International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

E-Voting using Blockchain Technology

Sumith S[1], T Sandra Sasidharan[2], Remya Rajan[3], Nithya Ray Varghese[4], Ajeesh S[5]

[1,2,3,4]B.Tech Student, Computer Science and Engineering, APJ Abdul kalam Technological University, Kerala, India
[5]Asst. Professor, Computer Science and Engineering, Mount Zion College Of Engineering, Kadammanitta, Kerala, India

---

Abstract - *Now a days crypto currency has become trending topic in software world. Crypto currency is digital asset designed to work as a medium of transaction that uses strong cryptography to secure financial exchange, and confirm the transfer of assets. Crypto currency is also known as decentralized digital money. Block chain stores transaction information which can be used to review the trustworthiness of transaction. The objective of this project is to use of block chain technology for transaction. Block chain is digital ledger of economic transactions that can be programmed to record financial as well as other transactions, it is difficult to forge. Since the information stored in block chain is not associated to personally identifiable information, it has at- tributes of anonymity. Block chain allows transparent transaction and verification. This block chain technologies characteristics are helpful in voting system that is strong, robustness, anonymity and transparency. Voting System is heart of our country. In this system fingerprint verification used to authenticate voter's identity.*

***Key Words*: Blockchain, Ethereum, Fingerprint verification**

1. INTRODUCTION

First and foremost, the ways of paper voting and E-voting maintain one thing in common, which is voters need to travel to the designated polling station to register their vote. The counting process of paper voting which completed manually or machine (physical counting) after the voting process. In contrast, E-voting is synchronously counting when each vote was cast. The last process will be the same to both that results by integrating all counts of each candidate from the polling stations. Since 1999, India has been one of the countries that have used EVMs for the election. Estonia was the first in the world to adopt an electronic voting system for its national elections. Soon after, electronic voting was adopted by Switzerland for its state-wide elections, and by Norway for its council election. For an electronic voting system to compete with the traditional ballot system, it has to support the same criteria the traditional system supports, such as security and anonymity. An e-Voting system has to have heightened security in order make sure it is available to voters but protected against outside influences changing votes from being cast, or keep a voter's ballot from being tampered with. Many electronic voting systems rely on Tor to hide the identity of voters. However, this technique does not provide total anonymity or integrity since many intelligence agencies around the world control different parts of the Internet which can allow them to identify or intercept votes. To resolve this limitations, blockchain technology is an irreplaceable existence. Nature of blockchain technology like an incontrovertible ledger, immutable, and distributed. Key features of blockchain technology are:

- Eliminate the central database. P2P Network that each node has the same blockchain (data) but distributed that resulting in no single point of failure.
- When a new data or so-called block creating, the previous block will be referenced by the new block that constructed an immutable chain which protects data from tampering.
- Control over half of the nodes in the network which made the system extremely secured. Furthermore, Ethereum brings additional enhancements while remaining the blockchain functionalities.
- Allow the developer to program and customize blockchain.
- Least CPU resources cost in terms of performance Moreover, with blockchain technology, the decentralized architecture and its consensus algorithm bring the security level to the higher than the centralized architecture (client-server).

Therefore, current research aims to investigate the importance of Blockchain technology for electronic voting to enhance the integrity, optimize the voting process, produce consistent voting results, and fortify the transparency of the voting system.

2. LITERATURE SURVEY

Nir Kshetri, Jeffrey Voas,[1] use digital currency analogy for voting. Here (Blochchain-Enabled E-Voting) BEV issues each voter a wallet containing a user credential. Each voter gets a single coin representing one chance to vote. BEV employs an encrypted keys and tamper-proof personal Ids. Require much energy to perform authentication and validation.

Ali Kaan Koc, Emre Yavuz, Umut Can Cabuk,Gokhan Dalkoloc, [2] building smart contract of ours, we have succeeded in moving e-voting to the blockchain platform and we addressed some of the fundamental issues that traditional evoting systems have, by using the potential of the Ethereum network and the blockchain structure. As a result of trials, the concept of blockchain and the security methodology which it uses, namely immovable hash chains, has become adaptable to polls and elections. There are some property that cannot handle solely using blockchain, for example authentication of voters requires additional mechanisms to be integrated.

F. Hao and P.Y.A. Ryan, [4] The idea of e-voting is considerably older than blockchain. So that, all celebrated examples to this point used suggests that of centralized computation and storage models. Esthonia may be a excellent example, since the govt of Esthonia is one in every of the primary to implement a totally on-line and comprehensive evoting resolution.

P. McCorry, S.F. Shahandashti, and F. Hao, [5] Switzerland is another one in all the few countries taking part within the electronic option trend. In Switzerland, celebrated for its widespread democracy, each national United Nations agency completes the age of eighteen will take an energetic or passive role within the elections, which can be command in totally different topics for several different choices. They need conjointly begun a politician work on a legal system known as remote option.

U.C. abuk, A. avdar, and E. Demokrasi [6] that Its necessary for US since elections will simply be corrupted or manipulated particularly in little cities, and even in larger cities placed in corrupt countries. Plus, large-scale ancient elections square measure terribly costly within the long run, particularly if there square measure many geographically distributed vote centers and countless voters. Also, the voters (mainly for members of organizations) can be on vacation, on a business trip or isolated for the other reason, which is able to create not possible for that specific citizen to attend the election and should lower the group action. E-voting are going to be in a position solve these issues, if enforced rigorously.

Estonian National Electoral Committee, [8] Their system remains in use, with several enhancements and modifications on the first theme. As reported, its presently terribly sturdy and reliable. They use sensible digital ID cards and private card readers (distributed by the government) for person-wise authentication.

E. Maaten [9] supply a secure selection atmosphere and show that a reliable e-voting theme is feasible victimization blockchain. Because, once e-voting is obtainable for everybody UN agency contains a laptop, or a transportable, each single body call may be created by individuals and members; or a minimum of peoples opinion are going to be a lot of public and a lot of accessible by politicians and managers. this may eventually lead humanity to actuality direct democracy.

3. EXISTING SYSTEM

Electronic Voting is the standard means of conducting elections using Electronic Voting Machines, sometimes called "EVMs" in India. India's Electronic Voting Machines (EVMs) have two main components (1) CONTROL UNIT, used by poll workers, which stores and accumulates votes, and (2) a BALLOT UNIT, located in the election booth, which is used by

voters. These units are connected by a 5 m cable, which has one end permanently fixed to the ballot unit. The system is powered by a battery pack inside the control unit. The ballot unit has 16 candidate buttons. If any are unused, they are covered with a plastic masking tab inside the unit. When there are more than 16 candidates, an additional ballot unit can be connected to a port on the underside of the first ballot unit. Up to four ballot units can be chained together in this way, for a maximum of 64 candidates. A four-position slide switch in the ballot unit selects its position in the chain. The Bharat Electronics Limited (BEL) and Electronics Corporation of India (ECIL) are the manufacturers of EVMs in India and the foreign companies in US and Japan supplying microcontrollers. They were introduced in Indian elections between 1998 and 2001, in a phased manner. The electronic voting machines have been used in all general and state assembly elections of India since 2004**.** Prior to the introduction of electronic voting, India used paper ballots and manual counting. The paper ballots method was widely criticised because of fraudulent voting and booth capturing, where party loyalists captured booths and stuffed them with pre-filled fake ballots. The printed paper ballots were also more expensive, requiring substantial post-voting resources to count hundreds of millions of individual ballots. Embedded EVM features such as "electronically limiting the rate of casting votes to five per minute", a security "lock-close" feature, an electronic database of "voting signatures and thumb impressions" to confirm the identity of the voter, conducting elections in phases over several weeks while deploying extensive security personnel at each booth have helped reduce electoral fraud and abuse, eliminate booth capturing and create more competitive and fairer elections. Indian EVMs are stand-alone machines built with once write, read- memory, read only memory. The EVMs are produced with secure manufacturing practices, and by design, are self-contained, battery-powered and lack any networking capability. They do not have any wireless or wired internet components and interface. The M3 version of the EVMs includes the VVPAT system.

In recent elections, various opposition parties have alleged faulty EVMs after they failed to defeat the incumbent. After rulings of Delhi High Court, the Supreme Court of India in 2011 directed the Election Commission to include a paper trail as well to help confirm the reliable operation of EVMs. The Election Commission developed EVMs with voter-verified paper audit trail (VVPAT) system between 2012 and 2013. The system was tried on a pilot basis in the 2014 Indian general election. EVMs and accompanying Voter-verified paper audit trail (VVPAT) are now used in every assembly and general election in India and a small percentage of the VVPATs are verified. On 9 April 2019, Supreme Court of India ordered the Election Commission of India to use VVPAT paper trail system in every assembly constituency but verify only about 2% of the EVMs i.e., 5 polling stations per constituency before certifying the final results. The Election Commission of India has acted under this order and deployed VVPAT verification for 20,625 EVMs in the 2019 Indian general election.

Fig 1: *Existing Voting System*

Disadvantages:

1) Physical security of machine
2) Secure storage of castes votes
3) Risk of vote tampering

4. PROPOSED METHODOLOGY

A voting system with a fingerprint verification is proposed in this project. The fingerprint recognition system consists of four stages: firstly, the sensor which

is used for enrolment & recognition to capture the biometric data. Secondly, the pre-processing stage which is used to remove unwanted data and increase the clarity of ridge structure by using enhancement technique. Thirdly, feature extraction stage which take the input from the output of the pre-processing stage to extract the fingerprint features. Fourthly, the matching stage is to compare the acquired feature with the template in the database. Finally, the database which stores the features for the matching stag. After the identification of the user it will process the voting system. We will be creating a web application for the process of voting. The voter selects the candidate and vote. The vote will be processed to the blockchain. The blockchain will be added to the blocks with specific hash values. So no data can be duplicated thus providing strong, robustness, anonymity and transparency for the project.

4.1 Voting

Electronic voting is a voting system that uses electronic means of casting and counting votes. Each voter has an unique ID number for voting purpose. The voter goes to a valve and receive a token, using the ID number. Each ID number is only grant to earn one token. Voter verification can be done by fingerprint recognition. Candidates list will displayed on web panel. The voter can vote online by dispatching the token to the account of the candidate they select. That voter cannot vote again, but the voter can examine the block chain to verify that the vote was correctly recorded, and also see the total votes for each candidate at any time. Live result will displayed at admin panel. Each vote is verified by the server, if valid then it digitally signed by the server for valid transaction. Invalid transaction where drops after verification.

4.2 Fingerprint Verification

Fingerprint verification is a process of confirming that a user is who they claim to be. It is one of the well known biometrics solution for authentication on computerized system. It is also known as fingerprint matching. In our system fingerprint verification used to validate voter's identity. Fingerprint matching having two steps i.e. feature extraction and fingerprint matching. Fingerprint Matching Algorithm uses ISO template.

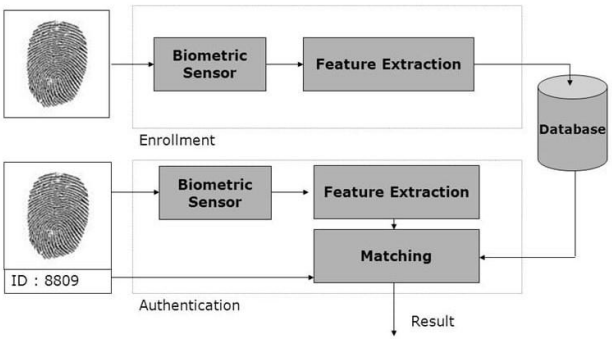


Fig 4.2: *Fingerprint Matching*

4.3 Blockchain

Since 2009, the blockchain technology revolution has come silently, Bitcoin which has been the first and one of the successful examples with the use of blockchain technology. Moreover, the author of Bitcoin was anonymous but leave a pseudonym called Satoshi Nakamoto (bitcoin white paper). According to the FT Technology reporter, Sally Davies, "Bitcoin creates Blockchain, email creates the internet. A massive electronic system allows the developer to develop applications with the Bitcoin, and currency is just one". Soon and later, in 2014, people realized that different kind of businesses other than cryptocurrency can use blockchain technology. Not with standing in 2018 currently, however, some people thought both Bitcoin, and blockchain is the same. The mission of blockchain technology is to redefine the "trust" of the system which eliminates middlemen like governments and corporations, that is, the next generations architecture – decentralization. With blockchain technology, the "trust" will be on the system or so-called smart code instead of middlemen who in charge both data privacy and security.

Here are 5 basic principles of the blockchain technology:

1. **Distributed database**. Each party on a blockchain has access to the whole database

and its complete history. No single party regulates the data or the information. Every party can validate the records of its transaction partners directly, without an intermediary.

2. **Peer-to-peer transmission**: Communication occurs straightforwardly between peers instead of through a central node. Each node stores and forwards information to all other nodes.
3. **Transparency with pseudonymity:** Every transaction and its respective value are visible to anyone with an access to the system. Each node, or user, on a blockchain has a unique 30-plus-character alphanumeric address that identifies it. Users can choose to remain anonymous or provide proof of their identity to others. Transactions occur between blockchain addresses.
4. **Irreversibility of records**: Once a transaction is inputted in the database and the accounts are updated, the records cannot be changed, because they are linked to every transaction record that came before them (this is basically where the term **"chain"** comes from). Various computational algorithms and approaches are deployed to ensure that the recording on the database is permanent, chronologically ordered, and available to all others on the network.
5. **Computational logic:** The digital nature of the ledger means that blockchain transactions can be tied to computational logic and in essence programmed. So users can set up algorithms and rules that automatically trigger transactions between the nodes.

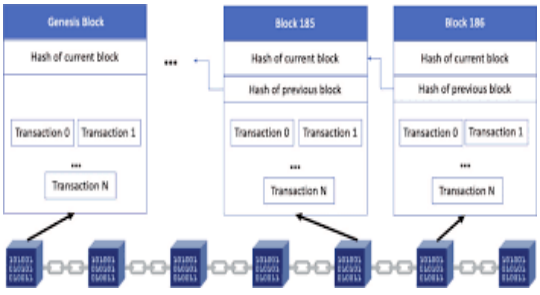


Fig 4.3: *Blockchain Structure*

4.4 Server

We use Ethereum stream to store for storing voters information and votes given by the voters. Ethereum asset are used for voting i.e for transaction. Webserver is just used for GUI of users and administrators for easy interface or access. Ethereum RPC-API are used for communication between webserver and Ethereum platform. Ethereum is an open source public blockchain based distributed computing platform featuring smart contract functionality. Ethereum provides a decentralized virtual machine, the Ethereum Virtual Machine (EVM), which can execute scripts using an international network of public nodes. The virtual machine's instruction set, in contrast to others like Bitcoin Script, is Turing-complete "Gas", an internal transaction pricing mechanism, is used to mitigate spam and allocate resources on the network. MetaMask is a browser plugin, available as the MetaMask Chrome extension or Firefox Add-on. At its core, it serves as an Ethereum wallet: By installing it, you will get access to a unique Ethereum public address, with which you can start sending and receiving ether or tokens. MetaMask is a browser extension that allows web application to interact with Ethereum wallet, allowing them to store and send any standard Ethereum-compatible tokens(so-called ERC-20 tokens).

4.5 REQUIREMENTS

Hardware requirements

- CPU: i5 Processor 64-bit 3.00 GHz 8.00 3.20 GHz
- RAM: 8 GB (or 16 GB of 1600 MHz DDR3 RAM)
- Storage: 500 GB. (600 GB for air-gapped deployments.) Additional space recommended if the repository will be used to store packages built by the customer.
- Fingerprint Scanner.

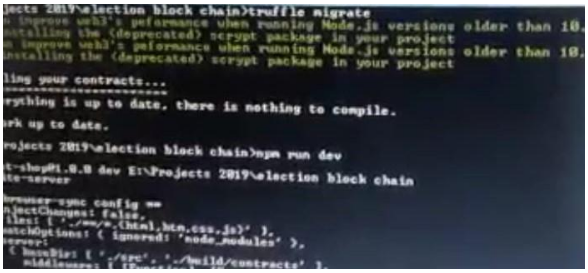
Software & system requirements

- Client environment may be Windows, macOS or Linux
- Python 3.6 IDE
- SQLite Database

5. SCREENSHOT OF PROPOSED SYSTEM

5.1 Ethereum

Here voting chain is created and started for further system process as shown.

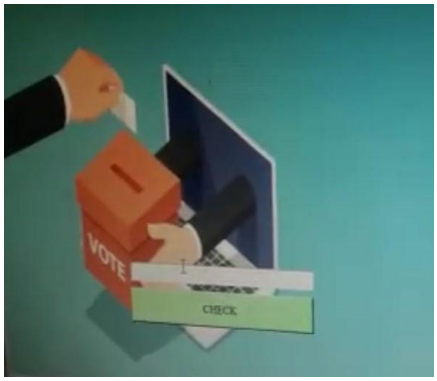


5.2 Home Page of Voting System

Here home page of our voting system is shown.

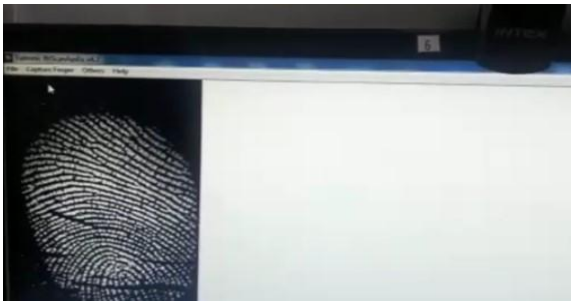
5.3 Voting Process Starting

Here while clicking on sign In button in home page voter can start voting process and voter have to check fingerprint for further voting.



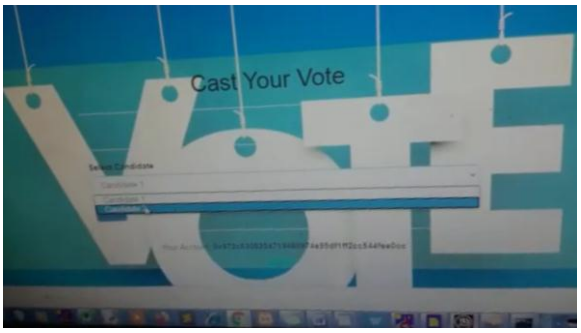
5.4 Fingerprint Verification

Here voter have to authenticate themselves by their registered fingerprint at the time of registration.

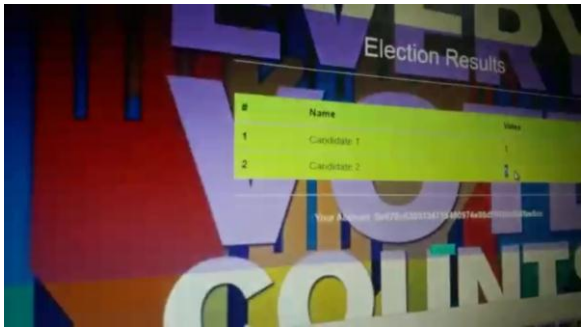


5.5 Voting

Here voter have to select candidate as per their choice for voting as shown.



6. RESULT ANALYSIS



Results of our proposed system shown on the basis of verification and voting count. In this, on the basis of security measures like Confidentiality, Integrity, Availability, Accountability, Non-repudiation, etc. the security analysis of the system carried out.

1)Confidentiality: The voting counts must be protected from external reading during the voting process. The association between recorded votes and the identity of the voter must be completely unknown within the voting systems.

2)Integrity: The computer systems (in hardware and system software) must be tamperproof. Ideally, system changes must be prohibited throughout the active stages of the election process. All data involved in entering and tabulating votes must be tamperproof. Votes must be recorded correctly.

3)Availability: The system must be protected against both accidental and malicious denials of service, and must be available for use whenever it is expected to be operational.

4)Accountability: All internal operations must be monitored, without violating voter confidentiality. Monitoring and analysis of audit trails must themselves be non tamperable.

5)Non-repudiation: Non-repudiation is the assurance that someone cannot deny the validity of something. Nonrepudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data.

7. CONCLUSION

A nation with less voting percentage will struggle to develop as choosing a right leader for the nation is very essential. Our proposed system designed to provide a secure data and a trustworthy E-voting amongst the people of the democracy. Block chain itself has been used in the Bitcoin system known as the decentralized Bank system. By adopting block chain in the distribution of databases on e-voting systems. One can reduce the cheating sources of database manipulation. Fingerprint verification used to authenticate voter's identity. This is useful towards secure voting system. As a result of our proposed system, the concept of blockchain and the security methodology which it uses, immutable hash chains, has become flexible to polls and elections.

REFERENCES

[1] Nir Kshetri, Jeffrey Voas Blockchain-Enabled E-Voting, 0740- 7459/18/33.00 2018 IEEE

[2] Ali Kaan Koc, Emre Yavuz, Umut Can Cabuk, Gokhan Dalkoloc "To- wards Secure E-Voting Using Ethereum Blockchain", 978-1-5386-3449- 3/18/31.00 2018 IEEE.

[3] C.D. Clack, V.A. Bakshi, and L. Braine, Smart contract templates: foundations, design landscape and research directions, Mar 2017, arXiv:1608.00771.

[4] F. Hao and P.Y.A. Ryan, Real-World Electronic Voting: Design, Analysis and Deployment, CRC Press, pp. 143-170, 2017.

[5] P. McCorry, S.F. Shahandashti, and F. Hao, "A smart contract for board- room voting with maximum voter privacy", International Conference on Financial Cryptography and Data Security.Springer, Cham, pp. 357-375, 2017.

[6] U.C. abuk, A. avdar, and E. Demir, "E-Democracy-The-Next-Generation- Direct Democracy-and-Applicability-in-Turkey.pdf.(Nov 2016).

[7] G. Wood, "Ethereum: a secure decentralised generalised transaction ledger", Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014.

[8] Estonian National Electoral Committee E-voting System, 2010. [Online].

Available: https://www.valimised.ee/sites/default/files/uploads/Eng/General Description E-Voting 2010.pdf.

[9] E. Maaten, Towards remote e-voting: Estonian case, Electronic Voting in Europe-

Technology, Law, Politics and Society, vol. 47, pp. 83-100, 2004.

[10] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system, [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[11] M. Hochstein, Moscows Blockchain Voting Platform Adds Service for High-Rise Neighbors, CoinDesk, 15 Mar. 2018; https://www.coindesk.com/moscows-blockchain-voting -platform-adds-service-for-high-rise - neighbors.