" E-voting using blockchain technology"

Prof. Pallavi Shejwal[1], Aditya Gaikwad[2], Mayur Jadhav[3], Nikhil Nanaware [4] ,Noormohammed Shikalgar[5]
[1]Assistant Professor, Department of Information Technology, BSIOTR, Pune, Maharashtra,India
[2]BE Student, Department of Information Technology, University of Pune, BSIOTR Pune ,Maharashtra , India
[3]BE Student, Department of Information Technology, University of Pune, BSIOTR, Pune, Maharashtra, India
[4]BE Student, Department of Information Technology, University of Pune, BSIOTR, Pune, Maharashtra , India.
[5]BE Student, Department of Information Technology, University of Pune, BSIOTR, Pune, Maharashtra , India.

Abstract

Increasing digital technology has revolutionized the life of people. Unlike the electoral system, there are many conventional uses of paper in its implementation. The aspect of security and transparency is a threat from still widespread election with the conventional system (offline). General elections still use a centralized system, where in one organization manages it. Some of the problems that can occur in traditional electoral systems is with the organization that has full control over the database and system. It is possible to tamper with the database of considerable opportunities. Block chain technology is one of solutions, because it embraces a decentralized system and the entire database are owned by many users. Block chain itself has been used in the Bitcoin system known as the decentralized Bank system. By adopting block chain in the distribution of databases on e-voting systems one can reduce the cheating sources of database manipulation. This project aims to implement voting result using block chain algorithm from every place of election. Unlike Bitcoin with its Proof of Work, this will be a method based on a predetermined turn on the system for each node in the built of block chain.

Keywords: *Security and Protection, Hardware, Online Information Services*

.

1. Introduction

Lately, electronic voting systems have begun being used in many countries. Estonia was the first in the world to adopt an electronic voting system for its national elections [1]. Soon after, electronic voting was adopted by Switzerland for its state-wide elections [2], and by Norway for its council election [3]. For an electronic voting system to compete with the traditional ballot system, it has to support the same criteria the traditional system supports, such as security and anonymity. An e-Voting system has to have heightened security in order make sure it is available to voters but protected against outside influences changing votes from being cast, or keep a voter's ballot from being tampered with. Many electronic voting systems rely on Tor to hide the identity of voters [4]. However, this technique does not provide total anonymity or integrity since many intelligence agencies around the world control different parts of the Internet which can allow them to identify or intercept votes.

2. Literature Survey

Increasingly digital technology in the present helped many people lives. Unlike the electoral system, there are many conventional uses of paper in its implementation. The aspect of security and transparency is a threat from still widespread election with the conventional system (offline).Block chain technology is one of solutions, because it embraces a decentralized system and the entire database are owned by many users.[1]

Bit coin introduces a revolutionary decentralized consensus mechanism. However, Bit coin-derived consensus mechanisms applied to public block chain are inadequate for the deployment scenarios of budding consortium block chain. We propose a new consensus algorithm, Proof of Vote (POV).The former guarantees the separation of voting right and executive right, which enhance the independence of bulter's role, so does the internal control system within the consortium . As for the latter, under the circumstance that at least Nc/2+1 commissioners are working effectively, our analysis shows that POV can guarantee the security, transaction ? [2]

There is no doubt that the revolutionary concept of the blockchain, which is the underlying technology behind the famous cryptocurrency Bitcoin and its successors, is triggering the start of a new era in the Internet and the online services. In this work, we have implemented and tested a sample e-voting application as a smart contract for the Ethereum network using the Ethereum wallets and the Solidity language.[3]

Block chain was first introduced by Satoshi Nakamoto (a pseudonym) , who proposed a peer to-peer payment system that allows cash transactions through the Internet without relying on trust or the need for a financial institution. Block chain is secure by design, and an example of a system with a high byzantine failure tolerance.[4].

Proof of stake protocol of block verification does not rely on excessive computations. It has been implemented for Ethereum and certain altcoins. Instead of splitting blocks across proportionally to the relative hash rates of miners (i.e. their mining power), proof-of-stake protocols split stake blocks proportionally to the current wealth of miners. The idea behind Proof of Stake is that it may be more difficult for miners to acquire sufficiently large amount of digital currency than to acquire sufficiently powerful computing equipment.[5]

E-voting is a potential solution to the lack of interest in voting amongst the young tech savvy population. For e-voting to become more open, transparent, and independently auditable, a potential solution would be base it on block chain technology. Block chain technology has a lot of promise; however, in its current state it might not reach its full potential.[6]

Electronic voting has been used in varying forms since 1970s with fundamental benefits over paper based systems such as increased efficiency and reduced errors. With the extraordinary growth in the use of block chain technologies, a number of initiatives have been made to explore the feasibility of using block chain to aid an effective solution to e-voting. It presented one such effort which leverages benefits of block chain such as cryptographic foundations and transparency to achieve an effective solution to e-voting. The proposed approach has been implemented with Multichain and in-depth evaluation of approach highlights its effectiveness with respect to achieving fundamental requirements for an e-voting scheme .[7]

Public block chains are open for all. Anyone can join them to post transactions and to participate in the mining and consensus process of adding new block of transaction to the block chain .These block chains usually use Proof of Work (PoW) or Proof of Stake (PoS) for consensus mechanism. Having more number of participants works well for this model, as it further reduces the possibility of a 51% attack.[8]

Permissioned block chains are built usually by organizations for their specific business need . Such block chains Are likely to have interfaces with existing applications of the organization. Organizations may opt for consortium block chains where limited trusted members mandatorily need to sign off a transaction. In fully private block chains, the write permission over the block chain is given to a central organization. The former are referred to as partially
decentralized by Buterin.[9]

A generic extension of block chain transactions to transfer stuff other than cryptocurrency is suggested by Zyskind et al. In their proposed system, the transactions are used to carry instructions for storing, queuing and sharing data. With increased number of mobile applications seeking complete access to user data such as contacts, messages, photos and a variety of other personal data, Zyskind et al. have provided the implementation architecture of a system which
uses block chain along with an offline storage mechanism in order to manage permissions explicitly for each line item, rather than giving complete access permission in definitely. Offline storage such as Level DB or any cloud storage can be used to limit the amount of data stored in the block chain. This could however result in a limited third party dependency, but makes the solution more scalable.[10]

3. Existing System

1) **College E-Voting System Using Visual Cryptography:**
In Colleges or Organizations, elections are conducted to elect Secretary and other members. Candidates may be from different departments so therefore it is difficult for them to coordinate vote from there. A web based polling system assists the process, with security measures by which they can vote confidentially from any department. This Internet voting system provides good solutions with security using Visual Cryptography. College E-Voting System Using Visual Cryptography (VC) aims at providing a facility to cast vote for critical and confidential internal college decisions. It has the flexibility to allow casting of vote from any remote place. The election is held in full confidentiality by applying appropriate security measures to allow the voter to vote for any participating candidate only if he logs into the system by entering the correct password which is generated by merging the two shares (Black & White dotted Images)using VC scheme.

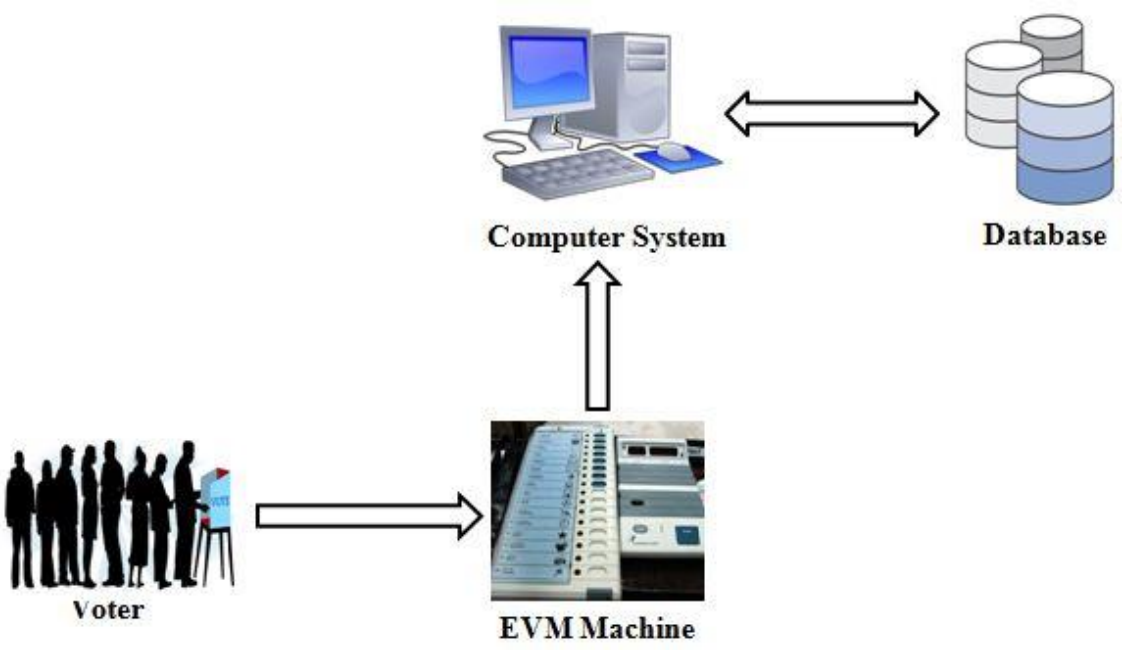


Fig. Existing System

2) Satoshi Nakamoto "Bitcoin: A Peer-to-Peer Electronic Cash System"
A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-

based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

3) Christopher D. Clack, "Smart Contract Templates: foundations, design landscape and research directions."
In this position paper, we consider some foundational topics regarding smart contracts (such as terminology, automation, enforceability, and semantics) and define a smart contract as an agreement whose execution is both automatable and enforceable. We explore a simple semantic framework for smart contracts, covering both operational and non-operational aspects. We describe templates and agreements for legally-enforceable smart contracts, based on legal documents. Building upon the Ricardian Contract triple, we identify operational parameters in the legal documents and use these to connect legal agreements to standardized code. We also explore the design landscape, including increasing sophistication of parameters, increasing use of common standardized code, and long-term academic research. We conclude by identifying further work and sketching an initial set of requirements for a common language to support Smart Contract Templates.

4) EppMaaten, "Towards remote e-voting: Estonian case"
This paper gives an overview about the Estonian e-voting system. Paper discusses how the concept of e-voting system is designed to resist some of the main challenges of remote e-voting: secure voters authentication, assurance of privacy of voters, giving the possibility of re-vote, and how an e-voting system can be made comprehensible to build the public trust.

5) **J Paul Gibson**, "A review of E-voting: the past, present and future"
Electronic voting systems are those which depend on some electronic technology for their correct functionality. Many of them depend on such technology for the communication of election data. Depending on one or more communication channels in order to run elections poses many technical challenges with respect to verifiability, dependability, security, anonymity and trust. Changing the way in which people vote has many social and political implications. The role of election administrators and (independent) observers is fundamentally different when complex communications technology is involved in the process. Electronic voting has been deployed in many different types of election throughout the world for several decades.

6) Muhammad Ajmal Azad, "M2M-REP: Reputation of Machines in the Internet of Things" 2017.
The Internet of Things (IoT) is the integration of a large number of autonomous heterogeneous devices that report information from the physical environment to the monitoring system for analytics and meaningful decisions. The compromised machines in the IoT network may not only be used for spreading unwanted content such as spam, malware, viruses etc., but can also report incorrect information about the physical world that might have a disastrous consequence. The challenge is to design a collaborative reputation system that calculates trustworthiness of machines in the IoT-based machine-to-machine network without consuming high system resources and breaching the privacy of participants. To address the challenge of privacy preserving reputation

system for the decentralized IoT environment, this paper presents a novel M2M-REP (Machine to Machine Reputation) system that computes global reputation of the machine by aggregating the encrypted local feedback provided by machines in a fully decentralized and secure way

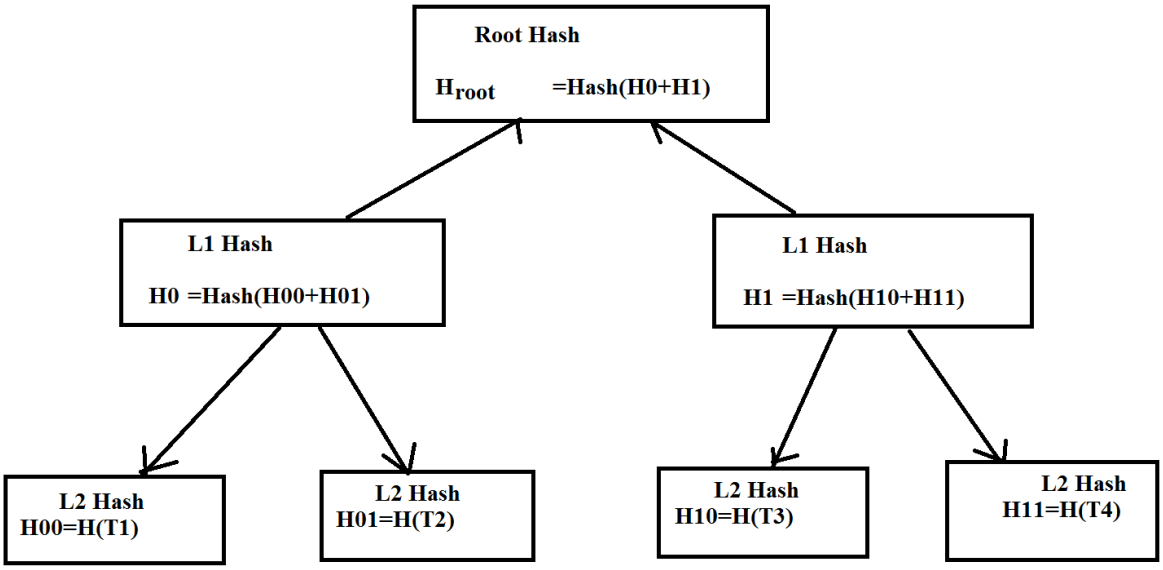
7) KashifMehboob Khan "Secure Digital Voting System based on Blockchain Technology."
Electronic voting or e-voting has been used in varying forms since 1970s with fundamental benefits over paper based systems such as increased efficiency and reduced errors. However, there remain challenges to achieve wide spread adoption of such systems especially with respect to improving their resilience against potential faults. Blockchain is a disruptive technology of current era and promises to improve the overall resilience of e-voting systems. This paper presents an effort to leverage benefits of blockchain such as cryptographic foundations and transparency to achieve an effective scheme for evoting. The proposed scheme conforms to the fundamental requirements for e-voting schemes and achieves end-to-end verifiability. The paper presents details of the proposed e-voting scheme along with its implementation using Multichain platform. The paper presents in-depth evaluation of the scheme which successfully demonstrates its effectiveness to achieve an end-to-end verifiable e-voting scheme.

4. Related Work

4.1 Open Block Chain : A blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree. Each block includes the cryptographic hash of the prior block in the blockchain, linking the two. The linked blocks form a chain. This iterative process confirms the integrity of the previous block, all the way back to the original genesis block.Blockchain technology aims at creating a decentralized environment where no third party is in control of the transactions and data. It is used in several domains due to its benefits in distributed data storage and the possibility of audit trails.

4.2 Closed Block Chain: A private network that maintains a shared record of transactions. The network is accessible only to those who have permission and transactions can be edited by administrators.Permission Blockchain inversely proportional to the previous type, operated by known entities such as consortium blockchains, where consortium members or stakeholders in a particular business context operate a Blockchain permission network. This Blockchain permission system has means to identify nodes that can control and update data together, and often has ways to control who can issue transactions. Private blockchain is a special blockchain permitted by one entity, where there is only one domain trust. The widely known Blockchain technology currently exists in the Bitcoin system which is the public ledger of all transactions. Bitcoin is a decentralized, peer-to-peer digital payments system based on the first public key cryptography. Bitcoin uses a consensus protocol called PoW (Proof of Work) based on crypto currency to ensure only legitimate transactions are allowed within the system.

Transaction In a Block:

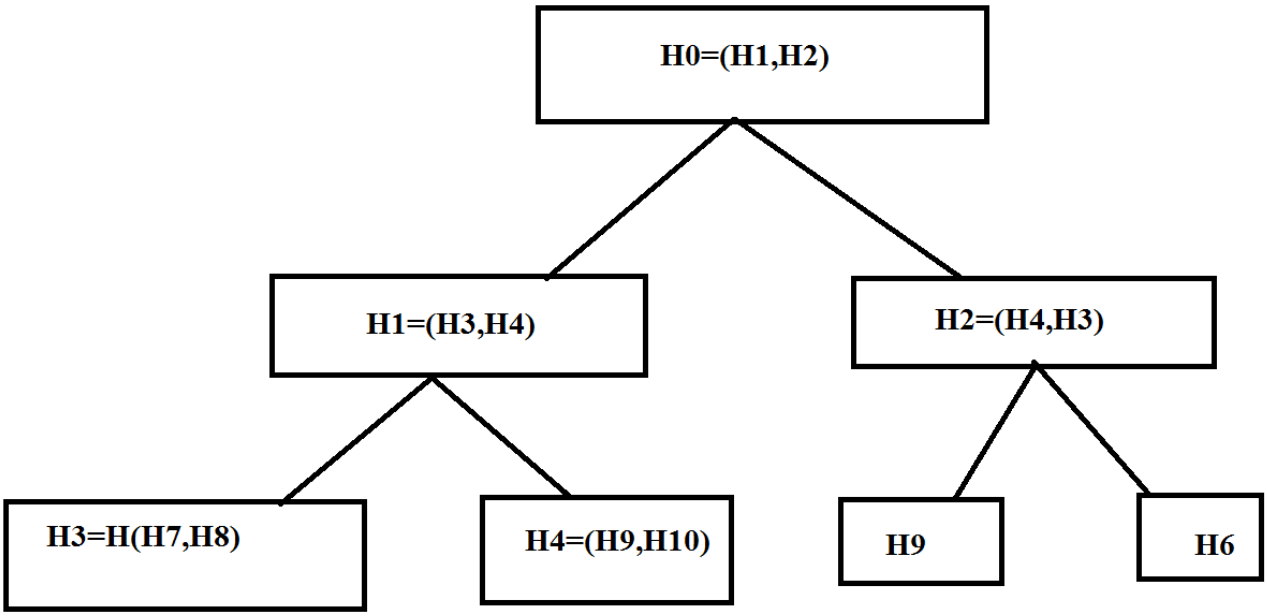


4.3 Cryptography: is used to preserve privacy and transparency at the same time, economic incentives are used to encourage desired behaviour of network actors who do not trust or know each other, nor have any legally binding agreements with each other. Cryptography is the practice and study of techniques for secure communication in the presence of third parties. Cryptography literature often uses the name Alice "A" for the sender, Bob "B" for the intended recipient, and Eve "Eavesdropper" for the adversary. There are two kinds of cryptosystems: symmetric and asymmetric.

1. Symmetric Cryptography: Two parties agree on a secret key (private key) and use the same key for encryption and decryption. The problem with this approach is that this method does not scale. If you wanted to communicate privately with somebody you would need to physically meet and agree on a secret key. In the world of modern communications, where we need to coordinate with many actors, such methods would not be feasible. Furthermore. Data manipulation in symmetric systems is faster than asymmetric systems as they generally use shorter key lengths. On the other hand, encrypting files and messages with asymmetric algorithms might not always be practical. The main reason is performance. Symmetric key cryptography is much faster and handles better the encryption of big files and databases, therefore, is still widely used.

2. **Asymmetric Cryptography (Public Key Cryptography):** Asymmetric systems use a public key to encrypt a message and a private key to decrypt it. Use of asymmetric systems enhances the security of communication. Private keys should be kept secret and a public key could be freely distributed between parties. In an asymmetric encryption scenario, two parties would distribute their public keys and allow anyone to encrypt messages using their public keys. Because of how a key pair mathematically works it is impossible to decrypt a message which got encrypted with a public key.

4.4 Merkle tree : In cryptography and computer science, a **hash tree** or **Merkle tree** is a tree in which every leaf node is labeled with the hash of a data block and every non-leaf node is labeled with the cryptographic hash of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of large data structures. Hash trees are a generalization of hash lists and hash chains.



4.5 Role Of Miner: This process begins when the voting process at each node has been completed. Before the election process begins, each node generates a private key and a public key. Public key of each node sent to all nodes listed in the election process, so each node has a public key list of all nodes. When the election occurs, each node gathers the election results from each voter. When the selection process is completed, the nodes will wait their turn to create the block. Upon arrival of the block on each node, then done verification to determine whether the block is valid. Once valid, then the database added with the data in the block.

4.5 E-voting System: E-voting currently widely used by some countries in the world, for example in Estonia. The country has been using the e-voting system since 2005 and in 2007 conducted online voting and was the first country in the world to conduct online voting. Since then, a legally binding online voting system has been implemented in various other organizations and countries such as the Austrian Federation of Students, Switzerland, the Netherlands, Norway, and so on . But it still has considerable security issues and the selection is often canceled. Although getting a lot of attention, online voting system is still not widely done in various countries around the world. The traditional voting system has several problems encountered when managed by an organization that has full control over the system and database, therefore the organization can tamper with the database, and when the database changes the traces can be easily eliminated. The solution is to make the database public, the database owned by many users, which is useful to compare if there are any discrepancies. The solution to the e-voting system is compatible with using blockchain technology. Blockchain technology allows in support of e-voting applications. Each voter's vote serves as a transaction that can be created into blockchain that can work to track voice counting. In this way, everyone can approve the final calculation because of the open blockchain audit trail, the vote count can be verified that no data is altered or deleted nor is there any unauthorized data entered in the blockchain.

5. Proposed System

The blockchain technology used mostly works the same as the blockchain technology contained in the E-voting system and focuses on database recording. The nodes involved in Blockchain that have been used by Bitcoin are independently random and not counted. However, in this e-voting system a blockchain

permission is used, for nodes to be made the opposite of the Bitcoin system and the Node in question is a place of general election because the place of elections must be registered before the commencement of implementation, it must be clear the amount and the identity. This method aims to maintain data integrity, which is protected from manipulations that should not happen in the election process. This process begins when the voting process at each node has been completed. Before the election process begins, each node generates a private key and a public key. Public key of each node sent to all nodes listed in the election process, so each node has a public key list of all nodes. When the election occurs, each node gathers the election results from each voter. When the selection process is completed, the nodes will wait their turn to create the block. Upon arrival of the block on each node, then done verification to determine whether the block is valid. Once valid, then the database added with the data in the block. After the database update, the node will check whether the node ID that was brought as a token is his or not. If the node gets a turn, it will create and submit a block that has been filled in digital signature to broadcast to all nodes by using turn rules in block-chain creation to avoid collision and ensure that all nodes into block-chain. The submitted block contains the id node, the next id node as used as the token, timestamp, voting result, hash of the previous node, and the digital signature of the node.

The block-chain with the smart contracts, emerges as a good candidate to use in developments of safer, cheaper, more secure, more transparent, and easier-to-use e-voting systems. In the proposed system we solve existing following problems solve. We need transparency, authentication and provability in the voting platform. We need to assure that the people who attend the elections are real people and use correct credentials that we know in electronic environments, and we should be able to prove that any time, also we need our elections are 100% transparent as desired. So, we need to gather and check signed and time stamped data of the elections. Because, nobody should be able to change the votes after they are casted. Also, we need individuality in elections, so that nobody can vote for someone else.

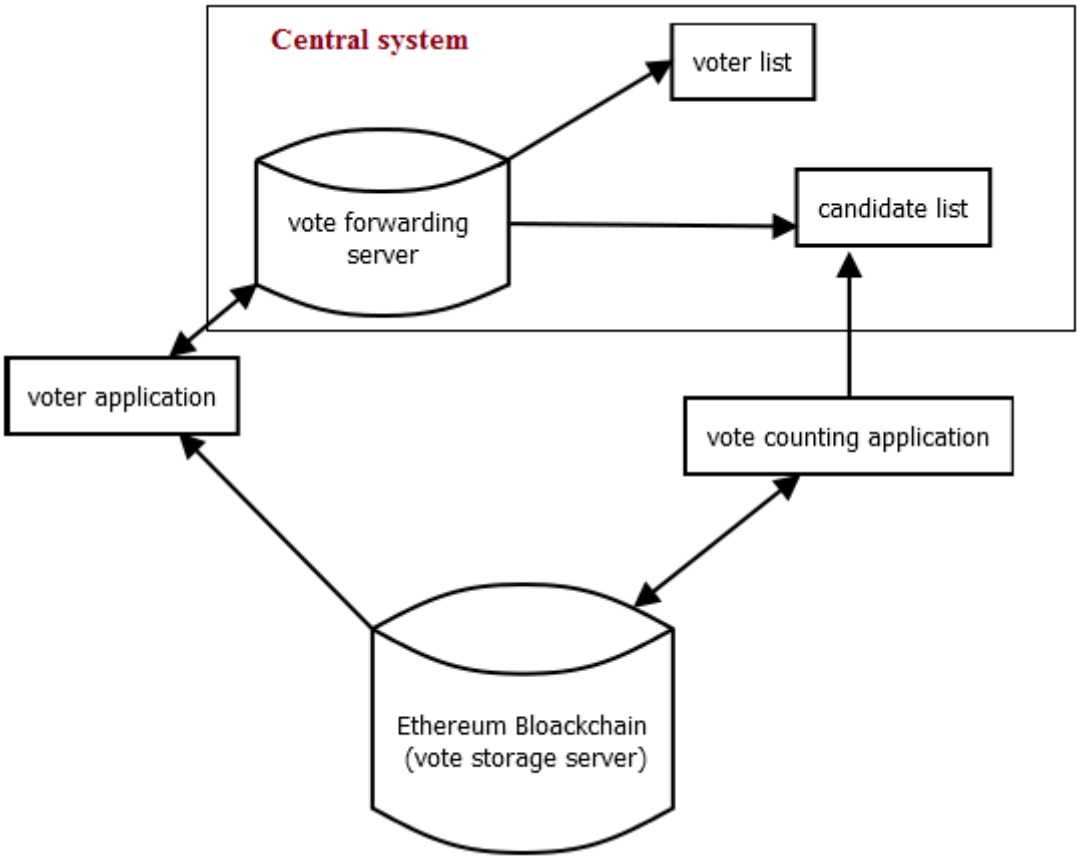


Fig. E-voting Architecture Diagram

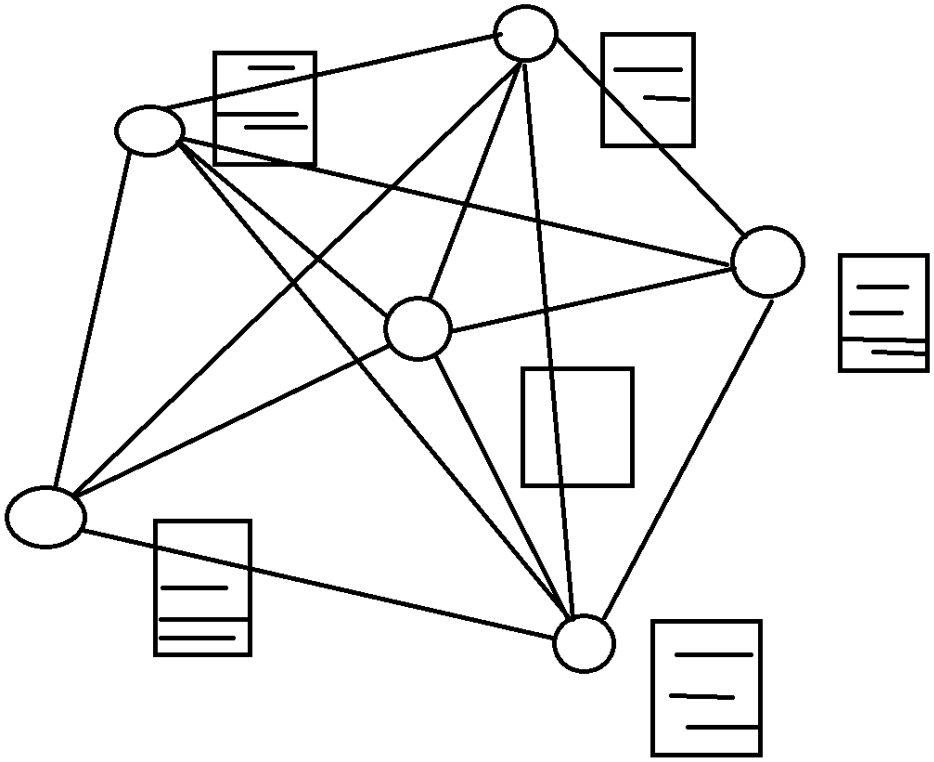
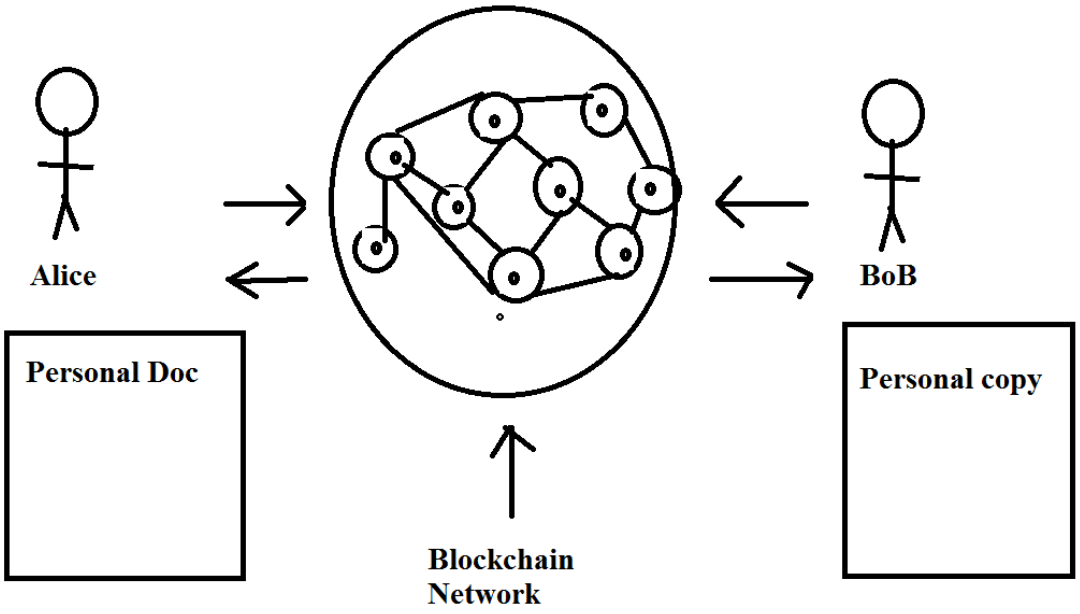


Fig. Architecture Of Block Chain

Use case Of Block chain:



Here, alice X and Bob wants to write the data in a personal doc, so here he write date in personal doc and over the network of block chain it get's exchanged and their personal copy gets updated.

6. Mathematical Model

Input: a set N Of user in the network

Input: a blockchain called B, $b_n$is the last block on the blockchain

Input: T, the deadline of voting

While Current Time()< T

For each n∈ N

Num Of Votes ←Do Vote();

for each num of votes ∈ votes

$vote_{max}$← Compare (numOfVotes);

m← Select Miner();

b_{n-1}←Get Trans(α);

$B' \rightarrow^{\text{Add Block (m,B,b}_b\text{);}}$

Foreach n∈ N

Broadcast(n)

7. Modules

In the proposed method, election is held in full confidentiality by applying appropriate security measures to allow the voter to vote for any participating candidate.

- **Admin:** admin can add candidate, voter, ward and election. He/she can perform update delete operation and declared result also.

- **Visual Cryptography:** Administrator (Election officer) sends share 1 to voter e-mail id before election and share 2 will be available in the voting system for his login during election. Voter will get the secret password to cast his vote by combining share 1 and share 2 using VC.

- **User:** Voter can vote only if he/she logs into the system by entering the correct password which is generated by merging the two shares (Black & White dotted Images)using VC scheme.

- **Block Chain:** Block chain is a distributed database that stores data records that continue to grow, controlled by multiple entities. Blockchain (distributed ledger) is a trustworthy service system to a group of nodes or non-trusting parties, generally block chain acts as a reliable third party to keep things together, mediate exchanges, and provide secure computing machines.

8. Conclusion and future work

A nation with less voting percentage will struggle to develop as choosing a right leader for the nation is very essential. Our proposed system designed to provide a secure data and a trustworthy E-voting amongst the people of the democracy. Block chain itself has been used in the Bitcoin system known as the decentralized Bank system. By adopting block chain in the distribution of databases on e-voting systems

one can reduce the cheating sources of database manipulation. This project aims to implement voting result using block chain algorithm from every place of election.

9. References

Ahmed Ben Ayed,"A Conceptual Secure Block Chain-Based Electronic Voting System",2017 IEEE International Journal of network &Its Applications(IJNSA),03 May 2017.

1. RifaHanifatunnisa, Budi Rahardjo," Blockchain Based E-Voting Recording System Design",IEEE 2017.
2. Kejiao Li, HuiLi,HanxuHou, KedanLi,Yongle Chen," Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain", 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems.
3. Ali KaanKoç, EmreYavuz, Umut Can Çabuk, GökhanDalkilic," Towards Secure E-Voting Using Ethereum Blockchain",2018 IEEE.
4. Supriya Thakur Aras, Vrushali Kulkarni," Blockchain and Its Applications – A Detailed Survey", International Journal of Computer Applications (0975 – 8887) Volume 180 – No.3, December 2017.
5. Freya Sheer Hardwick, ApostolosGioulis, Raja NaeemAkram,KonstantinosMarkantonakis," E-Voting with Blockchain: An E-Voting Protocolwith Decentralisation and Voter Privacy",IEEE 2018,03 July 2018.
6. Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan," Secure Digital Voting System based on BlockchainTechnology",IEEE 2017.
7. Huaiqing Wang, Kun Chen and Dongming Xu. 2016. A maturity model for blockchain adoption. Financial Innovation, Springer, Open Access, DOI 10.1186/s40854-016-0031-z
8. Buterin, Vitalik. 2015, On Public and Private Blockchains. [Online]https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/
9. Zyskindet. al. 2015. Decentralizing Privacy: Using Block chain to Protect Personal Data, 2015 IEEE Security and Privacy Workshops (SPW), San Jose, CA, USA, July 2015 [Online].Available: http://dx.doi.org/10.1109/SPW.2015 Jianliang Meng, Junwei Zhang, Haoquan Zhao, "Overview of the Speech Recognition Technology", 2012 Fourth International Conference on Computational and Information Sciences.