



Decentralized Voting System Using Blockchain

¹Sumit Gupta, ²Hrishikesh Gawde

¹Student, ²Student

¹Department of Information Technology, ²Department of Information Technology

¹Fr. Conceicao Rodrigues College of Engineering, Bandra, Mumbai, India

Abstract : The aim of this project is to build a blockchain based decentralized voting system which is more transparent, accurate, flexible, and secured than the current traditional voting system. The current centralized voting system lacks security and transparency. The current voting system are also prone to various attacks such as DDoS attacks, vote alteration, malware attacks etc. Also, EVM machines used in India have been very questionable in recent times by the opposition parties. Hence using blockchain we can create a voting system which will provide transparency and security. Blockchain based system have a peer-to-peer network for a private blockchain. Each peer has its own private and public keys to ensure strong encryption. Each vote is stored as a transaction in the chain. Hence vote can be back tracked, and voter can use it to ensure whether his vote is counted securely or not. Smart contracts are used further to make the system more efficient. Smart contracts are simple programs in blockchain which run when predetermined conditions are fulfilled. Thus, a blockchain based system will help in reducing the security breaches, human resource, paperwork involved, time, cost of expenditure on elections etc.

Index Terms: Blockchain, Decentralized, Smart Contract, Security

I. INTRODUCTION

India being democratic nation elections are regularly happening in different parts of the country. But organizing elections is not an easy task. It involves lot of human resource, time, cost etc. Elections in India are mostly conducted through EVMs. These EVMs are simple electronic machines which are used to record votes. But these EVMs have been criticized lately for its security breaches and lack of transparency. Opposition parties have been targeting EVMs for vote tampering and manipulation. Hence to overcome these problems we have proposed a blockchain based Decentralized voting system. Blockchain system can be defined as a distributed database which stores the information in a digital format and this information is shared among all the nodes of computer network. In Blockchain, information is stored in the form of blocks. Once the transaction is completed the blocks gets added to the chain with proper encryption. Thus, Blockchain can provide a decentralized architecture to build and run a voting system which is open, fair and independently verifiable. Various advantages of Blockchain based system over EVMs are as follows

- Decentralized control
- Votes are immutable
- No Single point of failure
- Data integrity
- Transparent Environment
- Cost of elections is less
- Less human resource and paperwork involved
- Person can vote anytime/anywhere

II. RELATED WORK

Blockchain system is a decentralized and peer-to-peer network. Initially blockchain was introduced to remove the centralized control role of banks. But nowadays blockchain is used for various purposes such as IOT, healthcare activities, cryptocurrency,

carbon dating etc. As there were lots of problem with current traditional voting system, that's when blockchain was introduced in e-voting system. Blockchain based e-voting was much more secured, transparent, and reliable [2]. The use of Smart Contract increases the degree of security and helps to develop a trust among voters [5]. Although there are lots of advantages of blockchain based system over traditional system but there are various challenges as well such as technical problems, legal issues, various types of attacks, social problems etc. [3]. We have described in this paper about how these challenges can be overcome. Blockchain based e-voting system can be implemented on a small scale as well such as in schools, colleges, offices etc. As elections have always been questionable for fraudulent practices blockchain based can be a perfect solution for a secured and a fair election [8].

IV. PROPOSED SYSTEM

Blockchain based voting system will require several tools to be installed on your computer namely Solidity, Smart Contract, Ganache, Truffle framework. Truffle framework is used to import Smart Contract on the blockchain while Ganache manages the internal operations of blockchain. For each transaction in a blockchain user will need to pay a transaction fee called as gas. Once the voting process is completed all the nodes on a network compete to complete the transaction. During implementation we will be using Ganache instead of nodes. Let's have a look at some of the preliminaries

Solidity

Solidity is a high-level language used for implementing Smart Contracts. Solidity is influenced by C++, Python and JavaScript. It is used to generate machine-level code. It is a primary language for all blockchain based running platforms.

Truffle Framework

Truffle is a popular development tool for Ethereum programmers. It is used for compilation, deploying and linking of smart contract. Truffle is also used for writing unit tests of the functions and design the front-end part of the Decentralized applications.

Ganache

Ganache is used to set up a personal Ethereum Blockchain network. Using Ganache user can interact with the Smart Contract in his own local Blockchain network. Ganache by default sets up with 10 default Ethereum address and pre-loads them with 100 simulated Ether each. These Ether are further used as a transaction fee during voting.

Smart Contract

Smart Contract is a computer program which runs when pre-defined set of conditions are met. Smart Contract executes code the same way as they are written by programmers. It is like traditional contract but in digital format. Smart contracts are written using simple logic such as if-then conditions, if-else, different types of loops and operators etc. Various advantages of Smart Contract are as follows

- Self-executing
- Immutable
- Lower transaction cost
- Greater degree of security
- Less time and Human resource
- Transparent

Now, let's have a look at the workflow

Voter can access voting website from PC/Laptop/Any other device. On voting site, voter is first directed to the Home Page. Home Page includes various type of information such as political parties, Party symbols, list of candidates and election related info. On Homepage we have VOTE button which will start the process of Voting. When voter clicks on the button, voter will be first redirected to the Authentication page. For Authentication we use Aadhar card details for verification. When the voter submits all his details then system goes through the Database of Registered voters. If the voters details match with the database records, then authentication is successfully. Otherwise, we show a Wrong details Error popup and redirect the voter to the Homepage of the site. After successful authentication voter is directed to the main Voting Page. The Voting Page consists of list with all the candidates and their symbols. A Vote button is provided next to each candidate. When voter clicks on the Vote button of the desired candidate a popup appears to confirm the Ethereum transaction. Once the voter confirms the transaction, a small transaction fee called Ether gets deducted from voters account and vote gets submitted for the selected candidate. Also, we have a flag set to check whether user has already voted or not. If user has already voted and tries to vote again, then a failed transaction error popup appears, and vote is not counted.

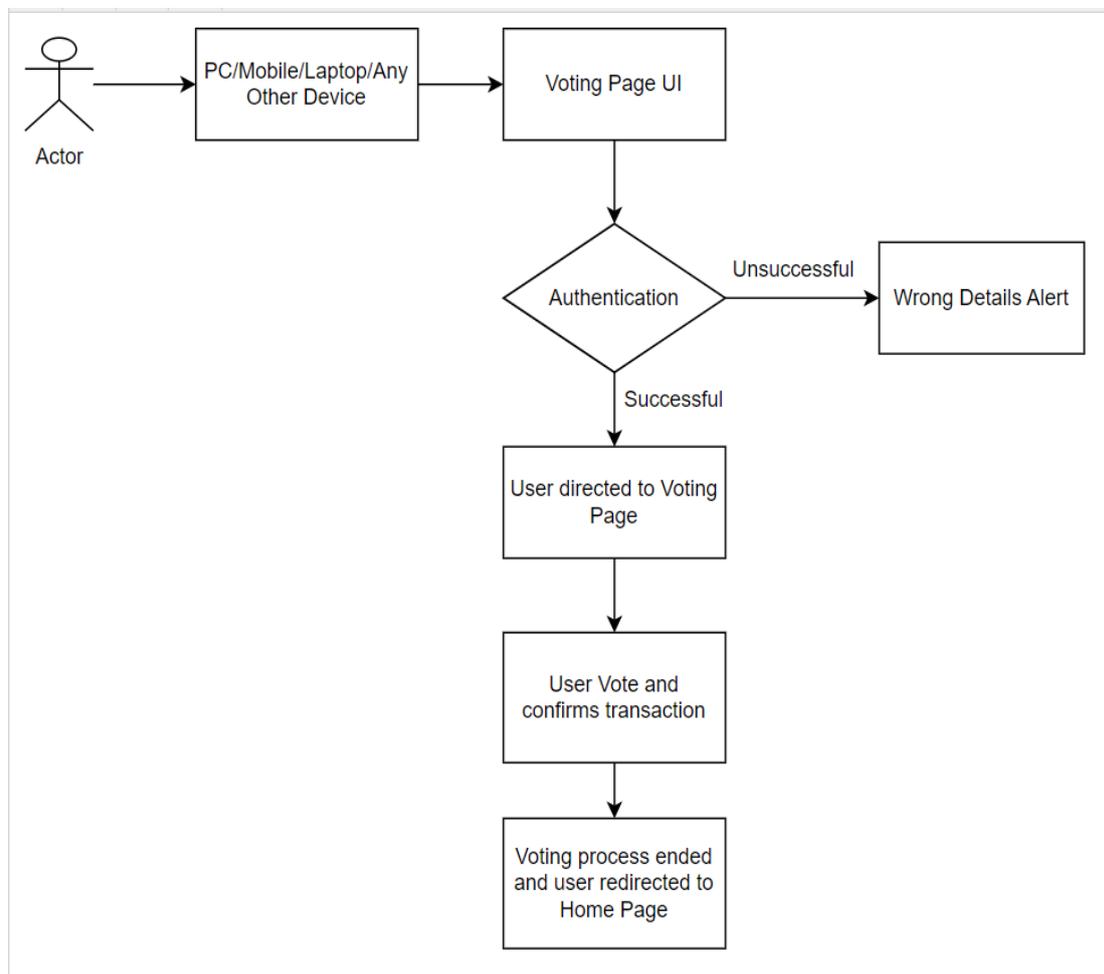


Figure 1: Process Workflow

In the Voting System, Ganache is used to deploy the local Blockchain. Smart Contracts are created on solidity, and we use Truffle framework to migrate this Smart Contract on the local blockchain. When the user votes, transaction fee called Ether is transferred from voters account to the candidate account. During voting only, a specific amount of Ether is distributed to all the voter’s account. Hence if user tries to vote again then transaction won’t be completed as user doesn’t have enough Ether in his account. In this system, transaction goes through all the blocks, and this gives a complete transparency to the voters

V. IMPLEMENTATION

The first job is to install all the preliminary software. A local blockchain is setup by using Ganache. As we can see in below snapshot Ganache displays the Address of all the accounts, Ether left, transaction count etc.

MEMORANDIC	HD PATH
giraffe pair panel visit proof eternal aafu! pear story bronze umbrella ripple	m/44'/50'/0'/0'/0'/account_index
ADDRESS: 0x36aF9720ECEb025D650159719ff33587f2B7C27c BALANCE: 100.00 ETH	TX COUNT: 0 INDEX: 0
ADDRESS: 0x59AAde632960750f459476066b2E6e80b304E707 BALANCE: 100.00 ETH	TX COUNT: 0 INDEX: 1
ADDRESS: 0x3abbFA4C19663d6Ca62D465BA02E2345BAE4C0cC BALANCE: 100.00 ETH	TX COUNT: 0 INDEX: 2
ADDRESS: 0x84Aef9d6b9a99c56A2cBd691507Cb9147c503774 BALANCE: 100.00 ETH	TX COUNT: 0 INDEX: 3
ADDRESS: 0x37a26D6A45FF4021C148Eec14ce8F3605807D4e0 BALANCE: 100.00 ETH	TX COUNT: 0 INDEX: 4
ADDRESS: 0x293958f126b5A4077CBEb9ce9e406E59629E65EF BALANCE: 100.00 ETH	TX COUNT: 0 INDEX: 5
ADDRESS: 0xf8CDe4f09958F5209c4f4E5A7B4CEEe720e37564 BALANCE: 100.00 ETH	TX COUNT: 0 INDEX: 6

Figure 2: Dashboard displays various information such as address, ethers, transaction etc

Truffle framework is now used to transfer the smart contract to a local blockchain using command line. Once the smart contracts are deployed, we start the project using npm directory.

```

Activities Terminal Tue 18:23
tito@tito-Vostro-15-3568: ~
File Edit View Search Terminal Help
eth_uninstallFilter
eth_accounts
eth_sendTransaction
Transaction: 0xf7e9306dcf848df07314a285012a0c5726db3518267c89ac4b5983ebb0dc498
Contract created: 0xdae13f70aed6956cd7ac721c01a585163678e32f
Gas usage: 375326
Block Number: 3
Block Time: Tue Apr 23 2019 18:17:56 GMT+0530 (IST)

eth_newBlockFilter
eth_getFilterChanges
eth_getTransactionReceipt
eth_getCode
eth_uninstallFilter
eth_accounts
eth_sendTransaction
Transaction: 0xa2137e4d2014d4a997519693acd09cde5ad9401e22d59dbfc02acbee7ef085b8
Contract created: 0x6e96e357d0fcd6b384e53a2077cbf9b5de8859bd
Gas usage: 375518
Block Number: 4
Block Time: Tue Apr 23 2019 18:18:13 GMT+0530 (IST)

eth_newBlockFilter
eth_getFilterChanges
eth_getTransactionReceipt
eth_getCode
eth_uninstallFilter
eth_accounts
eth_sendTransaction
Transaction: 0x69558a8ab5be47a9a5b1ac8e9ea518350f9c77c2644198a3f06d16b4d854024
Gas usage: 21720
Block Number: 5
Block Time: Tue Apr 23 2019 18:21:00 GMT+0530 (IST)

```

Figure 3: Various commands used to deploy and run smart contract

User Interface

Let's have a look at the UI of Voting System. When voter visits the voting page he will first need to submit the required details. We use the Aadhar No for authentication. Once user submits its details system will verify and if details are correct the voter will be redirected to Voting Page. Once the authentication is successful, the Smart Contract gets prompted for the ongoing election. On the Voting Page, user is presented with the ballot box which has a list of candidates a voter can choose from. Once the user votes and completes the transaction, a function in the smart contract adds one vote to the party which he voted for.

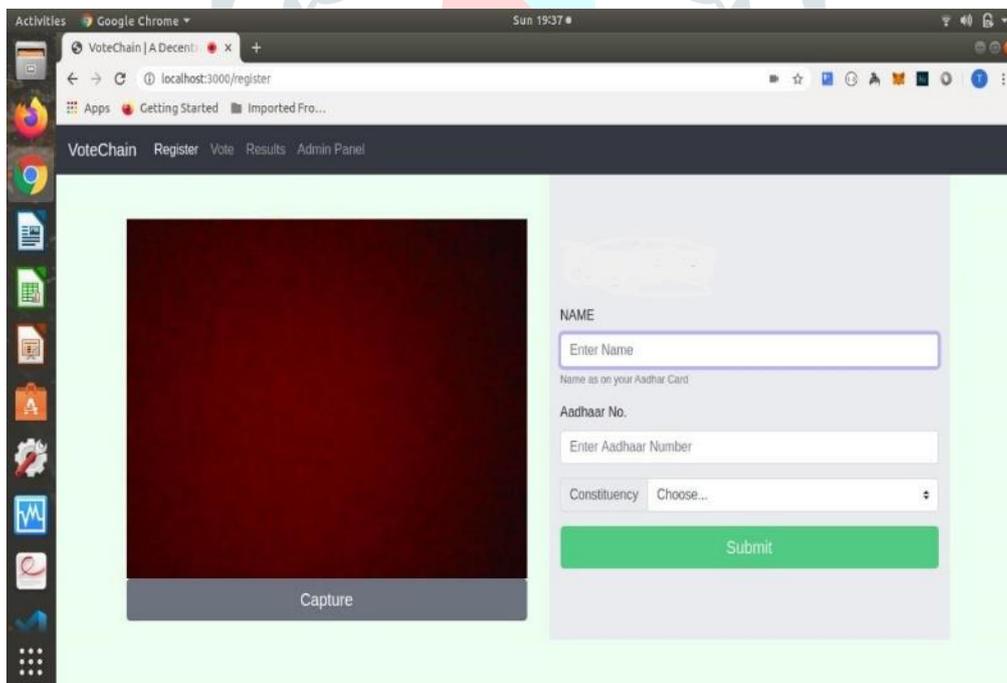


Figure 3 : Website login Page where users credentials are verified

VI. CONCLUSION

Recent developments in voting system includes the use of blockchain technology. Blockchain based e-voting system is safe, secure, transparent, and cost efficient. This paper suggests the use of blockchain based voting system using smart contract. Various advantages of Blockchain based system over traditional voting system are described in this paper. In addition to Smart Contract various other tools used for implementation include Solidity, Ganache, Truffle framework etc. As blockchain based system is decentralized, tampering and alteration of votes is not possible. Also proposed system can be accessed from anywhere and anytime through mobiles, laptops etc. Hence Blockchain based system is very cost and time efficient. Proposed system has a easy-to-use interface to cast their vote and review it. Thus, various advantages of Blockchain based system helps to develop a trust among voters and give them assurity that their vote is counted.

References

- [1] TechCrunch, (2018). Liquid democracy uses blockchain to fix politics, and now you can vote for it [Online].
- [2] Ayed, A.B. (2017). A Conceptual Secure Blockchain Based Electronic Voting System. International Journal of Network Security & Its Applications (IJNSA)
- [3] E. Elewa, A. AlSammak, A. Abdelrahman, T. ElShishtawy, "Challenges of Electronic Voting-A Survey", Advances in Computer Science: An International Journal.
- [4] Ethereum Blog. (2018). On Public and Private Blockchains - Ethereum Blog.
- [5] Hsiao JH, Tso R., Chen CM., Wu ME. (2018) Decentralized E-Voting Systems Based on the Blockchain Technology .
- [6] Gautam Srivastava¹, Ashutosh Dhar Dwivedi² and Rajani Singh²(2018); Crypto democracy: A Decentralized Voting Scheme using Blockchain Technology.
- [7] S. Raval, "Decentralized Applications: Harnessing Bitcoin's Blockchain Technology." O'Reilly Media, Inc. Sebastopol, California (2016).
- [8] Gjøsteen K, Lund AS (2016) An experiment on the security of the Norwegian electronic voting protocol.
- [9] R. Anne, R. Freeland, and G. Theodor Poulos, "E-voting requirements and implementation," in the 9th IEEE CEC/EEE 2007. IEEE, 2007.
- [10] Friðrik Þ. Hjálmarsson, Gunn augur K. Hreiðarsson, "Blockchain-Based E-Voting System," in the 2018 IEEE 11th International Conference on Cloud Computing.

