Blockchain for Voting System

Pragati Pawar[1], Namrata Kawale Shinde[2]
[1,2]*Department of Computer Science, Patkar-Varde College*

Abstract - Blockchain is an advanced technology that offers a new and advanced based online voting system. As we know that Online voting can give access to people to vote from anywhere with a secure internet connection, which makes it more easier to use and reduces the costs like printing ballots and setting up polling stations. But still, online voting may have challenges, like hacking and vote manipulation. But with this Blockchain technology can help and solve these problems by giving a decentralized and secure based system where votes are recorded on a digital ledger that will not be easily tampered and this ensures votes are right, legitimate, and secure from fraud. And Some countries, like Germany, Russia, Estonia, and Switzerland, are already using blockchain for voting systems. While blockchain makes voting more secure and transparent, there are still challenges like protecting voter information and speeding up the vote processing. To make blockchain voting systems more practical and this improves for other security issues. This research looks at today's blockchain voting systems, their benefits, and what majors to be done to make them better. Overall, blockchain can make online voting more reliable, tempered proof, and accessible, supporting the core values of democracy.

***Key Words*: Blockchain Technology, Online Voting, Vote Security, Decentralized System, Voter Privacy, voting Challenges**

I. INTRODUCTION

Voting is the main part of democracy, which gives people the authority to choose their leaders and takes part in important decisions. For many years, elections have depended on paper ballots, a method which is known by people and very trustworthy, but not everything that is 100% give surety. It also comes with challenges like high costs, logistic challenge, crowded lines and security issues at polling stations.

As time goes by, there is a need to change the system and bring something new that provides security as well as trust of citizens. So with time new electronic voting came into the picture. Which gives a faster and easier way for specific people who face struggle to reach polling stations, such as those living outside of the country or people with disabilities because they also have to write to give vote as it is their right also. E-voting can reduce costs, and process the counting of voting faster and easily accessible to everyone.

But as we say nothing gives 100%guarantee, as it also has some challenges. Like security issues, central authority which still controls the system, and reliability issues which make many people question the transparency of e-voting. There's always a chance that votes are being tampered with and not counted or recorded correctly, which can reduce the public trust in the election process. Ensuring a balance between transparency and security remains a main risk in digital voting.

Blockchain is technology which is more secure and it is decentralised means no central control on the system means that it saves the data in such a way that it is impossible to change the data without being caught or detected. In voting, blockchain makes sure that voting is recorded correctly and no one can tamper with the data, making the process more transparent and secure as everyone has the right to see it as the data is openly available. Citizens can view their data but cant change it. Blockchain in voting systems can reduce the risks of fraud, increase the security and maintain the privacy of user data, and allow people to vote from anywhere with secure internet connection. Some countries, like Germany, Russia and more countries are already using blockchain for voting to improve the security and transparency of their elections. Blockchain-based voting systems have advantages, including decentralization that means no single person can control the system, and have strong security, and transparency. But, there are still places that need improvement like ensuring that the system handles large numbers of votes and mainly that we need to ensure that people's systems are also protected from any kind of hacking. This research aims to improve the current state of blockchain-based voting systems, and look into their benefits and drawbacks, and discuss what needs to be done to make these systems more secure and widely

used.

This introduction sets the aim for understanding how blockchain could change the voting, and can make it more secure, transparent so users can use it freely without any fraudulent or transparency issues.

II. BACKGROUND

Blockchain is linked with cryptocurrencies like Bitcoin and smart contracts on platforms such as Ethereum. Bitcoin was the first to use blockchain for secure currency transactions. Ethereum is mostly used because it introduces smart contracts into the picture, this contract is executed based on certain conditions given in code and it self executes when it calls in a program. These smart contracts take advantage of blockchain security and distributed consensus to make sure that they run the same way as they program for without any tampering. The idea of smart contracts is not new; it was introduced in the late 1990s when Nick Szabo described this as a digital agreement which includes protocols for parties to perform actions.

In today's time blockchain is a mixture of different technologies: including data organizing and also a method of reaching agreement in a decentralized manner and cryptography and smart contract also. And blockchain work by. Creating a series of blocks which are linked together in a chain, each containing a secured crypto hash of the previous block, a timestamp, and transaction data. This Ensures that once data is filled in in a block, it will not change even if it changes it would be easily detected by the network.

Where traditional systems which run on central authority Blockchain run on a network of connected computers without any central authority in that all the nodes share the same data, and to maintain the security and trust of the user it uses special protocol called consensus algorithms to make sure that there is agreement between every node. To ensure the integrity Common consensus algorithms used Proof-of-Work (PoW) and Proof-of-Stake (PoS), which give incentive to users who introduce new blocks over the network.

Blockchain depends on Public key cryptography which plays an important role in giving security and enabled digital signatures. Each user in the network has a pair of secure cryptographic keys which are public keys which are openly given and a private key that remains confidential. These keys authenticate transactions and make sure that only the authenticated owner of a digital right can manage it. This makes sure that the system gives security and anonymity which is relevant in cryptocurrency transactions. However, in cases like online voting, where votes must be both private and verifiable, additional security measures are needed beyond what blockchain alone can provide.

Smart contracts have broadened the usages of blockchain beyond digital currency, allowing a variety of applications. A smart contract is a self -executing program that runs on the blockchain, that follows predefined rules that automatically run the code without the need for a middle man. This feature is more powerful because once a smart contract is deployed, it cannot be changed, and its execution is checked by the whole network, ensuring trust and transparency.

Although this technology have strength it also have some challenges and one of it are scalability as network is expanding the node still need to process each and every transaction which can slow down the system

As more participant join network the process or reaching consensus became quit difficult as it required more validator to validate and it became a quit difficult to communicate which can delay the process. And in addition the blockchain networks are also not immune to denial-of-service attacks, where the network is flooded by loads of transactions or exploit vulnerabilities in smart contracts, such as those with infinite loops.

But in this case public blockchain networks often reduce the risk of the DOS by using transaction fees, which reduce the spam by making it costly so it is difficult for spammers to spam the network with transactions. But On the other hand Private blockchain networks can reduce these issues by using strict access controls.

Despite its strength in various features like decentralization, security, and transparency, it required consideration when working with blockchain technology especially when being used for confidential data of citizen like online voting application.

2.1 CORE COMPONENT OF BLOCKCHAIN ARCHITECTURE

Node: Users or computers in blockchain layout (every device has a different copy of a complete ledger from the blockchain);

Transaction: It is the blockchain system’s smallest building block (records and details), which blockchain uses;

Block: A block is a collection of data structures used to process transactions over the network distributed to all nodes.
Chain: A series of blocks in a particular order;
Miners: Correspondent nodes to validate the transaction and add that block into the blockchain system;
Consensus: A collection of commands and organizations to carry out blockchain processes.

2.2 CRITICAL CHARACTERISTIC OF BLOCKCHAIN ARCHITECTURE

Cryptography: Blockchain transactions are authenticated and accurate because of computations and cryptographic evidence between the parties involved.

Immutability: Any blockchain documents cannot be changed or deleted.

Provenance: It refers to the fact that every transaction can be tracked in the blockchain ledger.

Decentralization: The entire distributed database may be accessible by all members of the blockchain network. A consensus algorithm allows control of the system, as shown in the core process.

Anonymity: A blockchain network participant has generated an address rather than a user identification. It maintains anonymity, especially in a blockchain public system.

Transparency: It means being unable to manipulate the blockchain network. It does not happen as it takes immense computational resources to erase the blockchain network.

III. HOW BLOCKCHAIN TRANSFORM VOTING SYSTEM

Blockchain technology can show many issues in the current election, like illegal voting, data integrity, and less transparency. But by using blockchain it makes the voting process more secure and transparent which can keep the overall integrity of the voting process and by implementing electronic voting on a blockchain, vote is protected as the data is distributed over all other nodes.

Traditional voting depends on central authority which may lead to tempering of data as the data is in control of central authority without and it also has the risk of data alteration without the risk of any verification. In the opposite of this blockchain data is distributed along with different nodes which makes it impossible for anyone to hack the data as if any one try to do it other nodes are able to see it. So this sure that data is tempered proof or any data alteration and results can be verified against other nodes in the network.
As digital decentralized, an encrypted ledger blockchain offers strong protection against fraud. And also the blockchain based voting system reduces the risk of electronic voting by creating a tamper proof environment, as we know that no single entity including the government is in control. For this system to work effectively it must operate on fully decentralised infrastructure independent of central authority.
blockchain presents a new model for electronic voting, which ensures that the elections are free, fair and trusted. This innovative approach can improve the administration of elections and voter participation, making the voting process more secure and temper proof.

IV. SECURITY REQUIREMENT FOR VOTING SYSTEM

Anonymity: in this voter identity should remain secure and the information that who gives vote should be secure.
Auditability and Accuracy: in the it gives surety that result is tamper proof as no one should temper or recount the vote.

Democracy/Singularity: in this only eligible should be able to give vote and it must be for one vote at time. And no one should be able to give vote twice.

Vote Privacy: in this after the vote is casted the identity of the voter should be kept confidential and no one should link that who casted the vote.
Robustness and Integrity: the system must be able to handle any kind of error during vote cast and data must be tamper proof.

Availability and Mobility: voting system should be available throughout during when vote is casted.

Verifiable Participation/Authenticity: there should be a system that can verify that every eligible voter has given the vote.

Accessibility and Reassurance: polling stations must be available to everyone who wants to give a vote and only eligible voters should be allowed to cast their vote. And all votes must count accurately.

Recoverability and Identification: the system should be able to keep track of all information and restore it if any kind of error occurs.

Voter Verifiability: the voter must be able to check that they have casted the vote correctly This used both public verification and private verification.

V. ELECTRONIC VOTING ON BLOCKCHAIN

Electronic voting is a system where vote is counted and recorded on mobile phone and laptop. The process used key functions like registering vote and then casting votes, and final result. Electronic voting offers easy and efficient voting but it also has some risk associated with it.one of the major issues is hacking as we can protect the system of every individual. Some or many user systems may be vulnerable which can result in tempering of data.

But blockchain technology gives solutions to these problems. Unlike most electronic voting systems which depend on a single central server, blockchain stores the data on a decentralized network. This means keeping data only on one server. This technology keeps the data on different servers making it much difficult for any single point of failure to that system. Each vote is encrypted and store in a secure, tamper-proof ledger that access access to every people who is in network

In blockchain voting system votes are checked through a consensus process in which multiple nodes or computers check each encrypted vote. This decentralised technology makes sure that the voting process is tamper proof and secure. Although recorded vote is available to everyone as it is on a public network, individual voter identities are protected and remain enclosed. This system allows anyone to check the vote and count without being able to verify that this individual person has given a vote to this specific party. By combining transparency and cryptography, security blockchain technology is more reliable than traditional electronic voting systems, enhancing trust in the electoral process.

VI. CURRENT BLOCKCHAIN-BASED VOTING SYSTEM

Recently, several emerging companies have been working with blockchain based voting systems to improve transparency and integrity of vote. but the systems face scalability challenges. Existing blockchain networks like ethereum and bitcoin faced challenges handling large amounts of transactions which needed for national elections. Despite blockchain's advantage, its current transaction fall as compared to payment method systems like Visa, which processes approximately 150 million transactions daily. This raises concern about blockchain feasibility were speed and efficiency are important.

VII. RESULTS

Recent advancement in blockchain technology has led to the development of several new platforms to improve transparency of voting systems. Despiste this blockchain based voting system face challenges like scalability challenges or if something goes wrong with data or vote so there is no one to blame for this same. Current systems like Bitcoin and Ethereum are not able to handle these large transactions which are required for elections. These systems face many issues with both transaction speed and volume, which make them less comparactive then traditional payment networks like Visa, which manages 150 million transactions per day. Real-world case highlight this limitation, such as delays in Bitcoin and network congestion on Ethereum cause by applications like Crypto Kitties.

VIII. CONCLUSION

Blockchain technology systems show great improvement in electronic voting systems by making them more secure, transparent, and temper proof and reliable for election. It gives a way that vote is recorded correctly and counted correctly. Which can increase the trust of citizens in the voting process However, recently this blockchain based system faces challenges with handling large numbers of transaction., this limits their ability to manage elections. While blockchain has many advantages, it needs more development to handle voting

for a large number of the population. Further advancements are needed to handle voting on a large scale. ongoing research and new innovation are needed to improve these challenges and make blockchain a practical option for national election.

IX. ACKNOWLEDGMENT

This research paper was made under the guidance of Mrs. Namrata kawale so i would like to thank Mrs. Namrata Kawale for her invaluable support and guidance throughout this research. Her contributions were greatly appreciated.

REFERENCE

[1] Liu Y., Wang Q. An E-voting Protocol Based on Blockchain. IACR Cryptol. Eprint Arch. 2017;2017:1043. [Google Scholar]

[2] Shahzad B., Crowcroft J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. IEEE Access. 2019;7:24477–24488. doi: 10.1109/ACCESS.2019.2895670. [CrossRef] [Google Scholar]

[3] Racsko P. Blockchain and Democracy. Soc. Econ. 2019;41:353–369. doi: 10.1556/204.2019.007. [CrossRef] [Google Scholar]

[4] Yaga D., Mell P., Roby N., Scarfone K. Blockchain technology overview. arXiv. 20191906.11078 [Google Scholar]

[5] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. [(accessed on 28 July 2020)]; Available online: https://bitcoin.org/bitcoin.pdf.

[6] Garg K., Saraswat P., Bisht S., Aggarwal S.K., Kothuri S.K., Gupta S. A Comparative Analysis on E-Voting System Using Blockchain; Proceedings of the 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU); Ghaziabad, India. 18–19 April 2019. [Google Scholar]

[7] Kamil S., Ayob M., Sheikh Abdullah S.N.H., Ahmad Z. Challenges in multi-layer data security for video steganography revisited. Asia-Pacific J. Inf. Technol. Multimed. 2018;7:53–62. doi: 10.17576/apjitm-2018-0702(02)-05. [CrossRef] [Google Scholar]

[8] Jaffal R., Mohd B.J., Al-Shayeji M. An analysis and evaluation of lightweight hash functions for blockchain-based IoT devices. Clust. Comput. 2021 doi: 10.1007/s10586-021-03324-1. [CrossRef] [Google Scholar]