

Electronic Electoral System Using Blockchain Technology

P.Sathiyamurthi¹, Abinaya S², Nivedha S³, Kirubha P⁴

¹ Assistant professor, Dept of Information Technology

^{2,3,4} Dept of Information Technology

^{1,2,3,4} Dr.Mahalingam College of Engineering and Technology,Pollachi,Coimbatore,Tamilnadu,India

Abstract- The electronic electoral system makes the election process automated and digitalized as it replaces the traditional paper ballots into online voting system. It is an efficient way for conducting an election, which has the characteristic of being real-time and providing high safety for the voting system. The electoral system reduces the cost for conducting the election, as the government should spend some amount to the election administrators for conducting the traditional paper ballot election. It also increases user participation by allowing them to vote from anywhere in the country and allowing access from any device that has an internet connection. Also, this article aims to evaluate the application of blockchain as a service to implement distributed electronic systems. An electoral system is safe as it uses blockchain to store the data it holds data in the form of nodes and it is highly secured as a node's hash value will be in the previous node. First, we design the user's credentials page which contains the unified identification number and the GPS. Where GPS is used to track the user location where the user cast their vote. we design the ballot list to select the candidates in an authentic way. The implementation results show that it is an easier way to cast their votes with high security and brings out the accurate and quick publication of results. The electronic electoral system is highly secured as user's data can't be tracked, as data is encrypted by using cryptography technique and generates different hash value for each transaction.

Keywords- E-voting,Blockchain, Distributed System, GPS.

I. INTRODUCTION

Democracy is a system that allows the people to elect a person as a leader. The main motive is to elect a person as a leader to prevent abuses of power. Elections offer a great opportunity for the people to change the current ruling system. In democracy, they have followed two types of voting procedures, one is paper ballots and another one is electronic voting machines[1]. In paper ballots the vote is casted by using a paper where the candidates list and party logo will be present, as voter can makes a seal within the space provided where the name of the candidate for whom he/she intends to

vote.By using this method paper is a substance that is flammable and under circumstances, the paper where the votes were recorded in ballot might get damaged and it becomes impossible to retain the recorded votes[2]. With the change from manual to technological systems, the election system has become more efficient and advance.It provides faster result announcement, elimination of miscounting of votes or the simplicity of the vote casting method, the voting method has improved faster and provides high security than the paper ballots system [3].The people who are physically disabled find it difficult to vote through the paper ballot or through electronic voting machine, even though if they cast their votes they require someone to cast their vote on behalf of them. In such cases, their privacy of the voter while casting vote is violated [4]. To overcome the drawbacks of the paper ballots and electronic voting machine system, we have designed an online voting method.In the electronic electoral system, people can vote their votes in online through mobile phones or laptops, etc. The purpose of the system is to make the fraud and cheating process complex during the election process.In a paper ballot system, there is a chance that voter can registered in more than one area and can cast their vote multiple times. By creating an electronic electoral system, the double casting of votes can be eliminated. During the election time the Election Commission officials cast votes themselves and at the end they change votes from the voters list.[5]. So, it is known the need for a system for the true nature of voting.In our system, during the election time, the admin will initiate the election. When the election has initiated the candidate, the list is sent to the front end of the portal. The front end can display the list of candidates. The encrypted vote with the user information is sent to the initiate vote method at the backend of the process.

This initiate vote method calls the account validation method which validates the user using the unified identification number method and makes sure that the user has not voted yet.

II. FUNDAMENTALS OF E-VOTING AND BLOCKCHAIN

A. Workflow design

- (i) An election system should not allow forging of votes at the time of election.
- (ii) An election system should not allow traceability of the users votes.
- (iii) An election system should not allow third party to access the voting process.
- (iv) An election system should not allow an organization to control over tallying votes and determining the result of an election.
- (v) An election system should allow only eligible voters to vote by checking the unified identification number and GPS to be enabled at the time of election.

BLOCKCHAIN AS A SERVICE

The blockchain is an append-only data structure, where data is stored in blocks distributed ledger that cannot be tampered or deleted. This makes ledger immutable and cannot be hacked. There are two different types of blockchains, with different levels of restrictions based on who can read and write blocks in the blockchain. In a public block chain, people have access to read and write to everyone in the world. And in a private block chain restriction has set to who can read or write and interact with the block chain. Private blockchains also called as permissioned, where access can be granted to particular nodes that may interact with the blockchain. Smart contracts are programmable contracts that will execute automatically when it satisfies some pre-defined conditions. Smart contracts are used to automate the transactions and allow different parties to contract the agreements directly, without the help of a miners. Smart contracts assure the trust between the parties, as contracts are visible to all the users of the blockchain, therefore the agreements are easily verified [6].

BLOCKCHAIN SETUP

In our work, we setup a Ethereum permissioned blockchain to achieve privacy and security requirements for the system. Ethereum uses an algorithm that has a comparatively fast transaction through a metamask based on similarity as a stake. The Ethereum for the blockchain infrastructure is used to access across the entire development cycle [7].

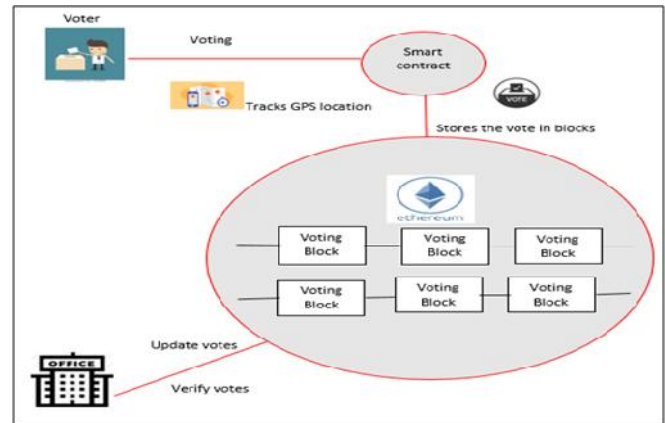


Figure 1: Election roles and process

SMART CONTRACT FOR ELECTION:

1) Roles in an election: The smart contract includes the roles of the parties which they participate in the election agreement.

- i) **Smart contract premier:** The role of the smart contract premier is to make out the life cycle of an election as like starting the election and registering the list of voters etc. They have the authority to decide the duration of the election and to assign block chain node permissioned to other parties.
- ii) **Balloter:** A citizen who is eligible to vote is called balloter. Balloters will be authenticated by the smart contract by unified identification number and can cast their vote and can view the result.

2) Proceeding of the election: The election proceeding includes a set of smart contracts deployed to the block chain that is initiated by the election administrators. The main activities involved in the election process are listed below:

Election making:

- 1) **Election premier:** The duty of the election premier is to create ballots for the election by using the smart contract technology.
- 2) **Balloter enrollment:** Once the election ballot is initiated the election administrators, should define the eligible voters list.
- 3) **Computing the election results:** The process of computing the election result is carried out by smart contract created for the election purpose. Each separate smart contract count the total votes automatically based on different locations [8].
- 4) **Votes verification:** In the process of voting transaction if a balloter has an email address, they will be registering their email address at the time of

registration. After the user votes for a candidate they will get a confirmation mail.

3)Transaction of the voting process:The voter interacts with the smart contract of the ballot for the voting transaction process. After the transaction, smart contract communicates with the block chain through the current transaction node to append the votes in blockchain. Each voter interacts with a ballot smart contract for the corresponding voting transaction. This smart contract interacts with the blockchain via the corresponding node, which appends the vote to the blockchain. As for each transaction the address will be changed, and the balance value of the ether will be reduced automatically[9]. After it is linked with the block chain using the ganache and hash value generated during the transaction. For the voting transaction sender address will be generated in a hexadecimal format which is initiated as hash value of the voter, for the contract address the same format as hexadecimal is generated. Gas price will be initiated during the transaction and base gas value will be used as a miner also it reduces the gas price in account. Mined block number will be assigned for the transaction to store the data in blockchain as block. And Tx data value will be generated for user as 0xfbe1c1c for the future reference to fetch the block details.

Table 1: Example of an account details in our system

Address	Balance	Txcount	Index
0x17511281b...	97.5759 ETH	0	1
0x14911277b...	97.3567 ETH	0	1

Table 2: Sample for a transaction details in electronic electoral system

Sender address	To contract address	Value	Gas used	Gas price	Gas limit	Mined in block	TX data
0xB53F0A51c	0x927D0D	0.00ETH	32177	20000000000	47177	617	0xfbe1c1c
0xB53E0A51c..	0x927D0D..	0.00ETH	42486	20000000000	42486	611	0x8617edb

Sketch and Execution:

1) The voters have to do the verification for performing the voting process online. The user registration is performed for security purposes. Without registration, the user cannot perform the voting process. So, the user will be logged in to the system by entering their unified

identification number and it is stored in the database. The unified identification number is mandatory for user registration. The user also wants to enter the email id for their voting confirmation. After the user has selected a candidate the user will get an email confirmation[11].

- 2) After the verification, the user will be navigated to the voting page. On that page, voters have the provision to view the list of candidates who are nominating for the election. Then the user can select a candidate to whom the user wants to vote. After submitting the vote, if the user provided an email address they will get a confirmation mail “your vote is successfully casted”. If the user doesn’t have mail id, it moves to the next page and initiating that their vote is cast successfully and there will be a link to view the result. Once the election is ended they can view the result[12].
- 3) Admin can start the election and also he can end the election. Admin gives the date for a voting process so the members have to perform the voting process within the particular date specified. It has the authority to stores the user information and performing the adding, deleting, updating the election candidate information. Only if the admin end the election users can view the election. Administrators load the election ballots to start the election.

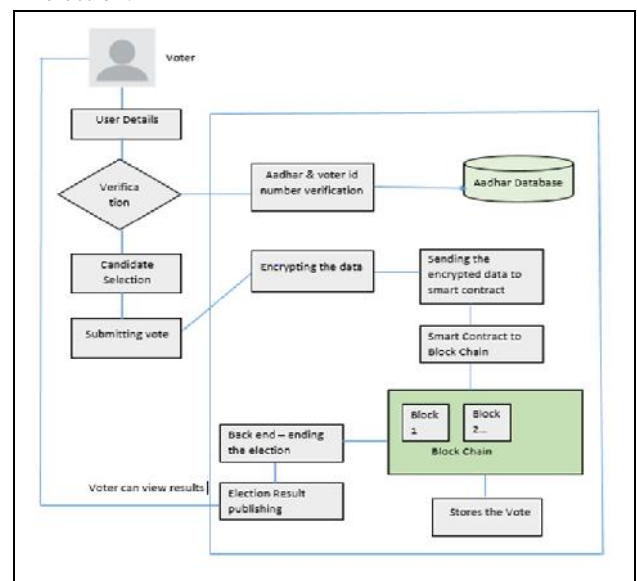


Figure 2: Design diagram of electronic electoral system

4) Our electoral voting system is secure because the user can cast their vote only by entering the unified identification number. No other information is taken as input from the user. On the other hand, the admin has the only right to start and end the election. Although there are many voting systems is available but their security level is low. For every transaction hash value will be generated as it is

difficult to trace and no one can hack any of the modules in the system.

III. RELATED WORK

Below we will be discussing the various research paper and similar fields of study, i.e electronic voting system.

Decentralized e-voting systems based on the blockchain technology[13], in this paper, they have designed a decentralized e-voting system without any miners. The idea is to combine the block chain technology with the homomorphic encryption and a secret sharing scheme. There are seven roles in the system 1) Balloters 2) Registration of voter and Authentication server 3) Web portal for election 4) Storage Database 5) Distributed data servers 6) smart contract agreement. To vote in an election the voter needs to be authenticated. For the authentication process signature verification has to be done.

To do the signature verification, server generates a RSA-based public/private key pair. To register the user in an election user code generation and verification of voter's identity has to be done. In this decentralized e-voting systems based on the blockchain technology, they concluded some security factors: voter eligibility, protecting the voter's identity for security, unrepeated votes, ballot entitlement, and ballot verifiability. As conclude it increases the voter's confidence and also reduces the resources used in election.

Blockchain based e-voting system[15], this paper portrays some of the limitations in existing system and proposes some of the block chain frameworks on electronic voting system. The paper makes some contributions for the e-voting system i) e-voting system permissioned blockchain ii) Analyzing the framework for existing block chain.Go-Ethereum permissioned proof of authority(POA) blockchain is used to achieve user's privacy and e-voting requirements security by which the user vote in a secured environment. For all the eligible voter, will receive a identity wallet during the election. A unique key is provided for all the eligible voters during all the election time. This system used in the voting transaction will not release any detailed information about the individual balloter who cast the vote for a particular candidate.

Towards the intelligent agents for blockchain e-voting system[16], this paper uses the intelligent agents and multi-agent system for Auditable Blockchain voting system which combines blockchain technology into one supervised non-remote internet voting system which is the end to end verifiable. The system is established to use blockchain technology in e-voting system that will be audited and verified

by the balloters. The three main components used in ABVS architecture are: super node, trusted node, polling stations. It reduces the burden on blockchain node by using the computing resources which is located in polling stations. By using this system it is easier to detect the attempts to break in e-voting system and also not possible to change or modify the data/information from outside. It allows the third party to read the encrypted message by without decrypting the data is considered as main disadvantages. The voter is identified by the identity information without the voter's choice.

IV. CONCLUSION

The proposed system is implemented in the ganache blockchain. Electronic electoral system is used to automate the voting process where user can cast their vote in their own location. There is no way to make forgery of votes, as forgery of votes can be done in the traditional paper ballots. It reduces the manpower for conducting the election. Counting of votes is done automatically by the smart contract in electronic electoral system. There is a feature of email confirmation to the user after they cast their vote. The administrator can track the location of the user where they have casted their vote. While using this technology system is more reliable. This also makes the whole process faster cheaper also efficient compared to the existing system. It is tested that smart contract and front end web application satisfies all the requirement needed for processing the election task. The web page is validated by checking the user inputs. This system is user-friendly, so everyone can use it easily. For this, we used a smart contract to secure user's data. So, there is no chance to hack the user's data and cast the votes multiple times. In the future, we add the camera accessibility for this system. By using electronic electoral system, we conduct the election fast and in easier way. This can reduce travel and other administrative costs. And also the result will be out after few hours. We have tested the application using Ethereum Tester and it passes all the unit tests.

REFERENCES

- [1] Gautam Srivastava, Ashutosh Dhar Dwivedi, Rajani Singh," Phantom protocol as the new crypto Democracy", Springer,2018
- [2] Sarah P.Everett, Kristen K.Greene, Michael D.Byrne, Dan S.Wallach, Kyle Derr, Daniel Sandler, Ted Torous", Electronic voting machines versus traditional methods: Improved preference, Similar performance", CHL,2008
- [3] P.Noizant,"Blockchain Electronic vote",Elsevier,2015
- [4] D. AshokKumar; T. UmmalSariba Begum, "Electronic voting machine", IEEE 2012

- [5] Haibo Yi," Securing e-voting based on blockchain in P2P network", Springer,2019
- [6] Fridrikp. Hjalmarsson, Gunnaugur K. Hreidarsson, Mohammad Hamdaqa, GisliHjalmtysson, "Blockchain-Based E-Voting System",IEEE,2018
- [7] Jonathan Alexander, Steven Landers and Ben Howerton, "Netvote: A Decentralized Voting Network ", Netvote-White-Paper-v7,2018.
- [8] "What Are Smart Contracts? A Beginner's Guide to Smart Contracts", Blockgeeks, 2016.
- [9] Andrew Barnes, Christopher Brake and Thomas Perry, "Digital Voting with the use of Blockchain Technology", Plymouth,2016
- [10]Michal Pawlak, Aneta Poniszewska - Maranda, Natalia Kryvinska, "Towards the intelligent agents for blockchain e-voting system",Elsevier,2018.
- [11]C. Burton, C. Culnane, S. Schneider, Vote: verifiable electronic voting in practice[J]. IEEE Secure. &Priv, 2016
- [12]Pierre Noizat," Block chain Electronic Vote",Elsevier,2015.
- [13]Jen-Ho Hsiao, Raylin Tso, Chien-Ming Chen,Mu-En Wu, "Decentralized E-Voting Systems Based on the Blockchain Technology,Springer,2018
- [14]Yiningliu,Quanyu Zhao, "E-voting scheme using secret sharing and K-anonymity",Springer,2018
- [15]Michal Pawlak, AnetaPoniszewska-Maranda, Natalia Kryvinska, "Towards the intelligent agents for blockchain e-voting system",Elsevier,2018
- [16]Andresen,G.2012,BIP-0016 (Bitcoin Improvement Proposal), 2012
- [17]Springall, D. Finkenaur,. Durumeric, Z.Kitcat,J.Hursti, H.MacAlpine, M.Halderman, "Security analysis of the Estonian internet voting system", jhalderm,2016
- [18]Merkle,R.C., 1980.Protocols for public key cryptosystems,IEEE Computer Society
- [19]P. Fairley, Blockchain world - Feeding the blockchain beast if bitcoin ever does go mainstream, the electricity needed to sustain it will be enormous[J]. IEEE Spectr,2017
- [20]Ajit Kulkarni, "How To Choose Between PublicAnd Permissioned Blockchain For Your Project", Chronicled, 2018.
- [21]E.Peck,K.Moore,The blossoming of the blockchain[J]. IEEE Spectr,2017
- [22]Jelurida,"JeluridaWhitepaper,2017
- [23]A. Dorri, M. Steger, S. Kanhere, et al., Blockchain: a distributed solution to automotive security and privacy[J].IEEECommun. Mag,2017