Blockchain based electronic voting system

Goutam Hukeri

Abstract

Modern elections are conducted using electronic voting machines (EVMs), which record each voter's ballot in a single database. And then, looking into numerous various voting systems, it was discovered that the majority of them utilize centralized data storage as their database. Since the entire data is stored in one place, these centralized databases are easily hackable and susceptible to manipulation. As a result, the data used to count the votes may be inconsistent and hence give us the wrong outcome.

Therefore, by utilizing blockchain technology, we are able to construct a decentralized application where data tampering is virtually impossible because blockchain technology employs a decentralized mechanism to store data at a single location.

Using blockchain technology, the primary goal of the e-voting system is to provide a foundation for an e-voting system.

Similar to a traditional voting system, this one allows voters to cast their ballots using a mobile device and a web browser, exactly as they would have done with a paper ballot in the past. In order to better understand how blockchain technology will be employed in the E-voting system, this paper will provide an overview of the technology.

Keywords: Bitcoin, Distributed ledger technology (DLT), Distributed application, Digital signature, hashing, Merkle tree, Time stamp, Data tampering

1. Introduction

Building safe E-voting system is a challenging task. Online voting was presented by the US Pentagon in 2005, but it did not work effectively because the votes were not legitimate. Therefore, we can integrate blockchain technology used in an electronic voting system to create a system that is less hackable and in which data cannot be tampered with. Blockchain is a new method of decentralized data storage that will have many uses in the future.

1.1 Blockchain

In all sectors, blockchain technology is becoming crucial. Blockchain is a distributed, decentralized ledger technology that keeps track of a digital asset's provenance. Distributed ledger technology (DLT), often known as blockchain, employs cryptographic hashing and decentralization to make any digital asset. transparent.

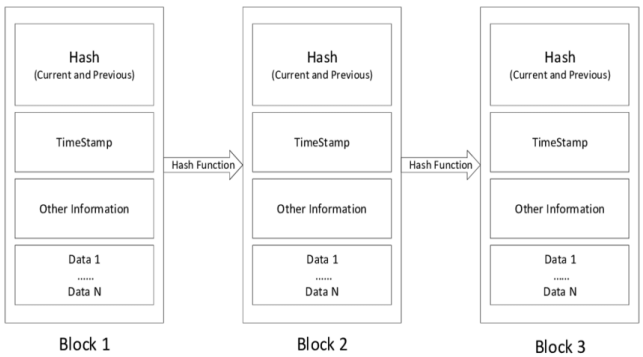
Google Doc is a simple way to teach blockchain technology. A document will be distributed when it is made and made available to numerous as opposed to being copied, persons and transferred. As a result, a decentralized distributed chain is created that may give everyone access simultaneously. Everyone will be able to see all modifications that are made because they are all recorded in real time and no one will have to wait for the other party to make changes. A Google Doc is simpler than blockchain, yet the idea is the same.

As it eliminates fraud, lowers risk, and increases transparency in a scalable manner, blockchain is seen as a promising technology. Blockchain features an extensive database that keeps track of an expanding number of records of data that are protected from manipulation. Decentralization prevents a solitary point of failure, which can happen. within centralized systems. Like the name suggests, a blockchain is a chain of interconnected blocks, each of which is connected to the next via encryption. Two keys for cryptography a private key and a public key make up a blockchain.

These secrets enable two parties to conduct successful transactions. The two keys are assigned hey serve as a secure identity reference specific to each person. This identity is used to control transactions and is known as a digital signature. Each block includes transaction information, a timestamp, and the previous block's cryptographic hash value. Blockchain controls a peer-to-peer network that facilitates node communication and fresh block validation in order to use distributed ledger.

The arrangement of blockchain is shown in

Figure 1: Blockchain Arrangement



Blocks: Every chain, as depicted in figure 1, is made up of several blocks. A transaction is stored in each block and is encoded into a Markle tree after being hashed. Every block has a cryptographic hash of the one before it, and the links between the blocks resemble a chain. Each block contains a time stamp, a digital signature, as well as other relevant information. It should be noted that the block does not include any information regarding the identities of specific users.

This block is sent over the network, and the transaction is successful when the right user uses his private key to match the block with the key in the block. The three basic parts of a block are the data in it, the hash, which is a 32-bit whole number. Blockchain technology uses hash encryption, namely the SHA256 algorithm, to secure data. When a block is constructed, a random nonce will be produced. The hash must begin with a large number of zeroes because it is quite tiny. When the initial block is created, a nonce generates the cryptographic hash.

Miners: Miners carry out the mining process by adding new blocks to the chain. Each block in the blockchain contains a distinct nonce and hash. but it also makes reference to the chain's prior block's hash. As a result, mining a block might be difficult, especially on long chains. Finding nonce that generate hash is a challenging arithmetic problem that requires specialized software to accomplish. Since the nonce is just 32 bits long and the hash is 256 bits, it takes almost 4 billion iterations to find the proper combination. All network nodes accept a change when a block is successfully mined.

Nodes: With blockchain technology, the chain cannot be owned by a single computer. Instead, it is dispersed with the aid of chain-connected nodes. Nodes can be of any type, such as a computer or other electrical device that keeps copies and maintains network functionality.

1.2 Challenges in Voting system

- **Voter privacy:** Only the voter's information and the people they voted for are visible. The number of votes cast in the entire election is the only information that has been made public.
- **Absence of evidence:** There is no proof that bribery or other forms of fraud are being used to influence the votes being cast.
- **Scalable:** Voting processes must be adaptable enough to operate on a big scale as well.
- **Speed:** The election result must be announced within a few hours of the procedure's conclusion.
- **Low cost:** When designing a system, cost is one of the main considerations. The system needs to be economical.

1.3 E-Voting using blockchain

Almost every industry has embraced blockchain but voting is one of the most relevant. Blockchain-based electronic voting has the following benefits.

- Open and distributed ledgers' increased transparency.
- Transparency of distributed and open ledgers.
- Security and dependability (particularly in the face of Denial-of-Service assaults)
- Strong integrity for both the voting process and individual votes, or immutability

Voting data is disseminated via blockchain to hundreds of computers, making it difficult to change or annul votes after they have been cast. By safeguarding personal information, this technique encourages increased confidence between citizens and governments.[8] Blockchain will make it possible for everyone to vote by smartphone or computer via apps, eliminating the need for lines at polling places. A government's current platform can be remodeled rather than changed in order to implement blockchain technology. The primary drawback a balance transfer between two parties can be recorded in a short text string, and blockchain can process this. The majority of the infrastructure required for the storing of blockchain material, however, is provided by the Interplanetary File System (IPFS), which offers a persistent decentralized web.

2. LITERATURE SURVEY

This section introduces research conducted by a few researchers. A review article on blockchain technology for the advancement of the future was proposed by Quoc Khanh Nguyen and Quang Vang Dang. By outlining many areas for more research,

This article provides an overview of Blockchain the potential of technology to advance the Three distinct things are referred to by the term "bitcoin," including the blockchain platform, the digital currency, and the protocol that governs how transactions are carried out. The distributed ledger is organized into two primary network types in this paper's description of blockchain, including permission-less networks like bitcoin, which anyone may join without prior authorization. The permissioned network, which is a private network only accessible to a select group of trusted entities that obtained permission to join the network in to ensure that transactions are genuine, is where participants the transaction can be validated by this type, and may participate in consensus and block building. Ethereum consortium blockchain is a blockchain service that Microsoft has launched. Development of the future. This essay examined how the fourth industrial revolution, in which robots totally replace people in the workforce, will affect society. This paper discusses how blockchain technology works in general. Blockchain technology is a peer-to-peer decentralized ledger that offers a way to store and share information publicly on peer-to-peer computer systems through crypto protocol.

This research paper also discusses the benefits of blockchain, including its decentralization, which makes it less vulnerable to assault, and its ability to execute short insurance requests that can be evaluated quickly utilizing AI. It outlines the relevance of blockchain for the fourth industrial revolution and for society. Blockchain can speed up insurance and payment processes, ease travel by enabling travel insurance providers to automate payments, which saves a ton of time, and safeguard corporate identities in the banking and internet sectors. Supply chain management, security, less bureaucracy, improved safety and openness in government operations, and many more. A review paper titled "Blockchain Technology: Overview of Bitcoin and Future Insights" was proposed by Hussein Hellani, Abed Ellatif Samhat, Maroun Chamoun, Hussein El Ghor, and Ahmed Serhrouchni. This essay examines the blockchain technology that makes it possible for digital currencies like bitcoin to exist. The requirements and advantages for security, databases, and networks are also highlighted in this study. This research paper explains how Bitcoin works as an electronic and cash peer-to-peer system

Three distinct things are referred to by the term "bitcoin," including the blockchain platform, the digital currency, and the protocol that governs how transactions are carried out. The distributed ledger is organized into two primary network types in this paper's description of blockchain, including permission-less networks like bitcoin, which anyone may join without prior authorization. Participants of this kind can validate transactions and take part in consensus and block building on the permissioned network, a private network that is only open to a small number of reliable organizations that have been granted access to join the network in order to validate transactions. Ethereum consortium blockchain is a blockchain service that Microsoft has launched.

Figure 2: Distributed Ledger Technology

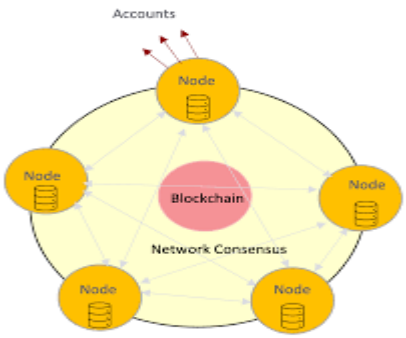


Figure 2. depicts the topology of a distributed ledger, where distributed ledgers are used to increase security and productivity in enterprises, particularly those that deal with unidentified or new clients. An example of a distributed ledger is a blockchain, which consists of immutable Records are timestamped by hashing them into a continuous chain of hash-based proof-of-work, digitally storing data in blocks of transactions, and validating them using a consensus method based on the distributed ledger's live data. review article on the design of an electronic voting recording system based on blockchain by Rifa Hanifatunnisa and Budi Rahardjo. The blockchain technology that is utilized to record the results of every election is discussed in this study. This paper makes the case that using blockchain technology is one way to lessen voting-related issues. Because blockchain is timestamped, programmable, and highly available, this article demonstrates its uses. In this study, a blockchain-based database recording method for electronic voting was proposed.

Figure 3: Flow Chart Design

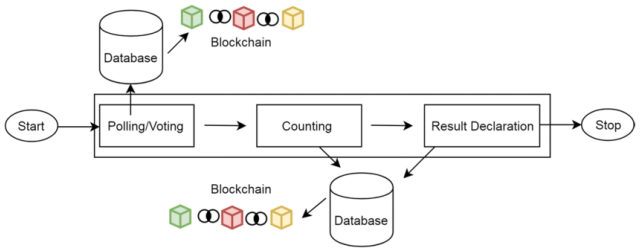


Figure 3 shows they presented a technique in which the process begins after each node's vote is over in their recommended flow chart for blockchain technology. A public key and a private key are generated by each node before voting starts. Each node's public key was distributed to all other nodes, enabling each node to have a list of all the other nodes' public keys. The data will be uploaded to the block's database as soon as it is determined to be authentic. To verify whether the node ID that was brought as a token has actually been updated, the node will query the database. A review paper was suggested by Ahmed Ben Ayed. A hypothetical computerized voting system built on the blockchain. They proposed an electronic voting system with four key requirements: authentication, which allows voters who have already registered to do so; anonymity, which forbids any connection between voter identities and ballots; accuracy, which requires that each vote be distinct and counted; and verifiability, which calls for system verification to ensure that all votes are correctly counted. Along with providing for all of these essential demands, it also provides options that boost productivity, adaptability, and mobility. In the proposed approach, a unique transaction that replaces the candidate will be the first to be added to the block.

The base node, in contrast to the other transactions, will only include the name of the candidate and will not be tallied as a vote. Every time a vote is cast, the blockchain is updated with the results. The voter's data from before you will be added to the block in order to verify that the system is operating correctly. Since each block is connected to the others, it would be easy to identify which block is malfunctioning. The user sends their vote to the candidate's node, which then logs it on the Blockchain. To achieve decentralization, the voting system will feature a node in every electoral district. This method's assumption that voters will cast their ballots through a secure device is its main flaw. Despite the safety of this procedure, malicious software that has already been placed on a voter's device could allow hackers to cast or alter ballots. The inability to reverse a vote in the event of an error is one of the system's shortcomings. A single vote may be cast by the user.

3. DISPLAY OF THE E-VOTING SYSTEM

Because the decentralized process used by blockchain technology prevents data from being kept in a single location, we may design decentralized applications where data manipulation is virtually impossible. Consequently, to create an application that is We employed blockchain technology in the voting application to create a system that is less hackable and in which data cannot be altered. The operation of the e-voting system is shown in

Figure 4. Creating the environment for blockchain technology: Due to the wide variety of blockchain frameworks, creating the environment requires research.

- Ethereum, Multichain, Hyperledger, and other frameworks are among them. The blockchain environment in this project will be built using the Ethereum foundation. Ethereum offers a comprehensive blockchain implementation removing the need for the laborious process of setting up a whole blockchain and freeing developers to focus more on developing applications. Install NodeJS on the PC by downloading the setup file from the website.

- The Ethereum framework's development environment is provided by NodeJS, a JavaScript framework. Install the fundamental packages and files now.

- Creating a smart contract for a blockchain-based ledger that stores data blocks for an electronic voting system. Multiple transactions are contained in each block of data. Before these transactions are put to the blockchain ledger's blocks, the smart contract first verifies them. Transactions cannot be added to the block if they have not been verified. Solidity was used to write the smart contract. A method to determine if a smart contract is error-free is offered by the Remix platform. The remix smart contract is being tested.

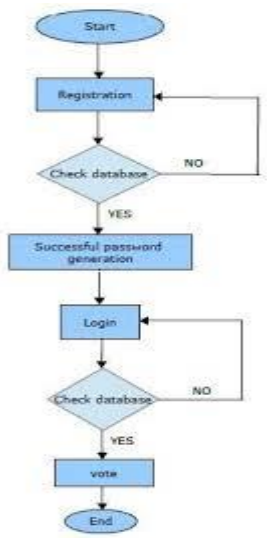
- Using ReactJS and Firebase for authentication, the interface for the two modules manager and voter was created.

- Creating a user interface (UI) for the management, where elections may be formed by adding new parties and their members, as well as a UI to display the election's outcomes. The UI for both modules' authentication is made using ReactJS. The voter and manager databases are stored on Firebase, a NoSQL database.

- An interface has been developed for the voter and manager modules. The management module will have features for including members' names and parties' total vote count in order to display results in app

The voter module's UI just includes the names of the parties and a voting option because it is used for voting. Every time a voter casts a ballot, a transaction is created that requires confirmation. After confirmation, the vote is added and tallied.

Figure 4: How to implement an electronic voting system:



3.1 Technology used for E-voting

- Metamask: With the help of Metamask users can view the scattered web of the present in their browser. Additionally, it lets you operate Ethereum in your browser without the need to run an entire Ethereum node. It provides a secure identification block and an interface for managing identities across several websites and signing blockchain transactions.

- NodeJS: For networking and server-side applications, NodeJS is an open-source, cross-platform environment. JavaScript is used to develop NodeJS applications, which may be used with Linux, OS X, and Windows. It also provides several JavaScript modules, which simplifies the process of building web apps with NodeJS.

- ReactJS: An array of reusable user interface components is made possible by a JavaScript package known as ReactJS. It generates UI components.

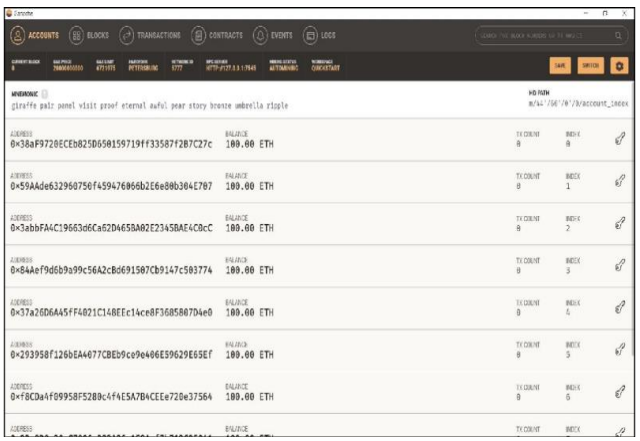
This may display data that evolves with time. The V in MVC is usually represented by React. React offers a faster and easier-to-understand programming model. React may be built on the server using Node, and native apps can be charged using React Native. React implements one-way reactive data flow, which is easier to grasp and requires less boilerplate than traditional data binding.

4. IMPLEMENTATION & RESULTS

(i) Setting up:

Launching Ganache is the first step towards running local blockchain.

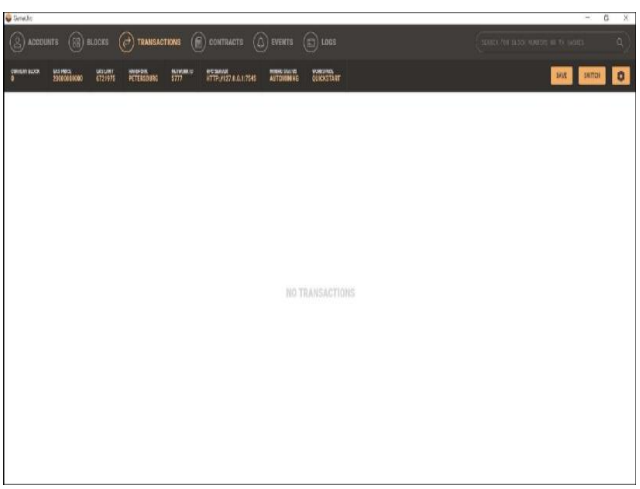
Figure 5: Configuring Ganache



(ii) No Transaction:

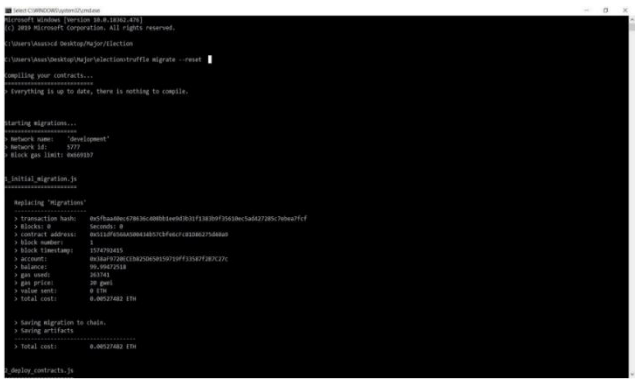
Since we haven't completed any transactions yet, there won't be any after putting up Ganache. The image below shows that there isn't a transaction.

Figure 6: No Transaction



Currently, we are using the truffle framework to issue a command on the command line that transfers the smart contract to the blockchain. Also, we have used the NPM directory with a command. For this, the following commands are being used:

Figure 7: Run the Truffle Framework Command Line.



Using the NPM directory and a cmd, we launch the project after moving the smart contract.

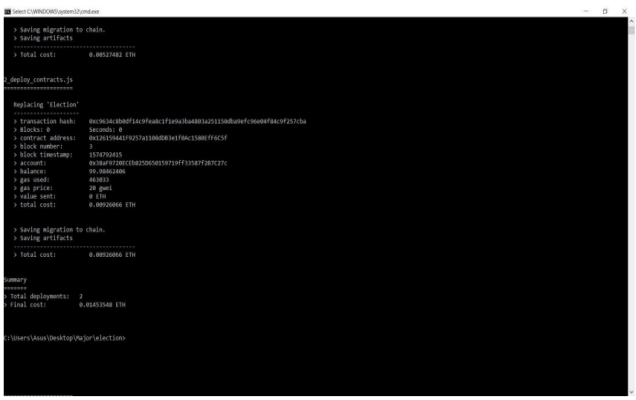


Figure 8: Using the NPM Directory Command Line

(iii) User Interface:

Users communicate with the electronic voting system through the user interface. The user interface appears as shown in the photo below. The screen that loads will stay up until the electorate logs in using Metamask.

Figure 9: Loading Screen

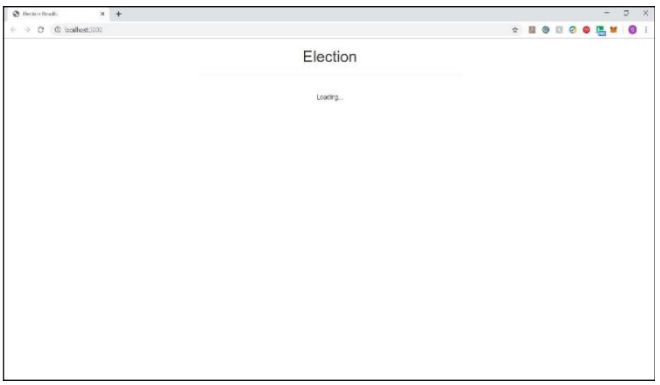
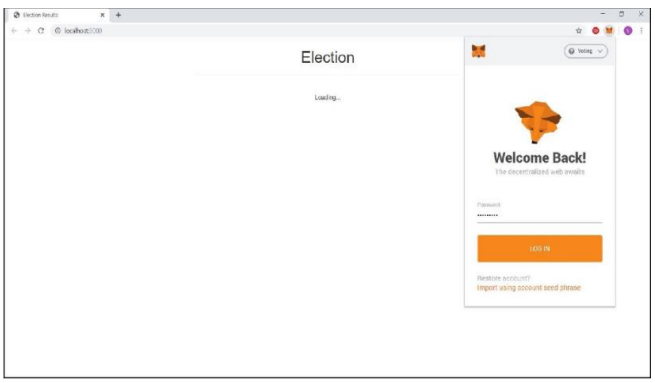
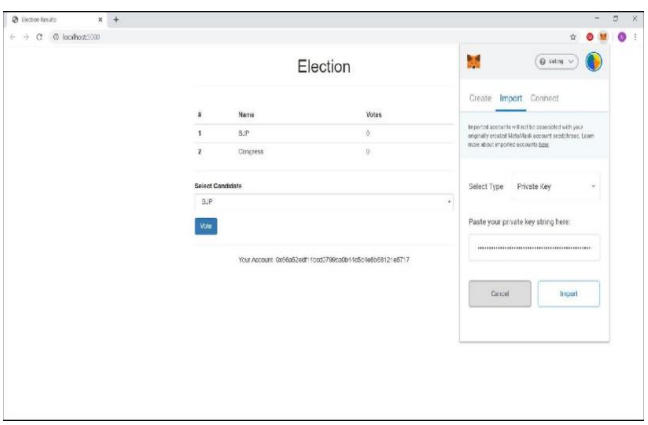


Figure 10: Constituency Registering Through Metamask.



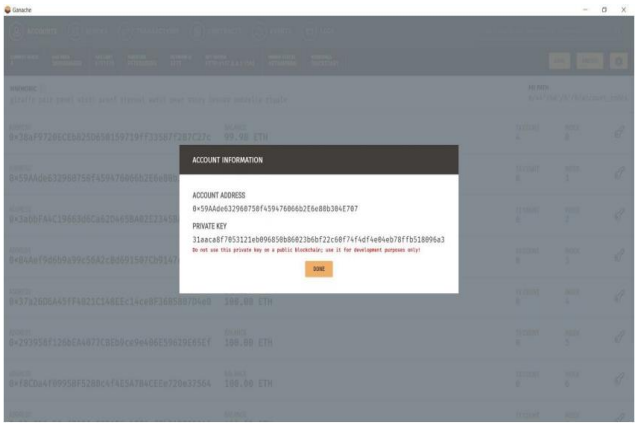
The user cannot vote until they import their account by supplying their private key. The main screen appears blank when the user logs in.

Figure 11: Main Screen



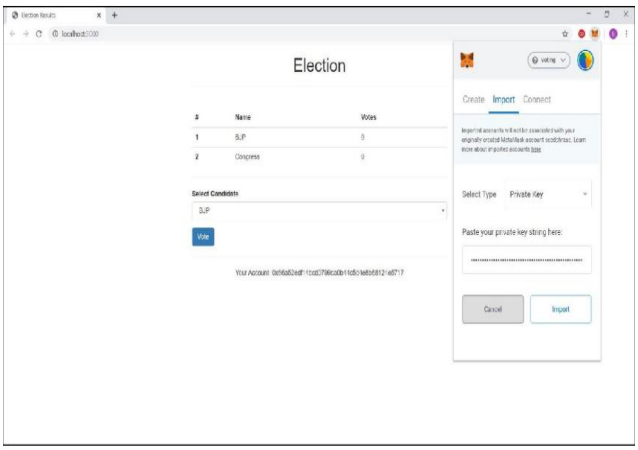
The user receives the private key ahead of time, which will resemble Figure 12.

Figure 12. Private Key



The voter enters the private key above to import their account.

Figure 13. Importing Account



After confirmation, the voter is taken to the main page, where they are unable to vote and can only view the results. Those who import their accounts can also cast a vote in a similar way.

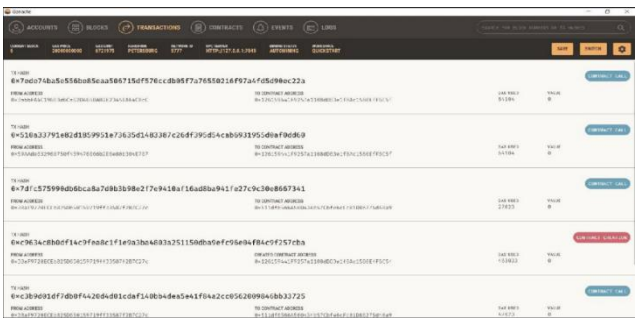
Figure 14. Confirming Transaction

(iv) Checking the transactions

To make it convenient for the user to total their votes, the transaction list will be made public. By examining the transaction list, users can verify the votes they cast. A complete transaction list will like the one shown in Figure 16.

Figure 15. Results on Main Page

Figure 16. Transaction list



5. CONCLUSION

A hybrid system that allows for cases where whitelisted access is necessary but all transactions are public is a permissioned, public, shared blockchain. Transparency is going to be present, which is important in democracies. Even though there are solutions, electronic voting might bring forth new problems, such as protecting anonymity, especially when using public permission-less blockchains. One of the major problems is the potential speed at which the transactions might be validated. The electronic voting system is one area where blockchain technology may eventually make sense, despite the fact that it is regularly hailed as the answer to many problems.

REFERENCES

[1] Quang Vang Dang and Quoc Khanh Nguyen. Fourth International Conference on Green Technology and Sustainable Development (GTSD), January 2018, **"Blockchain Technology for the Advancement of the Future"**

[2] Ahmed Serhrouchni, Maroun Chamoun, Hussein El Ghor, Hussein Hellani, and Abed Ellatif Samhat. The 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET) featured a paper titled **"On Blockchain Technology: Overview of Bitcoin and Future Insights."**

[3] Budi Rahardjo and Rifa Hanifatunnisa**. A review article on the design of an electronic voting system based on blockchain** was presented at the 2017 11th International Conference on Telecommunication Systems, Services, and Applications (TSSA).

[4] Sahil K. Aggarwal, Sai Krishna Kothuri, Sahil Gupta, Kanika Garg, Pavi Saraswat, and Sachin Bisht. 4th International Conference on Internet of Things: Smart Innovation and Usages, 2019. **A Comparative Analysis on E-Voting System Using Blockchain.**

[5] Ahmed Ben Ayed. **International Journal of Network Security & Its Applications (IJNSA)**, Vol. 9, No. 3, May 2017. A CONCEPTUAL SECURE BLOCKCHAIN- BASED ELECTRONIC VOTING SYSTEM.

[6] S. Nakamoto 2008, www.Bitcoin.Org, p. 9, **"Bitcoin: A Peer-to-Peer Electronic Cash System."**

[7] B. Witzoee and A. G. Malvik. Bitcoin Applications of the **Elliptic Curve Digital Signature Algorithm in Bitcoin**, pp. 1–5, 2016.

[8] Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang3. **An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,** IEEE 6th International Congress on Big Data, 2018

[9] Gunnlaugur K. Hreidarsson and Fridrik P. Hjalmarsson. **E-Voting System Based on Blockchain**, 2018.

[10] David Khoury, Ali Kassem, Elie F. Kfoury, and Hamza Harb. IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), 2018. **Decentralized Voting Platform Based on Ethereum Blockchain**.

[11] Julija Golosova and Andrejs Romanovs. **The Benefits and Drawbacks of Blockchain Technology,** DOI 978-1-7281-1999-1/18, 2018.

[12] C. Brake, T. Perry, and A. Barnes. **Using blockchain technology for digital voting,** Team Plymouth Pioneers at Plymouth University, 2