iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** III **Month of publication:** March 2022

DOI: https://doi.org/10.22214/ijraset.2022.41005

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

Blockchain Voting: A Comparative Analysis

Dr. C. Viji[1], Akash Kumar[2], Ayesha Noorayen[3], Humera Amjad[4], Mohammed Abrar[5]
[1, 2, 3, 4]*Department of Computer Science, HKBK college of Engineering, Bangalore, India*

Abstract: ***The electronic voting has emerged over time as a replacement to the paper-based voting to reduce the redundancies and inconsistencies. The historical perspective presented in the last two decades suggests that it has not been so successful due to the security and privacy flaws observed over time. This project is about decentralizing authority to record, count and verify votes and the voters, rather than having a central authority. We are using blockchain technology which is a distributed database. With its immutability property and decentralized architecture, it can run and support a voting scheme that is open, fair and independently verifiable. The project will be developed in Ethereum framework which primarily uses Solidity as a language. Ethereum's backbone is its decentralized virtual machine called Ethereum Virtual Machine. The application will be deployed on the thirdweb(web3.0). Overall this project is a potential roadmap for blockchain technologies developing in the nation to support complex applications.***

Keywords: Blockchain, Cryptography, Cryptocurrency, Ethereum Framework, Solidity, Decentralization, Hashing, Dapp, Web3, Digitalizing.

I. INTRODUCTION

Considering the election system in India, where EVM is used as a voting system, we try to bring a solution that makes the democracy stronger by ensuring each and every vote matters and thereby creating a safe, secure and transparent system with the help of Blockchain.

This can be done by making the election system more accountable, transparent and inclusive. These principles are piled by several by various electoral process related obligations and various key-rights and freedoms and these are derived from public international law.

Any election can be called as accountable, transparent, inclusive and above all free only if:

1) Transparent Voting: Providing transparency at every step for people's faith in democracy.
2) The probity of Ballot: the voting system should be secure, immutable and mechanism should be provided to check the probity of ballot.
3) Privacy: Ensuring privacy of each and every voter.
4) Accessibility: Every eligible voter must have the accessibility for proper voting.
5) Equality to all contestants: Every voter should be treated equally and fairly.
6) Assuring stakes to all Stakeholders: Assuring everyone gets the right to vote.
7) Onto Voting: One voter one vote.

II. RELATED WORKS

This analysis deals with the existing voting system in the country, the EVM frauds and the votes getting compromised. This raises questions over the democratic systems and political parties which are popular in headlines. We are proposing a system which ensures transparency traceability and flexibility.

A. Electoral fraud

Election manipulation, and vote rigging are popular in news these days. There is a simpler way to manipulate the votes like: pressing the button for someone else.

The election commission has ordered re-polling in Haryana's Faridabad after video clips emerged in a polling agent of a party member going up to the balloting unit and pressing the button before voters had a chance to do so. This sort blatant fraud is supposed to be prevented by the commission's micro-observers and by polling agents of other party.

Videos and reports from a few places around the country have found EVMs being transported without the appropriate level of security mandated by the guidelines. This has led to the fears the ruling party has not hacked the EVMs that people voted on but is somehow trying to swap actual EVMs with other ones.

B. EVM Frauds

The devices that India relies on to conduct elections, Electronic Voting Machines, have been in the news over the last few years, as politicians and activists have raised questions about whether they are at risk of being tampered with. With counting of votes set to take place on Thursday, the issue has dominated the news cycle, particularly with fresh allegations that EVMs are being transported without appropriate security.

Electronic voting machines (EVMs) were supposed to be the cure for the malady of booth-capturing in elections in India, but in the present form of use they have only worsened the problems. Moreover, EVMs also do not meet the legal requirements set out in the Information Technology Act, 2000.

EVMs, as they are being used by the Election Commission of India (ECI), create worries about the very legitimacy of the choice of governments through elections based on them, and raise questions about whether the ECI has become partisan in its defense of EVMs.

The duties of the ECI as set out in Article 324 of the Constitution include ensuring that elections conducted by it are free and fair, and reflect the will of the voters.

To be considered free and fair, the international standards an election has to meet are:

1) Individuals have to be accurately identified as eligible voters who have not already voted;
2) Voters are allowed only one anonymous ballot each, which they can mark in privacy;

There are three parts to the electronic voting machine.

The first is the control unit, which is held by the election officer at every booth. This collects and records each vote, and has a battery so that the machine doesn't depend on erratic power supply to work. The second is the balloting unit, which is a panel with a series of buttons next to which are the names, party symbols and, this year, photos of candidates.

Once voters have pressed the button of the candidate, a paper slip is generated and is displayed for seven seconds before dropping into a storage box. This Voter Verifiable Paper Audit Trail machine allows voters to check whether the party they selected was the same as the vote that the EVM registered. Later, these slips can then be audited against the votes actually counted by the EVM to ensure they tally.

Most importantly, no part of the EVM is "networked". These are extremely simple machines, like pocket calculators, with no connection to the internet, no operating system and no way of being altered without physical access to the machines.

However, these EVM machines can be hacked in two ways, a) Either the display can be tampered, b) The electronic chip can be hacked to alter the entire data.

III. LITERATURE SURVEY

Voting is an essential part of any democratic system. It's the most important tool which makes the government for the people by the people and to the people. Until now the paper ballot and the EVM machine are in use in most of the countries across the world. Where the voters used to cast their votes on the paper or on the EVM machine which were later counted at the end of elections. The biggest drawback of this system is that the votes here cannot be automated instead voters have to physically go to the location and cast their votes. This type of voting makes the entire process very time consuming and expensive. Above all the process is not so secure, transparent and flexible and many questions have been raised on this issue.

This paper provides an alternative way for the existing voting system which has its system decentralized with the help of blockchain technology.

We can opt for online voting based on blockchain which is gaining momentum in modern society. It eliminates the need to print ballot papers or open polling station voters where they can vote from anywhere around the globe with an internet connection.

1) Paper titled "Blockchain Based E-Voting System" proposed an authorized secret-ballot election that would guarantee a secured, robust and transparent system for voting. This system has the potential to significantly optimize the cost and increase the voter turnout. There is no need to print the ballot papers and the voters need not to travel all the way to the ballot location. There are new threats being introduced here nonetheless, as we are moving the system online. Now a single vulnerability will lead to a large scale of manipulation of votes. Blockchain technology comes to the ground to overcome these issues which offer decentralization of the entire process by providing several decentralized nodes for electronic voting. This system also ensures the privacy of voters as the data is mainly hashed.

2) Paper titled "E-Voting Systems using Blockchain: An Exploratory Literature Survey" proposes blockchain with interconnected nodes that have their copy of distributed ledger having history of all the casting of votes. Data is processed and put in block through a process called Mining. Every block contains a hash of the previous block hence forms a chain of blocks. Estonia has been using electronic voting since 2005. The basis of the system is a national ID card given to all citizens. The votes cast is in encrypted form which is further decrypted at the time of counting and the election results is produced. This system does not ensure that there is no possibility of malicious attacks that compromise the client-side machine by changing the voter's votes without voter's knowledge. Another possibility is of the server-side attack which can alter the votes. Therefore, this system raises concern over the security of the votes and thereby the election is not fair.
3) Paper titled "Implementing Electronic Voting System With Blockchain Technology" talks about multiple features of the decentralized system like secure ecosystem, consensus algorithm, distributed ledger and the blockchain being chronological and time stamped. There are two blockchain platforms: Permissioned and permissionless blockchain system. Permissioned blockchain are those where everyone is allowed to participate in any transaction whereas in permissionless blockchain everyone is allowed to set their node and validate a transaction. Ethereum (also known as World Computer) is a permissionless blockchain platform which provides options to build decentralized applications which also makes every program and data. Ethereum blockchain has two primary components: a) Database & b) Code. In the voting system based on Ethereum blockchain, each vote is counted as a transaction which are public and available for verification. The smart algorithm used to verify that all the nodes within the network have same data copy and no data is invalid is called 'Proof of Work".

IV. BLOCKCHAIN PLATFORMS

A. *Two types of Blockchain:*

Permissionless Blockchains (trustless or public blockchains) are open networks available for every node to participate in validating transactions and data in blockchain. These are fully decentralized across several parties. Whereas in Permissioned blockchains (private blockchain or permissioned sandboxes) only previously designated parties or members take part in the data validation. They are mainly developed by private entities and lack anonymity. Though they have no central authority but a private group authorizes decisions.

B. *Ethereum framework and Solidity:*

Ethereum (World Computer) blockchain platform is used to build decentralized applications which provides universal accessibility and is verifiable. It's a globally distributed ledger. Every transaction in Ethereum requires gas, which makes it free from spams and useless valueless transactions. Database and Code are two primary components of Ethereum blockchain.

C. *Some Terminologies in Ethereum*

1) *Ethereum Address:* It is the identity on the Ethereum blockchain network of the form 00123lkdfsweir345845324kjljjasl which is associated with a primary key.
2) *Gas:* It's a small amount of ETH that we have to pay for every transaction.
3) *Ether and Denominations:* It is the native currency for Ethereum blockchain.
4) Smart Contracts: The digital agreement between multiple parties written digitally as code.
5) *Ethereum Account:* They are of two types:
a) Externally Owned Accounts
b) Contract Account
6) *Gas Price:* It is the price per unit ether.
7) *Ethereum Virtual Machine:* A powerful 256-bit Turing machine that is capable of running EVM Byte code. It is crucial to consensus engine and the part of Ethereum System.

D. *Hyperledger Fabric*

Hyperledger Fabric is a distributed ledger technology with a modular architecture. This will increase the HLF Degree of confidentiality, flexibility, resilience and extensibility. Anyone can adopt it as an enterprise framework industry. This fabric enables plug-and-play components such as consensus and membership services. Sustainable chain code the business logic of the system is hosted through the container. To justify the complexity that exists throughout the industry and to give HLF more flexibility to the designed developers Various pluggable components. The fabric uses the portable concept of membership an authorized model that integrates with industry standard identity management. You can also make dough Channels for groups of participants Another transaction book.

V. PROPOSED SOLUTION

As we see there are so many questions raised on the authenticity of the election which also makes us a trust deficient society. So, in the current scenario and the given constrains that we have, we propose a blockchain based voting system for the democratic election happening in the country. This will be a great tool to deal with the trust issues of the societies and engage people more in the democratic process.

The approach towards the problem is divided into three main phases. These three main phases are as follows:

1) Voter Registration
2) Election Announcement and Candidate Registration
3) Voting and Results

We will be using Hyperledger fabric as a blockchain plat-form for this solution. Chain code in Hyperledger fabric consists of models and controllers. The model represents real-world objects in the form of OOPs classes and controllers are responsible for carrying out the transaction over these models. Our solution consists of five models:

a) Admin model: Defines Officials involved in the election process
b) Voter model: Defines Voter
c) Candidate model: Defines Candidate
d) Election model: Defines Election
e) Voting model: Defines Vote Transaction

Admin models as it deals with all officials, any time a new officer has to be added to the system admin model is instantiated. Admin model can be used to define all officials including the election authority and verification authority.

A. Voter Registration

Registration of new voters in our proposed system:

1) *Application:* Voters fill out applications for a new VoterId.
2) *Verification:* Verification by many officers who are selected randomly for approving applicants.
3) *Voter Id Assignment:* If the application is approved a permanent Voter Id is assigned to the user and an entry is added to a Global State Database.

Here the voter model will be used to instantiate a voterblock.

Voter Model Fields:

a) Id - Voter Id
b) Voter Name - Name of Voter
c) Region Code - Zip Code of the region where voter's home address.
d) Voting Phase - Next Election voter can participate
e) Voting Permission - It is set to true only on election day
f) Voting Status - It is to check if the voter has voted or not
g) Validation Status - It marks the verification by authorities

B. Election Announcement and Candidate Registration

This phase has following steps:

1) Election Announcement: Election is announced for a particular region.
2) Voters Notification: Voters of the region where election is announced are notified of the election.
3) Candidate Registration: Candidate fills new application for contesting election.
4) Candidate Verification: Verification by many officers who are selected randomly for approving credentials of applicants. Each and Every transaction is noted on the National Election Blockchain and State Database.
5) Candidate Id Assignment: Approved Candidate will be assigned Id making him eligible to contest for the particular election.

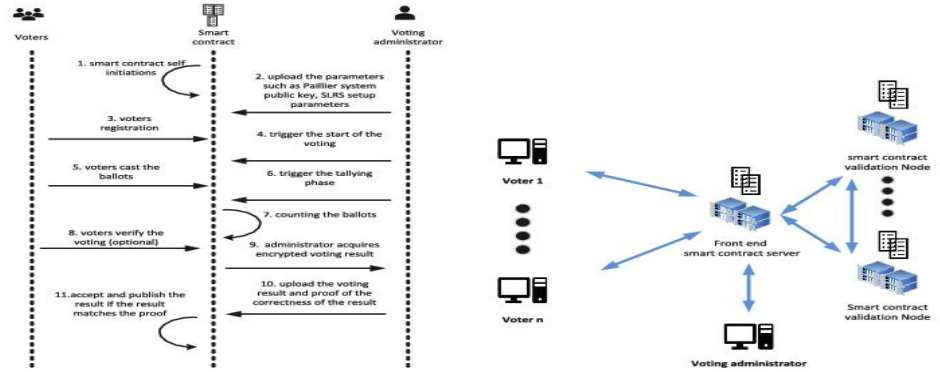
Here the election model & candidate model will be used to instantiate an election and candidate block.

Election Model Fields:

a) Id - Election Id
b) Region List - List of region zip codes for which election is being held.
c) Election Date - Date of the election.

Candidate Model Fields:

- Id - Candidate Id
- Candidate Name - Name of Candidate
- Candidature Phase - Election Id in which candidate is contesting
- Candidature Status - Last Standing Position of candidate
- Total Votes - Votes casted in the name of candidate
- Validation Status - It marks the verification by authorities



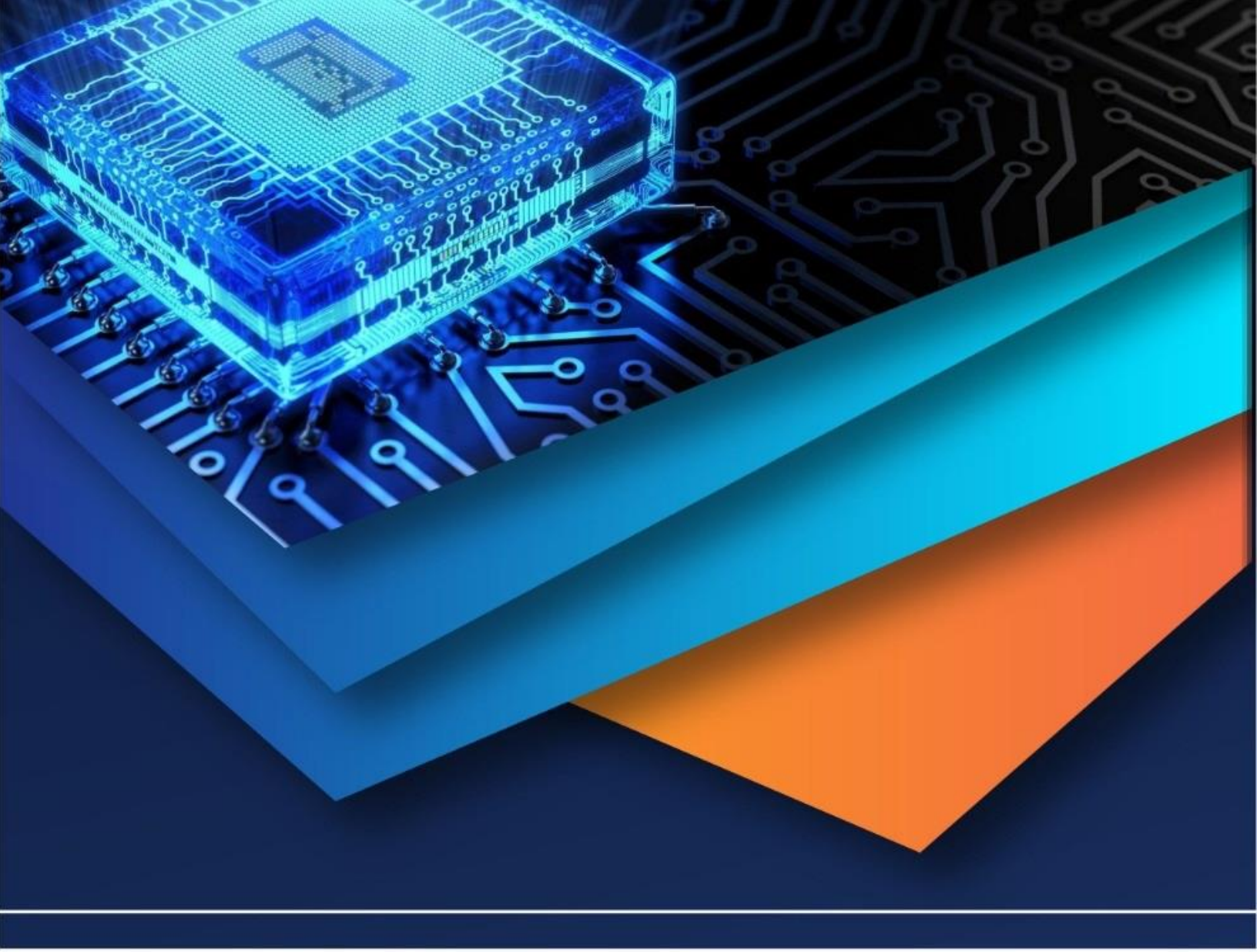
(a) The voting protocol diagram.(b) The blockchain evoting system.

VI. CONCLUSION

Idea of harnessing the prowess of Blockchain to make E-Voting more secure and efficient has merit to it. Security and Convenience is the key that makes the user comfortable and also eliminates the barrier between the voter and voting system in any case where voting takes place. Blockchain as a technology makes it possible. Blockchain not only has the power to make the process more digitally transparent but also make it more secure by being immutable. In this paper, we have proposed and implemented a blockchain-based electronic voting system that utilizes hyper-ledger to conduct secure elections while guaranteeing users privacy. By comparison of Ethereum and Hyperledger, it has been observed that Hyperledger is more efficient than Ethereum in most of the performance metrics and also it being permissioned chain it allows to maintain privacy of the voter.

REFERENCES

[1] Abhishek Kaudare, Milan Hazra, Anurag Shelar and Manoj Sabnis "Implementing Electronic Voting System with Blockchain Technology"
[2] "Supporting free and fair elections," https://www.usaid.gov/what-wedo/democracy-human-rights-and-governance/supporting-free-and-fairelections, accessed: 2020-01-24.
[3] "Can blockchain change the election scenario in India?" Available at https://link.medium.com/kgJJ2No5F3, accessed: 2019-12-22.
[4] "Features of blockchain technology," Available at https://guide.freecodecamp.org/blockchain/features/, accessed: 2020-01- 26.
[5] "An introduction to hyperledger," Available at https://guide.freecodecamp.org/blockchain/features/, accessed: 2020-01- 26
[6] S. Haber and W. S. Stornetta, "How to time stamp a digital document," in Advances in Cryptology-CRYPTO' 90, A. J. Menezes and S. A. Vanstone, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1991, pp. 99–111.
[7] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, Tech. Rep., 2019.
[8] G. Albeanu, "Blockchain technology and education," in The 12th International Conference on Virtual Learning ICVL, 2017, pp. 271–275.
[9] R. Cramer, R. Gennaro, and B. Schoenmakers, "A secure and optimally efficient multi-authority election scheme," European transactions on Telecommunications, vol. 8, no. 5, pp. 481–490, 1997.
[10] P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in International Conference on Financial Cryptography and Data Security. Springer, 2017, pp. 357–375.
[11] N. Pandey and N. Singh, "Blockchain based voting system can better the way of elections in India."
[12] M. B. Verwer, I. Dionysiou, and H. Gjermundrød, "Trustedevoting (tev) a secure, anonymous and verifiable blockchain-based e-voting framework," in International Conference on e-Democracy. Springer, 2019, pp. 129–143.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY