Decentralized E-Voting System Using Blockchain

Dr S.Sekar*, C.Vigneshwar[1], J.Thiyagarajan[2], V.B.Soorya Narayanan[3], M.Vijay[4]

**Assistant Professor, Department of IT, SRM Valliammai Engineering College, Tamilnadu, India*
[1,2,3,4]Student, Department of IT, SRM Valliammai Engineering College, Tamilnadu, India

---

Abstract - *Developing a decentralized e-voting system that offers effective service to voters, compare to existing voting system, by offering transparency and flexibility which has been considered as challenge. Traditional voting system has been considered as flawed (like vote spoofing, vote phishing and capturing polling booth, etc.). The purpose of this paper is to overcome the limitation of existing e-voting system by implementing voter validation using Biometric, Dynamic Ballot loading and Acknowledgement after casting votes with the help of Blockchain technology. Blockchain is a dispersed and permanent record that is consensually shared and kept up in decentralized structure in various area. Blockchain is one of the rising innovation of current period and guarantee to improve the general versatility of e-casting a ballot. This paper gives review of a framework that utilization blockchain which transform current political race process into a computerized framework with upgraded security.*

***Key Words*: Biometric, immutable ledger, decentralized, Dynamic Ballot, Acknowledgement.**

1. INTRODUCTION

Voting is a process that is used to make a collective decision from a group of people. In the early stages the voting processes are made by debates and discussions. Then we moved to Electronic-voting machine(EVM) for elections. Participants of election are contemplate as Candidates and the one whom elect their candidate by casting their votes are Voters. Election authority are the one who are responsible for conducting election and collecting votes from voters. E-voting are introduced to change traditional voting system.

The fundamentals of election is to build democratic nation by collecting public opinion as votes. To get trust of participants the election process should be transparent and reliable. Inside this specific circumstance, the way to deal with casting a vote has been a consistently developing space. This evolution is primarily pushed through the efforts to make the device cozy, verifiable and obvious. In view of its significance, continuous efforts have been made to improve overall efficiency and resilience of the voting system. Electronic voting or e-voting has a profound role in this. In 1960 's punched-card ballots are used for elections, after introducing of internet technology e-voting has achieved remarkable progress.

Blockchain is one of the emerging technologies with strong cryptographic foundations enabling applications to leverage these abilities to achieve resilient security solutions. It is primarily a distributed decentralized database that maintains a complete list of constantly germinating and growing data records secured from unauthorized manipulating, tampering and revision. Blockchain allows every user to connect to the network, send new transactions to it, verify transactions and create new blocks. Each block is assigned a cryptographic hash (which will also be treated as a finger print of the block) that stays valid so long as the records inside the block isn't always altered. If any modifications are made inside the block, the cryptographic hash could trade at once indicating the exchange in the facts which can be because of a malicious hobby. Therefore, due to its strong foundations in cryptography, blockchain has been increasingly used to mitigate against unauthorized transactions across various domains.

2. LITERATURE SURVEY

1. Fri⍰k .⍰Hj⍰marsson, Gunnlaugur K. Hrei⍰rsson , “Blockchain-Based E-Voting System”. In this system election is represented by a set of smart contracts, which are instantiated on the blockchain by the election administrators. A smart contract for election is created and deployed on the blockchain network for every voting district.

2. Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis, “E-Voting with Blockchain: An E-Voting Protocol with Decentralization and Voter Privacy”. In this system commercial protocol like Bit congress, Follow My Vote, TIVI are used as e-voting protocol.

3. Haibo Yi, “Securing e-voting based on blockchain in P2P network”. In this paper a synchronized model of voting records based on DLT and user credential model based on elliptic curve cryptography are developed.

4. Clement Chan Zheng Wei, Chuah Chai Wen, “Blockchain-Based Electronic Voting Protocol” In this system an architecture suitable to be used in both mobile app and any computational device that connected to the Internet are developed. Every voter is required to install a voting application interface before the voting phase.

3. PROPOSED WORK

This section discusses a proposed decentralized e-voting system using blockchain to conduct the election. We endorse a design to integrate blockchain technology into cutting-edge e-balloting device. And the design consists of the following module.

[1] User validation using biometric.
[2] Dynamic ballot loading.
[3] Acknowledgment after casting their vote.

3.1 USER VALIDATION USING BIOMETRIC

In this module the voter information like Name, Gender, Address, Biometric are collected at the Voter Registration phase of election process using which the voters are verified at the time of voting.

3.2 DYNAMIC BALLOT LODING

In this module based on the residence location of the voter and participants of the election are loaded in the ballot. In which the voter need to select their desired participant. So the voter didn't need to travel to their residence to cast their vote they can cast in nearby polling both. No outside observer can determine for whom a voter voted so that ballot privacy is achieved.

3.3 ACKNOWLEDGEMENT AFTER CASTING THEIR VOTE

A transaction ID is generated in the blockchain network after making a transaction. If voters cast their vote in blockchain network a transaction ID is generated for every transaction and this transaction ID is given as acknowledgment to the user using which voter can verify their vote.

4. SYSTEM ARCHITECTURE

Figure 4.1 illustrate the architecture diagram of decentralized e-voting system using blockchain. The actor of this systems are Election Authority, Registration Authority, Voters and candidates.

Election Authority (EA) - The EA is responsible for creating a vote, proscribing the voter numbers of the voting, paying the vote casting fees for the bitcoin address generated mechanically within the backend. The EA has its own bitcoin address. The tally of votes are made by EA and the results are published.

Registration Authority (RA) - The voter should register in RA to get ready to vote. The candidate should register in RA with his information and the RA will give him the id of candidate.

Voters (V) - The voters should be a set of list.The voter should transfer his public key(*PKi*) to EA. At the time of voting voter are verified by using Biometric and thereby system ensure individual verifiability. A voter cannot interact with a coercer during the election to prove how he or she is voting.

Candidate (C) - The candidates should be a set of list.

For each candidate there will be candidate id to which the vote count is added.

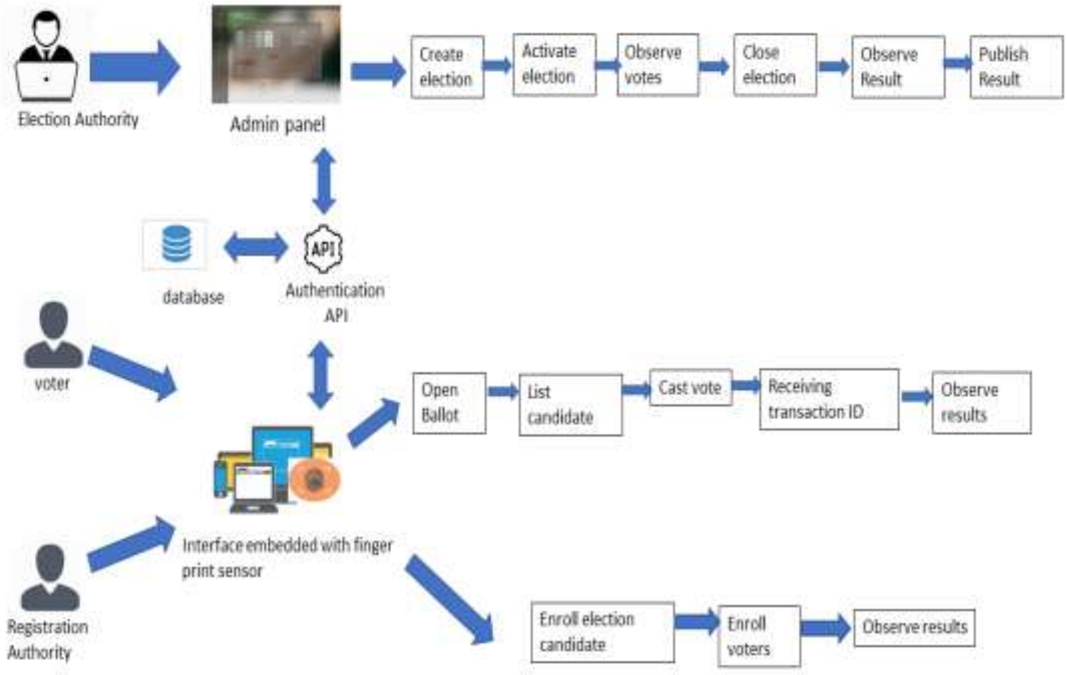

Fig – 4.1 Decentralized e-voting system architecture

5. IMPLEMENTATION OF THE SYSTEM

The system uses Apache Web, MySQL database, PHP, Solidity, Ganache, MD5 hashing algorithm. Figure 5.1 illustrates the flow of system.

Apache Web Server- An apache web server is an open source web server creation, deployment and management software. It used to host our decentralized e-voting web application in http server.

MySQL Database- MySQL is an open source relational database management system(RDBMS). It is storage used to store all our election information like candidate and voter information.

PHP- It is an open supply preferred motive scripting language this is mainly ideal for net improvement and may be embedded into HTML

Smart Contract- An smart contract is a tiny program with the rules of election being directly written into lines of code.

Solidity- Solidity is an object- oriented programming language for writing smart contracts. It is used for implementing smart contracts on blockchain platform. In our system the election rules are developed as a smart contracts using Solidity.

MD5- Message-digest version 5 algorithm is an hash function producing 128 bit hash value. It is one way hash function. It is used to provide authentication in our system.

Homomorphic Encryption- Homomorphic encryption is a form of encryption that allows operation on cipher texts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext.

Quorum- Quorum is an Ethereum based distributed ledger protocol that helps transaction and settlement privacy. The number one features of Quorum are Transaction and settlement privateness, Voting-primarily based consensus mechanism, Network and peer permissions management, Higher overall performance

MetaMask -MetaMask was created to increase the accessibility of the Ethereum blockchain to the user. A plug-in for Chrome, MetaMask acts as an Ethereum browser, allowing users to manage their Ethereum wallet and interact with decentralized applications and smart contracts without running a full node.

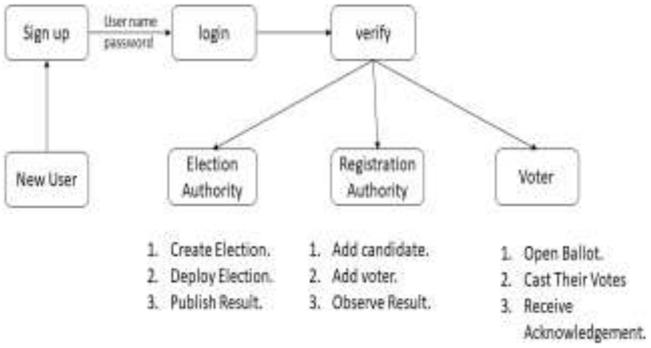

Fig – 5 Decentralized e-voting system flow diagram

5.1 Role of Voter

At time of voting voter biometric information are scanned and hashed using MD5 algorithm and the hash are checked with the election database. If the hash matches the user is redirected to respective voting page and the candidate are listed in the web page. Voter select their desired candidate and vote count are increased in the bitcoin address of the candidate. Once voter cast their vote the voting fees in their Bitcoin address is set as zero. Hence repetition of votes is not possible.

Fig – 5.1 Biometric authentication

5.2 Role of Election Authority

Election Authority is responsible for deploying the initial Register and creator of smart contracts. The Election Authority also has the ability to grant or re-vote ballot creation permission for registered voters/creators.

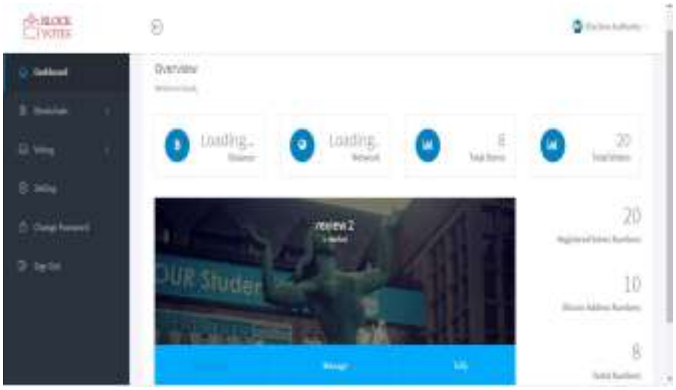

Fig – 5.2 Election Creation

5.3 Role of Registration Authority

The role of Registration authority is as soon as the EA has Deployed election in the Blockchain Network. It is RA chargeable for adding candidates and Voters to the election.

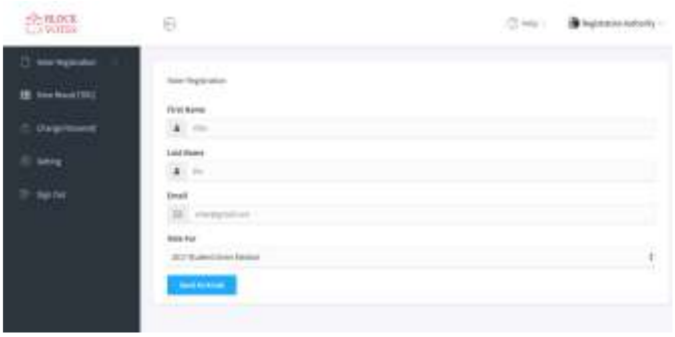

Fig – 5.3 Voters Registration

6. CONCLUSION AND FUTURE WORK

The concept of adapting virtual vote casting systems to make the general public electoral system quicker and less difficult, is a compelling one in current society. Making the electoral manner cheap and brief, normalizes it inside the eyes of the voters, eliminates a certain strength barrier between the voter and the elected respectable and puts a positive amount of pressure at the elected legitimate. It additionally opens the door for a greater direct form of democracy, allowing electorate to explicit their will on character bills and propositions. In this paper, we brought a completely unique, blockchain-based digital vote casting device that utilizes clever contracts to allow cozy and fee efficient election even as guaranteeing citizens privacy. We have outlined the structures structure, the design, and a safety analysis of the gadget. By evaluation to previous work, we have proven that the blockchain technology offers a new possibility for democratic countries to strengthen from the pen and paper election scheme, to a extra cost- and time-green election scheme, whilst increasing the safety measures of the todays scheme and provide new opportunities of transparency. Using an Ethereum personal blockchain, it is possible to send masses of transactions according to second onto the blockchain, using every factor of the smart contract to ease the load at the blockchain. For nations of more length, some measures ought to be taken to withhold extra throughput of transactions consistent with 2d, as an example the discern & infant architecture which reduces the number of transactions stored on the blockchain at a 1:100 ratio with out compromising the networks protection. Our election scheme lets in man or woman citizens to vote at a balloting district of their selecting even as making certain that each man or woman electorate vote is counted from the right district, that can potentially boom voter turnout

REFERENCES

[1] Fri�k �Hj�marsson, Gunnlaugur K. Hrei�rsson. (2018). Blockchain – Based E-Voting System. Available at: https://skemman.is/bitstream/1946/31161/1/Research-Paper-BBEVS.pdf.

[2] Mrs. Harsha V. Patil, Mrs. Kanchan G. Rathi, Mrs. Malati V.Tribhuwan. A Study on Decentralized E-Voting System Using Blockchain Technology. Available at: https://mail.irjet.net/archives/V5/i11/IRJET-V5I1109.pdf.

[3] Clement Chan Zheng Wei, Chuah Chai Wen. Blockchain-Based Electronic Voting Protocol. Available at:http://joiv.org/index.php/joiv/article/download/174/169

[4] Gaby G. Dagher, Praneeth Babu Marella, Matea Milojkovic and Jordan Mohler3. Secure Voting System using Ethereum's Blockchain. Available at:https://www.researchgate.net/publication/322874160_BroncoVote_Secure_Voting_System_using_Ethereum's_Blockchain.

[5] Geth.ethereum.org. (2018). Go Ethereum. Available at: https://geth.ethereum.org/

[6] Vitalik Buterin. (2015). Ethereum White Paper. Available at: https://github.com/ethereum/wiki/wiki/White-Paper.