International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 10, Issue 3, March - 2020
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 6.661

E-VOTING TOWARDS SECURED BLOCKCHAIN

ARCHANA S[1]
Bachelor of Computer Applications, Sri Krishna Adithya Arts and Science College

BRINDHA K[2]
Assistant Professor,Dept,of BCA, Sri Krishna Adithya Arts and Science College

Abstract—In our social life , internet plays an major role. Internet has been a rich ground for innovation and creativity. Some of the problems that occur in the traditional method of the electrol system .There is an private organization which cntrols the entire election, It is possible to tamper the database with the considerable opportunities. Distributed ledger technology is a existing technological advancement in the information technology world. Cryptocurrency and its underlying technologies has been gaining popularity for transaction management. Transaction information is maintained in the blockchain, which can be used to audit the integrity of the transaction.Blockchain are digital leger in which transaction are made in bitcoin or another cryptocurrency are recorded chronologically and publically. Public election are the basis upon which democracy is build. Thus it is utmost important that government ad organization want to held an non fraudulence representative election. Several methods are employed in order to allow citizens to cast their votes, such as ballot based voting, purely electronic voting machines, among others.However the current voting system provides unsatisfactory non transparency voting system, There might be chance for the changing votes thus it does not provide trust to people among the government .To solve this we need a transparent voting system with recorded details instead of stepping back to the old system we are introducing new technology along with the e-voting called blockchain .In this paper we can see the role of the blockchain towards e-voting.

***Keywords:*—e-voting, democracy, transparency, blockchain.**

I. INTRODUCTION

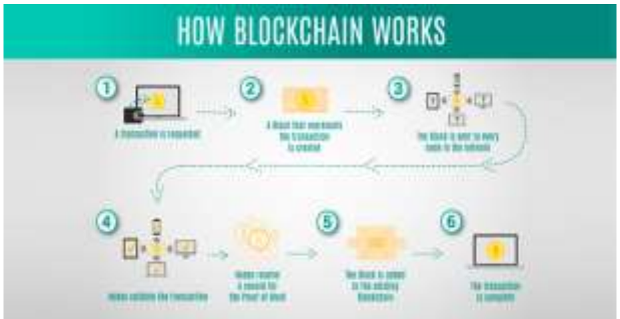
Blockchain was introduced in 2008 when santoshi nakamoto created first cryptocurrency called bitcoin. The bitcoin blockchain technology is a decentralized ledger. The blockchain technology were using in many fields especially in financial transaction. It is a digital of any transcation , contracts that need to be recorded independently. It is most secured way for transcation compared to all the methods and information are recorded .There are numerous way for doing transaction but in all methods an intermediate party. So there is a chance to pay the commission for the third party or third party can involve some fraudulence action . Blockchain relief an makerters from these tension by providing an peer to peer trancastion and recording details without an third party, the information will be open to everyone so no one change the original information. It contains an digtal ledger ,the details of the participants are recorded. The recorded details will not able to share each other only they can view . The ledger will be recorded in many system because when one system shows an error or some wrong information we can able to refer another system .Fradualance happened not only in finnce field but also in election. It is a big issue to solve this problem blockchain came into this area called E-voting . Blockchain evoting was introduced by Moscow authority inorder to implement the active evoting system.It was launched in 2014.In this paper we can see about it.

II. BLOCKCHAIN

A. INTRODUCTION:

Blockchain was introduced by SANTHOSHI NAKAMOTO in the year 2008.He proposed a new system for the exchange of most popular cryptocurrency called Bitcoin. Bitcoin is a money which represent value in the future like investing money in gold, dimond etc., When we have money in our hands then we will spend it for buying new things daily then we don’t have any savings in our future ,we don’t have any money to spend in any emergency arrives,day by day our expenses will increase it will not godown.Income will godown but expenses not,to solve this issues people are started to investing in some valuable things, likethat we can invest our money in the Bitcoin called cryptocurrency.Bitcoin is the largest cryptocurrency in the market we can transfer a value using a digital currency. There are many drawbacks in using a paper currency note example: when RBI bank are manufacturing the rupees note and deliver it to all other banks and the nearby banks distributing the money for the public .The money is transferring with the help of third party to the public, there is some possibility of involving some crime activity by the bankers there might do some corruption.Currency is supplied to the public with the help of centralized authority,To avoid this Bitcoin is introduced. Bitcoin only do peer-peer transaction without centralized authority but the details are not recorded ,to record the details of the participant bitcoin uses a Blockchain technology .It is a digital ,transparent ledger. Bank contain a ledger which is centralized and non-transparent ,it is maintained by the manager of the particular bank and the data and a ledger are stored only in the manager or incharger system ,there might be a change of fraudulence attack and doing some criminal activity, To be secure and transparent blockchain technology is used everywhere .

B. WORKING PROCESS IN BLOCKCHAIN: Blockchain is the digital transparent ledger .



Explanation: A transaction is requested by any international company or an bitcoin ,railway sector,bank etc., the given input into the block it performs Hashing functions i.e., the block applies an hashing algorithm to the input there are several hashing algorithm eg.;sSHA-256 the output will be received in 256 char length as a hash key.The given data will be stored in the block as a hash key value. Now the block is created and it will be posted publicly ,that block will send to each and every node(computers)Every person can view the block and every node must check whether the transaction is done by valid person and verify it,each and every node will receive a proof of work ,the nodes want to prove that they solve a computational mathematical work and submit the proof after that only the block will be added to the blockchain before adding any block into the blockchain a prior information should be given to all the blocks contained in the blockchain.The process of adding a block into the blockchain called “MINING”. In fact, the odds of solving one of these problem on the Bitcoin network were about one in 15.5 trillion in January 2020. To solve a complex math problems at those odds, computers must run programs that cost them significant aounts of power and energy.

.Proof of work does not make the hackers impossible to attack the block contain in the blockchain but it make them somewhat useless. If the hacker want to coordinate an attack an blockchain then they would control more than 50% of the computer power on the blockchain so as to be able to overwhelm all other nodes in the network.Given the tremendous size of the Bitcoin Blockchain, a so called 51%attack is almost certainly not worth the effort and likely impossible.

Evoting:

E-voting or electronic voting refers to the computerized voting system that use the electronic ballot than the paper ones.They are also called as direct-recording electronic machines. The election which was held using paper completely insecured any one can change the vote and the fradualance activity become exceed .so the e-voting system came into existence .E-voting machines consists of three types:

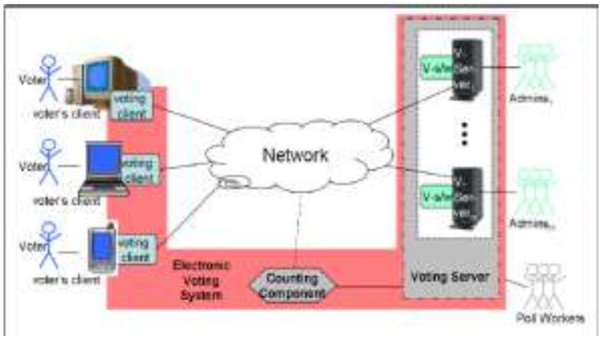
- Touch screen machines that let the voters cast votes by touching an electronic ballot on a LCD screen.
- Punch-key machines that use a keypad for making selections on the ballot
- Wheel machine that require the voters to rotate the wheel and press a button.

There are many issues arises in the past voting system , so congress passed the help America vote, among other things, designated about $4billon to states to improve election procedures and replace the past method(punch card machines) with the new E-voting machines.

Working process of e-voting:

E-voting machine contains two parts control unit and ballot unit. Ballot unit was acessed by the voter .when the voter press a ballot button in the ballot box a name of the voter and id was automatically send to the control unit box through the wire connection. After the voting process completed the ballot box was closed and sealed .A control unit contain an memory chip and removable memory card. Every votes are stored in both memory chip and removable memory card at the end of the election pool workers remove the memory card and taken it to the tabulation center and loaded on the computer and the votes are tabulated getting an unofficial election result. After few days when official tallies are the elections officials check and compare the votes in memory chip and the memory card when it is equal then the result will be announced officially.

PROBLEMS TO CONSIDER:



E-voting is entirely centralized and non-transparent voting method. aThe criminals able to create an duplicate digital LED display and fixed into the control unit,the display will show only a vote favour to the one part . Even some technical hackers can able to hack and change the votes using a single mobile . It is not a safe way . To make a voting system secure and transparent way we aare introducing an blockchain technology in the E-voting.

BLOCKCHAIN TOWARDS SECURE E-VOTING:

The E-voting using an secured blockchain was provided to conduct a well secured election without any criminal involvement. Blockchain would contain an transparent and decentralized leger i.e, records. This method provide us security,immutability,fairness,verifiability, distributed records.

- Immutability: When we want to add a new ledger then it provides an reference to the entire blockchain and show the details of the new block.
- we can prevent a tamper.
- VERIFIABILITY: The ledger is open and distributed to all the nodes, each and every transaction of the party are recorded in all the node so all the nodes can verify it by sending a proof of work.
- Distributed consensus: A distributed consensus protocol to determine who can append the next new transaction to the ledger.

  The entire node came to known before any new proposed block ledger add to the permanent part of the blockchain it is well verified by the nodes. This is achieved through the cryptography. This provides an security level very high compared to all other system.so we are implementing this blockchain technology to the E-voting. Blockchain solves an various issues faced by the current e-voting system by making a entire system as decentralized without involved any thirdparty, itsolves transparency, security, accessibility, audibility etc., in the current e-voting system.

  Since the blockchain provide us a permanent record of transaction (votes) and votes are distributed to every nodes and can be traced back when and where it happened without the voters identity.Past votes cannot be changed and future voted cannot be hacked because every votes are maintained by every nodes.If the attacker want to hack the record means the attack should have 51%of the cpu power,to alter the records.It is impossible.Even when the hackers achieve that while incorrectly achieving user votes with their real IDs of radar,end to end voting systems could allow voters to verify whether their vote was correctly entered in the system,making the system extremely safe.

IMPLEMENTATION OF THE E-VOTING BLOCKCHAIN USING ETHEREUM:

Etheruem is a platform in which application can be build which is decentralized and open to every one. Bitcoin provide us only the transaction using an blockchain.In order to implement blockchain in all the fields etherum was created .It is a platform to create a decentralized application with the usage of blockchain technology.Ether crypotocurrency in whose blockchain are generated by the etherum platform.Ethereum platform provides a decentralized complete turning virtual machines.called Ethereum virtual machines or EVM. EVM is used to run a Decentralized application. , it is a platform for running an etherum network.

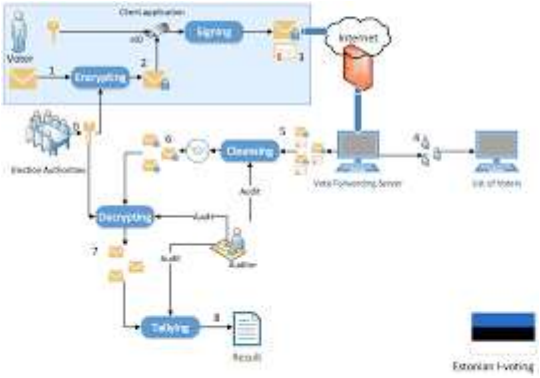
CORE COMPONENTS OF THE ETHEREUM:

- Smart contract: Smart contract is a backend logic and storage process. It is a self executing agreement between the buyer and the seller which is written in the lines of code.The code and agreement are exist across the blockchain whether the transaction send properly i.e,the buyer received the product or not. Nick Szabo, an American computer scientist who invented a virtual currency called "Bit Gold" in 1998, defined smart contracts as computerized transaction protocols that execute terms of a contract.
- Smart contracts render transactions traceable, transparent, and irreversible.
- It is combined with the EVM bytecode and deployed with the etherum blockchain for execution.

SYSTEM ANALYSIS:

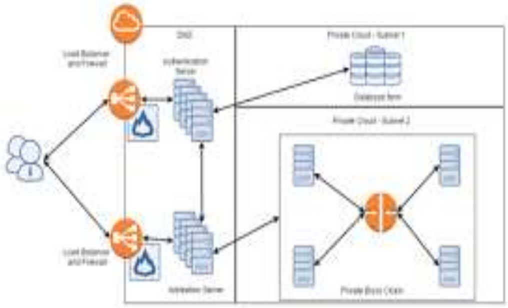
Existing system:

Now a days digital voting system were implemented in most of the country all over the world. Estonica was the first country implementing online voting in 2005 and since 2007. Estonia was implemented the online voting i.e, i-voting in the Parlimentary election held o 2015 and 30.5% of votes were recorded. An ID card is given to each citizen and the card holds identification details of the owner. The card contain completely encrypted files the person holding an card can able to perform all the online and electronic activities including online banking services, digitally signing documents, access their information on government databases and i-voting. In order to put their vote the user want to insert their card into the card reader and access the voting website on the computer then the voter should enter their PINCODE ,the card reader will check whether the person is eligible for voting. Once confirmed, they are able to cast/change their vote up until four days before election day. Voters can use their mobile phone while card reader is not there in their computer system. The vote forwarding server will transfer every voter to the vote storage server which is encrypted,the votes are stored until election was over,then the votes identification is cleaned taken to the vote counted server by DVD which makes votes decentralized and result was announced. The vote counted server was disconnected to all the network .Each stage of this process is logged and audited. During 2003 logged election Election commission were found that this method was insecure. One such risk is the possibility of malware on the client side machine that monitors the user placing their vote and then later changing their vote to a different candidate. Another risk the hacker can able to modify the DVD and place the duplicate one ,through that it is possible to count the vote favour to one party. However, this report has also come under criticism from the Estonian Information Systems Authority.



PROPOSED SYSTEM:

To solve this issues we are implementing an blockchain technology with the existing system.



NETWORK ARCHITECTURE:

This shows user interaction with the system.

PARTS AND FUNCTIONALITY:

AUTHENTICATION SERVER:

Authentication server is a type of network server that validates and authenticates remote users or it nodes connection to the application or server.This system is used to validate all the credentials given by the user .It is a traditional centralized web server .It maintains a backend database connected to the information of all citizens.This system is used to register their vote in the election ,after registering it was verified by AS server if it is valid then user can create an login account and also creates an blockchain account when all the credentials are valid, Typically it validate the identity and granting person for each nodes. It also creates accounts on the blockchain system for the users when they vote. The blockchain account is used by the Arbitration Server to vote for a candidate of the users' choice. The AS also authenticates the token provided to the Authorization Server by the user while voting.

ARBITRATION SERVER:

Arbitration Server(AR) The Arbitration Server acts as an intermediary between a user and the Blockchain voting system. It verifies the user while voting using the Authentication Server. The AR is a blockchain thin client that sends the users' vote to a blockchain node [3]. It also sends the user the key to encrypt their vote. The AR sends the users' vote to the appropriate node to be added to the blockchain. The user can verify their vote using the AR as an intermediary.

BLOCKCHAIN:

The actual voting process will take place in the blockchain.The user vote is sent to one of the nodes in the system ,the node will verify and send the copy to all other nodes then it will add to the blockchain using the smart contract. Smart contract verify each node whether the transaction are in the proper way or not. The node add verified transaction to the blockchain ,it contains all the records.

PROCESS OF THE SYSTEM:

The voting process takes place in two steps an registration and process of voting. In this method we are adding a verification step user can able to verify their vote and data records are decentralized transparent to every one no one can able to change the vote.

REGISTRATION:

This process starts by user interacting with the Authentication server. As a authentication server stores an users information in the backend database , the user want to register the personal identifiable information (pii) and scan support documentable to upload into the system, users picture also taken for verification .The AS checks whether the registered information is matched with the AS server database, if it matches then it allowed to create a login account the user can able to give an username of his/her choice then password to login it was maintained separately

This ensures privacy and anonymity while voting ,then the process will continue for the next user .

VOTING:

The process of voting involves various steps .The candidates of the election was given an blockchain account so that they can view the result i.e., number of votes they gain. The user register their details and it was verified by the Authentication server when it is correct then user can able to create an login account as mentioned in the previous process. During the voting day the user want to login the created account with the username and the password already given during registration. An image is taken and compared with the registered image to ensure the owner of the account. A short video is taken to the user and send it to the AS it will examine the users emotional condition with the help of machine learning technology. It will detect the emotion percentage of the user and if it identifies whether the is in fear or some abnormal condition ,it the result shows the person was not in the normal state he had some fear and told the user to try after 5 minutes. When the system detect and give the message as the person in fear then voter access will be stop completely in that system and ask them to go some open place such as school, library so that they can feel relax without any stress. It is most consider thing the person who is going to register their vote should be in very relax manner and absolutely behave in the normal way.

After the user login into the account the system would create an public key for each user and then send it to the AS, it is very important to create a unique key for each voter . AS will associate the public key with the username . The main purpose of the key is to create an account in the blockchain so that the details of the voter would be saved permanently and there is no chance of changing the vote ,it provides completely safety to all votes. An ether is added to the username to allow the voter to vote. AS will send back an session token to the user. The user would that token to the AR after it would verified by the AS. The verification and generation between user, AR, AS can be done by using an Needham-Schroeder protocol, this would prevent the from the third party accessing .The AR will send an verification message along with the public key , by which user can send a vote to the blockchain,then the user will encrpt their vote with the public key and again send it to the AR. The AR make sure it doesn't able to read the vote which is encrypted after ensuring that it will send to the appropriate node.The node will decrypt the message or vote by using an private key then it will send to the blockchain account of the candidate. The node verify its transaction according to the smart contracts. This contract would check whether the vote was duplicate or not and its validity.After this process the node would pass this transcation to all other nodes in the blockchain and recorded everywhere it become impossible to change the votes .

VERIFICATION OF THE VOTE:

The result will be verified according to what type of election was held. Some election will allow interim result or some do not. In either case people want to verify whether their vote counted or not. The election which allow the interim result one of the nodes in the blockchain can be viewable and publically accessible. It contain an website such as www.blockchain.info .Visiting these type of website and enter an public key given to the user voter can able to verify, but those publicly accessible node are only in the readable format ,the votes cannot be changed or altered .This provides extremely secured platform for voting. If election commission decided to keep the interim result secretly.A verification message will send to the user in the binary format via AR.AR is used to verify the votes, it acts as a thin client server. The user will able to check the result at the end of the election.

COUNTING VOTES:

At the end of the election the number of votes are counted and the winner candidate will be announced.The winner party rule the country for five years In the old system the result will be announced by the third party i.e., election commission.In this type of election a particular amount of ether will be given to the voter and they transfer it the candidate's account .The candidate who having higher amount of ether amount are announced as winner party. For users who abstained from voting, their ether will be sent to an Abstain Account. This ensures their vote does not get misused.

Recounting the votes:

There are instances of disputes in the results of an election. These can be resolved in the proposed system easily. The entire tree associated with a single account root can be made public for people to verify if their vote has been tallied or no [5]. This makes the system transparent for users. Since no one knows which user is associated with which account, it protects the users' anonymity in voting. The public keys for each transaction in the blockchain system can be mapped to accounts in the AS. The list of public keys generated gives the list of people who voted. By mapping this list with the public keys associated with each transaction, the election can be verified.

ECONOMIC BENEFITS:

- Economic advantages of the system Cost benefit analysis of proposed system Cost of labor per person = $80/hour
- Requirement of 25 people over 12 months to build and test the system One time Cost to customer = $4,000,000
- Cost of hardware and maintenance for 1st election = $100,000,000 for a voter base of 100 million (based on EC2 calculator) (Includes data center costs, network equipment and bandwidth)
- For subsequent election cycles cost = $50,000,000
- Cost of running a ballot based election = $2 per person [6] = $200,000,000 for 100 million voters.
- The cost of running the election for the 1st year using proposed system = $104,000,000

SOCIAL BENEFITS:

This system creates an very positive impact towards election. Trust and confident towards election have increased while implementing this blockchain method .It pull all the criminals and hacker in the harder situation .It provides a transparent and independent ledger contains the voter details so voter can view whether their vote are counted reached to the right candidate for whom they put their vote. This system provides people to trust the government in more efficient way.It is a better platform comparing to the paper ballot system.

CONCLUSION:

In this paper we have seen the overview of blockchain technology and it is used not only in election but also in various fields .Here we have seen the usage of blockchain technology in the election.

REFERENCES

[1] Bhagwat Shraddha, Khamkar Sandhya, Nimbhore Sandip, Prof. Hirave. K..S, "Towards Secure E-Voting using Ethereum Blockchain," Department of Computer Engineering H.S.B.P.V.T COE, Kashti, Maharashtra, India. volume 9, issue 4.

[2] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa , Gísli Hjálmtýsson, "Blockchain -Based E-Voting System",
School of Computer Science Reykjavik University, Iceland {fridrik14, gunnlaugur15, mhamdaqa, gisli}@ru.is.

[3] Dr. Prasath , Joshwa Daniel Raj , Kabesh , Karthikeyan , "E-VOTING SYSTEM USING BLOCKCHAIN," vol:6,issue:0, 1Associate Professor, Dept. of Computer Science and Engineering, KPRIET, Tamilnadu, India 2,3,4Student, Dept. of computer science and Engineering, KPRIET, Tamilnadu, India.

[4] Prof. Pallavi Shejwal, Aditya Gaikwad, Mayur Jadhav, Nikhil Nanaware ,Noormohammed Shikalgar Assistant Professor, Department of Information Technology, BSIOTR, Pune, Maharashtra,India, "E-voting using blockchain technology,"Dec 2018,vol:5,issue:04.

[5] D. Dwijesh Kumar, D. V. Chandini, B. Dinesh Reddy, Debnath Bhattacharyya and Tai-hoon Kim, "Secure Electronic Voting System using Blockchain Technology".