

A Research Paper on E-Voting Using Blockchain Technology

TANIKELLA SAI CHARAN¹, SRINANDA PENTAPATI², Mrs. R. PREMA³

¹B.E Graduate(IV year), Department of Computer Science and Engineering, SCSVMV, Kanchipuram

²B.E Graduate(IV year), Department of Computer Science and Engineering, SCSVMV, Kanchipuram

³Assistant Professor, Department of Computer Science and Engineering, SCSVMV, Kanchipuram

Abstract – An electronic voting system that uses blockchain technology completes the stage of establishing a secure and transparent environment for decisions where voters will actually want to vote only once and the vote will not be interrupted. The operation of the block chain will ensure that the votes are kept in line with them and that the situation is not deceived by any outsider. Protected electronic voting structures use a block chain which is a separate, distributed and tracking transaction record that follows peer-to-peer transactions. Each vote given will be considered a role as one job. These votes will be counted and the results will be reported immediately. Voting is a very important and important event organized in all countries by secret ballot or by ballot. Such processes have many drawbacks such as vote disruption, low turnout and so on. To overcome all this, we will introduce a series of voting programs.

Key Words: BLOCKCHAIN, E-VOTING, VOTES, BALLOT.

1. INTRODUCTION

Extensive research has been done on electronic democratic structures that give voters the ability to vote whenever they need to use a mobile phone, PC or other electronic gadget. Block is a variety of transactions. The Block chain has significant features such as Permanent Resistance, Downsizing, Security, Direct Progress and Nameless. A strong blockchain emerges as a promising rival for building a highly secure, secure and direct E voting framework. Block chains have become an important new feature in the short term. Therefore, voting using a block chain can be considered the safest way.

An online voting framework is a democratic framework in which any citizen can exercise his or her democratic rights anywhere in the country. Various sectors such as innovation, social media and political decision-making organization are identified by disputes regarding voting on the web. Electronic voting is ready to change the normal voting system, which is less complicated and more open to voters. This is legal if the web produces a voting form because democratic structures can be displayed on any PC with a web connection. These tactics reduce the cost of many laws to some voters by creating more ways in which they can produce a voting form. There's a chance to kill long lines at review stations and offer better reception for people who are mentally ill, experiencing illness, serving in the military or living abroad as well as those

who are away from close rides and others who feel hard to see. upward channel. Additionally, posting a voting form on the web can cover the cost of voters' great opportunity to make the voting form at any time. Young people between the ages of 18 and 30 are special voters and the web is a process to attract those citizens who seem to be the hardest to reach.

1.1 Actual Architecture of E- Voting

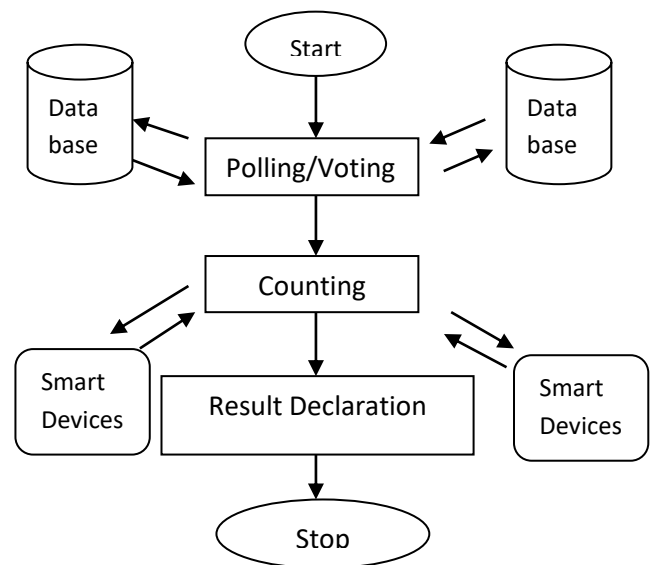


Fig 1. Actual Architecture of E-Voting

1.2 Literature Survey

We did a lot of research before starting our project which included a lot of research papers published under various books. During the detailed reference for the literature research, we came across some words that include:

- Truffle • Ethereum and ethers • Web3.js • Metamask
- Ganache

Truffle

Truffle is a tool that makes it easy for designers to build blockchain-based applications with respect to Ethereum. It allows designers to build and test solid contracts and create public and private organizations that use regional languages such as JavaScript. A remarkable and attractive feature about Truffle is its command line tool. We can use a variety of important commands, for example, assemble, move, repair, etc. The control center is a quick and easy way to connect with the blockchain.

Ethereum and Ethers

Ethereum is an open source platform based on blockchain innovation standards. The main advantage of Ethereum is that it allows developers to assemble and submit fixed applications. Ethereum assists designers by performing tasks based on their needs, and this means that developers can build many different applications. Ethereum uses nodes to replace individual cloud compounds and servers demanded by essential Internet services. These nodes are managed by volunteers. The idea is for these nodes to associate with each other into a "global PC." This will help to provide a framework for people all over the world. The glorified Ethereum model is the only one that will not help itself against hacking and closure, as no feature will have authority over your personal information. Ether is the sender of a computer service as collateral or bond and is a solution to the installment issue. Ether acts as a currency as it does not require an outsider to support or manage the transaction. However, Ether is not really a digital currency. It is often considered a fuel for Ethereum organization applications.

Web3.js

Web3.js is a visual interface for the Program with a large JavaScript library, which allows developers to accept their smart contracts. Depending on the complexity of the Divided Applications application, a designer may incorporate complex conclusions by designing Java-driven dynamic projects or even familiarize themselves with their Dedicated application experience with Python-coded intelligence-related projects. This is linked to our nationally distributed blockchain application with a conference called JSON RPC. One can no doubt connect with everything directly in the order line by performing a Web3 even.

Metamask

MetaMask is a simple crypto wallet. MetaMask can assist designers in testing and evaluating dApp transactions. MetaMask successfully collaborates with a local blockchain operating engine engine. Inside your Truffle console, duplicate your localhost hole, and paste it into a custom RPC accessible for system extension. Records can be successfully imported from Truffle to MetaMask.

MetaMask has been an amazing and well-known commitment to the Ethereum biology system. Developers can undoubtedly switch between blockchains. In the event that the client visits dApp, MetaMask acts as a blockchain mediator. The MetaMask GUI is also very easy to use. It consistently connects the client with the blockchain. MetaMask notifies the client to support the exchange. This and other exchanges are a fee that a client may pay in other cryptographic fees to associate with a blockchain

MetaMask has been an incredible and well known commitment to the Ethereum biological system. Developers can undoubtedly switch between blockchains. At the point when a client visits a dApp, MetaMask goes about as a mediator of the blockchain. MetaMask's GUI is likewise extremely easy to use. It associates a client to the blockchain consistently. MetaMask prompts a client to support an exchange. This exchange is here and there just a charge a client may pay in some cryptographic money to associate with the blockchain

Ganache

Ethereum smart contracts are programs executed inside the setting of exchanges on the Ethereum blockchain.

Ethereum Ganache frames part of the Truffle Suite, a bunch of engineer devices that permits clients to reproduce blockchain conditions locally and test savvy contracts. Ethereum Ganache is a neighborhood in-memory blockchain intended for improvement and testing.

2. BLOCKCHAIN FOR E-VOTING

Blockchain is another new, growing trend for a large segment of businesses. Blockchain was first proposed for cryptocurrency (Nakamoto, 2008). The smart part of a streaming blockchain network does not have a fixed data set. Blockchain data is updated in all hubs in the subject building. The three components of a blockchain are segregation, transparency, and consistency. All transactions are placed in blocks. When a block is checked by peer notes, at that point, it is removed from the blockchain. Each block contains a summary of tasks. Blocks are organized with a sequential application, permission, to record a board frame, which allows people to share data reliably. It is a secure site, where it is blocked by the entire organization, not just one client.

Table -1: Types of block chain

S.No	Type	Description
1	Public Blockchain	Open Block chain
2	Private Blockchain	Centralized (Multichain)
3	Consortium	Managed by group of individuals

4	Hybrid	Same as private, but strict.
---	--------	------------------------------

The Blockchain was originally named from the square and the chain, a complete trading list called a blockchain, associated with the cryptography strategy. Each square connected above the previous block. Blockchain is a scattered information base and is managed by a peer-to-peer organization. Used for storing and accessing information. Each square contains a square head and a trade. The square header corresponds to the title Hash of block block, time stamp, nonce, and Merkle root esteem. The health information posted in the forum cannot be changed. An important use of blockchain is to stay away from distractions. Blockchain is a standard trading record. Allows some people in circles to transfer information to various providers without meeting with outsiders and checking for exchanges. Perhaps instead of storing the record on a single server, it is stored on different laptops, making data no doubt difficult to edit or delete. Those well-designed brand name tags around the process that ensures any data embedded in the blockchain are important and strengthens trust among collectors

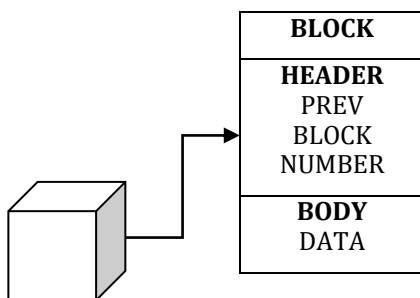


Fig 2. A Block in block chain

2.1 Properties of Blockchain

The key structures of the block chain are distribution, transparency, consistency, independence, open source, anonymity and consistency.

- Blockchain as a data structure: Blockchain contains a list of functions and sets it as a block. The design starts with a single block called the first block. As part of the exchange increase, more blocks were added. The previous block was connected to the current block. The blockchain provides this type of information structure. The blockchain is usually designed to be carefully designed and uncluttered.
- Decentralized: Shared Organization; framework collection makes it seem like a fragmentation and one of the key features of an amazing blockchain development. Anyone can store the app and, later, access the app via the web without the need for external support. Keep any exchanges such as securities, records, contracts, computer asset.etc, and

in the future access the exchange with the help of a secret key.

- Consistency: Consistency is the way in which a blockchain framework can allow and trust trading before they add to the chain. Work violates one of the agreed terms, at which point the exchange will appear to be invalid. The chains of the block are passed on to a show-based show, which may be a small permit or authorization. The community agreement stipulates that anyone can try to combine trade and have an interest in the agreement. In license-based shows, nodes must be authorized and monitored in order to contribute to or facilitate exchanges in the series.

3. E-Voting using block chain

Blockchain is becoming an important new feature, with many different operating cases. While distributed applications, for example, text sharing has been around since the days the Web became the foundation of our lives, their use in secure and consistent trading goes back to 2008. Since then, with the rise of Bitcoin, individuals and organizations have become increasingly aware of the benefits that blockchain innovation offers.

One of the newest but most inspiring blockchain applications is in the voting booth. In the normal course of events, email voting will eventually become standard. Electronic voting will improve the political race process by making it faster, more straightforward, and less expensive while increasing the number of voters and supporting compulsory voter support systems. Like many experts in this field, electronic voting requires advanced security measures, which can only be provided by blockchain technology with its own distribution environment where the voter cannot interfere with his or her vote.

The main advantages of a blockchain voting system are:

- Transparency
- Security
- Anonymity
- Processing time

4. METHODOLOGY

While carrying out a blockchain empowered electronic democratic framework we consider existing and past e casting a ballot framework. Different cycles of characterizing jobs assessing structures, security and lawful issues ought to be considered. We have called the system designed as EVOTE and it will always be so mentioned throughout the paper. It aims to provide a real-time online application that can be used to vote on selection of any size. It will aim to work not only voting processes that take place in organizations but also in them

villages, suburbs and elections at the national level. Also, we have tried to keep the application as simple as possible in order can work on older systems like the ones on it villages.

In our electoral system we have defined the election as a smart contract. So in our network the choice is agreement between participating nodes. And the wise a defined contract includes defining each role participant, election process and terms and conditions during the election process.

Every participant must be defined for a specific role. Most people can be given the same role either a different role.

a) Administrators

Administrators will oversee all operations of election. They can be given creative tasks the election is valid, see the votes that determine the time period close selection and calculation and disclosure of results.

b) Voters

A voter is a primary participant who cast a vote in an election. A voter can verify his or her eligibility and self-certification and upload election votes .They can vote and confirm the vote they cast.

c) Constituency Nodes

Administrators make the election process smarter contracts use appropriate constituency nodes representing each region. These nodes authenticate voters through smart contracts. If a voter is present verified by all constituency nodes and then the voters' vote will be processed and added to blockchain.

4.1 Election as a smart contract

In our political decision framework we have characterized a political decision as a shrewd agreement. So in our organization the political decision is the arrangement between the participating nodes. When the smart contract is characterized it incorporates characterizing the jobs of every member, cycle of political decision and terms and conditions inside the election process.

4.2 Election Process

The voting process is done by the arrangement of smart contracts gets that are empowered into the blockchain. The smart contracts are characterized appropriately as for jobs characterized to the members in the organization. The administrators has the ability to commence the election, add the candidates, verify the registered candidates and end the elections. Administrators can also create the voting ballots by means of decentralized applications. An admin can also define the candidates and

voting constituencies. The smart contract creates the ballot and deploys into the blockchain.

This voting process is consisted of multiple procedures in it. The voter can also register through the registration tab with the help of private key that will be generated at the administrator server.

With the help of that private key, the voter enables the gas transaction through metamask platform and register himself. For verification of every voter, the admin has to spend the gas in other words, ethers. Verification is done with respect to the voter id and name that is provided at the time of pre registration.

When an individual voter casts his/her vote, they interact with the secret ballot.

The smart contract interacts with the blockchain and if the code is matching, then the vote is added. A voter once casted a vote, has no permission to cast another vote. This is because, the private key generated will work only once per individual.

Once the election is ended, the announcement of the winner is very crucial. Since the whole process is carried out digitally, the number of votes casted to an individual is counted automatically and the administrator ends the polling. Now each voter can view the result in the website in their systems.

4.3 Actual Architecture of project

Admin will create a voting instance by launching/deploying the system in a blockchain network (EVM), then create an election instance and start the election with the details of the election filled in (including candidates for voters to vote).

Then the likely voters connect to the same blockchain network register to become a voter. Once the users successfully register, their respective details are sent/displayed in the admins' panel (i.e. verification page).

The admin then will check if the registration information (blockchain account address, name, and phone number) is valid and matches with his record. If yes, then the admin approves the registered user making them eligible to take part and cast their respective vote in the election.

The registered user (voter) following the approval from the admin casts their vote to the candidate of interest (from the voting page).

After some time, depending on the scale of the election the admin ends the election. As that happens the voting is closed and the results are displayed announcing the winner at the top of the results page.

Here is the outline of the working process of our project in the form of architecture. We are also going to attach the screenshots of the working website to make it clear for the viewers of this paper.

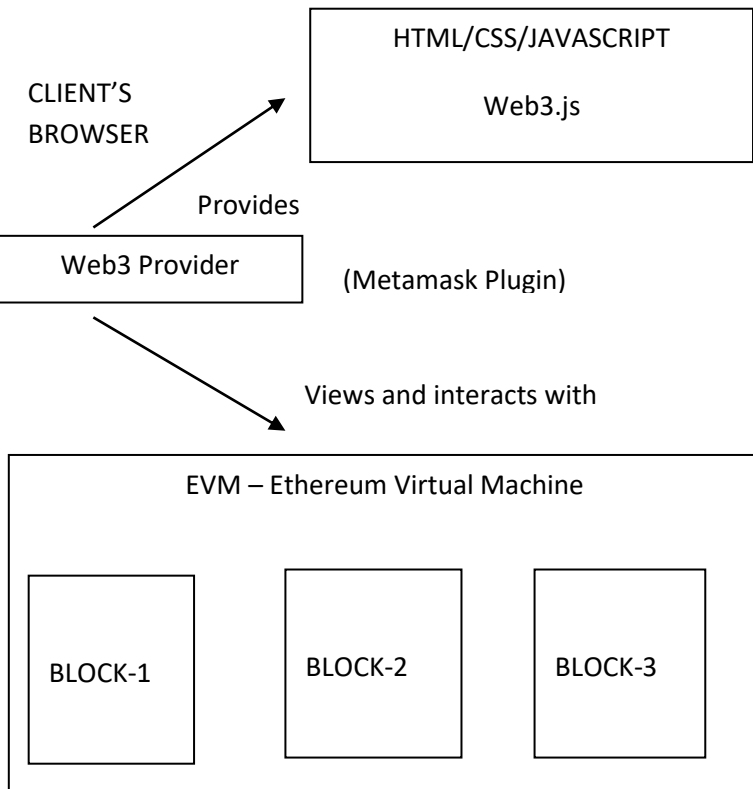


Fig3. ACTUAL ARCHITECTURE OF PROJECT

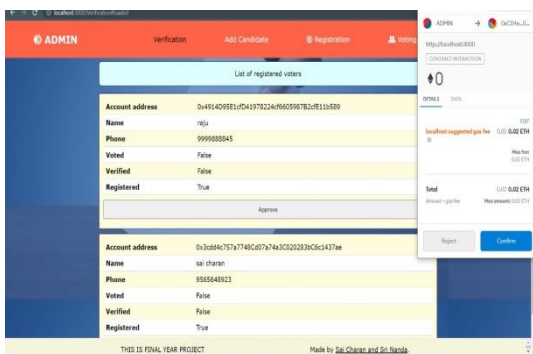


Fig4 (Admin's view of the platform)

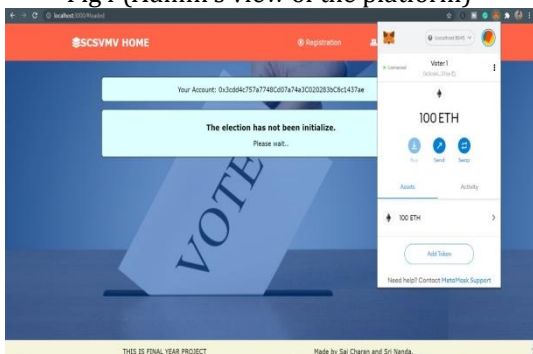


Fig5 (Voter's view of the platform)

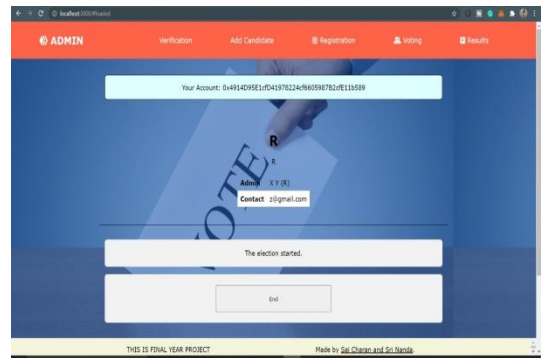


Fig6 (Admin commencing election)

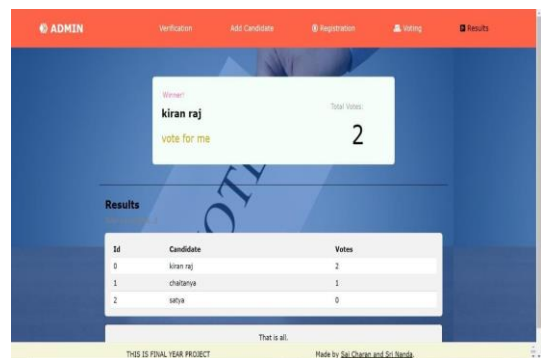


Fig7 (End of election and results displayed)

6. CONCLUSION

At this point, toward the finish of this paper, we can infer that we have gone over many exploration papers connected with electronic democratic framework utilizing block chain innovation and eventually we have discovered that there are multiple ways and ways to deal with fabricate an electronic democratic framework with the assistance of square chain innovation. We have additionally observed that there are different innovations like Ethereum, truffle to know about to achieve our task.

REFERENCES

- [1] Karneedi, Kishan. (2020). E-Voting using Blockchain. 10.13140/RG.2.2.29954.71360
- [2] Jayapal, Cynthia & Sekar, Navin & Sekar, Raghul & Suresh, Rajkumar. (2020). Secured Voting Using Blockchain. 10.1109/ICCCA49541.2020.9250859
- [3] Prajapati, Anjali & Reddy, Vandana. (2020). Online Voting System Using Blockchain. 10.1007/978-981-15-5397-4_67.
- [4] Febriyanto, Erick & Triyono, & Rahayu, Nina & Pangaribuan, Kelvin & Sunarya, Po. (2020). Using Blockchain Data Security Management for E-Voting Systems 1-4. 10.1109/CITSM50537.2020.9268847

- [5] Somya Sharma, Vibhor Garg, Shubham Kumar, Research Paper Guide - Ritin Behl, Po (2020). Voting System using Blockchain.

BIOGRAPHIES

“TANIKELLA SAI CHARAN, pursuing fourth year in bachelor’s degree in Computer Science and engineering department in SCSVMV University, Kanchipuram”



“SRINANDA PENTAPATI, pursuing fourth year in bachelor’s degree in Computer Science and engineering department in SCSVMV University, Kanchipuram”

“Mrs. R. PREMA, Assistant Professor in the Department of Computer Science and Engineering, SCSVMV University, Kanchipuram.”