Voting System Based On Blockchain

Mr.Adnan Hasan, Ms.Avi Panwar
Department of Computer Science and Engineering
Meerut Institute of Engineering and Technology,Meerut,U.P.,India

Abstract

Even now, the necessity to travel to vote is a major factor in the rising abstention rates. Due to the elimination of travel requirements, remote electronic voting will enhance turnout.Since the 1970s, many versions of electronic voting, often known as e-voting, have been employed. These systems have inherent advantages over many technique-based methods, including enhanced efficiency and decreased errors. The widespread use of these systems still faces obstacles, particularly in terms of enhancing their robustness against potential flaws. Blockchain is a cutting-edge technology that has the capacity to improve the overall robustness relating to electronic voting systems.The current issues with electronic voting may be resolved by incorporating blockchain technology. Vote is a blockchain-based voting system that is presented in this work.maintains vote privacy, improves accessibility, and is transparent, safe, and reasonably priced. In order to enable the management of voters and auditable voting records,e-Vote creates a voting framework at the scale of a university that makes use of Blockchain and smart contracts on Ethereum. e-Vote uses a few cryptographic methods, such as homomorphic encryption, to increase voter security anonymity. To show usability, scalability, and effectiveness, our implementation was put into use on Ethereum's Testnet. Two components are required for the blockchain-based voting project to function and integrate as a whole. One of them will be the Election Commission, which is in charge of setting up elections and adding registered parties and candidates who are running for office using smart contracts. The voter's module will be on the other end,enabling each voter to cast a ballot for the Assembly Constituency that best represents them. To prevent tampering, the vote will be recorded on the blockchain. Blockchain promises to increase the robustness of e-voting systems and may be a novel technology of the modern era.

1. Introduction

The Internet is the best invention that humans have ever made. However, the internet has some shortcomings. Consider a scenario in which there is a single point of authority, you are depositing money or casting a vote, and we are expected to trust him or her with our information, money, or vote. The current system's flaw is that there is just one point of failure or control. The Authority might or might not be dishonest or corrupt. The answer is to adopt a decentralized, distributed system that evaluates transactions, votes, and data based on the consensus of users and peers.

1.1 What is Blockchain ?

A chain of cryptographic links connects a collection of blocks to form a blockchain.Blockchain, one of the most advanced technologies, offers strong cryptographic foundations that let programmes benefit from these features. and create trustworthy security measures. The data in this instance has been broken up into blocks and connected. Every block has a unique hash value that serves as an identifier for the block. A link is created between each block by incorporating the current block with the hash of the block before it. To sum up, a block is made up of the data section, section, hash, and previous hash. The created chain of blocks is no longer stored in a single machine. Every user has a copy of the blockchain, also known as a distributed ledger. When someone tries to alter the data, the hash value is altered, the link is broken, and the hash value is altered. The attacker must modify and recalculate the hashes of succeeding blocks in order for the attack to succeed. Users curate each block once it is made depending on their consensus, and each block can either be accepted or rejected. Consequently, security, immutability, and transparency are provided by blockchains. Public, private, and consortium blockchains are the three main types of blockchains now in use.

1.2 Three Parts of Blockchain

A blockchain can be studied as a database that is distributed across its users. The essential is distributed across its users. The essential requirements of a blockchain are Peer to Peer networking, Asymmetric to Peer networking, Asymmetric Cryptography, Hashing Cryptography, and Hashing.

i. Ethereum

Ethereum is a blockchain that supports smart contracts and is open-source and decentralized. Ether is the name of the platform's native cryptocurrency (ETH). It has the second-largest market capitalization among cryptocurrencies, behind Bitcoin. Ethereum is the blockchain that is used the most. Ethereum was conceptualized by programmer Vitalik Buterin in 2013. The project started raising money through crowdfunding in 2014, and on July 30, 2015, the network launched with 72 million pre-mined tokens.Turing-complete scripts can be run on the Ethereum Virtual Machine (EVM), which can also run decentralized apps. Ethereum has been utilized for numerous initial coin offerings and is used for decentralized financing. A piece of code known as a smart contract is used to make decisions and conduct transactions. Ethereum's SmartUsing the computer language Solidity, contracts are produced. Ether (ETH), a native cryptocurrency for Ethereum, is comparable to Bitcoin. Being a programmable blockchain, many developers can use this blockchain service in their applications.

ii. Smart Contracts are technologies that, when certain criteria are satisfied, can automatically complete transactions without the assistance of a middleman business or entity. Despite the fact that the idea isn't specific to any one platform or network, smart contracts are frequently connected with Ethereum, a blockchain that was created to support them. Consequently, a cost known as Gas is attached to the contract in order to carry out or deploy it.
Executing on a shared network is typically more expensive and time-consuming than performing the network in a conventional setup.

iii. Election Process

The election is a formal way of making decisions. A democratic society has its foundations in voting. Elections are powerful as they are the deciding factors for the fate of an organization/country organization/country. The question of Transparency and parency and Security is still unanswered.

- Administrator – Manages and conducts the election
- Candidate – Participant in the election
- Voter – Person who is entitled to vote.

Traditional elections use a centralized system where a body is trusted to conduct and manage the whole process. Some problems with this structure are administrative authority may be compromised, and tampering may occur.

1.3 Goals and Purpos

The primary objective of this project is to develop a web application using blockchain technology that will enable voters to cast ballots from anywhere as long as they have valid citizenship in the country in which they wish to cast their ballots. This application will also safeguard each and every vote to ensure that every vote counts. The majority of current research focuses on security, accuracy, respectability, speed, protection, and review capacity; nevertheless, the frameworks in place are somewhat defenseless against attacks.Cons of the Current System

1. A centralized design.
2. Easily attacked.
3. Unreliable.
4. The opaque procedure for casting votes.

The current systems are vulnerable to assaults and are either highly hard to maintain or readily hackable. The main issues are data integrity and security,and the suggested remedy must be capable of resolving all issues with the existing systems.

1.4 Existing System

An essential component of a democratic society is voting. Voting is a technique for making decisions, and security is crucial. The systems in place are

1. Voting Method: Prior to 2004, India used a paper-based voting method. This is referred to as a ballot system on paper. Voters utilize it and it is put in the voting booth.
2. Electronic Control System: Electronic voting machines were adopted to address issues with ballot duplication and damage. Votes are assembled and stored there for use by poll workers.
3. Current Digital Voting Methods: There are a variety of digital voting systems in use now across the globe. To become more familiar with contemporary implementations, notably in Estonia, we examined some of these systems.

Since 2005, Estonia has permitted electronic voting, and in 2007, it became the first nation to offer online voting. 30.5% of the ballots were cast in the 2015 legislative election.were cast via the country's i-voting technology (Vabariigi Valimiskomisjon, 2016). All citizens of Estonia are issued a national ID card, which serves as the system's cornerstone.

These cards include encrypted files on them that serve to identify the owner and grant access to a variety of online and electronic activities, such as online banking, digital signatures on documents, access to personal data in public databases, and i-voting. (Digital ID card without a date)

1.5 Problem Statement

The use of computer technologies to enhance elections has been the subject of numerous studies. These studies discuss the hazards associated with implementing an electronic voting system due to software issues, insider threats, network vulnerabilities, and auditing difficulties.

1.6 Proposed System

We have suggested redesigning the current online voting system such that it incorporates Blockchain technology. When compared to the current system, which was detailed on the previous page, the suggested system provides the following advantages.

• Until they become citizens of the country, users can cast their votes from anywhere in the world.
• There is no need to wait in line to cast a vote, which will save time and lessen the workload. • The voting is saved in the Blockchain, making it tamper-proof.

Using two distinct sets of modules, we have focused on the following concepts: election commission and voter (s). Elections are created by the Election Commission, which also adds registered candidates and parties to contest them.The REST API for an election is hosted on the Blockchain of Ethereum, and the details are shown at the voter's front end for voting. Following the voting, the Election Commission receives the vote total from our blockchain infrastructure. Due to the fact that we did not use smart contracts in the traditional sense, our blockchain framework cannot function on other platforms. The disadvantage of not having voter authentication is that the main net must host it, a different web3 provider must be used to communicate with it, and there is no public API for voter ID.

The following are the project's development goals:

• to improve the current electronic voting system with the help of blockchain technology.
• To ease the burden of setting up an election booth and holding physical elections.
• Since voting is done entirely online, non-resident Indians may participate.
• We are expected to get knowledge of the blockchain concept and how it may be applied to various industries.

2.SYSTEM DESIGN AND ARCHITECTURE

2.1 Modules

The project has been broken up into numerous modules, with separate modules assigned to each functionality. Any software consists of a number of systems, each of which has multiple subsystems. These subsystems in turn have even more subsystems. As a result, building an entire system at once that includes all necessary functions is a laborious task that, due to its vastness, is prone to error.

If the partitioned modules can be solved, modified, and compiled separately, effective modular design can be realized. The project modules are listed as follows:

Candidate: A group of lists should represent the candidates. When a member of a group or community runs for office, they must submit the necessary information to RA. There should be a list of candidates. Voting for each candidate is defined as Ci.

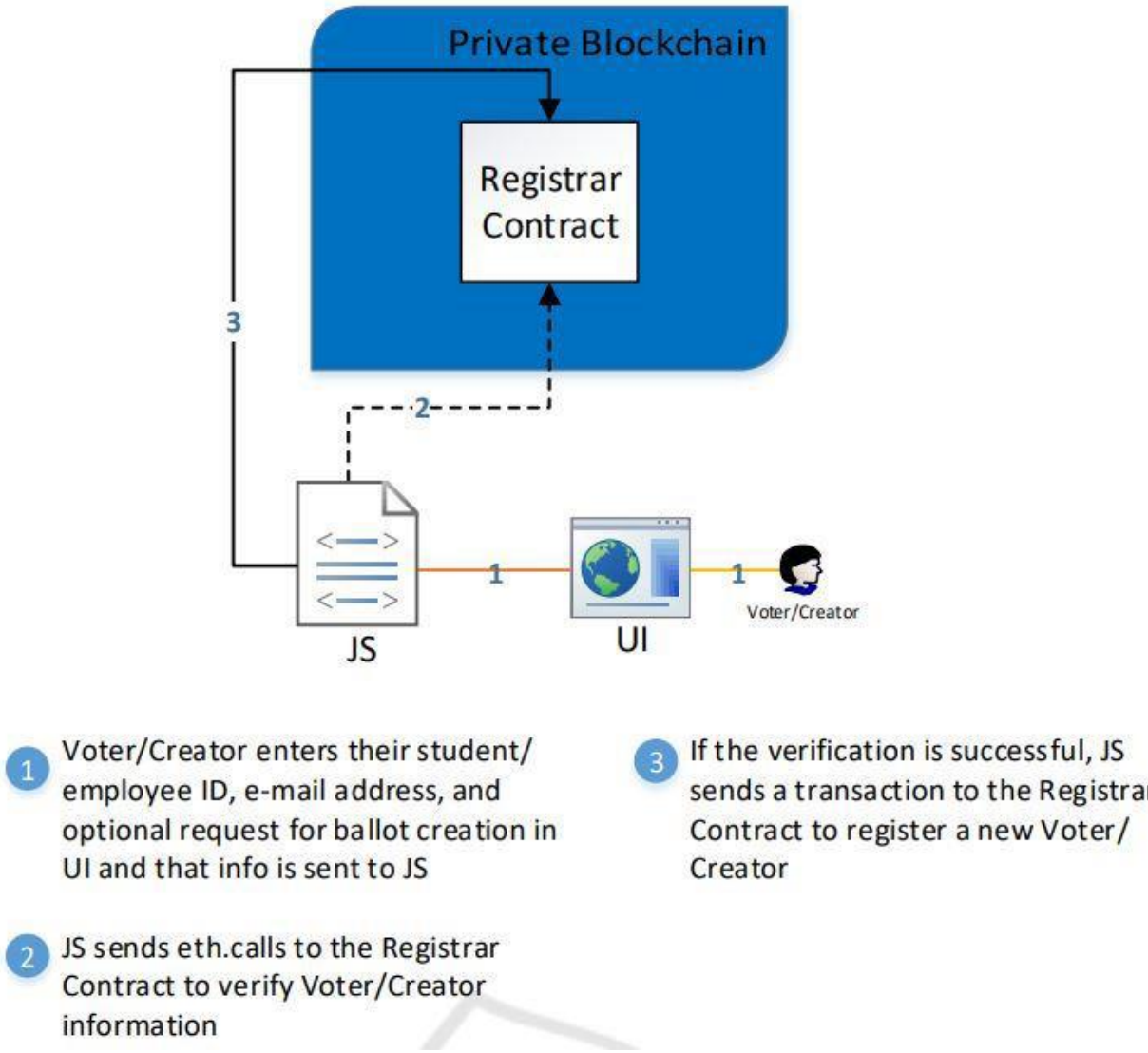
the registering authority In order to cast a ballot, the voter needs to register with RA. The candidate should provide his details while registering with RA, and RA will then provide him with the candidate's ID. Voter: A set of lists should represent the voters. Each voter's right to cast a ballot is defined as The voter needing to give EA his public key (PKI/Token).

Voters will import onto the voting portal using the Metamask extension in this module and cast their votes after receiving a personal ETH wallet. A voter register in our system to cast a ballot using a valid student or employee ID and email address.

Election Authority (Admin): The EA is responsible for starting the election, creating a vote, and limiting the voter numbers The transaction's voting, and payment of voting costs were generated automatically in the backend. The Election Commission will be the body in charge of setting up the smart contract, registering candidates and parties, and starting the election in this module. The initial Registrar and Creator smart contracts must be released by the Administrator. Additionally, the administrator has the power to allow or remove registered voters' and creators' access to create ballots.

Solidity Programming: It acts as both the gatekeeper and the keeper of records.It records all voters and creators who have registered, together with ballot IDs, voting contract addresses, and whitelisted email domains**.** The contract links together the voter's information and data from various ballots. Due to this, the contract is able to retrieve Voting. sol address information and perform voter verification and permission modification. The Administrator is the owner of this Agreement.The tiers indicated below refer to various levels or layers where activities take place.

Client: A client is any user or software that requests to use the system to carry out an operation. A presentation layer is used by clients to communicate with the systemPresentation Layer: This layer is in charge of the client-side presentation of data, i.e., it gives users a way to interact with the program and cast votes.Resource manager: The resource manager is in charge of organizing (storing, indexing, and retrieving) the data required to support the logic of the program. This resource manager is the Ganache-maintained Local Blockchain server.Application logic: This logic determines what the system performs in practice. It takes charge of establishing the business processes and carrying out the business rules. The three-tier architecture is used in the development of the blockchain voting system and its deployment.



Private Blockchain Concept

2.2 **Overall Implementation Process**

Initial Setup

The Registrar and Creator contracts must be initially installed by the administrator in order to turn onUsers will be able to sign up for the system, cast their first ballots, and make additional voting contracts. the chief executive must whitelist a list of email domains who are able to register to vote and participate in the electoral process while generating the Registrar Contract.

Register Voter

Throughout this phase, the voting process will be the most similar to the current one. A reputable third-party operating in the Electoral Commission's role will still need to monitor the registration process. The main distinction is that user IDs for the voting program, rather than polling cards as they are now, will be distributed. In order to cast their ballots for their constituency, voters must still register. To check whether the user has already registered and whether the provided domain is on the whitelist, it uses Ethereum to call the registrar contract (eth. calls). If all of those criteria pass, a transaction is sent to the registrar contract to save the voter's information, including their ID, email, and Ethereum address. The user's email address and Ethereum address are connected. to prevent double registration. During the registration procedure, individuals have the option to request the creation of ballots; while this request is currently granted automatically, it will eventually be manually processed by the administrator.

Create Ballot

By completing the necessary fields in E-vote.html, a user who is authorized to cast a ballot can spawn a new voting contract. Once the creator has provided their registered email address, chosen whether to make an election or poll, decided which type of ballot to produce, and defined the ballot's title,Only after determining the voting options and the maximum number of votes per voter can a ballot be produced. During this process, the creator has the ability to ask for a whitelisted ballot. The creator enters the list of email addresses permitted to vote on their ballot if a whitelisted ballot is utilized.In the event that the inventor opts not to create a whitelisted ballot, then anyone whose email address contains the whitelisted domain may vote. The author also specifies the election's finish date and time or poll.

Vote

The voting procedure itself will differ greatly. Registered voters will be able to establish a transaction on each of the channels on which they are eligible to vote by using the provided IDs to log into the application. They will have the option of selecting from among the available candidates for the channel or selecting "None of the above" if they prefer to cast a procedural vote. This transaction will transfer ownership of the corresponding ballot to the selected candidate upon submission. Similar to the finality of dropping the vote into a ballot box in the current system, changing the ownership of the ballot cannot be undone once it has been done. The user can use his or her registered email address to vote for a specific option on the ballot after it has been loaded. VotingApp.js collects the information from the voter when they click the "vote" button, and then it checks the voter's registration by placing eth. calls to the registrar contract.and Ethereum address. After the voter has been confirmed, the Voting Contract receives an eth. call to determine whether the ballot is on the whitelist or not.

Get Votes

The more transparent the voting procedure is, the better off this phase will be. Immediately after the voting session is over, an event will be set off that gives each voter read-only access across all channels. All participants will be able to check for irregularities in the votes cast in each channel or constituency. Shared queries will make it possible for participants and election officials to quickly determine who won and, in elections where demographic data is retained, the demographic groups that supported the victors. get votes serves as a function for retrieving data.GetVotes is called in the VotingApp JavaScript files each time a voter opens the ballot or successfully casts a vote. GetVotes sends an eth. call along with the hashed options in order to obtain the current total encrypted votes. It would either display the time when users can check back for the results or decode the votes, depending on the election style and time limit. The encrypted vote total is delivered by GetVotes to the truffle or metamask servers.where the private key will be used to decrypt the votes.

2.3 Development Algorithm

Distributed algorithms are algorithms that run on distributed systems.Numerous distinct computers that don't share memory make up a distributed system. Each CPU communicates with its own memory via communication networks. To implement communication in networks, a process on one system communicates with a process on another machine. Since many distributed system techniques carry out tasks that other system processes need, they frequently need a coordinator.

The Ring Algorithm

Systems using rings can use this approach(both physically and conceptually). This algorithm limits each process to only communicating with the process immediately to its right and assumes that communication between processes is one-way. In this method, a list called an active list is used. that contains the system's running processes' priorities. This approach presupposes that the system's processes are organized into a logical ring. The building is seen in the following figure. All messages can only be transmitted in one of two directions—clockwise or counterclockwise—making it unidirectional. The distribution of the ring locations could be done using the network addresses' numerical order..The disadvantage is that should the token regenerate after being lost, it will need to be replaced. Finding the lost tokens, though, could be difficult. If the token is still in use and goes unreceived for a considerable amount of time, it might not be lost.

Algorithm

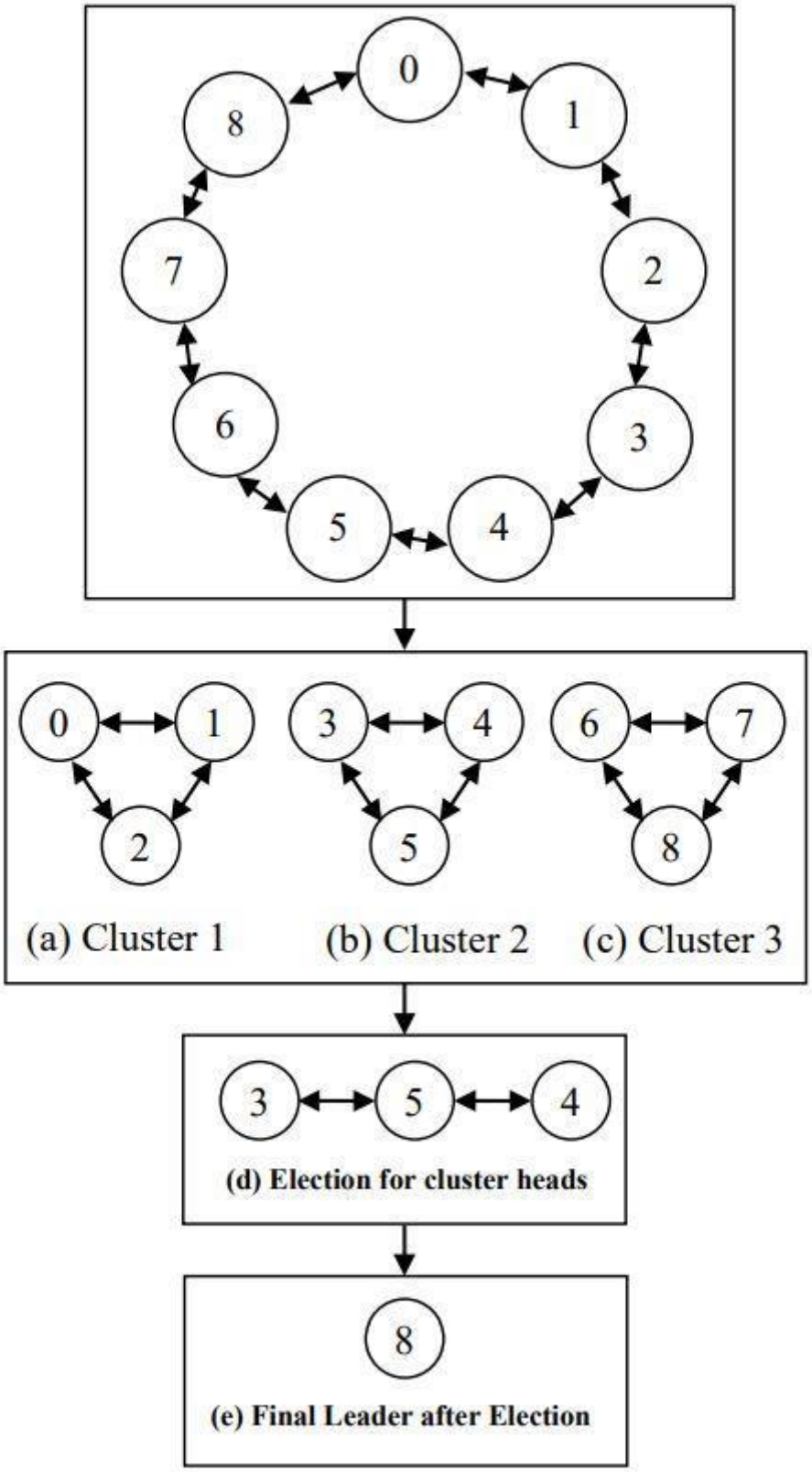
Process P1 builds a new active list that is initially empty if it notices a coordinator failure. It adds number one to its active list and sends election messages to its neighbor on the right.

Process P2 has three possible responses when one of the processes on the left sends it a message:

(I) P1 forwards the message and adds 2 to its active list if the message received does not already contain 1 in it.

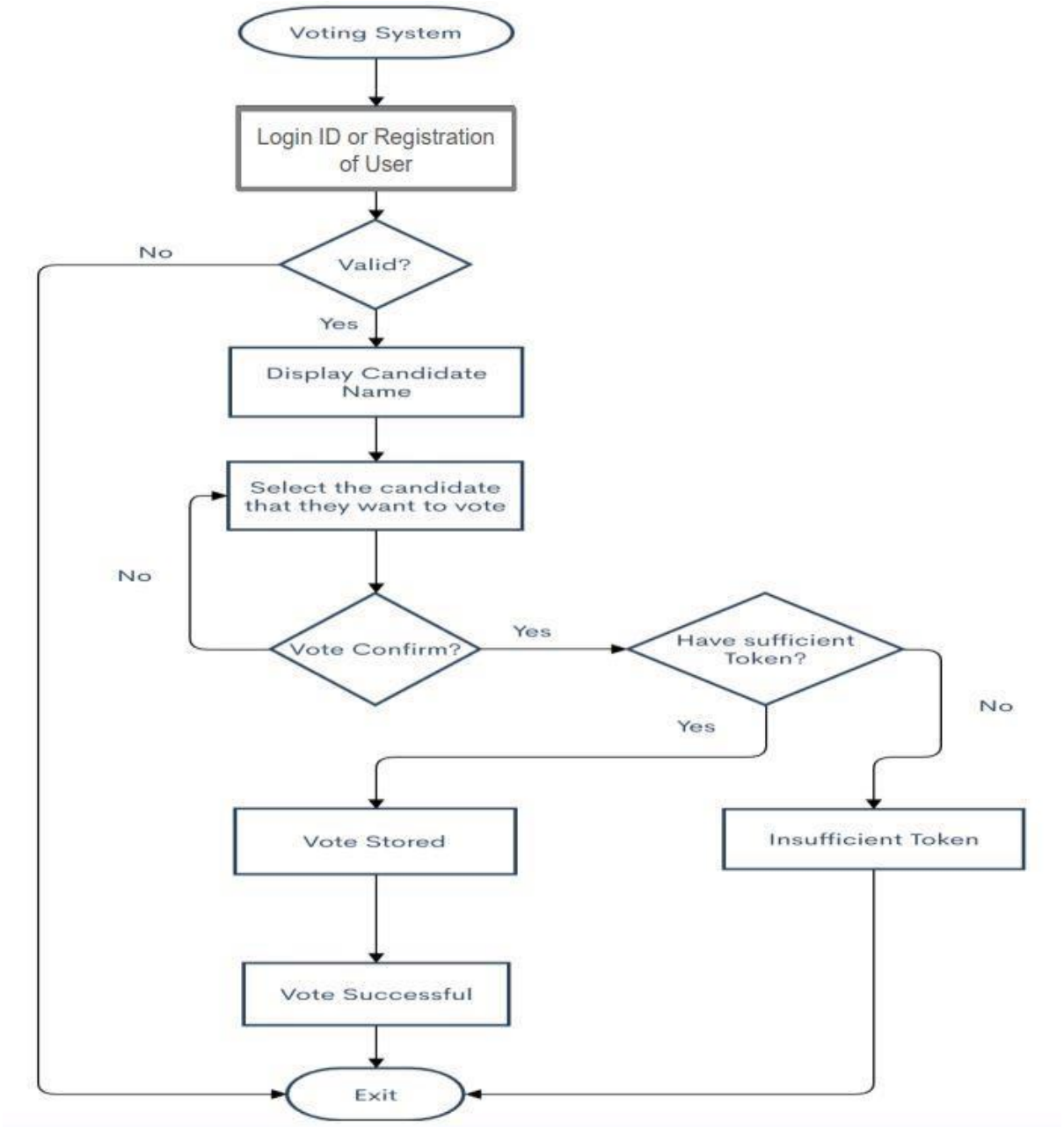
(II) A new active list with the numbers 1 and 2 is created if this is P1's first election message that it has ever sent or received. Election messages 1 and 2 are then sent.

(III)The numbers of all other processes in the system are now on Process P1's active list if it receives its own election message number 1.Process Pnow chooses number as the new coordinator from the list.


0
1
2
3
4
5
6
7
8
0
1
2
3
4
5
6
7
8
(a) Cluster 1
(b) Cluster 2
(c) Cluster 3
3
5
4
(d) Election for cluster heads
8
(e) Final Leader after Election

2.4 Flowchart

Below is the Overall Flow Chart of this project.



3.IMPLEMENTATION

3.1 Smart Contract Concept

Smart contracts are pieces of computer code that automatically execute all or a portion of an agreement when posted on a platform based on a blockchain. As will be covered in more detail below, the code may serve to execute certain terms of a standard text-based contract, such as the payment of money from Party A to Party B, or it may serve to convey only the parties' agreement. The numerous nodes on the blockchain enable the duplication of the code, It benefits from the permanence, security, and immutability that a blockchain offers. Due to this replication, the code is actually executed as soon as a new block is added to the blockchain. If the parties have indicated through the commencement of a transaction that particular requirements have been satisfied, the code will execute the step that is triggered by those parameters.If

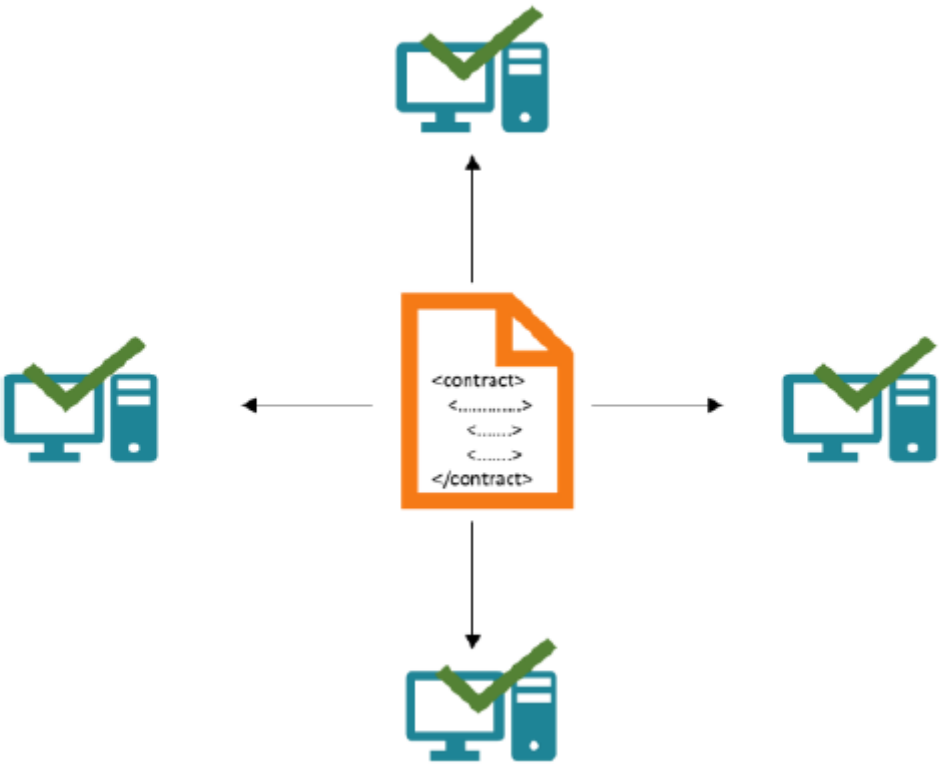
such a transaction has not yet begun, the code will do nothing. A programming language like Solidity, which was developed specifically for creating these kinds of computer programmes, is used to produce the majority of smart contracts. The smart contract is run across a blockchain network, and the code for the contract is stored on each of the network's many computers. This ensures that the facilitation and implementation of the contractual terms will be more secure and transparent. Additionally, since every participant in the blockchain network checks a smart contract's source code, they don't require an intermediary to execute. By removing the middleman from the contract, the cost to counterparties is significantly reduced.

How are smart contracts implemented?

The parties shall first determine the terms of the contract. The agreed-upon clauses are subsequently translated into programming code. In essence, the code contains a variety of conditional statements that outline several circumstances for a potential future transaction.

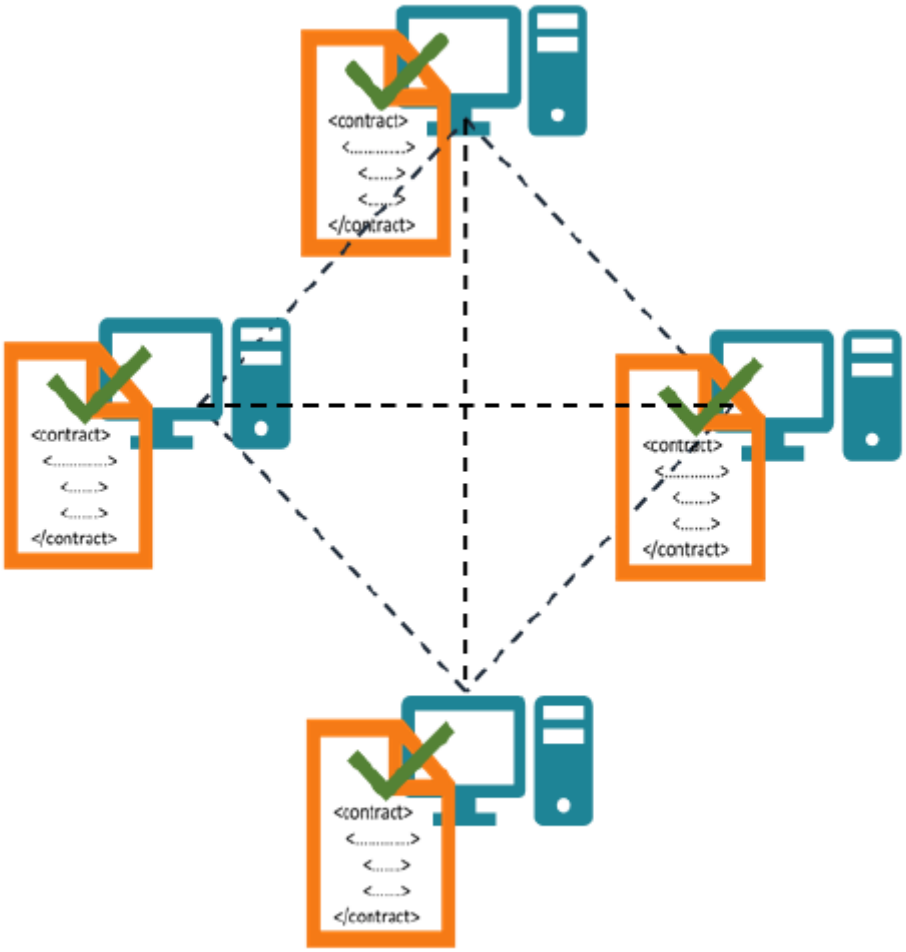
Transfer contract terms into code

When a piece of code is written, it is replicated among the blockchain's users and stored in the network.



The code is stored in a blockchain and replicated between participants

All of the computers in the network then run and carry out the code. The appropriate transaction is carried out if a condition of the contract is met and has been confirmed by every user of the blockchain network.

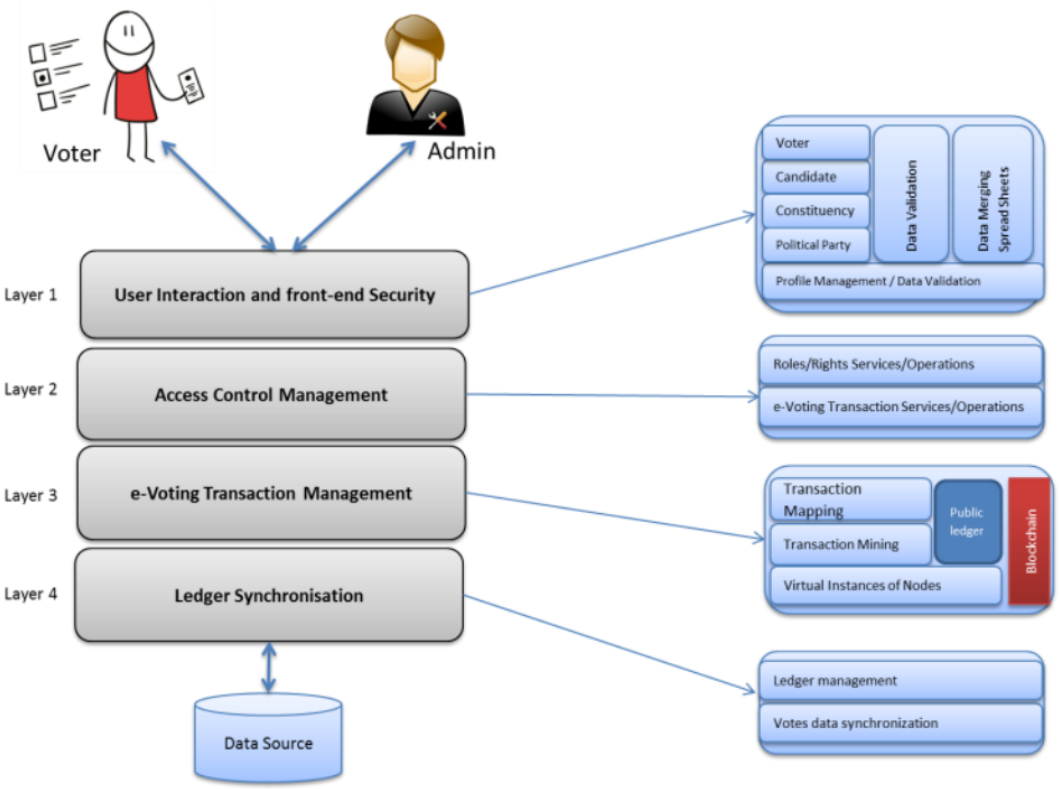


When a term is satisfied, computers in the network verify its correctness.

3.2 Methodology

We have tried to create a system and service that reduces the size of attack vectors to thwart possible malicious attacks. To make certain that we have considered each step of the voting process, we have attempted to review and analyze our design from a variety of angles. The report's discussion of potential dangers related to our proposal and its recommended countermeasures can be found in this section. One danger is forgetting one's voter ID, password, or poll card on election day. As they are unable to enter the system, the voter will be unable to cast their ballot in this situation. The voter returning later that day with the correct information is one potential risk mitigation or the deployment of an additional authentication method, like the phone. As an alternative, a forgotten password feature might be introduced to the voter registration website. This feature would function similarly to how Other websites offer password recovery features. But this increases the chance that a hacker will attempt to change a voter's password.covertly. A 51% attack could represent a risk to our suggested design. The assault is based on the idea that someone might conceivably have influence over a large portion of the hash rate used for digital voting, which would allow them to alter the public ledger. The likelihood of this kind of attack happening is very low.
due to the astronomical price required to buy technology capable of processing at this level. We also have the additional security of an auditor who monitors network connections and node locations. Systems like bitcoin do not currently have this feature. 2016 (LearnCryptography.com) The main attack vector for hackers in our system is the online voting portion because they can take advantage of voters utilizing their own devices in a number of different ways. programmes that the client may download and use to connect securely to the polling location may be developed as a defense against this.Voting involves three unique pieces of identification: a voter's identification number (UK citizens have national insurance numbers), the password they provided when registering, and their ballot, which has a QR code. The user will input the

authentication details in a different way for each of the two ways to vote (web browser and physical polling station), but they must submit all three pieces of information in order to cast a ballot.Each user will be registered to vote in a certain constituency, thus they can only do so in person at a local polling location inside that constituency or onlineat the website listed on the voting card. It is imperative that you remember this. To ensure that votes are counted within the proper network, each constituency must have its own web server and URL.) To make sure the voter hasn't already used up their vote, the polling place will check the voter blockchain behind the scenes. The station will then let the user proceed to the voting screen if they do have a vote. If not, the user will receive the proper response from the system. For a process schematic, see Appendix B Figure 6. The vote will become a transaction after the voter selects their vote (from a list of alternatives that includes abstaining) and confirms the submission. It will then be encrypted using the public key of the appropriate constituency.This transaction is received by the constituency node, which records it in a block and then pushes the modification to each node linked to that particular constituency node. After updating the entire network, the connected nodes communicate the information to their peers. Once the vote is validated, the voting location will generate a transaction to delete the user's vote from the voter blockchain. It's crucial to understand that there are two separate blockchains: one stores transactions relevant to which users have registered and which people still have a vote, and the other contains the actual content of the vote (such as the party that received the most votes). We guarantee voter privacy when casting their ballot by utilizing these two different blockchains.



Architecture of Proposed system

4.Conclusion

An honest and reliable voting procedure is essential to every democracy. Voters must have confidence in the voting process because successful democracies are dependent on credible elections. Elections conducted using traditional paper ballots, however, lack trust. The notion of changing digital voting technology to streamline, expedite, and lower the cost of the public political process is appealing in today's culture.Making voting easy and affordable helps voters accept it as usual, which reduces the power disparity between them and elected officials and puts some pressure on them. Additionally, allowing citizens to express their opinions on particular ideas and bills, paves the entranceway to a direct democracy. This project has evolved into a blockchain-based electronic voting system that protects voter anonymity and makes use of smart contracts to enable safe and economical elections. The architecture, design, and security analysis of the system are provided in broad strokes.

In the forthcoming release of this application, it has been suggested that differentIt is necessary to construct client designs for other functions, such as the election commission and candidates affiliated with a specific party, in addition to the existing voting client design. Because we are unable to include the most recent versions of the Aadhar or Voter SDK into our programme, the current versions also lack authentication. In order to promote the largest possible voter participation, the upcoming edition is also likely to include a message prompt encouraging each voter to cast their ballot on election day.

5. References

[1] Wolchok, Scott, et al. ``Security analysis of India's electronic voting machines." Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010.

[2] Ohlin, Jens David. "Did Russian cyber interference in the 2016 election violate international law?" Tex. L. Rev. 95 (2016): 1579.

[3] Ayed, Ahmed Ben. "A conceptual secure blockchain-based electronic voting system." International Journal of Network Security & Its Applications 9.3 (2017): 01-09.

[4] Hanifa Tunisia, Rifa, and Budi Rahardjo. "Blockchain based e-voting recording system design." 2017 11th International Conference on Telecommunication Systems Services and Applications. IEEE, 2017.

[5] Yu, Bin, et al. ``Platform-independent secure blockchain-based voting system."
International Conference on Information Security. Springer, Cham, 2018.

[6] Feng Hao, P.Y.A. Ryan and Piotr Zielinski. (2008). Anonymous voting by two-round public discussion. Available at: http://homepages.cs.ncl.ac. uk/feng.hao/files/OpenVote_IET.pdf

[7] The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. Available at: https://users.ece.cmu.edu/~{}adrian/ 731-sp04/readings/dcnets.html.

[8] Patrick McCorry, Siamak F. Shahandashti and Feng Hao. (2017). A Smart Contract for Boardroom Voting with Maximum Voter Privacy Available at: https://eprint.iacr.org/2017/110.pdf.

[9] Ronald Cramer, Rosario Gennaro and Berry Schoenmakers. A Secure and Optimally Efficient Multi-Authority Election Scheme Available at: http://www.win.tue.nl/~berry/papers/euro97.pdf

[10] Agora (2017). Agora: Bringing our voting systems into the 21st century Available at: https://agora.vote/Agora_Whitepaper_v0.1.pdf