Designing an E-voting Framework Using Blockchain: A Secure and Transparent Attendance Approach

*Syarifah Bahiyah Rahayu[1, 2]
[1]*Cyber Security & Digital Rev. Ind. Centre*
[2]*Fac. of Def. Science & Tech*
National Defence Uni. of Malaysia
Kuala Lumpur, Malaysia
syarifahbahiyah@upnm.edu.my

Andrianto Arfan Wardhana
Microsoft Indonesia
Jakarta Stock Exchange Building Tower II,
Senayan, Kebayoran Baru
Jakarta Selatan, Indonesia
andrianto.wardhana@microsoft.com

Moon-Gul Lee
Dept. of Defense Science,
Korea National Defense University
Nonsan, Republic of Korea
bombslee@naver.com

Abstract— **With the increasing demand for secure, trustworthy, and transparent voting systems, electronic voting (e-voting) has emerged as a promising solution to address the shortcomings of traditional methods. However, traditional e-voting systems face numerous challenges in ensuring integrity, privacy, and auditability such as paper-based ballots and electronic voting machines. These traditional systems are susceptible to issues such as voter fraud, coercion, and a lack of transparency, undermining the democratic process. This paper proposes a novel approach to designing an e-voting framework using blockchain technology. By leveraging the distributed ledger and consensus mechanisms of blockchain, our framework aims to provide a secure, transparent, and tamper-resistant voting system. These features enable the creation of a secure and transparent voting system that ensures the integrity of votes, protects voter privacy, and enables verifiability and auditability of the entire voting process. The paper presents the key components, design considerations, and benefits of the proposed framework, along with an analysis of its potential challenges and future directions for research and development. The system architecture of the proposed framework establishes communication channels, data flows, and interfaces that facilitate voters' attendance, secure interactions and information exchange within the voting system. The use of smart contracts helps enforce the rules and conditions of the voting process on the blockchain, ensuring the accuracy and fairness of the electoral outcome. In conclusion, the proposed e-voting framework using blockchain technology has the potential to revolutionize the electoral process by providing a secure, transparent, and tamper-resistant voting system. By addressing the challenges of traditional e-voting systems and leveraging the inherent features of blockchain technology, we can enhance the integrity, privacy, and trustworthiness of the voting process.**

Keywords—e-voting, blockchain, trust, transparent, distributed ledger

I. INTRODUCTION

In the era of digital advancements, electronic voting (e-voting) systems have garnered significant attention as a means to enhance democratic processes. The imperative for a secure and transparent approach to voting has become paramount, given the challenges encountered by traditional voting methods, including voter fraud, coercion, and a lack of transparency. This paper offers an overview of the historical and contextual framework of e-voting systems, highlighting the significance of reliable and trustworthy voting systems in democratic governance.

Trustworthy voting systems play a pivotal role in maintaining the integrity and credibility of democratic elections. Traditional voting methods, while effective to a certain extent, have exhibited vulnerabilities that can compromise the sanctity of the voting process. Instances of voter fraud, tampering, and limited transparency have highlighted the need for more secure and transparent approaches to voting. E-voting systems have the potential to address these challenges by leveraging technology, encryption, and cryptographic protocols to ensure the accuracy, privacy, and verifiability of votes.

The demand for secure and tamper-resistant e-voting systems has grown in response to the shortcomings of traditional methods. By adopting advanced security measures, such as multi-factor authentication, end-to-end encryption, and robust auditing mechanisms, e-voting systems can bolster the integrity of the electoral process. Additionally, the use of blockchain technology has gained attention for its ability to provide transparency, immutability, and decentralized consensus, thereby mitigating the risk of manipulation and ensuring the trustworthiness of the voting system.

The problem revolves around the need for an e-voting framework that guarantees the integrity, privacy, and auditability of the voting process. Traditional e-voting systems have faced significant challenges in these areas, raising concerns about the accuracy and trustworthiness of election outcomes. The encountered various challenges have undermined the security, transparency, and trust in the voting process. Traditional e-voting systems have been susceptible to security breaches, including unauthorized access, hacking, and tampering of votes. This compromises the integrity of the electoral process and raises doubts about the accuracy and fairness of election outcomes.

The lack of transparency in traditional e-voting systems has been a persistent issue. Voters often have limited visibility into the voting process, making it difficult to verify the accuracy and authenticity of their votes. This lack of transparency erodes trust in the system and undermines the democratic principles of openness and accountability. Besides, traditional e-voting systems are susceptible to manipulation or tampering of votes, whether through malicious activities or vulnerabilities in the system. This poses a significant threat to the integrity of elections and undermines the democratic ideals of free and fair voting. Moreover, the centralized nature of traditional e-voting

systems places considerable power and control in the hands of a few authorities. This concentration of authority can lead to concerns about bias, manipulation, or improper influence over the voting process, further taking away trust in the system. Therefore, there is a need to design and implement an e-voting framework that addresses these concerns and ensures the integrity, privacy, and auditability of votes.

The rise of e-voting systems presents a promising solution to address the limitations and obstacles posed by conventional voting approaches. With the rapid evolution of technology, the demand for secure and transparent methodologies has grown, aimed at ensuring the integrity and impartiality of electoral processes. Thus, this paper serves to provide a comprehensive understanding of the subject matter, highlighting the relevance and necessity of dependable voting systems within democratic frameworks.

The subsequent sections will explore the design considerations, technical aspects, challenges, and future directions in the development of e-voting systems. By addressing these issues, the aim is to contribute to the advancement of secure and transparent voting systems that uphold the principles of democracy and foster public trust in the electoral process.

II. Background Work

A. Traditional E-voting Systems

Traditional e-voting systems encompass paper-based voting and electronic voting machines. In paper-based voting, voters mark their choices on physical ballots, which are then collected, manually counted, and tallied. Electronic voting machines, on the other hand, involve the use of electronic devices for casting and tabulating votes. While traditional e-voting systems have their strengths, such as familiarity and ease of use, they also suffer from significant weaknesses. These weaknesses have raised concerns about the integrity, privacy, and transparency of the voting process.

Paper-based voting systems, while widely accepted, are prone to errors during the manual counting and tabulation process. Illegible or improperly marked ballots can lead to misinterpretation or miscounting of votes. Moreover, the manual nature of paper-based systems makes them vulnerable to human errors, manipulation, and deliberate tampering. Electronic voting machines offer the advantage of efficient vote counting and quick result tabulation. However, they have been subject to concerns regarding their security and potential for tampering. Vulnerabilities in the software or hardware of electronic voting machines can lead to unauthorized access, manipulation of votes, or hacking attempts.

Some challenges associated with traditional e-voting systems are including ballot distribution and result tabulation. The distribution of paper ballots to voters presents logistical challenges. Delays or errors in ballot distribution can result in voters being unable to cast their votes, leading to disenfranchisement. Additionally, the management of absentee or remote voting poses additional challenges in traditional systems. Unfortunately, traditional systems rely on manual counting and tabulation, which can be time-consuming and prone to errors. The consolidation of results from various polling stations introduces the potential for mistakes, miscalculations, or intentional manipulation during the tabulation process.

B. Challenges in Traditional E-voting Systems

Traditional e-voting systems face specific challenges that impact their integrity, privacy, and transparency. These challenges include the potential for vote manipulation, coercion of voters, lack of auditability, limited transparency, and the reliance on centralized authorities responsible for managing the voting systems. For instance, traditional e-voting systems are susceptible to vote manipulation, either through unauthorized access to electronic voting machines or the alteration of paper-based ballots. Malicious actors can exploit vulnerabilities in the system to tamper with votes, potentially influencing the election outcomes.

Besides, traditional systems are vulnerable to coercion, where voters may be pressured or coerced into voting in a particular way. Coercion can occur in various forms, such as through intimidation, bribery, or other forms of manipulation, compromising the freedom and secrecy of the voting process. The lack of auditability in traditional e-voting systems can be challenging to trace and verify the authenticity of votes, making it difficult to detect and address any irregularities or discrepancies in the results. In addition, the lack of transparency in traditional systems raises concerns about the accuracy and fairness of the voting process. Voters may have limited visibility into the handling, counting, and tabulation of votes, undermining confidence in the system. Furthermore, traditional e-voting systems often rely on centralized authorities responsible for managing the voting process. This concentration of authority raises questions about the independence and impartiality of these authorities, potentially leading to doubts about the integrity of the electoral process. Thus, these vulnerabilities undermine trust in the voting process and compromise the democratic principles of free and fair elections.

Notable incidents and case studies have exposed vulnerabilities in traditional voting systems. This is including instances of compromised electronic voting machines, lost or mishandled paper ballots, and concerns about electoral fraud. Consequently, it has raised doubts about the effectiveness and security of traditional e-voting systems.

In the early 2000s, security researchers identified significant vulnerabilities in Diebold electronic voting machines. These vulnerabilities allowed unauthorized access and manipulation of votes, highlighting the risks associated with centralized electronic voting systems. During the 2000 U.S. presidential election, the use of paper punch-card voting systems led to controversies surrounding the "hanging chads" issue [1][2]. The imperfect removal of punched holes on the ballots resulted in difficulties in accurately determining voter intent, casting doubts on the reliability of the voting process. In 2014, researchers discovered security vulnerabilities in the e-voting system used in Estonia's parliamentary elections [3]. The vulnerabilities potentially allowed attackers to manipulate votes, demonstrating the risks associated with electronic voting systems.

These incidents underscore the importance of adopting a more secure and transparent approach to e-voting, highlighting the need for robust mechanisms, such as blockchain technology, to address the vulnerabilities and challenges faced by traditional systems.

C. Blockchain Technology

Blockchain technology is a decentralized and transparent system that enables secure and tamper-resistant record-keeping of transactions or information. It operates on the fundamental principles of decentralization, transparency, immutability, and cryptographic security. Blockchain relies on a distributed ledger, where multiple participants maintain a copy of the ledger, ensuring consensus and trust without the need for a central authority. It has been used in various fields [4].

Blockchain utilizes a distributed ledger, where each participant holds a copy of the ledger. This decentralized nature ensures that no single entity has control over the entire system, promoting transparency and reducing the risk of fraud or manipulation. While consensus algorithms enable participants in the blockchain network to agree on the validity of transactions and reach a consensus. Popular consensus algorithms include Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT).

These algorithms ensure that the majority of network participants agree on the state of the ledger, maintaining the integrity of the system. The other component, cryptographic techniques are employed to secure transactions and ensure data integrity. Public-key cryptography is used to verify the authenticity of participants and enable secure digital signatures. Hash functions are utilized to create unique identifiers (hashes) for each block, ensuring data integrity and immutability. The last component is immutability. Once data is recorded on a blockchain, it is nearly impossible to alter or delete. The combination of cryptographic hashes, decentralized consensus, and sequential linking of blocks ensures the immutability of the recorded information. This feature enhances the trustworthiness and integrity of the data stored on the blockchain.

Blockchain technology offers benefits such as transparency, immutability, enhanced security, and the potential to eliminate the need for central authorities [5]. However, limitations include scalability concerns, energy consumption in certain consensus algorithms, and the need to navigate regulatory considerations.

Thus, blockchain generally build upon combination of four main components such as distributed ledger, consensus algorithms, cryptographic techniques and immutability as shown in fig.1.

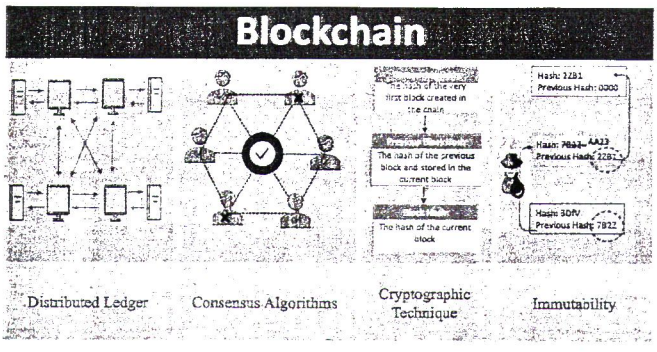

Fig. 1 Blockchain components

D. Blockchain in E-voting Systems

There has been significant research and exploration of the integration of blockchain technology in e-voting systems. Academics, researchers, and organizations have undertaken studies, projects, and pilot implementations to assess the potential benefits of blockchain in the voting process. These efforts aim to enhance the security, transparency, and trustworthiness of e-voting systems.

Academic studies have investigated the application of blockchain in e-voting, exploring its potential advantages [6]. These studies have examined the immutability of votes, the ability to verify and audit transactions, and the transparency offered by blockchain technology. Projects and pilot implementations have been carried out to assess the feasibility and effectiveness of blockchain-based e-voting systems in real-world scenarios [7].

Blockchain technology provides solutions to the challenges faced by traditional e-voting systems. The immutability of votes recorded on the blockchain ensures the integrity and tamper-resistance of the voting process. Transactions on the blockchain can be verified and audited, providing transparency and accountability in the voting system. By eliminating the need for centralized authorities, blockchain-based e-voting systems enhance trust and reduce the risk of manipulation.

Various blockchain-based e-voting models have been proposed and explored in the literature [8], [9]. These models differ in their design, consensus algorithms, and governance structures. Consensus algorithms suitable for voting systems, such as Proof of Stake (PoS) or Proof of Authority (PoA), have been investigated for their ability to provide secure and efficient validation of votes. These models and algorithms offer benefits in terms of security, privacy, and efficiency, addressing the limitations of traditional e-voting systems.

III. Designing the E-voting Framework

The proposed e-voting framework adopts a distributed and decentralized system architecture to ensure the integrity, transparency, and security of the voting process [10]. The architecture comprises various components that work collaboratively to facilitate the voting process. Such key components of the e-voting framework include voter interface, identity management, ballot generation and distribution, blockchain network, consensus mechanism, and auditing and verification. Table 1 shows the summary for each key component.

TABLE I. Key Components of E-voting Framework

Key Component	Description
Voter interface	An interface for voters to access the system and cast their votes securely. It may involve user-friendly interfaces, such as web or mobile applications, enabling voters to authenticate themselves, select their preferred candidates, and securely submit their votes
Identity management	Provide a proper identification and authentication of voters. It incorporates robust mechanisms, such as digital signatures or cryptographic protocols, to verify the identities of voters and prevent fraudulent or unauthorized access.
Ballot generation and distribution	Creating unique and tamper-proof ballots for each voter. It securely distributes these ballots to voters, ensuring their confidentiality and integrity during the distribution process.
Blockchain network	The underlying infrastructure of the e-voting framework. It consists of a distributed ledger

Key Component	Description
	where all transactions (votes) are recorded in a transparent and immutable manner. The blockchain network ensures the integrity of votes, provides transparency, and eliminates the need for centralized authorities.
Consensus mechanism	Validate and agree on the order and validity of transactions (votes). It can utilize various consensus algorithms, such as Proof of Work (PoW), Proof of Stake (PoS), or Practical Byzantine Fault Tolerance (PBFT), to achieve consensus among network participants.
Auditing and verification	Focusing on the integrity and accuracy of the voting process. It allows auditors and election organizers to independently verify the votes recorded on the blockchain, ensuring transparency and accountability.

The e-voting framework involves several communication channels, data flows, and interfaces to facilitate the voting process. Interface allows voters to securely record their attendance, access the system, authenticate themselves, and interact with the voting interface to cast their votes. The use of blockchain technology in voter attendance offers increased accessibility. This will allow voters to participate from anywhere, eliminating the need for physical presence at polling stations. This accessibility is particularly beneficial for individuals who may face geographical, logistical, or mobility challenges that would otherwise hinder their ability to participate in traditional face-to-face voting. Voters can securely access the system and mark their attendance using their unique cryptographic identity, eliminating the need for time-bound or location-specific voting. The decentralized and immutable nature of the blockchain makes it highly resistant to tampering or manipulation. Each attendance record is securely recorded on the blockchain, providing a transparent and auditable trail that can be independently verified, thus bolstering the credibility and trustworthiness of the attendance data. The use of blockchain technology instills trust and transparency in the attendance process. As each attendance record is recorded on the blockchain and visible to all network participants, it ensures transparency and accountability. This transparency builds confidence among voters, as they can independently verify the accuracy and integrity of the attendance data. By leveraging the unique features of blockchain, attendance systems can enhance the inclusivity, integrity, and transparency of the electoral process, ultimately strengthening democratic participation and confidence in the system.

Besides, integrated system with ease-to-use interface should be established between various components of the system, such as the voter interface, identity management component, blockchain network, and auditing/verification module. These interfaces allow seamless interaction and data exchange among the components to ensure the smooth operation of the e-voting framework

The e-voting framework must provide secure communication channels, such as encrypted connections or secure protocols, are established between the voter interface, identity management component, and blockchain network to ensure the confidentiality and integrity of data transmission. The data flows from the voter interface to the identity management component for authentication, then to the ballot generation and distribution component for ballot issuance. When the votes are cast, they are recorded on the blockchain network, creating a transparent and immutable transaction record.

The integration of blockchain technology into the e-voting framework involves utilizing blockchain as the underlying infrastructure to ensure the integrity, transparency, and security of the voting process. The votes cast by voters are recorded as transactions on the blockchain. Each vote is treated as a transaction, containing relevant information such as the voter's identity, candidate selection, and timestamp. This transaction recording ensures an immutable and transparent record of all votes. The use of decentralized consensus may achieve agreement on the validity and order of transactions (votes) among network participants. The selection of a suitable consensus mechanism, such as Proof of Work (PoW), Proof of Stake (PoS), or Practical Byzantine Fault Tolerance (PBFT), is crucial to ensure the security, scalability, and efficiency of the e-voting system. The chosen consensus mechanism should align with the specific requirements of the e-voting system, considering factors such as the number of participants, trust assumptions, throughput requirements, and the desired level of decentralization. Blockchain provides inherent security through cryptographic techniques. Votes recorded on the blockchain are encrypted and digitally signed to ensure the confidentiality and integrity of the data. This encryption safeguards the privacy of voters and protects against unauthorized access or tampering.

Embedding smart contract will add-value to the e-voting framework. Smart contracts, which are self-executing and tamper-proof pieces of code, can be implemented within the blockchain to enforce the rules and conditions of the voting process. Smart contracts define the logic and behaviour of the e-voting system, ensuring that votes are cast and counted according to predefined rules. Thus, smart contracts can facilitate voter verification, prevent double voting, enforce voting eligibility criteria, and manage the overall workflow of the voting process. They provide transparency and automation, reducing the reliance on centralized authorities and increasing the trustworthiness of the e-voting system. By implementing smart contracts on the blockchain, the e-voting framework ensures the execution of voting rules without the need for intermediaries, enhancing the efficiency, transparency, and auditability of the voting process.

The integration of blockchain technology into the e-voting framework through transaction recording, decentralized consensus, data encryption, and the use of smart contracts establishes a secure, transparent, and trustworthy voting system. It ensures the immutability and integrity of votes, allows for efficient consensus among participants, and enforces the rules of the voting process in a transparent and automated manner. Fig.2 shows the overview of the proposed e-voting framework.

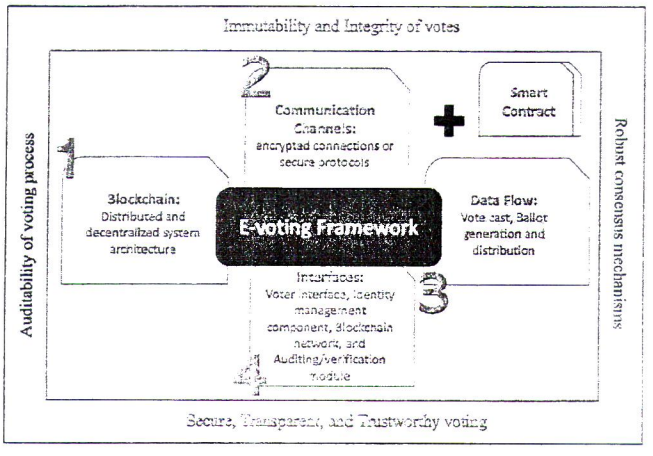

Fig. 2 Overview of e-voting framework

The proposed e-voting framework must align with a robust system architecture that leverages blockchain technology at its backend. Thus, it will set the foundation for an exceptionally secure and transparent approach to the electoral process. This alignment is essential as it establish the synergy between the e-voting components and the inherent features of blockchain, to provide the integrity and credibility of the entire electoral process.

In this architecture, blockchain technology play the role of the underlying framework that underpins the entire e-voting ecosystem. It serves as the immutable and tamper-proof ledger that securely records each stage of the electoral process - from voter registration and ballot creation to vote casting and result tabulation as well as post-election audit and accountability. Through its distributed and consensus-driven nature, blockchain establishes an unbreakable chain of trust that assures the accuracy of recorded transactions and the transparency of the system's operations.

By embedding blockchain technology at the system's backend, the architecture not only ensures data security through cryptographic encryption but also guarantees the verifiability of each vote cast. The decentralized nature of blockchain mitigates risks associated with single points of failure or manipulation, promoting trust in the process among stakeholders. This innovative alignment empowers the proposed e-voting framework to rise above the limitations of traditional methods, promising a democratic electoral process that is characterized by its security, transparency, and unwavering commitment to the fundamental principles of integrity and fairness.

Integration of the e-voting system's component with blockchain technology will enhance system architecture in terms of secure and transparent approach as shown in Table 2 above.

TABLE II. SYSTEM ARCHITECTURE ALIGNMENT WITH BLOCKCHAIN

System Architecture Feature	Blockchain Technology	Description
Voter Registration and Identity Verification	Verify using digital identity verification mechanisms.	The verification establishes a secure connection between the voter and their cryptographic identity on the blockchain.
Ballot Creation and Distribution	Encrypted ballots are stored on the blockchain and made accessible to authenticated voter.	blockchain's immutability ensures the tamper-proof creation and distribution of ballots. Once created, ballots are encrypted and assigned unique identifiers
Casting Votes and Smart Contracts	Integration of smart contracts, which execute predefined rules and condition.	Voters access their encrypted ballots through a secure interface. Upon selection, their votes are encrypted and recorded as transactions on the blockchain.
Consensus Mechanism and Verification	Applying consensus algorithm to validate each vote, ensuring agreement across the network on the correctness of transactions.	Verification process enhances security by preventing fraudulent or tampered votes from being incorporated into the final tally.
Privacy and Anonymity	Use of cryptographic techniques to safeguard voter privacy and anonymity.	Pseudonymous identities and encrypted transactions maintain the confidentiality of voters while still enabling the verification and auditability of the voting process.
Result Tabulation and Transparency	Facilitates transparent result tabulation by examining the blockchain's transparent ledger	Once the voting period concludes, stakeholders can independently verify the outcome.
Immutable Recordkeeping	Maintaining a tamper-proof record of the entire voting process, where each transaction is permanently recorded.	To ensures a transparent trail of the electoral journey.
Trust in Decentralization	Decentralization to contribute trust and transparency.	Place trust in the network's consensus mechanism and cryptography, ensuring a more reliable and accountable system.
Post-Election Audit and Accountability	Provide post-election audits.	Verify the recorded transactions in terms on accuracy and integrity of the results.

IV. CONCLUSION

As a conclusion, several key findings have emerged regarding the design and implementation of an e-voting framework using blockchain technology. Traditional e-voting systems face challenges such as potential vote manipulation, coercion, lack of auditability, limited transparency, and reliance on centralized authorities. These challenges undermine the integrity and trustworthiness of the voting process.

Blockchain technology offers potential solutions to the challenges faced by traditional e-voting systems. By leveraging its decentralized nature, immutability, transparency, and cryptographic security, blockchain can enhance the integrity, transparency, and security of the voting

process. The integration of blockchain technology in e-voting systems provides benefits such as tamper-resistant recordkeeping, increased transparency, improved auditability, and enhanced voter privacy and anonymity. Blockchain-based e-voting frameworks can address the challenges of traditional systems by providing secure and transparent recordkeeping, robust consensus mechanisms, voter authentication, and auditability of the voting process.

Further research should be conducted to address scalability challenges associated with blockchain-based e-voting systems. Scalability solutions, such as layer-two protocols, should be explored to accommodate a large number of transactions and participants without compromising the efficiency and security of the system.

ACKNOWLEDGMENT

The author would like to thank National Defense University of Malaysia for financially supporting the conference paper under self-fund grant SF0111 – UPNM/2020/SF/ICT/1

REFERENCES

[1] L. Read, "The Past, Present, and Future of American Election Security: A Survey," 2022.

[2] B. Grofman, "Prospects for Democratic Breakdown in the United States: Bringing the States Back In," *Perspect. Polit.*, vol. 20, no. 3, pp. 1040–1047, 2022.

[3] P. Ehin, M. Solvak, J. Willemson, and P. Vinkel, "Internet voting in Estonia 2005–2019: Evidence from eleven elections," *Gov. Inf. Q.*, vol. 39, no. 4, p. 101718, 2022.

[4] S. Bahiyah Rahayu, L. Vasanthan, A. M. Azahari, J. Chai, and P. Malaysia Sdn Bhd, "Military Supply Chain Management And Blockchain Development," pp. 93–105, 2021.

[5] R. Taş and Ö. Ö. Tanrıöver, "A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting," *Symmetry*, vol. 12, no. 8. 2020.

[6] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtýsson, "Blockchain-based e-voting system," in *2018 IEEE 11th international conference on cloud computing (CLOUD)*, 2018, pp. 983–986.

[7] G. Rathee, R. Iqbal, O. Waqar, and A. K. Bashir, "On the design and implementation of a blockchain enabled e-voting application within iot-oriented smart cities," *IEEE Access*, vol. 9, pp. 34165–34176, 2021.

[8] S. Singh, S. Wable, and P. Kharose, "A review of e-Voting system based on blockchain technology," *Int. J. New Pract. Manag. Eng.*, vol. 10, no. 04, pp. 9–13, 2021.

[9] S. Park, M. Specter, N. Narula, and R. L. Rivest, "Going from bad to worse: from Internet voting to blockchain voting," *J. Cybersecurity*, vol. 7, no. 1, p. tyaa025, Jan. 2021.

[10] M.-V. Vladucu, Z. Dong, J. Medina, and R. Rojas-Cessa, "E-Voting Meets Blockchain: A Survey," *IEEE Access*, vol. 11, pp. 23293–23308, 2023.