2020 International Conference for Emerging Technology (INCET)
Belgaum, India. Jun 5-7, 2020

Implementing Electronic Voting System With Blockchain Technology

1st Abhishek Kaudare
B.E. Information Technology
Vivekanand Education Society's Institute of Technology
University of Mumbai
Mumbai, India
abhishek.kaudare.dev@gmail.com

2nd Milan Hazra
B.E. Information Technology
Vivekanand Education Society's Institute of Technology
University of Mumbai
Mumbai, India
milanhazra234.mh@gmail.com

3rd Anurag Shelar
B.E. Information Technology
Vivekanand Education Society's Institute of Technology
University of Mumbai
Mumbai, India
anurag.shelar1000@gmail.com

4th Manoj Sabnis
Associate professor, Information Technology
Vivekanand Education Society's Institute of Technology
University of Mumbai
Mumbai, India
manoj.sabnis@ves.ac.in

***Abstract*—Elections and voting are the basic mechanisms of a democratic system. There have been various attempts to make modern elections more flexible by using digital technologies. Basic characteristics of free and fair elections are intractability, immutable, transparency and the privacy of the involved actors. This corresponds to a few of the many features of blockchain-like decentralized ownership, the immutability of chain, anonymity and distributed ledger. This work-in-progress paper attempts to do a comparative analysis of various blockchain technologies under development and propose a 'Blockchain based Electronic Voting System' solution by weighing these technologies based on the need for the proposed solution. The main aim of this paper is to present a robust blockchain-based election mechanism that not only will be reliable but also flexible according to present needs.**

***Index Terms*—E-Voting, Blockchain, Ethereum, Hyperledger, Distributed Ledger Technologies**

I. Introduction

This paper considers the Indian Election System for study and tries to propose a solution for the Indian Election System by limiting the scope. The most important principle that defines an election is that they must represent the free expression of the will of the people. This kind of expression is only possible if the elections are 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. [1]

A. Characteristics of free and fair elections

Any election is eligible to be considered free and fair if it features the following characteristics:

1) **Transparency:** Any Election has to be transparent at every step. Everything should be available for scrutiny to all its stakeholders.
2) **The integrity of Ballot:** The votes cast in a ballot should be secure and immutable. There has to be a mechanism to check the integrity of the ballot.
3) **Privacy of Voter:** Votes cast by voters should be kept private to them and there should be no way that votes to voter match could be found.
4) **Accessible to every voter:** An election must be organized so that it should be accessible to every eligible voter.
5) **Equal Treatment to all Contestants:** Every contestant should be treated equally and there should be no unfair procedural advantage to any of the contestants.
6) **Ensuring Eligibility of all Stakeholders:** It should be made sure that there are necessary checks for verifying the eligibility of all voters and contestants.
7) **One Voter One Vote:** Every voter should have only one vote.

B. Features of Blockchain

The various features of blockchain and innumerable applications can be implemented at multiple levels of voting. Decentralized technology plays an important role in how citizens can get the knowledge of candidates, how secure and transparent our voting systems are and how blockchain can secure them. With the help of blockchain, it is possible to keep track of voter's eligibility and legitimacy. [2]

Some of the features of Blockchain are as follows:

1) **Decentralized Technology:** The network is decentralized. No Individual is solely responsible for governing the network. Rather it is maintained by peer nodes making it decentralized. [3]
2) **Secure Ecosystem:** Decentralized network has no central authority hence no one can tamper with it without

978-1-7281-6221-8/20/$31.00 ©2020 IEEE

a consensus. Encryption adds layer of security to the system.

3) **Consensus:** Consensus algorithm is the spine of any decentralized network. Consensus algorithms are at the core of this architecture.
4) **Distributed Ledger:** Blockchains use Distributed Ledger Technology (DLT) to store and access the data around.Unlike traditional databases, distributed ledger do not have a central database or administration functionality.
5) **Chronological and Time stamped:** Blockchains, ideally, are just very sophisticated linked lists where each block is a repository that stores information pertaining to a transaction and also links to the previous block in the same transaction. These blocks are arranged in an order and are time-stamped during creation to ensure a fair record. [4]

II. Working Of Blockchain

A blockchain consist of blocks holding information arrange in a series. Blockchain is basically a ledger distributed over the network. Blockchain has a robust architecture of linked list that is immutable. Every block has some data hash of previous block and hash of itself. Let's take an example: The Bitcoin blockchain stores the details about a transaction that contains sender-receiver and amount. A block also has a hash, you can compare a hash to any type of bio-metric value. The contents of the block are always unique. Once the block is being created, the hash is being calculated. Any Modification with the block will cause the changes in the hash that is created by the block, As hash is the essential part of the blockchain. The third element inside a block is the hash value of the previous block. This effectively creates a chain of blocks with each block pointing previous block and thus making it computationally impossible to mutate any block. [5]

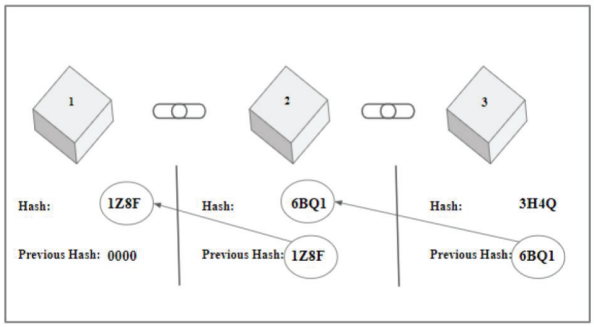

Fig. 1. Basic Working of Blockchain

In figure 1 We can see there are 3 blocks. Each block has a hash and hash of the previous block. The block number 3 points to block number 2, and block number 2 points to block number 1. The first block is called the Genesis block. Tampering with any of the blocks it will cause a change in the value of hash due to which the whole chain will be compromised. Security of Blockchain comes from its creative hashing and the proof-of-work mechanism and one more way that blockchain secures itself is by being distributed. Rather than using a central entity to manage the chain, blockchain uses peer to peer network and every peer is allowed to join, when someone joins the network they get a full proof copy of the blockchain. The node can use this to check that everything is in proper order and nothing is tampered. When someone creates a new block. The block is sent to every peer in that particular network. Each node then rectifies the block to make sure that it has not been altered. Once the verification is done by all the nodes then a consensus is generated. So to tamper blockchain, all the blocks in the chain need to tamper which is not possible by any means of computational power.

As the blockchain has progressed there is another interesting concept of Smart Contracts. [6] They have various applications and forms in different types of blockchain. If we are using Ethereum then we have to write Smart Contracts. In Hyperledger we write Chaincode. [7]

III. Basics of Different Voting Systems

Around the world different types of voting systems are used for different applications including elections, plebiscite, board decisions, etc. Some of the methods used for voting are:

1) **EVM Based System:** Electronic Voting System is the one in which we use a machine to handle the process of voting in India. EVM consists of two units namely control unit and ballot unit which are connected by a cable. The polling officer is in charge of the control unit. The ballot unit is for the voters to cast their votes. These units are sealed and directly opened on the vote counting day. Major criticism faced by EVMs is that these systems use microprocessors internally which can be subjected to tampering.
2) **Paper Ballot based System:** Here, voters are provided a paper ballot (usually a piece of paper) which consists of names of all candidates. These paper ballots are provided at the polling station. The major disadvantages of such a system are the high duration required to calculate votes, manpower, wastage of paper, ease in manipulation, etc.
3) **Head Count Method:** This approach is more popularly used in the Upper and Lower House of Indian Parliament when you need to get the count of members in support of a proposition and vice versa. Here we have a leader who instantiates the voting and declares the result. It is a trust and authority model. Here the speaker is trusted by the members and given authority by the constitution to conduct voting declare results.
4) **Database Approach:** Here, we have a centralized database managed by an authority which has the right to manipulate the database. The database consists of rows and columns. Each time a voter votes, the corresponding candidate's count gets incremented by one. Backtracking of votes is possible in this approach.

IV. Literature Survey

1) Paper titled **"A Secure and Optimally efficient Multi-Authority Election Scheme"** proposed a multi-authority secret-ballot election scheme that would guarantee robustness, universal verifiable, and privacy. where voters will participate using a computer, and the main consideration is the voter's efforts.In this system voters cast their ballot on a bulletin board. The bulletin board works with extended memory such that any part can access its content but won't be able to modify the data. The ballot does not contain any information about the vote itself but it does have an acknowledgment that it is a valid vote. The final tally is done when the deadline is over can be verified by any individual against the product of all submitted votes. This ensures verifiable due to the encryption method used. [8]
2) Paper titled **"A Smart Contract For Boardroom Voting with Maximum Voter Privacy"** had proposed the internet voting protocol with decentralized features and maximum voter privacy using Open Vote Network (OVN). The OVN is a smart contract for the Ethereum Blockchain. After implementing this system the creators concluded that it costs 0.73$ per voter on this system. They had an upper limit for the number of voters to 50 to reduce the gas usage. However, the researchers soon found out that OVN is susceptible to DOS attacks. It could also suffer through traffic jams during the transaction which could delay the voting process for a longer time. Hence this implementation is successful for boardroom meetings with a major drawback that each individual who wishes to vote needs to download the entire copy of the network. [9]
3) Paper titled **"Blockchain Based Voting System Can Better the Way of Elections in India"** proposed a system for the Indian Election System based on the Hyperledger Network. The booth agents at different polling booths act as different nodes. These agents are selected by the Election Commission of India. For each phase, the consent of 5 nodes is to be considered. Membership Service Provider is also present on polling booths which helps to authenticate the voters and generate public and private keys. Here they have suggested having three phases. During the preparation phase, a voter has to go to the nearest authorized voting center and register with his credentials so that his name is included in the Hyperledger network. [10] During the Voting Phase, the MSP issues the public and private keys to the voter. Once the voter casts a vote for a candidate it is counted as a transaction. The process of the Hyperledger network begins here. Each transaction is endorsed by at least 5 nodes. These transactions are sent to the ordering services and later to the main chain. The Post Voting phase includes steps such as recording votes in the main chain after validation, locking the authority of the voter for the time frame, counting of votes and so on. The validation is done by 5 different nodes to avoid any manipulation which is still computationally impossible. [11]
4) *Suporn Pongnumkul, Chaiyaphum Siripanpornchana, and Suttipong Thajchayapong* in their paper **"Performance Analysis of Private Blockchain Platforms in Varying Workloads"** compared the two most popular Blockchain technology platforms viz Ethereum and Hyperledger. They developed an application that can transfer money from account A to account B. On comparing execution time, they found that as the no of transactions increases, the execution time increases. However, Hyperledger's execution time is always less than that of Ethereum.On comparing latency it was found that on less no of a transaction, Ethereum's latency is 2x times that of Hyperledger. Also on varying no of transactions the change of average throughput of Hyperledger is relatively larger than that of Ethereum. [12]
5) According to *Denis Kirillov, Vladimir Korkho, Vadim Petrunin, Mikhail Makarov* in their paper **"Implementation of an E-Voting Scheme Using Hyperledger Fabric Permissioned Blockchain"** proposed a system that can integrate traditional paper voting with blockchain technology which increases the trust among the participants. Due to rapid development of ledger based technology and their potential to solve existing problems a modified version of the earlier developed protocol is being cited in this paper. [13]

V. Blockchain Platforms

A. Permissionless vs Permissioned Blockchain System

Permissionless Blockchains are open ecosystems where anyone can set up their node. These allow everyone to be a validator and transact over the system. It is also known as Public Blockchain. It is a truly decentralized system owned by each individual running a node. There is no central authority and every transaction is completely transparent. 'Ethereum' is a Permissionless Blockchain

Permissioned Blockchains, on the other hand, are controlled ecosystems. Permissioned Blockchain typically involves identified participants that maintain the node. Permissioned Blockchains are goal-specific as they are implemented in an environment where participants have a common goal but don't trust each other completely. These are maintained by organizations that are concerned with the control over data but want to maintain some transparency. Anyone who has to participate in this blockchain has to get permission from a central authority. It is used by the government and banks who are comfortable in complying with regulations. These blockchains give the flexibility to choose the level of transparency on data. These blockchains can have varying levels of decentralization. Hyperledger Fabric is a type of permission blockchain.

B. Ethereum

Ethereum, also called World Computer is a blockchain platform used to build decentralized applications in which every program and action is universally accessible and verifiable as it is available on the global Ethereum network. Ethereum is a global distributed ledger where everyone agrees to run the same program and data, hence it is a global shared processing protocol. To reduce spams and disincentive valueless transactions, we require gas i.e ether in case of Ethereum.

Ethereum, also called World Computer is a blockchain platform used to build decentralized applications in which every program and action is universally accessible and verifiable as it is available on the global Ethereum network. Ethereum is a global distributed ledger where everyone agrees to run the same program and data, hence it is a global shared processing protocol. To reduce spams and disincentive valueless transactions, we require gas i.e ether in case of Ethereum. [14]

But it is impractical to expect everyone to have a copy of the entire blockchain network. So the blockchain community has introduced concepts like blockchain servers, metamask, etc wherein you need not invest heavily in RAM and disk space and at the same time maintain decentralization.

Ethereum Blockchain has two primary components:

1) **Database:** All transactions within a blockchain network are stored in blocks.When an application is deployed it is considered as a transaction. In the case of our voting system, each vote being cast is counted as a transaction. These transactions are public and are available for verification. So to make sure that all nodes within the network have the same data copy and no invalid data is written to the network, blockchain uses a smart algorithm called 'Proof of Work'. [15]
2) **Code:** The business logic or the application code is written in the form of contracts in the Solidity Programming language. Solidity compiler is used to compile it to Ethereum byte code and this byte code is deployed to the blockchain.

Important terms to understand Ethereum:

- **Smart Contracts:** It is a written agreement between two or more parties written digitally in the form of code. Once a contract is deployed it cannot be modified . In this way agreement is being enforced.
- **Ether and Denominations:** The native currency for Ethereum blockchain is ether. There are currency exchanges where either can be converted to USD or EUR.
- **Ethereum Address:** Address is your identity on the network of the form 001d3f2efe111827552a4027bd3ecf1f086ba0f8 associated with a primary key. This combination of address and primary key is used to interact with the network.
- **Ethereum Account:** Ethereum has two types of accounts
  1) **Externally Owned Accounts (EOA):** They are combination of public address and private key used to send/receive ether to and from accounts and send transactions to blockchain.
  2) **Contract Accounts:** They don't have a corresponding private key and it is generated when contracts are deployed to the blockchain.
- **Gas, Gas price and Gas Limit:** Ethereum yellow paper describes a gas as the amount of work done in a transaction. Gas price is the price set for every single unit of ether. Since we are unaware of the amount of ether that will be consumed in a transaction, we specify a limit on the maximum gas units we are willing to spend on a transaction. This is called the Gas limit.
- **Ethereum Virtual Machine:** It is a simple, powerful 256-bit Turing machine capable of running EVM Bytecode. EVM is a part of the Ethereum system and it is crucial in consensus engine. Whenever you run the client or browser, the EVM starts to sync, validation, and execution of transactions.

C. Hyperledger Fabric (HLF)

Hyperledger Fabric is a distributed ledger technology, consisting of a modular architecture. This gives HLF a higher degree of confidentiality, flexibility, resilience, and scalability. Being an enterprise framework it can be adopted by any industry.

The fabric allows components, such as consensus and membership services, to be plug-and-play. Chain Codes which hold the business logic for the system are hosted over containers. To accommodate the complexity that exists across the industry and to give more flexibility to developers HLF is designed for various pluggable components.

The fabric uses a portable notion of membership for the permissioned model, which can be integrated with industry-standard identity management. The fabric also can also create channels, which enable a group of participants to create a separate ledger of transactions. [16]

Hyperledger Fabric runs on Execute-Order-Validate model fabric architecture consisting of modular development blocks:

1) **Ordering Service:** It establishes consensus on the order of transactions and broadcasts updates to peers. It is made of Ordering Service Nodes. Ordering service works across networks and parallelly orders transactions from other clients too. It maintains a shared ledger.
2) **Membership Service:** It enables the permissive nature of fabric i.e. provides cryptographic identities to peers. It typically provides X.509 certificates to participants. Every organization has to have a Membership Provider Node.
3) **Smart Contract (chaincode):** They are the smart contracts of fabric they are the logic written in a standard programming language that runs in isolation of containers.
4) **Local Ledger:** Each peer maintains a local ledger that is a snapshot of the latest state. It is a key-value store. It is of append-only and immutable nature. HLF stores data in ledger and state database. Here ledger is the

actual blockchain and state database is the record of latest committed transactions and is mutable.

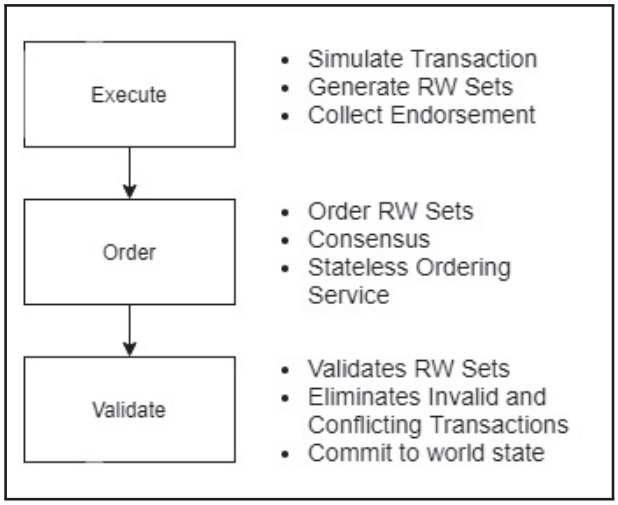

Fig. 2. Execute-Order-Validate Architecture of HLF

1) Execute: The client sends transactions to 'Endorsing Peers' specified by 'Endorsement Policy'.

- **Endorsement Policy:** It is a set of rules defined for endorsement of transactions by System Administrators. It specifics which endorsing peers will be used for which type of transactions.
- **Endorsing peers:**
  - Validates cryptographic signature of client.
  - Simulates Transactions i.e. it runs the chaincode but does not save the changes to the ledger.
  - Generates and returns 'R-W Sets'.
- **R-W Sets:** R-W stand for Read-Write. They capture what was Read and what is to be Written to ledgers. R-W sets are signed by endorsers.

If the majority endorsers validate the transaction then the client sends R-W Sets along with endorsed transaction to the 'Ordering Service'.

2) Order: The order of transactions has to be established to make sure that all the updates made to the world state are valid before committing to the network.

This ordering service sets the order for committing transactions and accordingly sends endorsed transactions to Committing Peers.

3) Validate: The Committing peers validate the RW sets by cross verifying it with its world state for 'Read' and checks for consistency for 'Write', accordingly mark them as success or failure.

If successful they are committed to locally stored ledgers and updates the Blockchain State.

D. Advantages of HLF over Ethereum for E-Voting Systems

We are considering Ethereum and Hyperledger for our proposed solution as they are the most popular frameworks in permission-less and permissioned paradigms respectively.

Below mentioned points compared the two platforms over "technical characteristics" of free and fair election:

1) **Transparency:**
   - Hyperledger provides transparency over transaction to organisations in the same channel. Provisions can be made to publish these transactions to the public.
   - Ethereum by nature is completely transparent.
2) **The integrity of Ballot:**
   - Both the platforms provide immutability of ledger.
3) **Privacy of Voter:**
   - As the hyperledger is controlled by central authority it can control the privacy of voters.
   - But this is not possible to provide in the Ethereum as it is a permissionless platform.
   - Definition of the transaction is also an important factor. Transactions are to be defined such that no logical relationship can be established between vote to voter.
4) **Accessible to every voter:**
   - In Hyperledger this is decided by central authority.
   - Ethereum by nature is designed to be permissionless so can be accessed by everyone.
5) **Ensuring Eligibility of all Stakeholders:**
   - As the hyperledger is controlled by central authority it is possible to give access to only eligible stakeholders.
   - Permissionless nature of Ethereum makes it impossible to give controlled access.
6) **One Voter One Vote:**
   - Both the platforms can ensure one voter one vote.

The voting system used in elections by nature has to be transparent concerning voters and candidates but it also has to be permissioned to allow only eligible voters and candidates to participate in elections. This all can be ensured by Hyperledger. Although one has to trust the central authority for accessibility and fair treatment of all stakeholders in the case of Hyperledger, these are moral considerations and can hinder both the systems. Only accessibility is an advantage of Ethereum based permissionless system over Hyperledger but this is also its disadvantage as it can't ensure eligibility of voters.

The performance of Hyperledger Fabric is also better than that of Ethereum. Suporn Pongnumkul, Chaiyaphum Siripanpornchana, and Suttipong Thajchayapong in their paper "Performance Analysis of Private Blockchain Platforms in Varying Workloads" conclude that "Assessment shows that Hyperledger Fabric achieves higher throughput and lower latency when compared to Ethereum when the workloads are diverse up to 10,000 transactions. Also, differences between these two platforms concerning execution time and average latency become more significant as the number of transactions grows. The average throughput of Hyperledger Fabric also varies at a much more agile rate than that of Ethereum". The authors of the above-mentioned paper ran certain tests

to compare the throughput and latency of both the systems. Hyperledger Fabric performed at a maximum throughput of 299.85 tps compared to 38.93 tps of Ethereum at a load of 102 transactions. At the peak load of 104 transactions, Hyperledger Fabric performed at 159.76 tps compared to 20.60 tps of Ethereum. Hyperledger Fabric was able to handle 104 transactions in 34.04 seconds whereas Ethereum took 484.76 seconds for the same load. Below are some images of performance graphs from the above paper. [17]

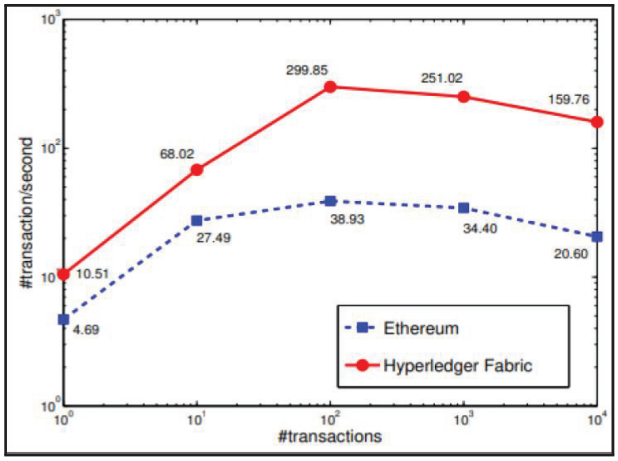

Fig. 3. Average throughput of Ethereum and Hyperledger with varying number of transactions

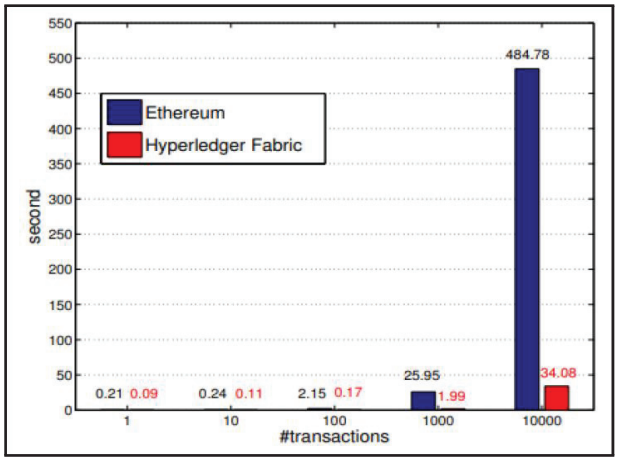

Fig. 4. Comparison of average latency between Ethereum and Hyperledger

All the above points conclude that Hyperledger Fabric is more suitable for E-Voting than Ethereum both, in regards to functionality and performance.

VI. Proposed Solution

According to Denis Kirillov, Vladimir Korkho, Vadim Petrunin, Mikhail Makarov, the government and corporate are still facing some difficulties in using E-voting. Various attempts and practises have been made to adapt the Blockchain based voting system. Seeing the constraints and problems we are proposing an integrated voting platform supported by Blockchain Technology for a National Election Scenario. [13]

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 platform for this solution. Chaincode 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:

1) **Admin model:** Defines Officials involved in the election process
2) **Voter model:** Defines Voter
3) **Candidate model:** Defines Candidate
4) **Election model:** Defines Election
5) **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 Voter Id.
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 voter block.

Voter Model Fields:

1) **Id -** Voter Id
2) **Voter Name -** Name of Voter
3) **Region Code -** Zip Code of the region where voter's home address.
4) **Voting Phase -** Next Election voter can participate
5) **Voting Permission -** It is set to true only on election day
6) **Voting Status -** It is to check if the voter has voted or not
7) **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:

1) **Id -** Election Id
2) **Region List -** List of region zip codes for which election is being held.
3) **Election Date -** Date of the election.

Candidate Model Fields:

1) **Id -** Candidate Id
2) **Candidate Name -** Name of Candidate
3) **Candidature Phase -** Election Id in which candidate is contesting
4) **Candidature Status -** Last Standing Position of candidate
5) **Total Votes -** Votes casted in the name of candidate
6) **Validation Status -** It marks the verification by authorities

C. Voting and Results

We propose two types of voting centers

- **Temporary Voting Centers:** These centers will be setup only in the region of election. This will just have the ***Polling Machines*** which will just act as clients.
- **Permanent Voting Centers:** These centers will exist on permanent basis for voters away from their home constituency. This will host the ***peers of the hyperledger***. There must be at least one permanent voting center per district.

This phase has following steps:

1) **Permitting Voter:** On the day of election voters are assigned permission to vote. Voters are given one time use keys and voters are notified of it.
2) **Casting Vote:** At voting centers voters have to enter their voting id and voting key for validation then they are allowed to cast vote. As the votes are cast the votes count of the candidate is also changed. Simultaneously their voting permission is revoked and voting key is deleted.
3) **Ending Election:** At a predetermined time voting permission is revoked and voting keys are deleted for the remaining voters who didn't participate.
4) **Result Announcement:** After ending the election the candidate with most votes will be announced as winner.

Here the voting model will be used to instantiate a voting block.

Voting Model Fields:

- **Id -** Voting Transaction Id
- **Candidate Id -** Candidate to which vote it cast
- **Election Id -** Election Id of the election

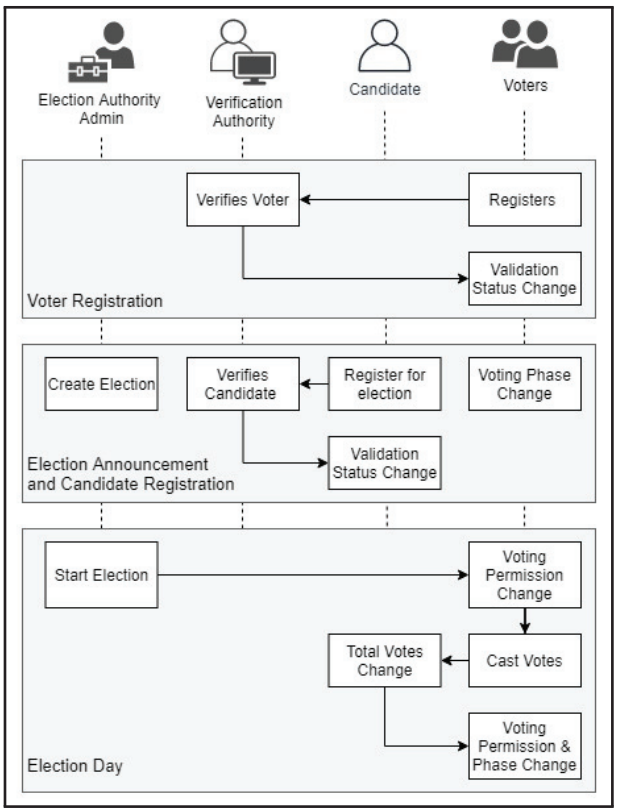

Fig. 5. Functional Flow Diagram

All the three phases have to occur in a sequential manner. Figure 5 shows the functional flow diagram. All the entities are shown horizontally and phases are arranged vertically. All the events occur in a vertical sequence.

VII. Implementation And Results

For a technology demonstration, we have used hyperledger fabric 1.4.0 as a blockchain development framework. Hyperledger Fabric offers support to multiple programming languages like go and node js. We have used node JS for the system.

Software Specification:

- Hyperledger Fabric v1.4.0
- Node Js v8.9.0
- npm v6.13.4
- Ubuntu 16.04
- Docker v18.09.7
- Docker-compose v1.17.1

Hyperledger fabric 1.4.0 was the latest stable version during the software requirement specification stage. Hyperledger Fabric has a system dependence of node 8.x and Linux based operating system. For ease of development, we have also used "convector suite" to set up hyperledger fabric over Ubuntu.

Basic network has been set up to demonstrate hyperledger. Basic network consists of two organisations consisting of two

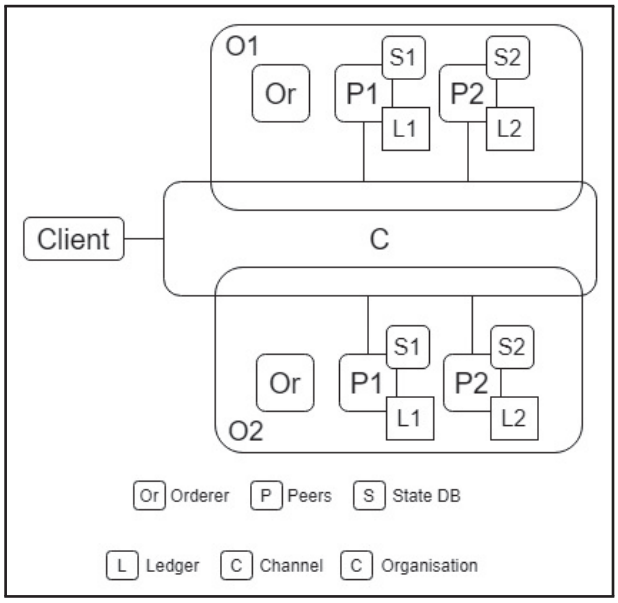

Fig. 6. Hyperledger Network Diagram

peers each and one channel. Figure 6 represents the structure of Hyperledger network. Here chaincode will be installed at both the peers and both the peers will act as an endorser and committing peers.

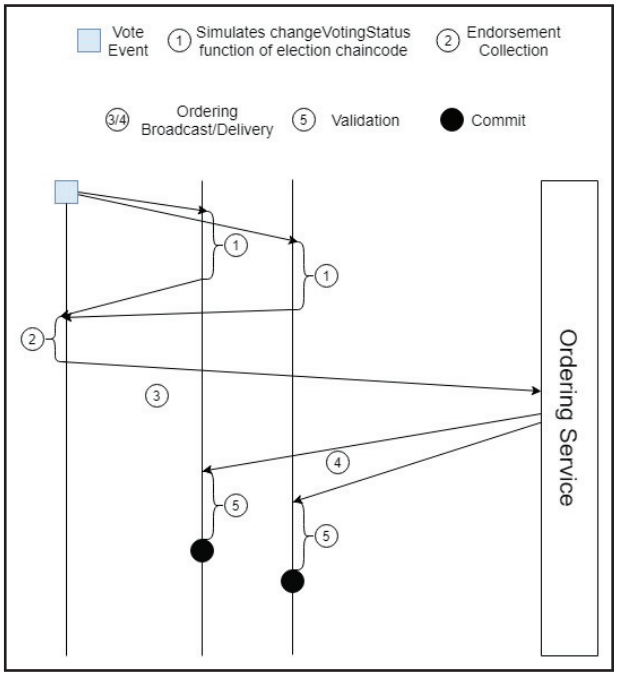

Fig. 7. Hyperledger Fabric High Level Voting Transaction Flow

Figure 7 shows the high level transaction flow of voting transaction, here the vote is casted and the event triggers a client which sends the transaction to endorsing peers and collecting their endorsements. This endorsement is transferred to the ordering service which orders the transaction and send them accordingly to committing peers which commit transactions after validating them.

```
[hurley] - Complete network deployed
[hurley] - Setup:
        - Channels deployed: 1
            * ch1
        - Organizations: 2
            * org1:
                - channels:
                    * ch1
                - users:
                    * admin
                    * user1

            * org2:
                - channels:
                    * ch1
                - users:
                    * admin
                    * user1
```

Fig. 8. Command line snippet of network setup

Figure 8 show the complete implementation of the basic network on Ubuntu command line by “Convector Suite - hurley”.

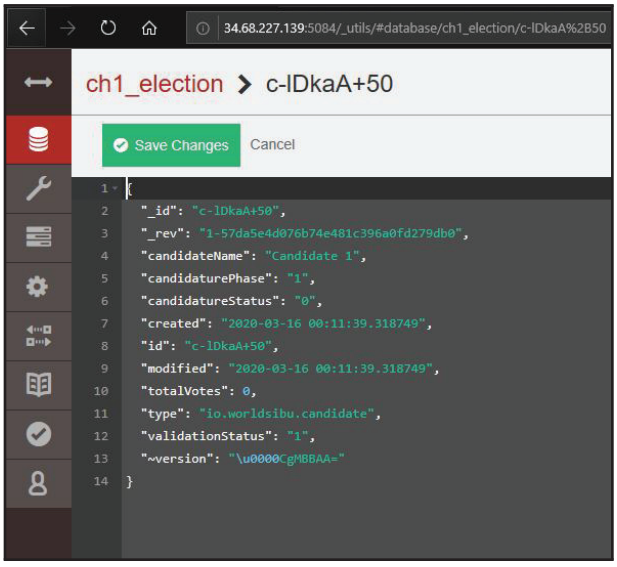

Fig. 9. Snippet of a a Candidate Block at a certain committed state represented as a document on Couch DB

We are using CouchDB as a State Database. It represents a block state as a json document. Figure 9 shows one such document consisting of a candidate block after it has been instantiated.

Figure 10 shows the result page of our system. We had tested our system with 1000 votes. The results are arranged in chronological order with the candidate with most votes on top.

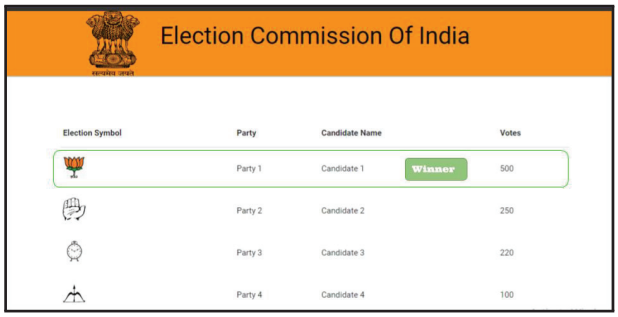

Fig. 10. Results Page Screenshot

VIII. 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 hyperledger 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] "Supporting free and fair elections," https://www.usaid.gov/what-we-do/democracy-human-rights-and-governance/supporting-free-and-fair-elections, accessed: 2020-01-24.

[2] "Can blockchain change the election scenario in india?" Available at https://link.medium.com/kgJJ2No5F3, accessed: 2019-12-22.

[3] "Features of blockchain technology," Available at https://guide.freecodecamp.org/blockchain/features/, accessed: 2020-01-26.

[4] "An introduction to hyperledger," Available at https://guide.freecodecamp.org/blockchain/features/, accessed: 2020-01-26.

[5] 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.

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, Tech. Rep., 2019.

[7] G. Albeanu, "Blockchain technology and education," in *The 12th International Conference on Virtual Learning ICVL*, 2017, pp. 271–275.

[8] 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.

[9] 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.

[10] N. Pandey and N. Singh, "Blockchain based voting system can better the way of elections in india."

[11] 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.

[12] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," in *2017 26th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 2017, pp. 1–6.

[13] D. Kirillov, V. Korkhov, V. Petrunin, M. Makarov, I. M. Khamitov, and V. Dostov, "Implementation of an e-voting scheme using hyperledger fabric permissioned blockchain," in *International Conference on Computational Science and Its Applications*. Springer, 2019, pp. 509–521.

[14] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," *white paper*, vol. 3, no. 37, 2014.

[15] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y," *ACM SIGMETRICS Performance Evaluation Review*, vol. 42, no. 3, pp. 34–37, 2014.

[16] C. Cachin *et al.*, "Architecture of the hyperledger blockchain fabric," in *Workshop on distributed cryptocurrencies and consensus ledgers*, vol. 310, 2016, p. 4.

[17] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," in *2017 26th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 2017, pp. 1–6.