

Design of a Secure Block Chain based E-Voting System

S. Uma¹, R. Maheshwari², J. K. Mayuri³, R. Sowndharya⁴, S. Vano Jenifa⁵

¹Professor & HoD, Dept. of Information Technology, Hindusthan Institute of Technology, Coimbatore, India

^{2,3,4,5}Student, Dept. of Information Technology, Hindusthan Institute of Technology, Coimbatore, India

Abstract: Today's world election is the most important process for modern democracy. A large section of the population does not trust the existing electoral patterns, due to the loop holes for cheating the electoral process. Here the need for proposing an electoral system which will be secure and accepted by the entire population was felt. The electoral system using blockchain technology is proposed to maintain the secrecy of the individuals, the vote casted etc., the stored data cannot be modified and remains intact and safe from attacks. The proposed system is more efficient and is not susceptible to having compared with existing system.

Keywords: Online Voting, Using Desktop, One Time Password

1. Introduction

The Blockchain technology originates from the underlying architectural design of the crypto currency bitcoin. It is in the form of distributed database while records are taken in the form of transactions, a block is a collection of these transactions. With the use of blockchain a secure digital voting can be devised. A blockchain is a distributed, immutable, inconvertible, public ledger. This technology works through four main features:

- The ledger exists in many different locations: No single point of failure in the maintenance of the distributed ledger.
- There is distributed control over who can append new transactions to the ledger.
- Any proposed "new block" to the ledger must reference the previous version of the ledger, creating an immutable chain from where the blockchain gets its name, and thus preventing tampering with the integrity of previous entries.
- A majority of the network nodes must reach a consensus before a proposed new block of entries becomes a permanent part of the ledger.
- These technological features operate through advanced cryptography, providing a security level equal and/or greater than any previously known database.

2. Literature survey

Block chain technologies brings massive momentum in the

last few years. Blockchains are distributed ledgers that enable parties who do not fully trust each other to maintain a set of global states. The parties agree on the existence, values and histories of the states in this paper we survey the state of the art, focusing on private block chains. We analyze both in-production and research system in four dimensions:

- Distributed ledger
- Cryptography
- Consensus Protocol
- Smart Contract

3. Existing system

In the existing system, the most common way for conducting the election in a country is through a paper ballot system. With the technological development it was then conducted using electronic voting machine (EVM) and using internet these methods are referred to as e-voting. When voting was done using a machine in a polling station and I-voting when using a web browser.

A. Limitations of the existing system

The existing method of voting has several limitations and is easily susceptible to frequent or cheating activities in which case the entire election system will breach the advantage of modern democracy. Some of the limitation of the existing voting system are listed below:

- The sealed voting boxes in which the casted ballot papers are stored could be tampered or replaced.
- In the paper ballot voting system, the election result is based on manual counting of the votes which may not be correct /biased for a larger count of votes.
- The manual voting system may lead to decreased efficiency and accuracy.
- In the internet based I-voting system the authorization of the voter may be tampered.
- The server may be directly infected by the hacker.
- The electronic voting machine could be programmed to cast all the votes to a particular party which may lead to cheating of democracy.
- Though vote casted by a voter could be verified by giving a print out of the vote casted, the EVM could

still be programmed to cast the votes for a particular party.

4. Proposed system

The security of digital voting is always the biggest concern when considering to implement a digital voting system. In the proposed system (Bc E-voting) the blockchain technology is used to keep track of the vote casted securely. Thus, blockchain is used to potentially solve the security issues in the e- voting system, with this method all the parties will come to a consensus and the final results declared. Because of the blockchain audit trail and it is easy to verify that no votes were changed/removed. Illegitimate votes were not added.

A. System architecture

The election commission will create an election system. After that voter should registered where the OTP will generate for the particular E-mail. For purpose of checking whether it is a valid user or not. If it is a valid user they can vote for the candidates as their wish.

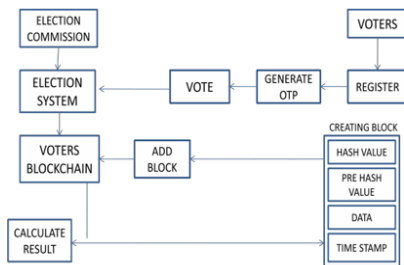


Fig. 1. System architecture of proposed system

The votes are stored in a separate block which is connected with one to another. So that it is safe. After the election process is over results can be calculated easily

B. Use case diagram

Here first the admin creates an election then people can login with their details and they can vote. After the election process is complete the admin can view the result.

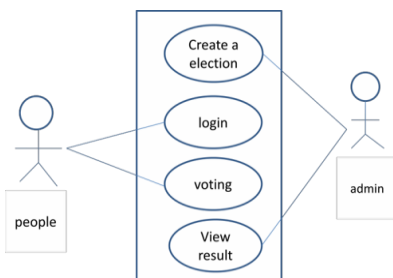


Fig. 2. use case diagram of proposed system

C. Advantages of proposed system

The advantages of the proposed system are

- Enhanced Security
- Increased efficiency and speed

- Improved traceability
- Improved Trust

5. Implementation

The implementation of BC E-voting system consists of the following six modules:

- Home Module
- Create Election Module
- Candidate Module
- Alliance Module
- Registration Module
- Result Module

A brief explanation of each of these modules is given below:

A. Home module

In home module, information about online voting system. Information about various parties, participating in this election.



Fig. 3. Home module



Fig. 4. List of parties

B. Create election module

Election administrators create election ballots using a smart contract in which the administrator defines a list of candidates for each voting district. The smart contract are then written on to the Block chain, where district nodes gain access to interact with their corresponding smart contract.



Fig. 5. Create election module

C. Candidate module

If a voter is out of station, they can get the detail knowledge

about following candidates who are participating in the particular booth.

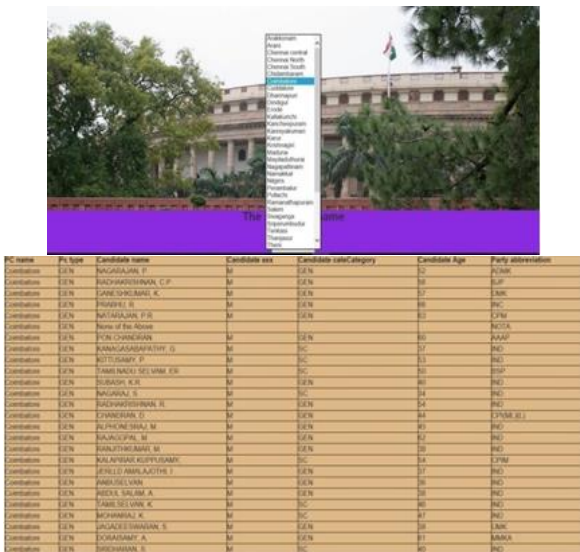


Fig. 6. Candidate module

D. Alliance module

An electoral alliance is an association of political parties or individuals that exists solely to stand in election.

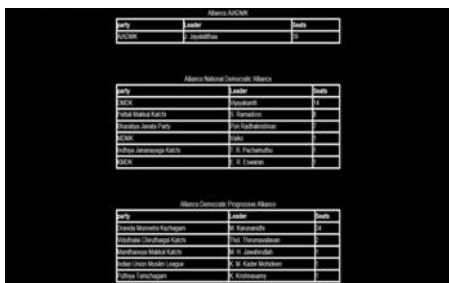


Fig. 7. Alliance module

E. Registration module

The registration of voter's phase is conducted by the election administrators. When an election is created the election administrators must define a deterministic list of voters. A unique wallet is generated for each voter for each election that the voter is eligible to participate in.



Fig. 8. Registration module

F. Result module

Verifying votes: In the vote transaction, each voter receives the transaction ID of his/her vote. In our e-voting system, voters can use this transaction ID and go to an official election site using a blockchain explorer and locate the transaction with the corresponding transaction ID on the blockchain. voters can, therefore, see their votes on the blockchain, and verify that the votes were listed and counted correctly. This type of verification satisfies the transparency requirement while preventing traceability of votes. Tallying results: The tallying of the election is done on the fly in the smart contract. Each ballot smart contract does their own tally for their corresponding location in its own storage.

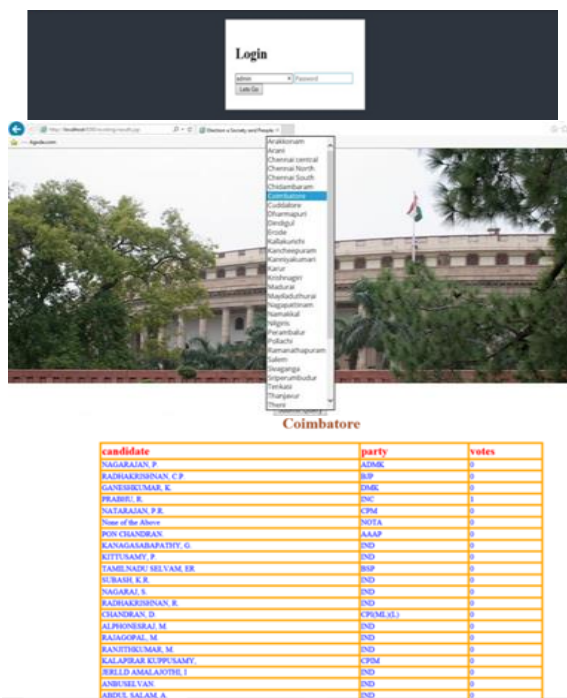


Fig. 9. Result module

6. Conclusion

E-voting, is a potential solution to the lack of interest in voting amongst the young tech savvy population. Due to fraudulent and cheating activities carried out in the existing voting system. For e-voting it becomes more open, transparent, and independently auditable, a potential solution will be to use in the blockchain technology. This paper explores the potential of blockchain technology and its usefulness in the e-voting scheme. The paper proposes an e-voting scheme by name BC E-VOTING system highly secure and dependable. The implementation and related performance are given in the paper along with the challenge presented by the blockchain platform to develop a complex application like e-voting. The paper presents two potential paths forward to improve the underlying platform to support e-voting and other similar application. The project concludes that by using blockchain we can manage the voting directory and also, we can avoid failure for voting list

and fraud detection. The block manages the hash values and dataset.

7. Future enhancement

The Bc E-voting system can be improved by including Biometric authentication.

References

- [1] Friorik P. Hjalmarsson, "Block chain- Based E-Voting System" –IEEE 11thInternational conference on Cloud Computing," 2018.
- [2] Nir Kshetri and Jeffrey Voas, "Block chain Enabled E-Voting," IEEEBlockchain Initiative
- [3] Jonathan Alexander, Steven Landers and Ben Howerton, "A Decentralized Voting Network," 2018.
- [4] TechCrunch, "Liquid democracy uses block chain to fix politics, and now you can vote for it," 2018.
- [5] Michael Del Castillo, "Sierra Leone Secretly Which Holds First Blockchain-Audited Presidential Vote," 2018.
- [6] Ethereum Blog, "On Public/Private Blockchains," 2018.
- [7] Bitfury.com, Digital Assets on Public, 2017. [Blockchainsresearch/bitfurydigital_assets_on_public_blockchains-1.pdf](https://blockchainsresearch/bitfurydigital_assets_on_public_blockchains-1.pdf)