Blockchain based digital voting system: A secure and decentralized electoral process

Amitabh Bhargava
Amity Business School
Amity University
Greater Noida, UP, India
amitabhbhargava1@gmail.com

Ajay Rana
Amity School of Engineering and Technology
Amity University
Greater Noida, UP, India
ajayphdmba@gmail.com

Deepshikha Bhargava
Amity School of Engineering and Technology
Amity University
Greater Noida, UP, India
deepshikhabhargava@gmail.com

2022 5th International Conference on Contemporary Computing and Informatics (IC3I) | 979-8-3503-9826-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/IC3I56241.2022.10073137

***Abstract*: Voting is the right of every citizen to make significant decisions regarding the selection of their respective government. The contemporary voting techniques such as ballot boxes, Electronic Voting Machines and digital voting systems can be susceptible to security concerns such as DDoS attacks, fraudulent votes, vote tampering and manipulation and virus assaults. The proposed method an attempt to propose a secure electoral process with the use of block chain technology. This article proposes the use of Blockchain Technology to mitigate faults in existing e-voting system and offers more safe, trustworthy, and transparent system. The proposed block chain based digital voting proposes data security and decentralization to address the challenges with the current voting method.**

Keywords - Digital Voting, Blockchain, Ethereum, Smart Contracts

I. INTRODUCTION

The underlying concept of decentralization has steadily garnered attention with the rise of blockchain technology. The main objective of research is to improve the electoral process by using blockchain to create a digital ledger. The rule of one vote per person applies to all eligible voters on all voter lists. Using a digital ledger, this is simple to do. Votes can be cast in any number of ways. The method will be straightforward, and the results will be automatically counted. EVMs are faster and more efficient than they are now. Originally designed for a crypto currency, blockchain was utilized to create distributed databases (bitcoin). The transactions made by users utilizing blocks are recorded on the blockchain.

Blockchain makes it feasible to create a secure and reliable voting system. For elections, Ethereum blockchain technology will be used. The digital ledger will assist in maintaining a list of all voters, and each voter will be able to vote, with the vote being automatically counted and the transaction completed by the digital ledger.

A. E-Voting

When the voters cast ballots using electronic devices, it is known as electronic voting. The Internet, computer coding, and mobile streaming are all covered by electrical equipment. Voters can vote from anywhere and participate in various election processes.

Disadvantage of e-voting system are electronic Voting Can Be Compromised by Hackers, electronic Voting Makes Fraud Easier, voting can be affected by producer bias.

B. Blockchain

Bitcoin, a crypto currency network, is managed by Satoshi Nakamoto, who launched Blockchain in 2008. Blockchain is a free method that may be used by any organization, notably to manage external electronic data without the need for a central controller. Due to the lack of a central regulator, blockchain deployment is transparent and unaffected. Because no personally identifying information is shown immediately in the block, blockchain offers users with anonymous names. Voting using e-Blockchain must retain the highest level of security and privacy. To maintain the integrity of all blockchains, blockchain technology employs cryptographic hash functions and digital signatures. Each block in the 338 blockchain contains a spreadsheet, a previous block hash, a miner address, a list of unverified operations, and a random number. A cryptographic hash algorithm will be used to feed the data spreadsheet. The hash output should be short enough for network servers to receive blocks. The size of the hash output is determined by a random number in a block spreadsheet. Trial and error is the only way to find the small hash. The block will be rejected if it has a large hash effect dispersed over the network. Different nodes will sometimes find different answers in the same block at the same time. The blockchain will then see a momentary split as some nodes accept one version of the solution while others receive another. The rule is then followed by Blockchain. "The blockchain with the longest chain is the correct chain." This notion depending on the consensus of all network miners If one node chain is longer than another, the old blockchain will be discarded and the longest new chain will be adopted as the valid blockchain across the network. The use of blockchain technology in the E-voting protocol can improve the voting process' security and protect each voter's privacy. Electronic blockchain-based voting the protocol is independent and does not require individual confidence. They have the right to vote through registered voters. Electronic gadgets with internet access. The entire vote the records will be made public and can be verified by any of the employees. No one can influence the voting process in any way.

C. Blockchain Architecture & Core Components

A node is a user or a computer in blockchain architecture (each device has its own copy of the whole ledger from the blockchain); transactions are the smallest blockchain system (records and data) used by blockchain. A block is a set of data structures used to carry out network transactions between many nodes. A chain is a logical arrangement of blocks. Journalists: Miners take notes in order to authenticate transactions and upload them to the blockchain system. Compatibility refers to a set of rules and organizations for implementing blockchain protocols.

D. Characteristics of Blockchain Architecture

1) *Cryptography*: Due to computational and cryptographic evidence among stakeholders, blockchain transactions are confirmed and accurate.

2) *Consistency*: Any blockchain document cannot be modified or erased; everything can be tracked in a blockchain block, which is known as provenance.

3) *Distribution*: All dispersed information might be accessed by any member of the blockchain network. As seen in the primary procedure, the compatibility algorithm permits system control.

4) *Anonymous*: An address, rather than a user identify, has been generated by a blockchain network participant. It maintains anonymity, particularly in the social blockchain system.

5) *Transparency*: The inability to fool a blockchain network is known as transparency. It is not possible since clearing the blockchain network requires a lot of computing power.

E. Hash Function

The integrity of the blockchain is verified using the cryptographic hash function. In a blockchain, process each block, one at a time for the hash function, combining the hash from the preceding block each time. To receive a new block over the whole network, each block must have a valid hash value from the previous block and the current block's hash value. A hash result written at the beginning of the next "malicious block" block is no longer compatible when a malicious block is added to the centre blockchain. The blockchain network will never accept this "cruel" chain unless all subsequent blocks in the series have the same hash value as the preceding one. The extra block should complete the chain's feature on acceptance, but doing so will be challenging. In each block, there are backward transitions. If a cruel attacker was able to resolve an additional block and modify the hash out of the first list in the next one block to match the "malicious" block, the attacker would also need to change the output hash of the sequence block matching block that was not previously resolved. To properly execute any alterations to a blockchain, the intruder must resolve all subsequent blocks. To properly convert it, the attacker must have the most powerful computer and network. Because when an attacker solves a "malicious" chain's whole block, additional chain nodes might start solving fresh and more durable blocks. As a result, a "cruel" hacker chain will be rejected since its length is less than the required blockchain entire network permission.

F. Digital Signature on Blockchain

A blockchain is authorized via a digital signature [20]. Two keys are required for a valid digital signature. The first is a secret key, which is a long random character unit used to obtain access to all of the account's data. Never give out the secret key to anyone. The second is the public key, which is complemented with a secret key known as the I account address. Anyone can still get their hands on the public key. The digital signature system is incredible. To obtain the hash value, the message is first accelerated. The sender's secret key was then used to sign the hash value. Digital signature refers to this method. Finally using the sender's public key, the recipient receives the message along with a digital signature and verifies the sender's digital signature. To modify a block in a blockchain, an attacker must first change the content of the block, then duplicate the digital signature to match "malicious" changes. Because of the hash function's "one-way" function, it can only achieve it by trial and error, as the vital adjustments take too long, to properly get the right hash. For example, guessing the entire solution combination through the SHA-256 hash will take around 1050 years to complete. As a result, digital signatures have been shown to protect blockchain block integrity.

G. Smart Contract: Ethereum

Blockchain is a sequence of blocks that form a continuous ledger. Each block comprises hundreds to thousands of transactions, which are guaranteed by miners on the blockchain network before being compiled and transported at the end of the main chain.

Mining is a compliance technique that allows miners to validate transactions and packages before sending them to the end of the chain. It can keep detailed records of each block's orders, use the method to gain consensus among miners, and prevent attackers from disrupting the block. No one may cheat or cancel their transaction by interrupting any part of the block. Because each block retains the previous block's hash value, the block's internal content cannot be easily disturbed once it is completed. If the block is interrupted, the succeeding blocks should be affected as well, implying that reaching this goal will need a significant amount of computing power. To put it another way, any attempt to engage in double spending will fail. Because blockchain is a public and transparent record, any blockchain network

participant can query or check the transaction's content to assure non-refusal. Ethereum has a fair value and has overcome the problem of Bitcoin's restricted flexibility. The most important contribution of Ethereum is a smart contract that allows users to run apps on private chains. Furthermore, only authorised individuals may engage in a private or cooperative series to reach a consensus [11, 14,15].

Ethereum creates a contract address, which allows anyone with the address to communicate and send messages through contract.

H. Advantages of decentralized voting system using blockchain

Blockchain technology creates a spatial distribution system that is accessible across an untrustworthy network of players. Using the appropriate structure, apply blockchain technology to an electronic voting system to include characteristics such as data secrecy, data integrity, and data authentication. We will describe how to incorporate the features of the blockchain into an electronic voting mechanism in this article. This is a voting system based on the blockchain.

When the proposed system is operational, the protocol promises to provide a secure electronic voting process. We create a blockchain-based protocol that transforms an optional protocol into a default control system without relying on any one business point. Finally, on this page, we go over the characteristics of our electronic blockchain-based voting mechanism.

However, there are new obstacles and restrictions that must be overcome. Our proposed protocol is described in this document. Electronic voting yields faster results Internet voting can boost turnout Why In the Long Run, Electronic Voting Is More Cost-Effective

II. LITERATURE REVIEW

A very few articles have been published recently that highlight the security and privacy issues of electronic voting systems based on blockchain. That Shows comparisons of chosen blockchain electronic voting systems.

Mc Corry et al. [1] presented a block chain based self-tallying Internet voting system. They used open vote network which as a decentralized double round protocol to support small scale voting. This method has limitation of non-calculation, even if only one voter misses/delays voting [20].

Ahmed Ben Ayed [2] Presented a voting system on blockchain in which they used a simple interface where first they have an authentication page on which voters first login with the valid authorization to cast a vote otherwise their e-Voting [16, 17] system does not allow to access their content for registering the vote. Systems that allow ownership to be improperly built are often at risk in which the attackers demanded a large number of false identities and cast a vote in a box containing illegal votes. Voting will be done with the help of friendly interface.

Hj´almarsson [3] et al. also presented a new voting scheme based on the blockchain technology. The voters can check their result with the help of smart contract at the time of voting. However, the methodology does not ensure the privacy of voters and the transparency of the result.

Layi et al. (2018) [4] presented an electronic voting system differentiated by an anonymous name (IDEE) that required a low level of confidence among participants, They think that in current election the current voting system for date is suitable .but unfortunately their system is not strong enough to handle DoS attacks because there was no outsider company mandate in the participants. They think that in the big electoral election, the current voting suitable for small scales due to limitations of platforms. Although the use of the system for a date is fine. But, their presented system is not strong enough to for polling the post-election procedure. This program is the only Signature Ring keeps the privacy of each voter, it is hard to manage and coordinate a few signatory organizations.

Shahzad et al. (2019) [5] made the BSJC's proposal for "proof of completeness" as a suitable method of electronic voting. They tried to address security issues in elections. The challenges of this research are high risk of data breach due to involvement of a third party and delayed voting process.

Gao et al.(2019) [6] developed a blockchain dependent anti-quantum electronic voting protocol includes research functionality. They also made changes to the Niederreiter code-based algorithm to make it proof against quantum attacks. Key Generation Center (KGC) is an noncertified cryptosystem that acts as a controller. It not only notice the anonymity of the voter but also helps the performance of the survey However, a review of their system reveals that, while the number of voters is modest, the use of security and efficiency are great in a small election. But when the number is high, some efficiency is reduced in order to provide better security and privacy.

Khan, K.M.(2020) [7]developed a block-based voting architecture (BEA) proposal that conducted rigorous testing of licensed and unlicensed blockchain structures for a variety of factors including voter turnout, size of blocks , block production rate, and performance speed of the block . Their analysis also reveals interesting findings on how these parameters influence the overall balance and reliability of the electronic voting model.

However, this model has a flaw in that it uses a standard database to store voter information, which allows anyone to tamper with it.

Another drawback was that under their concept, anyone can run for office, making it difficult for the election commission to determine who is eligible.

Yi introduced the Blockchain-based Electronic Voting Scheme (BES) is a project that uses blockchain technology to improve the security of electronic voting on peer-to-peer networks. A distributed document (DLT)-based BES could be used to combat vote fraud. On the P2P network [13], the application was tested and designed for Linux programs. The attack of the opposing rate is a major issue in this procedure. This method necessitates the engagement of third parties and is not well suited for usage in a multi-agency system in a single location. A distributed procedure, or the utilization of multiple secure computers, may be able to overcome the problem. However, in this case, the computer cost is critical, and it can be avoided if the computing job is difficult and there are too many variables.

1) Some of the already build platforms on voting System Using Blockchain: The voting sector is being improved by the following enterprises and organizations, which were established but mostly formed in the last five years. They all have a strong belief in the blockchain network's ability to improve performance. The diagram below depicts various internet forums, their compatibility, and the technologies employed to improve the system. Voting systems based on blockchain are now experiencing growth issues. These programs should only be used in moderation. However, because they use existing blockchain frameworks such as Bitcoin, Ethereum [22], Hyperledger Fabric, and others, their systems do not scale adequately at the national level to process millions of transactions. We give a scalability analysis of prominent blockchain platforms. Scalability is a problem that develops from blockchain value propositions; as a result, adjusting blockchain settings is difficult. It is not enough to raise the block size or shorten the blocking time by lowering the hash complexity to gauge blockchain. Before reaching the transaction required to compete with corporations like Visa, which holds an average of 150 million dollar every day, the power of measuring approaches its limit in each case. According to a 2018 report by Tata Communications, 44 percent of organizations use blockchain in their research and refer to frequent challenges that arise from the adoption of new technology. From an architectural standpoint, the unresolved equity problem is a barrier to blockchain adoption and practical implementation. "Blockchain-based solutions are relatively slow," according to Deloitte Insights. For organizations that rely on efficient asset processing systems, the slow pace of Blockchain transactions is a serious issue. The public got a taste of scalability issues in 2017 and 2018 when the Bitcoin network experienced major delays and overcharging, and the popular Crypto kitties programme took down the Ethereum blockchain network (a network of thousands of reduced applications relying on it).

2) Follow my vote: It is a blockchain-based firm with a secure online voting platform [9] that allows users to verify ballot boxes in real time to track democratic progress. This forum allows voters to vote for their preferred candidate from a wide range of locations. It may then utilize their identities to open the ballot box and obtain their vote, as well as verifying that both are right and that the election results are statistically accurate.

3) Voatz: This Company has developed a mobile - application based on blockchain where one can do voting remotely and anonymously and making sure each and every vote is counted correctly.

The Voters are being authenticated using their unique signatures like fingerprints or retinal scan, also the voters can also verify the candidates standing in the elections

4) Polyas: This Company was founded in 1996 in Finland. It uses blockchain tech ology to develop voting system which it provides to public as well as private sector.

This company has been certified and under the German Federal Office for Information Security for electronic voting system applications in 1996. This company has now grown it customer base to USA and Europe

5) Luxoft: The international I.T service provider Luxoft Harding Inc in partnership with The City of Zug and the Lucerne University of Applied Sciences of Switzerland developed the first ever electronic voting system based on blockchain technology. Luxoft made platform which drived the government's adoption of blockchain based services and established the Government alliance Blockchain to promote the use of blockchain technology in more of government related services.

6) Agora: A party has sent off a computerized blockchain surveying stage. It was laid out in 2015 and was utilized sparingly in Sierra Leone's official political decision in March 2018. Marketplace structures are based on new mechanical advancements: a custom blockchain, interesting versatile security, and a conventional consistence instrument. The vote is a conventional image in the Agora environment. It energizes residents and chose authorities, who go about as political race screens all over the planet, to concede to a protected and straightforward constituent framework. The vote is a worldwide image of the Agora environment.

7) Security Requirements for the Voting System: Any electronic voting system must follow the below listed security requirements in order to be eligible.

8) Obscurity: All through the democratic interaction, the quantity of electors should be safeguarded from outer translation. Any relationship between the registered votes and the identity of the voters within the electoral structure will not be known.

9) Readability and Accuracy: Accuracy requires expects that the proclaimed outcomes be in accordance with the political race results. It implies that nobody can change the vote of different residents, that the last registration incorporates every single substantial vote, and that there are no accurate provisos for invalid votes.

10) Unity: The democracy is maintained when only eligible and authenticated voters can vote and no one can repeat their vote.

11) Vote for privacy: After voting, no one should be in a position to attach the voter's identity and vote. Computer secrecy is a soft form of secrecy, which means that voting relationships remain secretive for as long as the current level continues to change with the power of the computer and new methods.

12) Strength and Integrity: According to this requirement, only a large group of voters can not disturb the election process. This condition ensures that the authenticated and registered voters will not suffer from any problem while the voting process. Corruption of citizens and officials has been denied in the process of contesting the election results by arguing that one member did not perform his or her duties properly

13) Lack of Evidence: Although anonymous securities provide protection against electoral fraud, there is no way to assure that votes are cast in any way under the influence of bribery or electoral fraud. The origin of this question can be traced back to the beginning.

14) Transparency and Righteousness: It means that no one will know the details until the figure is released. To be the first to know, it avoids acts such as postponing voter decisions by publishing a prediction or delivering significant but erroneous rewards to particular individuals or groups.

15) Discovery and Travel: Voting systems must stay operational during the voting process. The voting area should not be limited by voting systems.

16) Participation and authentication: A condition additionally called a longing makes it conceivable to evaluate regardless of whether a solitary citizen has taken an interest in a political decision. This condition should be met while citizen casting a ballot becomes obligatory under the constitution (similar to the case in different nations like Australia, Germany, Greece) or in a social setting, where casting a ballot is viewed as an affront (as minor). Furthermore, a mid-term business board post submitted).

17) Accessibility and Verification: To guarantee that every individual who needs to cast a ballot has the valuable chance to observe a reasonable democratic stall and that surveying station should be open and available to the citizen. Just qualified citizens ought to be permitted to cast a ballot, and all votes ought to be determined precisely to guarantee that the political race is substantial.

18) Recovery and Identification: To avoid errors, delays, and attacks, voting systems can track and recover vote information.

19) Voter Verification: Verification implies that audit mechanisms are in place to ensure that they are carried out correctly. For this objective, there are three possible phases: (a) a clear confirmation compared to the poll, which is a weak need for each voter to guarantee that his or her vote is correctly considered; (b) a clear confirmation compared to the poll, which is a weak requirement for each voter to ensure that his or her vote is properly considered.

III. Motivation

The main motivation of this application is to improve the election system in India using Blockchain technology, especially in small towns, college elections like one that happens in Delhi University for students' union, elections happening at school level, also the goal is to reduce the workload of setting up and running an election booth [10].

The earlier method of voting was that the voter casts his/her vote in an enclosure, known as secret ballot. The ballot boxes are then sealed in presence of officers. Later, the EVMs that is electronic voting machines were introduced as they were much safer and tamper proof and ensure free and fair elections. In EVMs, the voter has to press the appropriate button to vote for candidate of his/her choice, and once the button is pressed the machine switches off and next voter turn comes in. This method was much faster and safer than the ballot boxes method which was totally manual.

But the problem with both the systems is that both the system requires tight security, so that no one can play around and comprise the security of the voting numbers.

So, here the blockchain based voting system can play a great role. Blockchain is basically distributed database which stores data in digital format, where records are stored in form of transactions in a block, a block is collection of these transactions. As in blockchain, the information can be stored, recorded and distributed, but cannot be edited, so there is no chance of the information being tampered with.

IV. Proposed Methodology

Several studies have been conducted on the use of computer technology to improve election results. This study reports on the risks of implementing an evoting system due to software issues, insider threats, network vulnerabilities, and auditing issues. We propose to develop an existing online voting system integrated with blockchain technology. The proposed system has the following advantages over the existing system. Consumers can vote anywhere in the world as long as they are Citizen of India. Since the votes are stored on the blockchain and there is no voting queue, it has anti-tamper features, which saves a lot of time and reduces the load.

The Ethereum platform is used to create a voting smart contract. The contract is in charge of both producing the poll and running the election. When the poll is finished, the results are calculated, and the outcome is displayed. It contains two modules that are engaged in polling: The first is the polling procedure, and the second is the voting process. Creating a poll includes Adding candidates, Election period, etc.

choosing a candidate, and voting are all part of the voting process. Finally the result is displayed.

Blockchain technology, which uses cryptographic hashes to assure end-to-end verification, is used to secure the votes. A successful vote cast is handled as a transaction in the voting application's blockchain to achieve this goal. As a result, a vote is recorded in the database's data tables and uploaded to the blockchain as a new block (after successful mining). The miners generate a transaction that is unique to each vote as soon as the vote is mined. If a vote is deemed malicious, miners will reject it.

It's important to remember that a voter's cryptographic hash is the only way to identify them in the blockchain. This property aids the verifiability of the entire voting process. Furthermore, this id is secret and cannot be seen by anyone, including the system operator, guaranteeing that individual voters' privacy is protected.

- Anonymity: This system will not display or record the names of people who have voted for a certain candidate, preserving the voters' anonymity.
- Accuracy: The votes are counted in real-time and can be displayed or hidden until the poll closes so that the voting trend is not affected.
- Verifiability: The Ledger is open to the public and anyone may check the results, but it is immutable, so the results cannot be changed.

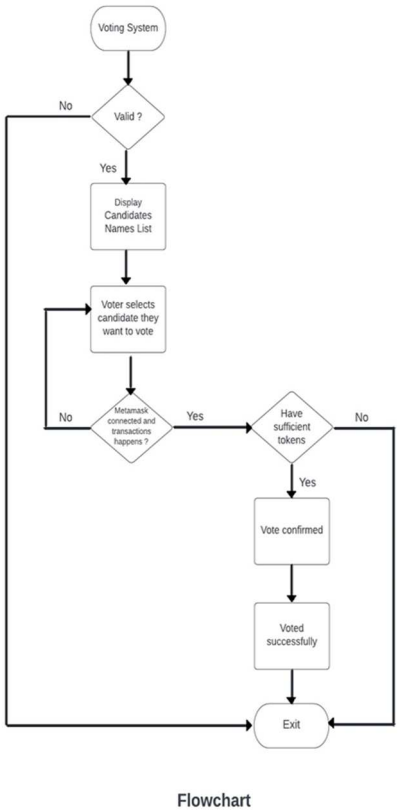

Figure 1: Proposed System

V. Implementation Details

The figure shows the flow chart of how the blockchain based voting system works. It consist of many modules but mainly three which are election manager who will be responsible for setting up the details over which smart contract will be made, who will be responsible for registering the candidates, next is the testing module which is responsible for testing the smart contract and for this we are using Mocha framework, and the last one is the voter's module where voters who are verified will be able to import their Ethereum using Metamask and cast their vote.

The system was implemented using Ethereum blockchain, Truffle, Ganache, Web3 js and Solidity for server side, and Metamask account's wallet is used at client side.

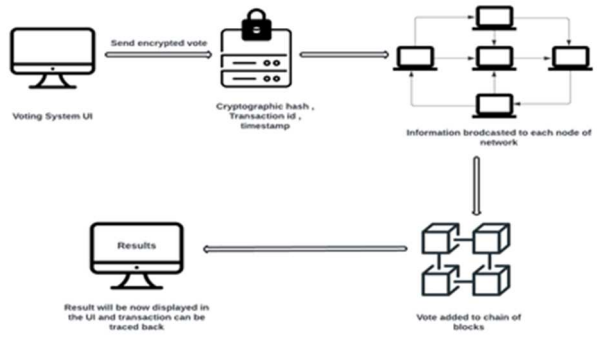

Figure 2 (a): Blockchain Implementation

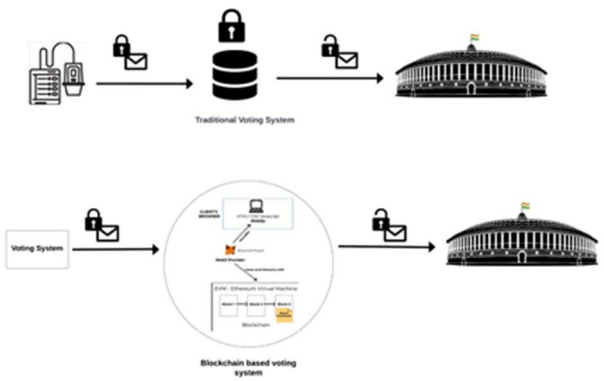

Figure 2 (b): Blockchain Implementation

Ethereum blockchain network is used to store the data as a medium of exchange or, so we use it store the votes. It uses the Ethash algorithm which stores the hash value of pervious block into the next block forming a chain of connected data blocks. So, whenever a new transaction happens, a new data block gets added. And if someone tries manipulate with the data in block, its hash value changes, and that's how we get to know that data is manipulated. Therefore, we store the votes casted by voters in form of transactions that are later used to calculate the count of votes.

Truffle framework is used for deployment of smart contracts on the network. Ganache provides us with lots of dummy Ethereum accounts for testing. Web3 js is the tool for developers to interact with Ethereum network. Solidity is mainly used for writing smart contracts code Mocha is the testing framework , used to test any type of JavaScript code , so can be used to test frontend application, backend application and even Ethereum application.

VI. Results And Discussion

The work on the depicted idea can be used in the improvement of a completely practical democratic system over a blockchain network. With the properties of immutability and decentralization of blockchain, appropriately executed on account of e-voting system, the chaos around the casting a ballot interaction can be reduced colossally [2, 12].

Also, the cryptography in blockchain leads to tighter security of voter's and candidate's information and public distributed ledger makes it easy for authorized authority to review the end results of the election.

Our blockchain based e-Voting system thus utilizes all the properties of blockchain network and smart contracts to provide a secure, hassle-less and cost-effective platform for voting to voters as well as candidates standing for elections. Therefore, comparing to other electronic voting system, using blockchain technology for developing voting system by developing nations, progressing from pen-paper or ballot box to this type of more cost-effective and highly transparent system, leads to development of the nation.

VII. Conclusion And Future Scope

This research takes advantage of blockchain property of transparency to create an effective e-voting solution. The proposed approach has been implemented with Multichain to meet the fundamental requirements for an e-voting scheme [18,19].

In order to continue this work, the authors are trying to expand this work as follows the contract can be changed to allow for numerous elections to be held at the same time.

Integration with security devices such as biometric and facial recognition modules.

For remote locations with limited access to technology, integration with hardware modules is recommended. The blockchain can be used to securely store user data

References

[1] McCorry, P., Shahandashti, S. F., Hao, F. (2017, April). A smart contract for boardroom voting with maximum voter privacy. In International conference on financial cryptography and data security (pp. 357-375). Springer, Cham.

[2] Ayed, A. B. A Conceptual Secure Blockchain Based Electronic Voting System. International Journal of Network Security Its Applications, 9(3), 01–09. https://doi.org/10.5121/IJNSA.2017.9301

[3] Hj´almarsson, F. ., Hreiarsson, G. K., Hamdaqa, M., Hj´almty´sson, G. (2018, July). Blockchain-based e-voting system. In 2018 IEEE 11th international conference on cloud computing (CLOUD) (pp. 983-986). IEEE.

[4] Lai, W. J., Hsieh, Y. C., Hsueh, C. W., Wu, J. L. (2018, August). Date: A decentralized, anonymous, and transparent e-voting system. In 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN) (pp. 24-29). IEEE.

[5] Shahzad, B., Crowcroft, J. (2019). Trustworthy electronic voting using adjusted blockchain technology. IEEE Access, 7, 24477-24488.

[6] Gao, S., Zheng, D., Guo, R., Jing, C., Hu, C. (2019). An anti-quantum e-voting protocol in blockchain with audit function. IEEE Access, 7, 115304115316.

[7] Khan, K. M., Arshad, J., Khan, M. M. (2020). Investigating performance constraints for blockchain based secure e-voting system. Future Generation Computer Systems, 105, 13-26.

[8] Yi, H. (2019). Securing e-voting based on blockchain in P2P network. EURASIP Journal on Wireless Communications and Networking, 2019(1), 1-9. [5] Shrestha, R., Sah, R., Shrestha, S., Sarawagi, S., Adhikari, N. B. (2019). Blockchain Interfaced Sacure E-Voting System. Journal of the Institute of Engineering, 15(1), 195-199.

[9] Sah, R., Rathod, P., Rane, P., Yadav, A., Lifna, C. S. (2020). Vote Block: A Digital Ledger. SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, 12(SUP 1), 256-259.

[10] Patil, H. V., Rathi, K. G., Tribhuwan, M. V. (2018). A study on decentralized e-voting system using blockchain technology. International Research Journal of Engineering and Technology (IRJET), 5(11), 48-53.

[11] Dhulavvagol, P. M., Bhajantri, V. H., Totad, S. G. (2020). Blockchain ethereum clients performance analysis considering E-voting application. Procedia Computer Science, 167, 2506-2515.

[12] Curran, K. (2018). E-Voting on the Blockchain. The Journal of the British Blockchain Association, 1(2), 4451.

[13] Yi, H. (2019). Securing e-voting based on blockchain in P2P network. EURASIP Journal on Wireless Communications and Networking, 2019(1), 1-9.

[14] Ethereum a public blockchain https://ethereum.org

[15] Khan, K. M., Arshad, J., Khan, M. M. (2018). Secure digital voting system based on blockchain technology. International Journal of Electronic Government Research (IJEGR), 14(1), 53-62.

[16] Benny, A. (2020). Blockchain based e-voting system. Available at SSRN 3648870.

[17] Hanifatunnisa, R., Rahardjo, B. (2017, October). Blockchain based e-voting recording system design. In 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA) (pp. 1-6). IEEE.

[18] Kshetri, N., Voas, J. (2018). Blockchain-enabled e-voting. Ieee Software, 35(4), 95-99.

[19] Fusco, F., Lunesu, M. I., Pani, F. E., Pinna, A. (2018, September). Crypto-voting, a Blockchain based e-Voting System. In KMIS (pp. 221-225).

[20] Subramanian, H. (2017). Decentralized blockchain-based electronic marketplaces. Communications of the ACM, 61(1), 78-84.

[21] https://medium.com/@filzatariq92/build-your-ethereum-dapp-on-windows-withtruffle-ganache-and-metamask-beginners-guide-8c62b55ef556