Ethereum based electronic voting system

#1Gaanam Shireesha ,#2Dr. K Santhi Sree

#1Master of Technology, #2 Professor

Department of computer science,

JNTUH School of Information Technology

Hyderabad, Telangana, INDIA,500085

ABSTRACT

Voting is the fundamental characteristics of every democratic country. E-Voting or electronic voting is a means for the election process to be conducted without the use of traditional paper ballots. An election, which takes place in the form of voting, is a process that involves members in mutual competition. Voting is the activity of choosing someone or something in an election. Blockchain technology is providing various opportunities for developing the new and existing digital services by providing the blockchain characteristics such as immutability, integrity, transparency, anonymity, etc. Blockchain is distributed ledger technology which provides decentralization. Electronic voting system using blockchain services provides the security, transparency. The working of blockchain will ensure the votes are maintained and the systems are not rigged by any third party. Every vote that is casted will be considered as an individual transaction. These votes will be counted and the voting results and winner of the election will be announced.

Keywords: *blockchain, decentralization, smart contracts, transactions, e voting.*

1.INTRODUCTION

Blockchain is a distributed ledger technology (DLT). Blockchain is a distributed data structure for storing and to maintain integrity, consistency of data. As it is distributed there is no need for a central authority to approve or complete the operations on this peer-to-peer based system [1].

Blockchain is chain of blocks. A block is a container data structure which contains a set of confirmed transactions. A block could contain different information, and a chain of these blocks evolves into a blockchain as long as it links one and other. The blocks are stored on the hard drives of many miners spread across the globe on a peer-to-peer network. The initial block in a blockchain is known as the 'Genesis block' or 'Block 0' [2]. Each block in the blockchain mainly consists of the hash value, data and previous block hash value. Hash of the block used for identifying the block among the chain of blocks. This hash value is generated based on the data of the block. Hash value is an alphanumeric fixed length of data and generated using cryptographic hash algorithm generally the secure hash algorithm is used. Previous hash value in the block used to maintain the chain among the blocks in the network.

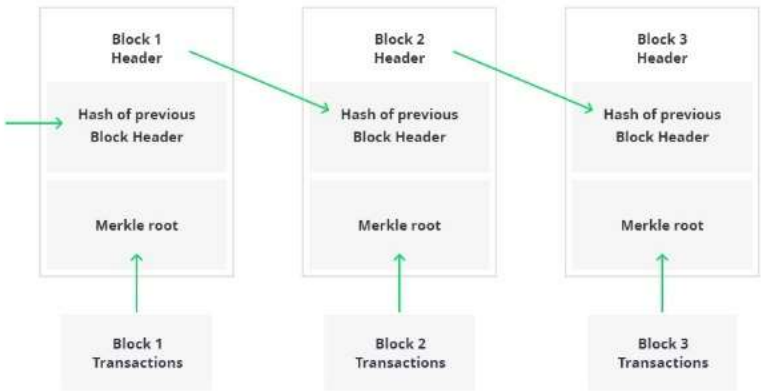

Figure 1. Structure of blockchain

All blocks in the Blockchain are composed of header, identifiers and long list of transactions. The block header contains metadata about a block. There are three different sets of metadata. The previous block hash, Mining competition for the network, Merkle tree root. Merkle tree root is a data structure to summarise the transactions inside the block. The user can verify whether or not a transaction is included in a block. Merkle trees are created be repeatedly hashing pairs of nodes until there is only one hash left which is called root hash. Each leaf node is a hash of transactional data, and each non leaf node is a hash of its previous hashes.

Merkle trees are binary and therefore require an even number of leaf nodes. In a single detail in any of the transactions or the order of the transaction's changes, so does the Merkle root.

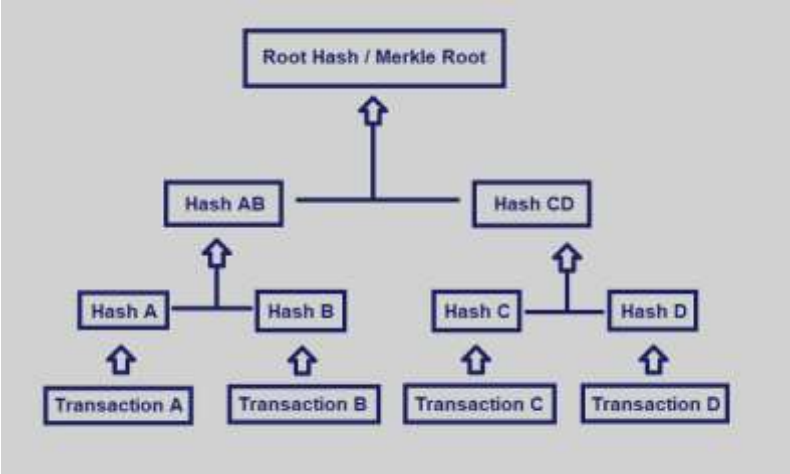

Figure 2. Merkle tree

Transactions are records of data in chronological order. Transactions are stored in Merkle tree inside the block. The transactions when submitted, are picked up by the blockchain network and is inserted into a pool of unconfirmed transactions. The transaction pool is a collection of all the transactions on that network that have not been confirmed yet. Miners on the network select transactions from this pool and add them to their 'block.' Transactions also contain metadata information which can be utilized to store data over the blockchain.

Electronic voting (e-voting) is one of the emerging applications of blockchain whereby researchers aim to leverage benefits such as integrity, anonymity and non- repudiation which are critical for a voting application.

2.LITERATURE REVIEW

There are lot of different practices are made to introduce the variations in electronic and online voting systems where different techniques and methodologies are used. Some of them guarantees the confidentiality and security to the system at some extent, still the voting information and process need to be control and manage with advanced systems that will ensures and guarantees the security and privacy of voter's and voter's information. A basic blockchain framework consists of distributed ledger, cryptography, consensus protocol, and smart contracts. Government agencies around the world are looking for opportunities related to the adoption of blockchain technology in the public sector (Deloitte Development LLC, 2017; Chiang et al., 2018), particularly for utilising the secure, distributed, open, and inexpensive database technology to reduce cost and bureaucracy, increase efficiency and for authenticating many types of persistent documents. Other blockchain applications in the public sector may include document verification, e-residency approaches (Sullivan and Burger, 2017) the development of more reliable and transparent taxation mechanisms, the development of more robust regulatory compliance frameworks and land management [3].

Governments throughout years are entrusted with managing and holding official records of both citizens and/or enterprises. Blockchain-enabled applications might change the way governments at local or state level operate by disintermediating transactions and record keeping. Blockchain governance aims at providing the same services that are offered by the state and its corresponding public authorities in a decentralised and efficient way while maintaining the same validity. Examples of such services include registration or legal documents, attestation, identification, marriage contracts, taxes and voting.

There are different blockchain development frameworks available. It is very important to choose the platform that is suitable for developing the problem statement. Blockchain started as open source, and there are many platforms available free to use. Some of the major platforms are Bitcoin, Ethereum, Multichain, Hyperledger, Corda, Quorum, BigChainDB, Stellar etc [4]. There are various examples of applications being built upon Blockchain, some of the major applications are Cryptpad- a decentralized document creation application, Humaniq – A fintech start-up which connects unbanked people with global economy, Angur – a peer to peer oracle and prediction market place, Filament – building the IOT applications over the blockchain.

2.1 Basic E-voting approach

The systems that are developed to caste the vote by means of digital approach using online portals and electronic devices use various encryption and decryption techniques to guarantee the secure data transaction. Existing electronic voting systems rely on proprietary and centralised design by a single entity, characteristics that harm the trust and confidence voters have to the voting process.

Electronic Ballot: Electronic voting systems may use electronic ballot to store votes in computer memory. When electronic ballots are used there is no risk of exhausting the supply of ballots. Additionally, these electronic ballots remove the need for printing of paper ballots, a significant cost.

3. PROPOSED DESIGN

In this paper I am implementing blockchain based electronic voting system. Using permissionless public blockchain services this application is developed and deployed on to the blockchain. The user can access this electronic voting system by registering the details into the system and cast the vote if there is any election period is specified.

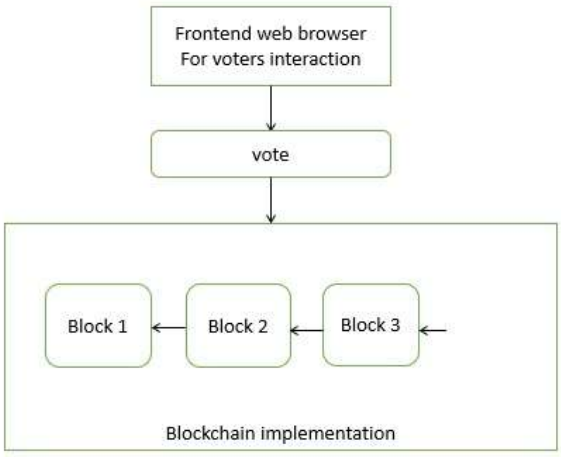

Figure 3. System architecture

In the first step of development environment setup is done for building decentralized applications. Installing all dependencies for developing the application that are meta mask, ganache, truffle suite, node js, npm. Meta mask brings Ethereum to the web browser.

In the second step of development writing smart contracts for the election. Smart contracts are lines of code or business logic that are stored on a blockchain and executed automatically when prescribed terms and conditions are accepted. At the most basic level, they are programs that run as they have been set up to run by the people who developed them. Solidity programming language is used for writing the smart contracts on Ethereum platform. Election contract involves adding the candidates who are participating in the election and voting function of the election.

After creating the server-side application, I have created client-side application that will interact with our smart contracts. Created our front-end with java script, CSS and HTML. To make our system more secure we have included one significant feature other than unique id and password is the email verification feature. System requests users to enter their email on which verification mail is send and then the system verifies the user. After creating the webpage, we need to log in to the blockchain.

To connect to blockchain we need to import one of the accounts from ganache- One of the dependencies which gives us 10 accounts with account address and some fake ethers, into MetaMask. To interact with the smart contracts that are deployed on the blockchain web 3 provider is used for integration of user interface and smart contracts.

Ethereum network provides a framework for blockchain creation and storage. Every block is created and its details are stored in an encrypted ledger. These created blocks are distributed among nodes which provides high fault tolerance to the system.

Finally, the processing and tallying of votes is done in results phase. Results are generated and displayed on website. Users can verify their votes using their own public key. This provides transparency to the voting system.

4. RESULTS AND DISCUSSION

User interface design for electronic voting system provides friendly interaction with the blockchain. Figure 4 represents the front design for voting system which includes the information about the web application of voting system that is about, results of voting, contact information etc,. Sign up is used for registration of the new user. Admin in this system adds the candidates of the election. After completion of voting winners will be announced.

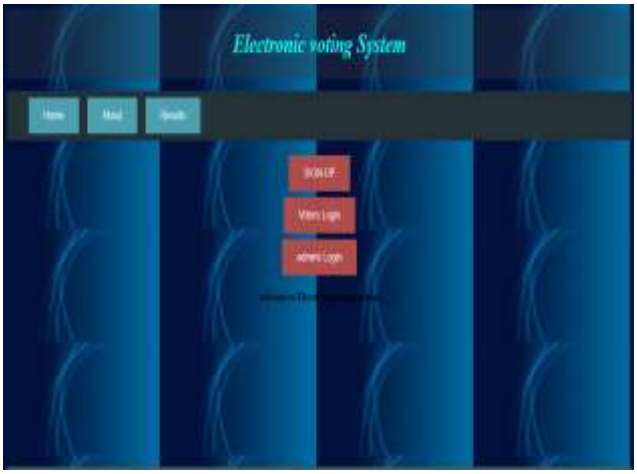

Figure 4. election system home page

Figure 5 represents the registration page for new user. This page takes the input from the user and the user enters the data into the page. This page validates the user details and takes the unique email and Aadhar number from the users. These details are stored in the database. On successful registration user can login into the system by providing respective details and caste the vote.

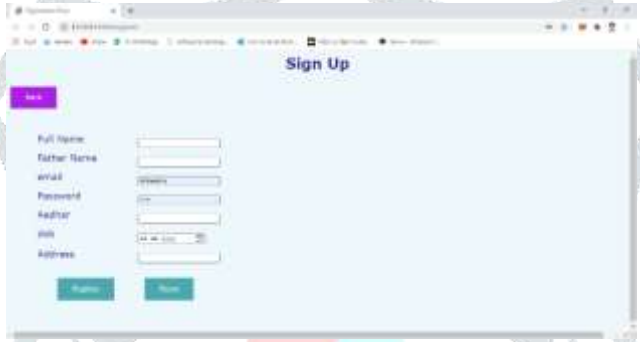

Figure 5. user registration page

To run this project truffle IDE used. Truffle is a command line application used for compiling and deploying the smart contracts on the blockchain. The following picture represents compiling of smart contracts using command prompt.

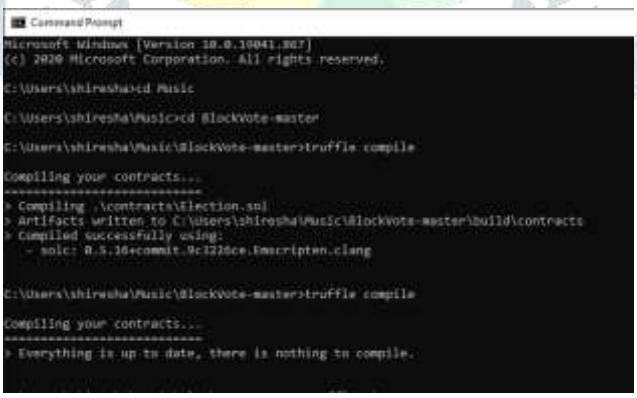

Figure 6. compiling contracts

On successful compilation of smart contracts, deploying the contracts on the blockchain using truffle migrate command. Figure 7 represents deployed contracts along with gas value and with different parameters .

Figure 7. Deploying the contracts

After deploying the contracts run the server to interact with the voting system. After running the server it redirects to homepage (fig.4). Connect the metamask to the website. By selecting the account from the metamask the voter can caste their vote to the candidate. The below figure 8 represents voting page for the voter.

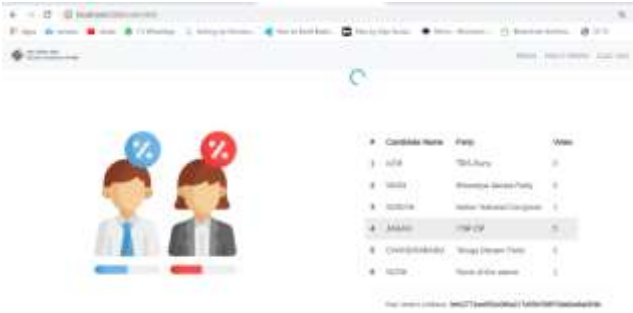

Figure 8. voting page

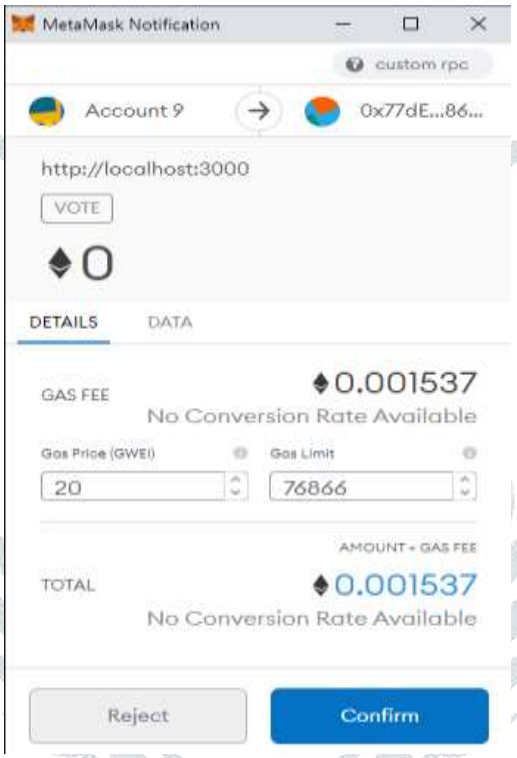

Figure 9. vote confirmation using metamask

After the vote is confirmed, a new transaction is created and added to the blockchain. Below figure 10 represents the transactions added into the blockchain. Successful completion of casting vote we can also recheck our vote to whom the vote is casted using the public address of the account from which vote is casted.

Figure 10. transactions in the blockchain

5.CONCLUSION

Democracies depend on trusted elections and citizens should trust the election system for a strong democracy. However traditional paper-based elections do not provide trustworthiness. Generally voting has to be perform by voter by going to the polling booth. Many voters like army NRI cannot come to the voting place. The advantage of transforming digital or online electronic voting systems is to make the public electoral process not too expensive, faster and uncomplicated. With the extraordinary growth in the use of blockchain technologies, a number of initiatives have been made to explore the feasibility of using blockchain to aid an

effective solution to electronic voting. A blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient election while guaranteeing voters privacy. Blockchain based e-voting provides integrity for the votes. The main reason for selecting blockchain as a service provider for voting system is it provides features like anonymity, transparency, security and immutability. As a future work, the researchers may try to investigate the blockchain based tools and techniques more deeply and develop this blockchain voting system into large scale use for best voting schemes.

6. REFERENCES

[1]. .Bitcoin.org (2009) Bitcoin Developer Guide. Available at:https://developer.bitcoin.org/devguide/block_chain.html#block-chain-overview

[2] Genesis block (2015) Available at: https://en.bitcoin.it/wiki/Genesis_block Genesis block - Bitcoin Wiki

[3]. Fran Casino, Thomas K. Dasaklis, Constantinos Patsakis, A systematic literature review of blockchain-based applications: Current status, classification and open issues,Telematics and Informatics,Volume 36,2019

[4]. Macrinici, D., Cartofeanu, C., Gao, S., Smart Contract Applications within Blockchain Technology: A Systematic Mapping Study, Telematics and Informatics (2018)

[5]. Yu, Bin, et al. "Platform-independent secure blockchain-based voting system." International Conference on Information Security. Springer, Cham, 2018.

[6]. Decentralized Computing Using Blockchain Technologies and Smart Contracts edited by Asharaf, S., Adarsh, S.

[7]. Digital Voting with the use of Blockchain Technology Team Plymouth Pioneers – Plymouth University Andrew Barnes, Christopher Brake and Thomas Perry

[8]. Metamask

[9]. Ethereum.org