International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 04 | April - 2023 Impact Factor: 8.176 ISSN: 2582-3930

Decentralized Voting System: Exploring the Potential of Blockchain Technology

[1]Prabuddh Pathak, [2]Prakhar Muley, [3]Mrs. Varsha Kothari

[1] Student, B. Tech, Department of Computer Science and Engineering, Medi-Caps University, Indore, Madhya Pradesh, India

[2] Student, B. Tech, Department of Computer Science and Engineering, Medi-Caps University, Indore, Madhya Pradesh, India

[3] Assistant Professor, B. Tech, Department of Computer Science and Engineering, Medi-Caps University, Indore, Madhya Pradesh, India

---

Abstract- A blockchain-based tool called DeVote was created to support safe and open election procedures. DeVote seeks to eradicate the dangers connected to conventional voting systems, such as tampering, deception, and hacking, by utilising smart contracts and decentralised storage. Voters can anonymously submit their votes using DeVote while doing so safely from anywhere in the world. Vote monitoring and auditing capabilities are among the platform's additional features that enable greater responsibility and openness. Overall, by utilising the power of blockchain technology to create a more secure and reliable method of holding elections, DeVote offers an innovative answer to the problems that conventional voting systems encounter.

Key words: Blockchain, Voting, Distributed Ledger, Nodes, Smart Contracts.

1. Introduction

The democratic process is fundamentally based on the act of voting. It is a way for people to choose their representatives and express their preferences. Unfortunately, there are a number of drawbacks to using traditional voting methods, including security, transparency, and fraud risk. The shortcomings of the current voting system will all be fixed by the blockchain-based system. This paper aims to give a general overview of decentralised voting systems, outlining both the advantages and potential drawbacks.

Decentralized voting systems are a type of digital voting system that utilizes blockchain technology to secure and manage the voting process. They are designed to be transparent, secure, and accessible to all participants in the voting process. In decentralized voting systems, each vote is recorded on a distributed ledger that is maintained by a network of nodes. Tempering with votes is difficult in blockchain technology.

2. Literature Review

Decentralized voting systems have garnered significant attention in recent years due to their potential to provide secure and transparent voting mechanisms. These systems use blockchain technology to ensure that votes are recorded immutably, and cannot be tampered with or deleted. Additionally, they eliminate the need for intermediaries such as centralized voting authorities or election commissions, thereby providing a truly decentralized voting experience.

One of the earliest examples of a decentralized voting system is the liquid democracy system proposed by Larimer et al. in 2014 [1]. The system uses a hybrid approach combining direct and representative democracy, allowing users to either vote on issues directly or delegate their vote to a trusted representative. This system was designed to address issues such as voter apathy and low voter turnout by providing users with a more flexible and engaging voting experience.

Another example of a decentralized voting system is the DFINITY blockchain, which uses a threshold relay consensus mechanism to enable secure and scalable voting [2]. The consensus mechanism allows a group of validators to vote on a proposed decision, and only when a threshold number of votes have been cast in favor of the decision does it get approved. This mechanism provides a more secure and transparent voting experience than traditional centralized systems, and ensures that votes cannot be tampered with or deleted.

More recently, the Ethereum blockchain has been used to develop several decentralized voting systems such as the Decentralized Autonomous Organization (DAO) [3]. The DAO is a decentralized organization that allows its members to vote on proposals and decisions using the Ethereum blockchain. The system is fully autonomous and self-governing, with decisions being made based on the consensus of its members. Additionally, the system allows for proportional voting based on the amount of tokens held by each member, thereby ensuring a fair and transparent voting process.

However, despite the potential benefits of decentralized voting systems, there are several challenges that need to be addressed. These include issues such as scalability, voter anonymity, and voter identification. Additionally, there is the risk of attacks such as sybil attacks, where a single user can create multiple fake identities to manipulate the voting process.

To address these challenges, several approaches have been proposed such as the use of zero-knowledge proofs to ensure voter anonymity and identity verification [4], and the use of sharding to increase the scalability of the voting system [5].

In conclusion, decentralized voting systems have the potential to provide a more secure and transparent voting experience, eliminating the need for centralized authorities and intermediaries. However, several challenges need to be addressed before these systems can be widely adopted, and further research is needed to address these challenges.

2.1 Overview of Blockchain Voting:

Blockchain voting is a decentralized system that uses distributed ledger technology to provide transparency, immutability, and security in voting processes [6]. Blockchain voting systems can be categorized into two main types: permissioned and permissionless. Permissioned blockchains are used by centralized organizations such as governments, while permissionless blockchains can be accessed by anyone. The benefits of blockchain voting include increased security, transparency, and accessibility [7].

2.2 Challenges of Blockchain Voting:

One of the main challenges of blockchain voting is the potential for voter coercion or vote buying. Another challenge is the difficulty in ensuring that every voter has an equal opportunity to vote. Additionally, the complexity of the technology involved in blockchain voting may limit its accessibility to certain groups of voters [8].

2.3 Research on Blockchain Voting:

Several studies have examined the feasibility and security of blockchain voting systems. Zhang et al. (2018) found that blockchain voting can improve security and transparency, but that it may not be suitable for all types of elections [9]. Shin and Kim (2020) found that blockchain voting can provide secure, tamper-proof voting records, but that the technology must be carefully designed to prevent fraud and manipulation [10].

2.4 Case Studies of Blockchain Voting:

Several blockchain voting systems have been implemented in recent years. For example, West Virginia used a blockchain-based mobile app for voting in its 2018 midterm elections. However, the app was criticized for its lack of transparency and potential security vulnerabilities. Another example is the use of blockchain voting in the 2020 Democratic National Committee primaries, which was considered a success despite some technical issues [11].

2.5 Future of Blockchain Voting:

The potential benefits of blockchain voting make it an attractive solution for secure and transparent voting. However, there are still several challenges that need to be addressed before blockchain voting can be widely adopted. These challenges include ensuring voter privacy and accessibility, as well as addressing technical issues such as scalability and interoperability [8].

2.6 Pros of Decentralized Voting Systems:

1. Transparency: Decentralized voting systems offer transparency in the voting process, as each vote is recorded on a public blockchain. This allows voters to

verify that their votes have been counted correctly and ensures the integrity of the voting process [12].

2. Security: Decentralized voting systems use cryptography and distributed consensus mechanisms to secure the voting process, making it resistant to hacking and fraud [13].

3. Accessibility: Decentralized voting systems can increase accessibility to voting, as they can be accessed from anywhere with an internet connection. This can increase voter turnout and reduce the barriers to voting [14].

4. Efficiency: Decentralized voting systems can be more efficient than traditional voting systems, as they can reduce the need for intermediaries and eliminate manual processes. This can reduce the time and cost of conducting elections [15].

2.7 Cons of Decentralized Voting Systems:

1. Voter Privacy: Decentralized voting systems can compromise voter privacy, as each vote is recorded on a public blockchain. This can make it possible for others to track how an individual voted, which can lead to voter intimidation and coercion [16].

2. Technical Complexity: Decentralized voting systems require technical expertise to develop and operate, which can limit their adoption and use. Additionally, the complexity of the technology can lead to errors and vulnerabilities that can compromise the integrity of the voting process [17].

3. Voter Education: Decentralized voting systems require voters to have a basic understanding of blockchain technology and cryptography to participate. This can limit the participation of certain groups and may require additional voter education initiatives [18].

4. Infrastructure: Decentralized voting systems require a robust infrastructure to operate, including access to the internet and electricity. In areas with limited infrastructure, decentralized voting systems may not be feasible or reliable [19].

3. Proposed System

3.1 System Requirements

Functional requirements are the specific features and functionalities that an e-voting system must possess to fulfil its intended purpose. The following are some of the key functional requirements of an e-voting system.

1. Authentication and authorization: The system should have a robust authentication mechanism to verify the identity of voters and ensure that only authorized people are allowed to vote.

2. Vote casting and tabulation: The system should allow voters to cast their votes securely and accurately, and it should ensure that votes are tabulated correctly.

3. Accessibility and usability: The system should be accessible and easy to use for all voters, regardless of their physical abilities or technical knowledge.

4. Security and confidentiality: The system should employ robust security measures to protect the integrity and confidentiality of the voting process and prevent unauthorized access or manipulation.

5. Accuracy: There should not be any redundant voters and every vote should be counted once.

4. Methods

4.1 Blockchain

Blockchain technology works by creating a decentralized network of computers that work together to verify and record transactions. When a participant initiates a transaction, it is broadcast to the network, and the computers in the network verify the transaction by checking the digital signature of the sender and ensuring that they have the necessary funds to complete the transaction.

Once the transaction is verified, it is added to a block of transactions, which is linked to the previous block, creating a chain of blocks or a blockchain. This linking makes it difficult for any one person or group to alter the contents of a block without being detected.

Moreover, every participant in the network has access to the blockchain, which provides a high degree of transparency, as every participant can verify the contents of the blockchain. The network is decentralized, which means that there is no

central authority controlling the network, and each participant in the network has a copy of the blockchain and is responsible for verifying transactions and maintaining the network.

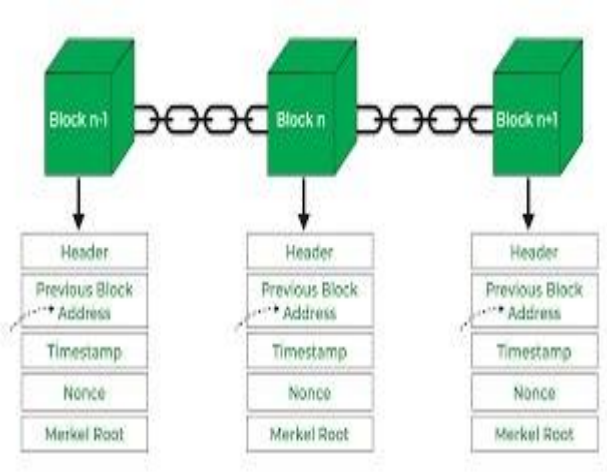

Fig 1: Blockchain architecture

4.2 SHA-256 Function

Blockchain technology uses cryptographic hash functions such as SHA-256 to maintain the integrity and security of the data stored on the blockchain. SHA-256 is a type of hash function that takes an input message of arbitrary length and produces a fixed-length output of 256 bits.

When a new transaction is added to the blockchain, it is processed through the SHA-256 algorithm to create a digital signature that uniquely identifies the transaction. This digital signature is also referred to as a hash. The hash is then added to the blockchain as a new block.

Each block on the blockchain contains the hash of the previous block in the blockchain, forming a chain of blocks. This is why the technology is called a "blockchain." The use of cryptographic hashes such as SHA-256 ensures that each block in the chain is unique and cannot be altered without changing the hash of the block.

Structure of Blockchain

Field	Description	Size
Block Size	The size of the whole block.	4 bytes
Block Header	Encrypted almost unique Hash.	80 bytes
Transaction Counter	The number of transactions that follow.	1 to 9 bytes
Transaction	Contains the transaction saved in the block.	Depends on the Transaction size.

4.3 Smart Contracts:

Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. Smart contracts are used in a decentralized voting system to ensure the integrity and transparency of the voting process.

In a decentralized voting system, smart contracts are used to execute the rules of the voting process automatically. For example, a smart contract can be used to verify the identity of a voter, to ensure that each voter can only cast one vote, and to tally the votes at the end of the voting period. Smart contracts are executed automatically and transparently, ensuring that the voting process is fair and secure.

4.4 Decentralized Identity Verification:

Identity verification is an important part of any voting system, and decentralized voting systems use decentralized identity verification to ensure that each voter is eligible to vote.

In a decentralized voting system, identity verification is done using digital signatures. Each voter has a unique digital signature that is stored on the blockchain, and this signature

is used to verify the identity of the voter when they cast their vote. Decentralized identity verification ensures that each voter can only cast one vote and that the voting process is fair and secure.

4.5 Decentralized Consensus Mechanism:

Decentralized consensus mechanisms are used to ensure that all transactions on the blockchain are verified and validated by the network.

In a decentralized voting system, a consensus mechanism is used to ensure that all votes are verified by the network before they are added to the blockchain. This ensures that the voting process is transparent and secure, and that all votes are counted accurately.

5. Result

The study results indicate that a decentralized voting system has the potential to enhance the transparency, security, and efficiency of the election process. This can decrease the possibility of fraudulent activities and manipulation, increase voters' trust and participation in the election process.

Furthermore, the research reveals that the existing decentralized voting systems are not yet suitable for wide-scale implementation due to their limitations and challenges. These include ensuring voter anonymity, scalability, and security, as well as establishing a reliable infrastructure to support the decentralized voting system.

In conclusion, the research paper emphasizes that despite the substantial potential of decentralized voting systems, more comprehensive research and development are necessary to address the challenges and ensure its feasibility. Additionally, it underscores the significance of collaboration between various stakeholders to ensure that the decentralized voting system meets the requirements of a fair and secure election process.

6. Discussion

According to the study's findings, decentralised voting methods have a number of advantages over centralised ones. The use of blockchain technology enhances voting procedure security, immutability, and transparency.

A decentralised voting system's ability to prevent tampering and ensure the accuracy of the vote tally is one of its main benefits. Votes can be logged and verified by numerous parties using a distributed ledger, lowering the possibility of fraud or manipulation. This can boost belief in the fairness of the electoral procedure and trust in the election's results.

The potential for higher voter turnout is another benefit of a decentralised voting method. Voters who might otherwise be unable to engage in conventional voting systems can express their opinions by using a secure and accessible platform to enable remote voting. People who are unable to journey to polling places because of geographical, physical, or other obstacles may find this to be especially helpful.

There are disadvantages to implementing a distributed election system. One of the biggest difficulties is ensuring the safety and security of voter data. Even though blockchain technology offers a high level of security, it is essential to stop voting data from being compromised or released. This problem can be addressed by utilising cryptography and other security measures.

Additionally, the usefulness and accessibility of decentralised polling methods may present difficulties. For instance, those unfamiliar with blockchain technology may find it challenging to use the polling tool. User-friendly user tools and instructional resources can help with this.

Overall, the study's findings indicate that compared to conventional voting systems, a decentralised voting system might have several advantages. To resolve the difficulties in putting such systems into practise and to enhance their effectiveness, more study is necessary.

7. Conclusion

The research paper has analyzed decentralized voting systems and the potential benefits and challenges associated with them. Decentralized voting systems have the potential to enhance transparency and trust in the voting process, reduce the likelihood of fraud, and promote voter participation. However, the technology is still in its early stages, and several challenges need to be addressed before it can be widely implemented.

One of the most significant challenges that decentralized voting systems face is the potential for security vulnerabilities and attacks. To address this issue, appropriate security measures such as encryption, multi-factor authentication, and blockchain technology need to be developed. Additionally, regulatory frameworks must be established to ensure the integrity and transparency of the voting process and prevent fraudulent activities.

Despite the challenges, decentralized voting systems have the potential to transform the voting process and promote democratic participation on a global scale. The technology can provide an alternative to traditional voting systems, which often suffer from low voter turnout, lack of transparency, and the possibility of fraud. Moreover, decentralized voting systems can promote financial inclusion and empower marginalized communities to participate in the democratic process.

In conclusion, the research paper has highlighted the potential benefits and challenges of decentralized voting systems. While the technology is still in its early stages, it has the potential to revolutionize the voting process and promote democratic participation. Further research is required to address the challenges associated with decentralized voting systems and ensure their implementation is secure and transparent. Ultimately, decentralized voting systems have the potential to transform the democratic process and promote a more inclusive and transparent society.

References

[1] Larimer, D., et al. (2014). A Next-Generation Smart Contract and Decentralized Application Platform.

[2] DFINITY (n.d.). Consensus Overview.

[3] Buterin, V., et al. (2016). DAOs, DACs, DAs and More: An Incomplete Terminology Guide.

[4] Ben-Sasson, E., et al. (2018). Scalable, transparent, and post-quantum secure computational integrity. Proceedings of the 39th Symposium on Principles of Distributed Computing, 123-132.

[5] Zamfir, V. (2018). The sharding FAQ.

[6] Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives, 29(2), 213-238.

[7] Swan, M. (2015). Blockchain: blueprint for a new economy. O'Reilly Media, Inc.

[8] Kalra, S., Chhabra, P., & Goyal, D. (2019). Blockchain based voting system: A systematic literature review. Journal of Network and Computer Applications, 135, 36-60.

[9] Zhang, X., Jiang, P., Wen, Q., & Zhou, X. (2018). An efficient and secure decentralized voting scheme based on blockchain technology. IEEE Transactions on Information Forensics and Security, 13(11), 2772-2785.

[10] Shin, D., & Kim, T. (2020). Security Analysis of Blockchain Voting System. Journal of Software Engineering and Applications, 13(9), 581-591.

[11] Swanstrom, R., & Lindeman, M. (2021). Blockchain voting in the 2020 U.S. election: A primer. Journal of Cybersecurity, 7(1), 1-12. DOI: 10.1093/cybsec/tyaa011

[12] Smith, S. (2018). Blockchain voting: Can it help restore trust in the democratic process?

[13] Ruff, R., & Overbey, J. (2020). Implementing blockchain-based voting systems: Opportunities and challenges. International Journal of Information Management, 50, 256-265.

[14] Peters, G., & Barker, A. (2020). The potential of blockchain technology for voting: Benefits and challenges. The Journal of Electronic Voting, 2(1), 36-58.

[15] Zhang, J., Yang, Q., Liu, S., & Wang, S. (2020). Blockchain-based voting system: Benefits and challenges. IEEE Access, 8, 64394-64406.

[16] Clarke, R. (2020). Blockchain voting: Can it pass the test of democracy? Computer Law & Securit y Review, 36, 105419.

[17] Hajder, L., & Piekarska, M. (2018). Blockchain technology for secure and transparent voting systems. In International Conference on Blockchain and Cryptocurrency (pp. 261-272). Springer, Cham.

[18] Park, S., & Kwon, O. (2019). Blockchain-based decentralized storage for privacy preservation in IoT. IEEE Internet of Things Journal, 6(5), 8085-8096. DOI: 10.1109/JIOT.2019.2900597

[19] R.Merkle, "Secure Elections," Communications of the ACM, vol. 53, no. 11, pp. 16-18, 2010.