of such events have been achieve which motivates us to investigate it further.

2.4 Author: GEETANJALI RATHEE, RAZI IQBAL, OMER WAQAR, ALI KASHIF BASHIR
Year: 2021
Title: On the Design and Implementation of a Blockchain Enabled E-Voting Application Within IoT-Oriented Smart Cities
Methodology: secure and transparent e-voting mechanism through IoT devices using Blockchain technology
Advantage: The privacy and security flaws are successfully resolved. Is validated extensively against baseline mechanism by comparing various security parameters.
Disadvantage: The accuracy of proposed mechanism will be further validated and confirmed over real-time data set

3.MODULES

- Candidate
- User(Voter)
- Registration
- Signature Generation
- Voting

CANDIDATE: In this Module the Admin will manage the profile of candidate. First, the admin will collect the details of candidates then the admin will register candidates by filling up the details of candidates. These details will display at the voter site for knowing the details and voting the candidate.

USER (VOTER): User can visit the site, if the user wants to vote registration then voter enters to registration interface and filling up the form from this can make a request to the admin. The request will be goes to Admin. The User has to wait up to verification completed by administrator. After Verification

has done, by user interface voter login using their username and password and make vote for required candidate on particular election Date.

REGISTRATION: The user should provide their Entire information such as Full name, surname, Email-id, password, Branch, Class, Batch, Contact no, Date of Birth, Roll-no and Gender. User should give student Rollno or unique ID at the time of registration. Admin will verify and maintain the above details in the database.

Signature Generation: In this module, signature is generated for each users. By this signature only, the user can access their data. ECC algorithm is used in this module to generate the signature. Secret key Sk is generated using ECC (Elliptic Curve Cryptography) hashing algorithm. Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization.

VOTING

In this Module the voter can log in into their account by username and password, after login the voter can give vote to candidate if there is an election scheduled on that date. Each Vote is consider as one transaction, and ECDSA is the algorithm used to hash the transaction details. The blockchain is a digital ledger of past transactions. A transaction is an exchange of information between different entities that is broadcasted to the network. The transactions are stored in blocks in chronological order, and every block contains a hash of the previous block creating a chain of blocks. The first block in the chain, called genesis block, is the only block that does not contain the hash of the previous block. That block is almost always hardcoded into the software.

RESULTS

By the admin can know entire details about voter and different candidate details and the results announced by administrator. Calculation of the election results are automatically. The candidate having the highest count will be winner of election.

4.Existing System

• Integrity of the election process will determine the integrity of democracy itself. So the election system must be secure and robust against a variety of fraudulent behaviours, should be transparent and comprehensible that voters and candidates can accept the results of an election.
• But in history, there are examples of elections being manipulated in order to influence their outcome.
• In a voting system, whether electronic or using traditional paper ballots,the system should meet the following criteria: Anonymity, Tamper resistant, Human factors.

4.1 Advantages

• The system is a highly coupled application,flexible one.
• The key focus on providing easy method to add, delete and update propertiesfor administrator.
• The users are also provided user ID and key for online voting. He can do

online voting from anywhere over India.
• Data security and strong authentication feature provided to protect user credentials.
• By the admin can know entire details about voter and different candidate details and the results announced by administrator. Calculation of the election results are automatically

4.2 Disadvantages
• Trust is most important in voting mechanism; trust is not handled efficiently in this existing system.
• The security flaws in the system could be a huge risk, as intruders can enter the system to rig the votes.
• It could not secure a voter's identity, and also required complex computing.
• The system was able to collect votes from users but due to complex computation, upon higher user rate the latency became an issue.
• The identities of the voters became vulnerable. The system could not compute a large amount of data hence it has failed to be implemented at a large scale.

5.Proposed System
• We propose the framework to use blockchain technology for creating a decentralized system to perform government scheme processes with ease,transparent, auditable, and immutable.
• In this proposed framework, we used ECDSA-VM (Elliptic Curve DigitalSignature Algorithm with Vote Mechanism) is proposed to give trust for the users.
• This method is handled by Digital signature, so it cant be modified by intermediate users.
• The proposed model consists of a decentralized consortium architecture that combines both the security and privacy of a Permissioned Blockchain and the openness and transparency of a Permission-less Blockchain.
• The target of the model is to efficiently handle the government tender process securely. The system mainly consists of three types of entities: government officials, citizens and schemesV.

5.1 System Requirements:
Our e-Voting solution will include four main requirements that can be illustrated as shown below:
* **Authentication**: Only people already registered to vote can cast a vote. Our system will not support aregistration process. Registration usually requires verification of certain information and documents to comply with current laws, which could not be done online in a secure mannermanner. Therefore, the system should be able to verify voters' identities against a previously verified database, and then let them vote only once.
*** Anonymity:** The e-Voting system should not allow any links between voters' identities and ballots. The voter has to remain anonymous during and after the
election.
*** Accuracy:** Votes must be accurate; every vote should be counted, and can't be changed, duplicated or removed.
*** Verifiability:** The system should be verifiable tomake sure all votes are counted correctly. Beside the main requirement, our solution supports mobility, flexibility, and efficiency . However, we will limit this paper's discussion to the four main requirements.

CONCLUSION

We have proposed an electronic voting system based on the Blockchain technology. The system is decentralized and does not rely on trust. Any registered voter will have the ability to vote using any device connected to the Internet. The Blockchain will be publicly verifiable and distributed in a way that no one will be able to corrupt it will be addressed in future research papers

REFERENCES

1. Subariah Ibrahim, Maznah Kamat, Mazleena Salleh, and Shah Rizan Abdul Aziz " Secure E-Voting With Blind Signature ", 4th National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia, January 14-15, 2003.
2. Nurzhan Zhumabekuly Aitzhan and Davor Svetinovic, "Security and Privacy in Decentralized Energy Trading through Multi-Signatures, Blockchain and Anonymous Messaging Streams " ,IEEE Transactions on Dependable andSecure Computing.
3. Ahmed Ben Ayed, "A CONCEPTUAL SECURE BLOCKCHAIN- BASED ELECTRONIC VOTING SYSTEM ", International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, May 2017.
4. C. Meter and A. Schneider and M. Mauve, "Tor is not enough: Coercion in Remote Electronic Voting Systems. arXiv preprint. (2017).
5. SAGAR SHAH QAISH KANCHWALA HUAIQIAN MI, "Block Chain Voting System ", https://www.economist.com/sites/default/files/northeastern.pdf
6. Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson,
   Mohammad Hamdaqa, "Blockchain-Based E-Voting System ", 11th International Conference on Cloud Computing 2018, IEEE.
7. Rifa Hanifatunnisa and Budi Rahardjo , "Blockchain Based E-Voting Recording System Design "IEEE.