RESEARCH ARTICLE OPEN ACCESS

Decentralize Electronic Voting System Using Blockchain

Poonam Patil [1], Seema Mane [2]

Computer Engineering, GOVT. Residence women Polytechnic, Tasgaon - India.

ABSTRACT

Developing an electronic voting system that satisfies the legal requirements of legislator. Our current Election system inherit the use of EVMs which in various source have been proven to be hackable & not tampered proof. This makes the candidate & citizen not trust the Election System. This paper aims to evaluate the use of blockchain technology to build distributed electronic voting system. The problem with people living far from the native and not able to migrate for voting is one of the issues. This leads to the smaller number of votes in elections. More generally we aim to build a system that not only improve the voting but also ensure transparency of the process and will also build trust among the people.

Keywords — Blockchain, distributed ledger, decentralized, Hyperledger.

I. INTRODUCTION

In every country, when it comes to election the security of election is important factor to be considered. The Computer Security field for decades have studied the various way of doing electronic voting, with increasing the security and minimizing cost of the system. Election in India used to happen before EVMs via paper ballot. Paper ballot system was replaced by EVMs in local, state and general (parliament) election in India. The Paper Ballot system was easily tampered and manipulated while election i.e. like adding additional votes, changing of ballot box, etc. Vulnerabilities can be found through the voting process from start to end. Security of ballot box while transferring or at Election booth. So, use of Electronic Voting Machine EVMs came into existence in late 90s.The EVMs were first time used in general election in GOA in 1999.Then later in 2003, all by-election and state election started using EVMs, encouraged by this election commission decided to use only EVMs for Lok Sabha Election in 2004.

Electronic Voting machine have been viewed as flawed by the security community. Anyone with physical access to the machine can manipulate it, thereby affecting all votes casted on the machine. There are cases when the loosing candidate trying to blame the EVMs for their loss. EVMs have never built trust among the Candidates in the Election. When the independent security expert analyzed the machine, they said the machine can be hacked easily i.e. one can open it and change the display easily to print wrong number of votes and other way was changing the buttons sensors to vote for wrong candidate when being pressed for particular one. There are various studies on how EVMs can be tampered or hackable.

Our current Election System lacks to build trust among the candidate standing in the election. People voting for candidate

aren't 100% assured that their votes are reaching desired candidate correctly i.e. it also lacks in transparency to the voters.

We inherit the use of blockchain technology. Blockchain in simple words means distributed ledger due to this the records in blockchain are immutable and are linked to one another. Main features of Blockchain:

I. The ledger exists in various different location: A single node failure wouldn't stop the ledger from working.
II. Due to distributed control new record is verified by all node then added to the ledger
III. A "new block" always provide reference to the previous version of the ledger. This create an immutable chain from where the blockchain gets its name and hence prevent the record from getting tampered.
IV. Before new block entry gets permanently added to the ledger the network nodes must reach a consensus.
V. The consensus is an algorithm which makes all the node agrees to particular decision before adding the record to the ledger.

II. LITERATURE SURVEY

The various other existing system except paper ballot & EVMs are as follow:

Estonia i-Voting: - Estonia was the first country to implement election via internet enable using smartphone or computers. The voters needed to log in to the application using the government issued ID cards and cast votes. Only 30% used the i-voting. As it uses internet and websites to cast votes from remote location. The various issues such as buying of votes or votes by forcing, malware in voter's system, etc. are found by the security community.

Votem:- It uses Digital Voting mechanism. Developed using Ethereum Blockchain using ERC20 Token. In VOTEM one need to have a smartphone and need to download app from Appstore or play store. VOTEM use VAST Token to cast votes i.e. user have VAST Token and they send those tokens to candidate they wish to elect. Ethereum uses proof of work concept to process the blocks which contains the votes casted to the candidate to be verified. Thus, any party with 51%% more processing/mining power are able to manipulate the blocks and also be able to double spend the votes. Also, POW algorithm require a lot of processing power to process large number of votes per second. So, using limited power comes limited processing of votes and that may delay result of election.

Voatz :- Another Digital Voting application which uses Mobile Application to cast votes. But in this it takes fingerprint, Facial image to recognize and validate and verify the identity of the user. Here they are trying to secure the voting system but yet there new vulnerabilities due to the complexity of the system. VOATZ was used in West Virginia Election in 2018 and only 40-50 people voted using the VOATZ application. VOATZ provided the user transparency and traceability like features. Agora: - It is swiss protocol company developed a custom blockchain. It is developed on the consensus mechanism "proof of concept". It is yet permissioned and public ledger as per company. It has been used in Sierra Leone election in 2018. Working of Agora: - People uses paper ballot to select candidate and then that paper ballot would be used to store the record on the distributed ledger. It is nothing but a Distributed databased like functionality.

There are many different projects that show how the blockchain is used in the voting process. Each and every one has their own drawbacks and limitations.

III. PROPOSED SYSTEM

Our goal is to develop a system without disturbing the process of the existing Election System. Our system aims to replace the EVMs. The election process would be same but in place of EVMs we place our device which would be connected to the internet securely (independent Modem in device OR over router/ Wi-Fi connection. There would be slight change in the process before and after then voter votes at booth. Like the voter needs to update its voter id before election with newly generated Voter ID card. The newly generate Voter ID card would have a cryptographic key/ hash embedded to it. The newly generated Voter ID card would also have an option to be linked to Aadhar card to ensure validation of user and stop user from double time voting. Now at the Election time the VOTER needs to carry the ID and swipe or scan it in our Device that verify that voter is valid and display his information for couple of seconds and asks the voter to select the desired candidate. Now when Voter select the candidate then a new transaction is created in the form of vote and send that to multiple node of the distributed ledger to validate whether the voter have voted before and if not, then the distributed node agree to consensus algorithm and then the vote of the voter is permanently written to the ledger. This cannot be undone or irreversible as the nature of blockchain is irreversible and each and every record written to the ledger cannot be reversed.

We use IBM's Hyperledger Fabric platform to develop our System.The use of public ledger will state public information. This will cause many issues. So, we choose the Hyperledger Fabric platform. It provides permissioned blockchain which has both private as well as public property. In other blockchain platform, there is word called as smart contract. But in Hyperledger Fabric smart Contracts are changed with more efficient "Chain Code".

Smart Contract/Chain code: - Smart Contract are trackable and irreversible application that executes in a decentralized environment. Once the smart contract has been deployed nobody can edit the code or change it execution behaviour. Smart contract execution guarantees to bind parties together to an agreement as written. This creates a new powerful type of trust that does not rely on single party. Smart Contract enables better management for realizing and administering digital agreements because they are self-verifying and self-executing. The Chain code and smart contract is the same thing. Only difference is chain code is used in Hyperledger and smart contract is used in Ethereum.

In our system we can define a particular smart contract. Example: -consider a State Election to be held. That particular state has 200 number of seats combine all the parties the parties which win 101 seats will rule over the state. We design a blockchain such that there reside a blockchain in blockchain OR blockchain connected to blockchain i.e. the sub district is connected to another blockchain and that blockchain result will be carried forward to the main blockchain. The chain code is developed in such a way that the on-election day it will be given time to run in that period from 10 am to 7 pm. After than at the end the chain code calculates the amount and declare the result based upon the agreement 101/200. This can't be changed. To enter into Election the candidate who is standing will need to get a key from the Election commission so that it validates that the candidate is valid. Before election start the following sub, district candidate come to the election booth with their desired key and then election starts. This way the election wouldn't be irreversible and no manipulation would be possible. Only the voter with the valid Voter ID card will be able to bypass the login at device placed in the voting booth.

Security: - As the Hyperledger makes use Byzantine-fault tolerant (BFT) consensus. That means the various

processing nodes are located at various location. So, to manipulate the result of blockchain one has to hack all the location server node at same time and after that manipulate the consensus of the Fabric which cannot be changed once declared at the initial stage. If one node goes down the robustness of the fabric would set backup node to continue the work of the failed node.

The data at the ledger is secured using two-way transport layer security (TLS). The Access Control decision regarding which user are able to which transaction, are based on user's identity attributes. Example - Other user changing information of the voted person, OR, candidate standing in election trying to tamper the voter's votes is not possible. In our system the voter itself don't have control to change his data because once vote is done it should not be changed. So, this all is taken care by smart contract or chain code.

The initial nature of blockchain is public ledger i.e. each and every person can see all data. But in Hyperledger Fabric it doesn't send the sensitive data together to those organization that don't need to have it in the first place. This can be done by using Hyperledger Fabric feature called "Private channel data". The sensitive data here is only shared with those that need to have access to it. In our system we create separate private channel of separate district in state. So, the votes don't get mixed up with the other district system.

IV. SYSTEM DESIGN

I. **System Overview: -** The fig 1) show a general flow of how voting process going to be held. Here the Voter verify his identity and with the given voter id card and then proceed to cast vote on the touch device. The votes of voter will be combined in the block of size of 10 votes and each block will need to be verified by the parties in the chain. After the verification by the parties that the votes in the following block are unique and valid then only, they are allowed to get added to the ledger which stores hem permanently and are irreversible.

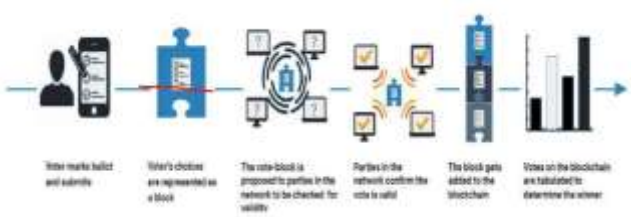

Fig 1. System Architecture

II. **System Entities: -**

1. Election office: - In our system EC will be responsible to organise smart contract.
2. User / Voter: - They need to carry their unique new voter ID card along with them to get verified at the election booth which allow them to vote.
3. Parties: - parties can be anyone who deploy servers / node to contribute for processing in the chain. They can be either the parties standing for the vote OR These can be done by Election office.

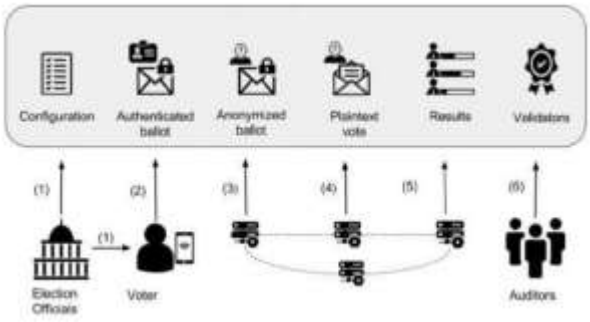

Fig 2 . System Entities

V. RESULT

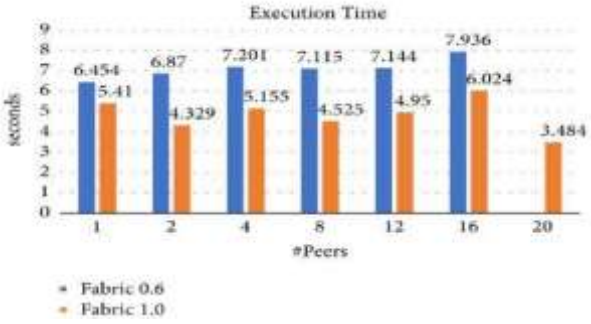

Fig 3. Result

The use of block chain in this voting system will provide security. It also decentralize ledger. The performance of the system will also increase. This will help cut the number of people required to audit the votes at the end of the day, here in fig 3) we can see that in Hyperledger it takes 5-8 sec to process 1000 transaction. Whereas Bitcoin does 5 TPS / Sec and Ethereum does 15 TPS / Sec. This leads to the huge increase in the scalability of the voting system i.e. the system would be able to cast 700-1000 votes per 5-8

seconds depending. The results me vary with respect to the chain code and security procedure the blocks have to go through.

VI. CONCLUSION

The idea of adapting digital voting system to make the public election process cheaper, faster and easier. It also opens the door for a more direct form of democracy, allowing voters to express their will on individual bills and proposition. In this paper, we introduced a unique, blockchain-based electronic voting system that utilizes smart contract to enable secure and cost-efficient election while guaranteeing voters privacy. By comparing to previous work, we have shown that blockchain technology offers a new possibility for democratic countries to advance from the pen and paper or EVMs election scheme, to a more cost and time efficient election scheme while increasing the security of today's scheme and offer a new possibility of transparency.

REFERENCES

[1] Nicholas Weaver (2016). Secure the vote Today: https://www.lawfareblog.com/secure-vote-today
[2] TechCrunch, (2018). Liquid democracy uses blockchain to fix politics, and now you can vote for it [Online]. Available at: https://techcrunch. com/2018/02/24/liquid-democracy-uses-blockchain
[3] Vitalik Buterin. (2015). Ethereum White Paper. Available at: https:// github.com/ethereum/wiki/ wiki/White-Paper.
[4] Feng Hao P. Y. A. Ryanand, Piotr Zielinski (2008). Anonymous voting by two-round public discussion.http://homepages.cs.ncl.ac.uk/feng.h ao/files/OpenVote_IET.pdf
[5] Jonathan Alexander, Steven Landers and Ben Howerton (2018). Netvote: A Decentralized Voting Network Available at: https://netvote. Io/ wp-content/uploads/2018/02/Netvote-White-Paper-v7.pdf
[6] Ronald Cramer, Rosario Gennaro and Berry Schoenmakers. A Secure and Optimally Efficient Multi-Authority Election Schemehttp://www.win.tue.nl/~berry/papers/euro97.pdf

[7] Agora (2017). Agora: Bringing our voting systems into the 21st century Available at:https://agora.vote/Agora_Whitepaper_v0.1.pdf
[8] Patrick McCorry, Siamak F. Shahandashti and Feng Hao. (2017). A Smart Contract for Boardroom Voting with Maximum Voter Privacy. https://eprint.iacr.org/2017/110.pdf
[9] Pete Martin : Votem – Voting for Mobile World https://www.votem.io/assets/docs/wp.pdf