Ensuring Trust and Integrity: A Revolutionary Approach to Electronic Voting Through Blockchain

Misni[a1], Bambang Jokonowo[a2], Hadi Santoso[a3]

[a] Mercu Buana University, Jl. Meruya Selatan No.1, Kembangan, Kota Jakarta Barat, 11650, Indonesia
[1]Misni.muhammad@mercubuana.ac.id, misnisuwito@gmail.com* [2]Bambang.jokonowo@mercubuana.ac.id, [3]hadi.santoso@mercubuana.ac.id
* corresponding author

ARTICLE INFO

Article history
Received 29 Jul 2023
Revised 08 Sep 2023
Accepted 12 Des 2023

Keywords
E-voting System
Blockchain
Smart Contract
Dapps
Public Key Cryptoghraphy

ABSTRACT

The voting method has recently been a subject of continuous discourse in numerous countries. Nevertheless, the utilization of electronic voting systems raises apprehensions about several security aspects, including but not limited to eligibility, anonymity, privacy, integrity, accuracy, and impartiality. This paper introduces an innovative strategy for augmenting the security and dependability of an electronic voting system by utilizing Blockchain technology. By eliminating the requirement for physical receipts, countering coercion (specifically, vote-selling), and guaranteeing universal verifiability, this approach aims to mitigate voter distrust in the government or governing body. This technology effectively upholds the principles of voter secrecy and verifiability. Election transparency is upheld through Blockchain technology, which serves as a secure repository for all voting transactions. Concurrently, individual voters' anonymity is preserved through a sophisticated procedure that integrates ring and within-blind signatures. In addition, the system has incorporated sophisticated card-based voter authentication and security procedures, which have been implemented with the assistance of the governing body and executed through the Dapp platform. This technology will provide a comprehensive solution and provide more excellent compatibility for elections conducted on a large scale.

1. Introduction

A general election is the activities undertaken by the community in the democratic framework known as democratization by voting. Election activities are also conducted in various countries all over the world. Many efforts have been made to support the practice process of the secure electoral system. Conventional electoral systems are slow because to determine an election's outcome, one must first collect ballots and then be counted by a single central authority. Their votes, whether are included or whether the ballots are damaged, they cannot be confirmed [1]. Action or behavior dirty, impose will, and coercion will harm all parties involved in elections, especially voters and the nation's future. Individuals who engage in bribery can influence voters by offering incentives for their support for specific politicians, exerting undue influence on the electoral process. Additionally, these individuals may coerce voters into casting their ballots in favor of candidates who have been directed to act in a manner that undermines the principles of voter justice.

Nevertheless, the existing electronic voting system remains suboptimal and has encountered numerous challenges, including authentication, privacy, eligibility, fairness, correctness, and data integrity concerns. Notably, one of the primary obstacles is the susceptibility to bribery or coercion. In recent years, some electronic voting systems utilizing Blockchain technology have emerged, purporting to offer enhanced electoral processes[2][3][4][5]. Hence, one of the most challenging issues is security in election systems, which can cause invalid elections if the system cannot sort it out.

Numerous electronic voting systems have utilized Blockchain technology in elections during the past few years. The presence of Blockchain technology can provide a solution to these problems by voting and[6] as a transparent public bulletin board, which is immutable. One noteworthy attribute of Blockchain technology is its ability to create a structure that tackles the issues mentioned above by offering a complete method of confirming the integrity of the data stored inside the system. The development of an electronic voting system is proposed, wherein the verification process is made accessible to ordinary voters rather than limited to specialized institutional authorities. Using Ethereum's smart contract, making the whole process more comfortable [7][8], they built their voting system using Blockchain.

The utilization of the Ethereum Blockchain facilitates the verification and preservation of non-malleability within the election system. The system also provides authentication and verification to secure the Newest Smart Cards based on Token-based authentication models [9]. Smart Card is encrypted to prevent unauthorized use and to be used for identification and authentication [3]. Furthermore, it facilitates the storage of password files, seed files for one-time passwords, biometric picture templates, and PKI certificates. Additionally, it encourages the creation of asymmetric key pairs [10].

Moreover, e-voting is also promising, with various convenient, efficient, and secure facilities to record voters' votes and votes count quickly and accurately. This can lead to interest in e-voting, which can produce many enhancement [11][12] to civic engagement in the electoral process; efforts should be made to augment community participation in voting. The topic of electronic voting has been extensively explored in the literature, focusing on both the threats mentioned above and potential benefits. However, there is a limited number of individuals who participate in the discussion of the use of modern concepts designed to improve security and streamline the implementation of electoral procedures. The primary aim of this paper is to distinguish between prior conceptions by utilizing an updated framework. Our proposed model provides a comprehensive solution and demonstrates greater adaptability for large-scale elections.

The primary contribution of the research undertaken can be delineated as follows: To commence, our objective is to create a design that optimizes the effectiveness of an election security system by utilizing Blockchain technology. This design addresses privacy, coercion-resistance, receipt-freeness, and verifiability, ensuring a robust and reliable system. The second contribution pertains to examining and assuring security qualities such as integrity, authenticity, feasibility, accuracy, fairness, individual verification, and universal verification order. These attributes are crucial in establishing the validity of the voting system. Additionally, we analyze specific overarching criteria and focus on the third contribution that must be satisfied to facilitate the development of a precise and authorized election system. Finally, the design of the e-voting system that we suggest is anticipated to serve as a foundation for enhancing comprehensiveness, effectiveness, and efficiency.

The remaining parts of this paper are divided into several subsections. Section 2, proposed methods, including a decentralized application (Dapp), A Smart contract, Ethereum, and Cryptography primitives (hash function, public-key cryptography, digital signature, and zero-knowledge-proof. Section 3, results and discussion, including a decentralized application (Dapp), implementation of a Smart Contract, Ethereum architecture for the e-voting systems, and Cryptography primitives to enhance the security of the e-voting systems, security and privacy, coercion-resistant, receipt-freeness, verifiability, end-to-end verifiability. Section 4, Conclusion and future work.

2. Methods

In order to ensure security, transparency, and integrity, the implementation of blockchain technology in electronic voting systems requires the use of a variety of different methods. Several studies have examined the use of blockchain technology in electronic voting systems, focusing on the different methods and approaches that have been investigated. This section reviews the basics of our proposed framework, including the decentralized application (Dapp), the smart contract, the Ethereum platform, and the cryptographic primitives.

2.1 A decentralized application (Dapp):

A decentralized application (Dapp) [11] is a program operating on a decentralized computer network, such as a Blockchain. The system is intentionally built to possess open-source characteristics, ensuring transparency and autonomy eliminating any form of centralized authority governing its functioning.

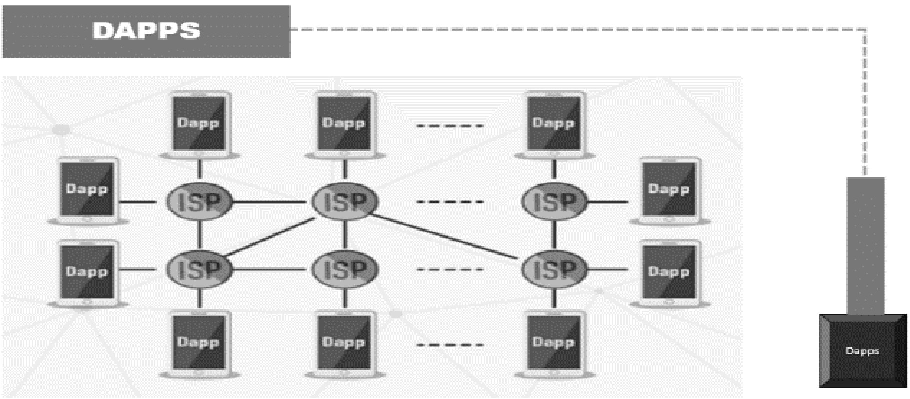

Fig. 1. Decentralized applications (Dapps)

Decentralized applications (Dapps) have a wide range of applications, encompassing financial transactions, supply chain management, and social media platforms. Dapps use blockchain technology to ensure the security, transparency, and immutability of data stored and exchanged on the network. Dapps also implement privacy-preserving techniques such as encryption and zero-knowledge proofs to protect user data. However, challenges include the use of API services, which can pose privacy risks. Proposed solutions include creating blockchain platforms that protect user privacy and provide a reliable environment for using apps and continuously improving and updating security measures to stay ahead of potential threats. Decentralized applications (Dapps) have a wide range of applications, can be shown in Figure 1.

2.2 A smart contract

A smart contract is an arrangement encoded within lines of code and can execute itself autonomously [7][8][12][13]. The contracts mentioned above are executed automatically upon the fulfillment of predetermined circumstances. Intelligent contracts are securely recorded on a Blockchain, guaranteeing their transparency, immutability, and enhanced security. Ethereum, a prominent Blockchain technology, has gained recognition for its notable facilitation of smart contracts. Smart contracts facilitate programmatic logic by executing pre-defined operations through transaction-based mechanisms. The reliability of smart contracts within blockchain networks depends on their security and functionality. Critical aspects of smart contracts include their ability to autonomously execute and enforce contractual agreements without the need for intermediaries. They eliminate the need for intermediaries and maintain the integrity of transactions within the blockchain network.

Comprehensive security analysis of smart contracts is essential to detect and address vulnerabilities that could compromise their integrity and reliability. Smart contracts are pivotal in facilitating automated and secure transactions within blockchain networks. Security analysis techniques, such as vulnerability detection and e-voting case development, are critical to ensuring the reliability and soundness of smart contracts within decentralized systems.

2.3 Ethereum

Ethereum is a decentralized blockchain network known for its open-source nature [14][15][16]. It enables the advancement and execution of intelligent contracts. The platform was initiated by Vitalik Buterin in 2013, and subsequently, the venue was formally formed in 2015. The native digital currency of the Ethereum platform is known as Ether (ETH) to facilitate transactions and provide incentives to members within the network. The Blockchain of Ethereum is a platform for developing and deploying decentralized applications (Dapps). Its function includes smart contract execution, which allows for automation and trustless interactions between parties. It hosts a wide range of decentralized applications (Dapps) that leverage the platform's smart contract capabilities to provide various services and functionalities, such as decentralized finance and governance.

Security analysis of Ethereum is crucial to protect the integrity and reliability of its smart contracts, cryptocurrency, and Dapps. Key security aspects include custom function modifiers, vulnerability detection, and low-level function replacement. Security analysis methods, such as vulnerability detection and low-level function replacement, are essential for identifying and addressing potential security vulnerabilities, ensuring Ethereum's reliability and integrity in various applications.

2.4 Cryptography primitives

Cryptography primitives[17] [18] [19] are essential foundational components in constructing secure communication and transaction systems. Within Blockchain and Ethereum, the utilization of many cryptographic primitives is prevalent as follows. Hash functions are cryptographic algorithms that are designed to be one-way functions. The operational mechanism involves the reception of an input and the subsequent generation of a hash, a fixed-size output. The Keccak-256 hash function is employed in Ethereum to safeguard data integrity and generate addresses for user accounts and smart contracts [20][21]. Public-key cryptography is a cryptographic methodology that employs a dual set of keys, consisting of a public key and a private key, to encrypt and decrypt messages. Ethereum employs elliptic curve encryption, specifically the secp256k1 curve, to produce public and private key pairs for user accounts. This cryptographic mechanism safeguards the integrity and confidentiality of transactions and smart contracts inside the Ethereum network [20][22]. Digital signatures ensure messages' genuineness and unaltered state within a decentralized system. Digital signatures in Ethereum are generated by utilizing the private key associated with an account and can then be verified by employing the public key related to that account. This mechanism guarantees the execution of transactions and smart contracts by the designated participants while preventing any unauthorized alterations [20][21]. Zero-knowledge-proofs are a type of cryptography that lets voters show that their vote was correct without giving away any information about their vote. This system makes sure that the voting process is private and anonymous [20][21].

3. Results and Discussion

The proposed electronic voting system, built upon Blockchain technology, will utilize the following decentralized application (Dapp), smart contract, Ethereum platform, and cryptographic primitives to guarantee security, reliability, and anonymity. The e-voting system will employ a decentralized application (Dapp) to streamline the voting process, guaranteeing transparency and upholding the system's integrity [20][21]. The implementation of smart contracts [20][22] will facilitate the automated execution of the voting process, thereby guaranteeing adherence to the established norms and conditions while eliminating the necessity for intermediaries. Ethereum is slated to serve as the foundational architecture for the e-voting system, offering the essential computing resources and security attributes [20][22]. Cryptography primitives will be employed to enhance the security of the e-voting system. These primitives encompass [20][21][22]. By utilizing decentralized applications (Dapps), smart contracts, the Ethereum Blockchain, and cryptographic primitives, the suggested electronic voting system has the potential to provide a more efficient and dependable alternative to conventional voting methodologies. However, additional research and development are required to effectively tackle the obstacles and limits of implementing such a system.

3.1 A decentralized application (Dapp)

The electronic voting system will utilize a decentralized application (Dapp) to optimize the voting process, ensuring transparency and maintaining the system's integrity [20]. Establishing a safe and transparent voting system can be accomplished through utilizing Blockchain technology, with a particular focus on the Ethereum platform. The operational framework of the system can be outlined as follows:

The proposed electronic voting system will be constructed upon a decentralized application (Dapp) utilizing Blockchain technology, specifically focusing on the Ethereum platform [16][23][24]. Blockchain technology is renowned for its prominent characteristics encompass anonymity, security, privacy, and reliability. The decentralized paradigm employed by the system enhances the reliability, safety, flexibility, and capacity to support real-time services. The proposed system would employ smart contracts, self-executing contractual agreements, and have their terms directly encoded into lines of code3. Smart contracts could be designed to verify registration and ascertain validity, safeguarding the integrity of the voting procedure [24]. Once implemented on the Blockchain, smart contracts exhibit resistance to tampering, hence augmenting the overall security of the system.

Voters would utilize the electronic voting system utilizing a web application, necessitating a web browser and a server4. Using a decentralized Blockchain technology would serve as a substitute for the current centralized database utilized in the voting system, effectively mitigating security concerns and facilitating the provision of instantaneous results.

3.2 Implementation of Smart Contract

Integrating smart contracts into the electronic voting system would enable the automated execution of the voting process, ensuring compliance with defined rules and conditions and removing the need for intermediaries. An illustration of DApp Platform Design E-voting based on Blockchain shown in Figure 2. In the context of the e-voting system, the operational mechanism of smart contracts can be elucidated as follows: Smart Contract are capable of completing themselves, as the agreement's contents are explicitly encoded into lines of code [20]. Within the context of the electronic voting system, the utilization of smart contracts would involve the implementation of programmed protocols to verify both the registration status and the authenticity of participants, thereby safeguarding the overall integrity of the voting procedure. The user's text needs to be longer to be rewritten academically. Once implemented on the Blockchain, smart contracts become resistant to tampering, augmenting the system's overall security. Voters would utilize the electronic voting system utilizing a web-based application, necessitating a web browser and a server [25].

Using a decentralized Blockchain technology would serve as a substitute for the current centralized database utilized in the voting system, effectively mitigating security concerns and facilitating the provision of instantaneous results. An electronic voting system would enable individuals to exercise their voting rights remotely, eliminating the need for physical presence at polling stations and enhancing accessibility. Implementing the system would effectively safeguard the confidentiality and integrity of voters' identities and ballots, fostering confidence in the electoral framework. Smart contracts can autonomously execute the voting process, obviating the necessity for intermediaries and guaranteeing adherence to the stated standards and conditions[13]. Implementing this approach would enhance the efficiency and transparency of the voting process. Utilizing Blockchain technology, particularly Ethereum, would afford a safe and transparent framework for the electronic voting system. Blockchain technology is renowned for its prominent attributes, encompassing anonymity, security, privacy, and reliability[13]. The decentralized model of this system has several advantages, including enhanced reliability, safety, flexibility, and support for real-time services[25].

3.3 Ethereum architecture for the e-voting systems

Ethereum has been designated as the fundamental framework for the electronic voting system, providing crucial computational resources and security features. The utilization of Ethereum's Blockchain technology plays a significant role in enhancing the functionality and effectiveness of the electronic voting system. The proposed electronic voting system is designed to operate on a decentralized application (Dapp) utilizing Blockchain technology, specifically focusing on Ethereum [15][16]. The selection of Ethereum's Blockchain is based on its innovative contract capabilities, rendering it well-suited for many applications, such as electronic voting. Smart contracts are capable of executing themselves, as the agreement's contents are directly encoded into lines of code. This feature guarantees the integrity of the voting process. Blockchain technology, exemplified by Ethereum, offers a decentralized framework that engenders network dependability, security, adaptability, and the capacity to facilitate instantaneous services—the number [16]. The platform provides a transparent and trustworthy environment for implementing services, such as electronic voting, ensuring security and the ability to be audited [15][16]. An e-voting system would enable individuals to exercise their voting rights remotely, eliminating the need for physical presence at polling stations and enhancing accessibility.

A decentralized Blockchain technology would be a viable alternative to the current centralized database utilized in the voting method. This transition effectively tackles security concerns while also offering the advantage of instantaneous result generation. The Blockchain technology of Ethereum can address both functional and non-functional requirements of an e-voting system. These criteria include ensuring data integrity, maintaining voter identification confidentiality, enabling transaction auditability, and providing scalability. The system can ensure the integrity of election data, maintain the confidentiality of voter identities to their selections, and handle a substantial load. The efficacy of Ethereum's Blockchain technology in the e-voting system has been assessed and analyzed, revealing its capacity to facilitate safe transactions, enable auditability, and offer a superior alternative to traditional client-server architectures[15][16]. The system's architecture conforms to essential electronic voting properties and incorporates a certain level of decentralization.

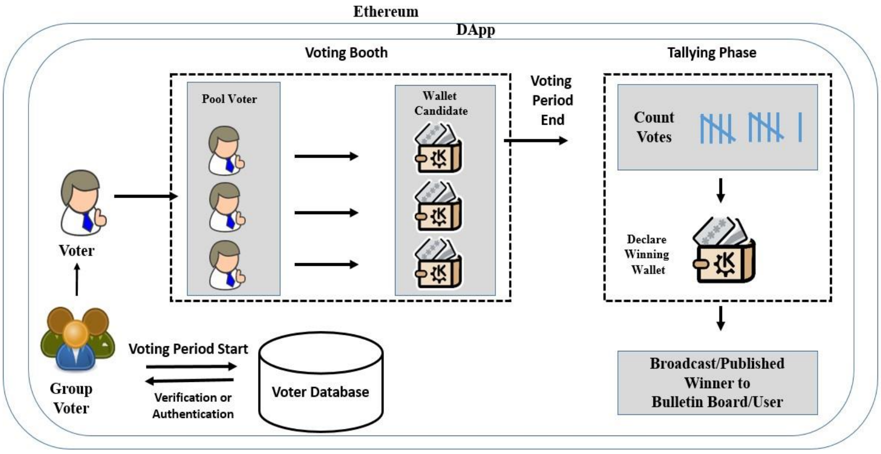

Fig. 2. An illustration of DApp Platform Design E-voting based on Blockchain.

3.4 Cryptography primitives to enhance the security of the e-voting systems

Cryptography primitives are of utmost importance in bolstering the security of the electronic voting system. These fundamental elements can encompass: Bilinear pairings are utilized in identity-based cryptography to enhance the security needs of protocols that rely on public critical infrastructure (PKI) while circumventing the need for the extensive infrastructure associated with PKI protocols. The user's text needs to be longer to be rewritten academically. Individuals are engaged in many stages of the electronic voting process, including the establishment, authentication, voting, and tallying. Their primary objective is to guarantee privacy, accuracy, and resilience. Threshold cryptography is a technique that facilitates the collaborative execution of cryptographic operations, including key generation and decryption, while ensuring the confidentiality of individual private keys [26][27].

Utilizing bilinear pairings in conjunction with it allows for fulfilling the security prerequisites of an electronic voting protocol, obviating the necessity for the comprehensive infrastructure typically associated with a public key scheme. Elliptic Curve Cryptography (ECC) is a cryptographic scheme that falls under public key cryptography [28]. It leverages the mathematical properties of elliptic curves to offer robust security while utilizing comparatively smaller key sizes. The utilization of this technology is prevalent across diverse applications, notably in electronic voting protocols, where there is a demand for robust security measures and enhanced efficiency of cryptographic primitives [29]. Digital signatures are crucial in ensuring the credibility and unaltered state of messages within the e-voting system [30]. Various cryptographic methods can serve as the foundation for these systems, including the widely utilized Elliptic Curve Digital Signature Algorithm (ECDSA), which finds application in elliptic curve cryptography [29]. By utilizing cryptographic primitives, the electronic voting system may effectively guarantee the security and integrity of the voting process. This includes safeguarding the confidentiality of voter identities and choices and establishing a dependable platform for democratic decision-making.

In addition, the e-voting system can utilize various cryptography methods to ensure the security and integrity of the voting process. Various cryptographic methodologies can be utilized for secure communication and data protection. Public-key cryptography is a cryptographic technique that facilitates the secure exchange of information between a voter and a system while ensuring both secrecy and integrity. Public-key cryptography is a cryptographic technique that utilizes a pair of keys, consisting of a public key and a private key, to enable the encryption and decryption of messages. In cryptographic systems, the public key is employed to encrypt messages, while the private key is utilized for decryption. This technology guarantees that the intended recipient may only access the message and remain unaltered during transmission. Hash functions are utilized to create a unique identifier for each vote, ensuring the anonymity of votes and facilitating the verification process. Hash functions are cryptographic techniques designed to function as one-way functions, implying that it is computationally impractical to reverse their output. The functions above are designed to accept input of varying sizes and produce a consistent output of a predetermined size, commonly referred to as a hash value or digest. The resulting output is distinct and exclusive to the given input, and even a minor alteration in the input results in an entirely dissimilar output. This methodology guarantees the uniqueness of each vote and prevents any possibility of tracing it back to the individual voter.

Digital signatures are a cryptographic technique that can be utilized to authenticate the voter's identity and ensure the voting process's integrity. Digital signatures employ a fusion of public-key cryptography and hash functions to guarantee the integrity of the message during transmission and verify the sender's authenticity. Signing a message is performed by the sender with their private key, while the recipient employs the sender's public key to authenticate the signature. Zero-knowledge proofs refer to a cryptographic methodology that allows voters to validate the correctness of their vote while preserving the confidentiality of their individual voting choices [31][32]. Zero-knowledge proofs enable one entity to demonstrate to another entity their knowledge of a particular piece of information while preserving the confidentiality of the information itself [33][34]. This methodology can guarantee the precise tabulation of votes while maintaining the confidentiality of the voter's selection.

Using cryptographic methods, the electronic voting system can effectively safeguard the security and integrity of the voting procedure. This includes preserving the confidentiality of voter identities and choices and establishing a reliable platform for democratic decision-making.

3.5 Security and privacy

To safeguard the voting process, the e-voting system must guarantee confidentiality, integrity, and availability. This includes the safeguarding of voters' privacy, the prevention of vote tampering, and the establishment of robust defenses against any threats to the system [35][36].

In order to guarantee the integrity of the e-voting system and protect the voting procedure, it is imperative to enact the following measures:

1. Confidentiality: To maintain the confidentiality of voter identities and selections during the communication process between the voter and the system, it is recommended that the e-voting system incorporates encryption techniques, specifically public-key cryptography. Implementing this measure effectively mitigates the risk of illegal access to confidential data and upholds the privacy of individuals participating in the electoral process.
2. Integrity: To ensure the integrity of the votes, the system must employ cryptographic primitives, like hash functions and digital signatures. Hash functions can produce a distinct identifier for every vote, facilitating the verification process. Additionally, digital signatures can be employed to authenticate the voter's identity and ensure the vote's integrity. These measures are designed to guarantee the integrity of the votes by preventing any unauthorized tampering or alteration while also providing mechanisms for detecting such attempts.
3. Availability: The e-voting system should be designed to accommodate a substantial volume of users and any network interruptions, thereby guaranteeing the system's availability during the voting duration. This objective can be attained by employing a resilient and expandable infrastructure, such as the Ethereum Blockchain, which can manage substantial transaction quantities and furnish a dependable framework for electronic voting.
4. Threat defenses: The system should include solid defensive measures to counter various threats, including but not limited to Distributed Denial of Service (DDoS) attacks, malware infiltration, and insider attacks. This objective can be achieved by conducting routine security

audits, adhering to secure coding techniques, and deploying suitable access restrictions and monitoring tools to identify and address any security breaches.

By implementing these security measures, the electronic voting system may effectively ensure confidentiality, integrity, and availability during the voting process. This guarantees the protection of voters' privacy, prevents unauthorized tampering with votes, and maintains the system's resilience against potential security threats. Consequently, this can establish a credible and dependable framework for democratic deliberation.

3.6 Coercion-resistance

The concept of coercion-resistance pertains to the ability of a voting system to effectively safeguard against the manipulation or undue influence of voters, thereby ensuring that they are neither compelled nor coerced to cast their votes in a predetermined manner [37] [38] . Put differently, the electoral system must refrain from disclosing any data of a compelled voter's selection, which may be exploited to authenticate the coerced vote. The preservation of privacy and freedom of voters necessitates the presence of coercion-resistance measures.

1. Coercion-resistance in remote E-voting systems: The concept of coercion-resistance within remote electronic voting systems. Remote electronic voting (E-voting) systems have been identified as having inherent security vulnerabilities, such as susceptibility to coercion and the potential for vote-selling[38][39]. A comprehensive examination has been undertaken to evaluate the efficacy of current remote electronic voting systems in terms of their capacity to uphold coercion, vote-selling, and voter-coercion resistance. Efficient coercion resistance can be achieved by utilizing mechanisms such as blind signature-based voting procedures and anonymous credentials, as proposed in existing literature.
2. Coercion resistance in a mobile-based internet voting application: The proposed mobile-based internet voting application architecture integrates deep learning-based face identification to enhance coercion resistance. The application incorporates multi-factor authentication, blockchain technology, and asymmetric encryption standards to guarantee the necessary security attributes within a voting system, all while delivering a seamless voting experience to the voter[40].
3. Challenges and practical aspects of coercion-resistant remote voting systems: The challenges and practical considerations associated with developing and implementing coercion-resistant remote voting systems. The concept of coercion-resistance holds significant complexity within cryptographic voting methods, particularly when considering remote and internet-based elections. Preserving the confidentiality and autonomy of the voter's decision, unaffected by any potential negative influence, is paramount. The concept of coercion-resistance exhibits a significant correlation with the practice of vote-buying, necessitating the implementation of supplementary measures for efficient execution[41][42].

3.7 Receipt-freeness

Receipt-freeness is a fundamental attribute that guarantees the inability of a voter to generate a verifiable record that substantiates their voting choices. The significance of this attribute lies in its ability to deter the practice of vote-buying when a voter can exchange their vote for monetary gain by producing a receipt as evidence of voting in a specific manner. In a system that does not provide receipts, the ballot cast by a voter and the accompanying receipt should be indistinguishable, hence rendering it infeasible for the voter to substantiate their vote without disclosing the contents of their ballot[39][43].

1. Importance of receipt-freeness in electronic voting systems: The significance of ensuring receipt-freeness in electronic voting systems: Receipt-freeness is a fundamental security prerequisite that guarantees that a voter is not provided with any form of receipt that would allow them to substantiate their voting choice to external parties. The preservation of this attribute is crucial in ensuring the confidentiality of electoral processes and safeguarding voters' privacy, even in cases where voters may threaten their privacy. The achievement of

receipt-freeness poses a significant challenge in cryptographic voting protocols, particularly in remote and internet-based elections.

2. The interplay among receipt-freeness, vote-privacy, and coercion-resistance: Receipt-freeness, vote-privacy, and coercion-resistance are three discrete yet interconnected security attributes inside electronic voting systems. The concept of coercion-resistance entails the notion of receipt-freeness, which in turn involves the preservation of vote-privacy. To clarify, if a system exhibits resistance to coercion, it concurrently possesses the attribute of being devoid of receipts. Furthermore, if a system is receipt-free, it guarantees the preservation of vote privacy. The features mentioned above are articulated through observational equivalence, which plays a vital role in safeguarding the integrity and privacy of the voting process[44].
3. Challenges in achieving receipt-freeness: The attainment of receipt-freeness in electronic voting systems presents a formidable challenge, particularly when considering the need to maintain a balance with other essential security attributes, such as verifiability. Specific electronic voting systems already in use partially meet the necessary criteria, prompting ongoing research efforts to design protocols that both provide receipt-freeness and verifiability while upholding security measures[45].

3.8 Verifiability

The concept of verifiability pertains to the inherent feature that enables individuals to ascertain the accuracy and validity of election outcomes independently. Verifiability encompasses two distinct forms: individual verifiability, which grants each voter the ability to confirm the inclusion of their vote in the ultimate total, and universal verifiability, which extends the opportunity for anyone to authenticate the accuracy of the final tally. The importance of verifiability cannot be overstated in upholding the transparency and integrity of the voting process[46][47].

1. Verifiability in electronic voting systems: Verifiability in electronic voting systems pertains to the capacity of voters, election officials, and the general public to autonomously ascertain the accuracy of the election procedure and the precision of its outcomes. The property of verifiability is paramount in upholding the integrity and reliability of the voting system[48].
2. Verifiability in generative search engines: Verifiability is essential for generative search engines, characterized by their ability to produce results for user queries immediately. In the present context, verifiability refers to the requirement for systems to provide comprehensive and precise citations. This entails achieving high citation recall, where all claims are fully supported, and high citation precision, where each citation supports its associated statement. Nevertheless, it is worth noting that current generative search engines frequently exhibit unsupported assertions and imprecise references, giving rise to apprehensions over their reliability and credibility[49].
3. The enhancement of verifiability in AI-based systems: AI-based systems can enhance the verifiability of information, as exemplified by its application in increasing the verifiability of Wikipedia through the utilization of AI. Within this context, a verification engine, characterized as a neural network, can effectively forecast how much a document substantiates a given claim. This process can aid in identifying prospective instances of failed verifications and contribute to enhancing reference quality for existing claims [50].

1. Verifiability in other domains: Verifiability is a concept that extends beyond its application in a specific domain. It is pertinent to consider the verifiability of other domains, including the Data-Driven Variational Multiscale Reduced Order Model [51] and the verifiability of a safe and efficient cloud-centri Internet-of-Medical-Things-enabled smart healthcare system [52]. Verifiability plays a crucial role in these particular circumstances by ensuring the accuracy and integrity of systems and safeguarding the associated data's privacy.

3.9 End-to-end Verifiability

End-to-end refers to a system or process encompassing all stages or components necessary for its completion or functionality. The e-voting system must exhibit its capacity to attain end-to-end verifiability, enabling voters and other entities to check the accuracy of the voting procedure. The aspiration for universal adoption is a vital feature of any e-voting system [53]. End-to-end verifiability is a critical feature of the e-voting system, enabling voters and other entities to check the accuracy of the voting procedure.

1. Scantegrity II is a practical improvement for optical scan voting systems that enhances the integrity of elections by employing confirmation codes printed on ballots using invisible ink36. In the electoral process, individuals exercise their voting rights by marking ballots, similar to the usual optical scan method. However, a distinct writing instrument, known as a specialized pen, facilitates the development of invisible ink. The verifiability of election integrity encompasses an end-to-end process that enables voters to verify the accurate inclusion of their votes while maintaining the confidentiality of their voting choices. Additionally, it allows any individual to verify that the total is accurately computed based on the votes that have been included.
2. Provotum is an end-to-end verifiable remote electronic voting system that operates on blockchain technology [54][55]. It utilizes a public permissioned blockchain as a bulletin board where all Blockchain data can be verified by the general public, with the authorization granted to only those entities capable of signing blocks. A novel remote electronic voting system is proposed by Pronotum, which operates on a fully decentralized Blockchain. This system utilizes a permissioned Blockchain as a public bulletin board, enabling the explicit delegation of trust among various permissioned Blockchain nodes.
3. Secure End-to-End Verifiable Internet-Voting System: This system allows voters to move about and discreetly place their ballots on public computers, thereby enabling the advantage of early voting. The primary objective of the proposed system is to provide universal support for the election process by utilizing biometric and voter identification characteristics. The system furnishes a digital witness to each voter, allowing them to verify the accuracy of their recorded vote and allowing the general public to examine the proper tally of all recorded ballots.

By implementing end-to-end verifiability in the e-voting system, voters and other entities can check the accuracy of the voting procedure, ensuring transparency and trust in the electoral process.

4. Conclusion

In conclusion, the evidence mentioned above supports the proposed hypothesis. This paper examines the E-voting system and investigates the transformative capacity of Blockchain technology in altering electoral procedures. The research has yielded significant findings and proposed novel approaches to improve the E-voting system.

The primary findings of this inquiry can be summarized as follows: Blockchain technology offers a resilient foundation for enhancing the security of electronic voting systems while fostering trust among stakeholders. The immutability, transparency, and utilization of cryptographic primitives contribute to its significant resilience against tampering and fraudulent activities, enhancing the voting process's credibility and reliability. Transparency and accountability are inherent features of Blockchain technology, as it operates decentralized, allowing for the verification of every transaction and vote by all relevant stakeholders. The abovementioned measure fosters transparency and accountability, mitigating apprehensions regarding potential manipulation and guaranteeing an equitable electoral process. The suggested enhancements aim to utilize Blockchain technology to establish an E-voting system that is more inclusive and accessible. This system would cater to a broader spectrum of voters, including individuals with disabilities or geographical constraints. The protection of voter privacy has been prioritized by implementing sophisticated cryptographic methods. These techniques safeguard sensitive information, guarantee confidentiality, and uphold the system's integrity. Utilizing Blockchain technology in electronic voting systems enhances the efficiency of the election process by streamlining operations, resulting in cost reduction and eliminating intermediaries such as central authorities and auditors.

As we progress, there exist various suggestions for prospective research and advancement in this field: Additional research should prioritize enhancing user experience to optimize E-voting systems' usability, hence fostering increased acceptance and usage. Scalability is a crucial aspect to consider in Blockchain-based E-voting systems, particularly concerning accommodating a more significant number of voters and elections. Therefore, it is recommended that future research endeavors focus on investigating potential scalability solutions for such systems. Establishing well-defined regulatory frameworks for Blockchain-based E-voting should be a collaborative effort between governments and international organizations. These frameworks aim to resolve legal and jurisdictional concerns associated with this emerging technology. Education and Awareness: It is imperative to implement awareness campaigns and educational programs to disseminate information to the general public and electoral authorities regarding the advantages and potential limitations of Blockchain-based E-voting systems.

The findings of our study indicate that implementing Blockchain technology is a viable avenue for substantial enhancements to the E-voting system. These improvements mainly bolstered the system's security, transparency, and accessibility. The implementation of these enhancements is not only viable but imperative for the advancement of contemporary democratic systems. Our vision entails a future in which Blockchain technology is utilized for E-voting, serving as a fundamental component of electoral procedures. This implementation aims to guarantee equitable, effective, and reliable elections for every member of society.

References

[1] D. L. Chaum, “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms,” *Commun. ACM*, vol. 24, no. 2, pp. 84–90, 1981, doi: 10.1145/358549.358563.

[2] U. M. Qabs and F. M. Al-Naima, “Design and implementation of a smart card simulator,” in *2008 International Conference on Computer and Communication Engineering*, 2008, pp. 217–220.

[3] S. C. Alliance, “Card Payments Roadmap in the United States: How Will EMV Impact the Future Payments Infrastructure?,” *White Pap. Febr.*, 2011.

[4] F. Hao, P. Y. A. Ryan, and P. Zieliński, “Anonymous voting by two-round public discussion,” *IET Inf. Secur.*, vol. 4, no. 2, pp. 62–67, 2010, doi: 10.1049/iet-ifs.2008.0127.

[5] M. Kadam, P. Jha, and S. Jaiswal, “Double spending prevention in bitcoins network,” *Int. J. Comput. Eng. Appl.*, vol. 9, no. VIII, 2015.

[6] M. Rockwell, “Bitcongress–Process for block voting and law,” *Retrieved December*, 2017.

[7] L. Rura, B. Issac, and M. K. Haldar, “z,” *Int. J. Electron. Gov. Res.*, vol. 12, no. 3, pp. 71–93, 2016.

[8] Z. Zhao and T.-H. H. Chan, “How to vote privately using bitcoin,” in *Information and Communications Security: 17th International Conference, ICICS 2015, Beijing, China, December 9–11, 2015, Revised Selected Papers 17*, 2016, pp. 82–96.

[9] K. Lee, J. I. James, T. G. Ejeta, and H. J. Kim, “Electronic voting service using block-chain,” *J. Digit. Forensics, Secur. Law*, vol. 11, no. 2, p. 8, 2016.

[10] M. Gasson, M. Meints, and K. Warwick, “D3. 2: A study on PKI and biometrics,” *FIDIS Deliv.*, vol. 2, 2005.

[11] H. Garg, M. Singh, V. Sharma, and M. Agarwal, “Decentralized Application (DAPP) to enable E-voting system using Blockchain Technology,” in *2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA)*, 2022, pp. 1–6.

[12] A. M. Al-Madani, A. T. Gaikwad, V. Mahale, and Z. A. T. Ahmed, “Decentralized E-voting system based on Smart Contract by using Blockchain Technology,” in *2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC)*, 2020, pp. 176–180.

[13] J. Díaz-Santiso and P. Fraga-Lamas, “E-Voting System Using Hyperledger Fabric Blockchain and Smart Contracts,” *Eng. Proc.*, vol. 7, no. 1, p. 11, 2021.

[14] V. Buterin, “Ethereum white paper,” *GitHub Repos.*, vol. 1, pp. 22–23, 2013.

[15] A. Wicaksana, “Towards secure and auditable e-voting system with go ethereum,” *Turkish J. Comput. Math. Educ.*, vol. 12, no. 10, pp. 3006–3012, 2021.

[16] A. Bhawiyuga, A. Basuki, and N. W. Tiera, “An Ethereum Based Distributed Application for Ensuring the Integrity of Stored E-Voting Data,” in *Proceedings of the 6th International Conference on Sustainable Information Engineering and Technology*, 2021, pp. 235–239.

[17] G. Gallegos-Garcia, R. Gómez-Cárdenas, and G. I. Duchén-Sánchez, “Identity-based threshold cryptography for electronic voting,” 2009.

[18] G. Gallegos-García, R. Gómez-Cárdenas, and G. I. Duchén-Sánchez, “Identity based threshold cryptography and blind signatures for electronic voting,” *WSEAS Trans. Comput.*, vol. 9, no. 1, pp. 62–71, 2010.

[19] E. Blanchard and T. Selker, "Origami voting: A non-cryptographic approach to transparent ballot verification," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 12063 LNCS, pp. 273–290, 2020, doi: 10.1007/978-3-030-54455-3_20.

[20] K. Mehboob Khan, J. Arshad, and M. M. Khan, "Secure Digital Voting System based on Blockchain Technology."

[21] K. Isirova, A. Kiian, M. Rodinko, and A. Kuznetsov, "Decentralized electronic voting system based on blockchain technology developing principals.," in *CMIS*, 2020, pp. 211–223.

[22] H. D. Park, "A decentralized e-voting system based on blockchain network," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, 2019.

[23] A. Priyadharshini, M. Prasad, R. Joshua Samuel Raj, and S. Geetha, "An Authenticated E-Voting System Using Biometrics and Blockchain," in *Intelligence in Big Data Technologies—Beyond the Hype: Proceedings of ICBDCC 2019*, 2021, pp. 535–542.

[24] D. Rangelov, B. S. K. Subudhi, P. Lämmel, M. Boerger, N. Tcholtchev, and J. Khan, "Design and Specification of a Blockchain-based P2P Energy Trading Platform," in *2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 2021, pp. 636–643.

[25] M. Saim, M. Mamoon, I. Shah, and A. Samad, "E-Voting via Upgradable Smart Contracts on Blockchain," in *2022 International Conference on Futuristic Technologies (INCOFT)*, 2022, pp. 1–6.

[26] L. T. A. N. Brandão, N. Mouha, and A. Vassilev, "Draft NISTIR 8214 Threshold Schemes for Cryptographic Primitives Challenges and Opportunities in Standardization and," vol. 8214, 2019.

[27] M. Davidson, "NIST Roadmap Toward Criteria for Threshold Schemes for Cryptographic Primitives NIST Roadmap Toward Criteria for Threshold Schemes for Cryptographic Primitives."

[28] W. J. Caelli, E. P. Dawson, and S. A. Rea, "PKI , Elliptic Curve Cryptography , and Digital Signatures '," vol. 18, pp. 47–66, 1999.

[29] C. A. Lara-nino, A. Diaz-perez, and M. Morales-sandoval, "Elliptic Curve Lightweight Cryptography : A Survey," *IEEE Access*, vol. 6, pp. 72514–72550, 2018, doi: 10.1109/ACCESS.2018.2881444.

[30] G. Kaim *et al.*, "Post-quantum Online Voting Scheme To cite this version : HAL Id : hal-03355875 Post-Quantum Online Voting Scheme," 2021.

[31] U. Feige, A. Fiat, and A. Shamir, "Zero Knowledge Proofs of Identity 2 . Interactive proofs of knowledge," pp. 210–217, 1987, doi: 10.1145/28395.28419.

[32] O. Goldreich and Y. Oren, "Definitions and Properties of Zero-Knowledge Proof Systems *," pp. 1–32, 1994.

[33] T. A. Silde, *Doctoral thesis Tjerand Aga Silde Privacy-Preserving Cryptography from Zero-Knowledge Proofs*. 2022.

[34] P. Ioannis and P. Chaidos, "Zero Knowledge Protocols and Applications," 2017.

[35] N. R. Pradhan, A. P. Singh, N. Kumar, M. M. Hassan, and D. S. Roy, "A flexible permission ascription (FPA)-based blockchain framework for peer-to-peer energy trading with performance evaluation," *IEEE Trans. Ind. Informatics*, vol. 18, no. 4, pp. 2465–2475, 2021.

[36] S. Baloglu, S. Bursuc, S. Mauw, and J. Pang, "Election verifiability revisited: Automated security proofs and attacks on Helios and Belenios," in *2021 IEEE 34th Computer Security Foundations Symposium (CSF)*, 2021, pp. 1–15.

[37] A. Juels, D. Catalano, and M. Jakobsson, "Coercion-resistant electronic elections," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6000 LNCS, pp. 37–63, 2010, doi: 10.1007/978-3-642-12980-3_2.

[38] P. resistance in a practical secret voting scheme for large scale elections Grontas, A. Pagourtzis, and A. Zacharakis, "Coercion resistance in a practical secret voting scheme for large scale elections," in *2017 14th International Symposium on Pervasive Systems, Algorithms and Networks & 2017 11th International Conference on Frontier of Computer Science and Technology & 2017 Third International Symposium of Creative Computing (ISPAN-FCST-ISCC)*, 2017, pp. 514–519.

[39] Y. Ruan and X. Zou, "Receipt-freeness and coercion resistance in remote E-voting systems," *Int. J. Secur. Networks*, vol. 12, no. 2, pp. 120–133, 2017, doi: 10.1504/IJSN.2017.083836.

[40] S. Pooja, L. K. Raju, and U. Chhapekar, "Face detection using deep learning to ensure a coercion resistant blockchain-based electronic voting," *Eng. Sci.*, vol. 16, pp. 341–353, 2021.

[41] K. Krips and J. Willemson, "On practical aspects of coercion-resistant remote voting systems," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11759 LNCS, no. September, pp. 216–232, 2019, doi: 10.1007/978-3-030-30625-0_14.

[42] C. Kempka, "Matters of coercion-resistance in cryptographic voting schemes." Karlsruhe, Karlsruher Institut für Technologie (KIT), Diss., 2014, 2014.

[43] K. Braunlich and R. Grimm, "Formalization of receipt-freeness in the context of electronic voting," in

2011 Sixth International Conference on Availability, Reliability and Security, 2011, pp. 119–126.

[44] S. Delaune and S. Kremer, “Formalising security properties in electronic voting protocols,” *Deliv. AVOTE*, vol. 1, p. 151, 2010.

[45] H. N. Oo and A. M. Aung, “Design and formal analysis of electronic voting protocol using AVISPA,” in *2017 2nd International Conference for Convergence in Technology (I2CT)*, 2017, pp. 1–8.

[46] N. Chondros *et al.*, “Distributed, end-to-end verifiable, and privacy-preserving internet voting systems,” *Comput. Secur.*, vol. 83, no. August, pp. 268–299, 2019, doi: 10.1016/j.cose.2019.03.001.

[47] I. Brightwell, J. Cucurull, D. Galindo, and S. Guasch, “An overview of the iVote 2015 voting system.”

[48] F. Waismann and F. Waismann, “Verifiability,” *How I see Philos.*, pp. 39–66, 1968.

[49] N. F. Liu, T. Zhang, and P. Liang, “Evaluating verifiability in generative search engines,” *arXiv Prepr. arXiv2304.09848*, 2023.

[50] F. Petroni *et al.*, “Improving wikipedia verifiability with ai,” *Nat. Mach. Intell.*, vol. 5, no. 10, pp. 1142–1148, 2023.

[51] B. Koc, C. Mou, H. Liu, Z. Wang, G. Rozza, and T. Iliescu, “Verifiability of the data-driven variational multiscale reduced order model,” *J. Sci. Comput.*, vol. 93, no. 2, p. 54, 2022.

[52] M. Kumar and S. Chand, “A secure and efficient cloud-centric internet-of-medical-things-enabled smart healthcare system with public verifiability,” *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10650–10659, 2020.

[53] J. Viana *et al.*, “Deep Attention Recognition for Attack Identification in 5G UAV scenarios: Novel Architecture and End-to-End Evaluation,” *IEEE Trans. Veh. Technol.*, pp. 1–17, 2023, doi: 10.1109/TVT.2023.3302814.

[54] C. Killer *et al.*, “Provotum: A blockchain-based and end-to-end verifiable remote electronic voting system,” in *2020 IEEE 45th Conference on Local Computer Networks (LCN)*, 2020, pp. 172–183.

[55] C. Killer, M. Eck, B. Rodrigues, J. von der Assen, R. Staubli, and B. Stiller, “ProvotuMN: Decentralized, Mix-Net-based, and Receipt-free Voting System,” in *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2022, pp. 1–9.