ISSN: 2581-3404 (Online) IF: 5.445 (SJIF)

IJIRTM, Volume-7, Issue-4, August-2023.

Biometric Voter Verification Using Blockchain Voting through Electronic Media

Ashutosh Kumar[1], ChinmayBhatt[2]

CSE, SRK University, Bhopal, In dia[1, 2]

ashu9.nit@gmail.com[1],chinmay20june@gmail.com[2]

Abstract: *ELECTION is a process of establishing democracy in the country. It is also one of the most challenging task, one whose constraints are remarkably strict. There has been the extensive adoption of Direct-recording electronic (DRE) for voting at polling stations around the world. Starting with the seminal work by Chaum, published in IEEE Security & Privacy in 2004, research on end-to-end (E2E) E-voting has become a thriving field. Informally, the notion of being E2E verifiable refers to have two properties: First, each voter is able to verify if their vote has been cast as intended, recorded as cast. Second, anyone can verify if all votes are tallied as recorded. By contrast, in the traditional paper-based voting system, a voter cannot verify how their vote is recorded and tallied in the voting process. In traditional voting process, a voter goes to polling station and shows his/her voter Identity card and after finding his/her name in eligible voters list he is a given to vote the candidate of his choice. In the case of EVM(Electronic Voting Machine) their security is a big challenge before the officials. Thus the system depends on the trustworthy individual at the polling stations and during counting, thus leading to the introduction of the automated paperless secure e-voting system. This work mainly focuses on developing an E-Voting system which is much more secure, verifiable and does not involve the requirement of too many trustworthy individuals at every level. We aim at using Blockchain to make voting much secure and also using ring signature and Fingerprint Authentication for additional security.*

Keywords: Blockchain, Secure Voting, Biometric Voting.

Introduction

The central issues of any e-voting system are considered to be authentication and privacy. Citizens cast their votes in the polling station on EVM(Electronic Voting Machine) which can be tampered and so it is a challenge for central government, police and election commission to make sure that no tampering is done by keeping these machines secure. Also after the voting ends it takes time for election commission to release the results as vote counting takes time. This voting system is inefficient and takes a delay in counting the votes. Thus our project aims at developing the voting system which is more secure and reliable and much more automated than the current system. The current voting system is not secured as EVMs can be tampered also the user does not end to end verified. Fake IDs are made on the name of people who are dead and votes are cast. Thus a system with more security and reliability is required.

So we propose a system which makes use of Blockchain to cast and store votes and to authenticate users we will be using biometric details such as a fingerprint.

Firstly blockchain technology was used within Bitcoin and is a public ledger of all the transaction. Blockchain consists of several blocks associated with each other. The blocks are related because the hash values of the previous block are used in the next block creation process. The effort to change any block's information will be more difficult because it must change the next blocks. The initial block is called the genesis block. These transactions are stored by a Blockchain in a block, the block eventually becomes completed as more transactions are carried out. Once the block is complete it is then added in a linear, chronological order to the blockchain. Also, our system will make use of ring signature which makes sure that votes cast are as intended and tallied as cast.

Current Voting Methodology

India, one of the largest democratic country in the world with the population of 133.92 crore makes use of Electronic Voting Machines (EVM) for its voting process. However for Presidential Elections India uses paper Ballot method as only the people elected democrats vote for the President. EVMs are under the control of Election Commission of India (ECI) which aims at conducting fair elections in the country. It distributes the EVMs in different regions as per the constituencies, ranging from large metropolitan cities to small remote villages with less or no connectivity. Constituencies are further divided into sub-regions and for each sub region we have one or two polling stations where voters go to vote. These machines save 3840 votes. So ECI distributes in different regions as per the registered voters in that area. The process is difficult and it also consumes lot of time. Also procedure is prone to manual errors.

Recently ECI developed another system to give voters confirmation that their votes are recorded as casted by them. The system is called 'Voter Verifiable Paper Audit Trail' (VVPAT), which prints the voters choice on a small piece of paper so that voter can see it and after that it is dropped in a sealed box. That receipt is not for voter to take home. This allows the voter to know that the vote was placed correctly and addressed previous concerns that votes were being cast to a default candidate on a potentially rigged machine.

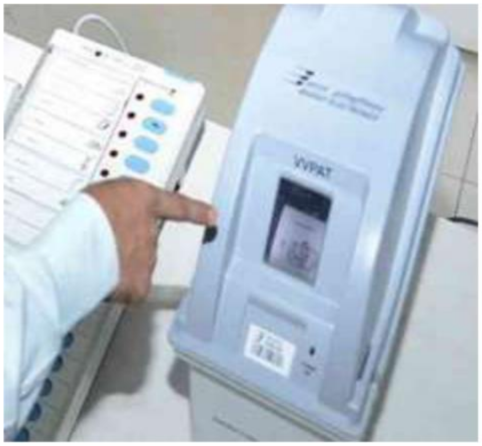

Fig 1.1

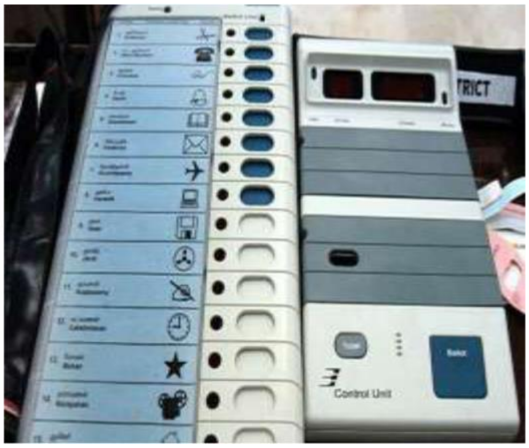

fig 1.2

The key benefits of this system are:

- **a.** The hardware is built in such a way that it runs on 6 volt battery and it is very robust.
- **b.** The polling is offline, and all machines are returned to the ECI who is responsible for preventing voter fraud and conducting fair elections.

Other Countries like Nepal, Bhutan, Namibia and Kenya has brought Indian manufactured EVMs to conduct election in their countries.

Further, the manual authentication method of physically identifying voters in their registered voting constituency is also something that should be avoided, potentially allowing people to place votes for a candidate in their home state even if they are travelling, which can drastically increase voter turnout.

Software Based Voting

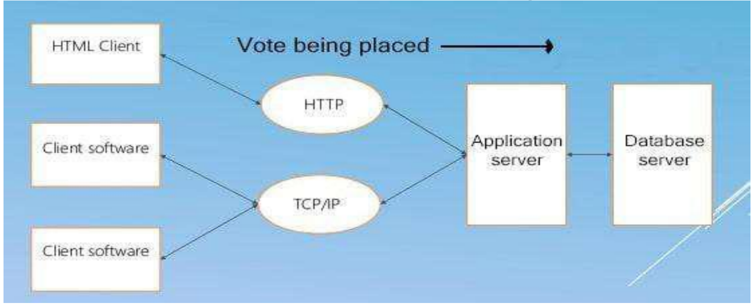

Fig1.3

In traditional Voting systems, votes are being cast on the client and then the choice is to be submitted to the server where a central database keeps track of all the cast votes.. The database is used to store each individual's vote so that it is possible to re-count all the votes, instead of merely tracking the votes with a counter for each candidate. This makes the system possible to verify that no voter fraud has occurred, such that there were no duplicate votes. Since votes are not placed until they are sent to the server, we can ensure that the server validates the voter's identity and choice to prevent fraud.

While the following obvious security concerns of a software application could be applied, some of the more domain-specific ones are:

1. A single Voting System would not be able to handle load of multiple voters placing their votes simultaneously. We would need allow voters to place votes to one of many servers.
2. As there are multiple voting servers, it becomes more difficult to ensure that there are no duplicate votes placed across servers.
3. An attacker could spoof a voting machine's signature over the network and place unauthorized votes.

Why Blockchain?

Blockchain architecture provides good solutions to our key problems:

High volume: Being the voting method decentralized, single central server won't be taking load of all the voters as votes will be placed all across the nodes.

Merkle trees:It ensures that largest of voters which are verified and authorised is accepted and it makes difficult for unauthorised votes to modify a vote which is already placed.

Redundancy: There are multiple exact replicas of the voting results, created at the time of voting. It would be necessary to fake a vote on all of the redundant servers.

Blockchain was originally implemented by Santoshi Nakamoto for Bitcoins. He used a technique called Proof of work(PoW) to add a new block in the chain. Bitcoin - the digital gold, has a current value of $112 billion USD. Blockchain brings such cryptocurrencies to play. Blockchain forms a network by its distributed ledger which is use for doing the transactions. Crypto currencies are tokens used within these networks to pay for these transactions. In PoW method all the miners on the network have to solve a difficult mathematical problem for a reward, while also adding all previous transactions to the chain. This can be very intensive and cost may be high for smaller scale but while conducting elections on such a large scale it will be effective.

Consent is the process which makes sure that all the nodes must agree on all votes which are placed and that their ledgers are precisely same and updated. achieving faster consent at scale is a one big problem before the new crypto currencies and startups dependent on it. This will result in faster approval of transactions and this will lead us probably a step closer to our solution. Currently it takes too much time to confirm a bitcoin transaction, which is wondering if you sent it to the wrong address or at least that much time in which the receiving party have to wait before they can access it. While Visa, which provide card solutions to banks can handle 24000 transactions per second. That's more like it.

Delegated Proof of Stake

Delegated Proof of Stake (DPoS) is one of the fastest concord algorithms, as used by the EOS token. They claim to confirm 3000 transactions every second across 21 'delegated' servers. The catch with Proof of Stake is that EOS doesn't aim to achieve concord on all available nodes. In each confirmation round, a random server is chosen to be the 'block producer', the node responsible for creating the new block and sending it to all the other delegates. The block producer then tallies all votes that were placed on it and sends it to every other delegate to confirm it. If any unauthorized node tries to propose a block out of turn, the block is rejected by its peers since only the chosen delegate for each epoch is allowed to propose a block. A similar architecture can be proposed for voting, with the voting machines acting as regular nodes and a set of dedicated servers acting as delegates for vote confirmation.

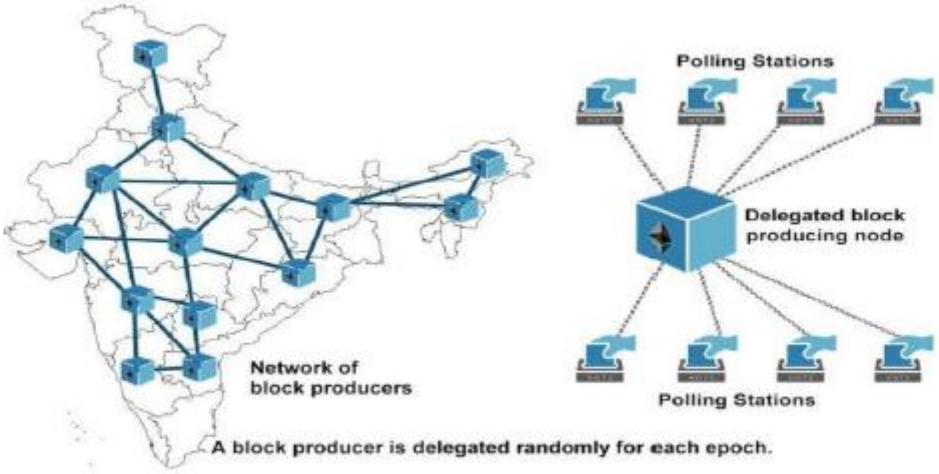
Polling Stations
Delegated block producing node
Network of block producers
Polling Stations
A block producer is delegated randomly for each epoch.

Fig 1.4

When the network adds a block of votes to the chain, one of the 'delegates' is randomly chosen to confirm the validity of the votes that make up the current block. To achieve consensus on the votes that have been placed this block is then placed to other delegates. The voter authentication method have to be bypassed by the malicious actor and then the invalid vote can be successfully placed on a randomly chosen delegate server.

We can evenly spread the load faced during balloting, while distributing the vote confirmation effort across multiple delegates. We can ensure that the system maintains redundancy in the case certain delegates experiencing excess load or unexpected failure through deterministic selection of the block producer. In this manner we can design a fault tolerant system that will significantly streamline the balloting process.

Smart Contracts for Election

Smart contracts are trackable and irreversible which are being executed in a decentralized environment. The change in code or in execution cannot be done once the smart contracts are being deployed. Parties are being bind together to an agreement that guarantees the execution of the smart contract. With the help of smart contract it is possible better management for realizing and administering digital agreements because they are self- verifying and self-executing. An open source blockchain platform is provided by etherium which can be used to deploy smart contracts. For writing smart contracts a new programming language called solidity was introduced by etherium. Such System can be implemented using smart contracts also. The different roles of smart contract are as follows:

1. **Election Administrators:** They manage the lifecycle of election; there are many trusted institutions and companies which are enrolled with this role. The type of election and the lifetime of the election is being decided by the election administrators. They create aforementioned election, configure ballots, register voters and assign permissions nodes.
2. **Voters:** Voters can authenticate themselves for the elections they are eligible for, load election ballots, cast their vote and verify their vote after the election is complete. When the voters cast their vote they can be awarded with the tokens in the election or in near future, which could be integrated with the smart city project.
3. **District nodes:** When the election administrators create an election, each ballot smart contract are being deployed onto the blockchain representing each district votes. When the ballot smart contract are created, then they can interact with each of the corresponding ballot smart contact. When the vote has been cast by the individual voter from his smart contract, the vote data is being verified by all of the corresponding district nodes and every vote they agree upon are appended on the blockchain when block time has been reached.

Boot nodes: With the help of boot nodes each district node can communicate with each other. The boot node do not keep any state of the blockchain and is ran on an static IP so that the district nodes find its peers faster.

Conclusion

Thus we propose a system which is more reliable and secure and require less labour. Such systems will bring the more transparency in Indian Democracy and may as the secondary result of this system we can expect our country to go on top in World Democratic Index and also better government can be expected.

References

1. S. Shah, Q. Kanchwala, and H. Mi, “Block Chain Voting System,” 2016.
2. Christian, “Desain Dan Implementasi Visual Cryptography Pada Sistem E-Voting Untuk Meningkatkan Anonymity,” Institut Teknologi Bandung, 2017.
3. C. Dougherty, “[Vote Chain◌ள : Secure Democratic Voting],” 2016
4. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Www.Bitcoin.Org, p. 9, 2008.
5. D. A. Wijaya, Bitcoin Tingkat Lanjut. 2016.
6. H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. J. Kishigami, “Blockchain contract: A complete consensus using blockchain,” 2015 IEEE 4th Glob. Conf. Consum. Electron. GCCE 2015, pp. 577–578, 2016.
7. C. Cachin and M. Vukoliü, “Blockchain Consensus Protocols in the Wild,” 2017.
8. C. Meter, “Design of Distributed Voting Systems,” no. September, 2017.
9. A. Barnes, C. Brake, and T. Perry, “Digital Voting with the use of Blockchain Technology Team Plymouth Pioneers – Plymouth University,” 2016.
10. T. Martens, “Verifiable Internet Voting in Estonia,” October, pp. 1– 7, 2009.
11. Follow My Vote, “Why Online Voting.” [Online]. Available: https://followmyvote.com/. [Accessed: 01-Jan-2017].
12. L. J. Wu, K. Meng, S. Xu, S. Q. Li, M. Ding, and Y. F. Suo, “Democratic Centralism◌ள : a hybrid Blockchain architecture and its applications in Energy Internet,” pp. 176–181, 2017.
13. Gemalto, “Benefits of Elliptic Curve Cryptography,” no. March 2012.
14. D. Hankerson, S. Vanstone, and A. J. Menezes, Guide to elliptic curve cryptography. 2004.