Open Access Library Journal
2022, Volume 9, e9010
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Design of a Secured Database System Using Blockchain Technology

Ignatius Chukwunwendu Ifedibasia, Moses Okechukwu Onyesolu, Daniel Ugoh

Department of Computer Science, Nnamdi Azikiwe University, Awka, Nigeria
Email: ignatiusifedibasia5@gmail.com, mo.onyesolu@unizik.edu.ng, d.ugoh@unizik.edu.ng

How to cite this paper: Ifedibasia, I.C., Onyesolu, M.O. and Ugoh, D. (2022) Design of a Secured Database System Using Blockchain Technology. *Open Access Library Journal*, **9**: e9010.
https://doi.org/10.4236/oalib.1109010

Received: June 16, 2022
Accepted: July 25, 2022
Published: July 28, 2022

Abstract

In this paper, a decentralized electronic voting system that provides inputs and outputs information support to admin/users in order to update their voting information while being capable of exhibiting different properties of blockchain security without the need for a third party. In this research, the Object Oriented Analysis and Design Methodology were adopted. The high level model of the proposed system was also designed and displayed in a format easily understandable to the user.

Subject Areas

Information Technology

Keywords

Database System, Blockchain, Voting System, Security, Decentralized, Transparency

1. Introduction

This paper presents the Design of a Secured Database System using Blockchain Technology.

A blockchain is a distributed, decentralized ledger or database that facilitates the process of recording transactions (digital events) in a business network [1]. In other words, a blockchain is a distributed, transactional database that is shared across all the nodes participating in a network. A transaction in the public ledger is verified by consensus of a majority of the participants in the network. Once the transaction is verified in the block and added to the blockchain, it is nearly impossible to erase or mutate the records. A transaction is the transfer of value between bitcoin wallets that gets included in the blockchain. Bitcoin wallets keep a secret piece of data called private key, which is used to sign transactions, providing mathematical proof that comes from the owner of the wallet. The signature also prevents the transaction from being altered by anybody once it has been issued. All transactions are broadcast to the network and usually begin to be confirmed within 10 - 20 minutes, through a process called mining.

Kiayias and Yung [2] proposed a self-tallying voting system that does not require any trusted third parties for vote aggregation and any private channel for voter-to-voter privacy but an important part of an election scheme, which is usually compromised in election protocol design in favor of others. Another scheme, Prêt à Voter based on Chaum [3], a new kind of receipt sets a far higher standard of security by letting voters verify the election outcome, even if all election computers and records were compromised. The system preserves ballot secrecy, while improving access, robustness, and adjudication, all at lower cost which was proposed in Chaum *et al.* [4] that ensures privacy by constructing the ballot with two columns, *i.e.* voting options are listed in one column and the voter's choice is entered in an adjacent column.

Adida and Rivest [5] proposed work based on Prêt à Voter but using homomorphic tabulation and it uses scratch stripes to allow off-line auditing of ballots. Bohli *et al.* [6] proposed that Bingo Voting was a verifiable and coercion-free voting scheme, which is based on a trusted random number generator which inhibits vote buying and intimidation because of its paper receipt. Adida [7] presented Helios, the first web-based, open-audit voting system which has cross scripting vulnerability. Chaum *et al.* [8] proposed Scantegrity that achieves end-to-end (E2E) verifiability with confirmation codes that allow voters to prove to themselves that their ballots are included in the final tally as they really are but it still has design flaws and vulnerabilities. Sandler *et al.* [9] developed the VoteBox, a complete electronic voting system that combines several recent e-voting research results into a coherent whole that can provide strong end-to -end security guarantees to voters. VoteBox machines are locally networked and all critical election events are broadcast and recorded by every machine on the network.

Hao *et al.* [10] proposed a two round protocol that computes the tally in two rounds without using a private channel or a trusted third party which provides exceptional efficiency compared to related techniques. It places considerable pressure on the electoral administration by requiring it to run a second election a short time after the first, thus significantly increasing both the cost of the overall election process and the time that elapses between the holding of an election and the declaration of a result. According to Khader *et al.* [11], a protocol was proposed to improve the robustness and fairness of the two round protocols. Bell *et al.* [12] proposed STAR-Vote. A secure, transparent, auditable, and reliable voting system which is a collaboration between a number of academics and the Travis County (Austin), Texas elections office, which currently uses a DRE voting system and previously used an optical scan voting system. Straight Party Voting (SPV) still needs to be addressed in order to make the system have the highest usability.

Hao *et al.* [13] proposed a new End-to-End (E2E) verifiable e-voting protocol for large-scale elections, called direct recording electronic with integrity (DRE-i). While the removal of tallying authorities in DRE-i significantly simplifies election management, the pre-computation of ballots necessitates secure ballot storage, as leakage of pre-computed ballots endangers voter privacy.

Shahandashti and Hao [14] proposed an E2E verifiable voting system named DRE-ip (DRE-i with enhanced privacy), that overcomes limitations of DRE-i [8]. Furthermore, Choi *et al.* [15] proposed a blockchain-based e-voting system that provides voter anonymity by issuing a voter certificate based on a blockchain address which makes it less decentralized, with no transparency because it's not open to the public. Finally, Koussema and Haga, H. [16] presented the design and implementation of a highly secure and reliable database system for resident records management system using blockchain technology. Prototype development proved the possibility to use the blockchain technology for a large amount of data management systems with highly secure and reliable features.

This paper is divided into different sections as follows: Section 1 contains the introduction, Section 2 presents a brief review of previous approaches relating to the study area and the gap in exploring the proposed model; Section 3 introduces materials and methods employed for developing the model; Section 4 focuses on the results and detailed discussion of results; Section 5 presents the conclusion to the paper.

2. Related Works

Kiayias and Yung [2] proposed a self-tallying voting system that does not require any trusted third parties for vote aggregation and any private channel for voter-to-voter privacy. In this work, they introduced a new election paradigm with strong voter privacy as its primary objective. The paradigm is built around three useful properties of voting schemes which are:

1) Perfect Ballot Secrecy; ensures that knowledge about the partial tally of the ballots of any set of voters is only computable by the coalition of all the remaining voters (this property captures strong voter privacy as understood in real world elections).

2) Self-tallying; suggests that the Post-ballot-casting phase is an open procedure that can be performed by any interested (casual) third party.

3) Dispute-freeness; suggests that disputes between active parties are prevented altogether, which is an important efficient integrity component. They presented a novel voting scheme which is the first system that is dispute-free, self-tallying and supports perfect ballot secrecy. Their design paradigm obviates the need for voter-to-voter interaction (due to its dispute-freeness and publicly verifiable messages), and in addition their paradigm suggests a novel "corrective fault tolerant" mechanism. This mechanism neutralizes faults occurring before and after ballot casting, while self-tallying prevents further faults. Additionally,

the mechanism is secrecy-preserving and "adaptive" in the sense that its cost is proportional to the number of faulty participants. As a result, their protocol is more efficient and robust than previous schemes that operate (or can be modified to operate) in the perfect ballot secrecy setting.

Another scheme Prêt à Voter based on Chaum [3], a new kind of receipt sets a far higher standard of security by letting voters verify the election outcome, even if all election computers and records were compromised. The system preserves ballot secrecy, while improving access, robustness, and adjudication, all at lower cost proposed in Chaum *et al.* [4]. It ensures privacy by constructing the ballot with two columns *i.e.* voting options are listed in one column and the voter's choice is entered in an adjacent column. Chaum *et al.* [4] presented an election scheme designed to allow voters to verify that their vote is accurately included in the count. The scheme provides a high degree of transparency whilst ensuring the secrecy of votes. Assurance is derived from close auditing of all the steps of the vote recording and counting process with minimal dependence on the system components. Thus, assurance arises from verification of the election rather than having to place trust in the correct behavior of components of the voting system. The scheme also seeks to make the voter interface as familiar as possible.

Adida and Rivest [5] proposed work based on Prêt à Voter but using homomorphic tabulation. It uses scratch stripes to allow off-line auditing of ballots. They presented Scratch & Vote (S&V), a cryptographic voting system designed to minimize cost and complexity.

1) Ballots are paper-based and can be printed using today's technology

2) Ballots are universally verifiable without election official intervention, and

3) Tallying requires only one trustee decryption per race.

Scratch and Vote combines the multi-candidate election techniques of Baudron *et al.* [17] with the ballot-casting simplicity of Chaum and Ryan's paper-based techniques. In addition, S&V allows each voter to participate directly in the audit process on Election Day, prior; to casting their own ballot.

Bohli *et al.* [6] proposed Bingo Voting. This is a secure and coercion-free voting using a trusted random number generator. Their work presented a new verifiable and coercion-free voting scheme Bingo Voting, which is based on a trusted random number generator. As a motivation for the new scheme two coercion/vote buying attacks on voting schemes are presented which show that it can be dangerous to let the voter contribute randomness to the voting scheme. A proof-of-concept implementation of the scheme shows the practicality of the scheme: all costly computations can be moved to a non-time critical pre-voting phase.

Adida [7] presented Helios. Helios is the first web-based, open-audit voting system. Helios is publicly accessible today: anyone can create and run an election, and any willing observer can audit the entire process. Helios is ideal for online software communities, local clubs, student government, and other environments where trustworthy, secret ballot elections are required but coercion is not a serious concern. With Helios, they hoped to expose many to the power of open-audit elections.

Chaum *et al.* [8] proposed Scantegrity that achieves end-to-end (E2E) verifiability with confirmation codes that allow voters to prove to themselves that their ballots are included in the final tally as they really are. Scantegrity is a security enhancement for optical scan voting systems. It's part of an emerging class of "end-to-end" independent election verification systems that permit voters to verify that their ballot was correctly recorded and counted. On the Scantegrity ballot, each candidate position is paired with a random letter. Election officials confirm receipt of the ballot by posting the letter that is adjacent to the marked position. Scantegrity is the first voting system to offer strong independent verification without changing the way voters mark optical scan ballots, and it complies with legislative proposals requiring "unencrypted" paper audit records.

Sandler *et al.* [9] developed the VoteBox, a complete electronic voting system that combines several recent e-voting research results into a coherent whole that can provide strong end-to-end security guarantees to voters. VoteBox machines are locally networked and all critical election events are broadcast and recorded by every machine on the network. VoteBox network data, including encrypted votes, can be safely relayed to the outside world in real time, allowing independent observers with personal computers to validate the system as it is running. They also allow any voter to challenge a VoteBox, while the election is ongoing, to produce proof that ballots are cast as intended. The VoteBox design offers a number of pragmatic benefits that can help reduce the frequency and impact of poll worker or voter errors.

Hao *et al.* [10] proposed a two round protocol that computes a tally in two rounds without using a private channel or a trusted third party which provides exceptional efficiency compared to related techniques. In this work, they added a self-tallying function to the anonymous veto network (AV-net), making it a general-purpose voting protocol. The new protocol works in the same setting as the AV-net as it requires no trusted third parties or private channels, and participants execute the protocol by sending 2-round public messages. Compared with related voting protocols in past work, theirs is significantly more efficient in terms of the number of rounds, computational cost and bandwidth usage but is neither robust nor fair in certain conditions [11].

Khader *et al.* [11] proposed a protocol to improve the robustness and fairness of the two round protocols. However, the protocol has two drawbacks. First, if some voters abort then the election result cannot be announced, that is, the protocol is not robust. Secondly, the last voter can learn the election result before voting, that is, the protocol is not fair. Both drawbacks are typical of other decentralized e-voting protocols. Their paper addresses these issues: they proposed a recovery round to enable the election result to be announced if voters abort and they added a commitment round to ensure fairness. In addition, they provide a computational security proof of ballot secrecy.

Bell *et al.* [12] proposed STAR-Vote. This is a secure, transparent, auditable, and reliable voting system which is collaboration between a number of academics and the Travis County (Austin), Texas elections office, which currently uses a DRE voting system and previously used an optical scan voting system. STAR-Vote represents a rare opportunity for a variety of sophisticated technologies, such as end-to-end cryptography and risk limiting audits, to be designed into a new voting system, from scratch, with a variety of real world constraints, such as election-day vote centers that must support thousands of ballot styles and run all day in the event of a power failure. This paper describes the current design of STAR-Vote which is now largely settled.

Hao *et al.* [13] proposed a new End-to-End (E2E) verifiable e-voting protocol for large-scale elections, called Direct Recording Electronic with Integrity (DRE-i). In contrast to all other E2E verifiable voting schemes, theirs does not involve any Tallying Authorities (TAs). The design of DRE-i is based on the hypothesis that existing E2E voting protocols' universal dependence on TAs is a key obstacle to their practical deployment. In DRE-i, the need for TAs is removed by applying novel encryption techniques such that after the election multiplying the ciphertexts together will cancel out random factors and permit anyone to verify the tally. They described how to apply the DRE-i protocol to enforce the tallying integrity of a DRE-based election held at a set of supervised polling stations. Each DRE machine directly records votes just as the existing practice in the real-world DRE deployment. But unlike the ordinary DRE machines, in DRE-i the machine must publish additional audit data to allow public verification of the tally.

If the machine attempts to cheat by altering either votes or audit data, then the public verification of the tallying integrity will fail. To improve system reliability, they further present a fail-safe mechanism to allow graceful recovery from the effect of missing or corrupted ballots in a publicly verifiable and privacy-preserving manner. Finally, they compare DRE-i with previous related voting schemes and show several improvements in security, efficiency and usability. This highlights the promising potential of a new category of voting systems that are E2E verifiable and TA-free. They called this new category "self-enforcing electronic voting".

Shahandashti and Hao [14] proposed end-to-end (E2E) verifiable voting system named direct recording electronic with integrity and enhanced privacy (DRE-ip), that overcomes limitations of DRE-i [8]. Instead of pre-computing cipher texts, DRE-ip encrypts the vote on the fly during voting process. DRE-ip achieves E2E verifiability without tallying authorities (TAs), but at the same time provides a significantly stronger privacy guarantee than DRE-i. In Chaum [3] end-to-end verifiability is achieved through the Mixnet protocol that recovers the plaintext ballot in an unlikable manner by randomizing the cipher-text through a chain of mix servers. Nearly all verifiable e-voting schemes require trustworthy authorities to perform the tallying operations.

An exception is the DRE-i system which removes this requirement by pre-computing all encrypted ballots before the election using random factors that will later cancel out and allow the public to verify the tally after the election.

While the removal of tallying authorities significantly simplifies election management, the pre-computation of ballots necessitates secure ballot storage, as leakage of pre-computed ballots endangers voter privacy. Their work addressed this problem and proposed DRE-ip (DRE-i with enhanced privacy). Adopting a different design strategy, DRE-ip was able to encrypt ballots in real time in such a way that the election tally can be publicly verified without decrypting the cast ballots. As a result, DRE-ip achieves end-to-end verifiability without tallying authorities, similar to DRE-i, but with a significantly stronger guarantee on voter privacy. In the event that the voting machine is fully compromised, the assurance on tallying integrity remains intact and the information leakage is limited to the minimum: only the partial tally at the time of compromise is leaked.

Choi *et al.* [15] proposed a blockchain-based e-voting system that provides voter anonymity by issuing a voter certificate based on a blockchain address. Their paper applies the critical encryption technique to the blockchain and satisfies the requirements for voting such as verifiability, anonymity, fairness, non-reusability, competence, safety, transparency, and non-ticketing with propose system design and implementation method. The e-voting election monitoring committee generates a threshold group encryption key, and the proposed blockchain based e-voting system guarantees confidentiality by a threshold group encryption algorithm during the voting process. The voting result is encrypted through a homomorphic encryption algorithm and stored in the blockchain. Thus, the released voting results ensure safety, confidentiality, transparency, and non-vote ticketing. In addition, the proposed blockchain-based e-voting system guarantees the unity and competence of voting through the blockchain's smart contract.

Koussema and Haga, H. [16] presented the design and implementation of highly secure and reliable database system for resident records management system using blockchain technology. In their prototype, each event of resident such as birth, moving, employment and so on, is assigned to data fragment and certain amount of data fragment, says 20 fragments were packed into block. They also developed the web application interface to avoid installing any applications in users' PC or smartphone. Prototype development proved the possibility to use the blockchain technology to large amount of data management system with highly secure and reliable features.

3. Materials and Methods

Blockchain technology works by creating an environment that is secure and transparent for the financial transactions of virtual values such as bitcoin. Hash codes of each block keep records safe in the blockchain. This is mainly because irrespective of the size of the information or document, the mathematical hash function provides a hash code of the same length for each block. So, attempting to change a block of information would generate a completely new hash value [18].

A network that is open to everyone and concurrently maintains user's anonymity undoubtedly raises trust issues regarding the participants. So, to build the trust the participants need to go through several consensus algorithms such as Proof of Work and Proof of Stake. The digital cryptocurrency bitcoin uses the first-ever blockchain technology [19]. It is a digital store of value that enables peer to peer transactions over the internet without the intervention of a third party. The blockchain network is a decentralized structure that consists of scattered nodes (computers) that inspect and validate the authenticity of any new transactions that attempt to take place. This combine agreement is done through several consensus models by the process of mining. The process of mining demonstrates that each node trying to add a new transaction has gone through and solved the complex computational puzzle through extensive work and deserves to get a reward in return for their service.

For the validation of a transaction, the network must confirm the following conditions: The sender account holds sufficient bitcoin balance that it intends to transfer. The amount intended to transfer has not already been sent to some other recipient. Once a transaction has been validated and agreed upon by all the nodes, it then gets added to the digital ledger and protected using cryptography that uses a public key that is accessible to all the other nodes and a private key that must be kept secret [20]. **Figure 1** shows the transaction process in blockchain network. To maintain the transactions using digital currency in the blockchain network, one need to have an understanding of the digital wallet which is used to store, send, and receive digital currency. A digital wallet or a cryptocurrency wallet is a string of letters and numbers forming a public address associated with each block in the blockchain. This public address is used whenever a transaction takes place; that is, the bitcoin currency is assigned to the public address of the specific wallet. However, to prove the ownership of the public address there is a private key associated with the wallet that serves as the user's digital signature that is used to confirm the processing of any transaction. The user's public key is the shortened version of his/her private key generated through complex and advanced mathematical algorithms [21].

For example, let us consider someone is trying to send you some digital currency such as bitcoin, as the transaction is being processed, the private key in your wallet should match the crucial public address of your wallet that the currency has been assigned to. If both these keys match, then the digital currency amount is transferred to the public address of your wallet.

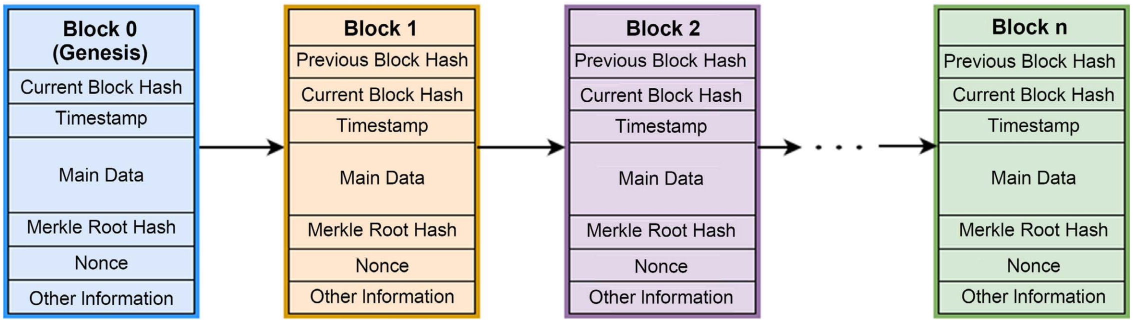

Figure 1. A sequence of blockchain showing block structure [18].

Main data: Blocks will contain transaction data. This transaction data depends on the usage factor of blockchain, that is, the relevant services for which the blockchain is implemented. For financial institutions like banks, financial transaction data will be stored.

Timestamp: The timestamp will also exist in the blocks. Here, the timestamp refers to the date and time when a particular block is generated.

Hash: The hash corresponding to each block is a unique identifier that is generated using a cryptographic hash algorithm such as SHA-256. Hash of the current block and hash of the previous block will be stored in the block. Hashes make the blocks immutable. Hashes are generated using the Merkle tree function. It is stored in the header of the block.

Merkle tree root hash: It consists of all the hash values relating to every transaction that took place in a block and performs a mathematical hash calculation generating a 64-character code [22]. The hash of the Merkle tree root of all the transactions in the block is stored for effective processing and easier verifying of data within a short time.

Nonce: A nonce is a randomly generated 4-byte number that can be used once in a cryptographic transaction process. During the mining process in a Proof-of-Work algorithm, the nonce is used as a counter that the miners are trying to solve in order to generate a new block. The aim is to calculate a hash value less than a given target value, which depends on the difficulty of the complex mathematical problem.

Block properties: Each block inside blockchain mainly consists of three parts, such as Hash of the previous block, Data, hash of current block as shown in **Figure 1**. Data on the block can be anything. It can be transaction records, medical records, insurance records, law records, property ownership records, etc.

The methodology that is adopted in this work is Object Oriented Analysis and Design Methodology (OOADM). Object Oriented Analysis and Design Methodology (OOADM) is the principal industrial proven methodology for developing high quality object oriented systems.

The prevailing software development methodology involves three aspects:

1) Object Oriented Analysis (OOA) which deals with the design requirement and the overall architecture of a system and is focused on describing what the system should do in terms of key object in the problem domain.

2) Object Oriented Design (OOD) which translates system architecture into programming constructs (such as interface, classes, and method descriptions).

3) Object Oriented Programming (OOP) which implements these programming constructs.

The fundamental idea behind an object oriented language is object decomposition, breaking, combining the data and functions that operate on that data into a simple unit, the object are discussed and built by modeling real world instance. Object Oriented Analysis and Design Methodology (OOADM) was adopted because it will help in studying the existing system into a useful application, easier maintenance since objects may be understood as stand-alone entities and objects are potentially reusable component.

The proposed system consists of nodes (computers in design) that are closed to human interference. Any input that cannot be considered as vote will be ignored in this system. For such a system, stealing votes or changing votes are totally blocked. Second issue is saving system from hackers. In order to manipulate votes, hackers need to enter the system as a citizen at proposed solution. Also, it is guaranteed that a citizen can only vote for one time. Although a hacker may obtain the citizen information and entered into the system, he cannot vote more than one time.

In a blockchain system, every transaction is related to the previous one. So, changing an accepted transaction is impossible for such a system. Due to the consistency of the blockchain, data will always be consistent and voting will be reliable. In a case of manipulation of the system such as changing votes or stealing votes, other connected nodes will already be synchronized. So, the changed data will be identified instantly. After citizen's vote, it is added to the blockchain. Any vote has a guarantee from the system about being immutable. During the voting process, in the voting transaction each voter receives the transaction ID of their vote. Using this transaction ID in this work, decentralized electronic voting system, voters can use a blockchain explorer (Metamask serves as the ethereum browser) to go to an official election site and find the transaction with the corresponding transaction ID on the blockchain. Instead, on the blockchain, voters can see their votes, and verify that the votes were registered and counted correctly. This authentication process satisfies the transparency criteria, while minimizing the traceability of votes.

The proposed system is designed to use electronic Identification or passwords to authenticate the elector in order to introduce a form of secure authentication.

Figure 2 describes the detailed processing:

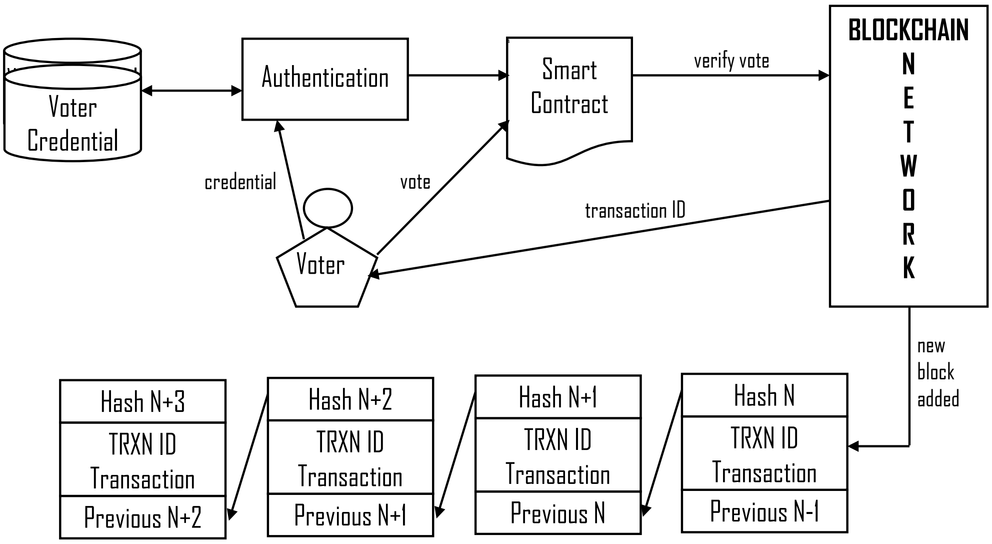

Figure 2. Voting process.

1) The system verifies the credentials of the voter.

2) After the positive authentication, the corresponding smart contract is prompted for continued voting. Candidates are listed on smart contract. A voter may choose to do so.

3) When a candidate has been selected by a voter he or she proceeds to sign its vote.

4) When the vote is verified as valid, consensus has been reached on the particular vote. The elector receives a transaction identification of his corresponding vote.

5) The vote will then be added to the block after the verification.

Figure 3 shows the overall working of proposed system.

3.1. Class Diagram

The proposed system is made up of six (6) classes containing all of the information required to manipulate a given object as shown in Figure 4.

Figure 4 is the class diagram of the proposed system. It shows the building blocks of a secured database system using blockchain technology. This class diagrams depict the static view of the model or part of the model, describing what attributes and behavior it has rather than detailing the methods for achieving operations. In Figure 4, the following classes are depicted:

1) Voting class

2) Dashboard class

3) Result class

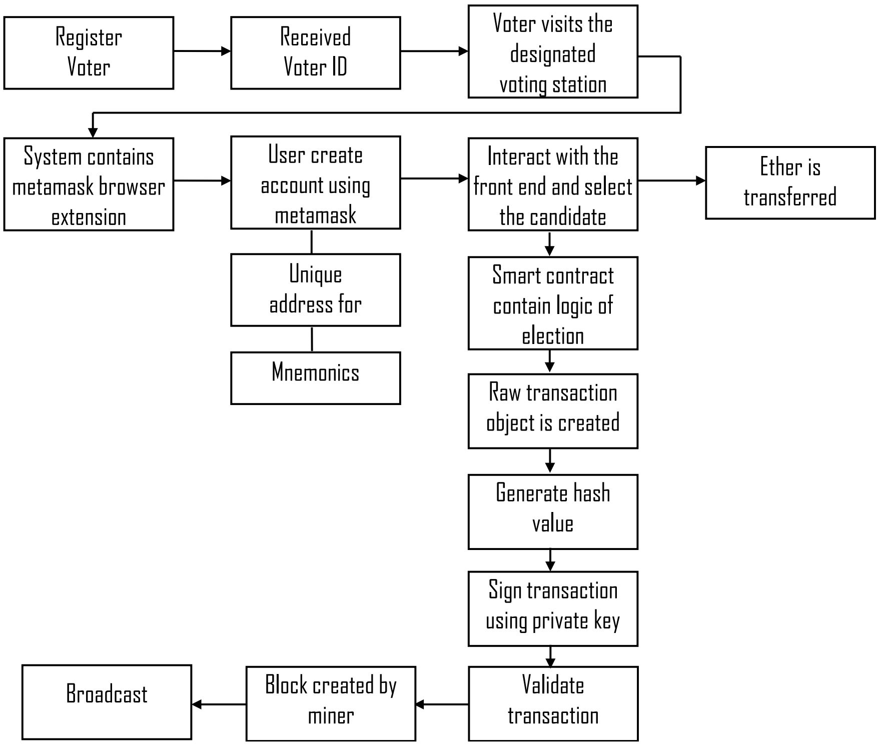
Register Voter
Received Voter ID
Voter visits the designated voting station
System contains metamask browser extension
User create account using metamask
Interact with the front end and select the candidate
Ether is transferred
Unique address for
Mnemonics
Smart contract contain logic of election
Raw transaction object is created
Generate hash value
Sign transaction using private key
Validate transaction
Block created by miner
Broadcast

Figure 3. Overall working of proposed system.

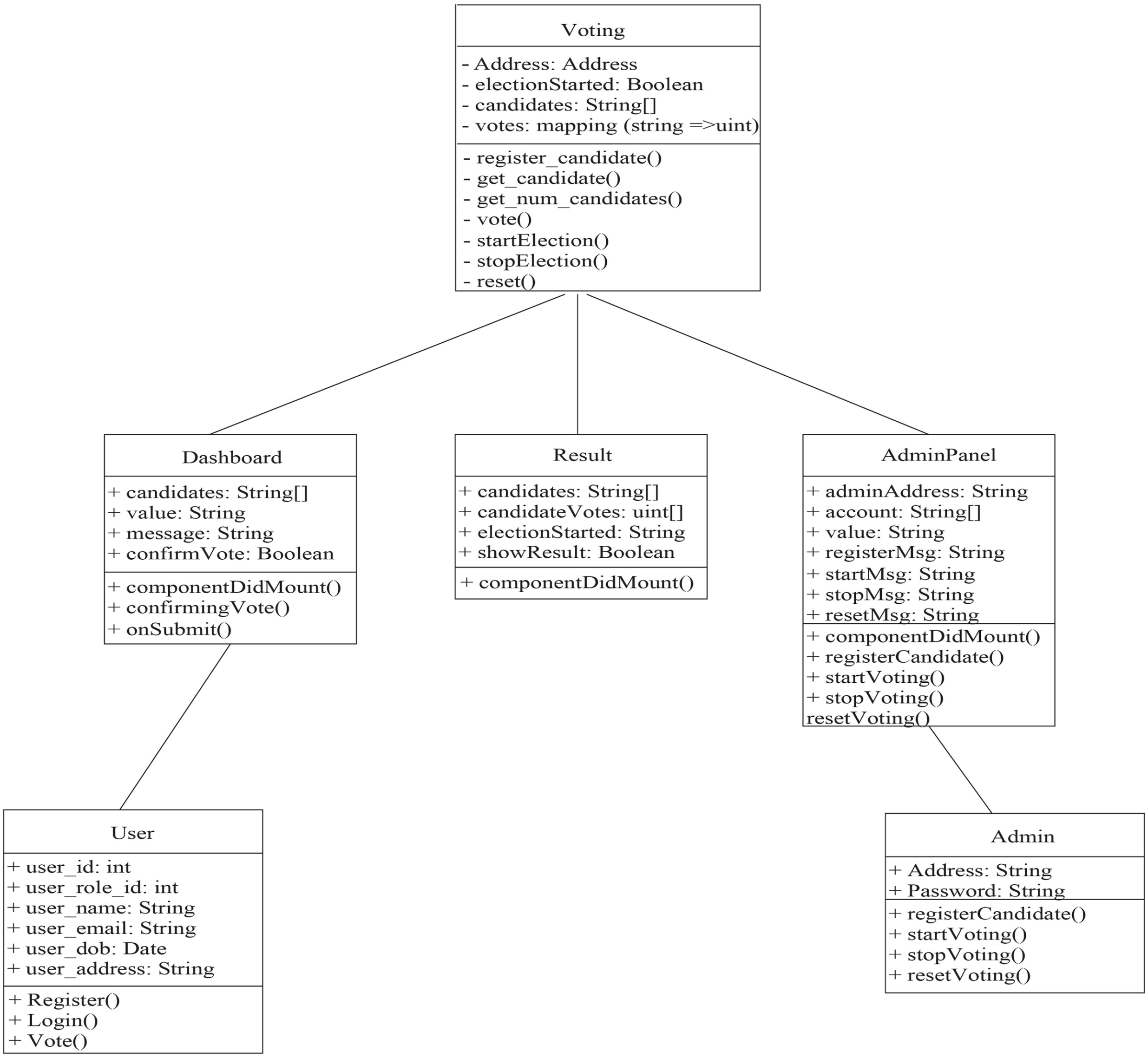

Figure 4. Class diagram.

4) AdminPanel class

5) User class

6) Admin class

Each class contains various attributes and methods (Functions) which call other class attributes to share data.

1) Voting class contains attributes such as address, electionStarted, candidates, votes and functions such as register_candidate, get_candidate, get_run_candidate, vote, startElection, stopElection and reset.

2) Dashboard class contains attributes such as candidate, value, message, confirmVote and functions such as componentDidMount, confirmingVote and onSubmit.

3) Result class contains attributes such as candidate, candidateVote, electionStarted, showResult and functions such as componentDidMount.

4) AdminPanel class contains attributes such as adminAddress, account, value, registerMsg, startMsg, stopMsg, resetMsg and functions such as componentDidMount, registerCandidate, startVoting, stopVoting and restVoting.

5) User class contains attributes such as user_id, user_role_id, user_name, user_email, user_dob, user_address and functions such as register, login and vote.

6) Admin class contains attribute such as address, password and functions like registerCandidate, startVoting, stopVoting and resetVoting.

In Figure 4, the Admin register candidate through the admin panel of the voting system and has the ability to start, stop as well as reset voting and view result. User on the other hand has the ability to register through the dashboard of the voting system, login with their credential and vote his/her desired candidate.

3.2. Use Case Diagram

Use case diagram was also used in the modeling of the new system. Use case modeling is the process of modeling a system's functions in terms of business events, who initiated the events, and how the system responds to the events. Use case is a behaviorally related sequence of steps (a scenario), both automated and manual, for the purpose of completing a single business task. Use cases are initiated or triggered by external users or systems called actors. An actor represents anything that needs to interact with the system to exchange information. An actor is a user, a role, which could be an external system as well as a person. Figure 5 shows the Use Case diagram of the new system. Here, the voter will be able to

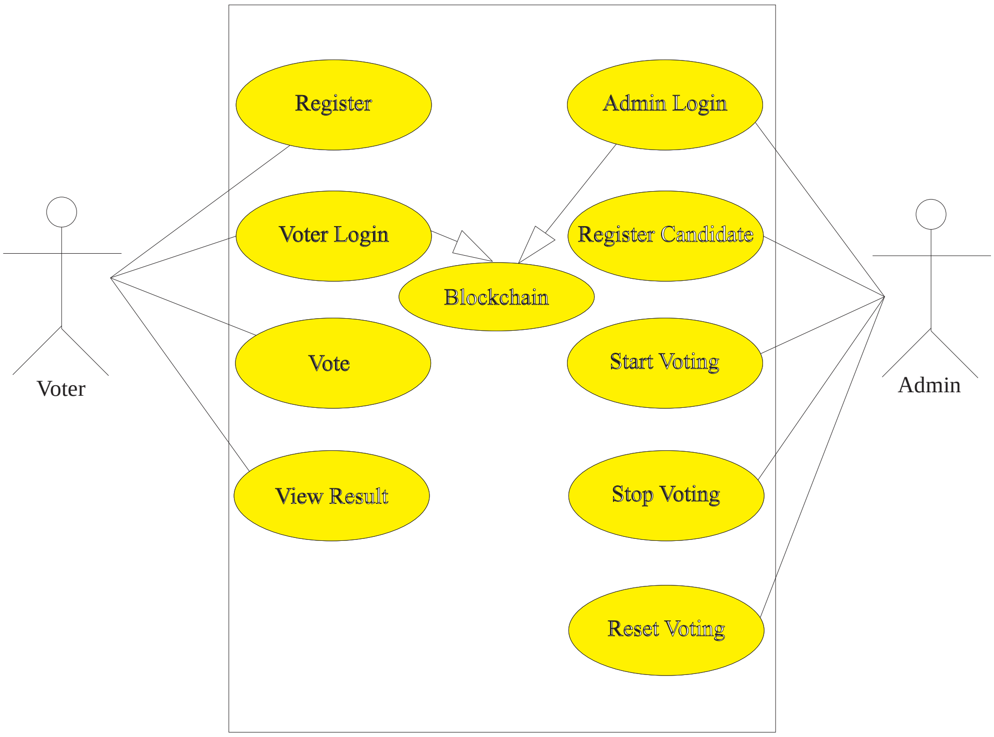

Figure 5. Use case diagram.

register, login with their details, vote and view result. Admin will be able to login with their details, register candidate, and start voting, stop voting and reset voting. It is guaranteed that voter can only select their desired candidate and vote once.

3.3. Activity Diagram

Figure 6 shows the activity diagram of the new system. The activity diagram of the new system shows the steps involved in designing the program intended to derive the new model for a secured database system using blockchain technology. It shows how the new system will perform. The system starts by creating user account and its types (admin or voter), if this process is successful, the user is prompted to put in login details usually their username and password. If the correct password is entered the admin/voter will have access to their displayed user interface respectively to select and vote their desired candidate with a feedback mechanism. The admin has the option of adding candidate, start, stop and reset voting.

3.4. Sequence Diagram

Figures 7-9 depict the sequence diagram of the new system. It shows objects as

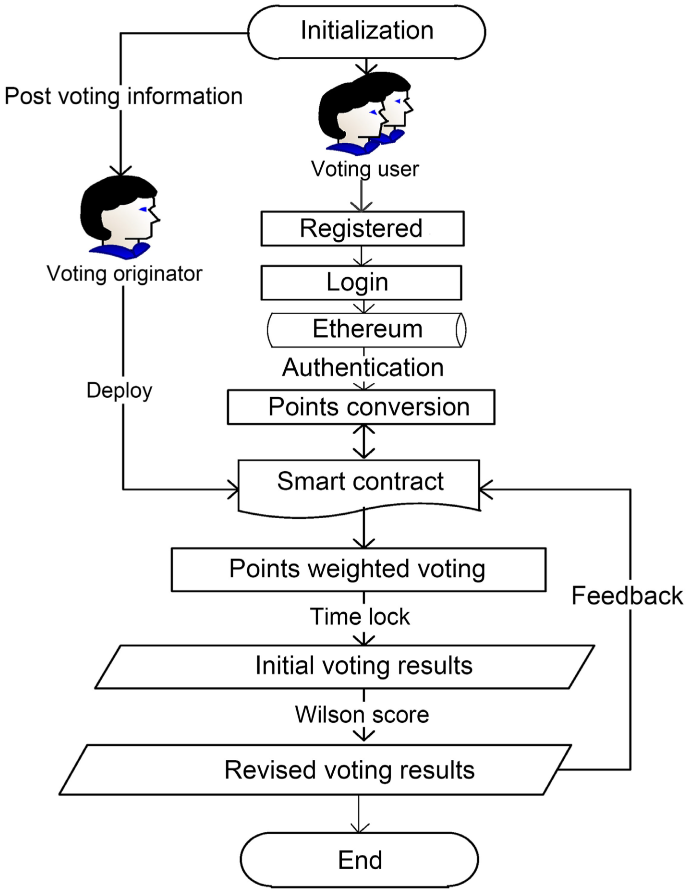

Figure 6. Activity diagram.

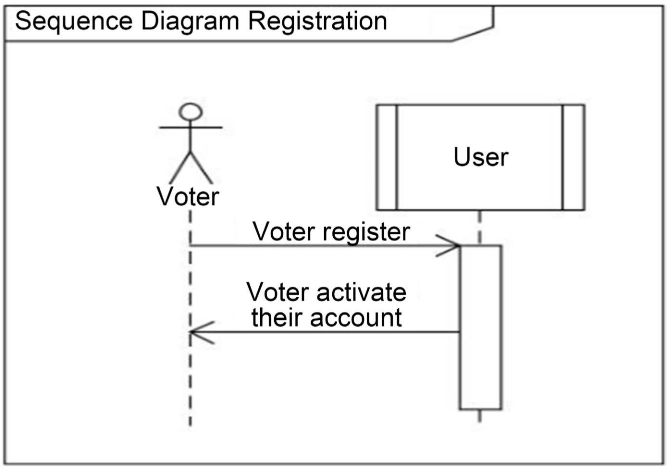

Figure 7. Sequence diagram for Registratio.

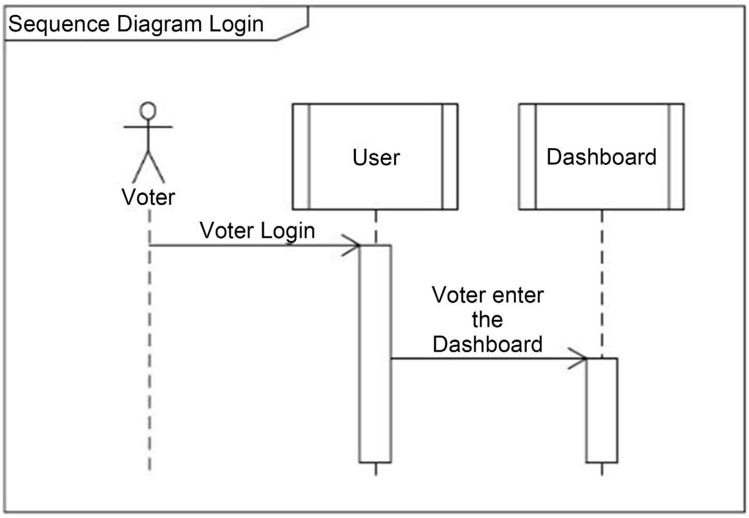

Figure 8. Sequence diagram for login.

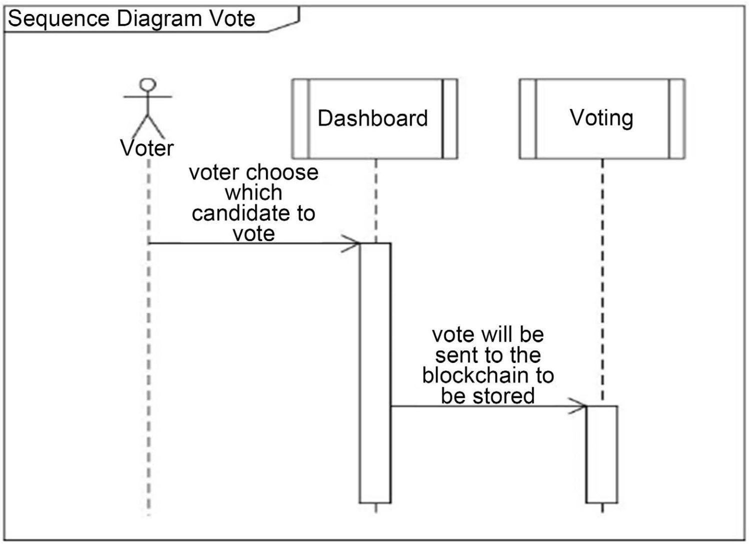
Sequence Diagram Vote
Voter
Dashboard
Voting
voter choose which candidate to vote
vote will be sent to the blockchain to be stored

Figure 9. Sequence diagram for vote.

lifelines running down the page and with their interactions over time represented as messages drawn as arrows from the source lifeline to the target lifeline. Sequence diagrams are good at showing which objects communicate with which other objects and what messages trigger those communications. Here, Figure 7 depicts the sequence diagram for voter registration where by the voter activates his/her account. Figure 8 depicts the sequence diagram for voter login with his/her details through the dashboard. Finally, Figure 9 depicts sequence diagram for vote whereby the voter choose which candidate to vote, after which will be sent to the blockchain to be stored.

3.5. Collaboration Diagram

In modeling the new system, collaboration diagram will be used (Figure 10). Collaboration diagrams show how messages flow between objects in an object oriented application and also imply the basic associations (relationships) between classes. Messages are added to the associations and are shown as short arrows pointing in the direction of the message flow. The sequence of messages is shown through a numbering scheme. The collaboration begins with the voter registration through the dashboard after which he/she can login to the system; once the login is successful the system will display receipt showing that the login was successful, then the voter can now caste his/her vote to desired candidate which will be processed in the ethereum smart contract as well as communicate

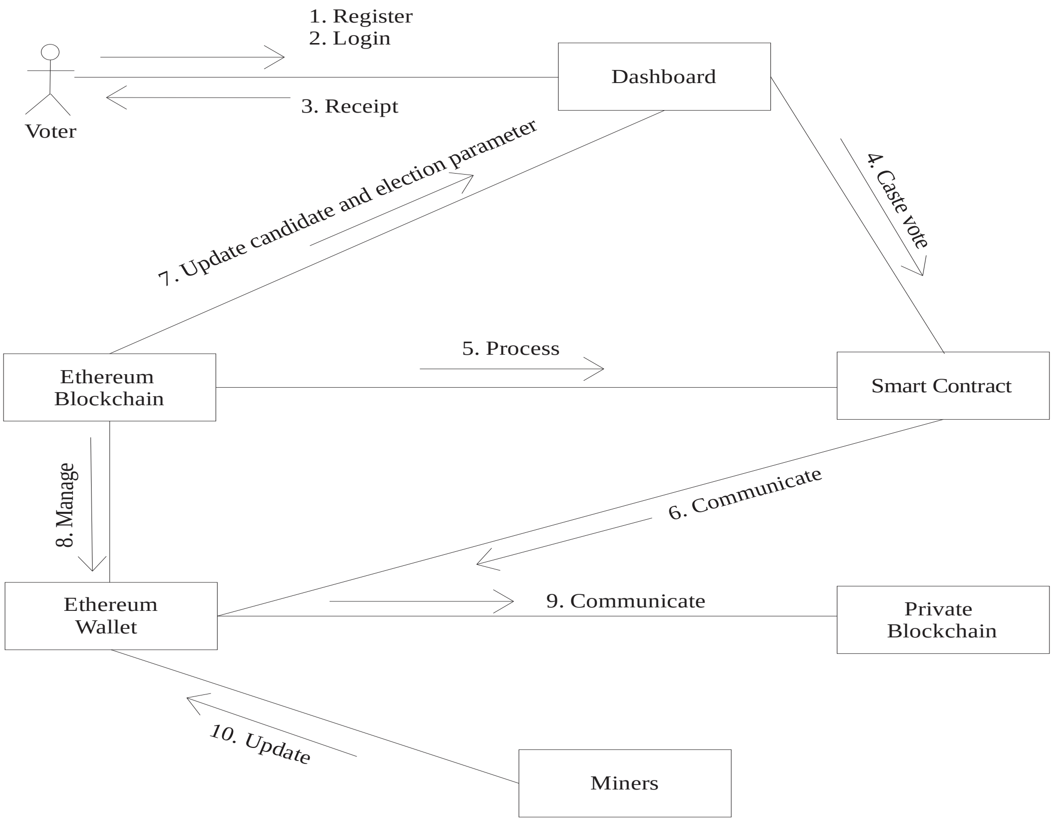

Figure 10. Collaboration diagram.

with the ethereum wallet. Ethereum blockchain update candidate and election parameter through the dashboard and manages ethereum wallet which communicate directly with the private blockchain and updated by miners. Figure 10 shows the collaboration diagram of the proposed system.

3.6. Dataflow Diagram

Figure 11 depicts dataflow diagram of the proposed system. Dataflow diagram (DFD) will be used to model the new system by showing the graphical representation of the flow of data through an information system, modeling its process aspects. Dataflow diagram shows the way information flow through a process or system. It includes inputs and output, data stores and various sub processes the data moves through. Here, dataflow diagram begins with voter registration and login with his/her detail after successful authentication the system display receipt showing that login was successful, then the voter can now caste his/her vote to desired candidate which will be processed in the ethereum smart contract as well as communicate with the ethereum wallet. Etherum blockchain update candidate and election parameter through the dashboard and manages ethereum wallet which communicate directly with the private blockchain and updated by miners. Figure 11 shows the dataflow diagram of the proposed system.

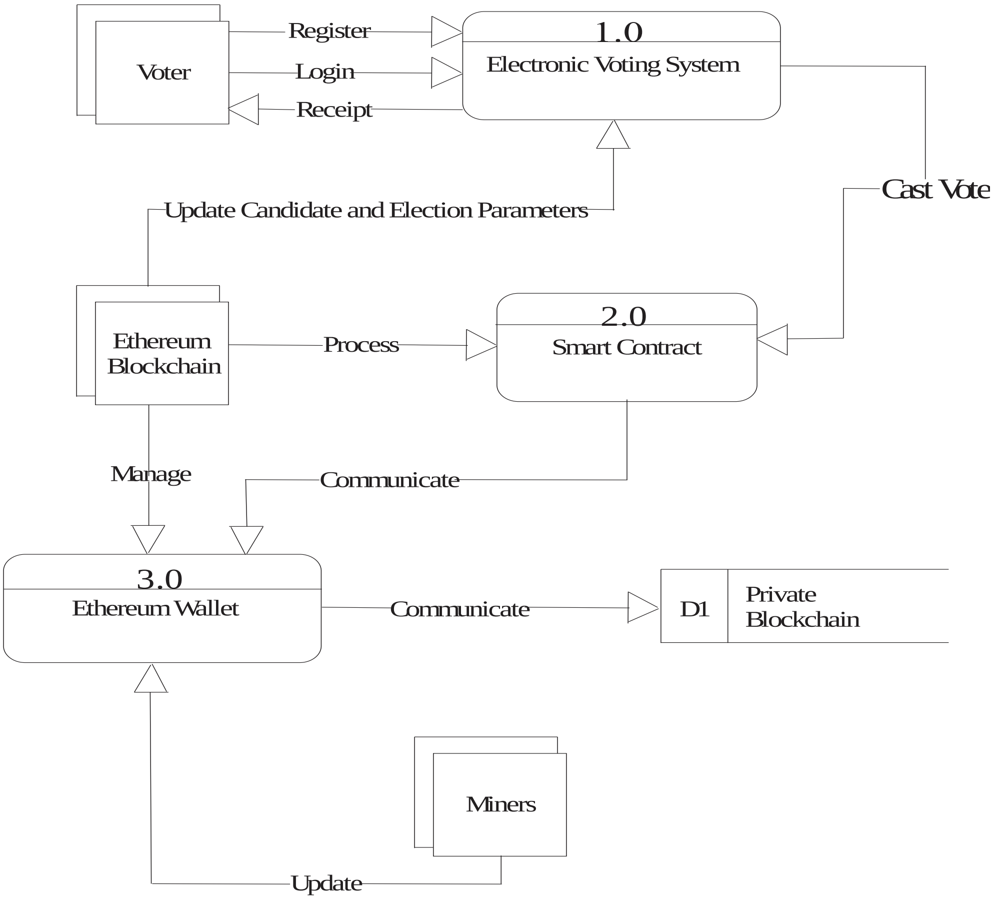

Figure 11. Dataflow diagram.

3.7. Package Diagram

Figure 12 depicts package diagram of the proposed system. Package diagram will be used to model the new system by showing organization and arrangement of various model elements in the form of packages. A package will be used in grouping of related unified modeling language (UML) elements, such as diagrams, documents, classes, or even other packages. Each element is nested within the package, which is depicted as a file folder, then arranged hierarchically within the diagram. Package diagram is used to simplify complex class diagrams; you can group classes into packages.

Here, package diagram begins with decentralized electronic voting system which comprises other packages such as E_voting, interface, voter and administrator package. Interface package is further broken down into three packages such as Dashboard_Interface, Result_Interface, and AdminPanel_Interface with corresponding classes such as Dashboard, Result and AdminPanel respectively. The packages such as E_voting, voter and administrator have classes such as voting, user and admin respectively. Here, package diagram begins with voter registration and login with his/her detail, after successful authentications, then the voter can caste his/her vote to desired candidate which will be shown/view through Result_Interface. Administrator on the other hand can as well view the

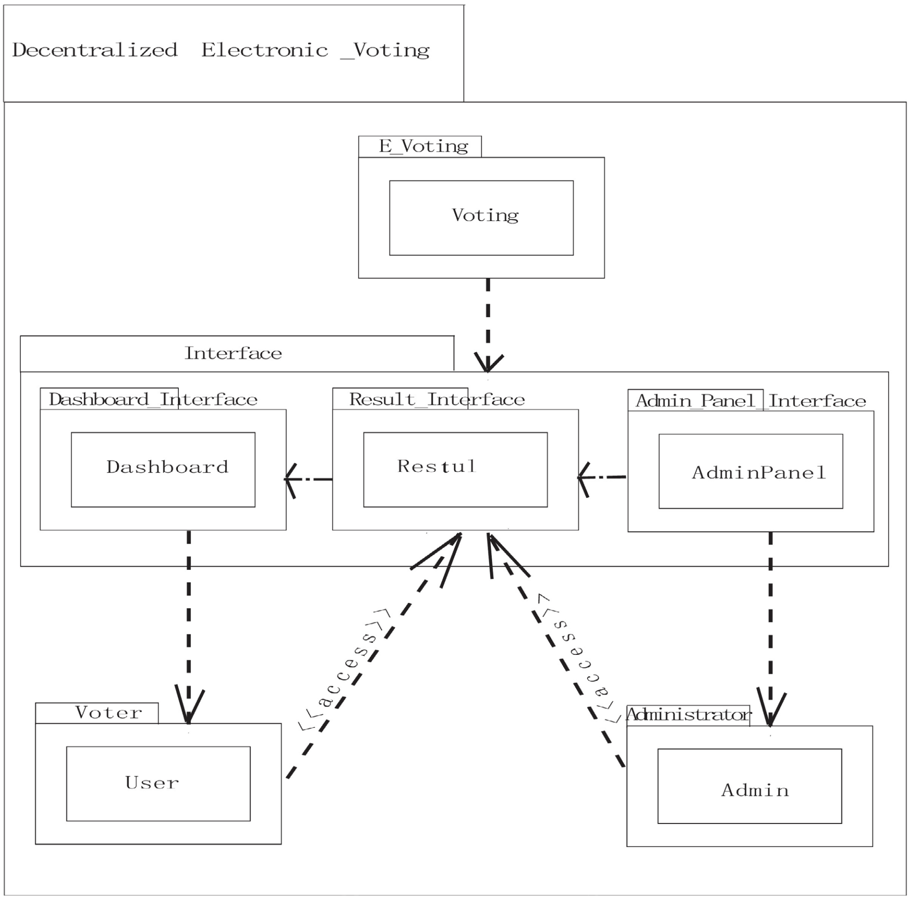

Figure 12. Package diagram.

result after successful login through the AdminPanel_Interface. Figure 12 shows the package diagram of the propose system.

3.8. Overall Working of Proposed System

Figure 3 depicts the overall working of proposed system whereby a voter goes to the system, gets registered as well as received voter ID which helps him/her to go to a designated voting station consisting of metamask browser where account was created and interact with the front end and select a desired candidate. Here, ether is transferred to the wallet of the candidate. Smart contract contain logic of election where raw transaction object is created generating hash value that can be signed using private key as well as validate transaction after which block is created by miner and broadcast to the entire node in the blockchain.

3.9. Advantages of the Proposed System

Figure 2 depicts the voting process of the new system through which different advantages were achieved as follows:

1) Transparency in the voting process;

2) No vote tampering or manipulation;

3) Faster and accurate results;

4) Online voting will encourage more people to participate in the democratic process;

5) Increases trust as well as security in voting process;

6) Traceability of data in the voting process shared across a business network and delivers cost savings with new efficiencies.

Furthermore, data required during registration in the form of voter collection form includes unique ID which is a unique code generated from the system, first name, middle name, last name, date of birth, sex, marital status, disability, address, phone number, local government area (LGA), and state of origin.

3.10. High Level Model of the Proposed System

The high level model represents the overall structure of the new system comprising the major components or modules of the software. The following represents the high level model of the system that is being developed; the top-down high level model is shown in Figure 13.

4. Results and Discussion

We have considered several methods to compare our proposed system against existing systems.

In our proposed system, blockchain method was used to create an environment that is secured and transparent for decentralized electronic voting system whereby the hash code of each block keeps record safe and as well make the blocks immutable. So, to build the trust the participants need to go through several consensus algorithms such as Proof of Work and Proof of Stake. Furthermore,

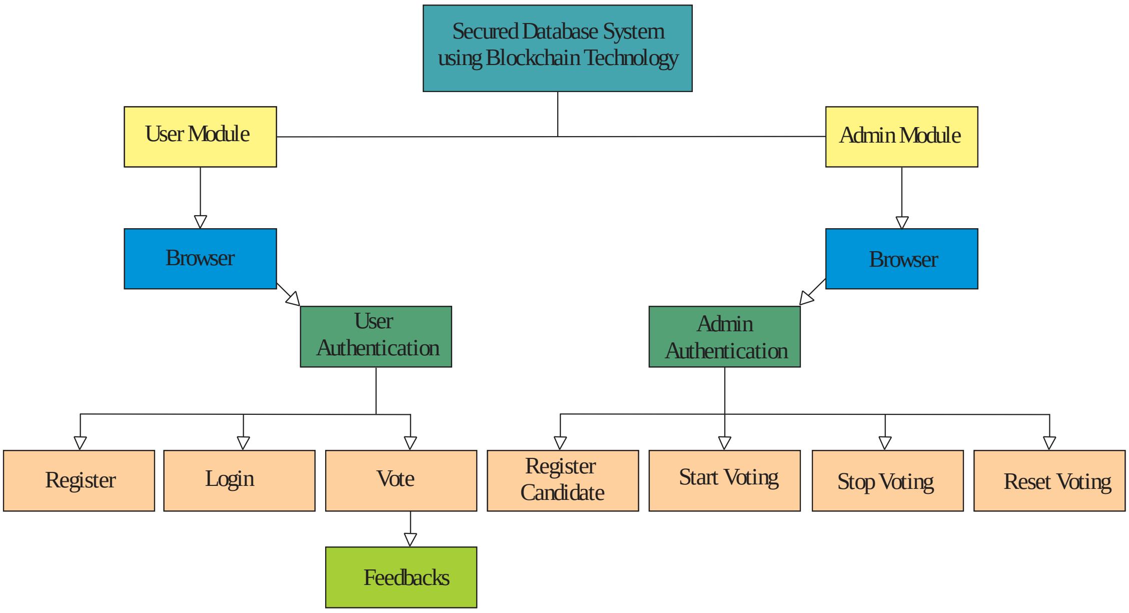

Figure 13. High level model of the proposed system.

Object Oriented Analysis and Design Methodology (OOADM) was also used to help us study the existing system into a useful application, easier maintenance since objects may be understood as stand-alone entities and objects are potentially reusable component.

Here, we designed a secured database system using blockchain technology and the end result is an electronic identity that is encrypted in a truly decentralized form, trusted and complete transparency which makes it very secured without any compromise or leakage of information. The system may not achieve unlinkability due to its complete transparency which is most important essence of public blockchain.

Kiayias and Yung [2] proposed a self-tallying voting system that does not require any trusted third parties for vote aggregation and any private channel for voter-to-voter privacy. Another scheme, Prêt à Voter based on Chaum [3], a new kind of receipt sets a far higher standard of security by letting voters verify the election outcome, even if all election computers and records were compromised. The system preserves ballot secrecy, while improving access, robustness, and adjudication, all at a lower cost which was proposed in Chaum *et al.* [4] that ensures privacy by constructing the ballot with two columns *i.e.* voting options are listed in one column and the voter's choice is entered in an adjacent column.

Adida and Rivest [5] proposed work based on Prêt à Voter but using homomorphic tabulation and it uses scratch stripes to allow off-line auditing of ballots. Bohli *et al.* [6] proposed Bingo Voting that was verifiable and coercion-free voting scheme, which is based on a trusted random number generator. Adida [7] presented Helios, the first web-based, open-audit voting system. Chaum *et al.* [8] proposed Scantegrity that achieves end-to-end (E2E) verifiability with confirmation codes that allow voters to prove to themselves that their ballots are included in the final tally as they really are. Sandler *et al.* [9] developed the VoteBox, a complete electronic voting system that combines several recent e-voting research results into a coherent whole that can provide strong end-to-end security guarantees to voters.

Hao *et al.* [10] proposed a two round protocol that computes the tally in two rounds without using a private channel or a trusted third party which provides exceptional efficiency compared to related techniques. In Khader *et al.* [11], a protocol was proposed to improve the robustness and fairness of the two round protocols. Bell *et al.* [12] proposed STAR-Vote. A secure, transparent, auditable, and reliable voting system which is a collaboration between a number of academics and the Travis County (Austin), Texas elections office, which currently uses a DRE voting system and previously used an optical scan voting system.

Hao *et al.* [13] proposed a new End-to-End (E2E) verifiable e-voting protocol for large-scale elections, called direct recording electronic with integrity (DRE-i). Shahandashti and Hao [14] proposed E2E verifiable voting system named DRE-ip (DRE-i with enhanced privacy), that overcomes limitations of DRE-i [8]. Finally, Choi *et al.* [15] proposed a blockchain-based e-voting system that provides voter anonymity by issuing a voter certificate based on a blockchain address.

The most recent research in electronic voting system, Design of Blockchain based e-Voting System for Vote Requirements which uses homomorphic encryption to achieve voter anonymity by issuing a voter certificate based on blockchain address. This necessitated the need to use different method of blockchain technology to achieve same purpose but truly decentralized electronic voting system based on public blockchain. A web based application that is capable of monitoring vote, casting a vote, encrypting votes, and adding votes to the blockchain. For easy allocation, Solidity Programming Language, Ethereum blockchain and smart contract was also used for this development, which makes the application easily accessible from any place.

5. Conclusions

The design of a secured database system using blockchain technology is important to the society.

As the world is advancing in a new technological age, especially in undeveloped countries like Nigeria that manage a lot of data due to its large population, there is a need to create a decentralized database system that will enable transparency in registering voters and casting votes without involving third party. If not adopted, may lead to mutability of data, single point failure regarding the third party and various security threats that might lead to malicious acts. This has contributed to the massive manipulation of votes in our voting system as well as being vulnerable to attackers. Therefore, introducing a blockchain-based database in our voting system will help minimize the scalability issues which will in turn creates trust between different participants who want to enter into a business agreement through the consensus algorithm, complete transparency of data and decentralized while keeping the users' privacy.

The system will enable the government and Independent National Electoral Commission to minimize the cost of conducting elections while increasing trust, security, transparency and traceability of data shared across a business network and as well encourage more people to participate in the democratic process.

If we cannot combat the single point of failure and mutability of data in our voting system as well as security threats that might arise while using our system, our voting system will surely be at risk. More research and innovation are needed to maintain the trust, transparency and decentralized form of a secured database system using blockchain technology as blockchain is still in its infancy.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Swan, M. (2015) Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc., Sebastopol. https://books.google.com/books?hl=en&lr=&id=RHJmBgAAQBAJ&oi=fnd&pg=PR3&dq=Swan,+M.+(2015).+Blockchain:+Blueprint+for+a+new+economy.+%22+O%27Reilly+Media,+Inc.%22.&ots=XRtEJY3Rk1&sig=tEnsKUSTZO7sIpRuDP65_BFCNeU

[2] Kiayias, A. and Yung, M. (2002, February) Self-Tallying Elections and Perfect Ballot Secrecy. In: *International Workshop on Public Key Cryptography*, Springer, Berlin, 141-158. https://link.springer.com/chapter/10.1007/3-540-45664-3_10 https://doi.org/10.1007/3-540-45664-3_10

[3] Chaum, D. (2004) Secret-Ballot Receipts: True Voter-Verifiable Elections. *IEEE Security & Privacy*, **2**, 38-47. https://doi.org/10.1109/MSECP.2004.1264852

[4] Chaum, D., Ryan, P.Y. and Schneider, S. (2005, September) A Practical Voter-Verifiable Election Scheme. In: *European Symposium on Research in Computer Security*, Springer, Berlin, 118-139. https://doi.org/10.1007/11555827_8 https://link.springer.com/chapter/10.1007/11555827_8

[5] Adida, B. and Rivest, R.L. (2006) Scratch & Vote: Self-Contained Paper-Based Cryptographic Voting. *Proceedings of the 5th ACM Workshop on Privacy in Electronic Society*, Alexandria, 30 October 2006, 29-40. https://doi.org/10.1145/1179601.1179607

[6] Bohli, J. M., Müller-Quade, J. and Röhrich, S. (2007, October) Bingo Voting: Secure and Coercion-Free Voting Using a Trusted Random Number Generator. In: *International Conference on E-Voting and Identity*, Springer, Berlin, 111-124. https://link.springer.com/chapter/10.1007/978-3-540-77493-8_10 https://doi.org/10.1007/978-3-540-77493-8_10

[7] Adida, B. (2008) Helios: Web-Based Open-Audit Voting. *USENIX Security Symposium*, Vol. 17, 335-348. https://www.usenix.org/legacy/event/sec08/tech/full_papers/adida/adida.pdf

[8] Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora, P. (2008) Scantegrity: End-to-End Voter-Verifiable Optical-Scan Voting. *IEEE Security & Privacy*, **6**, 40-46. https://doi.org/10.1109/MSP.2008.70

[9] Sandler, D., Derr, K. and Wallach, D.S. (2008) VoteBox: A Tamper-Evident, Verifi-

able Electronic Voting System. *USENIX Security Symposium*, Vol. 4, 87.

[10] Hao, F., Ryan, P.Y. and Zieliński, P. (2010) Anonymous Voting by Two-Round Public Discussion. *IET Information Security*, **4**, 62-67. https://doi.org/10.1049/iet-ifs.2008.0127

[11] Khader, D., Smyth, B., Ryan, P. and Hao, F. (2012) A Fair and Robust Voting System by Broadcast. *Lecture Notes in Informatics* (*LNI*), 285-299. https://orbilu.uni.lu/handle/10993/25419

[12] Bell, S., Benaloh, J., Byrne, M.D., Debeauvoir, D., Eakin, B., Kortum, P., McBurnett, N., Pereira, O., Stark, P.B., Wallach, D.S., Fisher, G., Montoya, J., Parker, M. and Winn, M. (2013) STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System. 2013 *Electronic Voting Technology Workshop*/*Workshop on Trustworthy Elections* (*EVT*/*WOTE* 13), Washington DC, 12-13 August 2013, 18-37. https://www.usenix.org/conference/evtwote13/workshop-program/presentation/bell

[13] Hao, F., Kreeger, M.N., Randell, B., Clarke, D., Shahandashti, S.F. and Lee, P.H.J. (2014) Every Vote Counts: Ensuring Integrity in Large-Scale Electronic Voting. 2014 *Electronic Voting Technology Workshop*/*Workshop on Trustworthy Elections* (*EVT*/*WOTE* 14), San Diego, 18-19 August 2014, 1-25. https://www.usenix.org/conference/evtwote14/workshop-program/presentation/hao

[14] Shahandashti, S.F. and Hao, F. (2016) DRE-ip: A Verifiable E-Voting Scheme without Tallying Authorities. In: *European Symposium on Research in Computer Security*, Springer, Cham, 223-240. https://doi.org/10.1007/978-3-319-45741-3_12 https://link.springer.com/chapter/10.1007/978-3-319-45741-3_12

[15] Choi, S., Kang, J. and Chung, K.S. (2021, June) Design of Blockchain Based e-Voting System for Vote Requirements. *Journal of Physics*: *Conference Series*, **1944**, Article ID: 012002. https://doi.org/10.1088/1742-6596/1944/1/012002 https://iopscience.iop.org/article/10.1088/1742-6596/1944/1/012002/meta

[16] Koussema, R.A. and Haga, H. (2020) Design and Implementation of Highly Secure Residents Management System Using Blockchain. *Journal of Computer and Communications*, **8**, 67-80. https://doi.org/10.4236/jcc.2020.89006

[17] Baudron, O., Fouque, P.A., Pointcheval, D., Stern, J. and Poupard, G. (2001) Practical Multi-Candidate Election System. *Proceedings of the Twentieth Annual ACM Symposium on Principles of Distributed Computing*, Newport, 26-29 August 2001, 274-283. https://doi.org/10.1145/383962.384044

[18] Haque, A.K.M. and Rahman, M. (2020) Blockchain Technology: Methodology, Application and Security Issues. https://arxiv.org/abs/2012.13366

[19] Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J. and Amaba, B. (2017, June) Blockchain Technology Innovations. 2017 *IEEE Technology & Engineering Management Conference* (*TEMSCON*), Santa Clara, 8-10 June 2017, 137-141. https://ieeexplore.ieee.org/abstract/document/7998367 https://doi.org/10.1109/TEMSCON.2017.7998367

[20] Wachal, M. (n.d.) What Is a Blockchain Wallet? SoftwareMill Tech Blog. https://blog.softwaremill.com/what-is-a-blockchain-wallet-bbb30fbf97f8

[21] Tschorsch, F. and Scheuermann, B. (2016) Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Communications Surveys & Tutorials*, **18**, 2084-2123. https://doi.org/10.1109/COMST.2016.2535718

[22] Lin, I.C. and Liao, T.C. (2017) A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, **19**, 653-659.