JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

E-Voting using Block Chain Technology

[1*]Yash G. Gupta, [2]Arun kushwaha, [3]Amar S. Rajeevan, [4]Bhagyashree Dhakulkar

[1,2,3,4]Department of Computer Engineering, Dr DY Patil School of Engineering and Technology, Pune, India

DOI: https://doi.org/10.26438/ijcse/v7i5.925931 | Available online at: www.ijcseonline.org

Accepted: 19/May/2019, Published: 31/May/2019

Abstract- The inflaming use of current digital technology has transformed the life of people. Unlike the current electoral system, there are various applications as such. Security is an outmost priority which is predominant in the election with the offline system. The existing electoral system still uses a Centralized system in which an organization has full access grant. The problems encountered are mostly due to outdated electoral systems with the organization that has total control over the system as well as the database. Database tampering is a major reason which causes huge problems in the system. Our answer to this problem is Block Chain Technology. Block chain Technology is an ideal solution as it holds a decentralized system and the database is owned by various users. Examples like Bit coin can be taken as a good example of Block Chain Technology application as it uses a decentralized bank system. By applying the concept of block chain in the existing electoral system, it can reduce the deceitful sources of database action. Our project aims to apply voting results using block chain algorithms from all place of election. Unlike Bitcoin, this process based on a pre-set turn on the system for each node in the built of block chain.

Keywords- Block Chain, Crypto Currency, E-Voting, Decentralized, Consensus, Marklee Tree.

I. INTRODUCTION

RECENTLY, EVMs are used in many countries. Estonia was the first in the world to accept an electronic voting system for its elections. Afterwards, it was adopted by Switzerland for its state elections, and then by Norway for its council election. For an EVM to compete with the conventional ballot system, it has to support the same standards the traditional system supports, such as security and anonymity. An E-voting system has to have intensified security in order to ensure that its available to all voter although protected against outside factors changing votes from being casted, or keep a voter's ballot fiddled with. Many electronic voting systems rely on Tor to hide the identity of voters. However, this mechanism does not provide total concealment or uprightness since many intelligence agencies around the world control different parts of the internet by which can allow them to identify or intercept votes. Increasingly digital technology in the present helped many people lives. Unlike the electoral system, there are many traditional 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 decentralized system and the entire database are owned by many users.[1]

Bitcoin presents a radical decentralized accord mechanism. However, this structure which is applied to public block chain are insufficient for the disposition situations of budding consortium block chain. Hence, it is recommend a new consensus algorithm POV i.e Proof of vote. [5,3]

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?

There is no doubt that the innovatory concept of the blockchain, which is the fundamental technology behind the famous cryptocurrency, Bitcoin and its beneficiaries, is prompting the beginning of a new epoch in the Internet and the on-line services. The current work, has employed and tested a sample e-voting application as a smart contract for the Ethereum network using the Ethereum wallets and the Solidity language. [2,4]

II. BACKGROUND

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 suppleness to allow casting of vote from any remotely place. The election is held in full concealment by applying appropriate security measures to allow the voter to vote for any partaking candidate only if he registers into the system by entering the correct password which is generated by merging the two shares (Black & White dotted Images)using VC scheme.[1,6]

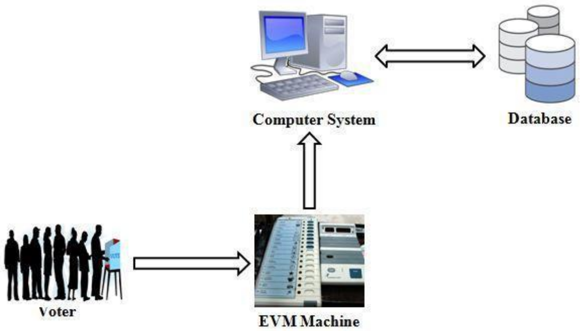

Fig 1: Existing System

III. METHODOLOGY

A. Properties of an Ideal Blockchain system.

1. Distributed

A **distributed database** is a database in which not all storage devices are attached to a common processor. It may be stored in multiple computers, located in the same physical location; or may be dispersed over a network of interconnected computers. Unlike parallel systems, in which the processors are tightly coupled and constitute a single database system, a distributed database system consists of loosely coupled sites that share no physical components.System administrators can distribute collections of data (e.g. in a database) across multiple physical locations. A distributed database can reside on organized network servers or decentralized independent computers on the Internet, on corporate intranets or extranets, or on other organization networks. Because distributed databases store data across multiple computers, distributed databases may improve performance at end-user worksites by allowing transactions to be processed on many machines, instead of being limited to one. [5,7,13]

In any kind of database system there are two key elements: the data itself and the processes that can read and modify that data. If both are centralized, it means the data and its access points are both on the same node. And if several nodes in a network need to share that data, they all need to connect to the same central point.[11,12,22,21]

To make sure no data is lost in case of a failure, you have to start distributing data, which means keeping several copies of it in such a way that, if any node fails, you can still retrieve the data from somewhere else. The ultimate distribution pattern is when each node in the network has a copy of all the data in the database. This way, any node can disconnect without preventing anyone from keeping instant access to all the data, especially if nodes are connected to each other in a peer-to-peer fashion. Now it's important to note that you can perfectly have distributed data with centralized access points. As a matter of fact, it is the easiest way to maintain consistency: only one node can modify the data, all the other nodes keep a copy of the data and synchronize with this central node in read-only mode. Now even if this central node fails, everybody still has a copy of the last version of the data, but the database cannot be modified until the modification node recovers. Another key advantage of distribution is that everyone can potentially see and verify the entire data set, which makes it very transparent. On the other hand, it does create new challenges when it comes to privacy and scalability. Privacy because, if each node has the full data set, then it can see everything, including information about users of the system. [15,14,16]

2. Decentralized.

To make sure no data is lost in case of a failure, you have to start distributing data, which means keeping several copies of it in such a way that, if any node fails, you can still retrieve the data from somewhere else.The ultimate distribution pattern is when each node in the network has a copy of all the data in the database. This way, any node can disconnect without preventing anyone from keeping instant access to all the data, especially if nodes are connected to each other in a peer-to-peer fashion. Now it's important to note that you can perfectly have distributed data with centralized access points. As a matter of fact, it is the easiest way to maintain consistency: only one node can modify the data, all the other nodes keep a copy of the data and synchronize with this central node in read-only mode. Now even if this central node fails, everybody still has a copy of the last version of the data, but the database cannot be modified until the modification node recovers. Another key advantage of distribution is that everyone can potentially see and verify the entire data set, which makes it very transparent. On the other hand, it does create new challenges when it comes to privacy and scalability. Privacy because, if each node has the full data set, then it can see everything, including information about users of the system. Each block includes the cryptographic hash of the prior block in the blockchain, associating 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.[1,9,10]

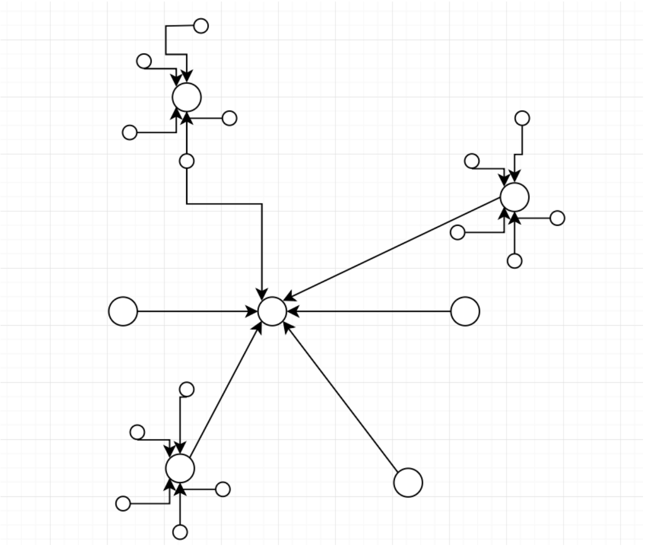

Fig 1 Representation of a distributed system.

3. Immutable

Immutable means that something is unchanging over time or unable to be changed.So in our context, it means once data has been written to a blockchain no one, not even a system administrator, can change it. This provides benefits for audit. As a provider of data you can prove that your data hasn't been altered, and as a recipient of data you can be sure that the data hasn't been altered. These benefits are useful for databases of financial transactions.Immutability is relative. For example if I send an email to a large list of friends, that data is pretty immutable from my perspective. To change it, persuade friends each to delete the email (or persuade Gmail and the people running all the mailservers . From a particular perspective, and with the control that is given, the email is immutable – One can't unsend or revoke it without collaboration and risk of detection.So immutability is relative, and relates to how hard something is to change.[1,18,19]

B. Closed Block Chain

Hyperledger Fabric is a platform for distributed ledger solutions underpinned by a modular architecture delivering high degrees of confidentiality, resiliency, flexibility, and scalability. It is designed to support pluggable implementations of different components and accommodate the complexity and intricacies that exist across the economic ecosystem.[2,17]

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 conglomerate members or stakeholders in a particular business context function 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 cryptocurrency to ensure only legitimate transactions are allowed within the system.[2]

C . Open Blockchain

Ethereum is an open-source, public, blockchain-based distributed computing platform and operating system featuring smart contract functionality. It supports a modified version of Nakamoto consensus via transaction-based state transitions. Ether is a token whose blockchain is generated by the Ethereum platform. 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 consignments 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, associating 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.[2,21]

C. Cryptography

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. It is the practice and study of techniques for secure communication in the existence of third parties. Cryptography literature often uses the name Alice "A" for the sender, Bob "B" for the envisioned recipient, and Eve "Eavesdropper" for the antagonist. There are two kinds of cryptosystems: symmetric and asymmetric.[22]

1. Symmetric Cryptography

Two parties agree on a secret key (private key) and use the same key for encryption and decryption. The trouble with this method is that this method does not scale. If you want to communicate privately with someone you would need to physically meet and agree on a furtive key. In the world of contemporary communications, where it need to synchronize with many actors, such methods would not be possible. Furthermore, data handling in symmetric systems is faster than asymmetric systems as they generally use shorter key lengths. On the other way, encoding files and messages with asymmetric algorithms might not always be a hands-on. The main motive is performance. Symmetric key cryptography is much faster and can handle better encryption of big files and databases, and hence, it is still widely used. [7,10]

2. Asymmetric Cryptography (Public Key Cryptography):

It uses a public key to encrypt a message and a private key to decrypt it. The use of asymmetric systems progresses the security of communication. Private keys should be kept a secret and a public key could be easily dispersed between parties. In an asymmetric encryption situation, two parties would circulate their public keys and allow anyone to encrypt messages using their public keys. Because of how a key pair mathematically works it is riotous to decrypt a message which got encrypted with a public key. [8,22]

3. 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 data block and every non-leaf node is tagged with the cryptographic hash of the labels of its child nodes. Hash trees allow efficient and secure authentication of the contents of large data structures. Hash trees are a generalization of hash lists and hash chains.[1,3,4,5,14]

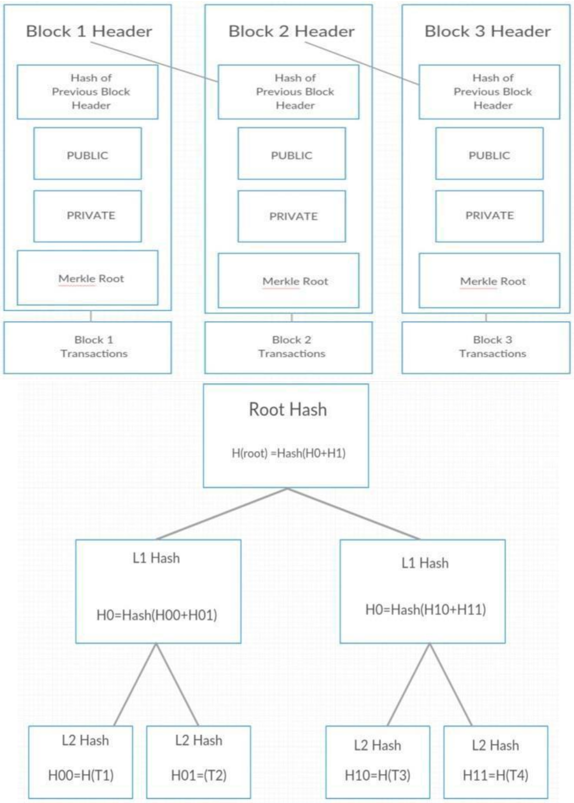

Fig 2: Markle Tree.

E. Blockchain Consensus

1. Proof of Work:

This protocol necessitates all nodes on the network to solve cryptographic conundrums by brute force. For example, in case of Bitcoin blockchain, the new transactions are cautiously committed and then based on the PoW output, a selected block created by the winning node is broadcasted to all the nodes, at a specific harmonization intervals. Once the block is transmitted using peer to peer communication to all other nodes, the same is included in the blockchain and any faltering transactions are rolled back [12]. By rule of probability, the consensus is achieved as 51% of power rather than 51% of people count. Effectively the computing power used by all other nodes except the winning node, is unexploited. [1,9]

2. Proof of Stake

Proof of stake protocol of block verification does not depend on on unnecessary computations. It implements 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. Our idea behind Proof of Stake is that it may be more difficult for miners to obtain sufficiently large amount of digital currency than to acquire adequately powerful computing equipment. For Us,it is also an energy saving alternative [10, 11]. A difference of POS is the Delegated Proof of Stake (DPOS) algorithm. Proof has been delegated proof of stake (DPOS) similar to POS, as miners get their priority to generate the blocks according to their stake. The major difference between POS and DPOS is that POS is a direct democratic while DPOS is representative democratic. Stakeholders elect their delegates to generate and International Journal of Computer Applications (0975 – 8887) Volume 180 – No.3, December 2017 31 validate a block. With significantly fewer nodes to validate the block, the block could be confirmed quickly, making the transactions confirmed quickly. Meanwhile, the parameters of the network such as block size and block intervals could be tuned by the delegates. DPOS is implemented by Bitshares. [11].

H. Comparison of Blockchain Consensus:

Algorithms Table 2 provides a quick comparison of the popular blockchain algorithms.

Algorithm	Pros	Cons
Proof of Work E.g.: Bitcoin, Litecoin, Dogecoin, Namecoin	• Considered very secure, as less prone to Sybil attack unless a mining node acquires • 51% of the pools	• Quite slow at the moment, only 1 block added in 10 mins • Driven by rewards assignedto solving the hash, may run into

	computing power. • Miners get rewards (as Bitcoins) • Prevents unlawful forking of the chain	problems as rewards dwindle • Consumes lot of electricity (mining likely to be centralized where electricity is cheap!) • Decisions are not final till 6 blocks are confirmed
Proof of Stake E.g.: Nxt, Mintcoin	• Less wasteful in terms of energy consumption • Less chance of hardware centralization • Potentially faster than Proof-of-work protocol• Possibly reduced possibility of selfish mining attack (assuming already rich miners are less likely to attack!)	• Miners are encouraged tohold on to their stake rather than converting it into at currency • Economic penalties for fraudulent attempts

IV. 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.[1]

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 the solution for existing following problems. It needs transparency, authentication and provability in the voting platform. The necessity to assure that the people who attend the elections are real people and use correct credentials that is known in electronic environments, and should be able to prove that any time, also it need our elections are 100% transparent as desired. So, gathering and checking signed and time stamped data of the elections. Because, nobody should be able to change the votes after they are casted. Also, it needs individuality in elections, so that nobody can vote for someone else.[1]

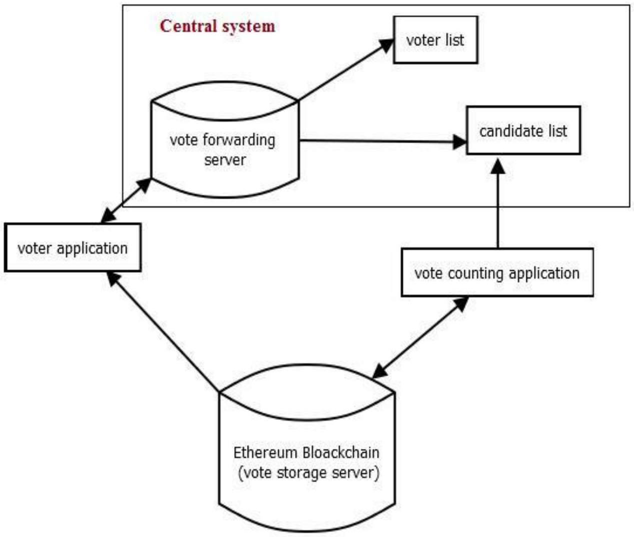

Fig 3 Representation of E-Voting System.

(1)Requesting to vote: The user login to the system his id/password - in this case, the E-Voting system will use his Social Safety no. as his address, and the voting authentication numbers provided to listed voters by the local establishments. The system will checked all info entered and, if coordinated with a valid voter, the user will be legal to cast a vote. Our e-Voting arrangement will not allow members to produce their own identities and register to vote. Systems that allow identities to be arbitrarily generated are usually susceptible to the Sybil attack [1], where aggressors claim a large number of fake identities and stuff the ballot box with illegitimate votes.

(2) Moulding a vote: Voters will vote either for their candidate or cast a complaint vote. Moulding the vote will be done through a welcoming user interface.

(3) Encoding votes: After the user casts his vote, the system will produce an input that contains the voter documentation number followed by the complete name of the elector as well as the hash of the preceding vote. This way each input will be unique and ensure that the encoded output will be unique as well. The encoded info will be chronicled in the block header of see if the results match. This way of chopping votes makes it nearly unbearable to reverse engineer, therefore there would be no way voters' information could be recovered.

(4) Adding the election to the Blockchain: After a block is created, and depending on the contender selected, the gen is recorded in the corresponding Blockchain. Each block gets linked to the previously cast vote.

V. EQUATIONS

k=hash meaning =ZML256^2
Looking for y such that F(y|z)<Target

y=y1|y2|y3|y4|y5

y1=Version

y2=hash Preceding block

y3=hash Markle Root

y4= Timestamp

y5=Target

Block Heder = y|z.

VI. BLOCKCHAIN CHALLENGES

Regulation is one of the biggest challenge for non-fiat currency. The rate of technical novelty is outdoing the rate at which regulations catch up. The currency fruition has seen a transformation in the order from authorization currency to e-money to virtual currency to cryptocurrency [13]. Cryptocurrency is the first decentralized version of currency. Some supervisory bodies hold the belief that cryptocurrency does no fulfill the purposes of money mainly due to its value unpredictability. [14] It is a challenge which is more from the domination viewpoint rather than from the cryptocurrency user’s perspective. There are already reports of Bitcoin being used for illegal activities, drug rackets, money laundering, etc. Trevor Kiviat [15] highpoints the difference between at currency and cryptocurrency and the challenges associated with cryptocurrencies regulation. IRS of USA have framed laws for taxation of Bitcoin holdings while Russia is considering banning Bitcoin due to the usage of this unfettered currency for unscrupulous purposes. China also has banned Bitcoins while Australia has approved a resolution to accept Bitcoin dealings. [16, 17] The Economist (2015) article - The magic of mining [18] a very important challenge of power consumption associated with mining and provides with some examples of how increasing power is being invested in mining activities to earn Bitcoins.

Bitcoin’s increasing adoption has led to concerns about the ability of the underlying blockchain technology to scale. Since Bitcoin is a self-regulating system that works by discovering blocks at approximate intervals, its largest transaction throughput is effectively covered at maximum block size, divided by the interval [19]. In their paper, Wei Xin et al. propose various strategies to improve private blockchain scalability. The have recommended and experimentally shown that optimization of parameters like block construction, block size, time control and deal security can lead to better performance and lower blunder rates. In the light of the fact that several international electronic primary financial exchanges have begun to announce they will explore the acceptance of blockchain technology in their trade dispensation and broadcasting for implementation and clearing, Peters and Vishnia [20] scrutinize the current status of supervisory requirements and the challenges faced by market participants in meeting them.

An stimulating tradeoff is exposed by the work by Rimba et. al. [21] On cost of storage and reckoning of business processes on a standard cloud environment vs. blockchain environment. As per the results of this experiment costs of a single business process (Incident Management) were comparatively higher on Ethereum blockchain than on Amazon SWF. However, the experiment is done for a limited scope of a single business process and the results may not be generalized, given the day- to-day advances in blockchain technology towards its optimization. One key restriction of Blockchain technology is the scalability issue due to which the size of the public or permission-less blockchain. Blockchain optimization and scalability is an area of much research. In [22], Gencer et al. propose a service oriented sharding technique to attain blockchain scalability and extensibility.

VII. EXPERIMENTAL RESULT

In this research simulation is done by using closed blockchain Tested using small number of nodes for implementation using
visualization, and large scale without using visualization with reference the number of election places in the college. Data
storage designs of e-voting systems play a very important role in real-world implementation, because how to think of

storing election data is key to protecting the privacy and integrity of the data. In the functional testing of the proposed method, it is possible to implement this method for e-voting records system because the required storage is adequate for present-day computer capacity with the results. Reliability testing is performed with the required capacity parameters on each number of nodes. With the number of nodes tested ranging from 1 to 500 many nodes assuming the number of nodes is the number of places of election then the resulting data as in. More number of nodes is directly proportional to the capacity required in the process of recording this e-voting. It is seen that more number of nodes needed, **it takes longer time** for this e-voting record system to work. In the database stored data block of all nodes that each block contains the Node ID, Next ID Node, List of Votes, Previous Hash, Digital Signature, and timestamp.In this simulation, if the node is down on the network or any other disturbance that causes the node can't broadcast block and then the node is disabled and the system has succeeded in continuing the sequence to the next node because there is counter time for each node which when the time has expired counter, Then the node knows that its turn has arrived "My Turn = TRUE"..

VIII. CONCLUSION

A nation with less voting percentage will fight to develop as choosing a right front-runner for the nation is very essential. Our future system designed to provide a secure data and a dependable E-voting amongst the people of the equality. Block chain itself has been used in the Bitcoin scheme known as the dispersed Bank system. By assuming block chain in the distribution of databases on e-voting systems one can reduce the double-dealing sources of database management. This project aims to implement voting effect using block chain procedure from every place of election.

REFERENCES

[1] Yash G. Gupta, Arun kushwaha, Amar S. Rajeevan, Govind Mhala and Bhagyashree Dhakulka, "Survey On E-Voting using Block Chain Technology",CiiT International Journal of Software Engineering and Technology, Vol 11, No 1, January 2019.

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

[3] RifaHanifatunnisa, Budi Rahardjo," Blockchain Based E-Voting Recording System Design",IEEE 2017.

[4] KejiaoLi, HuiLi,HanxuHou,KedanLi,YongleChen," 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.

[5] AliKaanKoç, EmreYavuz, UmutCanÇabuk, GökhanDalkilic," abcccTowards Secure E-Voting Using Ethereum Blockchain", 2018 cccccIEEE.

[6] Supriya Thakur Aras, Vrushali Kulkarni," Blockchain andItsApplications– A Detailed Survey", International Journal of Computer Applications (0975 – 8887) Volume 180 – No.3, December 2017.

[7] Freya Sheer Hardwick, ApostolosGioulis, RajaNaeemAkram,KonstantinosMarkantonakis," E-Voting with Blockchain: An E-Voting Protocolwith Decentralisation and Voter Privacy",IEEE 2018,03 July 2018.

[8] KashifMehboob Khan, Junaid Arshad, Muhammad Mubashir Khan," Secure Digital Voting System based on BlockchainTechnology", IEEE 2017.

[9] Huaiqing Wang, Kun Chen and DongmingXu. 2016. A maturity abcccmodel for blockchain adoption. Financial nnovation,Springer,OpenAccess,DOI10.1186/s40854-016-0031-z

[10] Buterin, Vitalik. 2015, On Public and Private Blockchains.[Online]https://blog.ethereum.org/2015/08/07/on-public-sand-private-blockchains

[11] Pilkington Mark. 2016 Blockchain Technology: Principles and saassaApplications, Research Handbook on Digital Transformations, casasaSocial Science Research Network

[12]BitFury group.2015. Public versus Private asassSBlockchainsPart1:PermissionedBlockchains,BitFury.comwhitepa pe sasas[O nline]:http://bitfury.com/content/5-whitepapers-research/public-aAaavs-private-pt1-1.pdf

[13] Cachin etal. 2017. Blockchain, cryptography, and consensus,IBMResearch,Jun2017,https://www.itu.int/en/ITU-T/Workshop and seminars.

[14]Gareth W. Peters, Efstathios Panayi, 2015. Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective, Aug 2015

[15]Trevor Kiviat. 2015. Beyond Bitcoin: Issues in Regulating Blockchain Transactions, HeinOnline.org.

[16]CNBCNews,2017,https://www.cnbc.com/2017/10/10/bitcoin-price-fallsafter-russia-proposes-ban-on-exchanges.html.

[17]AustralianTaxationOffice,https://www.ato.gov.au/General/Gen/Tax-treatment-ofcrypto-currencies-in-Australia---specifically-bitcoin/

[18]The magic of mining, 8 January 2015, https://www.economist.com/news/business/21638124- minting-digital-currency-has-become-big-ruthlesslycompetitive-business-magic.

[19]Wei Xin, et.al. 2017. On Scaling and Accelerating Decentralized Private Blockchains, 2017 IEEE 3rd International Conference on Big Data Security on Cloud,https://doi.org/10.1109/BigDataSecurity.2017.5

[20]Peters, G, Vishnia, Guy. 2016. Overview of Emerging Blockchain Architectures and Platforms for Electronic Trading Exchanges, Nov 2016, Elsevier, [Online]. http://dx.doi.org/10.2139/ssrn.2867344

[21]Rimba et.al. , 2017. Comparing Blockchain and Cloud Services for Business Process Execution, https://doi.org/10.1109/ICSA.2017.44

[22]Gencer et.al. Service-Oriented Sharding for Blockchains.[Online].http://fc17.ifca.ai/preproceedings/paper_73.pdf