ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 12, Issue, 11, pp.14960-14965, November, 2020

DOI: https://doi.org/10.24941/ijcr.40251.11.2020

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

E-VOTING SYSTEM USING BLOCKCHAIN

***Geeta Brijlal. Kotwani**

Department of Computer Engineering, DR. D. Y. Patil School of Engineering, Pune, India

ARTICLE INFO

Article History:
Received 20th August, 2020
Received in revised form
17th September, 2020
Accepted 25th October, 2020
Published online 30th November, 2020

Key Words:
Nutritional Psychiatry,
Coenzyme Q10, Brain Disordens,
Heart Diseases.

ABSTRACT

Conventional Elections have never satisfied Citizens and the losing legislative Parties due to some Obvious Reasons present in the Conventional Voting Systems Like Easy to Clog, Non-Transparency and Opaqueness. Over to it the Time taken to Conduct Elections is Extravagant. This Paper put forwards a much required Solution using the Secure Block chain Technology to Overcome all the Disadvantages present in the Conventional Voting System. With this Distributed Ledger Technology, Security, Privacy, Data Integrity and Disability to Hamper will be Attained resulting into People and Legislative Parties Faith and Trust in Casting their Votes. Thereby generating the Election Results in the Stipulated Time. This Paper will Induce the Requirements for Building E-Voting System using Blockchain and will also trace the Legal and Technological Limitations of Using Blockchain.

Citation: ***Geeta Brijlal. Kotwani.*** **2020.** "E-Voting System using Blockchain", *International Journal of Current Research*, 12, (11), 14960-14965.

INTRODUCTION

Voting is an Important and Integral Part of Democracy. Till Today, Paper was Used to Conduct Elections which led to Insecurity in the Minds of People and brought about In-Accuracy in the Final Results. But now as we enter into the 21st Century, Its time to change the Voting Methods according to the new Technological Inventions. Digital Voting Involves using Electronic Gadgets, new Technologies, Web of Information i.e. Internet, to Cast Votes. This Technology is coined as Electronic Voting or E-Voting.

There are 2 types of Voting:

- E-Voting which uses a Machine in a Poll Station
- I-Voting which uses a Browser.

Due to Orthodox Thinking many People don't have faith on Digital or Electronic Voting, they doubt on the Security of E-Voting System. One way the Doubt of Insecurity can be Resolved is by the Technology of Block chains. Block chain Technology is a Technology that stores records which are Transactional, also known as the Block, of the Public in several Databases, known as the "chain", in a network connected through peer to peer nodes. Customarily, this storage is referred as "Digital Ledger". The Digital Ledger is Synonyms to Google Spreadsheet which is shared among so many Computers in a Network connected through peer to peer nodes. Customarily it is referred "Digital Ledger". These Technological features operate through a Technology called Cryptography which is now used in Bitcoin. This Cryptography is even more Secure than the Databases. The Block chain Technology will therefore be Considered while designing the Vital Part of Democracy i.e. Voting. This Paper will evaluate the use of Block chain in Implementing an E-Voting System using Blockchain. Conditions to be Fulfilled by the E-Voting System using Blockchain:-

Following things should be fulfilled by the E-Voting System so that it can be used Confidently by the Nation when Conducting Important and Big Thing like Elections:-

- An Election System should be away from Compelled Voting.
- Traceability of a Vote to a Voter's identifying Credentials should Strictly be Prohibited.
- An Election System should be able to give Evidence to a Voter that his or her Vote is Counted.
- This System should only allow those Individuals which are Registered by the Administrator and are Eligible.

Blockchain is such a Technology in which once data stored cannot be changed or deleted. This makes this Technology Immutable.

Types of Blockchains:

- Public Blockchain:- No accessing restrictions are there. Anyone who has an Internet connection can send Transactions to it as well as become an Administrator. Networks offer Financial Incentives to those who are Securing the Network.
- Renowned Public Blockchains are the Bitcoin Block chain and the Ethereum Blockchain.
- Private Blockchain:- A Private Block chain is permission ed. To join the Block chain, Invitation by the Administrator is Mandatory. Participant and Validator Access is Restricted Strictly. For Private Block chains Distributed Ledger Technology (DLT) is used.
- Hybrid Blockchains:- As the name suggests, it is a Combination of Centralized and Decentralized Features.
- Sidechains:- A Sidechain is a Designation for a Blockchain Ledger that runs in Parallel to a Primary Block chain.
- Cryptocurrency also provides a platform for building distributed and immutable applications or smart contracts.

History of Blockchain: The Blockchain technology came into existence in the year 2008 when Satoshi Nakamato created the first Cryptocurrency called "BitCoin". Decentralized Ledger Combined with Proof of Work(PoW) is used in the Bitcoin Technology.

BLOCK-CHAIN

The Blockchain Structure is also known as an append-only data structure, such that new blocks of data can be written to it, but cannot be altered or deleted. Private blockchain limits the read and write access, only specific participants can verify their transactions internally. That makes the transaction on a private network cheaper, since they only need to be verified by few nodes that are trusted and with guaranteed high processing power. Nodes are very well-connected and faults can quickly be fixed by manual intervention, allowing the use of consensus algorithms which offer finality after much shorter block times.
In our Research we will use Permissioned Blockchain which will use the Proof of Authority(PoA) consensus Algorithm. A Consensus Algorithm is used to set restrictions on selected known entities to certify and validate Transactions on Blockchain. Here, this will help us to stop adding new People without Administrators Permission. This Algorithm Proves to be Helpful because it does not leak the Voter's Information and Voting Data.

Smart Contracts: Smart Contracts are a fixed line of code which are stored on the Decentralized Ledger i.e. Blockchain and are only executed when all predetermined terms and conditions are met. At the basic level, it can be explained that they are Software Programs that run as they've been set up to run by the people who developed them. Once the SmartContract is Deployed it cannot be changed neither its code nor its execution behavior. "Smart Contracts" Concept is Invented by Nick Szabo, who has a degree in law and computer science.

Zero Knowledge Proof: Another Important Concept which is not directly related to Blockchain but is Important in this E-Voting System using Blockchain is Zero Knowledge Proof. MIT researchers Silvio Micali, Shafi Goldwasser, and Charles Rackoff in the 1980s have Proposed Zero Knowledge Proof Encryption. In this method, one party (Prover) can prove that a specific statement is a true statement to the other party (Verifier) without disclosing any additional information.

Election as a smart contract

- **Administrator:** The Role of an Election Administrator is to Manage the Life Cycle of an Election. Trusted Government Officers and Institutions are Hired for this Role. The Election Type is Specified by the Administrators. The whole creation of the Ballots, Registration of the Votes, deciding the lifetime of the Election and Assigning the Permission ed Nodes is Completed by the Administrator.
- **Voters:** Voters who are Eligible to Vote can authenticate themselves, load ballots of Elections, cast their vote and cross-check their vote after election is over. Rewards can be given to Voters for Voting which can be in the form of tokens that can be used in an election in the near future, which could be integrated with a smart city project, thus encourage more and more people to come forward and Vote.
- **District Nodes:** Once Election is created by the Administrator, ballot smart contracts are deployed onto the Blockchain. When a vote is cast from the smart ballot, vote data is verified by District Nodes.
- **Boot Nodes:** A Boot node helps District Nodes in Discovering and Communicating with each other. Boot node is run on a Static IP ,so that the Peers are found by the District Node.

PROCESS OF ELECTION

Given Below are the Important Functions in the Election Process

Creation of an Election: In this Administrator creates the day, date and time of Election. The Candidates which are Selected Based on the Eligibility are Added in the Election by the Administrator, after this Process is done, the Information is Deployed on the Blockchain with the Information of Candidate and its District.

- Voter Registration: This thing is done by the Administrator where the Administrator should be sure that the Person he/she is Authenticating has a legal Govt ID and the Same Person should not be repeated by the Administrator.
- Transaction of Vote: The Voter has an Interaction between Ballot Smart Contract with the same voting district as defined for individual voter. There is an Interaction between the Blockchain and District Node. A Vote is a Transaction on the Blockchain. Each Vote or Transaction is Accumulated in the Blockchain. All the Information is Gathered in Blockchain which Person Voted which Party, at what Time and from which Location. To keep the Rule that One Person can Vote One at a Time, the weight of their Account is decreased by 1, therefore, enabling a single Person to Vote once, thereby, protecting the Election Rules.

Tallying Results: The Tallying of the Election is done according to the Location, for e.g Smart Contracts in the Location A will calculate Result of that area/location named A, Smart Contracts in location B will calculate the Results of their

	GO-ETHEREUM	EXONUM	QUORUM	GETH
DECENTRALIZED	OPTIONAL	YES	PARTIALLY	YES
PROGRAMMING LANGUAGE	Go,C, Java Script	RUST	Go,C, Java Script	Go
PRIVATE SUPPORT	YES	YES	YES	YES
TRANSACTION PER SECOND	DEPENDS	UP TO 5000 TRANSACTION PER SECOND	DOZENS TO HUNDREDS	HUNDREDS TO THOUSANDS
SMART CONTRACT LANGUAGE	SOLIDITY	RUST	SOLIDITY	SOLIDITY

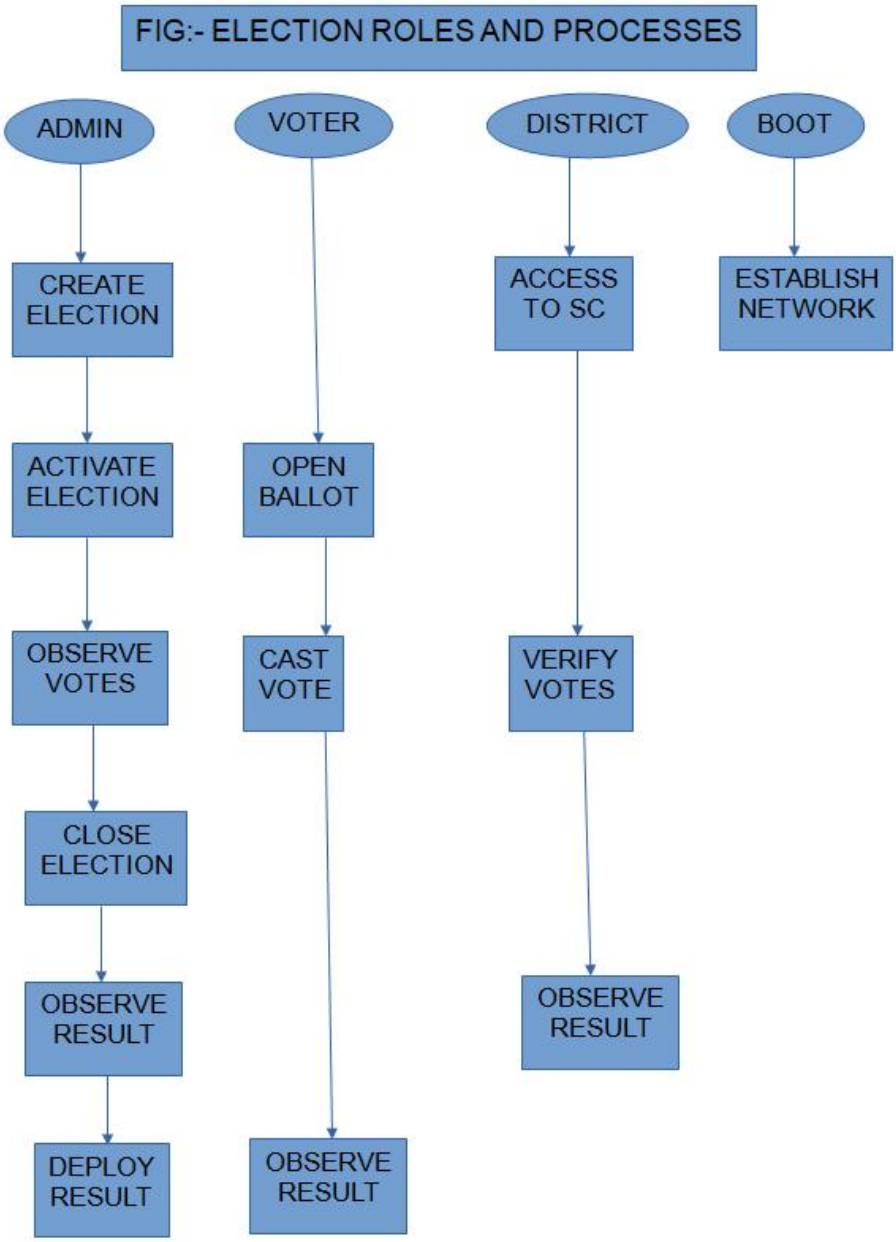

Table 1. Public transaction example

Tx HASH	BLOCK	AGE	FROM	TO	VALUE	(Tx FEE)
Oxdead...	2525	16 sec ago	Oxbeef...	Token	10 Ether	0.09
Oxface...	2526	16 sec ago	Ox4545	Ox2345	1 Ether	0.08

Table 2. Admin system transaction example

Tx HASH	BLOCK	TO	VALUE
Oxdeadbeef...	2525	N1SC	D
OxGI345edf...	2526	N2SC	P

Area and so on. The Deciding Result for different Smart Contracts is Published.

Vote Verification's: If a Person is not Satisfied or has a Doubt that whether his/her vote was counted or not then he/she can Generate a Receipt in which his/her Voting ID is Mentioned and can take that ID and Pin to a Government Official and can Verify whether it was counted on the Blockchain or not.

BLOCKCHAIN FRAMEWORKS

We will need Blockchain Frameworks for Execution of E-Voting System using Blockchain. The blockchain Frameworks which we will be using are:- Ethereum, Exonum, Quorum, Geth.

Ethereum: Ethereum is the Platform which brought in existence the Concept of Smart Contracts. This was Introduced in the Year 2015. It has become the most Preferred Blockchain Frameworks for creating decentralized Applications. It is an Open Source and a Global Platform. The Main Benefit in this Framework is that it can be rum without any lag, frauds are next to Impossible because if anybody tries to hamper the Data, he/she has to Crack a Mathematical Model/Equation which is quite Time Consuming like it can take Years & Years to crack that Mathematical Equation. Third Party can Never Interfere in this Framework.

Exonum: Implementation of Exonum is done by Rust Programming Language. This is Specifically used for Private Blockchains. Byzantine Algorithm is used in Exonum. Exonum supports 5000 Transactions per Second.

To make it more User-Friendly, Exonum is going to make it Platform Independent in the Coming Future.

Quorum: It Supports about hundreds to a thousand Transactions per Second. It is Ethereum Based Blockchain with Transaction Privacy.

Geth: It is also known as Go-Ethereum. It runs without Lag. No Third Party Interference is Allowed in Geth. No Fraud or Censorship is Allowed in Geth. This is the Most Friendly Framework of the above discussed. The Private or Public Network is determined by the Transaction Rate. Any Similar Blockchain Framework can be used instead of Geth Framework.

DESIGN AND IMPLEMENTATION

To make the Voting Secure, a user chooses a PIN consisting 5 Digits for its Corresponding ID. Every Individual Person has a Unique ID. To get Authenticated by the System, the user has to Scan ID and provide his PIN to Authenticate himself.

- Each User is allocated with Voting District, so the User can Vote anywhere in the Voting District on any Computer, as the name is enrolled on the Blockchain Framework of that Particular District.
- For a User to Successfully Vote, a Person has to Provide Unique ID generated by the System and Provide a Pin set by the user while Voting.
- If the Unique ID is Provided Correctly and the Pin Matches, the Vote is Casted.
- The User has to Select the Candidate who he/she has to Vote. After the Candidate is Selected, once again the User has to Re-enter the Unique ID and Password, once re-entered, the Vote is taken into Consideration.

SECURITY ANALYSIS

An Algorithm named Byzantine Fault Tolerance Algorithm is used to Locate Failed Nodes in the System. Attacker must DDoS each and every single Node in the Network which is kept Private. A Biometric Scan should be Introduced in the Future, to Avoid Multiple Voting by a Single Person, though now there's a Software which allows only 1 Voting by an individual, but there are Some Hackers which can Hack and allow Multiple Voting from a Single Person ID, therefore, to avoid this Thing, Biometric Scan can be Introduced in the Future. Sybil Attacks can be done on such Systems, but as our E-Voting System is a Private Blockchain, Sybil Attacks are not Possible. Private Blockchains have a Plus Point as they Provide a Strong Security and keep the Hackers at Bay. Therefore, our System is away from Sybil Attack because of private Blockchain Network.

INDEX OF FUNCTIONALITIES

1)Create a Ballot:-

```
struct voter{
unit weight;
bool voted;
unit8 vote;
address delegate;
}
```

2)Right to vote on this Ballot:-

```
function giverighttovote(address toVoter) public{
if (msg.sender != chairperson || voters(toVoter).voted) return;
voters(toVoter).weight=1;
}
```

3)Delegating Vote to the Voter:-

```
function delegate(address to) public {
Voter storage sender = voters(msg.sender);
if(sender.voted) return;
while(voters(to).delegate != address(0) && voters(to).delegate
!= msg.sender)
to = voters(to).delegate;
if(to == msg.sender) return;
sender.voted = true;
sender.delegate = to;
Voter storage delegateTo = voters(to);
if (delegateTo.voted)
proposals(delegateTo.vote).votecount += sender.weight;
else
delegateTo.weight += sender.weight;
}
```

4)Single Vote to Proposal:-

```
function vote(unit8 to proposal) public {
Voter storage sender = voters(msg.sender);
if (sender.voted || toProposal >= proposals.length) return;
sender.voted = true;
```

```
sender.vote = toProposal;
proposals(toProposal).voteCount += sender.weight;
}
function winningProposal() public view returns (unit8
_winningProposal)
{
unit256 winningVoteCount = 0;
for (unit8 prop= 0; prop < proposals.length; prop++)
if(proposals(prop).voteCount > winningVoteCount)
{
     winningVoteCount = proposals(prop).voteCount;
    _winningProposal = prop;
}
}
```

LEGAL ISSUES

Remote Area Voting: No coercion Resistance is Provided by the Remote area elections. In India, the Ladies are Forced to Vote According to whom Men tell them to Vote. A Family Member can watch on their Shoulder while Somebody is Voting. Thereby, leading to Non Configured Results. Hacking is easy in Remote Places as the Technicians in the Remote Area are not that much Skilled. In Villages, some People can take some bribe, change their Dressing Styles thereby becomes a Villager and can go and Vote as being some other Person, thereby Tempering the Election Results.

Transparency: Human errors can be Encountered while Counting the Votes. Non-Guarantee in the Counting of Votes is always an Issue in Elections. A New Law should be Introduced by the Government which should ensure Clear Transparency in this Essential Part of Democracy i.e. Elections.

Privacy of the Voters: The Information about who voted who should not be Leaked at any Cost. This Causes Insecurity to the People, as Someone can Attack that Person who has not voted according to him/her. Thereby, the Government should ensure and enforce a Law which will not allow to trace a Vote, thereby Ensuring Security to the Lives of People.

RELATED WORK

There are Some Companies which sell Token to Government and other organizations for Blockchain Elections. Agora is one of them which sells tokens for elections. Each Eligible Voter is allocated with a Unique Token by Government, where Agora gives a Token to the Government.

Six Steps of Agora Voting System:

- **Configuration:-** It is used to schedule a new Election Event.
- **Casting:-** The User's encrypted Vote is Saved on the Agora Network.
- **Anonymization:-** All Votes are Accumulated and Encrypted in Agora Network.
- **Decryption:-** The Votes are Encrypted in Computer Language, so a Person cannot understand and Misuse the Data. In this Decryption, the Information is Decrypted.
- **Tallying:-** Counting of Votes is Done in this Step.
- **Auditing:-** Election Results are Posted with the Validity of the Elections.

Integration of Blockchain and the Current Voting System is Done in The United Kingdoms Voting System where voting can be done from homes using Internet or can be done at Voting Districts. Care has to be taken that no person should vote on both on the Internet as well as at the Voting District. The Care is taken like the Unique ID can only be used once at either the Internet or at the Voting District. 4)There are some Decentralized Voting networks developed on the Ethereum Blockchain. Net Vote is one of them. There are Apps developed where Admins Set Election, date, Time, Registration Rules are set on the App. The Tally App is then used to count up the Votes and Generate the Final results.

Advantages of our e-voting system using blockchain

We are using the private Blockchain which has great Advantage over the Public Blockchains. They are not that much Efficient. In Public Blockchains Limits are Set in the Smart Contracts in Network. There is huge Traffic on public Blockchains which causes errors in Voting. Hacking has higher chances in the Public Blockchain. Efficiency is quite reduced in the Public Blockchains. Throughput of Votes is Effected in the Public Blockchain. District based Voting has a great advantage in our E-Voting System using Blockchain. Voting which is done remotely present false election result as it does not provide coercion resistance. Therefore, District based voting is a great advantage in our System. Less Time is Taken as Compared to the Traditional Voting System with more Accuracy.

Conclusion

To Overcome all the Shortcomings in the Present Voting System, we came up with the Modern Technology of Blockchain i.e. E-Voting System using Blockchain. By using this modern technology, following things can be Achieved:- Cheap Voting System, Accurate Voting System, Fast Voting System. Every Citizen desires to have a Transparent and Direct Form of Democracy which is clear cut obtained from this E-Voting System using Blockchain. Faith of People on the Voting System is Increased therefore, many People Come Forward for Voting, thereby Increasing the Percentage of the People Voted. The Pen and the Paper Election is Eradicated thereby creating Accuracy in the Voting System. Everybody Prefers Time ,and Cost Efficient Systems so this E-Voting System using Blockchain is apt for Transparent Democracy. Ethereum Private Blockchain allows hundreds and hundreds of Transaction in a Second. Utilization of the Smart Contracts lower the Load on the Blockchain. For Countries with Greater Population, some additional Technology should be added in this E-Voting System using Blockchain to avoid Errors.

REFERENCES

(1) https://en.wikipedia.org/wiki/Blockchain
(2) https://en.wikipedia.org/wiki/ Smart_contract#:~ :text= A%20smart%20contract%20is%20a,a%20contract%20or% 20an%20agreement.
(3) https://www.investopedia.com/terms/b/blockchain.asp
(4) https://appinventiv.com/blog/zero-knowledge-proof-blockchain/
(5) https://medium.com/hyperlegendary/6-blockchain-frameworks-to- build-enterprise-blockchain-how-to-choose-them-

2b7d50ba275c#:~:text=THE%20BIG%20SIX%20FOR%20ENTERPRISE%20BLOCKCHAIN&text=Hyperledger%3B%20Supported%20by%20Linux%20Foundation,low%20cost%20blockchain%20implementation%20framework.
(6) https://rubygarage.org/blog/best-blockchain-frameworks
(7) https://www.geeksforgeeks.org/sybil-attack/
(8) https://en.wikipedia.org/wiki/Sybil_attack
(9) https://cointelegraph.com/news/blockchain-for-elections-advantages-cases-challenges
(10) https://ieeexplore.ieee.org/document/8457919
(11) https://dataethics.eu/blockchain-based-voting-systems/

****