

# Vote Block - A Digital Ledger

Rishabh Sah, Purav Rathod, Pratik Rane, Anuj Yadav, Lifna C. S.

<sup>1,2</sup>Department of Computer Engineering, Vivekanand Education Society's Institute of Technology

## Publication Info

### Article history:

Received : 12 February 2020

Accepted : 24 May 2020

### Keywords:

Blockchain, Digital Ledger, Voting System, Electronic Voting Machine (EVM)

### \*Corresponding author:

Lifna.C.S

e-mail: lifna.cs@ves.ac.in

## Abstract

Fundamental right to vote or voting in elections forms the basis for democracy. Elections is the process for people to choose their representatives and express their preferences for how they are governed. In all earlier elections of India, a voter casts his/her vote using the ballot paper. This is very much prone to errors and time-consuming because of the EVMs, all the condensed materials like the ballot papers, ballot boxes and stamping are completely replaced into a simple box called ballot unit. The objective of our project is to create a Digital Ledger using Blockchain Technology for Elections. The Digital Ledger will help in keeping the list of all the voters and each and every voter will be able to vote. The Digital Ledger will automatically count the vote and complete the transaction. The digital ledger will make the voting process simple, efficient and faster compared to the current EVM system. Current EVM is bulky, less efficient and tampering issues with the existing system. Election Process takes too much time and money, which can be saved using our system. Voters need to stand in long queues which wastes time and productivity.

## 1. INTRODUCTION

The objective of this paper is to improve the election process by constructing a digital ledger through blockchain. All the eligible voter lists and single vote per person rule can be easily possible using a digital ledger. Votes can be automatically counted, and the process will be simple, faster, and efficient than current EVMs. Blockchain is originally used for generating distributed databases initially developed for a cryptocurrency (bitcoin). Blockchain makes a record of the transactions made by users using blocks. A secure and robust system for voting is possible through blockchain. To use Ethereum blockchain technology for elections. The digital ledger will help in keeping the list of all the voters, and each voter will be able to vote, and then the digital ledger will automatically count the vote and complete the transaction.

The overall paper is discussed in the following subsections as follows; starting with a discussion on the state-of-art techniques in blockchain followed by the Proposed System Architecture and implementation details

## 2. LITERATURE SURVEY

The basics of blockchain and its cutting edge applications are explained in brief, and the drawbacks of public ledgers and usefulness of a hybrid solution is also explained.[1] A hybrid solution is a peer to peer network, which is encrypted so it cannot be viewed even if it is public. In the study,[2] the authors have used blockchain technology to make a secure electronic voting system. An ID card was used for authentication via an IC (Integrated Circuit) with a pin for secure voting.

A wallet system that is used for voting purposes using blockchain technology. A vote is credited as a coin in the voter's wallet, which is transferred to the candidate once the vote is cast.[3] In paper [4], the authors introduce Secret Voting implemented using Enigma Protocol, which is a decentralized open-source protocol that lets anyone perform computation on encrypted data. Table 1 depicts the comparison of Traditional EVM's with blockchain-based Voting System.

Table 1: Comparison with Existing System

Traditional EVM system	Blockchain-based voting system
The result is slower as compared to blockchain-based voting systems.	The result is faster than a traditional EVM system.
Security issues the voting system, and the results can be tampered or changed.	No security issues present, more secure than the EVM based system. The votes are secure as Ethereum is used to store vote
It has hardware vulnerabilities that can be manipulated.	It doesn't have any hardware vulnerabilities and is durable.
EVM systems don't have any technological potential.	Blockchain-based systems have huge technological potential.

### 3. PROPOSED METHODOLOGY

The main difference between the proposed system and the existing system is the Ethereum Blockchain.[5] That is the system is not using a bitcoin-based blockchain System for the proposed Voting Blockchain deployment. The advantages of opting the blockchain-based Voting System is as follows:

- *More use cases:* Ethereum has many more use cases than Bitcoin does. Not only one can use it as a peer to peer transfer, but one can also use it to create one's own Initial Coin Offering (ICO). The ICO is a fundraising mechanism in which new projects sell their underlying crypto tokens in exchange for bitcoin and ether. It is even used to store data onto the blockchain.
- *Platform for ICO's:* You cannot just create your own cryptocurrency and expect that it would run efficiently. This is especially true if you're looking to do something specific with your cryptocurrency than what is already being done. Cryptocurrencies with open source codes can be copied and started by another company but having the ability to have it on a platform that is already one of the best is hard.
- *Mining to Staking:* Ethereum has said they will be looking to move over from mining to staking which is much more efficient and secure. Mining is the use of specific hardware that is used to confirm transactions on the blockchain. Staking also confirms transactions however it is done keeping your tokens or coins in your wallet.

Fig. 1, illustrates the Ethereum platform, which is used to write a smart contract for voting. The contract is responsible for creating the poll and also conducting the election. When the poll ends, the result is calculated, and the result is displayed. It includes two modules involved in Polling; one is creating the poll while the other is the voting process. Creating a poll includes Adding candidates, Election period, etc. Voting includes login, selecting the candidate, and casting a vote. In the end, the result is displayed.

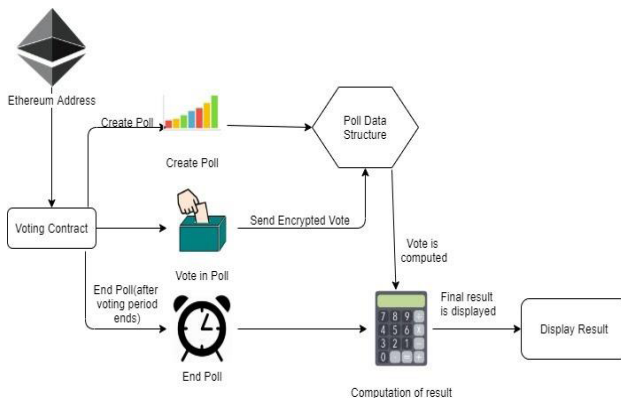


Fig. 1 : Proposed System Architecture for Vote Block

An authentication step is added to it where the user is verified by the biometric or Face ID. This model is for implementation at government body elections. Here a key is generated after login and verification, which is used to cast a vote. After the election period is ended the calculated vote is displayed. The authenticity of the voter is verified and checked if the ethereum address was used previously to cast a vote in the election, then the user is checked if it has cast a vote before.

After verification, the voting is allowed else the user is denied to vote. The user(voters) data and the votes are stored in different databases. The users database is a traditional database while the candidate, votes, and the casting vote are stored in the blockchain in secure and encrypted format. The permitted data can be accessed by a user using the interface. The basic principles of our project for implementation and deployment are:

- *Authentication:* The system will authenticate users from the voter list database, it will also check if the user has previously voted or not and also verify if the ethereum address is previously used for voting or not.
- *Anonymity:* This system will not display or store the users, who have voted for any particular candidate, maintaining the anonymity of the voters.
- *Accuracy:* The votes are counted in real-time, which can be displayed or can be hidden till the poll ends so that it does not affect the trend in voting.
- *Verifiability:* The Ledger is publically visible and can be verified by anyone for the result, but it is immutable so the results cannot be altered.
- Functional Requirements addressed by the Proposed System :
  - Mobile / Web App for Login
  - User Authentication
  - Blockchain to store the votes
  - Smart contracts to count votes
  - Voting history in the database as well as transaction stored in ledger, prevents users from voting again.
  - A feature for admin to create elections and for users to nominate themselves as candidates.

Non-Functional Requirements are as follows:

- Confidentiality of voters data is to be maintained
- Data integrity is essential for better classification.
- User interface should be simple and easy to interpret.
- It should support 24/7 availability.

### 4. IMPLEMENTATION DETAILS

The system was implemented with the following components on both the Server and client-side as follows. Server Side includes:

- *Ethereum Blockchain network* (for deployment) is the Public Blockchain on which the votes are stored

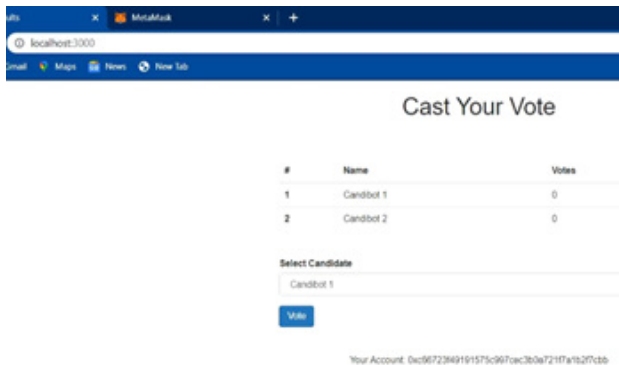


Fig. 2 : GUI for voting

- *Truffle Framework* is used to design the backend of the project
- *Ganache client (for testing)*: It is used in the testing phase to create dummy Ethereum accounts
- *Web3js (Ethereum JS API)*: web3js is a API use to connect the project to blockchain
- *Solidity (Smart Contract)*: Solidity is a language used by Ethereum to write smart contracts

Client-side includes a metamask E-Wallet (network connection). It is like a wallet where user ethers are stored which will be used for voting.

The Ethereum blockchain uses the Ethash algorithm, which uses the hash value of the previous block to store in the next block forming a chain of data blocks. When a new block is added to the chain, the encrypted data in the previous block is hashed and encrypted with the data of the new block and stored. If someone tries to manipulate the data of a block, its hash value changes, and thus we can say that the data is manipulated. Hence we store the votes casted to the candidates in the form of transactions that are used to count the vote.

## 5. RESULTS AND DISCUSSION

Fig. 2, depicts the basic Front End of the Voting App. This depicts the total number of candidates as well as the form of voting. The public address of the voter is also shown at the bottom of the page. After casting a vote we get a popup from the metamask wallet to confirm the gas payment for the voting process.

Fig. 3, shows the amount of gas required. After the payment is confirmed, then the vote is cast. After the confirmation, the payment vote is cast.

Fig. 4: clearly depicts that, there is no option to vote again as the current address is recorded as previously voted, thus multiple voting from a single account is prevented.

## 6. CONCLUSION AND FUTURE SCOPE

We have designed a smart contract for conducting Elections online. This contract is stored on ethereum, which is a

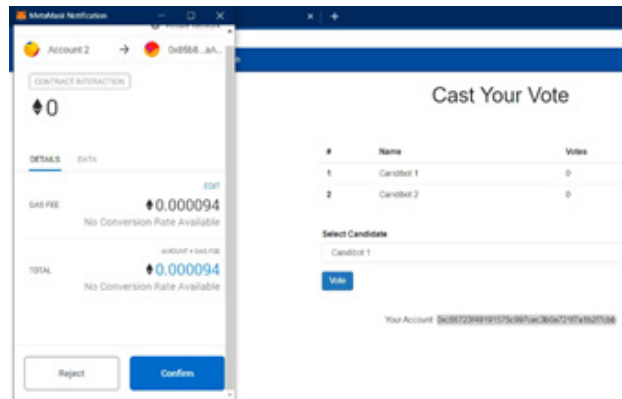


Fig. 3 : Voting In Progress



Fig. 4 : MetaMask Confirmation after Voting complete (User can't vote again with same id)

decentralized platform that uses ethers as currency, which will be charged every time when the user will cast a vote. The blockchain is visible and can be verified by the public. Since the data is stored in the blockchain it cannot be modified, and thus malpractice cannot be done. The authors are planning to extend this paper as follows:

The contract can be modified to conduct multiple elections at a time.

Integration with hardware modules for security like biometric and facial recognition.

Integration with hardware modules for rural areas with less exposure of technology.

User data can be stored securely in the blockchain.

## 7. ACKNOWLEDGEMENT

The authors gratefully acknowledge the support extended by India Innovation Challenge Design Contest (IICDC) for selecting their Project Idea for Semi-Finals with Group-ID 1502413. IICDC is organized by DST & Texas Instruments (TI) Inc. powered by AICTE mission, anchored by NSRCEL@IIMB and supported by MyGov.

## 8. REFERENCES

- [1] Pilkington, Marc. "11 Blockchain technology: principles and

- applications." *Research handbook on digital transformation* 225 (2016). A hybrid solution for a public blockchain.
- [2] Ayed, Ahmed Ben. "A conceptual secure blockchain-based electronic voting system." *International Journal of Network Security & Its Applications* 9.3 (2017): 01-09. An ID card based authentication system.
- [3] Nir Kshetri . " Blockchain-Enabled E-Voting" from University of North Carolina at Greensboro. A wallet based voting system.
- [4] Enigma - "Secret Voting Smart Contract with Enigma: A Walkthrough", Andrew Tam, 15th Aug 2018. A voting app made using Enigma protocol which is an open source protocol for encrypted data computation.
- [5] Ethereum a public blockchain <https://ethereum.org/>