ORIGINAL RESEARCH
published: 16 June 2022
doi: 10.3389/fbloc.2022.927013

Paillier Cryptosystem Based ChainNode for Secure Electronic Voting

Buhari Ugbede Umar, Olayemi Mikail Olaniyi*, Daniel Oluwaseun Olajide and Eustace Manayi Dogo*

Department of Computer Engineering, Federal University of Technology, Minna, Nigeria

Blockchain is a distributed and decentralized ledger of transactions that are linked together cryptographically leading to immutability and tamper-resistance, thereby ensuring the integrity of data. Due to the ability of blockchain to guarantee the integrity of data, it has found wide-range adoption in electronic voting (e-voting) systems in recent years, this is in a bid to prevent manipulation of votes. However, due to the distributed nature of the blockchain, opportunities arise for privacy intrusion of the data being secured. The translation of this privacy flaw in blockchain to e-voting systems is the possibility of violation of the privacy of the electorates. Consequently, in a bid to achieve integrity and privacy of votes in e-voting, this study presents the use of an open-source blockchain system, coupled with a privacy-oriented cryptosystem known as the Paillier cryptosystem, towards addressing the privacy concerns of the blockchain. The performance of the system was evaluated and a transaction throughput of 1424 tps was obtained for ten thousand simulated ballot transactions. Further evaluation was carried out on the system, by increasing the number of system transactions. This showed that the mining time of the blockchain increased by an average factor of 0.18 s for every thousand increases in the number of transactions. Also, the response time of the system to a range of user actions was evaluated over an increasing number of voters. Results obtained showed that the response time of the system for vote casting operations increased by an average of 0.33 min per thousand voters while for vote tallying there was an increase in response time by an average of 0.848 min per thousand voters. The scientific value of this study is the development of an integrity and privacy-preserving e-voting system consisting of an open-source nodechain coupled with a privacy-oriented cryptosystem known as the Paillier cryptosystem following the security requirements of e-voting systems. The proposed system addresses the issue of integrity in e-voting while still maintaining the privacy of the electorates.

Keywords: e-voting, blockchain, homomorphic encryption, proof-of-work, ballot

Edited by:
Kavita Saini,
Galgotias University, India

Reviewed by:
Manju Khari,
Jawaharlal Nehru University, India
Chellammal Surianarayanan,
Bharathidasan University, India

****Correspondence:***
Buhari Ugbede Umar
buhariumar@futminna.edu.ng

Specialty section:
This article was submitted to Blockchain Technologies, a section of the journal Frontiers in Blockchain

Received: *23 April 2022*
Accepted: *18 May 2022*
Published: *16 June 2022*

Citation:
Umar BU, Olaniyi OM, Olajide DO and Dogo EM (2022) Paillier Cryptosystem Based ChainNode for Secure Electronic Voting.
Front. Blockchain 5:927013.
doi: 10.3389/fbloc.2022.927013

1 INTRODUCTION

Electronic Voting (e-voting) is the adoption of electronic systems in aiding and supporting electoral processes, such as casting and counting votes (Prashantha et al., 2018). The advantages introduced into an electoral process by e-voting ranges from cost-effectiveness to efficient organization of elections (Alguliyev et al., 2019). Over the years, several e-voting systems have been proposed and developed by various researchers, while some have even been adopted by individuals, organizations, and countries. These e-voting systems are tending towards replacing existing conventional schemes of conducting elections (Risnanto et al., 2019). However, despite the merits introduced by e-voting in electoral processes, there exists a series of challenges that accompany e-voting systems. Some of these challenges include security attacks, lack of transparency, and in some cases, complexity and non-user-friendliness (Heiberg et al., 2015). In a bid to address the various challenges of e-voting systems, several studies have been carried out and several systems have been developed under the guidance of various functional and security requirements as established by Bungale and Sridhar (Bungale and Sridhar, 2016). Several technologies have been adopted by researchers in a bid to satisfy the various requirements. Cryptography is a field in mathematics and computer science, focused on the adoption of techniques for rendering data in an obfuscated manner, to allow for secure exchange between two or more parties (Barakat et al., 2018). It is one of the technologies that has been adopted in various forms, over the years in e-voting systems, towards achieving voter anonymity and privacy (Sarker et al., 2020; Sharma, 2016; Zhang et al., 2018), as well as vote auditability and verifiability (Gao et al., 2019; Bag et al., 2019; George et al., 2019; Kiayias et al., 2017).

In the field of computing, a technology being adopted for the protection of privacy is cryptography. Cryptography is the adoption of mathematical operations for the representation of information, in ways that are not readily usable and accessible by anyone which the information is not intended for (Halunen and Latvala, 2021). It has been adopted in various forms by researchers for various implementation of e-voting systems by encryption of the high-value data (votes), as can be seen in the case of (Darwish and Gendy, 2017; Almimi et al., 2019; Arnob et al., 2020a). However, at the point when votes are to be tallied and counted, these systems require that the encrypted data be decrypted for any meaningful computation to be carried out. This process is prone to security attacks and also a privacy flaw, hence the need for the adoption of a scheme, known as homomorphic encryption; which is a privacy-oriented scheme and can be integrated with the blockchain to help preserve the privacy of decentralized data through encryption, and at the same time allowing computations to be carried out on encrypted data without the need for the data to first of all undergo decryption. Also, e-voting systems require a *"next level of security"* which cryptography alone has not been able to provide. This *"next-level security"* is the integrity and immutability of data provided by blockchain technology (Christyono et al., 2021).

Blockchain is a distributed ledger of transactions, stored in blocks of data that are linked together cryptographically and are decentralized among various participants, resulting in the resistance to attack and immutability of such transactions (data) (Hanifatunnisa and Rahardjo, 2017; Abuidris et al., 2019; Zheng et al., 2017; Sugandh et al., 2021; Dayal et al., 2021; Nigam et al., 2022) by forcing trust among the various actors on the blockchain with the enablement of full transparency of transaction records (Hellani et al., 2020). Blockchain provides an improvement in the security and transparency of data records (Panwar et al., 2022). It is a technology being adopted in e-voting towards ensuring the integrity of electoral processes. Various implementations of blockchain technology in e-voting exists in literature, such as Ethereum (Yavuz et al., 2018), (Puneet et al., 2021), Hyperledger fabric (Zhou et al., 2020; Daramola, 2020), as well as open-source (Khan et al., 2018; Arnob et al., 2020b). Though these studies achieved immutability and integrity of the electoral process, they failed to consider the need to protect the privacy of electorates, as compensation for the privacy flaw of the blockchain (Wang et al., 2020).

Baskaran et al. in (Baskaran et al., 2020) established that the decentralized nature of a blockchain system provides an opportunity for identification of how transactions have taken place, which is a privacy flaw in voting. The translation of this privacy concern of the blockchain to e-voting systems is the possibility of determining how a particular electorate may have voted, which is a violation of the confidentiality and privacy requirements of e-voting systems. Therefore in the adoption of blockchain in e-voting systems, there is the need to put in place a scheme for the protection of voter privacy.

The contribution of this study is the proposition of an integrity and privacy-preserving e-voting system consisting of an open-source node chain coupled with a privacy-oriented cryptosystem known as the Paillier cryptosystem following the security requirements of e-voting systems (Bungale and Sridhar, 2016). This study takes into consideration the various techniques through which blockchain can be adopted in e-voting systems and provides insight into a suitable technique for preserving both integrity and privacy in e-voting.

The remaining section of the paper is organized as follows: **Section 2** presents a review of existing literature together with the fundamental concepts in the adoption of blockchain for electronic voting, with emphasis on the categories of blockchain implementation in e-voting systems, as well as an analysis of the various means by which privacy can be preserved on the blockchain, as well as a review of existing literature. **Section 3** gives the research method, with an illustration of the cooperation functionality of the various adopted schemes, as well as an overview of the performance metrics adopted for performance evaluation of the proposed system. **Section 4** presents the results obtained from the performance evaluation, as well as the implication of the results obtained, while **Section 5** lays the conclusion on findings from the study, stating the scientific contribution of the study, its limitation as well as recommendation for future research scope.

2 FUNDAMENTAL CONCEPTS AND LITERATURE REVIEW

This section presents fundamental concepts in the adoption of blockchain in e-voting systems.

2.1 E-Voting

E-Voting is the adoption of information and communication technology systems for supporting the casting, recording, and counting of votes in an electoral process. E-Voting systems introduce the advantages of increased voter convenience, electoral result accuracy as well as fast tabulation and counting of votes (for and Idea, 2011). For an e-voting system to be acceptable for use, it must satisfy some security and functional requirements, some of these requirements are (Liu and Wang, 2017; Bungale and Sridhar, 2016);

a. Confidentiality and Privacy: implies that the e-voting system must ensure that it is impossible to identify how or whom an electorate voted for.
b. Integrity: implies that the e-voting system must ensure that votes or any part of the electoral process are manipulated or compromised in any manner.
c. Voter Authenticity: implies that the e-voting system must adopt a mechanism for verifying the identity of an electorate.
d. Authority Distribution: implies that the regulatory power over the e-voting system should not depend on just one entity.
e. Transparency: implies that the electorates should have a general knowledge of the operation of the system and balloting procedure.

2.2 Blockchain in E-Voting

Blockchain is a distributed ledger system of transactions, stored in blocks of data that are linked together cryptographically and are decentralized among various participants, resulting in the resistance to attack and immutability of such transactions (data) (Hanifatunnisa and Rahardjo, 2017) (Abuidris et al., 2019; Zheng et al., 2017). Blockchain technology has found wide adoption in e-voting systems. The various e-voting system implementations that are based on the blockchain can be classified into three categories (Yu et al., 2018);

2.2.1 E-Voting as Smart Contracts

Smart contracts in blockchain refer to computer programs written to facilitate contractual terms, which are deployed on the blockchain for execution when certain predefined conditions and requirements are satisfied (Hu et al., 2018). Various e-voting systems have been developed as smart contracts and deployed on various blockchain platforms, as in the case of (Yavuz et al., 2018; Hjálmarsson et al., 2018; Patidar and Jain, 2019) that put forward e-voting systems as smart contracts using the Solidity language provided by the Ethereum blockchain network. Also, (Kirillov et al., 2019; Kost'al et al., 2019; Vivek and Yashank, 2020), proposed e-voting systems deployed as smart contracts using the Hyperledger blockchain framework. Though the various systems offered integrity and immutability of records, however, the adoption of smart contracts entails having to maintain a public ledger that is visible to every participant in the blockchain network and translates to a privacy issue (Nzuva, 2019). The implication of this to its adoption in e-voting systems is the possibility of compromising voter privacy. Also, there is the issue of resistance of smart contracts to the amendment of contractual terms and conditions, which does not allow for the reflection of real-life dynamics and changing conditions (Nzuva, 2019). The translation of this to the various e-voting systems that have adopted this approach, is the inability to introduce into the system, the dynamics that may occur in electoral processes.

2.2.2 E-Voting Through Cryptocurrency

Cryptocurrencies are assets based on a blockchain system, which adopt cryptography for securing the exchange and transfer of such assets, between the participants of the blockchain system (Giudici et al., 2019). E-Voting protocols have also been developed to adopt the use of cryptocurrency in electoral processes, as in the case of (Zhao and Chan, 2016; Jason and Yuichi, 2016; Bao et al., 2018) that adopted the bitcoin for developing an e-voting system protocol, as well as (Fusco et al., 2018) that adopted cryptocurrency from a permissioned blockchain system to support e-voting. These systems achieved decentralization of authority, immutability as well as public verifiability of the electoral process. However, the adoption of cryptocurrency in e-voting does not protect the privacy of electorates (Fleder et al., 2015). Also, the adoption of cryptocurrency introduces a bottleneck in the number of transactions (votes) that can be processed at a time by the system, as in the case of bitcoin, due to its slow transaction rate (Sänger, 2019).

2.2.3 E-Voting With Blockchain as Ballot-Box

In traditional voting systems, ballot-box refers to storage boxes into which ballots are cast by electorates during an electoral process. There are e-voting systems that have adopted a seemingly ballot-box approach in the adoption of blockchain for securing the electoral process. In such e-voting systems, votes (ballots) are digital messages of a predefined structure, which are sent as transactions to the blockchain (Sheer Hardwick et al., 2018). Various researchers have adopted this approach in developing blockchain-based e-voting systems as in the case of (Sheer Hardwick et al., 2018; Wang et al., 2018). This approach allows for the blockchain-based e-voting system to be developed to reflect real-life features and dynamics of e-voting systems, as well as an avenue for coupling a privacy-oriented encryption scheme with the blockchain system (Bellini et al., 2020). As such this study goes on to adopt this approach in developing an e-voting system.

2.3 Privacy Protection in Blockchain

Several schemes have been developed to address the privacy concerns of the blockchain. These schemes are classified into two main categories (Feng et al., 2019):

2.3.1 Identity Privacy Preservation Schemes

This is the category of blockchain privacy preservation schemes are aimed at the protection of addresses (identity) of senders and receivers of assets (such as cryptocurrency) exchanged on a blockchain system (Feng et al., 2019). Schemes under this approach include; Ring signature, Non-interactive Zero-Knowledge proof (NIZKP), and Mixing services. This category of schemes is not suitable for the preservation of privacy in a blockchain as a ballot-box e-voting system.

2.3.2 Transaction Privacy Preservation Schemes

This category of blockchain privacy preservation schemes aims at protecting the actual content of the transactions that take place on a blockchain system (Feng et al., 2019). Privacy preservation schemes in this category are:

a. Non-Interactive Zero-Knowledge Proof (NIZKP): is a scheme that allows for a party (prover) to prove to another party (verifier), the validity of a statement, without having to reveal any other information, through a process that does not involve interaction between the two parties (Blazy, 2012; Partala et al., 2020). NIZKP has been adopted in several blockchain-based e-voting systems (Sallal, 2019; Hjálmarsson et al., 2018). Though these systems guaranteed security, transparency as well as protection of voter privacy in e-voting, however, these approach suffers from scalability issues due to the enormous and massive computation cost requirements of generating the proofs (George and Samman, 2016; Bhardwaj, 2020).
b. Homomorphic Encryption: is a cryptographic scheme that allows certain computations to be carried out directly on ciphertext, without the need for initial decryption. The results obtained from such computations is a ciphertext which when decrypted, produces identical results as when the computations are performed on the plaintext (Zhang et al., 2020). Homomorphic encryption schemes can be classified into two categories, which are; Partially Homomorphic Encryption and Fully Homomorphic Encryption. Because the e-voting system would require only the addition of the ballots, a partially homomorphic encryption scheme is suitable for adoption in this study, due to the performance and protection it offers in place of utility functionality (Will and Ko, 2015).

2.4. Literature Review

(Jabbar and Alsaad, 2017) proposed a remote electronic voting system using the ElGamal cryptosystem for ensuring the security of votes. The system ensured the preservation of ballot privacy. However, the adopted ElGamal cryptosystem was, slow in performance during the encryption of votes. Also, (Mustafa and Waheed, 2021), developed an e-voting system using the permissioned Hyperledger Fabric (HLF) platform. The system adopted a blind signature scheme and Zero-Knowledge Proof (ZKP) to establish security, transparency, and privacy. However, the adoption of multiple identities obscuring schemes meant that the system traded performance for voter privacy. Also, an e-voting system with a universal verifiable voting vector was proposed by (Zou et al., 2017) to allow for the verification of ballots. The system ensured transparency and auditability of the entire ballot process. The system however failed to put in place modalities for the protection of voter privacy and confidentiality. (Pawlak et al., 2018) proposed a schema for the development of auditable and end-to-end verifiable e-voting systems through the adoption of multiple intelligent agent nodes, namely; super-node, polling stations, and trusted nodes. At the end of the election, the votes at the trusted and super-node chain are tallied and counted accordingly. The system allowed for suitability of the electoral process, however, it prioritized certain nodes in the blockchain network over others, causing some nodes to have outsized influence over the entire network, leaving room for manipulation of the electoral process. Wu, (Wu, 2017), implemented an e-voting system based on a private blockchain system with a three-entity model, namely the voters, registration authority, and election authority, all subject to public supervision. It also implemented ring signature together with RSA cryptosystem for unforgeability of ballots. The system ensured ballot anonymity. However, due to the decentralized nature of the blockchain system, it would be possible for the permitted participants of the blockchain to view the ledger of the blockchain and find out how voters had voted. Consequently, Liu and Wang, (Liu and Wang, 2017), proposed an e-voting system based on Proof-of-Stake (PoS) consensus Blockchain, with a blind signature. The system ensured, transparency and immutability of ballots. The adoption of Proof-of-Stake consensus by the system meant the need to prioritize some nodes of the blockchain over others, meaning that some nodes would have an outsized influence on the network (Zamostin, 2019). Similarly, Zhang et al. (Zhang et al., 2019) introduced an e-voting system based on the public Ethereum Blockchain system with message authentication and transmission mechanism, to prevent forging of ballots, together with Blind signature, for validation of message authenticity. The system ensured the prevention of vote manipulation with proper decentralization of authority. However, the adoption of public Ethereum meant that payments had to be made (in gas) equivalent to the amount of work done in mining the e-voting smart contract, thus, incurring additional expenses for the conduct of elections.

Yi, (Yi, 2019), also designed an e-voting system based on a private blockchain using a synchronized model of distributed ledger technology (DLT) for the prevention of ballot forgery and elliptic curve encryption of voter credentials, to provide authentication and non-repudiation. The distributed nature of the blockchain ledger however meant that the permitted participants of the blockchain were able to view how voters have voted, which is a privacy flaw. Consequently, Mohammedali and Al-Sherbaz, (Mohammedali and Al-Sherbaz, 2019), put forward an e-voting framework based on a private blockchain, coupled with an elliptic curve algorithm. The system achieved transparent balloting (casting of votes), there was, however, no proper decentralization of authority which gives room for manipulation of the integrity of ballots. Arun et al., (Arun, 2019), developed an e-voting system based on the currency transaction approach on the Ethereum blockchain, by the allocation of a digital coin to cryptographic wallets assigned to each voter. The system achieved audibility and transparency with the immutability of votes, however, failed to put in place considerations for the protection of the confidentiality of votes. Thereafter, Park, (Park, 2019), put forward the adoption of a decentralized Proof-of-Work (PoW) consensus-based blockchain for decentralization in an e-voting system. Though the system achieved immutability of votes, the permissioned nodes on the blockchain could probe the ledger of

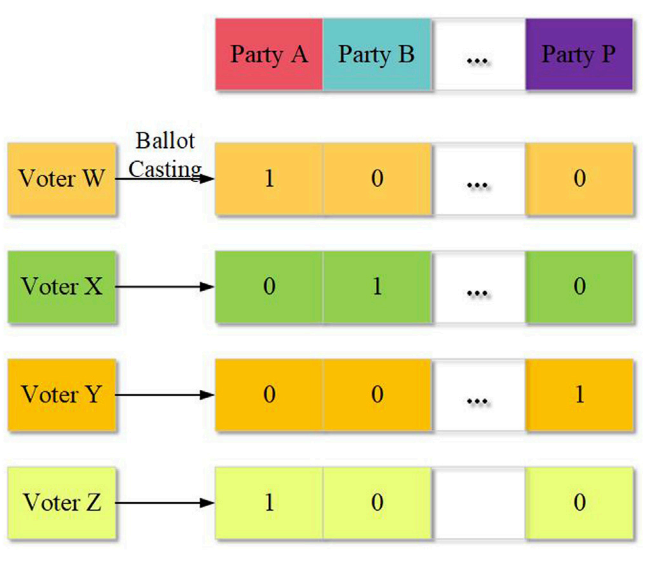


FIGURE 1 | Ballot structure.

transactions to see how electorates had voted, thereby compromising the privacy of the electorates.

After a careful review of the literature, it can be seen that the adoption of blockchain in e-voting systems guarantees integrity with the possibility of compromising the confidentiality of electorates. There is therefore the need to adopt a technique that ensures the protection of the confidentiality of the blockchain system. The following section, therefore, describes the technique adopted in this study for achieving the goal of protection of confidentiality with integrity in e-voting.

3 RESEARCH METHOD

This section describes the technique adopted in developing the e-voting system, with emphasis on the open-source blockchain system, the proof-of-work consensus, privacy preservation through the Paillier homomorphic encryption, the system architecture, deployment, as well as the metrics for evaluation of its performance.

3.1 Ballot Structure

Figure 1 gives an illustration of the structure of the ballots which will be passed as transactions to the blockchain serving as a ballot box. Consider an election with contestants *A, B, . . . , P* and electorates, *W, X, Y, Z.*

The ballot cast by each of the electorates is structured such that a voter cast a value of one for the contestant of their choice, and casts a value of zero for all of the other contestants in an array. Meaning that the ballot cast by each of the electorates is an array with a length equal to the number of contestants, *P* in the election. Taking an electorate, *W* that cast a ballot, $B_{WN,}$ for a candidate, C_S then;

$$B_{WN} = [V_{WA}, V_{WB}, \ldots, V_{WP}] \tag{1}$$

such that;

$$|B_{WN}| = P \tag{2}$$

and;

$$B_{WN} = \begin{cases} 0\ ;\ N \neq C_s \\ 1\ ;\ N = C_s \end{cases} \tag{3}$$

After a voter has cast their ballot, $B_{WN,}$ there is a need to preserve the confidentiality of the ballot through the process of encryption. This is done by the adoption of Paillier homomorphic encryption, which provides additive homomorphism needed to tally and sum together the encrypted votes. **Section 3.2** provides insight into how this is achieved.

3.2 Paillier Homomorphic Encryption

Paillier homomorphic encryption is a partially homomorphic encryption scheme that supports additive homomorphism, which is an operation that allows two ciphertexts to be multiplied, resulting in a ciphertext whose decryption is a sum of the corresponding plaintexts. Consider a scenario with two data, D_1 and D_2, both subjected to Paillier encryption operation, *E*, using a public encryption key (*n, g*), thereby producing two separate ciphertext values, C_{D1} and $C_{D2,}$ such that;

$$C_{D1} = E(D_1, S_1) \tag{4}$$

and;

$$C_{D2} = E(D_2, S_2) \tag{5}$$

where; S_1 and S_2 are two randomly selected integer values, such that;

$$0 < S < n \tag{6}$$

This encryption protocol is adopted for the encryption of each voter ballot, B_{WN}, as specified in **Eq. 1**, such that encryption of the ballot of an electorate, *W* is given by;

$$C_{DWN} = E\ (B_{WN}\ ,\ S) \tag{7}$$

$$C_{DWN} = [E([\ V_{WA}],\ S),\ E([\ V_{WB}],\ S),\ \ldots,\ E([\ V_{WP}],\ S)] \tag{8}$$

The value of $C_{DWN,}$ as specified in **Eq. 8** is the ballot transaction that is then sent by each electorate to the blockchain system which serves as a ballot box for e-voting.

After encrypting the ballots and committing the encrypted ballots to the blockchain, at the end of the electoral process, there is a need to tally and count the casted votes. Since the votes have been encrypted homomorphically, the Paillier cryptosystem provides additive homomorphism which allows computations to be carried out on encrypted data without the need for initial decryption. **Section 3.2.1** provides further insight into how additive homomorphism is achieved.

3.2.1 Additive Homomorphism Protocol

At the end of the electoral process, the encrypted voter ballot transactions are obtained from the blockchain ballot box and aligned for homomorphic addition. **Figure 2** illustrates the process of homomorphic addition of the ballots.

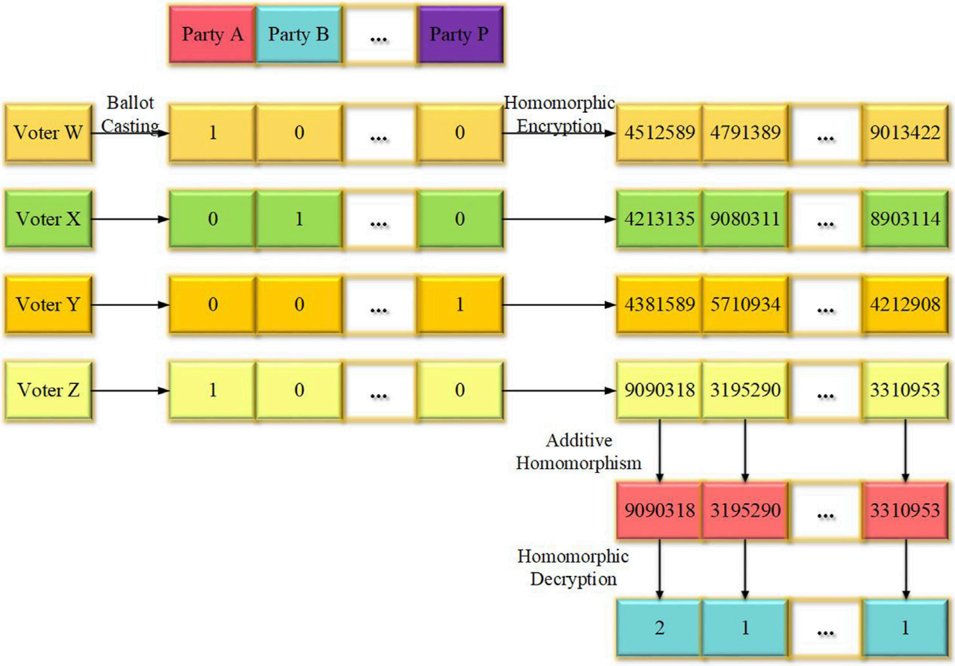


FIGURE 2 | Additive homomorphism.

The encrypted ballots are aligned and summed together through additive homomorphism, thereby obtaining a final encrypted sum, which is then decrypted to get the results of the election. The integrity and decentralization of the entire electoral process are achieved by the adoption of an open-source blockchain system as further described in **section 3.3**.

3.3 Node.js Open-Source Blockchain

Open source blockchain repository provided by (Emiceli, 2019; Traub, 2018), both implemented using Node. js (a back-end and cross-platform runtime environment), were adopted for developing a private blockchain system on which the e-voting system is based. In the blockchain, transactions are placed in blocks that contain;

a. A pseudonymous blockchain address of an electorate, with the prefix, 0x00FUTMCPE.
b. The pseudonymous blockchain address of the electorate authority, admin.
c. SHA256 digest (hash) of the previous block of transaction.
d. Transaction ID.
e. Nonce.
f. Ballot transactions in the form illustrated in (8).
g. SHA256 digest (hash) of the new block of transaction.

The blockchain system verifies the authenticity of transactions being carried out through the adoption of a consensus protocol. This consensus protocol is the backbone of the blockchain which helps prevent bad actors (nodes) from tampering with the blockchain. The consensus protocol in use in the adopted blockchain is further described in **Section 3.3.1**.

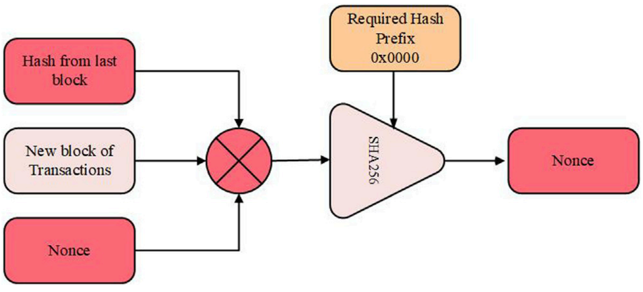


FIGURE 3 | Proof-of-work (PoW) consensus.

3.3.1 Blockchain Proof-Of-Work Consensus and Mining Protocol

The blockchain system adopts the Proof-of-Work consensus mechanism. **Figure 3** gives an illustration of the consensus mechanism used in mining new blocks of transactions.

The process begins by combining the hash of the previous block with the hash of the new block, together with a nonce value, which increments successively, until the prefix value of the SHA256 function is equal to the required hash prefix. If the process is not successful, then the nonce value is incremented, and the process is repeated until the process is successful. Then the nonce value is returned by the consensus, and the new block of the transaction can be added to the ledger of the blockchain. The various schemes adopted for the realization of the e-voting system are carefully put together following the system architecture laid out in **section 3.4**.

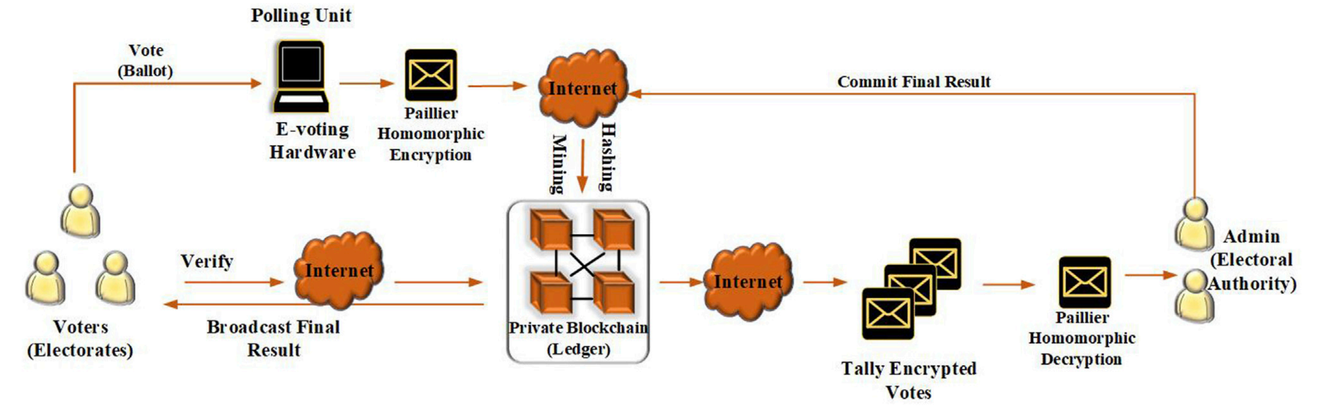


FIGURE 4 | System architecture.

3.4. System Architecture

Figure 4 shows the architecture of the system. At the core is the blockchain private blockchain system, which maintains a ledger. At the polling unit, the voters (electorates) cast their ballots, in the form specified in **Eq. 1**, after which the ballots are encrypted homomorphically, thereby transforming the ballots into the structure specified in **Eq. 8**. A new block of the transaction is then created, containing; the encrypted ballots, the pseudonymous address of the voter and the admin, the timestamp of the block creation, the hash of the previous block of the transaction, as well as the hash of the current block. Then the new block of the transaction is mined using the consensus mechanism as illustrated in **Figure 3**. After mining, the new block is committed to the ledger of the blockchain.

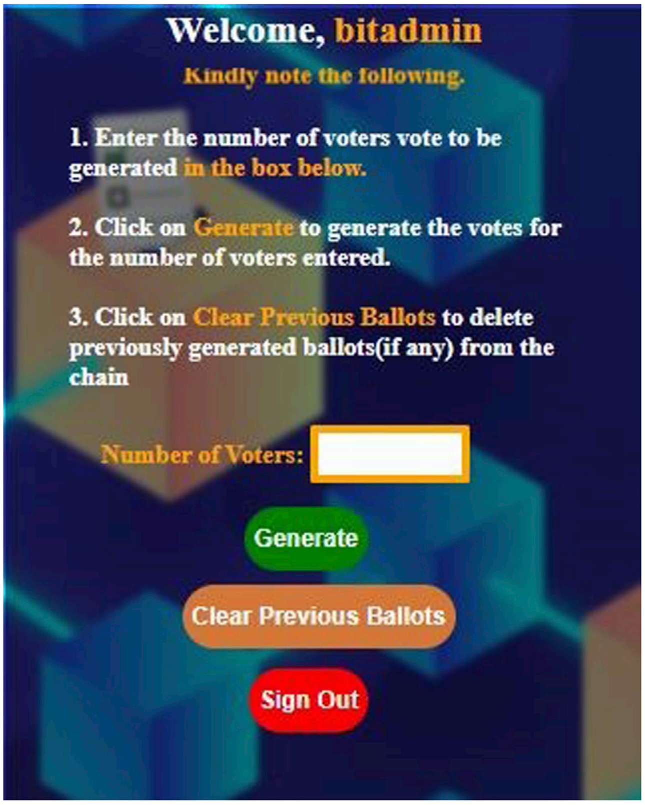
This process continues, until the end of the election when the electoral authority decides to end the election. Then the admin, by additive homomorphism, tallies the encrypted votes, thereby obtaining a final encrypted sum that can be decrypted to obtain the results of the election. The electoral authority can then proceed to make the result of the election public, by sending it to the email address of all the electorates that voted in the election.

3.4.1. Heroku Free-Tier Server Deployment

The blockchain was deployed on the cloud as a web app on the Heroku cloud application platform, using free tier hosting, which provides 512 MB of RAM with two process types. The block ledger of the blockchain is made public and can be accessed from anywhere, over the internet using the link, https://cpemachines.herokuapp.com/blockledger.

3.5. System Testing

This section explains how the performance of the system was evaluated in terms of the transaction throughput of the blockchain, as well as the system's response time to various user actions. The sequence of actions taken to test and evaluate the performance of the system is given below;


Welcome, bitadmin

Kindly note the following.

1. Enter the number of voters vote to be generated in the box below.

2. Click on Generate to generate the votes for the number of voters entered.

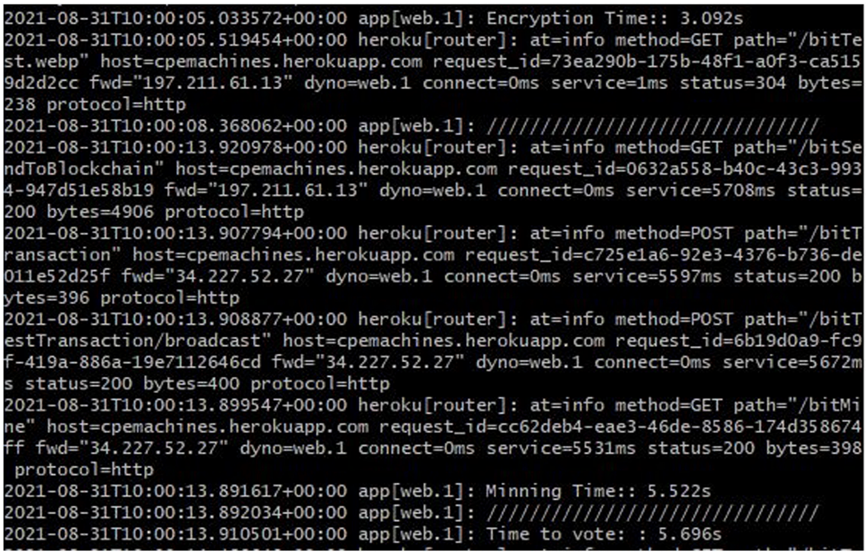
3. Click on Clear Previous Ballots to delete previously generated ballots(if any) from the chain

FIGURE 5 | System testing interface.

Step -1: An API endpoint was developed on the blockchain, to allow for simulation of a varying number of transactions, which is accessed through a webpage interface as can be seen in **Figure 5**.

Step -2: The console output function was invoked within the API to provide a real-time indication of the time taken to mine the various number of transactions.

Step -3: The command-line interface (CLI) window of the cloud-hosted e-voting platform was opened as shown in **Figure 6**.



```
2021-08-31T10:00:05.033572+00:00 app[web.1]: Encryption Time:: 3.092s
2021-08-31T10:00:05.519454+00:00 heroku[router]: at=info method=GET path="/bitTe
st.webp" host=cpemachines.herokuapp.com request_id=73ea290b-175b-48f1-a0f3-ca515
9d2d2cc fwd="197.211.61.13" dyno=web.1 connect=0ms service=1ms status=304 bytes=
238 protocol=http
2021-08-31T10:00:08.368062+00:00 app[web.1]: //////////////////////////////
2021-08-31T10:00:13.920978+00:00 heroku[router]: at=info method=GET path="/bitSe
ndToBlockchain" host=cpemachines.herokuapp.com request_id=0632a558-b40c-43c3-993
4-947d51e58b19 fwd="197.211.61.13" dyno=web.1 connect=0ms service=5708ms status=
200 bytes=4906 protocol=http
2021-08-31T10:00:13.907794+00:00 heroku[router]: at=info method=POST path="/bitT
ransaction" host=cpemachines.herokuapp.com request_id=c725e1a6-92e3-4376-b736-de
011e52d25f fwd="34.227.52.27" dyno=web.1 connect=0ms service=5597ms status=200 b
ytes=396 protocol=http
2021-08-31T10:00:13.908877+00:00 heroku[router]: at=info method=POST path="/bitT
estTransaction/broadcast" host=cpemachines.herokuapp.com request_id=6b19d0a9-fc9
f-419a-886a-19e7112646cd fwd="34.227.52.27" dyno=web.1 connect=0ms service=5672m
s status=200 bytes=400 protocol=http
2021-08-31T10:00:13.899547+00:00 heroku[router]: at=info method=GET path="/bitMi
ne" host=cpemachines.herokuapp.com request_id=cc62deb4-eae3-46de-8586-174d358674
ff fwd="34.227.52.27" dyno=web.1 connect=0ms service=5531ms status=200 bytes=398
 protocol=http
2021-08-31T10:00:13.891617+00:00 app[web.1]: Minning Time:: 5.522s
2021-08-31T10:00:13.892034+00:00 app[web.1]: //////////////////////////////
2021-08-31T10:00:13.910501+00:00 app[web.1]: Time to vote: : 5.696s
```

FIGURE 6 | Heroku CLI window of the developed system.

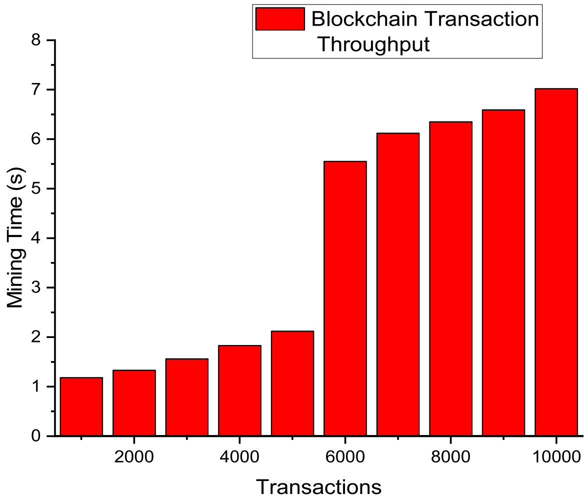


FIGURE 7 | Blockchain transaction throughput.

Step -4: The simulation webpage interface is opened up and by using the provided input section, values for a varying number of transactions were entered, with simulation carried out repeatedly and the average for the various repetitions was computed.
Step -5: By subjecting the obtained values to a graph plotting software (Origin pro), the results obtained from the testing are shown in **Figure 7**.
Step -6: Also, the response time values for the various user actions were noted from the CLI window, with the average value computed for each time the simulation for carried out.
Step -7: The obtained response time values for the user operations are summarized in **Table 1**.

TABLE 1 | System Response Time for various user actions.

Number of voters	Vote casting (min)	Vote tallying (min)
1,000	0.01	0.17
2,000	0.04	0.23
3,000	0.08	0.46
4,000	0.12	0.53
5,000	0.23	0.78
6,000	0.34	0.81
7,000	0.45	1.20
8,000	0.62	1.33
9,000	0.68	1.41
10,000	0.73	1.56

3.5.1. Blockchain Transaction Throughput

This is the measure of the rate at which the blockchain system mines and commits transactions to the ledger. It is calculated using **Equation 9** and measure in transactions per second (tps).

$$\theta = \frac{n}{m} \tag{9}$$

where; n is the number of transactions and; m is the mining time.

3.5.2. Response Time

This is the measure of the time that elapses between the initiation of an action by a user and the time when the results are displayed by the system to the user. The response time of the system was measured for varying user actions and presented accordingly in **Table 1**.

4 RESULTS AND DISCUSSION

By the developed API endpoint, as explained in **section 3.5**, the various number of transactions were generated and the time taken for the transactions to be mined was recorded accordingly. The blockchain transaction throughput of the blockchain system was then calculated using **Eq. 9**. **Figure 7** shows the graphical representation of the transaction throughput value.

$$Average\ system\ response\ time\ =\ \frac{Sum\ of\ all\ respective\ time\ taken\ to\ complete\ user\ action}{number\ of\ tests}$$

$$Average\ vote\ casting\ time = \frac{0.01 + 0.04 + 0.08 + 0.12 + 0.23 + 0.34 + 0.45 + 0.62 + 0.68 + 0.73}{10}$$

$$Average\ vote\ casting\ time = \frac{3.3}{10} = 0.33$$

$$Average\ vote\ tallying\ time = \frac{0.17 + 0.23 + 0.46 + 0.53 + 0.78 + 0.81 + 1.20 + 1.33 + 1.41 + 1.56}{10}$$

$$Average\ vote\ tallying\ time = \frac{8.48}{10} = 0.848$$

From calculations, the mining time of the blockchain increased by an average factor of 0.18 s for every thousand increases in the number of transactions. Also, the response time of the system to a range of user actions was evaluated over an increasing number of voters. Results obtained showed that the response time of the system for vote casting operations increased by an average of 0.33 min per thousand voters while for vote tallying there was an increase in response time by an average of 0.848 min per thousand voters.

Also, as can be seen in **Figure 7**, it was observed that the mining time increased steadily by an average factor of 0.18 s for every thousand increments in the number of transactions, up until the six thousand marks, when the mining time suddenly increased sharply to about 10 times the steady increment value. This is a result of the difficulty in calculating the nonce value for the PoW at that instant of time when the transactions were to be mined. This transaction throughput readings reflect in the response time of the system to actions that involve committing a change to the ledger of the blockchain. To measure the implication of the transaction throughput on the system, the response time of the system is measured for various user actions. The user actions include; vote casting and vote tallying operations through the process highlighted in **section 3.5.2**. The results obtained for the system response time are summarized in **Table 1**.

From **Table 1**, it can be seen that the response time of the system for vote-tallying operations increased linearly by a factor of 9.2 s for every thousand increments in the number of voters, while for vote casting, the response time increased linearly by an average factor of 4.8 s. The response time increment factor for the vote casting is less than that of vote tallying because, the process of vote casting involves only encryption of the ballots of voters, while the vote tallying process involves aligning, homomorphic addition, and final sum decryption of the encrypted ballots. The implication of these response time readings in **Table 1** is that increase in the number of voters and nodes in the blockchain system results in an increase in the time taken for the blockchain to process the various transactions.

5 CONCLUSION AND FUTURE SCOPE

In this study, the focus was on the preservation of privacy and integrity in e-voting by the adoption of blockchain and Paillier homomorphic encryption. This study has successfully combined the Paillier homomorphic encryption with an open-source blockchain system and was tested using a testing endpoint that simulated a varying number of transactions and voters. The mining time of the blockchain system for ten thousand simulated ballot transactions was 7.02 s, which translates to a transaction throughput of 1424 tps. The system achieved integrity and immutability of ballots through the blockchain system and also achieved protection of voter confidentiality through the Paillier cryptosystem.

The scientific contribution made by this study is first an assessment of the impact of blockchain technology on the bid to achieve electoral integrity in e-voting systems, with a reflection of a research gap existent in violation of confidentiality in e-voting as a result of the decentralized nature of the blockchain, resulting in the proposition to address the discovered research gap by coupling an open-source private blockchain system with Paillier homomorphic encryption. The applicability of this study spans from small-scale balloting activities to large-scale national elections.

The limitation of this study is a throttled performance resulting from deployment on a free-tier cloud server. In the future, this study looks forward to deploying the system on a paid-tier cloud server which will provide more computing resources and will therefore allow for faster mining of transactions, as well as faster response time.

Aside from the protection of integrity and protection of voter privacy, there is also the need to provide a means for verification of electorate authenticity. This study will therefore also, look into the adoption of a multi-factor biometric authentication mechanism in the future to help authenticate electorates and prevent irregularities associated with the process.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding authors.

AUTHOR CONTRIBUTIONS

BU reviewed and modified the content of this manuscript. OO wrote **sections 1**, and **2**, References, and the formatting of the manuscript. DO wrote **sections 3**, and **4**, and ED wrote **Sections 5**, and supplementary material.

ACKNOWLEDGMENTS

We want to acknowledge our reviewers for their contributions in making this manuscript better and publishable.

REFERENCES

Abuidris, Y., Hassan, A., Hadabi, A., and Elfadul, I. (2019). "Risks and Opportunities of Blockchain Based on E-Voting Systems," in 2019 16th Int. Comput. Conf. Wavelet Act. Media Technol. Inf. Process. ICCWAMTIP, 365–368. doi:10.1109/ICCWAMTIP47768.2019.9067529

Alguliyev, R., Aliguliyev, R., Aliguliyev, R., and Yusifov, F. (2019). Multi-criteria Evaluation + Positional Ranking Approach for Candidate Selection in E-Voting. *Decis. Mak. Appl. Manag. Eng.* 2 (2), 65–80. doi:10.31181/dmame1902119a

Almimi, H. M., Shahin, S. A., Daoud, M. S., Al Fayoumi, M., and Ghadi, Y. (2019). "Enhanced E-Voting Protocol Based on Public Key Cryptography," in 2019 International Arab Conference on Information Technology (ACIT), 218–221. doi:10.1109/acit47987.2019.8990991

Arnob, M. S., Sarker, N., Haque, M. I.-U., and Bhuyan, M. G. S. (2020). Blockchain-Based Secured E-Voting System to Remove the Opacity and Ensure the Clarity of Election of Developing Countries. *Int. Res. J. Eng. Technol.* 07 (1).

Arnob, S., Sarker, N., Haque, I.-U., Sarwar, M. G., and Bhuyan (2020). Blockchain-Based Secured E- Voting System to Remove the Opacity and Ensure the Clarity of Election of Deve. *Int. Res. J. Eng. Technol.* 7, 1826–1831.

Arun, S. S. S. (2019). Blockchain Enabled E-Voting System. *Int. J. Adv. Res. Comput. Commun. Eng.* 8 (4), 77–81. doi:10.17148/ijarcce.2019.8412

Bag, S., Azad, M. A., and Hao, F. (2019). *End-to-End Verifiable Cumulative Voting without Tallying Authorities*, 1–36.

Bao, Z., Wang, B., and Shi, W. (2018). A Privacy-Preserving, Decentralized and Functional Bitcoin E-Voting Protocol. in Proc. - 2018 IEEE SmartWorld, Ubiquitous Intell. Comput. Adv. Trust. Comput. Scalable Comput. Commun. Cloud Big Data Comput (Internet People Smart City Innov. SmartWorld/UIC/ATC/ScalCom/CBDCo), 252–256. doi:10.1109/SmartWorld.2018.00078

Barakat, M., Eder, C., and Hanke, T. (2018). *An Introduction to Cryptography*.

Baskaran, H., Yussof, S., and Rahim, F. A. (2020). A Survey on Privacy Concerns in Blockchain Applications and Current Blockchain Solutions to Preserve Data Privacy. *Commun. Comput. Inf. Sci.* 1132, 3–17. doi:10.1007/978-981-15-2693-0_1

Bellini, E., Ceravolo, P., Bellini, A., and Damiani, E. (2020). Designing Process-Centric Blockchain-Based Architectures: A Case Study in E-Voting as a Service. *Lect. Notes Bus. Inf. Process.* 379, 1–23. doi:10.1007/978-3-030-46633-6_1

Bhardwaj, C. (2020). *Zero Know Proof- its Explanation and Role in Blockchain*. Delhi – NCR, India: Appinventiv. https://appinventiv.com/blog/zero-knowledge-proof-blockchain/(accessed Sep., 202021).

Blazy, O. (2012). *Interactive and Non-interactive Proofs of Knowledge*. Barcelona, Spain: Longdom.

Bungale, P. P., and Sridhar, S. (2016). *A Framework for Receipt Issuing, Contendable Remote Poll-Site Voting." Departamento de Ciencias de la Computación*. Washington, DC: USENIX Association.

Christyono, B. B. A., Widjaja, M., and Wicaksana, A. (2021). Go-Ethereum for Electronic Voting System Using Clique as Proof-Of-Authority. *Telkomnika* 19 (5), 1565–1572. doi:10.12928/TELKOMNIKA.V19I5.20415

Daramola, O. (2020). *Architecture-Centric Evaluation of Blockchain-Based*.

Darwish, A., and Gendy, M. M. E. (2017). A New Cryptographic Voting Verifiable Scheme for E-Voting System Based on Bit Commitment and Blind Signature. *Int. J. Swarm Intel. Evol. Comput.* 6 (2). doi:10.4172/2090-4908.1000158

Dayal, M., Chawla, A., and Khari, M. (2021). Coalescence of Neural Networks and Blockchain. *Handb. Green Comput. Blockchain Technol.*, 31–44. doi:10.1201/9781003107507-3

Emiceli, D. (2019). *Chainode: Fast, Highly Scalable, and Lightweight Private Blockchain Network Based on node.Js*. Milan, Italy: Davide Miceli. Available at: https://github.com/davidemiceli/chainode (accessed Sep., 202021).

Feng, Q., He, D., Zeadally, S., Khan, M. K., and Kumar, N. (2019). A Survey on Privacy Protection in Blockchain System. *J. Netw. Comput. Appl.* 126, 45–58. doi:10.1016/j.jnca.2018.10.020

Fleder, M., Kester, M. S., and Pillai, S. (2015). Bitcoin Transaction Graph Analysis. [Online]. Available: http://arxiv.org/abs/1502.01657.

for, I. D., and Idea, E. A. (2011). *Introducing Electronic Voting : PolicyPaper*.

Fusco, F., Lunesu, M. I., Pani, F. E., and Pinna, A. (2018). "Crypto-voting, a Blockchain Based E-Voting System," in IC3K 2018 - Proc. 10th Int. Jt. Conf. Knowl. Discov. Knowl. Eng. Knowl. Manag. 3 Ic3k, 223–227. doi:10.5220/0006962102230227

Gao, S., Zheng, D., Guo, R., Jing, C., and Hu, C. (2019). An Anti-quantum E-Voting Protocol in Blockchain with Audit Function. *IEEE Access* 7, 115304–115316. doi:10.1109/ACCESS.2019.2935895

George and Samman (2016). *The Trend towards Blockchain Privacy: Zero Knowledge Proofs*. New York, NY: Coindesk. https://www.coindesk.com/trend-towards-blockchain-privacy-zero-knowledge-proofs (accessed Jun. 25, 2021).

George, G. T., Konnully, P., Nair, S. R., Tas, R., and Kumar, M. (2019). *[IJCST-V9i2p5]: Kevin Gabriel Houlder, Nithishwar P , Santhosh G , Venkatesh E.*

Giudici, G., Milne, A., and Vinogradov, D. (2019). Cryptocurrencies: Market Analysis and Perspectives. *J. Ind. Bus. Econ.* 47147 (1), 1–18. doi:10.1007/S40812-019-00138-6

Halunen, K., and Latvala, O.-M. (2021). Review of the Use of Human Senses and Capabilities in Cryptography. *Comput. Sci. Rev.* 39, 100340. doi:10.1016/j.cosrev.2020.100340

Hanifatunnisa, R., and Rahardjo, B. (2017). "Blockchain Based E-Voting Recording System Design," in Proceeding 2017 11th Int. Conf. Telecommun. Syst. Serv. Appl. TSSA, 2018, 1–6. doi:10.1109/TSSA.2017.8272896

Heiberg, S., Parsovs, A., and Willemson, J. (2015). Log Analysis of Estonian Internet Voting 2013-2014. *Lect. Notes Comput. Sci. Incl. Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinforma.* 9269, 19–34. doi:10.1007/978-3-319-22270-7_2

Hellani, H., Sliman, L., Samhat, A. E., and Exposito, E. (2020). Overview on the Blockchain-Based Supply Chain Systematics and Their Scalability Tools. *Emerg. Sci. J.* 4, 45–69. doi:10.28991/esj-2021-SP1-04

Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., and Hjálmtýsson, G. (2018). "Blockchain-based E-Voting System," in 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 983–986.

Hu, Y., Liyanage, M., Mansoor, A., Thilakarathna, K., Jourjon, G., and Seneviratne, A. (2018). *Blockchain-based Smart Contracts - Applications and Challenges*. Ihaca, New York: Cornell University, 1–26. [Online]. Available at: http://arxiv.org/abs/1810.04699.

Jabbar, I., and Alsaad, S. N. (2017). Design and Implementation of Secure Remote E-Voting System Using Homomorphic Encryption. *Ij. Netw. Secur.* 19 (5), 694–703.

Jason, P. C., and Yuichi, K. (2016). E-voting System Based on the Bitcoin Protocol and Blind Signatures. *IPSJ Trans. Math. Model. Its Appl.*, 1–6. [Online]. Available: https://www.researchgate.net/profile/Jason_Paul_Cruz/publication/317100187_E-voting_System_Based_on_the_Bitcoin_Protocol_and_Blind_Signatures/links/59d5a3ee458515140ee44e93/E-voting-System-Based-on-the-Bitcoin-Protocol-and-Blind-Signatures.pdf.

Khan, K. M., Arshad, J., and Khan, M. M. (2018). Secure Digital Voting System Based on Blockchain Technology. *Int. J. Electron. Gov. Res.* 14 (1), 53–62. doi:10.4018/IJEGR.2018010103

Kiayias, A., Zacharias, T., and Zhang, B. (2017). An Efficient E2E Verifiable E-Voting System without Setup Assumptions. *IEEE Secur. Priv.* 15 (3), 14–23. doi:10.1109/MSP.2017.71

Kirillov, D., Korkhov, V., Petrunin, V., Makarov, M., Khamitov, I. M., and Dostov, V. (2019). *Implementation of an E-Voting Scheme Using Hyperledger Fabric Permissioned Blockchain 11620 LNCS*. Springer International Publishing.

Kost'al, K., Bencel, R., Ries, M., and Kotuliak, I. (2019). *10th, and Undefined 2019, "Blockchain E-Voting Done Right: Privacy and Transparency with Public Blockchain*. ieeexplore.ieee.org. doi:10.1109/ICSESS47205.2019.9040770

Liu, Y., and Wang, Q. (2017). *An E-Voting Protocol Based on Blockchain*. Poland, Poznan: Cryptology ePrint, 1043. [Online]. Available at: https://eprint.iacr.org/2017/1043.pdf.

Mohammedali, N., and Al-Sherbaz, A. (2019). Election System Based on Blockchain Technology. *Ijcsit* 11 (5), 13–31. doi:10.5121/ijcsit.2019.11502

Mustafa, M. K., and Waheed, S. (2021). An E-Voting Framework with Enterprise Blockchain. *Adv. Distributed Comput. Mach. Learn.* 127, 135–145. doi:10.1007/978-981-15-4218-3_14

Nzuva, S. (2019). Smart Contracts Implementation, Applications, Benefits, and Limitations. *Ppar* 9 (5), 63–75. doi:10.7176/ppar/9-9-06

Panwar, A., Bhatnagar, V., Khari, M., Salehi, A. W., and Gupta, G. (2022). A Blockchain Framework to Secure Personal Health Record (PHR) in IBM Cloud-Based Data Lake. *Comput. Intell. Neurosci.* 2022, 1–19. doi:10.1155/2022/3045107

Park, H.-D. (2019). A Decentralized E-Voting System Based on Blockchain Network. *Int. J. Innov. Technol. Explor. Eng.* 18 (12).

Partala, J., Nguyen, T. H., and Pirttikangas, S. (2020). Non-interactive Zero-Knowledge for Blockchain: A Survey. *IEEE Access* 8, 227945–227961. doi:10.1109/ACCESS.2020.3046025

Patidar, K., and Jain, S. (2019). Decentralized E-Voting Portal Using Blockchain. *2019 10th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT*, 1–4. doi:10.1109/ICCCNT45670.2019.8944820

Pawlak, M., Poniszewska-Marańda, A., and Kryvinska, N. (2018). Towards the Intelligent Agents for Blockchain E-Voting System. *Procedia Comput. Sci.* 141, 239–246. doi:10.1016/j.procs.2018.10.177

Prashantha, N. C., Arpitha, Y. C., Preethi, R. B. K., Ranjitha, D., and Vinutha, T. (2018). Design and Development of Security Based Voting System for Government Using Raspberry Pi. *Int. J. Adv. Eng. Res. Dev.* 5 (5), 379–384.

Puneet, A., Chaudhary, A., Chauhan, N., and Kumar, A. (2021). "Decentralized Voting Platform Based on Ethereum Blockchain," in Proc. 2021 1st Int. Conf. Adv. Electr. Comput. Commun. Sustain. Technol. ICAECT 2021, 224–229. doi:10.1109/ICAECT49130.2021.9392580

Risnanto, S., Rahim, Y. B. A., and Herman, N. S. (2019). "Preparatory Component for Adoption E-Voting," in TSSA 2019 - 13th Int. Conf. Telecommun (Bali, India: IEEE), 31–34. doi:10.1109/TSSA48701.2019.8985461

Sallal, M. (2019). *VMV: Augmenting an Internet Voting System with Selene Verifiability*. Singapore: IEEE, 1–17. [Online]. Available: http://arxiv.org/abs/1912.00288.

Sänger, R. (2019). *On the Limitations of Cryptocurrencies the Inclusion of Coalitions in Double-Spending Attacks on Proof-Of-Work Based Cryptocurrencies*. [Online]. Available: https://ssrn.com/abstract=3731527.

Sarker, A., Byun, S., Fan, W., Psarakis, M., and Chang, S. Y. (2020). Voting Credential Management System for Electronic Voting Privacy. *IFIP Netw. 2020 Conf. Work. Netw.* 2020, 594–598.

Sharma, T. (2016). E-voting Using Homomorphic Encryption Scheme. *Ijca* 141 (13), 14–16. doi:10.5120/ijca2016909652

Sheer Hardwick, F., Gioulis, A., Naeem Akram, R., and Markantonakis, K. (2018). E-voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy. in Proc. - IEEE 2018 Int. Congr. Cybermatics 2018 IEEE Conf. Internet Things, Green Comput. Commun. Cyber, Phys. Soc. Comput. Smart Data, Blockchain, Comput. Inf (Halifax, Canada: IEEE), 1561–1567. doi:10.1109/Cybermatics_2018.2018.00262

Nigam, S., Sugandh, U., and Khari, M. (2022). The Integration of Blockchain and IoT Edge Devices for Smart Agriculture: Challenges and Use Cases. 507–537. doi:10.1016/bs.adcom.2022.02.015

Sugandh, U., Khari, M., and Nigam, S. (2021). How Blockchain Technology Can Transfigure the Indian Agriculture Sector. *Handb. Green Comput. Blockchain Technol.*, 69–88. doi:10.1201/9781003107507-6

Traub, E. (2018). *Erictraub/Learn-Blockchain-By-Building-Your-Own-In-JavaScript: Code Out Your Very Own Blockchain and Decentralized Network in the Javascript Programming Language*. Birmingham, UK: PacktPub. Available at: https://github.com/erictraub/Learn-Blockchain-By-Building-Your-Own-In-JavaScript (accessed Sep 20, 2021).

Vivek, S., and Yashank, R. (2020). E-voting System Using Hyperledger Sawtooth. ieeexplore.ieee.org [Online]. Available at: https://ieeexplore.ieee.org/abstract/document/9212945/(Accessed Sep 19, 2021).

Wang, B., Sun, J., He, Y., Pang, D., and Lu, N. (2018). Large-scale Election Based on Blockchain. *Procedia Comput. Sci.* 129, 234–237. doi:10.1016/j.procs.2018.03.063

Wang, D., Zhao, J., and Wang, Y. (2020). A Survey on Privacy Protection of Blockchain: The Technology and Application. *IEEE Access* 8, 108766–108781. doi:10.1109/ACCESS.2020.2994294

Will, M. A., and Ko, R. K. L. (2015). A Guide to Homomorphic Encryption. *Cloud Secur. Ecosyst. Tech. Leg. Bus. Manag. Issues*, 101–127. doi:10.1016/B978-0-12-801595-7.00005-7

Wu, Y. (2017). *An E-Voting System Based on Blockchain and Ring Signature*. Birmingham, UK: School of Computer Science, University of Birmingham.

Yavuz, E., Koc, A. K., Cabuk, U. C., and Dalkilic, G. (2018). "Towards Secure E-Voting Using Ethereum Blockchain," in 6th Int. Symp. Digit. Forensic Secur. ISDFS 2018 - Proceeding 2018-Janua, 1–6. doi:10.1109/ISDFS.2018.8355340

Yi, H. (2019). Securing E-Voting Based on Blockchain in P2P Network. *J. Wirel. Com. Netw.* 2019 (1), 1–9. doi:10.1186/s13638-019-1473-6

Yu, B., Liu, J., Sakzad, A., Steinfeld, R., and Rimba, P. (2018). *Platform-independent Secure Blockchain-Based Voting System*. Guildford, UK: Springer, Cham.

Zamostin, Y. (2019). *Proof of Work and Proof of Stake - what Are the Key Differences?*. Illinois, US: Coinifide. Available at: https://coinifide.com/proof-of-work-vs-proof-of-stake-what-are-the-key-differences/(accessed Jun06, 2021).

Zhang, J.-L., Zhang, J.-Z., and Xie, S.-C. (2018). A Choreographed Distributed Electronic Voting Scheme. *Int. J. Theor. Phys.* 57 (9), 2676–2686. doi:10.1007/s10773-018-3789-0

Zhang, Q., Xu, B., Jing, H., and Zheng, Z. (2019). *Ques-Chain: An Ethereum Based E-Voting System*. arXiv Prepr. arXiv1905.05041.

Zhang, R., Xue, R., and Liu, L. (2020). Security and Privacy on Blockchain. *ACM Comput. Surv.Mar* 52 (3), 1–34. doi:10.1145/3316481

Zhao, Z., and Chan, T.-H. H. (2016). How to Vote Privately Using Bitcoin. *Lect. Notes Comput. Sci. Incl. Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinforma.* 9543, 82–96. doi:10.1007/978-3-319-29814-6_8

Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr.*, 557–564. doi:10.1109/BigDataCongress.2017.85

Zhou, Y., Liu, Y., Jiang, C., and Wang, S. (2020). An Improved FOO Voting Scheme Using Blockchain. *Int. J. Inf. Secur.* 19 (3), 303–310. doi:10.1007/s10207-019-00457-8

Zou, X., Li, H., Li, F., Peng, W., and Sui, Y. (2017). Transparent, Auditable, and Stepwise Verifiable Online E-Voting Enabling an Open and Fair Election. *Cryptography* 1 (2), 13. doi:10.3390/cryptography1020013

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.