SECURE I-VOTING USING PROOF OF AUTHORITY BLOCKCHAIN WITH REPUTATION ASSIGNED BLOCKCHAIN CLIENTS

# Abstract

Election is one of the most important processes in a democracy. It is the right of every citizen of the nation. The Election Commission of India (ECI) introduced E-voting in a phased manner from 1998 to 2001 for easy access to voting for everyone. Since 2014, Electronic Voting Machines (EVMs) have been used for all assembly and general elections. The use of EVMs has been questioned several times since its inception. Following several allegations, the ECI in 2010 added Voter Verifiable Paper Audit Trail (VVPAT) technology. In recent years, blockchain has come out as the technology claiming to change the way the services are provided. A blockchain is a form of distributed ledger. A distributed ledger is, in essence, a database spread out over a large number of nodes. One of the characteristic properties of blockchain is that the data in it is immutable. This ensures that there is no manipulation of data once the votes have been cast. This also helps in ensuring that a single voter does not vote multiple times without the requirement of rate limits that have currently been implemented. Blockchain technology helps improve the quality of services delivered in this manner.

# CHAPTER 1 INTRODUCTION

A blockchain in very simple terms is a database. The nature of the database is different from a typical database. In a typical database, the data is stored in a centralised location with all CRUD functionality. In a blockchain there is no centralisation. The data is stored in various locations anywhere possible connected by a network. Each of the systems in the blockchain network is called a node. These nodes contain the records of the blockchain as a series of blocks chained together. Each node on a blockchain contains a full copy of all the transactions done on the blockchain. No blocks that have been added to the chain previously can be altered by any node. New blocks can be added by client systems that are part of the network (nodes) but cannot alter previous ones. To add new blocks they must adhere to a set of rules. This set of rules is known as a smart contract. When a block is proposed to be added to the chain, if the block is valid it is added immediately, otherwise it is discarded. To determine the validity of the block, all the nodes compare the new chain with records in their local copy. They then vote on whether the new chain is valid or not. A malfunctioning node would be able to correct its copy of the chain using data from the other nodes. A bad actor would be unable to make changes to the entire blockchain without making changes in the data of a large number of nodes to achieve a majority of votes in favour of his new chain. This number is sufficiently large to make the attack practically unviable.

The Election Commission of India is tasked with conducting all elections in India. We use a First Past the Post method to decide the majority. The election commission conducts the elections using Electronic Voting Machines for the people to cast their vote and count them. Current implementation of the EVM with Voter Verifiable Paper Audit Trail (VVPAT) has several problems. The code that is burned on the devices is not open source, the machines have memory chips that can be overwritten without any trace. They cannot indicate if they have been compromised. The current method of preventing booth capturing is by using rate limiter and wait times if the rate limiter is triggered. If a booth is captured with the support of the police force or overpowering the police, there is no way to prevent a bad actor from adding as many votes as they want. Also in this case, neither the election commission nor the public at large can find out if any of these voting booths have been compromised. In case of a breach in the storage warehouses where the EVMs are stored, it is not necessary to replace VVPAT slips as not all VVPAT slips are counted and counting them all would take too long to be feasible.

The immutability of block chains could be leveraged to prevent all these possible attacks and by keeping the code open source we could improve the level of trust in the system.

# CHAPTER 2 LITERATURE SURVEY

**Praneeth babu Marella et.al.,** proposed the Genvote method which provides a secure and private e-voting system which is easily accessible and customizable. Genvote is the e-voting system which utilizes the ethereum blockchain, smart contracts and homomorphic encryption for voter privacy. It is to be used in a university level system. It allows the ballot creation and voting process for customizing different types of ballots. It uses ethereum and solidity for the ability of creating and voting ballots. Ethereum calls (eth.calls) allows the nodes to send messages from one to another node without storing the messages. While executing eth.calls sending messages the size of the blockchain will be reduced. It is secure and has high privacy. The smart contracts implemented in Genvote will be multifunctional to prevent voter fraud and tallying votes for each ballot. With the help of pallier homomorphic cryptosystem blockchain and smart contracts that the author is able to propose a system that was inherited from the current e-voting system.

**Vivek S K et.al.,** proposed a system for the election process to be conducted without the use of traditional methods. Hyperledger framework is a framework designed to act as a blockchain network. It is named as a transaction processor. It provides a platform for the computational and logic of blockchain. In this the validator is responsible for validating the signature of the received block directing it to the transaction processor, and adding the block to the blockchain once it is sent back by the transaction processor. As a result designing and implementing e-voting systems using blockchain ensures an individual verifiability, dependability, reliability, consistency, auditability, anonymity, transparency, scalability, eligibility, authentication and fairness through principles of consensus, cryptography, digital signatures, and various blockchain mechanisms. The ideal implementation in terms of making the e-voting system faster, lighter and scalable is the Hyperledger Sawtooth framework, due to support for parallel processing transactions. The implementation can be performed into usage of frameworks like Hyperledger Sawtooth in designing and implementing realistic robust and practical e-voting systems in large scale voting scenarios. It not only encourages exploration of blockchain technology, but also demonstrates the possibility of utilizing blockchain to develop secure systems.

**Lipeng Wang et.al.,** author proposed the threshold signature provides a very secure and private type of voting. In this the voter needs to provide his fingerprints, retina and other proof for voting. These proofs will be verified with the database and he/she will be allowed to vote. In this the blinding process is used to hide the voters details from third parties. If already voted the voters details will be tagged in th database, if seen to be tagged he/she won’t be allowed to vote. This type of blockchain based e-voting system is done only in the selected Trusted centers. The threshold signature later is converted to digital signature, it is the password protection scheme, which utilizes cryptography to confirm source and integrity of the data.

**Roopak T M et.al.,** author proposed the Virtual Id of Aadhar based e-voting using blockchain. It integrates to the e-voting system to overcome the duplication of votes and allows service providers to make verification. The fingerprints are verified by comparing Aadhar fingerprint with the fingerprint of the local device then, it is converted to digital signature. Previously, those who wanted to e-vote have to register in the web based registration with their unique Aadhar Id provided by UIDAI. By verifying the voter details, the Election commission will decide whether he/she can vote or not. He/she must provide his/her fingerprint before the confirmation of vote. Also the voter will be provided with a private key for the encryption process and the commision members will be provided with the public key to decrypt and retrieve the vote also the signature is verified. Only when the fingerprint is matched the key will be generated to vote, else will be verified again. The major properties used in this are authentication, publicly verifiable and integrity.

**Sudharsan B et.al.,** proposed Electronic Voting Machine(EVM) to overcome the vote counting time, vote secrecy and the security of the voters identities. Anyone with less knowledge in electronics can tamper the EVM to produce dishonest results. Connecting EVM to the network makes them vulnerable to cyber attacks, so a security concept derived from a popular technology is blockchain. It is a peer-to-peer verification of all transactions. The integrity of the system is increased by the implementation of three layers namely fingerprint based voter identification, transaction verification by peers, chain tamper detection. The one who registered earlier are allowed to vote, by comparing their fingerprints with the Aadhar fingerprint. In case of physically challenged all ten fingers are verified, in other cases retina scan is done.

**Asraful Alam et.al.,** proposed IOT based voting using blockchain in order to prevent counterfeit voting. In this the voter needs to provide his/her fingerprints and id to the database for verification. If the identities provided by the voter matches he/she will be allowed to vote else the identities provided by the voter will be verified again. The vote will be done by the private key after the confirmation of identities given by the voter. The identities provided by the voter will be kept in various blocks of the blockchain based database and it will be verified with the EVM database, if matched will be allowed else will be rechecked or rejected. The ballots are stored in the distributed ballot ledger through blockchain. Despite the use of consensus algorithms the data can be modified in some other location, it is prevented by providing a unique private key to the administrators. The data can be modified or changed only by the access granted by the administrator. The requested id will be tagged after the vote, if someone tries to revote by the tagged id, the database will be rechecked, whether the id is tagged or not, if not will be allowed else will be rejected. The property of IOT based e-voting are maintain consensus algorithms, require proof of work throughout the chain, store data as a ledger into the blocks, synchronize the whole ledger throughout the network and offers decentralisation of the data.

**Joao Alves & Antonio Pinto** proposed a blockchain based E-voting system. It is considered as a way to achieve a stronger and more effective voting in democratic cities. The requirements may differ for e-voting but they are genetically verifiable and tamper resistant. The blockchain seems to fulfil at least some of the key requirements of EVS by, in particular, being an immutable, verifiable and distributed record of transactions. Government and public administrations that promote the use of EVS expect efficiency and economic gains. Blockchain is used for the purpose of keeping voter details more confidential by storing it in many places with unique private keys in each database. The voter can vote by using their fingerprint as a signature with a provided private key for each. Later the vote will be retrieved by the election commission members using a unique public key. Also all the requirements are not fulfilled by blockchain, this is mostly achieved by spending some digital currencies. Some principles of blockchain based e-voting system are generality, freedom, equality, secrecy, democracy, directness.

**Rumeysa Bulut et.al.,** proposed a blockchain based e-voting inorder to protect the details of the voter and to prevent the central authority problems in terms of all blocks having all data in the chain. Even if the data is deleted in all other nodes the last node will hold all the data, unless we change or modify or delete by admin password or private key. Here the public keys play the role that, whether the vote is added to the ballot or not. If a person casts his/her vote, he/she can’t vote again even if the hacker removes the voted details from the e-government record. The voted data will be stored in various places using blockchain with different databases with unique private keys. In this system every transaction is related to the previous one. So the changes can’t be made in such transactions and also it can’t be overridden. Mainly it is used to secure the voter details that are provided by the user at the place of vote with the existing database.

**Abhishek Kaudare et.al.,** proposed comparative analysis of several blockchain technologies for proposing a blockchain based e-voting system solution by considering these technologies.in this author considers the Indian Election System for study and proposes a solution for the indian election system. In this Hyperledger fabric is considered. Hyperledger fabric is a distributed ledger technology. It is flexible, scalable and has a higher degree of confidentiality. Hyperledger fabric is an enterprise framework which can be adopted to any kind of industry. Hyperledger fabric creates channels that enable the group of participants to create separate ledger transactions. blockchain-based e-voting system that utilizes Hyperledger fabric for conducting secure elections in guaranteeing voters privacy. It is observed that hyperledger is more efficient than ethereum in most of the performance it allows to maintain privacy of the voter.

**Samuel Agbesi et.al,** proposed e-voting recording system based on blockchain technology have demonstrated how the blockchain can solve the problems associated with handling results after voting has ended. It addresses the issues of vote tampering, because votes transactions are added to the block which are secure with cryptographic graph function which makes tampering of the votes stored in the blockchain which makes it immutable. On using a peer-to-peer network it allows copies of blockchain databases that are to be shared among the voters on the blockchain which brings trust and transparency in the election results. The concepts of tokenization added more integrity in the transmission of election results. Once the results are declared it can’t be modified in remaining polling stations.

**Jordi Cucurull, et. al.,** in their paper Blockchain-Based Internet Voting:Systems’ Compliance with International Standards compare various products for internet voting (i-voting) that are available on the market and their compliance with Council of EuropeE standards. The EU recommends Safe aggregation, Authentication, Equal voting rights, Integrity, Vote correctness, Cast-as-Intended verifiability, Recorded-as-Cast verifiability, Counted-as-Recorded verifiability, Eligibility, Confidentiality, Election fairness, Anonymity as the required standards in any i - Voting System. They also recommend Long-term privacy as a required standard.

**Auqib Hamid Lone and Roohie Naaz,**  in their paper “Reputation Driven Dynamic Access Control Framework for IoT Atop Proof of Authority Ethereum Blockchain (Rep-ACM)” created a system with the following properties:

Client devices are given reputation scores which are used to decide whether the device is allowed to send data in the next block to be proposed to the chain. The validators can penalize or reward client devices for the transaction data they send. Geth is a popular implementation of full blockchain node using the ethereum protocol that is used in this system too. Proof of authority is an implementation of the Istanbul Byzantine Fault Tolerance (IBFT) consensus algorithm also known as Byzantine Fault Tolerance(BFT). Client devices, known as participants are either subjects or objects. Those devices that are supervised by gateways are known as objects, other devices such as servers, user devices act as subjects. They may be either lightweight nodes or validator nodes. A feedback is received each time a subject accesses the network. The feedback is used to derive subject reputation and allows objects in the system to register their smart contracts that have Rep-ACM deployed in them.

**Pranav Kumar Singh, et al.,** in their paper “Managing Smart Home Appliances with Proof of Authority and Blockchain” proposed the following:

PoA is a Byzantine Fault Tolerant consensus algorithm for private and permissioned blockchains. The consensus mechanism relies on a set of nodes which are trusted entities known as validators. Validators collect transaction data from its clients and add blocks to the ledger during its round. Each validator may propose only one block in a round. If more than one block is proposed, then the nodes go into voting where the validators vote whether or not to add the block to the ledger. If a majority vote against, then the client is disqualified as compromised. The voting phase is also used to ensure that the currently proposed block is valid. It is a compromise between truly secure blockchains and an efficient blockchain. The validator nodes each contain an entire copy of the blockchain with all of the transactions ever made on the chain and are required to be up most of the time if not always. The data-collection endpoints are connected to validators which are connected in a peer to peer network.

**Auqib Hamid Lone and Roohie Naaz** in their paper titled “Reputation Driven Dynamic Access Control Framework for IoT Atop Proof of Authority Ethereum Blockchain (Rep-ACM)” proposed the a mechanism from which we gathered the following: Client devices are given reputation scores which are used to decide whether the device is allowed to send data in the next block to be proposed to the chain. The validators can penalize or reward client devices for the transaction data they send. Geth is a popular implementation of full blockchain node using the ethereum protocol. Proof of authority is an implementation of the Istanbul Byzantine Fault Tolerance (IBFT) consensus algorithm. Client devices, known as participants are either subjects or objects. Those devices that are supervised by gateways are known as objects, other devices such as servers, user devices act as subjects. They may be either lightweight nodes or validator nodes. A feedback is received each time a subject accesses the network. The feedback is used to derive subject reputation and allows objects in the system to register their smart contracts that have Rep-ACM deployed in them. This system may be used to decide which client has been compromised and which are safe.

# 

# CHAPTER 3 PROPOSED SYSTEM

## Introduction

After studying the above mentioned papers and analysing each of their merits and demerits, a proposal for a secure, networked, blockchain based Electronic Voting System. By the use of this system, we hope to achieve the standards recommended by Jordi Cucurull et. al., and the Council of Europe. We also hope this ensures smoother and faster election results.

## Consensus Algorithm

The consensus algorithm is the core part of any blockchain network. The consensus algorithm is used to decide whether the node attempting to write a record to the ledger is valid or not. The most popular consensus algorithm is the Proof-of-Work (PoW) algorithm. It cannot be used for this purpose as it is prohibitively energy and time intensive. Another popular consensus algorithm is Proof-of-Stake (PoS). It is not appropriate for this purpose as it requires the user to be invested in the network through monetary means. However a modified version of the proof of stake algorithm known as Proof-of-Authority offers a solution to this problem. The PoA algorithm uses the person’s identity as stake instead of a monetary value. Using a monetary value as stake would skew the voting process in favour of those who have invested more in the network. Thus the PoA algorithm ensures that all votes are treated equally.

One of the key requirements of a Proof of Authority implementation is the availability of a public identity database. The AADHAAR or any other such identity proof that the government provides contains way too much sensitive data to be made public. However Voter’s slip is a public document and can be used as a proof of stake

## Nodes

Currently Electronic Voting Machines in designated voting booths are being used as the medium for Voting. EVMs are also part of a larger process which assures all candidates of fairness. Whether this assurance of fairness is true or not is beyond the scope of the paper. To ensure the smooth transition from the current system, it would be prudent to retrofit these EVMs with networking and block transaction capabilities if possible or make a similar replacement with the same capabilities.

## Current EVM

The current EVM has a very simple design with just 16 buttons on one machine with the appropriate parties’ symbols next to the buttons. In case there are more than 16 candidates in one constituency, upto 4 machines can be daisy chained to support a maximum of 64 candidates. The current implementation of EVMs has 3 parts. The three parts being a voting unit, a counting/controller unit and a Voter Verifiable Paper Audit Trail (VVPAT) unit. The voting unit is the one with the buttons and is the one the voter uses to cast their vote. The counting/controller unit stores the votes in its memory and is also used to enable or disable the voting machine. The VVPAT unit contains a printer and a record box in which all the VVPAT slips for the votes cast on that machine are stored. On none of these units is any network connectivity available.

## Proposed EVM

We propose an EVM with the same number of units but with additional functionalities. The first additional functionality would be the authentication mechanism. The EVM would have an authentication mechanism that will permit the voter to cast their vote. The authentication mechanism would be primarily based on one of the AADHAAR biometric identities (facial authentication, fingerprint authentication). The EVM at the voting booth would be able to send encrypted tokens. The tokens would contain data regarding the voter’s preference. Each of these tokens will be used to add data in two different blockchains on the same network. These two blockchains are called voter blockchain and candidate blockchain. The voter block chain contains voter data and their preference in the current election. The candidate blockchain contains only the number of votes obtained by each candidate in each constituency. Once the voter preference has reached the validator node assigned to the client, the validator node would add candidate data to the secondary blockchain (candidate blockchain). The candidate blockchain would be made public once the duration of the election is over. The voter blockchain would be permanently permissioned. The tokens on the voter-blockchain are stored in such a way that each voter can only read their own transactions (votes).

In addition to the EVM at the voting booth, there will be several other nodes called validators at publicly visible but safe areas like the election office. These will be the most important nodes in the network and most of these will need to be powered up for the entire duration of the election. If more than 33% of these devices fail, then the whole network will be at risk of collapsing. Similarly, upto 33% of these devices can be compromised without endangering the legitimacy of the election results. However, no matter how many EVM nodes are compromised, the integrity of the elections won’t be compromised. This is because the validator nodes are the authorised stakeholders in the PoA system. Each of these validator nodes will collect transactions (votes) from the clients (EVMs) and while proposing each block will propose only transactions from one of the clients. By this method, if any of the clients are compromised, then immediately the compromised client can be identified and prompt action can be taken.

## Proposed System

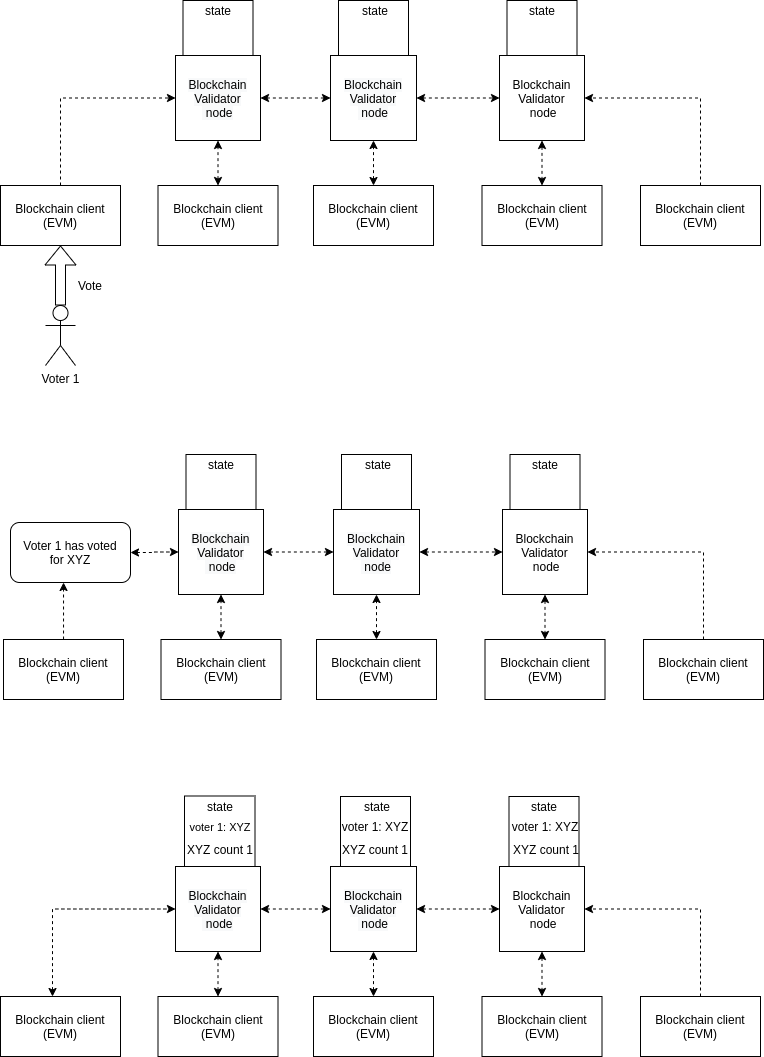


Fig 1. Voter 1 process

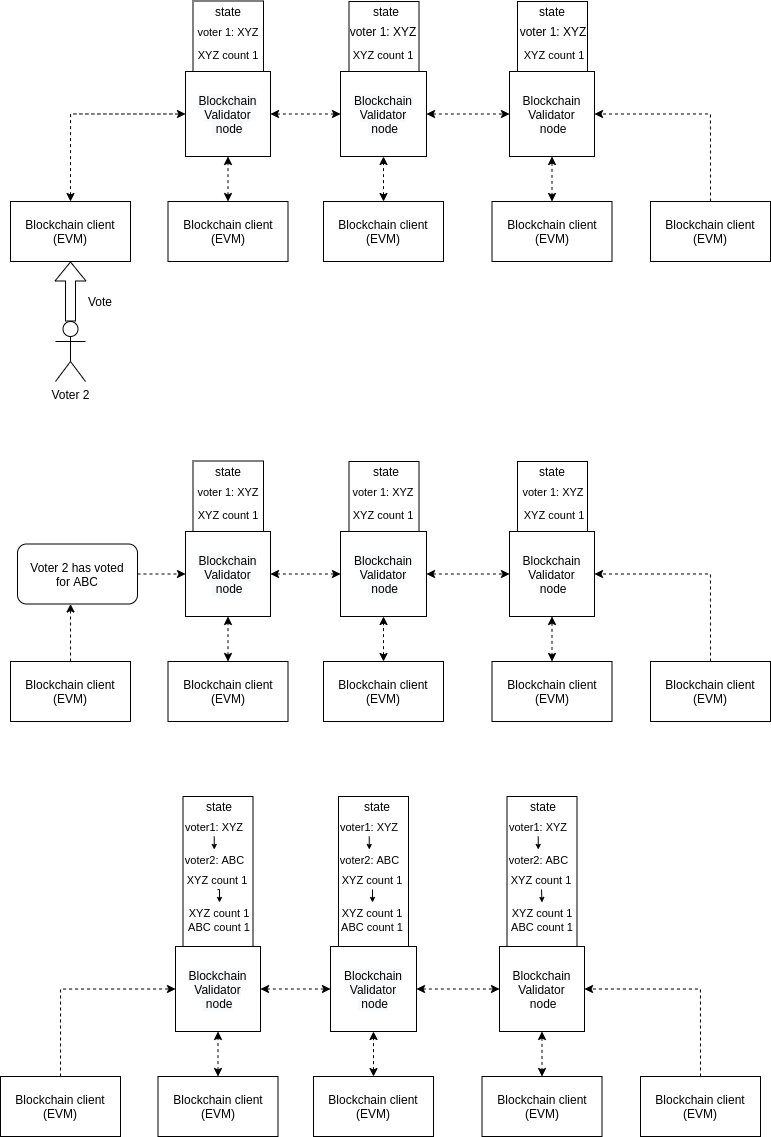


Fig 2. Voter 2 process

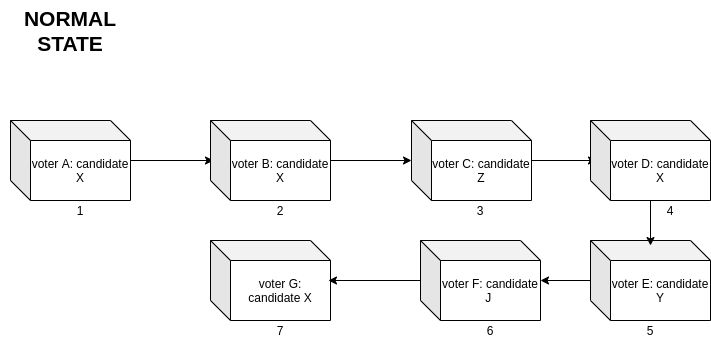
At the beginning of the election, each candidate files his nomination. Each accepted nomination will be given a unique id and these candidates are stored in a centralised database outside the blockchain. This is because there is a possibility of the EC disqualifying a candidate on various grounds. There are several other cases where the candidate’s name needs to be removed from the electoral roll. The validator nodes will need to be connected to this database in order to verify the correctness of the vote.

The voter would cast his vote after authentication using the authentication mechanism that would be added to the voting unit of the EVM. Each EVM is assigned a validator node. The relationship between EVM (blockchain client) and validator node is many to one. The voter’s id and preference is encrypted using asymmetric cryptography and sent to the designated validator node over HTTPS. The validator node collects each vote until it is given the turn to propose a block. It is expected to propose only one block per round. If it has collected multiple transactions in this time, it would propose all of them in that round. When this happens, the other nodes go into voting. They verify that the proposed blocks do not violate any constraints and vote for or against adding the blocks to the chain.

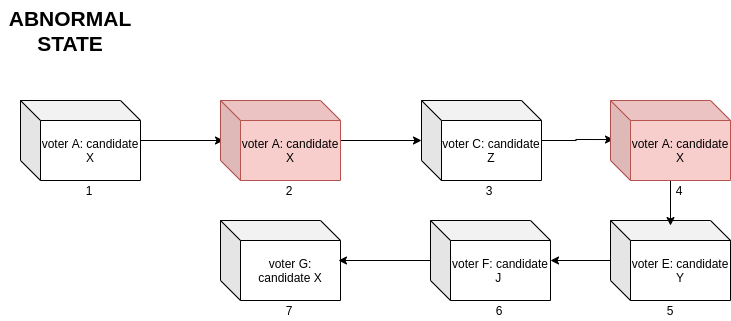
If the blocks get rejected, then the validator node must check all of the rejected blocks with the candidate database and the voter database and propose the verified ones alone in the next round. During this verification process, it must also check which client the blocks that failed came from. Once identified, those clients should be provided negative reputation points by their assigned validator node. The negative reputation points awarded must be much greater than the positive reputation points awarded on successful transactions being added to the chain to ensure early detection of any manipulation. If a client is awarded negative points during two consecutive rounds, then the validator node must immediately flag that client as compromised. Any transactions recorded from a compromised client is verified with the candidate and voter databases by the assigned validator node itself before being proposed as blocks during the next round in order to not bring down the efficiency of the rest of the network.

During voting in case of a fork, the validator nodes must choose such that the chain that is longest without violating any constraints can be accepted as the valid chain.

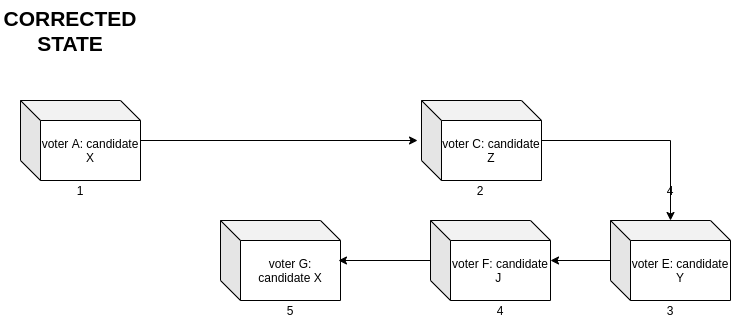
### Voter chain:



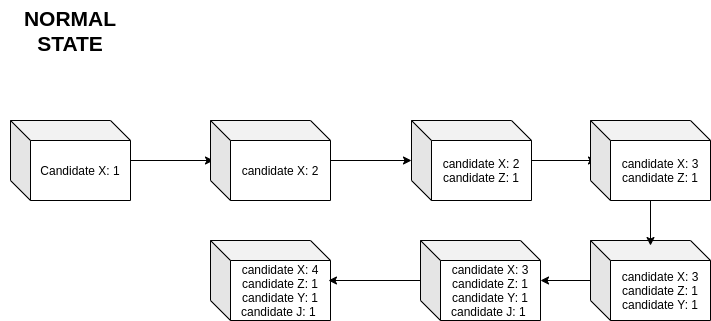
Each block on the voter chain contains the voter’s identity and their preference. The preference is stored as the id of the candidate they voted for.



Abnormal state is possible when there is some form of malpractice at a voting booth. The validator nodes can detect that the voter ‘A’ has already voted and their vote is in the chain. The newly proposed blocks (blocks 2 and 4) are discarded and only the first block is kept.



### Candidate chain:



There is no abnormal state since the blocks in this chain are added only after the voter’s block has been verified.

The last block added to this chain alone is enough to know the result of the election. However, to verify that there has been no malpractice or manipulation, anyone may verify their own record for recorded-as-cast verifiability.