SATBAYEV UNIVERSITY

Computing & Engineering

Volume 1 (2023), Issue 1, 1-5

https://doi.org/10.51301/ce.2023.i1.01

Blockchain-based voting system: a systematic literature review

A. Omar*, Zh. Kalpeyeva

Satbayev University, Almaty, Kazakhstan

**Corresponding author: abylay.omar@gmail.com*

Abstract. Democratic elections are a cornerstone of modern society, enabling citizens to exercise their right to vote and express their preferences for political leaders and policies. However, traditional voting systems have faced numerous challenges in recent years, including allegations of fraud, hacking, and misinformation. To address these challenges, many countries have started exploring new technologies that can help secure and modernize the voting process. One such technology is blockchain, a decentralized and tamper-proof database that allows multiple parties to maintain a shared ledger without the need for a central authority. By providing a transparent and immutable record of all transactions, blockchain technology has the potential to revolutionize the way we conduct elections, making them more secure, transparent, and efficient. In this paper, we will explore the benefits and challenges of using blockchain technology in voting systems.

Keywords: *blockchain, voting, e-voting, voting system, decentralized.*

1. Introduction

Blockchain technology has emerged as a promising solution for secure and transparent voting systems. By providing a decentralized and tamper-proof database, blockchain systems can help ensure the integrity of voting processes and increase public trust in democratic institutions. In this paper, we will explore the benefits and challenges of using blockchain technology in voting systems, drawing on case studies from around the world. We will also discuss some of the criticisms and concerns that have been raised about blockchain-based voting systems, and provide recommendations for future research and implementation. The topic of using blockchain technology in voting systems is important and worth studying for several reasons:

1. Ensuring the integrity of democratic processes: Voting is a fundamental component of democratic processes, and any attempt to manipulate or influence the outcome of an election can undermine the legitimacy of the democratic system. Using blockchain technology in voting systems can help ensure the integrity of the voting process by providing a transparent, tamper-proof, and auditable record of all transactions.

2. Increasing trust in the voting process: Trust is essential for the functioning of democratic systems, and any perceived lack of trust in the voting process can undermine public confidence in the democratic system. By using blockchain technology, voting systems can provide a high degree of transparency and security, increasing trust in the voting process.

3. Improving efficiency and reducing costs: Traditional voting systems can be time-consuming and expensive to administer, requiring significant resources and infrastructure. By using blockchain technology, voting systems can be designed to be more efficient and cost-effective, reducing the burden on election officials and taxpayers.

4. Facilitating more inclusive and accessible voting: Traditional voting systems can present barriers to participation for certain groups, such as people with disabilities or those living in remote areas. By using blockchain technology, voting systems can be designed to be more inclusive and accessible, allowing more people to participate in the democratic process.

5. Advancing the development and implementation of blockchain technology: Blockchain technology is a rapidly developing area with many potential applications, and the study of blockchain-based voting systems can contribute to the advancement of this technology by identifying challenges and opportunities for further development and implementation. Overall, the study of blockchain-based voting systems is important and worth pursuing because it has the potential to improve the integrity, efficiency, accessibility, and inclusivity of democratic processes, while also contributing to the development and implementation of blockchain technology.

2. Background

Blockchain is a type of distributed ledger technology (DLT) that allows multiple parties to maintain a shared database without the need for a central authority. In a blockchain system, each block in the chain contains a cryptographic hash of the previous block, making it difficult to tamper with past transactions. This makes blockchain technology well-suited for applications where transparency, security, and immutability are important.

One of the key features of blockchain technology is decentralization, which means that no single entity controls the database. Instead, all parties in the network have a copy of the database, and any changes to the database must be approved by consensus among the parties. This makes blockchain systems resistant to tampering and hacking, as any attempt to change the data in one copy of the database will be rejected by the other copies.

Another important feature of blockchain technology is transparency. In a blockchain system, all transactions are

recorded in a public ledger that can be accessed and verified by anyone in the network. This makes it possible to trace the history of any transaction and ensure that it has not been tampered with. Additionally, some blockchain systems can be designed to allow users to verify the integrity of their own transactions, further increasing transparency and accountability.

Blockchain technology has a wide range of applications, including cryptocurrency, supply chain management, digital identity, and voting systems, among others. By providing a secure and transparent way to record and verify transactions, blockchain technology has the potential to revolutionize many industries and enable new forms of collaboration and innovation.

2.1. Evolution of voting systems

The evolution of voting systems has been a continuous process, adapting to societal changes and technological advancements. From paper-based ballots to electronic voting machines, each iteration has aimed to streamline the voting process and address inherent challenges. However, these advancements have brought about their own set of concerns, particularly related to the security and transparency of the electoral process. Instances of hacking, manipulation, and doubts surrounding the accuracy of results have underscored the need for a more robust and secure voting infrastructure.

The origins of modern voting systems can be traced back to ancient civilizations where rudimentary forms of voting, often conducted in public forums, laid the groundwork for democratic principles. However, it wasn't until the 17th and 18th centuries that structured voting methods began to emerge.

1. Voice Voting and Paper Ballots

a. Early democratic practices involved voice voting, where citizens verbally expressed their choices. This method, while simple, lacked privacy and was susceptible to external influences.

b. The introduction of paper ballots marked a significant step forward. Voters could now cast their votes in writing, providing a level of secrecy and reducing the potential for coercion. This approach became widespread during the 19th century.

2. Lever Machines and Mechanical Voting

a. The 19th and early 20th centuries witnessed the introduction of lever machines and mechanical voting systems. These innovations aimed to streamline the voting process and eliminate errors associated with manual vote counting.

b. Lever machines, for instance, allowed voters to pull levers corresponding to their chosen candidates, automatically recording and tallying the votes. While these systems expedited the counting process, they posed challenges related to maintenance and reliability.

3. Punch Card and Optical Scan Systems

a. The mid-20th century brought about the adoption of punch card voting systems. Voters would use a punch tool to indicate their choices on a card, which was then tabulated by machines. This automated counting but was prone to inaccuracies and logistical issues, as highlighted by the infamous "hanging chads" in the 2000 United States presidential election.

b. Optical scan systems, introduced later, used technology to read marked paper ballots, addressing some of the issues associated with punch cards. These systems provided a more accurate and efficient means of tabulating votes.

4. Electronic Voting Machines

a. The late 20th century saw the rise of electronic voting machines, offering a departure from paper-based systems. These machines allowed voters to cast their votes electronically, aiming to reduce errors and streamline the counting process.

b. While electronic voting machines improved efficiency, they raised concerns about security vulnerabilities and the potential for tampering. Instances of hacking and doubts about the integrity of electronic voting systems prompted a reevaluation of their use in some regions.

5. Challenges and the Need for Innovation

a. Throughout this evolutionary journey, voting systems have faced persistent challenges, including issues of accessibility, security, and transparency. The desire for more inclusive, secure, and transparent elections has driven the exploration of innovative solutions, leading to the intersection of voting systems with emerging technologies, such as blockchain.

In this context, the emergence of blockchain technology represents a potential paradigm shift in the evolution of voting systems. By leveraging the principles of decentralization, immutability, and transparency, blockchain offers a unique opportunity to address longstanding challenges and pave the way for a more robust and trustworthy electoral process. The subsequent sections of this literature review will delve into the specific ways in which blockchain has been explored and implemented to enhance the security and transparency of voting systems.

2.2. The promise of blockchain in voting systems

Blockchain technology, originally conceived as the foundational architecture for cryptocurrencies, has garnered increasing attention for its potential to revolutionize various industries, with voting systems standing out as a domain ripe for innovation. The promises of integrating blockchain into voting systems are manifold and address some of the persistent challenges that traditional voting methods face:

1. Decentralization and Security

a. One of the key promises of blockchain in voting systems is the principle of decentralization. Traditional voting systems often rely on central authorities for oversight, which can be vulnerable to manipulation or hacking. Blockchain, being inherently decentralized, distributes the record of votes across a network of nodes, making it extremely challenging for any single entity to control or compromise the system.

b. The decentralized nature of blockchain enhances the security of the voting process, providing a safeguard against unauthorized access, tampering, or fraud. Each block in the chain is linked cryptographically to the previous one, creating a chain of blocks that is resistant to alteration.

2. Immutability and Transparency

a. Immutability, a fundamental characteristic of blockchain, ensures that once a vote is recorded, it cannot be altered or deleted. This feature instills confidence in the integrity of the electoral process, as voters and election officials can trust that the recorded votes remain unchanged.

b. Transparency is another crucial aspect facilitated by blockchain. Every participant in the network has access to a transparent and immutable record of the votes cast. This transparency not only engenders trust but also allows for

independent verification of the election results, fostering a more open and accountable electoral process.

3. Elimination of Fraud and Double Voting

a. Blockchain's cryptographic principles and consensus mechanisms significantly reduce the risk of fraudulent activities. Votes are securely recorded, and the transparency of the system makes it easier to identify and eliminate fraudulent attempts.

b. The use of cryptographic keys ensures that each voter can cast only one vote, preventing the possibility of double voting. This enhances the accuracy and fairness of the electoral process, addressing a common concern in traditional voting systems.

4. Accessibility and Inclusivity

a. Blockchain-based voting systems have the potential to enhance accessibility and inclusivity in the electoral process. The technology allows for remote and online voting, enabling individuals who face physical barriers or are geographically distant to participate in elections.

b. By leveraging blockchain, voting systems can potentially reach a broader demographic, including those with mobility challenges, expatriates, and individuals residing in remote areas.

5. Trust in the Electoral Process

a. The transparency, security, and immutability offered by blockchain contribute to building trust in the electoral process. Trust is a cornerstone of any democratic system, and blockchain's features help mitigate doubts and concerns related to the accuracy and legitimacy of election outcomes.

While the promises of blockchain in voting systems are compelling, it's essential to acknowledge that implementing such a transformative technology comes with its own set of challenges and considerations. Issues like scalability, user adoption, and the need for standardized protocols must be carefully navigated to fully realize the potential of blockchain in revolutionizing the way societies conduct their elections. The subsequent sections of this literature review will delve into the existing research and insights regarding the practical implementations and challenges associated with blockchain-based voting systems.

2.3. Challenges and Criticisms

While the promise of blockchain in voting systems is enticing, the integration of this transformative technology is not without its share of challenges and criticisms. Addressing these concerns is crucial for ensuring the viability, security, and widespread adoption of blockchain-based voting systems:

- Scalability Issues

Blockchain systems, particularly public blockchains, often face scalability challenges. As the number of transactions (votes, in this context) increases, the scalability of the network becomes a critical consideration. The time taken to reach consensus and add a new block to the chain can impact the speed and efficiency of the voting process. Scalability concerns become more pronounced in large-scale elections where millions of votes must be processed within a short timeframe. Researchers and developers are actively exploring solutions, such as sharding and layer-2 protocols, to address scalability issues in blockchain-based voting systems.

- User Experience and Accessibility

Blockchain technology, with its cryptographic keys and complex structures, can be intimidating for non-technical users. Ensuring a user-friendly interface and a seamless voting experience is essential for the widespread adoption of blockchain-based voting systems. Accessibility is another concern, especially for populations with limited access to technology. Implementing blockchain in a way that does not disenfranchise individuals without access to smartphones or reliable internet connectivity is a challenge that needs to be carefully navigated.

- Privacy Concerns

While blockchain ensures the security and immutability of votes, it also raises concerns about voter privacy. The transparent nature of the technology means that all transactions are visible on the blockchain. Striking a balance between transparency and the anonymity of individual votes is a delicate task that requires robust cryptographic techniques. Researchers are actively exploring privacy-preserving technologies, such as zero-knowledge proofs, to allow voters to prove the validity of their votes without revealing the specific details of their choices.

- Centralization Risks

Paradoxically, the decentralization touted as a strength of blockchain can face challenges that lead to unintended centralization. Issues such as the concentration of mining power or the dominance of a few key players in the blockchain network can compromise the distributed nature of the technology.

In the context of voting systems, a high degree of centralization can undermine the security and integrity of the process, potentially leading to manipulation or collusion. Designing blockchain protocols that mitigate centralization risks is a critical consideration.

- Cybersecurity Threats

As with any technology, blockchain-based voting systems are susceptible to cybersecurity threats. The decentralized nature of blockchain doesn't make it immune to attacks, and novel threats may emerge as the technology evolves. Ensuring the resilience of the voting system against cyber threats, including hacking attempts and denial-of-service attacks, requires ongoing research and the implementation of robust security measures.

- Regulatory and Legal Challenges

The integration of blockchain in voting systems may face regulatory and legal challenges. The legal frameworks surrounding elections vary across jurisdictions, and introducing a novel technology like blockchain may require updates and adjustments to existing laws. Regulatory challenges also extend to issues such as the legal status of blockchain transactions, the enforceability of smart contracts, and the handling of disputes in a blockchain-based voting system.

- Public Trust and Acceptance

Trust in the electoral process is paramount, and introducing a new and unfamiliar technology can raise skepticism among the public. Building confidence in blockchain-based voting systems requires transparent communication, education, and a demonstration of the technology's reliability. Public acceptance is crucial for the success of blockchain in elections, and addressing concerns about security, privacy, and usability is key to garnering widespread support.

Navigating these challenges and criticisms requires a multidisciplinary approach, involving not only technologists but also policymakers, legal experts, and the public. The subsequent sections of this literature review will delve into

the existing research that explores potential solutions and mitigations for these challenges, providing insights into the current state of knowledge in the field of blockchain-based voting systems.

3. Case studies

A blockchain-based voting system has both advantages and disadvantages. Advantages:

1. Increased transparency: Decentralized voting systems can provide a transparent and auditable record of all transactions, making it easier to detect and prevent fraud and manipulation.

2. Improved security: Decentralized voting systems are resistant to hacking and tampering, as they rely on a consensus mechanism among multiple parties to validate and approve transactions.

3. Reduced costs: Decentralized voting systems can reduce the costs of conducting elections, as they eliminate the need for central authorities and intermediaries.

4. Increased accessibility: Decentralized voting systems can be designed to be more accessible and inclusive, allowing a broader range of participants to engage in the voting process.

5. Enhanced voter privacy: Decentralized voting systems can protect voter privacy by allowing voters to cast their vote without revealing their identity.

Disadvantages:

1. Technical challenges and complexity: Implementing decentralized voting systems can be technically challenging and requires expertise in blockchain technology and cryptography [1].

2. Limited scalability: Decentralized voting systems may have limitations in terms of scalability, as the number of transactions that can be processed at any given time may be limited by the capacity of the network [2].

3. Potential for unequal participation: Decentralized voting systems may not be accessible to all voters, particularly those who lack access to technology or have limited technical skills. And there can be several DDos attacks while voting process [3].

4. Difficulty in ensuring the accuracy of vote counting: Decentralized voting systems may face challenges in ensuring the accuracy of vote counting, as errors or discrepancies may be difficult to detect and correct.

5. Lack of legal and regulatory frameworks: Decentralized voting systems may face legal and regulatory challenges, as they may not fit within existing legal frameworks and regulations for voting systems.

6. Security: There can be a bunch of an unpredictable attacks. Ddos, TLS, MM (man in the middle) attacks [4]. The client devices can have the viruses or some other mallware software.

In recent years, two major e-voting applications have been developed, but they have also been found to have significant security risks. Following the 2015 election, the Virginia Information Technologies Agency (VITA) conducted security tests on several aspects of their e-voting system, including physical security, network security, operating system security, data security, and the vote tally process. VITA discovered that the system had used unsafe security protocols and weak passwords, and that an attacker could compromise the confidentiality and integrity of the voting data. Due to these issues, VITA recommended discontinuing the use of the Advanced Voting System [5].

In addition, the Swiss government had been working on implementing an e-voting system for many years. Swiss Post was also involved in this effort and opened its applications for safety testing to the public in 2019 [6], believing in the transparency of the applications. However, international IT experts discovered a critical error in the source code of the Swiss Post application, which could not detect voting manipulation in the shuffle method. This error allowed hackers to replace valid votes with fraudulent ones. The IT experts noted that the codes were not standardized [7]. As a result of these critical issues, the Swiss government canceled the use of the system until a new appointment [8].

Over last there are several points of view based on blockchain based voting systems. Most of them bring the idea that it is hard to develop safe e-voting system itself [9,10]. The other part says that the blockchain based architecture gives an opportunity to design safe voting system.

4. Conclusions

In conclusion, the use of blockchain-based voting systems has the potential to provide numerous benefits, such as improved transparency, security, and efficiency. However, there are also significant challenges and limitations to consider, such as the need for widespread adoption, potential technical issues, and the risk of centralization. It is clear that further research and development are necessary to overcome these challenges and ensure the successful implementation of blockchain-based voting systems. As such, it is important for policymakers and researchers to carefully evaluate the pros and cons of these systems and work towards developing robust solutions that can effectively address the needs and concerns of all stakeholders. Ultimately, the adoption of blockchain-based voting systems could pave the way for more democratic and secure electoral processes in the future.

References

[1] Taş, R. & Tanrıöver, Ö.Ö. (2020). A systematic review of challenges and opportunities of blockchain for E-voting. *Symmetry, 12(8), 1328.* https://doi.org/10.3390/sym12081328

[2] Lauer, T.W. (2004). The risk of e-voting. *Electronic Journal of e-Government, 2, 177–186*

[3] Bokslag, W. & de Vries, M. (2016). Evaluating e-voting: Theory and practice. *arXiv:160202509*

[4] Cardillo, A. & Essex, A. (2018). The Threat of SSL/TLS Stripping to Online Voting. In E-Vote-ID 2018. *Electronic Voting; 11143, 35–50.* https://doi.org/10.1007/978-3-030-00419-4_3.

[5] Manpearl, E. (2018). Securing US election systems: Designating US election systems as critical infrastructure and instituting election security reforms. *BUJ Sci. & Tech. L., 24, 168*

[6] Zetter, K. (2019). Experts Find Serious Problems with Switzerland's Online Voting System Before Public Penetration Test Even Begins. *Retrieved from*: https://www.vice.com/en/article/vbwz94/experts-find-serious-problems-with-switzerlands-online-voting-system-before-public-penetration-test-even-begins

[7] Lewis, S.J., Pereira, O. & Teague, V. (2019). The use of trapdoor commitments in bayer-groth proofs and the implications for the verifiabilty of the scytl-swisspost internet voting system. *Retrieved from*: https://cva.unifr.ch/content/ceci-n%E2%80%99est-pas-une-preuve-use-trapdoor-commitments-bayer-groth-proofs-and-implications

[8] Clarke, D. & Ali, S.T. (2017). End to end security is not enough. In Security Protocols XXV. *25th International Workshop, Cambridge, UK*. https://doi.org/10.1007/978-3-319-71075-4_29

[9] Bollinger, L.C. & McRobbie, M.A. (2018). Ensuring the Integrity of Elections. In Securing the Vote: Protecting American Democracy. *National Academies of Sciences: Washington, DC, USA*

[10] Specter, M.A., Koppel, J. & Weitzner, D. (2020). The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in us federal elections. *In Proceedings of the 29th USENIX Conference on Security Symposium*

Блокчейнге негізделген дауыс беру жүйесі: әдебиеттерге жүйелі шолу

А. Омар*, Ж. Қалпеева

Satbayev University, Алматы, Қазақстан

**Корреспонденция үшін автор: abylay.omar@gmail.com*

Аңдатпа. Демократиялық сайлау азаматтарға сайлау құқығын жүзеге асыруға және саяси көшбасшылар мен саясаттарға өз қалауларын білдіруге мүмкіндік беретін заманауи қоғамның ірге тасы болып табылады. Дегенмен, дәстүрлі дауыс беру жүйелері соңғы жылдары көптеген қиындықтарға тап болды, соның ішінде алаяқтық, бұзу және жалған ақпарат бар. Осы міндеттерді шешу үшін көптеген елдер дауыс беру процесін қауіпсіздендіруге және жаңғыртуға көмектесетін жаңа технологияларды зерттей бастады. Осындай технологиялардың бірі блокчейн болып табылады, орталықтандырылмаған және бұрмаланбайтын дерекқор, ол бірнеше тараптарға орталық органның қажеттілігінсіз ортақ кітапты жүргізуге мүмкіндік береді. Блокчейн технологиясы барлық транзакциялардың мөлдір және өзгермейтін жазбасын қамтамасыз ете отырып, сайлауды қауіпсіз, ашық және тиімді етіп өткізу тәсілін өзгертуге әлеуеті бар. Бұл мақалада біз блокчейн технологиясын дауыс беру жүйесінде қолданудың артықшылықтары мен қиындықтарын зерттейміз.

Негізгі сөздер: *блокчейн, дауыс беру, электронды дауыс беру, дауыс беру жүйесі, орталықтандырылмаған*.

Система голосования на основе блокчейна: систематический обзор литературы

А. Омар*, Ж. Қалпеева

Satbayev University, Алматы, Казахстан

**Автор для корреспонденции: abylay.omar@gmail.com*

Аннотация. Демократические выборы являются краеугольным камнем современного общества, позволяя гражданам реализовать свое право голоса и выразить свои предпочтения в отношении политических лидеров и политики. Однако в последние годы традиционные системы голосования столкнулись с многочисленными проблемами, включая обвинения в мошенничестве, хакерстве и дезинформации. Чтобы решить эти проблемы, многие страны начали изучать новые технологии, которые могут помочь защитить и модернизировать процесс голосования. Одной из таких технологий является блокчейн - децентрализованная и защищенная от взлома база данных, которая позволяет нескольким сторонам вести общую бухгалтерскую книгу без участия центрального органа. Обеспечивая прозрачную и неизменяемую запись всех транзакций, технология блокчейн способна произвести революцию в проведении выборов, сделав их более безопасными, прозрачными и эффективными. В этой статье мы рассмотрим преимущества и проблемы использования технологии блокчейн в системах голосования.

Ключевые слова: *блокчейн, голосование, электронное голосование, система голосования, децентрализованная*.

Received: 10 December 2022
Accepted: 16 March 2023
Available online: 31 March 2023