

## E – Voting using Blockchain

Bindu Aradhya Janagani<sup>1</sup>, Udeda Suchithra<sup>2</sup>, Harsh Mohan<sup>3</sup> and Dr. Annapurna D<sup>4</sup>

<sup>1-4</sup>Department of CSE PES University Bengaluru, India

Email: binduaradhya07@gmail.com

**Abstract**—In a democratic country like India, voting has a huge role in selecting government officials and representing the citizen's opinions and how the governing body should work. However, there are many loopholes in the process that need to be resolved. A few of them are event costs, vote tampering, fake vote casting, etc. To handle the challenges, technological intervention can be a great potential in transforming the scenario. There will be no need to print ballot papers or set up polling stations—voters can vote from anywhere with internet access. Even though using the electronic mode, we have to face problems like maintenance and reliability. In the proposed method, using blockchain technology and adopting new protocols we can enable the system to be resilient to vulnerabilities and at the same time solve the purpose. This decentralized system comes to rescue and backs all the downsides of traditional voting.

**Index Terms**— Hyper-ledger fabric, Django, E-voting, Cryptographic Hashing.

### I. INTRODUCTION

Voting is a process of making collective decisions or expressing opinions between a party or group of people. Election campaigns and debates are often followed by the voting process. In the event of a vote, the candidate is the person who contests in the election and the voter is the person who votes for the candidate. Generally, a voter can vote according to the candidate list. The votes must not be signed and marked by voters in private constituencies in order to maintain anonymity. Clubs, non-governmental organizations, and voluntary organizations also use voting.

The traditional ballot voting system did solve the purpose of selecting a leader but there were a lot of malpractices followed in the system. This made it highly unreliable. The most popular issue that is often dealt with by the election commission is ballot tampering. Intentionally spoiling or falsifying ballots to prevent voters from enabling their right to vote or pretend that they have voted for someone other than the candidate for whom they actually intended. In 2020, a team of Stanford political scientists analyzed roughly 4.5 million voter records from the state of Washington for evidence of ballot fraud involving deceased individuals. They found 14 cases where a ballot may have been stolen and submitted on behalf of someone who had died, and even these cases may not have been fraud-related. [1]

### II. INCENTIVE FOR SET UP OF MODEL

It is often observed that people living in a faraway place from their registered constituency fail to appear for casting their vote. Through the influence of money and power, the parties capitalize on this situation in an attempt to carry out false practices. However, these situations are kept away from the media eye but happen in large numbers on the ground level at every phase.

Mis-recording of votes is another issue, where votes are recorded electronically or mechanically and then altered to meet requirements. This is a total breakdown of democratic rights. Also, the current system requires huge manpower and doesn't enable a remote voting feature. All these issues play a very important role in designing a sustainable system by ensuring at most care and electing the right leader in the public's genuine interest.

### III. RELATED WORK

The current system i.e the manual voting system using the EVM, consumes a sumptuous amount of manpower and it also lacks the option of remote access which proves to be a major drawback. Major challenges faced in the approach were: Transaction speed limit, Ethereum being a public chain - trust issue's, Ethereum fee fluctuations, scalability. Greater storage and processing overhead due to different blockchain for each candidate. Usage of a single blockchain can improve performance [2].

The design algorithm used is distributed node architecture large-scale voting scenarios with national nodes managing constituency nodes which in turn manage local nodes. This can be further improved by using Hyperledger Sawtooth to parallelize transactions [3].

The proposed system consists of greater delay as secret message provided by each voter has to be verified by the TTP with the election commission, which then generates a reference number that can be used to view candidates and cast a vote [4].

The proposed system utilizes elliptical curve cryptography in which voter generates signature of their vote block using a private key, with the signature verified using the voter's public key present in a Public Key Infrastructure database [5].

Proposed system consists of a district node which manages the smart contract of the boot node. Frameworks recommended are Exonium. Quorum and Geth [6].

### IV. PROPOSED METHODOLOGY

The model works at the institute level to provide a digitalized remote experience to users with complete trust and hence proving the lucrative use of Blockchain and other Cybersecurity techniques. We will also be using the Hyperledger fabric framework to uphold the security and immutable nature of our election system.

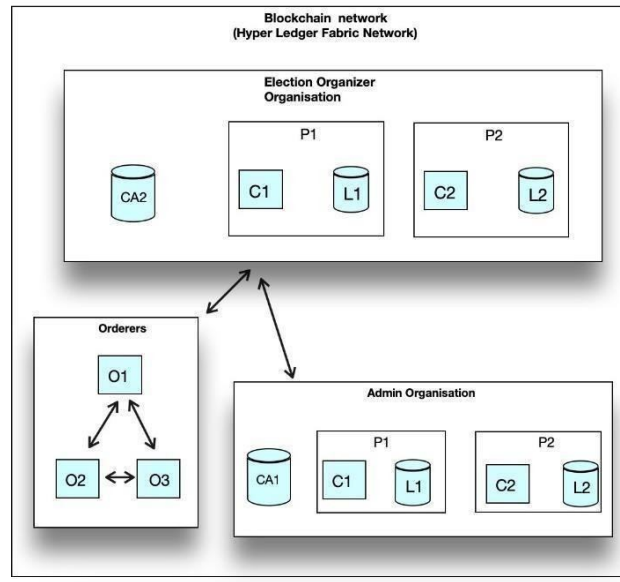


Fig.1.Blockchain network analysis-situs

Public record of votes, results and election organization is put out in ledger which functions as display board. The structural configuration indicates the business logic and the ledger state. Whereas the fabric certification authority is controlled by its own configuration as shown in CA1 and CA2. The functions of network analysis are identity creation for vote collectors and integration of these applications with the ledger. This is done by the two configurations namely election organizer and election manager. In the current implementation, the admin organization is not using CA1 but this can be amended in the future study. Supplementary redundancy is given

by the peers P1 and P2, that is if one peer is not functional the other takes over. The majority of the organization should accept the action to modify the ledger. In our scenario there are two peers, though this trait can be modified.

For instance, the configuration can be made in a way that only one organization (Election organization or admin organization) ought to accept the proceedings or to make firm that all bodies should agree on it. Furthermore, considering orderers, although if one goes down inside the network the transaction is made and it is controlled by raft protocol.

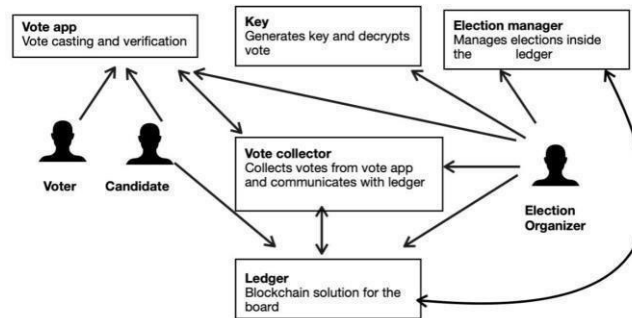


Fig.2.Architecture Diagram

## V. IMPLEMENTATION

The cryptographic libraries such as signature (DSS), hash (SHA-256) and Public key (ECC) are used. The voting interface contains a field which prompts the user to fill in their private key, this is used to validate the voter's authenticity. On successful verification the voter is allowed to cast the vote, the candidate description and party name is displayed sequentially. A random voter ID is generated by the system in order to store the transaction information and create the block without tampering. Upon successfully casting the vote from users end, the data is carefully collected and encrypted using the SHA 256 algorithm to support the Fabric framework. The algorithm is an unkeyed cryptographic hashing function which takes in input of a varying length and generates a 256-bit long output (It is the first and most widely used algorithm in various blockchains including bitcoin).

The backend of the page is built using Django as it takes less amount of storage compared to Docker and the efficiency in terms of speed is comparatively good. The tallied votes are displayed to all the users to maintain transparency.

Elections for different events can also be conducted by giving various group permissions like adding log entry, changing content type, viewing session, modifying vote backup and so on.

## VI. RESULTS

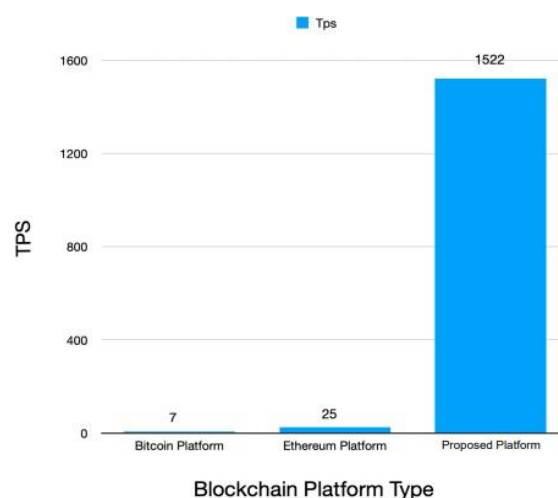


Fig.3.Comparing TPS (Transaction per second) for different blockchain platforms

The speed of processing plays a vital role for storing the transactions and this varies widely among different platforms. The transaction per second (TPS) is the measure of scalability of the network. To determine TPS average transaction time, block size and block time (time taken to create a new block in the chain) should be known. A lot of traditional platforms like Bitcoin and Ethereum take up to 7 TPS and 25 TPS respectively. Whereas our model which works on Hyperledger framework takes 1522 TPS this value is comparatively high and is very much suitable for handling for a large populated country like India. The predominant reason for such a huge variation is that in other platforms the successful nodes need to be validated by the minors, where the first need to compute the nonce value and then verify the transaction whereas there is no role of miners in the fabric as it is a public ledger and relies on the SHA 256 algorithm.

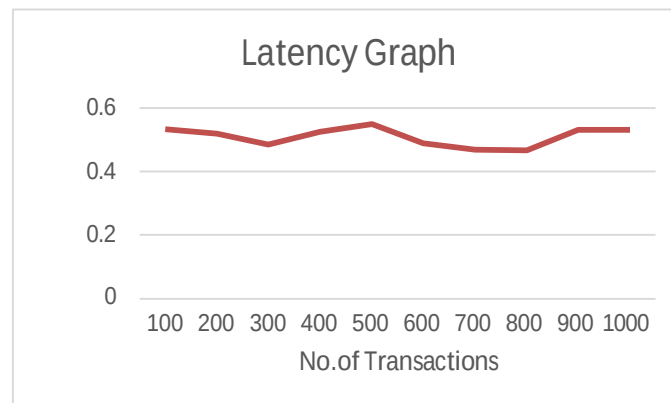


Fig.4. Graph depicting the latency Vs number of transactions

On performing various tests on the built model and analyzing the statistics for different samples ranging between 100 and 1000 group sizes, we have observed the average delay being very minimal. An average of 0.53159 seconds latency was observed. The model also has notably high transaction rates. With the procured results the system can be a good player in solving the challenges of the traditional voting system.

## VII. CONCLUSION AND FUTURE WORK

The project represents a simple and efficient way to conduct the electronic voting without tampering of votes. There will be negligible scope for malpractices and will reinstall trust among the voters in the election procedure. The suggested e-voting system was created and put to the test with the intention of determining whether a decentralized solution is feasible and could meet the most stringent requirements of both public environments and private corporate consortium. Preliminary findings show that blockchain satisfies e-voting scheme requirements for transparency, consistency, and resilience. Additionally, it is apparent that blockchain technology offers a breakthrough in process automation that is secure and unchangeable. The Hyperledger platform, which is used by huge MNC's like Walmart, Visa, Huawei etc., is a framework for handling supply chain by maintaining transparency and traceability within the network.

As a part of future work, over our development and research phase we understood that at one point of time the admin has to control over the decision making from the registered votes, to overcome this linking a permission-less chain to store all the information secured from the private chain will be good. This allows the chain to be public and keep adding blocks as and when a new vote is registered. This allows the chain to be publicly viewed and has no scope for tampering. We are yet to look at the other side of such development and understand the downside to. This will be taken up as our future work.

## REFERENCES

- [1] <https://siepr.stanford.edu/news/dead-people-dont-vote-study-points-extremely-rare-fraud>
- [2] Ahmed Ben Ayed "A conceptually secure blockchain based Electronic Voting System" (IJNSA) Vol.9, No.3, May 2017.
- [3] Patil, Harshal and Ladkat, Prathmesh and Jituri, Abhishek and Desai, Rohit and Shinde, Dr. Swati, Blockchain Based E-Voting System (May 18, 2019). Proceedings of International Conference on Communication and Information Processing (ICCIP) 2019.
- [4] Bijan Ganji Jamehshooran, Awaluddin. M. Shaharoun, Habibah Norehan Haron "Assessing Supply Chain Performance through Applying the SCOR Model" Vol 4, No 1 (2015).

- [5] Yi,H. Securing e-voting based on blockchain in P2P network. J Wireless com Network 2019, 137(2019).  
<https://doi.org/10.1186/s13638-019-1473-6>
- [6] F.P Hijalmarsson, G.K. Hreidarsson, M. Hamdaqa and G.Hjalmtysson, "Blockchain- Based e-voting system, 2018 IEEE 11<sup>th</sup> International conference on cloud computing(CLOUD), 2018, pps.983-986, doi:10.1109/CLOUD.2018.00151.
- [7] <https://www.mdpi.com/>