A Comprehensive Analysis of Blockchain-Based Voting Systems: Enhancing Transparency and Security

Atik Ullah Khan
American International
University-Bangladesh
Dhaka, Bangladesh
atikullahkhan96@gmail.com

Sumaiya Sultana Tarin
American International
University-Bangladesh
Dhaka, Bangladesh
21-45745-3@student.aiub.edu

Mushfequr Rahman
American International
University-Bangladesh
Dhaka, Bangladesh
21-45721-3@student.aiub.edu

Ahsanul Azmain
American International
University-Bangladesh
Dhaka, Bangladesh
21-45709-3@student.aiub.edu

Md. Faruk Abdullah Al Sohan
American International
University-Bangladesh
Dhaka, Bangladesh
farukabdullahh@gmail.com

ABSTRACT

Blockchain innovation has developed as a promising arrangement to move forward with straightforwardness and security in voting frameworks. Its decentralized nature and cryptographic security have the potential to avoid control, extortion, and cyber-attacks. This paper provides a comprehensive analysis of blockchain-based voting systems, exploring their potential to revolutionize electoral processes. By examining existing research, case studies, and practical implementations, we highlight how blockchain can enhance the integrity, transparency, and security of voting systems. Key issues such as voter privacy, accessibility, scalability, and resistance to fraud are discussed in detail. The survey concludes with a discussion of current limitations and future directions for research and development in this field, offering valuable insights for policymakers, and technologists committed to advancing democratic processes through innovative technological solutions.

CCS CONCEPTS

• **Security and privacy** → **Information flow control**; • **Social and professional topics** → *Government technology policy*; • **General and reference** → Surveys and overviews.

KEYWORDS

Blockchain, Decentralized, Security, Transparency, Survey, Voting frameworks

ACM Reference Format:
Atik Ullah Khan, Sumaiya Sultana Tarin, Mushfequr Rahman, Ahsanul Azmain, and Md. Faruk Abdullah Al Sohan. 2024. A Comprehensive Analysis of Blockchain-Based Voting Systems: Enhancing Transparency and Security. In *September 05 – 06, 2024, AIUB, Dhaka.* Bangladesh, 8 pages.

ICCA, September 05 – 06, 2024, AIUB, DHAKA

1 INTRODUCTION

Ensuring the fairness and integrity of electoral processes is crucial in today's world [1]. The development of blockchain technology has provided opportunities to improve the transparency and security of voting systems, resolving longstanding problems associated with traditional and electronic voting procedures [2]. Longstanding problems means those have remained unresolved for a long time, often requiring new or innovative solutions due to the ineffectiveness of traditional approaches such as voter fraud, lack of transparency, tempering and hacking, limited auditability, voter correction and so many. Traditional voting methods, whether based on paper or electronics, have encountered substantial difficulties with transparency, security, and reliability, often resulting in voter scepticism and the possibility of result manipulation [3] [4]. Blockchain technology provides a potential solution to these problems by guaranteeing that each vote is recorded as a transaction on an unchangeable ledger, which can be verified by all participants. This secure and transparent system ensures that votes are accurately counted and eliminates the possibility of fraud or manipulation. Blockchain technology allows for remote voting, increasing its accessibility for all eligible voters. Overall, implementing blockchain in voting systems has the potential to revolutionize the way elections are conducted and restore trust in the democratic process. [5]. By using cryptographic methods like digital signatures, homomorphic encryption, and zero-knowledge proofs, the security and privacy of blockchain-based voting systems are significantly improved. This ensures the protection of voter anonymity and the integrity of election outcomes [6].

Moreover, the decentralized structure of blockchain renders it impervious to cyberattacks, since tampering with the system would require gaining control over a significant majority of the network nodes. This distributed network consensus makes blockchain a highly secure and reliable technology for various applications, from finance to supply chain management. Additionally, the transparency and immutability of the system provide trust and accountability, further solidifying its appeal in the digital age. [7]. Smart contract implementation automates and simplifies the voting process, removing the need for middlemen and allowing for outcomes that can be verified and audited. By utilizing blockchain technology, the smart contract ensures transparency and security, reducing the potential for fraud or manipulation in the voting process. This not only saves time and resources but also increases trust and confidence in the overall integration of the system [8].

While blockchain-based voting systems offer numerous advantages, they still encounter challenges related to scalability, voter identification, and accessibility. Hence, further research and development are necessary to fully maximize their capabilities. Moreover, issues such as ensuring transparency, security, and privacy also need to be addressed to gain widespread acceptance and trust in blockchain-based voting systems. Collaboration between experts in blockchain technology, voting systems, cybersecurity, and policymaking will be crucial in overcoming these challenges and creating a robust and reliable voting solution for the future. By continuously improving and refining blockchain voting systems, we can pave the way for a more efficient, inclusive, and trustworthy democratic process [9] [10]. The integration of biometric technology into blockchain has the potential to solve issues surrounding the verification of voters' identities, thereby guaranteeing a safe and all-encompassing electoral system [11].

The study seeks to examine the advantages and difficulties of voting systems based on blockchain technology, offering insights into their capacity to transform democratic processes via improved transparency, security, and confidence in elections.

2 LITERATURE REVIEW

Traditional voting systems have problems with being clear, secure, and reliable. In recent years, blockchain in e-voting has become more important. Blockchain helps with these issues by providing a clear and tamper-proof record that everyone can check. Additionally, blockchain's decentralized nature means we don't need middlemen like election officials, making voting more efficient and inclusive [12].

S. Al-Maaitah et al. [13] introduced the applications of Blockchain technology in e-voting systems to improve the process of voting by enhanced security, privacy, and transparency. It highlighted a decentralized, immutable ledger that ensures trustless transactions and reduces costs, providing a secure infrastructure without third-party control. It explored the potential application of Blockchain technology in electronic voting systems to improve the voting process by addressing trustlessness, confidentiality, and protection challenges. The article evaluated different blockchain-infused e-voting platforms, some in the theoretical phase and others already utilized, showing enhancements in security, confidentiality, and cost-effectiveness. In general, the article emphasized the advantages of utilizing blockchain technology in electronic voting systems to surpass the constraints of conventional voting systems and enhance the overall voting experience for stakeholders. However, it might have limitations in providing comparison of different technologies and the potential risks and challenges.

K. V. Rao et al. [14] proposed in an article titled "Secure Electronic Voting (E-voting) System Based on Blockchain on Various Platforms" a voting method that combines blockchain technology with electronic voting systems for more security, lower cost of administration, and higher voter turnout. This article presented the design of a decentralized E-voting system that can be deployed on any platform using Hyperledger Fabric while using Paillier encryption and linkable ring signatures to achieve voter anonymity and vote authenticity. To mitigate the security threat and the limitation of voters' capacity, a decentralized trust, platform-independent, and more secure E-voting mechanism has been adopted without the support of a specific platform that incorporates the smart contract execution capability on the blockchain.

Kalyani et al. [15] introduced a Digitalized Voting System that aims to enhance transparency and trust in the electoral process by leveraging blockchain technology. The proposed system addresses the shortcomings of traditional and digital voting methods, focusing on minimizing instances of mishaps and injustice through components such as polling process, hashing algorithms, contract and block creation, data accumulation, and result declaration.

"Crypto-voting," a blockchain-based e-voting system designed to enhance security, privacy, and transparency in elections. The system used dual blockchains to manage voter registration and vote counting separately, leveraging Shamir's Secret Sharing and smart contracts. there may include the complexity of implementation, scalability issues, user accessibility challenges, security concerns, regulatory hurdles, and the need to gain public trust [16].

The use of Internet of Things (IoT) devices and Blockchain technology in e-voting systems for smart cities. They emphasize the importance of ensuring secure communication and privacy for voters. Their proposal includes innovative solutions such as detecting and resolving threats caused by intruders, using Blockchain to prevent data manipulation, and implementing rank choice e-voting and crypto-biometric approaches to ensure secure and confidential voting processes [17].

Due to the limitation of the current casting, a ballot system that there are no deep security features in the existing blockchain casting ballot framework and most of them are stage subordinate, authors proposed a blockchain-based democratic framework in which the electors' protection and casting a ballot exactness set up by homomorphic encryption, linkable ring signatures, and proof of work between the citizen and blockchain.

3 EXISTING BLOCKCHAIN-BASED VOTING SYSTEM

3.1 Case Studies

3.1.1 ***West Virginia's Blockchain Voting Trial:*** West Virginia implemented a trial of a voting system based on blockchain technology for the 2018 midterm elections. This trial specifically targeted military members stationed abroad. The objective of this effort was to enhance the security and ease of access for absentee voting. The method used a mobile application, enabling authorized voters to safely submit their votes via their mobile devices. The study was deemed successful and showcased the potential of blockchain technology to augment voting procedures [18] [19].

3.1.2 ***Estonia's E-Residency Voting System:*** Estonia has been at the forefront of digital governance and has conducted trials using blockchain technology for voting via its E-Residency Voting System. The e-residency program of the nation has investigated the use of blockchain technology to create safe voting systems that guarantee transparency and the inability to be changed for non-residents who want to use Estonian services [18].

3.1.3 ***Sierra Leone's Blockchain Voting:*** In 2018, Sierra Leone made history by becoming the first nation to use blockchain technology in a presidential election. The technology was used to calculate votes in real time, offering a transparent and tamper-resistant approach to guarantee the precision of the election outcomes. This application demonstrated the practicality of using blockchain technology in a real-life, extensive election environment [18].

3.1.4 ***Swiss Municipalities' Blockchain Voting Pilots:*** Various Swiss towns, such as Zug, have implemented pilot projects to test blockchain-powered voting systems. The pilots prioritized local referendums and voting procedures, to bolster the security and trustworthiness of electronic voting systems. The findings demonstrated that blockchain has the potential to provide a dependable substitute for conventional voting methods [18] [19].

3.2 Blockchain-based voting system

The blockchain-based voting system has three significant portions. A detailed description of these portions is given below.

1. **Election Commission (EC):** The election commission monitors the whole election process and ensures it flows smoothly. After a certain amount of time has elapsed, the EC will begin an election, activate it, and close it. The EC is responsible for monitoring the voting process and publishing the results shortly after the election. The Election Commission is also responsible for establishing a voter list by holding a voter registration process before the election. This is another important job of the EC.
2. **Voter:** Voters are those eligible to vote and registered to vote in their respective local election district to exercise their right to vote. Every voter can cast their ballot for one of the candidates.
3. **Crypto Server:** To protect users' privacy, it is necessary to disable unauthorized access to the voting system. To do this, each vote must be encrypted before being uploaded to the blockchain. A tiny node server, referred to as a crypto server, is the only one used here to keep the public and private keys. It does not save any information about voting, and participants in the election cannot access it.

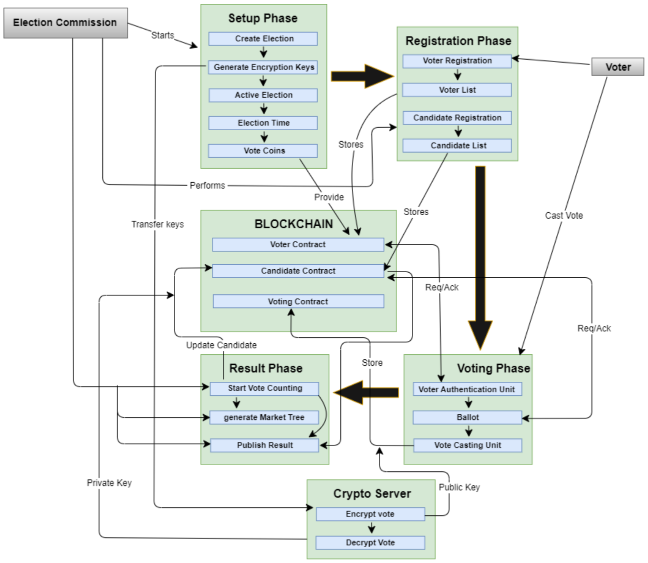


Figure 1: Blockchain-based voting system [20]

3.3 Working principles of the voting system

The working principles are discussed in this section.

1. **Setup Phase:**
   - **Create Election:**
     - The Election Commission initiates the election process.
     - Define election parameters (e.g., election name, date, time).
   - **Generate Encryption Keys:**
     - Generate a pair of cryptographic keys (public and private keys) for encrypting and decrypting votes.
     - Public keys will be used to encrypt votes, ensuring vote confidentiality.
     - Private keys will be used later to decrypt votes during the counting phase.
   - **Activate Election:**
     - Activate the election in the system, making it ready for voter and candidate registrations.
   - **Set Election Time:**
     - Define the timeline for the election, including the start and end dates and times for voting.
   - **Create Vote Coins:**
     - Generate digital tokens (vote coins) that represent voting rights.
     - These tokens will be distributed to registered voters during the voting phase.
   - **Store Initial Data:**
     - Store the election parameters, encryption keys, and vote coins on the blockchain to ensure immutability and transparency.
2. **Registration Phase:**
   - **Voter Registration:**
     - Voters register through an online portal or at designated registration centers.
     - Collect necessary information (e.g., identity verification, voter details).
     - Add registered voters to the voter list.
   - **Candidate Registration:**
     - Candidates register for the election by providing required details (e.g., personal information, political platform).
     - Verify candidate eligibility and add them to the candidate list.
   - **Store Registration Data:**
     - Store the voter list and candidate list on the blockchain to ensure that the data is tamper-proof and transparent.

(3) **Voting Phase:**
- **Voter Authentication:**
  - When a voter attempts to vote, authenticate their identity using the voter list stored on the blockchain.
  - Ensure that the voter is registered and has not yet voted.
- **Provide Ballot:**
  - Once authenticated, provide the voter with a digital ballot that includes all registered candidates.
- **Cast Vote:**
  - The voter selects their preferred candidate and casts their vote.
  - The vote is encrypted using the public key from the Crypto Server.
- **Store Vote:**
  - Store the encrypted vote on the blockchain.
  - Ensure that the blockchain records the vote immutably.

(4) **Result Phase:**
- **Start Vote Counting:**
  - At the end of the voting period, initiate the vote-counting process.
- **Decrypt Votes:**
  - Use the private key from the Crypto Server to decrypt the votes stored on the blockchain.
- **Generate Merkle Tree:**
  - Generate a Merkle tree structure from the decrypted votes.
  - The Merkle tree allows efficient verification of the integrity and authenticity of the vote count.
- **Generate Merkle Tree:**
  - Generate a Merkle tree structure from the decrypted votes.
  - The Merkle tree allows efficient verification of the integrity and authenticity of the vote count.
- **Count Votes:**
  - Count the decrypted votes and compile the results.
  - Ensure that the counting process is transparent and verifiable.
- **Publish Results:**
  - Publish the final vote counts and election results.
  - Store the results on the blockchain to ensure they are immutable and publicly verifiable.

3.4 System Transparency

Ensuring voter privacy while maintaining transparency is a critical aspect of any voting system, and blockchain-based systems are no exception. While blockchain technology offers robust mechanisms for transparency and security, the challenge lies in balancing these attributes with the need for voter privacy. Here is a more detailed discussion on how blockchain-based systems address voter privacy, supported by evidence and sources:

(1) **Cryptographic Techniques:**
- **Zero-Knowledge Proofs (ZKPs):** ZKPs allow one party to prove to another that a statement is true without revealing any information beyond the validity of the statement itself. This technique can be used in blockchain voting to verify voter identities and votes without exposing the details of the vote [21].

(2) **Homomorphic Encryption:**
- **Privacy-Preserving Computation:** Homomorphic encryption allows computations to be performed on encrypted data without decrypting it. In a voting context, this means votes can be tallied while keeping individual votes confidential [22].

(3) **Ring Signatures:**
- **Anonymous Voting:** Ring signatures enable a member of a group to sign a message on behalf of the group without revealing which member signed it. This provides voter anonymity while ensuring that only authorized voters can cast votes [23].

(4) **Mixnets:**
- **Vote Shuffling:** Mixnets shuffle and mix votes to break the link between voters and their votes, enhancing privacy. This technique ensures that even if an adversary observes the network, they cannot trace votes back to individual voters [24].

(5) **Decentralized Identifiers (DIDs):**
- **Self-Sovereign Identity:** DIDs enable users to control their digital identities without relying on a central authority. In voting systems, DIDs can be used to authenticate voters while preserving their privacy through pseudonymization [25].

4 IMPLEMENTATION CHALLENGES

(1) **Regulatory Compliance:**
- **Jurisdictional Differences:** Different countries and even regions within countries have varied electoral laws and regulations. A blockchain-based voting system must comply with these diverse legal frameworks, which can be complex and resource-intensive.
- **Data Protection Laws:** Compliance with data protection regulations like the General Data Protection Regulation (GDPR) in the European Union is critical. Blockchain's immutable nature can conflict with the right to be forgotten and other data protection rights.

(2) **Voter Authentication and Privacy:**
- **Identity Verification:** Ensuring robust and secure voter authentication while maintaining voter anonymity is challenging. Different jurisdictions have different standards for identity verification, which must be integrated into the blockchain system.
- **Privacy Concerns:** Protecting voter privacy while ensuring the transparency and immutability of the blockchain can be difficult. Legal frameworks need to balance these aspects to maintain voter trust and comply with privacy laws.

(3) **Election Integrity and Fraud Prevention:**

   - **Tamper-Resistance vs. Legal Recourse:** While blockchain technology provides tamper-resistant records, legal frameworks must be in place to handle disputes and provide recourse in case of technical failures or vulnerabilities.
   - **Auditability and Transparency:** Legal standards must ensure that blockchain-based voting systems are auditable and transparent to maintain public trust in the electoral process.

(4) **Technical Standards and Interoperability:**
   - **Standardization:** There is a need for standardized technical protocols to ensure interoperability between different blockchain systems and traditional electoral systems. Legal frameworks must support the development and adoption of such standards.
   - **Security Standards:** Establishing and enforcing robust security standards is essential to protect against cyber threats. Legal frameworks must ensure that blockchain-based voting systems adhere to these standards.

(5) **Implementation and Oversight:**
   - **Regulatory Bodies:** Establishing regulatory bodies to oversee the implementation and operation of blockchain-based voting systems is necessary. These bodies should ensure compliance with legal standards and address any arising issues.
   - **Transparency and Public Trust:** Building public trust in blockchain-based voting systems requires transparent and open processes. Legal frameworks should mandate public consultations and transparency in system development and implementation.

5 METHODOLOGY

We conducted a survey among all ages people. The survey population was approximately 115 participants. Among them, 2.6% were below 20 years old, 95.7% were in the 21-40 age group, and the remaining participants were above 60 years old. Most of the people who participated were from urban areas, primarily Dhaka city, with a few from rural areas and some from abroad. A questionnaire was created using Google Forms and distributed among the participants. The questionnaire included questions related to a Comprehensive Analysis of Blockchain-Based Voting Systems: Enhancing Transparency and Security (see Appendix for details). The responses were analyzed, and bar charts were generated to visualize the outcomes. This survey highlighted several key points from the paper on blockchain-based voting systems. The findings from our survey underscored the importance of transparency and security in voting systems, as well as the potential benefits and challenges of implementing blockchain technology in elections. By examining the responses, we aimed to understand better people's attitudes and perceptions regarding modern voting technologies and their potential to enhance electoral processes.

5.1 Cost Analysis

Implementing and maintaining a blockchain-based voting system involves significant costs that policymakers need to consider. Table 1 shows the implementation cost of a blockchain-based votiong system.

Table 1: Cost analysis for the system Implementation

Component	Description	Cost (USD)
Initial Development	Software development and integration	$60,000
Infrastructure Setup	Hardware, servers, and network setup	$30,000
Security Testing	Penetration testing and security audits	$15,000
Training and Support	Training election officials and technical support	$20,000
Operational Costs	Ongoing technical Support and system maintenance	$55,000
Total Cost		**$180,000**

6 RESULT AND DISCUSSION

In the traditional voting system, there are some major problems. These must be fixed to secure the voting system and make it transparent. Therefore, implementing electronic voting machines and online voting options with blockchain could be potential solutions to address these issues. These modern technologies can help increase accessibility, accuracy, and efficiency in the voting process. Additionally, strict security measures and protocols can prevent hacking and tampering with the results, ensuring a fair and reliable voting system for everyone. Figure 2 shows the problems in the traditional voting system. Most participants (53.9%) agree that there is a chance for tempering the votes, and around 27.8% of participants think that it is difficult to count the votes correctly. A smart and secure voting system can be the solution to these problems.

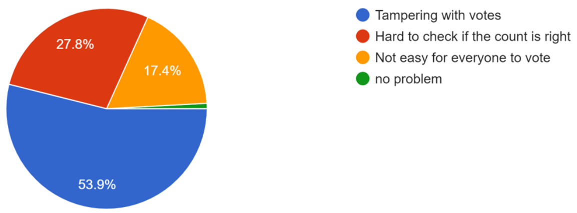


Figure 2: Problems with the traditional voting system

Figure 3 shows the familiarity of traditional voting systems among different age groups. In this survey, the number of participants above 60 is very low, and they are very familiar, whereas participants below 20 are very familiar and somewhat familiar with the traditional voting systems. It is seen that the highest number of participants are between the ages of 21-40. Among them, 62% are very familiar, 40% are somewhat familiar, and 8% are not familiar at all with the traditional voting systems.

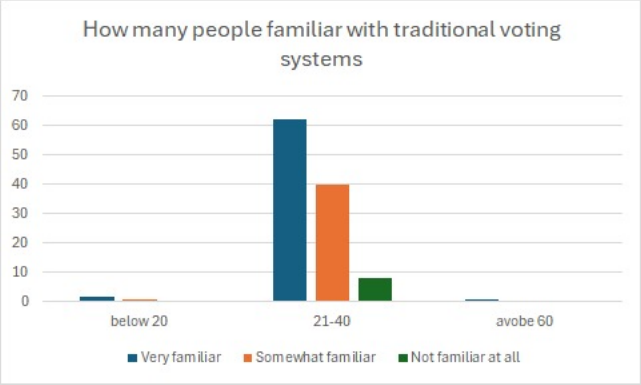


Figure 3: Familiarity with Traditional voting systems

Figure 4 shows the analysis of the survey named "Disadvantages with the Traditional Voting System". It illustrates that Doctors, Engineers, Teachers, and Sales professionals have less participation while students have higher participation. Most students think that the disadvantages of the traditional voting system are 60% voter fraud, 57% lack of transparency, and 33% inefficiency in vote counting. On the other hand, according to [13], traditional voting systems frequently come under the control and management of a centralized organization, which can raise questions about fairness and transparency. Traditional voting systems are susceptible to fraud, tampering, and manipulation. Paper ballots can be easily lost, altered, or destroyed, compromising the integrity of the election. Manual counting of paper ballots can be prone to human error, leading to inaccuracies in the final vote count.

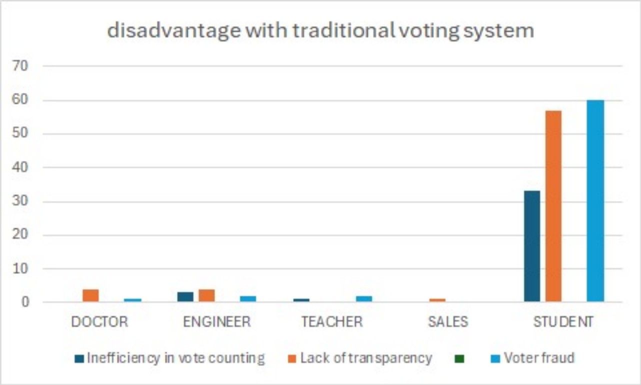


Figure 4: Disadvantages with traditional voting systems

Figure 5 shows the main challenges in blockchain-based voting systems. Participants think that the main challenges will be technical complexity, which is about 86%, 60% will be public acceptance, and 26% will be regulatory issues. According to [17], implementing a hierarchical architecture in e-voting systems can be complex but is crucial for ensuring the trustworthiness and security of IoT devices. Designing blockchain-based e-voting systems involves overcoming challenges related to algorithm evolution, software development, and lack of design guidelines. Developing efficient and user-friendly systems while ensuring security is a significant challenge [16]. Distinguishing between legitimate and malicious IoT devices to establish a secure communication environment is a substantial challenge in blockchain-based e-voting systems [17].

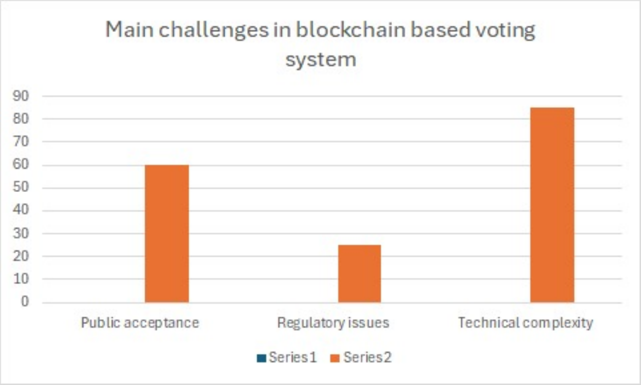


Figure 5: The challenges in Blockchain-based Voting Systems

Figure 6 shows what participants think about the security and transparency in blockchain-based e-voting systems. Around 80% of the participants believe that blockchain-based e-voting systems can improve security and transparency, and 15.7% of the participants are not sure about it. On the other hand, 4.3% of the participants think that a blockchain-based e-voting system will not improve security and transparency. According to [17], blockchain technology ensures transparency in the voting process by making all transactions visible to election bodies at every level, providing voters with notifications about the status of their votes, and boosting faith in democratic institutions. Security in blockchain-based e-voting systems involves integrating cybersecurity tools on the blockchain and cloud systems. This integration enhances the system's resilience against cyber threats, ensuring the integrity of the voting process [16].

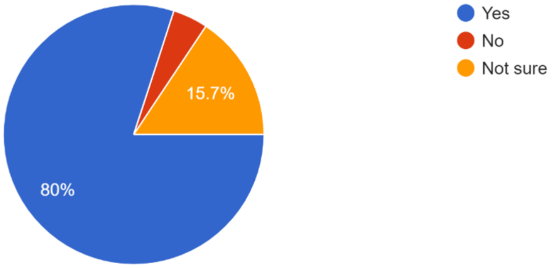


Figure 6: The Security and Transparency of Blockchain-based Voting System

Figure 7 shows what participants think about whether the blockchain-based voting system will be able to improve the issues of traditional voting systems or not. Around 70.4% of the participants believe that blockchain-based voting systems can improve the issues of traditional voting systems 9.6% of the participants think that it will not improve the issues of traditional voting systems, and 20% of the participants are not sure about it. A paper highlights that blockchain-based e-voting systems, like Crypto-voting, enable remote voting and increase accessibility for voters, including those living far from polling stations or voters abroad. This convenience improves voter turnout and engagement, addressing accessibility issues in traditional voting systems [16]. Blockchain's immutability ensures that once a transaction is committed and added to the chain, it cannot be easily altered without consensus from all nodes. This feature enhances the security of voting systems by providing a secure and unchangeable record of transactions, thereby mitigating potential fraud and manipulation [13].

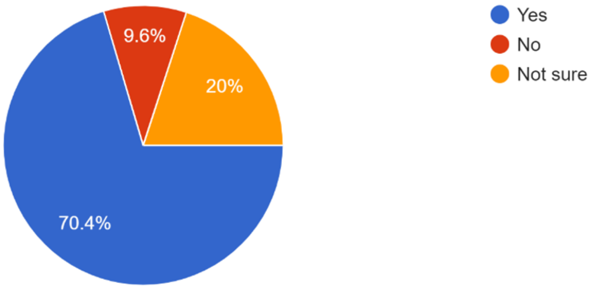


Figure 7: The improvement of traditional voting using Blockchain

7 CONCLUSION

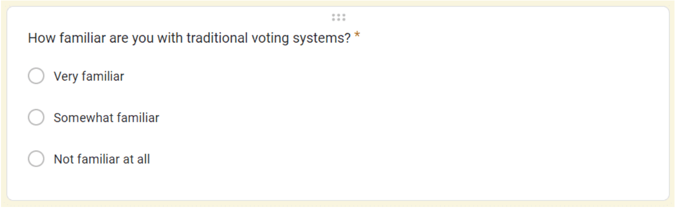
Blockchain technology has the potential for voting system transparency and security. Decentralization and cryptography may prevent control, extortion, and cyberattacks. The survey reveals that traditional voting systems face security, transparency, and efficiency issues. Most participants believe blockchain-based voting systems can improve security and transparency, but technical complexity and public acceptance remain significant challenges. Around 70.4% of participants believe blockchain can improve accessibility, accuracy, and efficiency. However, implementing blockchain requires overcoming technical, regulatory, and design challenges. Ensuring user-friendly interfaces and robust security measures is crucial for public trust and widespread adoption. Integrating blockchain technology into voting systems could be a significant step forward in advancing democratic processes through innovative and secure technological solutions.

REFERENCES

[1] Samia Yasmin, Md Faruk Abdullah Al Sohan, Md Navid Bin Anwar, Mehedi Hasan, and GM Farhad Hossain. Sfc: a lightweight blockchain model for smart food industry. In *2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, pages 699–703. IEEE, 2021.
[2] Security requirement analysis of blockchain-based e-voting systems, 2022.
[3] Voting application using blockchain technology. *International Journal For Science Technology And Engineering*, 2023.
[4] Blockchain based electronic voting system. *International journal of scientific research in science, engineering and technology*, 2023.
[5] Investigating the effectiveness of using blockchain technology for secure and transparent voting systems. *International Journal of Scientific Research in Science and Technology*, 2023.
[6] Blockchain-based electronic voting: A secure and transparent solution. *Cryptography*, 2023.
[7] Towards a systematic understanding of blockchain governance in proposal voting: A dash case study. *Social Science Research Network*, 2020.
[8] Blockchain-based e-voting protocols, 2022.
[9] Online voting system using blockchain technology. *International Journal For Science Technology And Engineering*, 2023.
[10] Development of blockchain-based e-voting system: Requirements, design and security perspective. 2022.
[11] Blockchain for electronic voting system-review and open research challenges. *Sensors*, 2021.
[12] Md Faruk Abdullah Al Sohan, Samiur Rahman Khan, Nusrat Jahan Anannya, and Md Taimur Ahad. Towards a secured smart iot using light weight blockchain: An aim to secure pharmacy products. *arXiv preprint arXiv:2206.06925*, 2022.
[13] Sarah Al-Maaitah, Mohammad Qatawneh, and Abdullah Quzmar. E-voting system based on blockchain technology: A survey. In *2021 International Conference on Information Technology (ICIT)*, pages 200–205. IEEE, 2021.
[14] K Varaprasada Rao and Sandeep Kumar Panda. Secure electronic voting (e-voting) system based on blockchain on various platforms. In *Computer Communication, Networking and IoT: Proceedings of 5th ICICC 2021, Volume 2*, pages 143–151. Springer, 2022.
[15] Mrs. K. Divya Kalyani, S.M.H. Sithi Shameem Fathima, Sowndarya Lakshmi, Hemanth Krishna, and P. Manikanta. Digitalized voting system using blockchain technology. *International Journal of Advanced Research in Science, Communication and Technology*, 2024.
[16] Francesco Fusco, Maria Ilaria Lunesu, Filippo Eros Pani, and Andrea Pinna. Crypto-voting, a blockchain based e-voting system. In *KMIS*, pages 221–225, 2018.
[17] Geetanjali Rathee, Razi Iqbal, Omer Waqar, and Ali Kashif Bashir. On the design and implementation of a blockchain enabled e-voting application within iot-oriented smart cities. *IEEE Access*, 9:34165–34176, 2021.
[18] Sarvesh Tanwar, Neelam Gupta, Prashant Kumar, and Yu-Chen Hu. Implementation of blockchain-based e-voting system. *Multimedia Tools and Applications*, 83(1):1449–1480, 2024.
[19] Akshit Kumar, Sourabh Menaria, Karan Sagar, Aaditya Choudhary, and Parveen Kumar Bajaj. A blockchain-based voting system for elections. In *International Conference on Communication and Intelligent Systems*, pages 365–379. Springer, 2023.
[20] Syada Tasmia Alvi, Mohammed Nasir Uddin, Linta Islam, and Sajib Ahamed. Dvtchain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system. *Journal of King Saud University-Computer and Information Sciences*, 34(9):6855–6871, 2022.
[21] V. Np. Zero-knowledge proofs in blockchain voting. *HackerNoon*, November 2023.
[22] Michela Iezzi. Practical privacy-preserving data science with homomorphic encryption: an overview. In *2020 IEEE International Conference on Big Data (Big Data)*, pages 3979–3988. IEEE, 2020.
[23] Yifan Wu. An e-voting system based on blockchain and ring signature. *Master. University of Birmingham*, 2017.
[24] Stefan Popoveniuc. *A framework for secure mixnet-based electronic voting*. PhD thesis, The George Washington University, 2009.
[25] Asem Othman and John Callahan. The horcrux protocol: a method for decentralized biometric-based self-sovereign identity. In *2018 international joint conference on neural networks (IJCNN)*, pages 1–7. IEEE, 2018.

A APPENDIX

The survey questionnaire is given below:

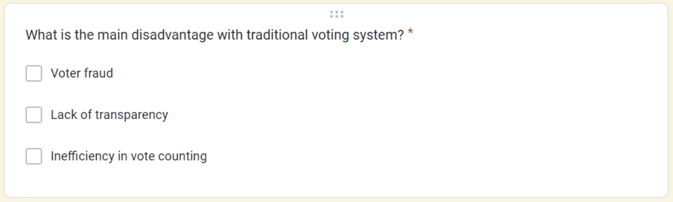


How familiar are you with traditional voting systems? *

○ Very familiar

○ Somewhat familiar

○ Not familiar at all

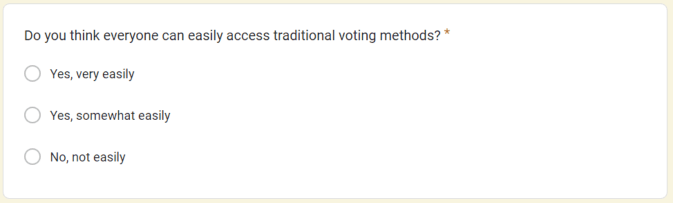


What is the main disadvantage with traditional voting system? *

□ Voter fraud

□ Lack of transparency

□ Inefficiency in vote counting

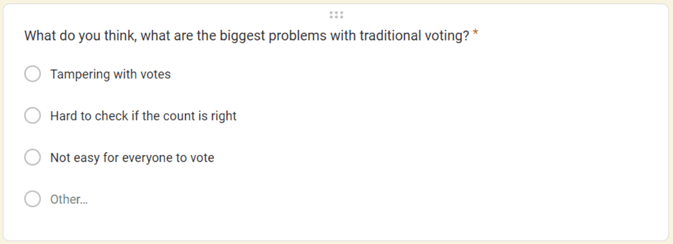


Do you think everyone can easily access traditional voting methods? *

○ Yes, very easily

○ Yes, somewhat easily

○ No, not easily



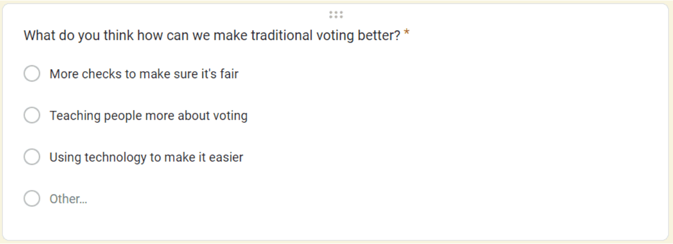
What do you think, what are the biggest problems with traditional voting? *

○ Tampering with votes

○ Hard to check if the count is right

○ Not easy for everyone to vote

○ Other...



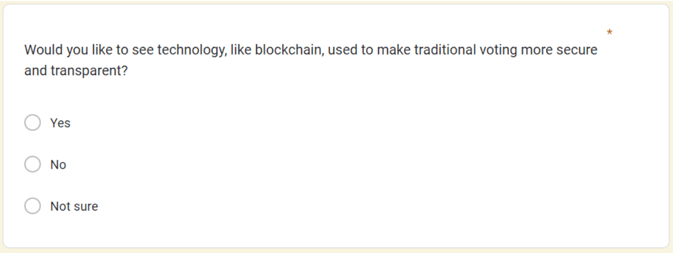
What do you think how can we make traditional voting better? *

○ More checks to make sure it's fair

○ Teaching people more about voting

○ Using technology to make it easier

○ Other...

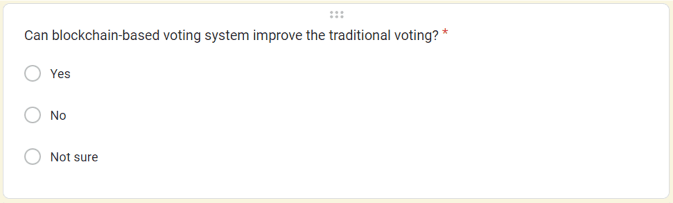


Would you like to see technology, like blockchain, used to make traditional voting more secure and transparent? *

○ Yes

○ No

○ Not sure

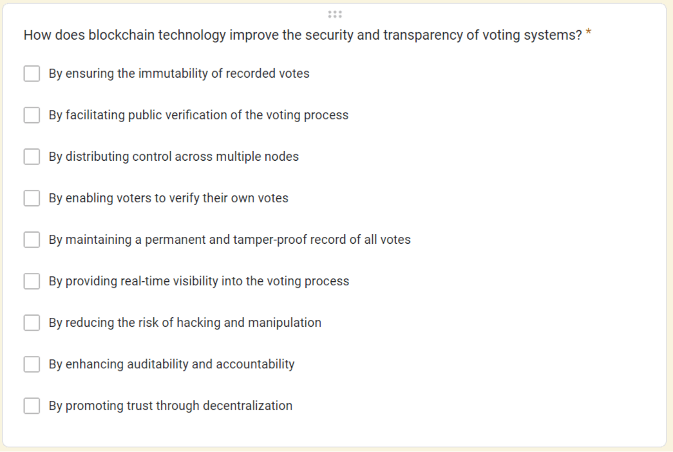


Can blockchain-based voting system improve the traditional voting? *

○ Yes

○ No

○ Not sure



How does blockchain technology improve the security and transparency of voting systems? *

□ By ensuring the immutability of recorded votes

□ By facilitating public verification of the voting process

□ By distributing control across multiple nodes

□ By enabling voters to verify their own votes

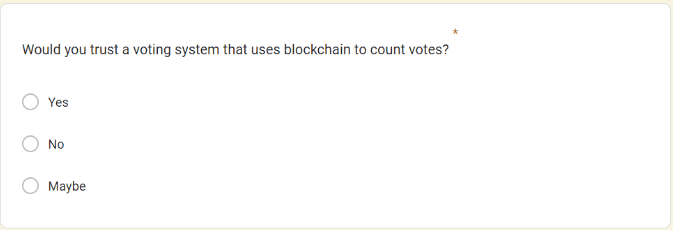
□ By maintaining a permanent and tamper-proof record of all votes

□ By providing real-time visibility into the voting process

□ By reducing the risk of hacking and manipulation

□ By enhancing auditability and accountability

□ By promoting trust through decentralization

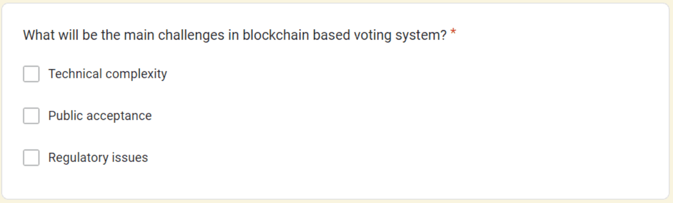


Would you trust a voting system that uses blockchain to count votes? *

○ Yes

○ No

○ Maybe



What will be the main challenges in blockchain based voting system? *

□ Technical complexity

□ Public acceptance

□ Regulatory issues