Research Article:

E-Voting based upon Blockchain System

Prateek Sharma
Computer Science Department, Chandigarh University
Punjab, India
itsprateek078@gmail.com

Abha Gupta
Computer Science Department, Chandigarh University
Punjab, India
abha.e16490@cumail.in

Anant Dev Pandey
Computer Science Department, Chandigarh University
Punjab, India
pandeyanant8055@gmail.com

Aman Singh Negi
Computer Science Department, Chandigarh University
Punjab, India
amann4204@gmail.com

Kunwar Vabhav Mishra
Computer Science Department, Chandigarh University
Punjab, India
vabhavmishra62@gmail.com

Rohit Garg
Computer Science Department, Chandigarh University
Punjab, India
gargrohit351@gmail.com

Abstract*—Heading to this journey of modernization, where everyone is choosing online systems in each and every sector especially after the hit of COVID-19 in past few years. Then why should we limit our journey to this offline era of voting and choosing representatives for the elections? We all are known to this fact that even after choosing electronic voting too, centralized system is being used by this online voting system which is again not at all trustworthy as they are having full access to the web services or web applications upon which they are performing voting and hence could lead to many problems before us such as vote theft, vote losses and even much more. DDOS (Distributed Denial of Service) attacks could be performed on these websites and can flood their services with thousands of requests which could crash their whole server and much more threats are even possible. But, with use of this Blockchain technology using our connected components, the consumption of energy will surely be minimized and resource utilization will be maximized along with increased security and reliability too as we will be giving extreme security to our Ballot which will be providing security functions to our votes. Hence with our designed project, we will be seeing that how these fixtures will be working and securing the ballot with full reliability and will be giving us secure vote counts.

Keywords – Blockchain, Decentralized, Smart contract, Truffle, Ganache, Meta Mask.

I. Introduction

Electronic Voting System using Block chaining can be used in many contexts even in every level of voting whether at small scale for smaller elections and at larger level for large scale elections too. In a country like India, where population is raising to billions, we cannot risk our voting system with trust issues and reliability issues. Hence, Blockchain system comes in the first priority whenever this state of trust is used as each and every block of Blockchain will be containing the hash codes of our data count. Whenever someone intentionally or forcefully be trying to intend and change the hash code, then it will bring change in connected blocks too and the culprit could easily be founded. For example, an exam is being conducted in a university in different classes and students sitting in a class are kind of connected blocks of blockchain. In this exam let us say, if a student is cheating from his friend and the next student is again cheating from that student. In this case, at the time of verification, whole class could be easily caught as the answer sheets of those students will be highlighted different from others as the same content is copied by his friend from his friend's answer sheet. Exactly same, each node in blockchain will be containing data, address of previous node, a nonce value will be generated which will be generating the number as output of the hashed function in a Blockchain. Instead, we can state that in this Blockchain network there is no one or not any kind of trustworthy link or medium but the transactions will be approved by all the blocks and hence each and every block is a trusted authority in this system of Blockchain. This Blockchain based voting will obviously be attracting the youth to follow up and choose the upbringing leader. By keeping and addressing the issues of reliability, scalability and security, this model has been designed. We have designed our system by seeing the limitations of previous models where it was seen that false counts were being found in some models. As we are assuming that this voting system be working upon large scale, hence we inclusion of electoral commission is must as they will be providing the information of voters to include upon and authentication and authorization of their identity as well. The number of Parties along with the standing electoral name also should be included by the electoral commission only. With the use of Application Programming Interface, we will be displaying the progress to voter's end and the count will be kept at our blockchain platform of Ethereum until the election commission will be taking the count of the number of votes taken out in the progress.

II. Surveys

We have looked upon different surveys, some based upon literature and on the real grounds too.

(A) Literature Based Surveys :

- *A Survey of Blockchain Security and Solutions (2017):* Maintained by Alharby M. & Moorsel A.V. This Paper mainly focussed upon the security challenges which can affect Blockchain systems such as leakage of votes, vote theft and privacy loss. We have focussed upon the challenges and overcome them.

- *Towards secure and transparent electronic voting using Blockchain Technology(2018):* Maintained by Weber I.E. This Paper mainly focussed upon the authentication issues of the voter and their education, privacy of the

voter, auditing of smart contracts. We have worked upon the authentication system very well and have overcome the issues as well too.

- *Post Quantum Blockchain: Secure Blockchain Voting (2019):* Maintained by Bensberg. This Paper mainly focussed upon the adoption and intaking of Quantum Cryptography and adding digital signatures too including SHA Algorithm so that the voter can include the signature using its private key and then recipient can verify it using the sender's public key and then validating the identity. We have included the post outcomes of these surveys so that security and reliability could be maintained.

(B) On Ground Based Surveys :

- *On Ground Survey of 2020:* According to the survey of 2020 the percentage of eligible voters who casted their vote are listed as follows:

TABLE I. 2020 GROUND SURVEY

- *On Ground Survey of 2021:* According to the survey of 2022 the percentage of eligible voters who casted their vote are listed as follows:

State	***Assam***	***Bihar***	***Kerala***	***Tamil Nadu***
Voters (in million)	*23.3*	*72.8*	*27.1*	*62.6*

TABLE II. 2021 GROUND SURVEY

- *On Ground Survey of 2022:* According to the survey of 2022 the percentage of eligible voters who casted their vote are listed as follows:

TABLE III. 2022 GROUND SURVEY

State	***Assam***	***Bihar***	***Kerala***	***Tamil Nadu***
Voters (in million)	*26.8*	*75.9*	*31.1*	*69.8*

State	***Assam***	***Bihar***	***Kerala***	***Tamil Nadu***
Voters (in million)	*29.8*	*78.9*	*33.7*	*71.5*

III. Problem Definition

Whenever we utter this word of voting whether of any type it could be traditional voting, Voting using Electronic Voting machine, or an online voting system, there are few scenarios and some tick marks which should be ticked marked before starting the process :

• Age-Limit: The voters having age above 18 and 21 will only be considered as legit.

• Single Countability: Voter will be allowed to vote only once at a time.

• Security & Confidentiality: The choice made by the approved voter will be considered as confidential and no other middleman will be getting this information about anyone's choice.

• Upgradability: System should contain all the upgrades available in the future so that no discrepancies could remain.

A. Age-Limit

Whenever the verdict of age limit is called then identification of limit of age in this sector is a complex thing in itself. Various identification, authentication and authorization techniques should be used so that no illegal voter could participate. Election Commission need to make use of identity card as authorising card and should use voter's Aadhaar card number as digital signature for an individual voter. As Aadhaar card number is said to be unique number given to every unique person who are legal residents of India but issue which persists here is of age-limit as even below age limit persons are also containing Aadhaar card, hence some verification mechanisms should be used so that proper Age-Limit should be given.

B. Countability

The most important accept upon which voting system is mainly used is to maintain verification and single count of votes so that one person cannot vote more than once at a time. For this matter, we have designed a sign up page and verification thereafter deploying votes upon blockchain after approving transaction by every block and thereby producing a QR receipt based upon the identity and single count of voter after which voter won't be able to vote again. Hence, countability will be taken in accordance in each manner so that confidentiality at its peak could be maintained and efficient system is to be made. When the votes are distinguished for each encryption, it is easy to segregate thereby.

C. Security & Confidentiality

Security and Confidentiality are other two main concerns which should be kept in mind in a secure system. It should be kept in mind that no one should get the information about the voter's choice. Only this will lead to a confidential and secure system because if anyone be knowing about one's decision of his/her confined voter then it will basically be resulting in unfairness and biasing as well. Hence security and confidentiality should be kept in mind. For securing this confidential system, we

have referred to our cryptographic algorithms which will be taking care of all the measures required for confidentiality.

D. Upgradability

For any further changes in the models in the upcoming time if any update persists let us say any sort of discrepancy or it could be an update regarding the REST API too then it should allow this feature of auto-upgradability and removing redundancies as well. As various consensus mechanisms have to be approved for validating the transaction so gas limitations should not be existing in the future times as well so that the continuous flow could be maintained in a proper manner. Any upgradable changes should not be kept unchanged and proper upgradation system should exist. Proper abstraction should be embedded in the system because hiding details from the outer world is another measure upon which work should be done in a consistent manner in order to remove risks of security and removing vulnerabilities. Hence, proper upgradability should exist in our system.

IV. Blockchain Background

Blockchain is a ledger that operates in a decentralized and distributed manner and consists of chain of blocks which store tamper proof data. It serves as the backbone for digital currency like Bitcoin and Ethereum. The addition of a new block to the chain is a crucial process. The following steps describe how a block is added to the chain during any transaction.

1) *Users initiate transactions using their Digital Signatures:* To initiate a transaction on a blockchain, users start by digitally signing it with their private keys. This digital signature acts as cryptographic evidence to verify the transaction's authenticity. It verifies that the individual initiating the transaction indeed possesses the private key connected to the sending address. Implementing this step ensures the transaction's security and integrity.

2) *Users broadcast their transactions to Nodes:* Once users have created a signed transaction, they proceed to broadcast it to the network. This broadcasting process usually takes place via a peer-to-peer network where interconnected nodes, which are essentially computers or servers participating in the blockchain network, are involved. By broadcasting the transaction, it becomes visible and accessible to the nodes within the network.

3) *One or more Nodes begin validating each transaction:* After receiving the transaction, one or multiple nodes in the network assume the task of validating it. Validation involves verifying that the sender has enough funds to complete the transaction and that the transaction complies with the rules and protocols of the blockchain. This procedure guarantees that any deceitful or invalid transactions are not incorporated into the blockchain.

4) *Nodes aggregate validated transactions into Blocks:* After validating a group of transactions, nodes bundle them together into a block, which acts as a container for a set of verified transactions.

5) *Nodes Broadcast Blocks to each other:* The nodes within the network share the newly formed block with each other to ensure that all nodes have an identical ledger of transactions.

6) *Consensus Protocol is used:* For validating transactions on a sequence of blocks we have efficiently made use of different consensus protocols such as Proof of Work having its applications in Bitcoin and Proof of Stake, having its applications in Ethereum. These consensus algorithms aid in achieving agreement among nodes.

7) *Block reflecting the "true state" is chained to prior Block.:* Once consensus is achieved, the new block is appended to the existing blockchain. It includes a reference to the previous block, creating a chain. This chaining of blocks ensures the preservation of the complete transaction history and enables all nodes to maintain and agree upon the "true state" of the blockchain.

V. Proposed System

We've endeavoured to develop a voting system that incorporates blockchain technology. This system doesn't aim to replace the existing voting methods; instead, it offers a novel approach to conducting elections that prioritizes enhanced security, transparency, and tamper resistance.

A. System Architecture

Figure 1 represents system architectures of our voting system.

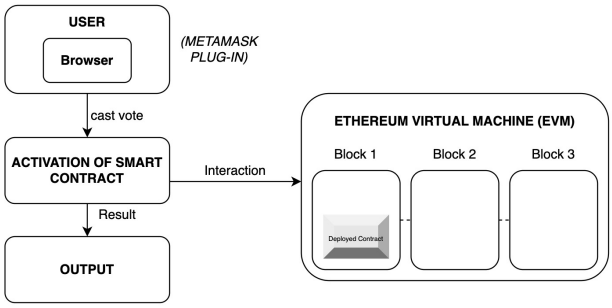


Fig. 1. System Architecture Overview of the system architecture:

1) *Registration:* The registration process allows eligible voters to enrol in the system. Users provide their personal details and, if required, verification documents to establish their eligibility. This information is collected securely and stored in the system's database.

2) *Authentication:* Once registered, users can log in to the website using their credentials. This step ensures that only authorized voters who have completed the registration process can access the platform. Additional security measures such as multi-factor authentication may be implemented to protect the login process.

3) *Smart Contract Activation:* In the system, blockchain technology is used through smart contracts. These contracts are self-executing agreements that contain the rules of the election in their encoded form. Activating the smart contracts involves initializing them to establish the election's rules, dates, and terms. This ensures that the election is conducted fairly and transparently based on predefined rules.

4) *Data Storage:* MySQL is used to store details of users like name, unique id, gender, and phone number.
5) *Result:* After the voting period concludes, the system processes the votes recorded in the blockchain. The result is calculated and verified through the smart contract, ensuring the accuracy of the outcome.

B. *Requirement Analysis*

The front-end of the system is built with HTML or Bootstrap and the back end utilizes a blockchain. The core logic of the voting system is implemented in Solidity, a programming language specifically designed for smart contracts. The smart contract defines the candidate names and symbols. Smart contract is a self-executing program that triggers when a predefined condition meets. Truffle is used to compile contracts written in solidity.

In the blockchain context, any modification or update is referred to as a "transaction." Transactions are the way in which the external world interacts with the Ethereum network. To perform a transaction and change the state stored on the Ethereum network, a transaction fee or service charge is required. Within the Ethereum network, the native cryptocurrency, ether, is primarily used as the transaction fee, also called "gas."

For this project, Ganache-CLI is used to quickly establish a private network. This setup enables almost instant mining of transactions on the network.

MetaMask is a browser extension that act as a bridge between for user to interact with DApps.

TABLE IV. SOFTWARE REQUIREMENTS

Operating System	Window 7
Compiler	Truffle
Language	Solidity, HTML, Java Script and CSS
Software	Ganache
Plugin	Metamask

C. *Contract Creation*

The initial step to develop our application is to install all required dependencies like truffle and so on, then we have to create our contract. To create the smart contract, begin by using the "contract" keyword, followed by specifying the contract name.
Now, it's essential to establish a data structure comprising four key variables. These include:

1) "id" to store the unique identifier of each candidate,
2) "name" for holding the candidate's name,
3) "party" for storing the political party to which the candidate belongs, and
4) "voteCount" to maintain a tally of the number of votes each candidate receives.

Figure 2 shows the code block of the required structure.

```
contract Election {
    struct Candidate {
        uint id;
        string name;
        string party;
        uint voteCount;
    }
}
```

Fig. 2. Code block of the structure

After Creating the structure, it is necessary to craft a constructor responsible for initializing the contract. This constructor accomplishes this task by introducing a predefined set of candidates into the election. You can find the code block for this constructor in Figure 3.

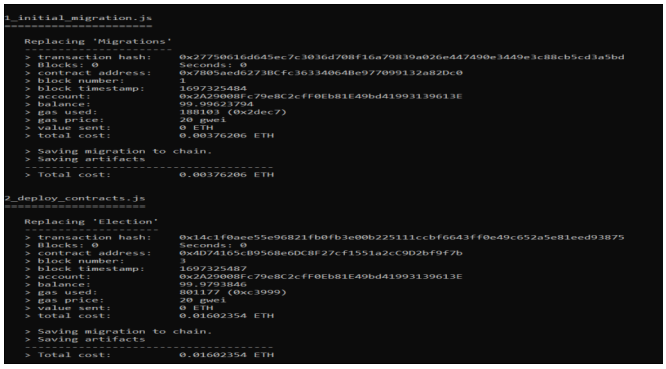
```
constructor () public {
    add (candidate1 , party1);
    add(candidate2 , party2);
    add(candidate3 , party3);
    }
function add (string memory
name,string memory party) private {
        candidatesCount ++;
        candidates[candidatesCount] =
Candidate(candidatesCount,
name,party, 0);
    }
```

Fig. 3. Constructor code block

Finally, we require two data structures first will map from address to bool. This map is employed to prevent the same address from casting multiple votes. It marks the user's address as "True" once they have cast their vote.

The second map is a mapping from uint to candidate. It serves the purpose of linking a candidate's unique identifier with their corresponding structure instance.

VI. RESULT



Compiling and Deployment of Contract

Fig. 4. Deployment of Contract

Creating private blockchain using Ganache

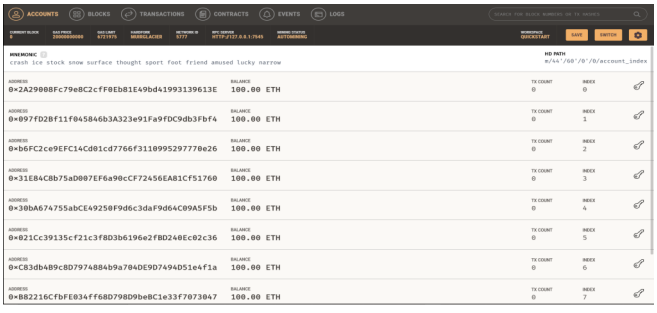
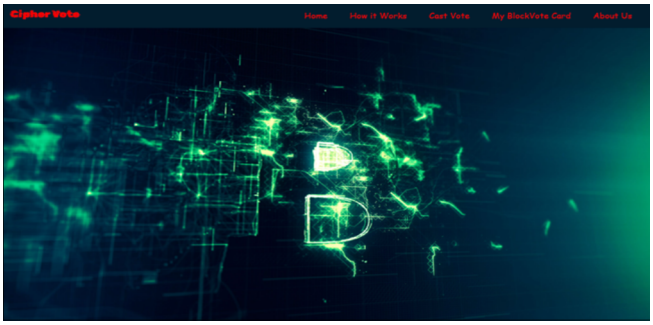


Fig. 5. Ganache

This is the Home page of our website

Figure 6: Home Page



This page shows the list of candidates and gives permission to cast vote.

Figure 7: casting vote

This Page includes request for the gas fee to complete voting.

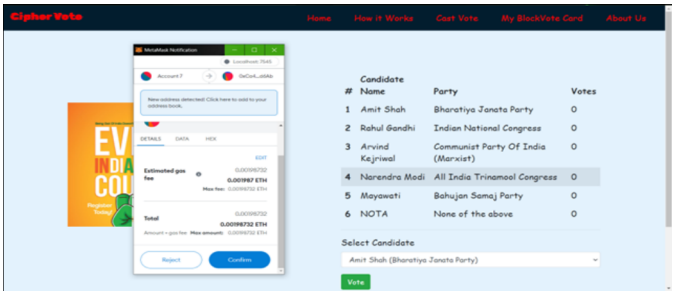


Fig. 8. Confirming the transaction to cast vote.

This page displays the confirmation of the voting process.

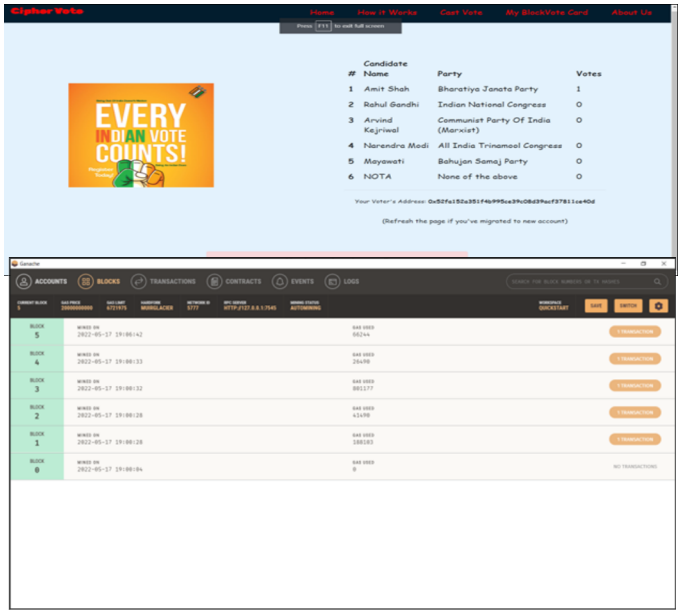


Fig. 9. Voting Complete

This page includes details of block mined after transaction.

Fig. 10. Blocks Mined after transaction.

VII. Conclusion

This paper presents a new electronic voting system that utilizes blockchain technology. Our system incorporates smart contracts to ensure secure and cost-effective elections, all while protecting voter privacy. Compared to previous methods, our research shows that blockchain technology provides democratic nations with the opportunity to transition from conventional pen-and-paper voting to more efficient and secure alternatives. Additionally, these advancements contribute to a more transparent electoral process.

The subject of electronic voting continues to be a topic of discussion among political and scientific communities. While there have been some successful examples, many attempts have faced difficulties in achieving the same level of security and privacy as traditional elections. Usability and scalability challenges have often been encountered.
This system has notable limitations, such as a fixed addition of blocks to the chain, high electricity consumption, and vulnerabilities in smart contracts. Nevertheless, it remains the most secure method for conducting elections.

By this juncture, we can confidently assert that our journey has been enriched with a wealth of knowledge derived from extensive research and hands-on experiences. Our exploration has delved into various technologies, encompassing the likes of Truffle, Ganache, blockchain, and MetaMask. These insights have not only broadened our understanding but have also equipped us with a valuable set of skills and insights. This learning journey has paved the way for our continued growth and expertise in the ever-evolving realm of technology and blockchain.

References

[1] S. Wolchok, Scott, et al. , ""“Security analysis of India’’s electronic voting machines.,”" ProceedingsProc. of the 17th ACM conferenceConference on Computer and communicationsCommunications securitySecurity., ACAcad. MMed., 1-14, 2010 [doi:10.1145/1866307.1866309].

[2] J. D. Ohlin, Jens David. , ""“Did Russian cyber interference in the 2016 election violate international law.,”" Tex. L. Rev., vol. 95, p. 1579, (2016): 1579.

[3] A. B. Ayed, Ahmed Ben. , "A conceptual secure blockchain-based electronic voting system." International Journal of Network Security & Its Applications 9.3, (2017): , pp. 01-09.

[4] R. Hanifatunnisa, Rifa, and and Budi Rahardjo. , ""“Blockchain based e-voting recording system design.”" 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA). IEEE, 2017, 2017 [doi:10.1109/TSSA.2017.8272896].

[5] B. Yu, Bin, et al. , ""“Platform-independent secure blockchain-based voting system.”" International Conference on Information Security. Cham: Springer, Cham, 2018.

[6] Y. Liu, Y.; and Q. Wang, Q. , “An E-voting Protocolprotocol Basedbased on Blockchainblockchain,”. IACR Cryptal. Enprint Arch. 2017, vol. 2017, p. 1043, 2017.

[7] B. Shahzad, B.; and J. Crowcroft, J. , “Trustworthy Electronicelectronic Votingvoting Usingusing Adjustedadjusted Blockchainblockchain Technologytechnology,”. IEEE Access 2019, vol. 7, pp. 24477– -24488, 2019 [doi: 10.1109/ACCESS.2019.2895670].

[8] K. M. Khan, K.M.; Arshad, J.; Khan, M.M. et al. , “Secure digital voting system based on blockchain technology,”. Int. J. Electron. Gov. Res. 2018, vol. 14, no. 1, pp. 53–-62, 2018 [doi:10.4018/IJEGR.2018010103].

[9] K. R. Alam, K.R.; Maruf, A.; Rakib, R.R.; Ali, G.G.N. et al. , “An Untraceableuntraceable Votingvoting Schemescheme Basedbased on Pairspairs of Signaturessignatures,”. Int. J. Netw. Secur. 2018, vol. 20, 2018.

[10] B. Adida, B., De Marneffe, O., Pereira, O. and Quisquater, J.J. et al., 2009. , “Electing a university president using open-audit voting: Analysis of real-world use of Helios,”. EVT/WOTE, vol. 9, (no. 10), 2009.

[11] E. Ben-Sasson, E., Chiesa, A., Genkin, D., Tromer, E. and Virza, M. et al., 2013. , SNARKs for C: Verifying programProgram executionsExecutions succinctlySuccinctly, 2013.

[12] D. Chaum, D., 2004. , “Secret-ballot receipts: True voter-verifiable elections,”. IEEE security & privacyIEEE Secur. Privacy Mag., vol. 2, (no. 1), 38-47, 2004 [doi:10.1109/MSECP.2004.1264852].

[13] A. Parsovs, A., 2016. , Homomorphic Tallying for the Estonian Internet Voting System. IACR Cryptology, 2016.

[14] Hudson 2017, “EIP’s Secret-ballot receipts: True voter-verifiable elections,”. IEEE securitySec. & privacyPrivacy, 2017.