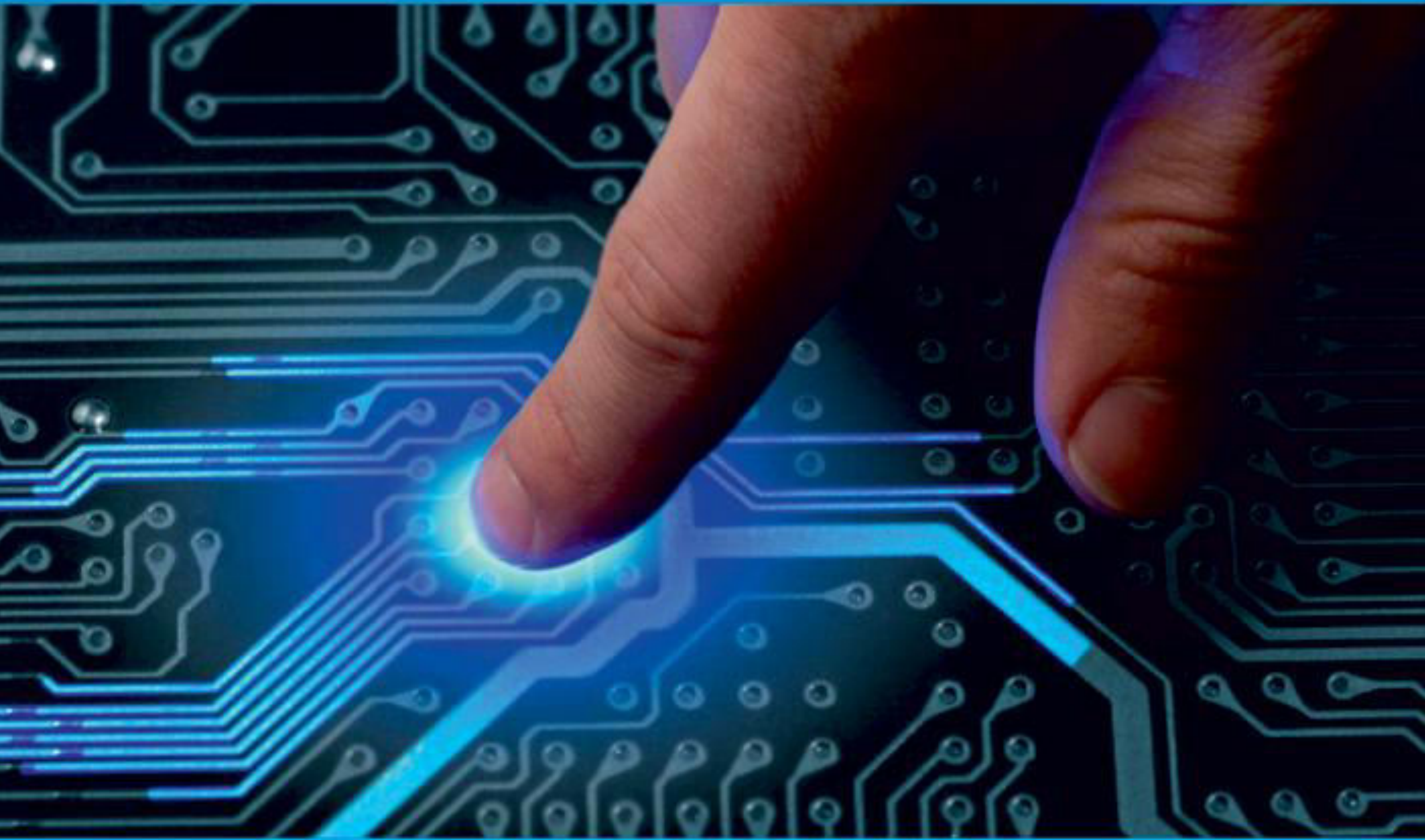
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 6, June 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906202 |

A Secured system for E-voting using Blockchain Technology

Manjusha Sanke[1], Siddhi Malik[2], Akshada Navelkar[3] , Varshjit Gawas[4], Harsh Raikar[5]

Assistant Professor, Dept. of Information Technology, S.R.I.E.I.T., Shiroda-Goa, India[1]

UG Student, Dept. of Information Technology, S.R.I.E.I.T., Shiroda-Goa, India[2,3,4,5]

ABSTRACT: It has been a challenge for a long time to build an electronic voting system that satisfies legal requirements of legislators. Distributed ledger technologies are an exciting technological advancement in the information technology world. Blockchain technologies offer an infinite range of applications. This paper aims to evaluate the application of blockchain as service to implement distributed electronic voting systems. It highlights the requirements of building electronic voting systems and identifies the legal and technological limitations of using blockchain as a service for realizing such systems. The paper starts by evaluating some of the popular blockchain frameworks that offer blockchain as a service. We then propose a electronic voting system based on blockchain that addresses all limitations we discovered. More generally this paper evaluates the potential of distributed ledger technologies through the description of a case study, namely the process of an election and implementing a blockchain-based application which improves the security and decreases the cost of hosting a nationwide election.

KEYWORDS: Blockchain, E-voting, Security, Transaction, Hash, Crypto-voting, Ethereum.

I. INTRODUCTION

There is a lot of mistrust towards the government which has made the democratic process of voting more critical than ever. In such situations, there is need for a fair and transparent voting system so that people can cast their votes freely. By making use of block chain, a secure and robust system for digital voting can be devised.

Electronic voting machine is used in many countries for counting votes which is improvement over the earlier traditional paper ballot. Although e-voting machines are cost efficient and vote counting is fast and easy still this system is not very highly secure. The present process of elections takes lot of voters' time to cast a vote. The machine takes a lot of time to detect or sense the touch which leads to pressing of the button on the machine twice or more. Traditional voting system uses centralized system, and there is one organization that manages it. It is possible to alter the database but by adopting blockchain technology which is a decentralized system we can prevent tampering and manipulation.

Blockchain is a shared, distributed ledger that facilitates the process of recording transactions and tracking assets in a business network. Blockchain stores transaction data — in blocks that are linked together to form a chain. As the number of transactions grows, so does the blockchain. Each block contains a hash (a digital fingerprint or unique identifier), time stamped batches of recent valid transactions, and the hash of the previous block. The previous block hash links the blocks together and prevents any block from being altered or a block being inserted between two existing blocks. In this way, each subsequent block strengthens the verification of the previous block and hence the entire blockchain [1].

The main aim is to present a digital voting system which is highly secure, reliable and transparent. In fact, this system will allow the voters to verify their vote. The voter does not have to go anywhere to cast his vote or stand in a long queue which leads to wastage in his time. The voter can register from anywhere provided he should have internet connection to the device which he/she is using to register. Once the registration date is over, the voter even if he/she tries to access the website page it would show error indicating he cannot register. The voter's aadhar number is taken as the unique id and security is provided during voting process using blockchain technology. Once elections are done the login page won't be accessible. The result page will display the final result of the election who he been elected in which constituency alone with his party name, his name and party symbol and his picture along with total number of votes.

II. LITERATURE SURVEY

Electronic voting offers convenience to the voters and the authority over the conventional paper-ballot process. Security is a major challenge in electronic voting. Research has been done in the domain of e-voting.Usually the remote voting operation can be done via mobile devices or personal computers. Through Crypto-voting system, it will be possible to guarantee the continuity with the traditional voting operation and the accessibility also to IT-illiterate. People can vote in a traditional way reaching an e-voting polling station. The voting operation consists in marking a symbol in a “virtual” ballot paper showed on a flat touch screen.

The following key processes are involved:-

i. Requesting to vote: The user will have to log in to the voting system using his credentials- in this case, the e-voting system will use his Identification Number, his address, and the voting confirmation number provided to registered voters by the local authorities. The system will check all information entered and, if matched with a valid voter, the user will be authorized to cast a vote. Our e-Voting system will not allow participants to generate their own identities and register to vote. Systems that allow identities to be arbitrarily generated are usually vulnerable to the Sybil attack where attackers claim a large number of fake identities and stuff the ballot box with illegitimate votes.

ii. Casting a vote: Voters will have to choose to either vote for one of the candidates or cast a protest vote. Casting the vote will be done through a friendly user interface. For each voter a token is generated known as Ethereum, with initial Boolean value one, once a vote is casted it becomes 0. A voter can cast a vote if and only if Ethereum value is 1.In this way revoting problem is resolved.

iii. Encrypting votes: After the user casts his vote, the system will generate an input that contains the voter identification number followed by the complete name of the voter as well as the hash of the previous vote. This way each input will be unique and ensure that the encrypted output will be unique as well. The encrypted information will be recorded in the block header of each vote cast. The information related to each vote will be encrypted using SHA one-way hash function that has no known reverse to it. The only theoretically possible way to reverse the hash would be to guess the seed data and the encryption method and then hash it to see if the results match. This way of hashing votes makes it nearly impossible to reverse engineer, therefore there would be no way voters' information could be retrieved.

iv. Adding the vote to the Blockchain: After a block is created, and depending on the candidate selected, the information is recorded in the corresponding blockchain. Each block gets linked to the previously cast vote.

Table -1: Survey of various approaches

Reference paper	Approach	Technology
[2]	preparatory activities and formation of electoral lists, management of voting, ount of votes	Sidechain
[3]	Registration, voting mechanism & architecture, voting process	MySql
[4]	register/login, caste vote	MySQL
[8]	Register/login, requesting to vote, casting a vote encrypting votes adding vote to blockchain	Bitcoin
[9]	Casting verification tabulation	Vote forwarding server, vote storage server, Log server, vote counting server
[11]	consensus algorithm (PoW) voter access the voting system voter goes through identity verification process voter determines vote through the UI	Python(API server), Javascript, ES7, Solidity(smart contracts), MetaMask, Ganache

III. WORKING OF THE SYSTEM

E-voting system using block-chain works as a step towards creating secure and transparent environment for elections where the users will be able to cast their votes only once and will be able to view the total votes casted in real time without having the permission to edit the same after elections get over. The working of block-chain will ensure the votes are maintained and the systems are not rigged by any third party.

3.1. Existing System

Here are the issues with the current system:

- The electronic voting machine is open to any malicious program, if it gets affected.
- In election process, even one vote is valuable. The system can get affected by a virus that can destroy the data storage.
- Fake displays can be shown which depicts manipulated number, but fake votes are generated from the backend.
- Voters can not verify their vote, so it is easy for hackers to change large number of votes.
- The voter has to go on a specific place in-order to cast vote.
- The voter has to wait in a long queue which waste lot of time.
- The results of the elections get a month to be announced which is time-consuming.

3.2 Proposed System

The system is designed using a web based interface to facilitate user engagement. The system allows all the voters to participate in voting and develop a fair and healthy competition among all the candidates. Our system allows the admin to create elections, verify voters and add candidates.
In the proposed system, benefits of using block chain are:-

- Block chain is decentralized information sharing platform.
- Each block in the blockchain has a hash value that depends on data in the block. If someone tries to change the data, then the hash value will also change and system will inform that someone is trying to change the data. The blockchain based system will be secure, reliable and anonymous and will help increase the number of voters as well as build trust of people in their government.

Our various requirements are:
Authentication: Only people already registered to vote can cast a vote. Registration usually requires verification of certain information and documents, which is to be done online in a secure manner. Therefore, the system should be able to verify voters' identities and grant them permission to vote.
Accuracy: Votes must be accurate; every vote should be counted, and can't be changed, duplicated or removed.
Verifiability: The system should be verifiable to make sure all votes are counted correctly.

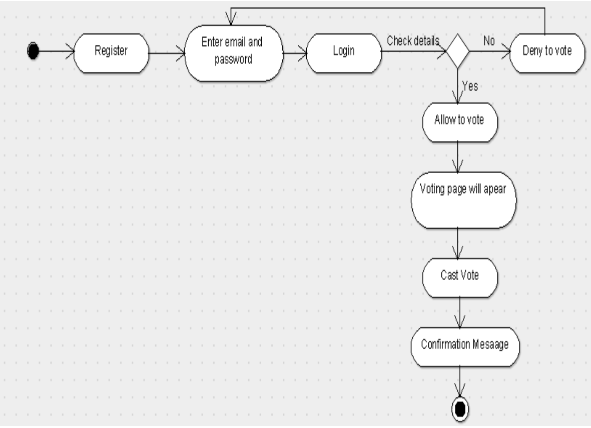


Fig -1: Activity diagram of System

3.2.1 Registration

The process of registering will be done by user interacting with the Authentication Server (AS) via a website. The AS contains information about voters in a database. The user enters his/her Personally Identifiable Information (PII) and scans supporting documentation to upload into system along with an email address. The user picture is also taken for verification. If the information is verified and correct, the user is allowed to create account. The user enters a email id and a password to log in. Also an entry is made next to the user database entry storing whether he/she has registered to vote. If the user information cannot be verified, he/she is not allowed to create an account.

3.2.2 Authentication:

The authentication is a process of verifying the users in order to allow them to login into the system. It will authenticate users using the email id and password provided by them during registration process. It verifies the details entered by user during registration process i.e. first name, middle name, last name ,DOB ,address ,constituency ,password ,mobile number, aadhaar, if the details match with aadhaar database then the user details are stored in the new database. The admin will then check the database and verify the user's identity and documents

3.2.3 Voting

The process of voting is a multi step process. It involves verifying your identity with the AS and then voting. On the day of voting each candidate is given an account on the block-chain system so they can get votes. During voting day, the user logs in to the authentication server using the email id and password created in the previous step. An image of the user is taken to ensure that the user is the owner of the account. This image is compared with the image taken during registration. Once the user logs in, their system would create a public key which they would send to the AS. The AS would add associate the key with the email id. The key would be sent to create an account for the user on the blockchain system to vote. A specific amount of ether (currency the user can use to vote) is added to users' account which enables them to vote. The AS would then send a session token back to the user. The user would be redirected to the AR(Arbitration Server). The user would provide the AR with the session token would verify it with AS. The AR would send a verification message to the user along with the public key of the block-chain node to which his/her vote would be sent. The user would encrypt their vote with the public key and send it to AR. This will ensure that the AR cannot read the users vote and hence the vote would remain a secret. The AR would send the encrypted vote to the appropriate node. The node would decrypt the message with their private key and send a specific amount of ether from users account to the candidates block-chain account. Each node would verify the transaction according to the smart contract. These contracts would verify a particular transaction was a duplicate one or no and check its validity. After this process the node would pass this transaction to other nodes in block-chain system.

3.2.4 Verification

The process of verifying the vote depends on the type of election it is. Some elections allow for interim results and some do not. In either case the voter must get a confirmation that his/her transaction has been approved by block-chain system. In case of the election that allows interim results, one of the nodes of the block-chain could be made publicly accessible. It would have a website where a user could enter their public key to verify whether their vote was counted. This node would not have the ability to add any transaction to the system. This will be implemented through smart contracts. If the organizers of an election want to keep the interim results a secret, he/she could only get a binary verification via the AR. Since the AR is a thin client it would act as an intermediary to verify the transaction. At the end if the election in above case, the user will be able to check the result for the election.

3.2.5 Counting

The process of counting votes of a candidate can be very simple. Each voter has a fixed amount of ether or currency value that they use to vote for a candidate of their choice. The candidate with the highest amount of ether in their account wins the election.

IV. Implementation

Ganache is a blockchain which provides us with personal ethereum blockchain used to run tests, execute commands, and inspect state while controlling how the chain operates.

It basically provides us ten accounts with 100 ethers (fake) each. Each account has an address and a private key which is unique to it.

A page displays a list of candidates who are standing for elections. The user can select the candidate of their choice from the given list and cast a vote.

In order to vote the voter will have to first import an account from the blockchain using its private key. After importing the account it will get connected to the site. After this the user can select a candidate of its choice to cast the vote.

After the user has clicked the vote button a transaction receipt will appear on the screen asking for confirmation of transaction. The user can then click on confirm button in order to cast his/her vote.

Finally a page will display the result showing the count of votes for each candidate.

V. Conclusion

The current ballot system has a large number of issues leading to political unrest in the country. E-voting has replaced paper voting and increased efficiency and reduced errors but there are security issues such as tampering of votes, the machine can get affected by a virus and destroy data stored in the system and fake display can show manipulated votes and the tallying process is slow. Our system handles voter privacy and provides a transparent system for verification of election. This system solves all the issues faced in voting process since it is reliable, tamper proof, efficient, easy to use and provides security by making use of blockchain technology.

References

1. Ravindhar Vadapalli,'Fundamentals of Blockchain', October 2020, ISBN: 301.345.908
2. Francesco Fusco, Maria Ilaria Lunesu , Filippo Eros Pani and Andrea Pinna, 'Crypto-voting, a Blockchain based e-Voting System', International Conference on Knowledge Management and Information Sharing, 2018.
3. Andrew Barnes, Christopher Brake and Thomas Perry, 'Digital Voting with the use of Blockchain Technology', Available at: https://www.economist.com/sites/default/files/plymouth.pdf
4. Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson , Blockchain-Based E-Voting System, Available at: https://skemman.is/bitstream/1946/31161/1/Research-Paper-BBEVS.pdf
5. Kashif Mehboob Khan, Junaid Arshad, Mohammad Mubashir Khan. , Secure Digital voting system based on blockchain technology, International Journal of Electronic Government Research, 2018.
6. Chris Dhalberg, Harvey Mudd College, Challenges in Designing an Electronic Voting System, Semantic Scholar 2006.
7. Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis ISG-SCC, Royal Holloway, University Of London, Egham, United Kingdom, E-Voting With Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy, Available at: researchgate.net.
8. Mrs. Harsha V. Patil, Mrs. Kanchan G. Rathi, Mrs. Malati V.Tribhuwan , A Study on Decentralized E-Voting System Using Blockchain Technology, International Research Journal of Engineering and Technology, 2018.
9. Drew Springall, Travis Finkenaue, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, J. Alex Halderman, Security analysis of the estonian internet voting system, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 2014.
10. Prof. Pallavi Shejwal , Aditya Gaikwad , Mayur Jadhav, Nikhil Nanaware , Noormohammed Shikalgar, E-voting using block chain Technology, IJSDR, May 2019.
11. Ong Kang Yi, Debashish Das, Block Chain Technology For Electronic Voting, Journal of Critical Reviews, Vol 7, Issue 3, 2020.
12. Sagar Shah, Qaish Kanchwala, Huaiqian Mi from Northeastern University, Block Chain Voting System Available at: https://www.economist.com/sites/default/files/northeastern.pdf.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

📱 9940 572 462 ✆ 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details