A Review on Distributed Blockchain Technology for E-voting Systems

A Review on Distributed Blockchain Technology for E-voting Systems

Rihab H Sahib [1] and Prof. Dr. Eman S. Al-Shamery [2]

[1,2] Department of software, Information Technology College, University of Babylon, Iraq

[1] rihab.sahib@student.uobabylon.edu.iq, [2]emanalshamery@itnet.uobabylon.edu.iq

Abstract. Election is an important event in all countries. Conventional voting suffers many issues, such as cost of time and efforts needed for tallying and counting results, cost in papers ,arrangements and all that it takes for a voting process to be achieved. Many countries such as Australia, Belgium, Brazil, Canada, Estonia, France, Germany, India, Italy, Namibia, the Netherlands ,Norway, Peru, Switzerland, the UK, Venezuela and the Philippines considered online e-voting systems, but the traditional e-voting systems suffer a lack of trust, it is not known if a vote is counted correctly, tampered or not. The voter has no guarantee that his/her vote is considered as they voted in elections, it's a lack of transparency. A solution is e-voting systems based on blockchain (sometimes referred as Distributed Ledger Technology (DLT)) has now turned to be promising for what properties it offer, such as, privacy, security, transparency, accuracy, decentralization in which no central control exist, and most of all, creates an immutable system, where citizens are allowed to vote from their location by using digital devices (smart phones, computers, electronic voting machines). Also, due to the COVID-19 pandemic, many technology applications are heading towards systems with all these properties, at the same time, maintaining social distancing. This review introduced many different ideas for implementing e-voting systems based on Blockchain and how the users (voters and candidates) interact with the system showing the voting process from the first step of registration to authentication till showing the final results. At the end of this review we will illustrate a table that contain all mechanisms used in the papers involved that covers the most important requirements needed for every e-voting system based on blockchain or Distributed Ledger Technology (DLT).

Keywords: blockchain technology, Distributed Ledger Technology, e-voting systems, electronic voting systems, elections.

1. Introduction

Elections are assumed to bring democracy to countries. Their role is important for the future of a citizen life in all countries around the world. Elections have to be trustworthy, ensure the security of citizen's privacy. Additionally, for counting votes, there should not be too much time, as long time waiting for results increases concerns about tampering results. The solution to ensure that each vote is counted correctly, neither central organization stores the database nor change votes (no third party can tamper any vote), and only eligible people are allowed to vote is blockchain technology [1]. Most e-voting system based on blockchain technology require some features that are the main needs agreed by all researchers mentioned in this paper. As the most frequent issue in traditional elections is the problem of security, data manipulation, trust and transparency [2]. Blockchain that was the backbone for bitcoin application, is now the most trusted technology for evoting systems. In this paper, many proposed systems are explained. All which aim to cover the needed requirement for a successful election process. However, the proposed systems differ in the idea of allowing a citizen to change his/her vote or not. Researchers from [1] to [16] proposed an e-voting system based blockchain where the ability of changing votes are totally blocked (the

voter votes only once). Some systems offer another chance for the voter to alter their votes before the time of election ends. Yi, 2019 [17] proposed a withdrawal model that was designed to allow voters change their votes, Hardwick and et al., 2018 [18] called this property Forgiveness. Other proposed system had allowed a protest vote, in which a blank vote is returned to show dissatisfaction of the voter or refusing election and/or the political system [19] [20].

2. Review for e-voting systems based on blockchain technology

This section will explore different ideas of e-voting systems based on this technology categorized depending on the property of allowing a voter to alter the vote .

2.1. E-voting systems based blockchain without the ability of changing a vote

2.1.1. Blockchain-Based E-Voting System

Hjálmarsson and Hreiðarsson, 2018 [1], proposed a blockchain-based e-voting system using permissioned blockchain to introduce "liquid democracy"* which is the ability for the voters to review the way their vote was casted at any moment. It use the consensus algorithm proof-of authority (POA), blocks are validated by validators that are a collection of approved accounts that set limits on a group of selected entities that are known to validate votes on the blockchain and arbitrarily monitor transactions using reputation at stake and identity. Smart contacts are pieces of code written in solidity language, with the Ethereum platform hundreds of transactions are sent per second on the blockchain ,as shown in figure 1 the smart contracts execute agreements to bind parties together which generates a strong relationship that does not depend on a one side party. Each process is performed by a set of smart contracts that is defined for each of the voting zone of the election. Administrators create election ballots as a decentralized application which interacts with an election creation smart contract, containing a list of nominees and voting districts, where each voting area is a parameter in each smart contract for a ballot. A Non-Interactive Zero-Knowledge proof (NIZKP) is a cryptographical method used for verification based on an ID that is electronic, PIN number and information for the area of a voter , by which one party(the prover) , can prove to the other party (the verifier) that the prover knows a value y, without giving any information other than that the verifier knows the value y. Every vote is attached to the blockchain by its identical smart contract of a ballot after it is verified and in return a citizen will receive the ID of the transaction for his vote. When an election end, the result for each smart contract is shown as each smart contract for a ballot does their own tally for their area of location in its own storage.

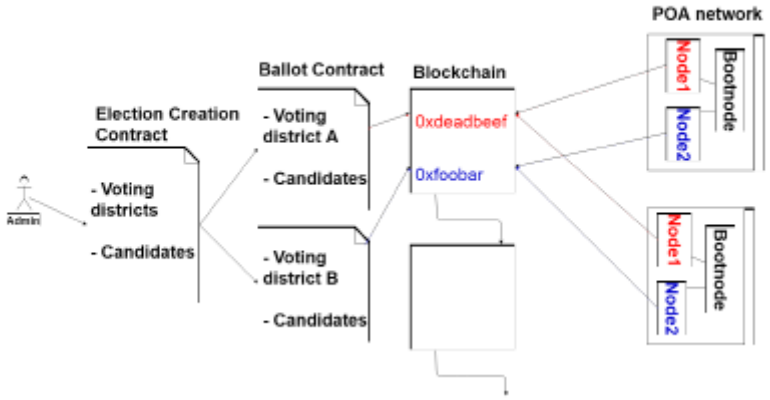

Figure 1: Election as a smart contract [1].

* Liquid democracy is term introduced by the researchers Hjálmarsson and Hreiðarsson referring to their own work.

2.1.2. E-Voting system using Blockchain technology

Indapwar and et al., 2020 [2] used Ethereum framework to provide an environment for blockchain that is a hybrid system (permissioned, public and shared blockchain) where all votes can be viewed by the public for transparency, and created smart contract for e-voting applications, in which blocks of data are stored in the ledger, where each block consist of multiple votes that are verified by the smart contract before they are stored in the blocks of blockchain ledger, otherwise the votes cannot be added to the block. A challenging issue is the speed for verifying transactions.

2.1.3. Blockchain Based E-Voting Recording System Design

Hanifatunnisa and Rahardjo, 2017 [3], proposed a method that depends on an in advance determination turn for every node in the blockchain and record the results of voting using the algorithm of blockchain from all places of election. it aims to preserve data integrity.

Figure 2: Flow Chart Design, [3].

Figure 2 shows the proposed design for blockchain technology. Before the beginning of the election process, every node will create a private and public key. The public key of each node is sent to all other nodes, so each node has a list of public keys of all nodes. Once valid, the votes will be added to the database in the block. After updating the database, the node will check if the ID that was brought as a token is his/ hers or not.

This paper used SHA256 hash function that functions as fingerprint of a data and seeked for any possible attacks on SHA-256 such as the brute force attack and man in the middle attack that are both time consuming and difficult to apply on the whole distributed blockchain .This paper strongly recommended to use SHA256 with its algorithm that has been proven to be safe and used with cryptographic algorithms for securing information.

2.1.4 Towards the intelligent agents for blockchain e-voting system

Pawlak and et.al ,2018 [4], proposed a system that uses intelligent and multi-agent system concepts for an Auditable Blockchain Voting System (ABVS), that merge e-voting with the technology of blockchain into one non-remote supervised internet voting application which is verified end-to-end. The proposed system consist of three phases phase of initiation, phase of voting, phase of counting and verification.

The benefit of the agent-based solution of ABVS e-voting system is to maximize the security of voting. Two types of agents operate in the voting phase (voting agent and authorization-configuration agent), by that, the application in the polling stations is reduced to the intermediary between the agents and the voter, that will control all jobs related to the processing and transmission of votes. Also, the agents would be casted by nodes, that is impossible to change, and would be easy to determine any attempts to hack the system. The proposed system can be showed in figure 3.

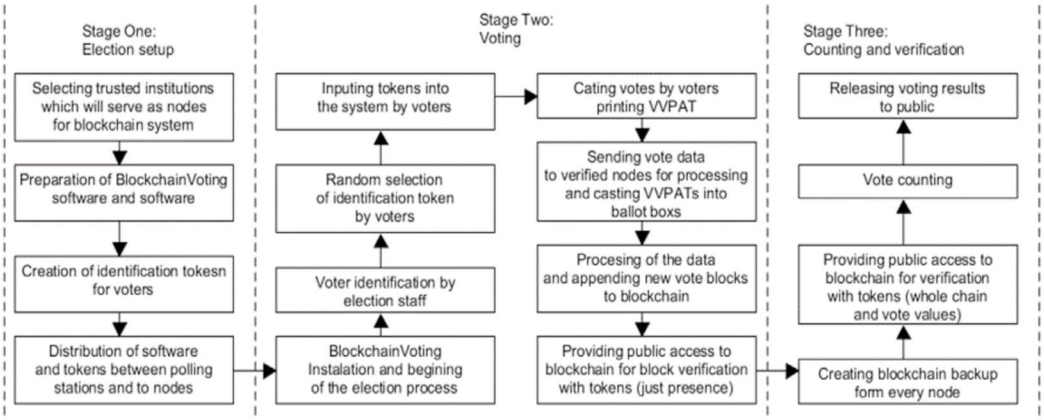

Figure 3: The ABVS voting process [4].

2.1.5. Crypto-Voting, a blockchain based e-voting system

Fusco and et.al, 2018 [5], proposed an e-voting system called Crypto-voting using permissioned blockchain technology. Implementing Crypto-voting system using two blockchains that are linked. The first one record voting procedures and voters, while the second counts the votes and provide results. The system shows the anonymization importance of the network consensus nodes. Voting procedures and results are done by Smart contracts. The proposed system maximizes the efficiency of the validation phase, the assignment of the candidates' vote, provide the automatic management of electoral lists, safe timing of voting abroad, integration of the identification process with that of voting secrecy and automatic and reliable technique to ensure the security of voting. Architectural issues such as privacy tools is used to protect the blockchain in the Cloud system.

2.1.6. Development of a Distributed Blockchain eVoting System

Awalu and et al., 2019 [6], proposed a multichain blockchain network where each candidate will have their own blockchains as shown in figure 4. It uses the round-robbing schedule which is responsible for scheduling the creation of blocks in a rotational way. The system consists of a graphic user interface GUI, an application server to manage all the procedures such as (reaching the authentication, arbitration server and the blockchain), an arbitration server checks the platforms, codes and requirements of the clients, to connect them to the appropriate application server, an authentication server hosted on the application server to increase security concerns, the system also consist of a remote database and a blockchain of miners that are trusted, which is a distributed network owned by government-public libraries and universities . The registration of candidates and voters is managed by trusted central authority. The voters use their biometrics, date of birth and name , which are then encrypted, hashed, and used to create an unique ID that is considered the ID of a voter. When election begins, the voter is authenticed by the system using the systems application and arbitration servers, compared to the unique ID and their biometrics. After authentication, the voter sends his or her vote using the GUI interface. The vote is registered as a vote on the blockchain and sent to the miners that are trusted in order to verify and add the block using the proof of Work Consensus (the default fees of a transaction is zero in a mutlichain blockchain , this is because, trusted miners are all working to ensure that the electoral process ends successfully). At the end of the election, the trusted central authority tallies the final results and present it to the public.

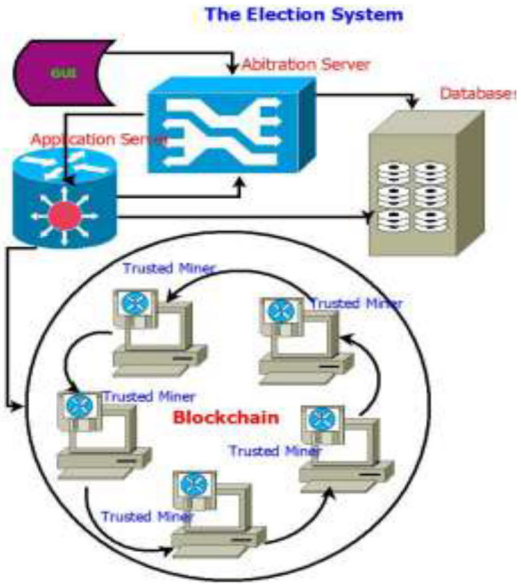

Figure 4: The election system, [6].

2.1.7. Blockchain-Based Electronic Voting System for Elections in Turkey

Bulut and et al., 2018 [7], focused on decreasing the latency (the waiting time for results)that is caused due to the distance between two voting machines. Synchronization of the system would have a performance issue if a single blockchain is represented for the whole country. So, a leveled architecture is designed, in which chains are spread over levels in order to decrease latency. Communication protocols are used periodically to communicate levels, that will need a time delay between the synchronization of levels, as the lower level consists on the chain of nodes where citizens perform their votes, and upper level consists of cluster of chains that saves data from the lower one, this distributed data among levels will decrease the collision between transaction.

2.1.8. Blockchain Based Secured E-voting by Using the Assistance of Smart Contract

Sadia and et al., 2019 [8], researchers proposed a system that uses smart contract for more privacy, security, and accuracy. The system results a transparent, immutable and independently verifiable procedure that rejects all attempts to manipulate votes. Figure 5 shows the functionality of the system. This system consist of three phases ,Prevoting , Voting and Post voting phase, the Organizer in the pre-voting phase determines the list of voters that are eligible, their fingerprint that match a binary value, candidates, start and the end of election (time and date) on the genesis block as an input. Voters are randomly grouped depending on the number of allowable voters, in which a random different time is created for each group, (condition1) checks if the voter is an eligible voter and verify if the voter is in group X then the flag X is true by executing smart contracts , this is done for more security where no votes is accepted after the flag is false (time is controlled by election authority).

After the first verification , a second verification is processed as the voter provides his/ her fingerprint that is converted to binary as a private key which is matched with the fingerprint within the eligible list that's in the genesis block. The hash function is the applied on the binary fingerprint to represent the identity of the voter for security and privacy using SHA256, the voter is then allowed to choose a candidate that are represented by unique strings of 0s and 1s, each ballot has a number and contains the hash function for the fingerprint of the citizen and the ballot string that is executed with the use of smart contract, this string is unique for each voter and has two substrings, choice string (candidate choice) and the random string of also 0s and 1s in order to prevent recognizing the choice made for which candidate. A Block is then generated to contain the ballot and another sibling block that consists of the voters' hashed fingerprint, As the voter broadcast the ballot containing block that is requested to be added in the chain, but the sibling block is not broadcasted yet. (Condition 2) is applied as peer nodes begin to work for the POW for the

block .Also, verify if the ballot is in a correct form and whether the voter has sent a vote before or not. In the post voting phase , when the time of voting process ends, all sibling blocks are broadcasted sequentially, and results are revealed. The proposed system offer a short specified time in case not all voters had voted .

2.1.9. Decentralized E-Voting System Using Blockchain

Sekar and et al., 2020 [9], proposed a decentralized e-voting system using blockchain for elections as shown in figure 6, the system consist of three modules, User validation using biometric information that is hashed by - Message-digest version 5 (MD5) algorithm to verify the user. Dynamic ballot loading rely on the residence location of citizens and loaded in the ballot. After casting their vote in which a vote ID is given as acknowledgment to the voter.

The voters must transfer their public key to the Election Authority (EA) that is charge of creating the eligible votes and paying the vote fees for the address of bitcoin that is created automatically within the backend. Also results are published by the EA that has its own bitcoin address.

The voter should register in Registration Authority (RA) , also the candidate should register in RA with his information in order to create an ID for that candidate. The voting fees for the address of bitcoin for the voters is zero as soon as the voter cast their vote , so there is no chance to repeat a vote more than once.

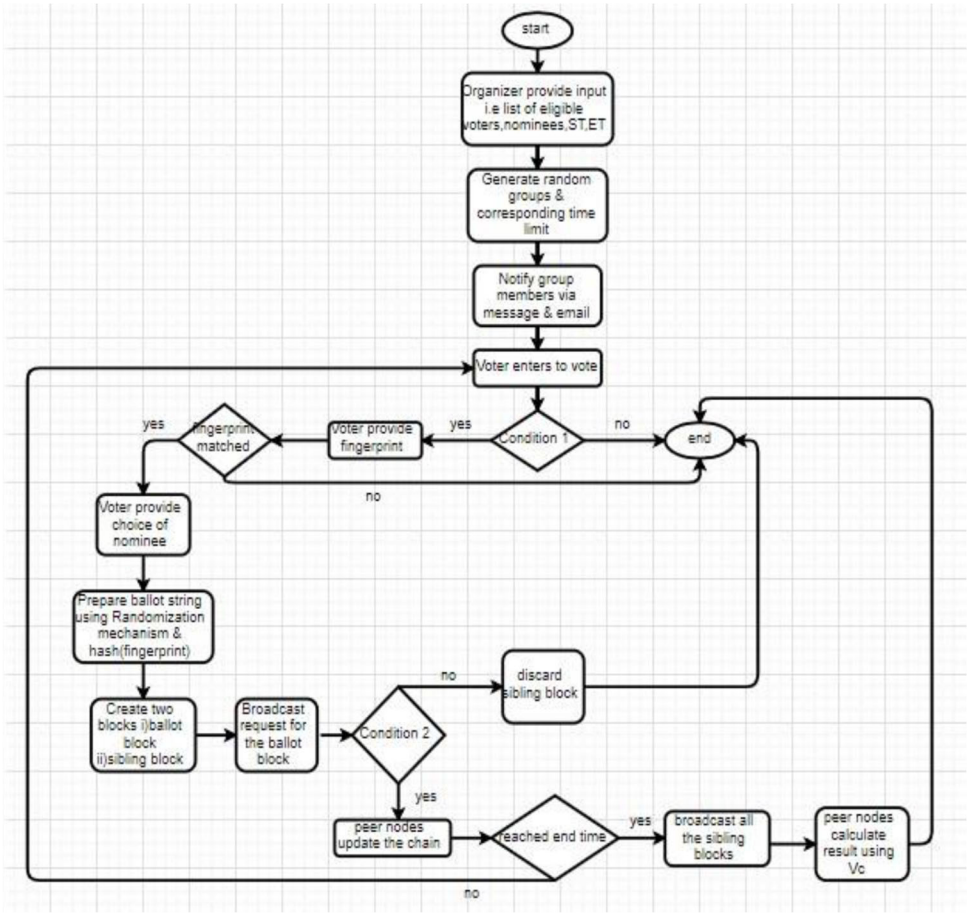

Figure 5: main diagram of the protocol [8]

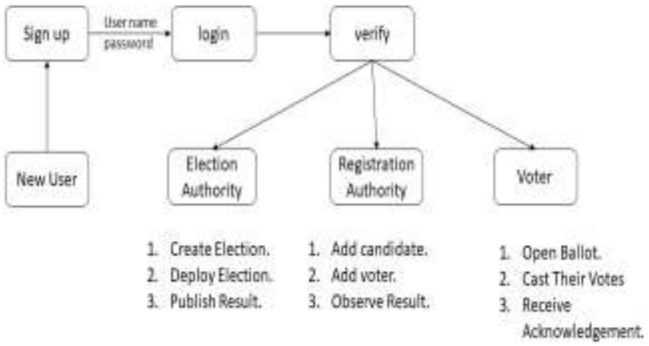

Figure 6: Decentralized e-voting system flow diagram [9]

2.1.10. Electronic Voting System Using Blockchain

Chaithra S and et, al., 2020 [10]**,** proposed a system shown in figure 7 in which every user logs in using an Id along with an added photo that will be used to verify the user using face detection (face detection is done by using haar cascades that are xml files used for detecting the face by using the facial features), then the user can cast the vote using ones crypto wallet key . Each transaction is contained within the smart contracts that makes the system more trusted, more firm and easy to use. Before the beginning of the voting process, every node creates a private and public key. Public key of every node will be send to every node in the network. When an election takes place, each node collects the votes from every voter. When this process ends, the nodes will stop until it's the turn to create a block (a vote is considered an individual block that is impossible to be tampered). A node will give-in the block completed digital signature to be transmitted to all nodes by applying turn rules in block-chain formation to make sure that all nodes are into the blockchain .

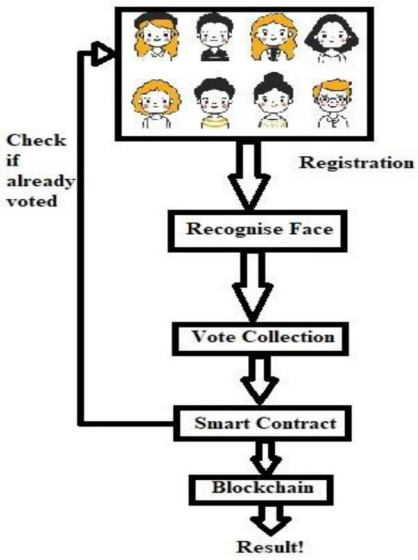

Figure 7: Electronic voting system using blockchain [10]

2.1.11. An IoT and Blockchain based Electronic Voting System

Raguvaran and et al, 2020 [11], merged blockchain technology with an Automatic Fingerprint Recognition System (AFPS) as shown in figure 8. Authentication is done by matching the finger that was enrolled before with specific template stored in database within the Module. a unique number is assigned for each fingerprint template that permits the voter to cast a vote, in case the voter voted before, an alarm rings to prevent him/her from voting again. Also, a message will be shown on the LCD if the voters' information is nor in the database. If the voter has an injured finger, then another approach is used for verifying the identity of voters, which is the keypad that is interfaced with a Microcontroller where they enter their other number in that keypad, and verify their details with supervisor before voting. the details(fingerprint or keypad) will be displayed on the monitor.

The voter chooses the party one wants to vote for that will be displayed on the LCD and a unique number will be created with the count for the chosen party that will be encrypted and stored in the server. (The IOT Cloud platforms controls all the interactions between the application layers and the hardware, connects user applications to remote devices). To overcome the problem of attacks that may happen , block chain is used to protect the data that is in a form of blocks from the hackers, since a copy of that data is shared with any number of systems and any attempt to alter votes will be close to impossible because the attacker will need to alter more than half the copies which is a hard and time consuming process. So blockchain will provide more trusted security to the stored data.

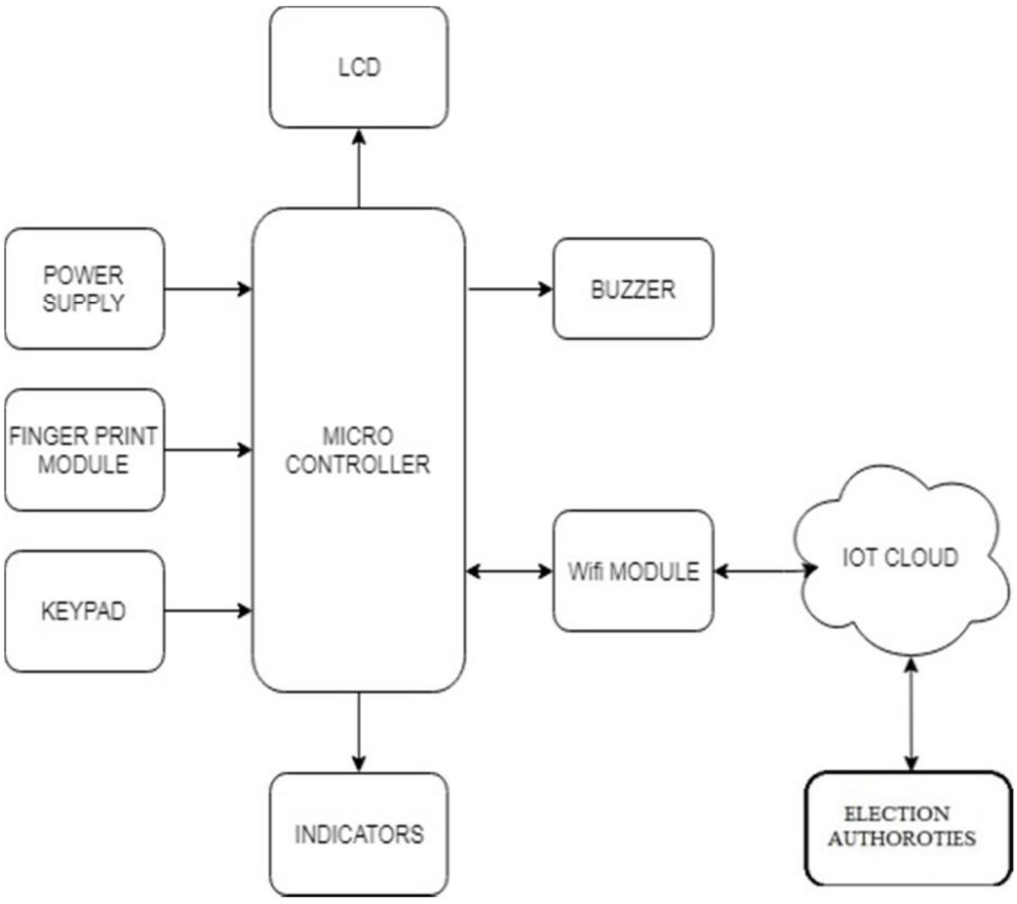

Figure 8: Architecture of the System [11]

2.1.12. Blockchain-based Electronic Voting System with Special Ballot and Block Structures that Complies with Indonesian Principle of Voting

Prasetyadi and et al., 2020 [12], proposed a voting protocol, a block transaction for a ballot design using a Universal Unique Identifier (UUID) and a block structure with the use of SHA256 . In prevoting phase, every citizen must create an UUID4 as pseudonym, prepares important information and a pair of public and private keys, then the organizer validate the identity of the voter, present the public key, and the pseudonym and private key are kept secret.

The second phase is the vote casting phase, as shown on figure 9, after signing the ballot, each voter send his/her own ballot to be accepted by the server, and before being moved to all nodes, the ballot will be verified for integrity and authenticity. If the pseudonym is unique, then data from a ballot that is verified are deemed to be valid, candidate identifier is valid, and the timestamp which is an integer or a float value is reasonable.

In the recording and counting phase, a block that is generated can contain any number of transactions, and then broadcasted. The votes will be counted and the 'unmarked' votes are the invalid votes in the ballot or the corresponding public key is not used for verification.

In the proposed system, the ballot consist of the UUID as voter's ID which is 32 bytes, the candidate ID with a varied length and timestamp that could be the generation time for the ballot or the receiving time of the ballot by the e-voting system. So , 43 bytes is the length of a ballot in minimum compared with the size of a transaction for bitcoin which is about 267 bytes. The design of the block in the proposed system does not contain difficulty target and a block version .

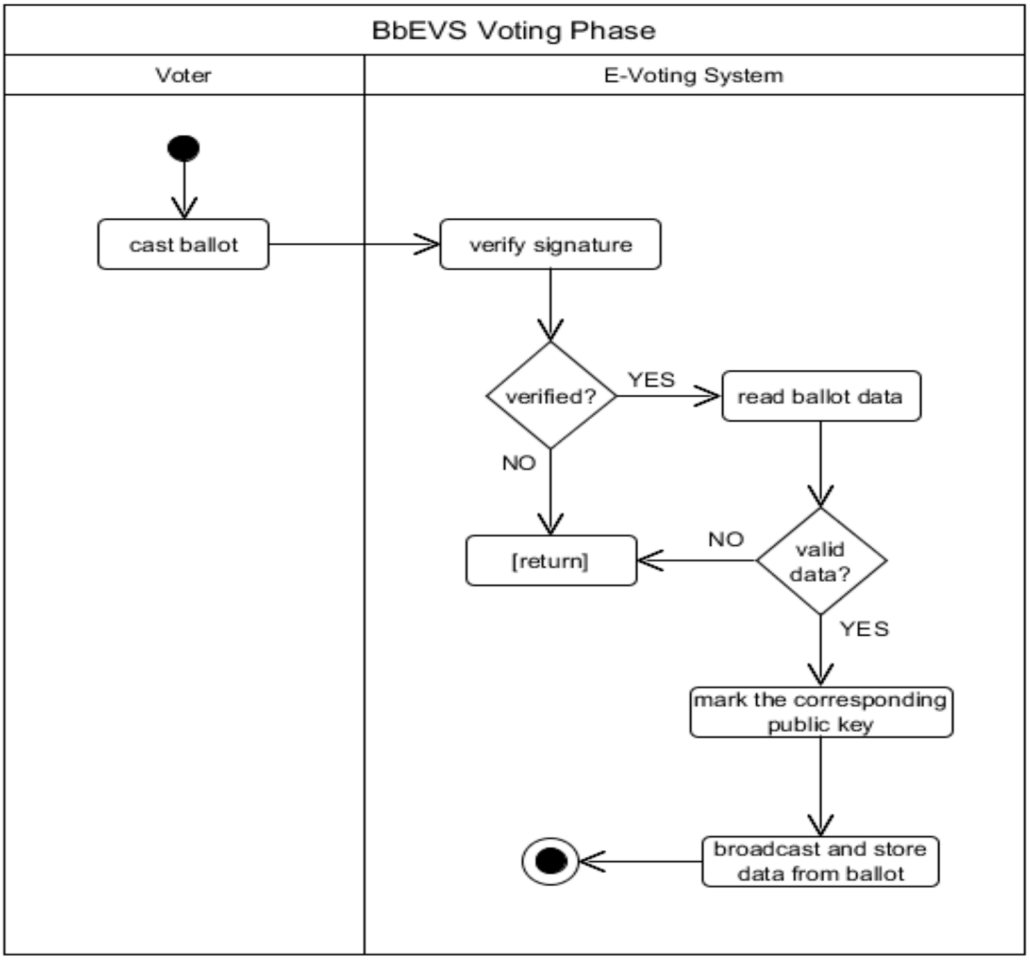

Figure 9: Diagram of vote casting phase [12]

2.1.13. Secure Digital Voting System Based on Blockchain Technology

Mehboob and et.al., 2018 [13], proposed a system consist of several layers as shown in figure 10. The User Interaction and Front-end Security layer deals with the administrator and voter. The main function of this layer is authorization and authentication, ensuring that only allowed users can access the system by depending on several methods ranging from username and password to fingerprinting or iris recognition.

Access Control Management layer provide services that helps layer 1 and 3 to obtain their functions, these services are voting transaction definitions performed by layer 3, roles definition and access control policies performed by layer 1.

e-Voting Transaction Management layer is the most important layer of the system, in which the vote for is mapped onto the blockchain to be mined containing the voters' information for authentication that will be used to generate the cryptographic hash resulting an ID for a vote. Several nodes are engaged in the phase of mining to finally get this vote chained.

Ledger Synchronization layer synchronizes the database with the multichain ledger. At the backend of the database, casted votes are kept in the data tables. A unique identifier is sent to voters by email or message in order to track their votes once they are mined and then added into the ledger of blockchain. The votes are secured by using cryptographic hashes for end-to-end communication. Voting results are also saved in the application's database for auditing and other operations at a later stage.

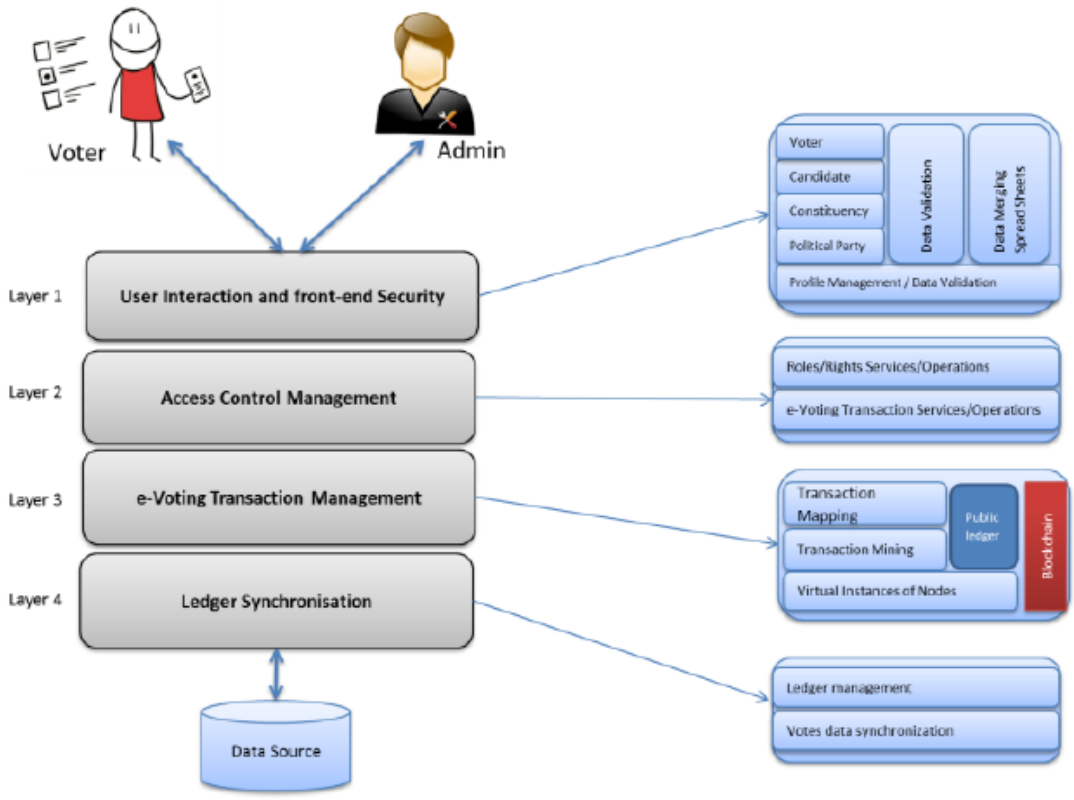

Figure 10: design of the e-voting system [13]

2.1.14. Election System Based on Blockchain Technology

Mohammedali and Al-Sherbaz 2019 [14], proposed a framework that consist of three blockchains for three types (candidates chain, voters chain and votes) as shown in figure 11, each user will have a pair of public and private key after he/she register in the voting framework using their national Id , the date of birth and type, the administrator will confirm the information of users by checking its private key with

the parent pair, the administrator will have to sign up as a voter in order to vote too. All nodes in the system are peer-to-peer network (P2P) in which all users on the network have a complete copy of the block and can always see the results after voters has voted, but cannot alter it.
When the voter votes for a candidate, he/she receives the candidates' details, a voter's opening key, and an earlier block with a hash signature that is a digital signature algorithm of the Elliptic Digital Signature Algorithm (ECDSA) for the user to be verified. After being verified and validated, this information will be encrypted such as timestamp, type, previous hash block and current hash block. The vote blockchain maintains all the blocks that contain voting information. To see the results the voter logs in with the information of whom he chose and the democratic result is taken from the vote blockchain and sent to the administrator and the voter to see the number of votes for every candidate.

2.1.15. A Blockchain Based E-Voting System
Pandey and et al., 2019 [15], proposed a system that uses blockchain to store votes as transactions each transaction of vote contain a hash of the whole vote in the form of a Merkle Tree, a Timestamp of casting the vote, the choice of vote, a unique ID for verifying the identity of the user and a One-Time Password that is used for user authenticity. The data that is the choice of vote is 4-byte long with one bit that refers to the choice of candidates. It will be considered invalid if this data field is set to more than one bit. A Merkle root is saved in a block that is the same to what is used in bitcoin. large space savings results from using a Merkle Tree structure, also allows efficient retrieval of a Vote. Each block consist of a hash value of previous block's, POW (using VoteMaker as a HashCash algorithm the that is used in bitcoin) and a Root of Merkle Tree of Votes.
The VoteMaker using SHA256 tries to find collisions in partial hash of the hashed nonce on all hexadecimal strings of length y that satisfy the property of a Binary Search Tree stored in-order in which the choice of length y is used to make the proof more harder. Similar to HashCash, creating a POW using VoteMaker where brute-forcing the values of nonce by using a counter, is considered an efficient way of arriving at a collision.
For voting and viewing vote results, a web framework is used. Before the voting phase starts, the view if candidates is that candidate details are gathered, by the sign-up feature for candidates in which a candidate dashboard that shows information on the voter demographics for votes received. Also, showing live statistics from the election.
The verification of the each voter is done by using a unique Id number, so there is no need for a voter to register before voting. Using a One-Time Password, the authenticity is verified by sending it to their mobile numbers. Hence, there are two views for the voter which are voter details are gathered and verified before a vote can be sent, and the results view that shows live statistics from the election. Once vote received, it is managed by the mining nodes in the blockchain and the web-framework makes a request to a gateway node which provides an access point for all requests made to and from the blockchain .
A script known as 'Read Blockchain' is used by the web server for scanning the blockchain network for any changes in real-time and updating the SQL server on the web framework to show the changes to the blockchain in order to provide results that are shown to all users.

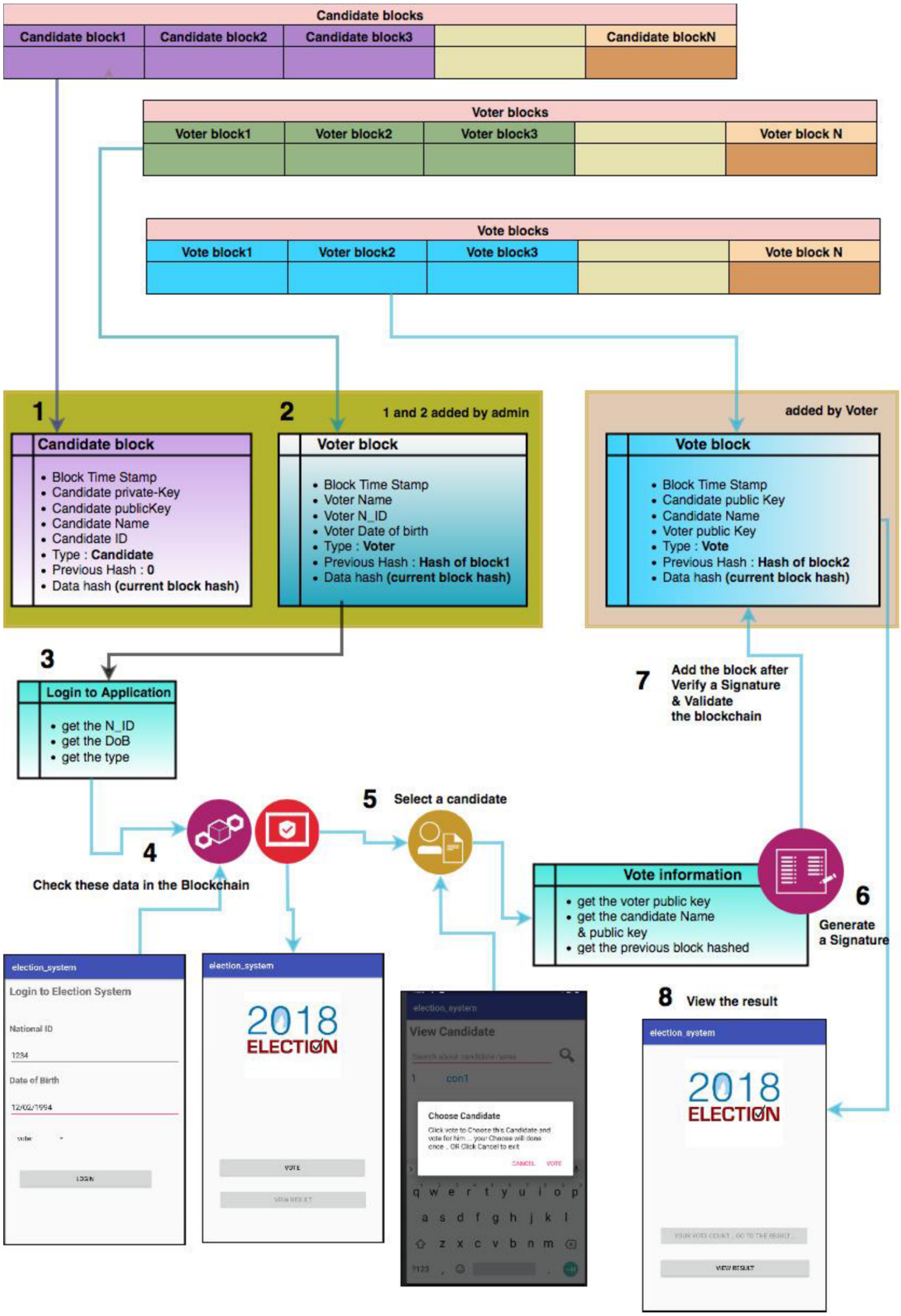

Figure 11: Architecture of the proposed e-voting system [14]

2.1.16 Blockchain-Based Electronic Voting Protocol

Zheng Wei and Chai Wen, 2018 [16], proposed a suitable blockchain based evoting system for storing and processing the result of the elections that can be used for applications on all sort of computational devices connected to the network. The system consist of three stages, prevoting , evoting session and post voting stage.

Before the voting stage, the voter must install a voting application interface. a public and private key pair will be created to the voter. Once the information of the voter is verified (name, identity card number, address and date of birth) by the application server that will then create and send an encrypted ID for the ballot along with a public key to the verified voter, the voters can access their ballot ID within the voting process using their private key to stop identity fraud, because the hacker is unable to access any ballot without the private key of the voter to decrypt the ballot. The application server saves all the voter and ballot information, the e-voting server in turn will store the ballot spreadsheet that will contain the voter's vote, voter public address signing the pseudonymous identity on the spreadsheet and the digital signature of the voter. Only by that, the voter knows his/her voting result . During an e-voting session ,the e-voting server will verify the voter information if it is recorded with the ballot ID. To keep privacy for the vote r result, the ballot will be accepted and recorded and will also be encrypted with the public key before adding it into the chain of the voter result . After the voting session end, post-voting process begins in which the application server private key will be announced to decrypt the encrypted ballot in order to count the result of the voter**.** Each ballot block consist of the ballot spreadsheet information, the hash value for the previous block and a random number that is considered as an additional pseudonymous information to the block. the genesis block will contain a special ID that represents the election and the last ballot block serve as a marking block that contain a special ID representing the end of voting phase in which any block added after it will not be valid.

2.2. E-voting systems based blockchain with the ability of changing a vote

2.2.1. Securing e-voting based on blockchain in P2P network

Yi, 2019 [17], designed a model that records votes based on DLT to avoid fraud votes as shown in figure 12. To provide non-repudiation and authentication ,a user model is designed based on elliptic curve cryptography. Also, an elimination model called withdrawal model that able the voters to alter their vote before the end of elections. By merging these designs, a blockchain-based e-voting project that meets the main needs of e-voting process is proposed. Each block consist of voter’s ID, vote, voter’s signature (marking the voting ballot by the voters private key as a signature so that no one can know the vote of that citizen) ,the voters' private key (to sign the hash of the vote, which is used for the authenticity of vote), timestamp that records submission time (in case blocks have an identical timestamp, the block with the higher signature value is collected), and the hash of the previous block. The voter casts ID, Vote, Timestamp and the Signature to the miner that will obtain the public key from the Public Key Infrastructure (PKI) according to voter’s ID.

The SHA-256 is used to create the hash value H, the miner then uses the public key to verify Signature and get H- , If H- and H are identical, the signature will be accepted. Otherwise, rejected. the miner then queries and verifies that voter has the right to vote . The miner creates a new block with the previous block’s hash value and the information of vote and adds it to the blockchain.The elimination process just allow the voter to change the vote before the end of elections. The new block generation is based on proof of work.

The researcher shows that blockchain with countermeasures to quantum computer attacks is a future research topic for many applications.

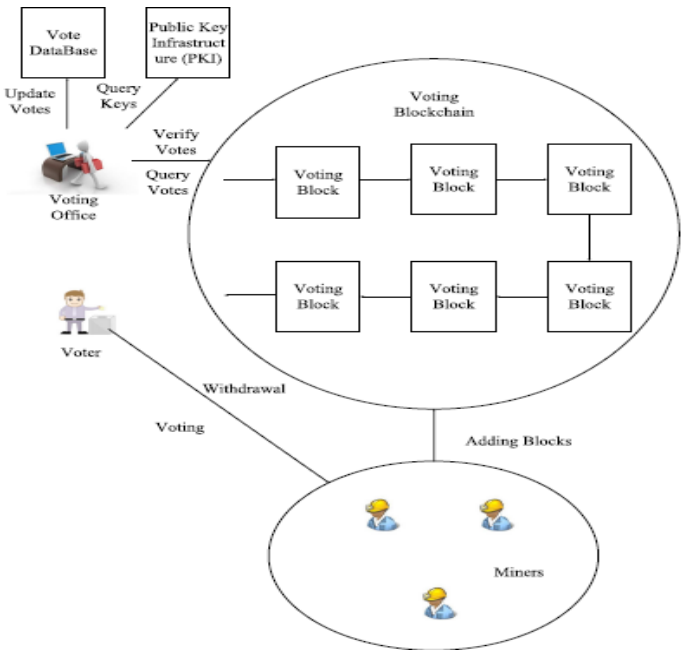

Figure 12: Blockchain-based e-voting scheme [17].

2.2.2. E-Voting with Blockchain: An E-Voting Protocol with Decentralization and Voter Privacy
Hardwick and et al., 2018 [18], proposed an evoting project that meets the main requirements for an e-voting system that is, transparent, secured, and independently verifiable, also providing a maximum degree of decentralization in which the voter controls as network nodes, with a property of forgiveness that allow voters to alter their votes.
The proposed system maintain the privacy of the voter by introducing a Central Authority that is a trusted party in which a citizen must authenticate his/herself to the central authority (CA) to receive a token that proves eligibility for a person to vote, then comes the phases, Initialization phase, where the initialization block will serve as the beginning block that contains all information for election as shown in figure 13, including the validating key of the CA's signature, the choices in which the voters can choose from. Preparation phase, when a citizen is considered eligible, a public key pair will be generated that will be used as a pseudonymous identity of the voter also deemed as a verifying key for that person. The voter will be asked to make a choice and generate a digital commitment of the choice made. Voting stage: all voters build and cast their votes to the network. Every voter is responsible also for collecting, validating and adding the valid votes in the blockchain by ensuring that the voter has voted only once, ensuring that CA's signature is validated . Otherwise, the vote is discarded as invalid . finally, the Counting phase in which, all voters are called to detect their final choice by casting a ballot opening message that contain the voter ID, the opening value of their vote commitment, and a signature over both values.
All nodes of the network will be verify the signature with the public key of the voter. If verified, the voters will then send the messages to their neighbor node (peer). And continue with the vote in their count. All nodes should have similar results since they operate on the same blockchain.

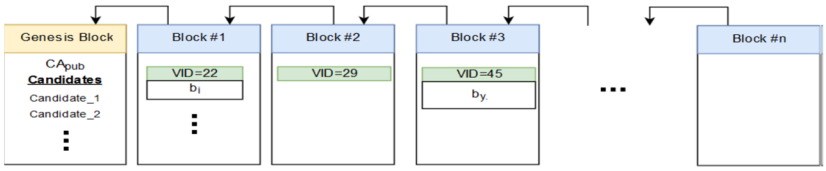

Figure 13: Flow Chart Design, [18].

2.3. E-voting systems based blockchain with the protest ability

2.3.1. A Conceptual Secure Blockchain-Based Electronic Voting System

Ben Ayed, 2017 [19], proposed a design for an electronic voting system that mainly covers four requirements, authentication where only eligible citizens are allowed to vote, anonymity where the voter has to remain anonymous, accuracy in which every vote is unique and counted, and the verifiability to ensure that all votes are correctly counted.

In this proposed system, the candidate will be the first transaction added to the block, containing the name of candidate and considered the base block, in which votes for that candidate is placed on top of base node and will not be counted as a vote. Each vote will get recorded and the blockchain will be updated , the proposed system allow a protest vote in which the voter can cast a blank vote if he /she are not satisfied . Security is ensured by having the previous voter's information in the block and since all blocks are connected to each other, it would be easy to find out if any of the blocks is compromised. each Vote is sent to a specific candidate's node, and the nodes then add the vote onto the blockchain. To ensure decentralization, the system will have a node in each area where the election is held. Limitations in this system is the ability change and cast a vote by a hacker using bad software that is installed in advance on the voter's device.

2.3.2. A Study on Decentralized E-Voting System Using Blockchain technology

Patil and et al., 2018 [20], proposed a system in which the candidate's name will be represented as the first special transaction (also called the foundation block that will not count as a vote)that is added to the block, where all votes for that candidate will be stored on top of that block. A protest vote is allowed , where the voter is able to send a blank vote if not satisfied with all candidates.

When a citizen votes, the vote which is a transaction will be recorded and the blockchain will be updated. The block will contain the previous voter's information for security as the blockchain is decentralized and cannot be tampered, so there is no choice for failing. The citizen's vote will be casted to one of the nodes on the system, that will then add the vote to the blockchain. To ensure the system is decentralized, the voting system will have a node in each location.

As shown in the figure 14, phase (1) after the voters log into the system using their information, a local authorities will send an arbitrarily confirmation number to each voter, this will make the system vulnerable to the Sybil attack , in which large number of fake identities can be created by attackers that stuff the ballot box with faked illegal votes. In (2) the voter will cast a vote in which a token is generated known as Ethereum, with a starting value 1, when a vote is sent it will become 0, so the voter cannot revote again.

In phase (3), the system will create a unique input that consists of the voter confirmation number followed by his/her name with the hash of the previous vote. The information will be encrypted within each vote using SHA that cannot be reversed. In phase(4) the vote is added to the blockchain after a block is created

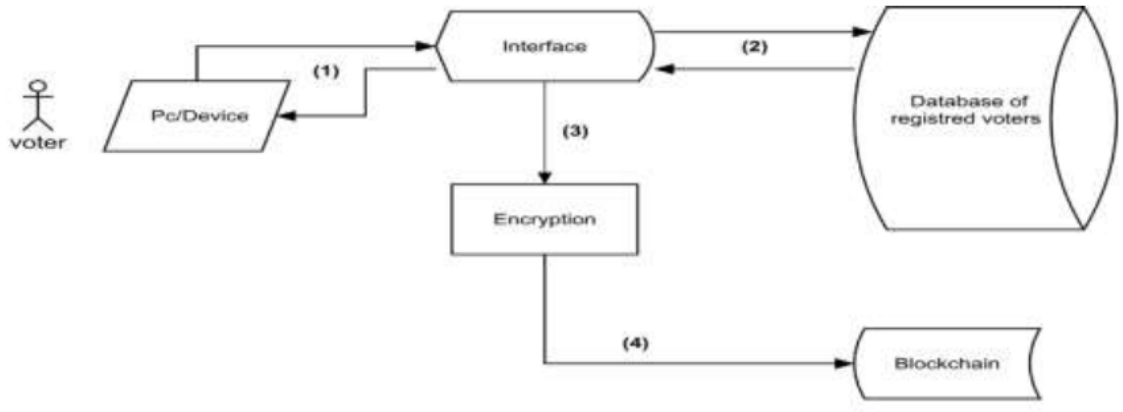

Figure 14: Blockchain Based Electronic Voting System[20]

2.4 . E-voting systems based blockchain with ranking candidates

Crypto-democracy: A Decentralized Voting Scheme using Blockchain Technology**,** Srivastava and et al., 2018 [21] proposed a model that is called PHANTOM that uses a directed acyclic graph of blocks, to generalize the initial blockchain technology, also known as blockDAG. PHANTOM protocol is used to confirm transactions, it is secure under any throughput that the network can support. It uses a greedy algorithm on the block DAG to distinguish between blocks mined by trusted nodes and those mined by noncooperating nodes that are corrupted from the mining protocol of DAG. And to reduce other issues such as threatening voters or polling booth capturing special voting project is adopted called the Borda count method. PHANTOM is considered an advance version of blockchain as it is faster in computation speed especially for countries with huge population . the blocks are represented as a tree. When generating a new block, a reference to the longest chain in the tree will be tipped and ignore the rest.

A multi-leveled decentralized ledger that is distributed is used dividing the network of the protocol into three levels as shown in figure 13, the National level contain the nodes which are not attached to any location. the PHANTOM protocol is applied and these nodes are responsible add blocks in the form of blockDAG in which all national nodes can communicate with each other. Constituency level consist of all the nodes that are considered to be at the same electoral area (the transactions of votes) in which these nodes are connected together and connected also to a subset of polling stations under that constituency where each node create the pair of keys , in which the public key is distributed among lower level that is the local level which is a group of all polling stations around the country. The nodes in local level use public keys to encrypt votes made by polling stations, the constituency nodes publish the private key to decrypt the data and count vote at the end of the voting phase.

The Borda count voting method is used in which voters rank candidates in order of whom they prefer. The candidate with the highest points is announced the winner. So, in case a voter is forced to vote for a candidate, he or she could give the second rank to the candidate he/she really prefer. For example, If there are n number of candidates, the candidate with first preference will take n points, candidates with second preference will have n-1 points and so on.

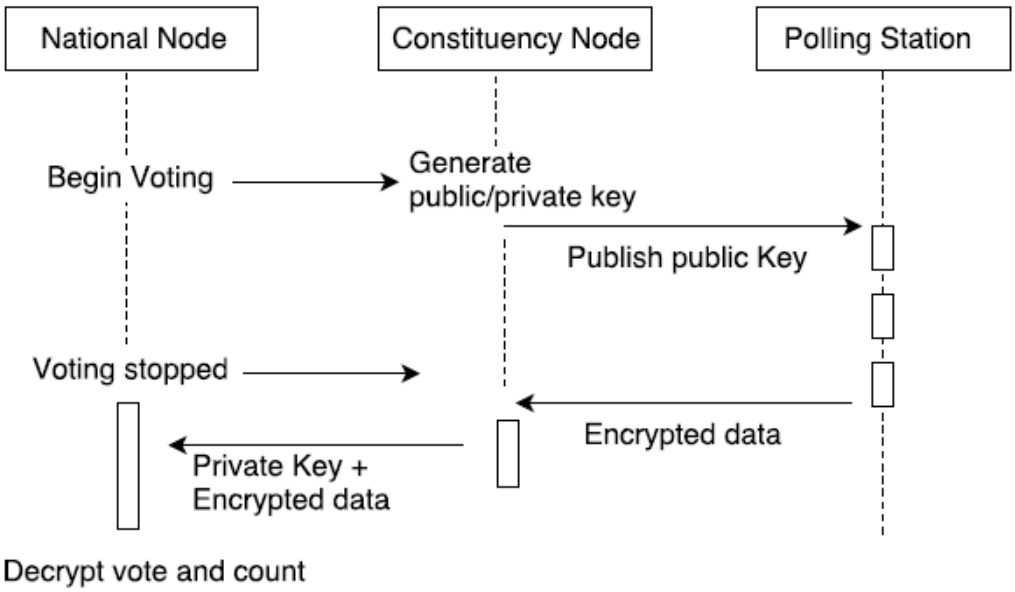

Figure 15: Levels and key pair Encryption [21]

2.5. E-voting systems based blockchain with known ability for changing the vote

2.5.1. BIDS: Blockchain Based Intrusion Detection System for Electoral Process

Odaudu and et.al., [22] proposed an electoral collation process joined with Blockchain technology into evoting system. The system has the following stages: Accreditation and verification, queuing, voters, casting votes, counting the votes and result sent to center. Each stage of collation process is encrypted and saved in a block, the generated transactions are hashed and the hash values are hashed again to introduce a parent block, all blocks are chained to form a peer network of that stage. At the voting stage, the results at a polling unit can be casted to the Local Government Area electoral collation. At collation center, all the block of hashed results casted from a section is nested to form a blockchain . In furtherance of the process, every collated result at the local center is further integrate into a blockchain of state collation and finally all results are sent into a centralized national database. each block in the blockchain keeps the record of the previous block header to prevent any attempt of altering the results. As any change happens will destroy that block of results and as well as all the following blocks.

2.5.2. *Block Chain based cloud computing model on EVM transactions for secure voting*

Sathya V and et al., 2019 [23] proposed a system that uses Blockchain technology for securing data storage with a traditional Electronic Voting Machine EVM that records the votes and update using a cloud based storage called Software as a service (SaaS). The ballot information for each voter is stored as a block and the hash of that block is sent to cloud based storages using low bandwidth internet, a server (receiver station) receives the data from the cloud and stores it in a hash table in a cloud in which the hash of each block will be compared with the hashes on EVM identifying the tampered votes that will be noticed once the votes are tallied and rejected as NOTA blocks.

3. Challenges of Blockchain

There exist several security attacks on blockchain that aim to tamper election for what the attacker side wants or to make election fail. The most attack that is known called identity theft and 51% attack [20]. A 51% attack is an attempt to change and interrupt the recording of new blocks by a group of miners who have to control more than 50% of the network and preventing other miners from completing blocks, at the same time, they will have to make all other following blocks valid in every node which makes this mission close to impossible. Most commonly on bitcoin application in which, the attackers would try to prevent the confirmation of new transactions, or stop or reverse payments between users [24]. Other form of attack is done by performing fraud actions in blockchain software by abusing the present of bugs. Other is to conspire with miners in keeping mined block private from the entire network[20]. However, attacking e-voting systems is rough mission due to all hard efforts and time consuming needed for controlling more than half the nodes on the network.

4. Blockchian important properties

An illustration of all mechanisms used to cover the properties for e-voting system based on decentralized immutable blockchain technology is shown in a single table for all the papers that have been reviewed.

Researchers	Architecture design	Security Considerations and other properties	Authentication of the voter	Ability to alter a vote	Validation
[1]	-permissioned blockchain - Ethereum private blockchain	offer new possibilities of transparency and other evoting requirements	electronic ID and PIN number and information on what voting district the voter is located in	No	proof-of authority-based networks PoA smart contract - SHA256
[2]	- Ethereum framework - smart contract - ReactJS and using Firebase for the authentication purpose - hybrid system	- transparency -privacy	User identity	No	smart contract - SHA256
[3]	blockchain permission protocol	- data integrity - auditability	ID	No	-private key and a public key - digital Signature - SHA256
[4]	Agent based blockchain for a non-remote and supervised voting system	transparency Auditability privacy	Unique VIT(Vote Identification Token)	No	Confirmed by a printout called voter-verified paper audit trail compared with VIT - SHA256
[5]	Cryptovoting system a multichannel hybrid system based on blockchain technology.	-Privacy - safe timing of voting abroad - integrable and enough reliable - verifying documents transparently	Voter information	No	Smart Contracts - SHA256
[6]	-multichain Blockchain network - arbitration server -distributed Database - an interactive multi-device graphic user interface GUI, - an application server	- transparency - privacy - scalability - receipt freeness -security - integrity - accuracy - auditable	-voter is expected to register his biometrics (finger prints -national identity number -date of birth -name and location, The voter will have unique ID number	No	- Proof of Work POW - Digital Signature - SHA256
[7]	leveled permissioned Blockchain	-Security and data integrity of votes - Privacy	identity that is provided by the government	No	Delegated Proof of Stake DPoS - SHA256

		-Smart Contracts - anonymously			
[8]	Smart contract with blockchain	- Anonymity - Privacy - Confidentiality - Transparency - Auditability - Consistency & Accuracy - Public verifiability & individual verifiability - Non-Repudiation	- Voters national ID - Voters fingerprint converted to binary	No	Proof of work POW - SHA256
[9]	- Apache Web Server - MySQL Database - Smart Contract - Quorum - MetaMask	- Transparency - Privacy - verified by using Biometric - smart contracts	- Name - Gender - Address - Biometric	No	Biometric information hashed using MD5
[10]	Ethereum blockchain with smart contracts	facial detection transparent -independently auditable, Privacy	unique Id an added picture	No	- face detection - digital signature - SHA256
[11]	Automatic Fingerprint Recognition System with multi chain block chain technology	- anonymity attribute - POWerful voting system - robustness - obscurity and transparency	Thumb finger print scanning - date of birth -name and address	No	Fingerprint- SHA256
[12]	- Universally Unique Identifier (UUID) Version 4 -Elliptic Curve Digital Signature Algorithm (ECDSA) With blockchain	- direct -public -free - confidential - honest, and fair. - accuracy and integrity	Pseudonym with private key and legal documents	No	- a pair of public and private keys, -Digital signature - SHA256
[13]	web-based interface with Multichain platform	- Transparency - end-to-end verification - integrity - anonymity -privacy protection and non-repudiation	finger print	No	cryptographic hash of the transaction (ID) using username and password ,fingerprinting or iris recognition. SHA256
[14]	Multichain with web application	Accurate and transparent	national ID, birthdate and type (candidate or voter)	No	- Public and private key - Elliptic Digital Signature Algorithm (ECDSA) -SHA512
[15]	blockchain as a distributed public ledger with Flask web framework	- transparency	Unique ID (UID)	No	Unique ID with returning a password Proof of Work SHA256

[16]	- combination of blockchain technology and a secret key with application server	- Authentication - Integrity - Publicly Verifiable - Voter Pseudonymity - Result consensus - Availability	- voter's name - voter's address - identity card number - date of birth	No	public and private key pair - SHA256
[17]	blockchain-based e-voting system for multiple candidates based on DLT	Covers essential requirements of e-voting process	For a voter to sign his/her vote v, he/she must create private and public keys	Yes	- POW algorithm - Voter's signature - SHA256
[18]	Public Blockchain	transparent - Fairness -Eligibility -Privacy -Coercion-resistance -Forgiveness	- Central Authority to verify the vote ID	Yes	Public key that acts as a pseudonymous Identity - digital Signature - SHA256
[19]	Multi blockchain	- Authentication - Anonymity - Accuracy - Verifiability	-Social Security Number - address -the voting confirmation numbers provided to registered voters by the local authorities	Allow protest vote (blank vote)	verify voters' identities against a previously verified database - SHA256
[20]	Ethereum blockchain	-transparent -independently auditable, - Privacy publicly verifiable	-Social Number -address voting number generated by the local - authorities	Allow protest vote (blank vote) but not change the vote	Match information - SHA256
[21]	PHANTOM protocol - Borda count	- Authentication -privacy - Accuracy	-unique identity number, -biometric information (fingerprint) and other related data	Order candidates based on priority only once	-a pair of public and private keys - SHA256
[22]	electoral collation process with Blockchain technology	-security and integrity -transparent -reliability	-thumb printing and other information	Not known	fingerprint - SHA256
[23]	Blockchain with Electronic voting Machine and cloud storage Software as a Service (SaaS)	- transparency -privacy	Id number	Not known	-Proof of work with SHA256 Comparing the hash of the voters id and choice with the hash table

5. Conclusion

Securing a country's important event like elections will always be a concern trying to prove the success of such systems for the aim of trust and satisfying citizens for a clean reliable direct online results and privacy. All these features can be covered by using Distributed Blockchain technology that was implemented initially by Satoshi Nakamoto in 2008 for cryptocurrency application known as bitcoin in

which electronic exchange of money between two sides is done with no centralization (directly no third party is involved). Since then, Blockchain as a distributed ledger technology took a massive part in the revolution of technology to be applied in many fields of science such as Banking industry, healthcare, contract management , reputable system, digital content distributed system and voting system**.** All meant to achieve the security it offers due to the hash algorithm that chains block of transactions to the blockchain database and store that data in many places that makes it a hard challenge to break. The mentioned ideas of proposing evoting systems are still under research as some details may be a future view to deal with details not mentioned such as the size of the ledger that holds the results and how it plays an important role in speeding the throughput time for revealing the final results, also how the huge population may affect the computing process of blockchain.

References

[1] Friðrik Þ Hjálmarsson and Gunnlaugur K Hreiðarsson 2018 Blockchain-based e-voting system *IEEE 11th Int. Conf. on Cloud Computing (CLOUD)* (San Francisco: CA, USA). https://doi.org/10.1109/CLOUD.2018.00151

[2] Aishwarya Indapwar, Manoj Chandak and Amit Jain 2020 E-voting system using Blockchain technology *Int. J. of Advanced Trends in Computer Science and Engineering* **9** No.3. https://doi.org/10.30534/ijatcse/2020/45932020 .

[3] Rifa Hanifatunnisa and Budi Rahardjo 2017 Blockchain based e-voting recording system design *11th Int. Conf. on Telecommunication Systems Services and Applications (TSSA*) (Lombok: Indonesia). https://doi.org/10.1109/TSSA.2017.8272896

[4] Michał Pawlak, Aneta Poniszewska-Mara´nda and Natalia Kryvinska 2018 Towards the intelligent agents for blockchain e-voting system *The 9th Int. Conf. on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN)* Vol 141 (Elsevier) pp 239-246. https://doi.org/10.1016/j.procs.2018.10.177

[5] Francesco Fusco, Maria Ilaria Lunesu, Filippo Eros Pani and Andrea Pinna 2018 Crypto-voting, a blockchain based e-voting system *10th Int. Conf. on Knowledge Management and Information Sharing* vol 3 (Seville: Spain) pp 223-227. https://www.researchgate.net/publication/327907758

[6] Ishaku Liti Awalu, Park Hung Kook and Joa San Lim 2019 Development of a distributed Blockchain e-voting system *the 10th Int. Conf. on E-business, Management and Economics (ICEME)* pp 207-216. https://doi.org/10.1145/3345035.3345080

[7] Rumeysa Bulut, Alperen Kantarc, Safa Keskin and Şerif Bahtiyar 2019 Blockchain- based electronic voting system for elections in Turkey *Faculty of Computer and Informatics Istanbul Technical University*. https://arxiv.org/ftp/arxiv/papers/1911/1911.09903.pdf

[8] Kazi Sadia, Md Masuduzzaman and Anik Islam Abhi 2019 Blockchain based secured e-voting by using the assistance of smart contract *Int. Conf. on Blockchain Technology* (Springer IETE) pp 161-176. https://www.researchgate.net/publication/336915031

[9] S Sekar, C Vigneshwar, J Thiyagarajan, V B Soorya Narayanan and M Vijay 2020 Decentralized e-voting system using Blockchain *Int. Research J. of Engineering and Technology (IRJET)* **7** Issue: 03 pp 312-324. https://www.irjet.net/archives/V7/i3/IRJET-V7I370.pdf

[10] Chaithra S, JK Hima and Rakshita Amaresh 2020 Electronic voting system using Blockchain *Int. Research J. of Engineering and Technology (IRJET)* **7** Issue: 07 pp 323-338. https://www.irjet.net/archives/V7/i7/IRJET-V7I757.pdf

[11] K Raguvaran, Santhoshkumar R, Sowmiya K, Tharun Raj J and Vasanthapriyan C 2020 An IoT and Blockchain based electronic voting system *Int. J. for Research in Applied Science & Engineering Technology (IJRASET)* **8** Issue VI pp 1383-1388. http://doi.org/10.22214/ijraset.2020.6224

[12] Gottfried Christophorus Prasetyadi, Achmad Benny Mutiara and Rina Refianti 2020 Blockchain-based electronic voting system with special ballot and block structures that complies with Indonesian principle of voting *Int. J. of Advanced Computer Science and Applications(IJACSA)* **11** No. 1 pp 164-170. https://thesai.org/Downloads/Volume11No1/Paper_21-Blockchain_based_Electronic_Voting_System.pdf

[13] Kashif Mehboob, Junaid Arshad and Muhammad Mubashir Khan January 2018 Secure digital voting system based on Blockchain technology *Int. J. of Electronic Government Research* **14**(1) pp 53-62. https://core.ac.uk/download/pdf/155779036.pdf

[14] Noor Mohammedali and Ali Al-Sherbaz 2019 Election system based on Blockchain technology *Int. J. of Computer Science & Information Technology (IJCSIT)* **11**, No 5 pp 13-31. https://aircconline.com/ijcsit/V11N5/11519ijcsit02.pdf

[15] Archit Pandey, Mohit Bhasi and K Chandrasekaran 2019 VoteChain: A Blockchain based e-voting system *Global Conf. for Advancement in Technology (GCAT)* (Bangaluru: India) pp 1-4. https://ieeexplore.ieee.org/document/8978295

[16] Clement Chan Zheng Wei and Chuah Chai Wen 2018 Blockchain-based electronic voting protocol *Int. J. on Informatics Visualization* **2** pp 336- 341. http://doi.org/10.30630/joiv.2.4-2.174

[17] Haibo Yi 2019 Securing e-voting based on blockchain in P2P network *J. on Wireless Communications and Networking (EURASIP)*. https://doi.org/10.1186/s13638-019-1473-6

[18] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram and Konstantinos Markantonakis 2018 E-voting with Blockchain: An e-voting protocol with decentralization and voter privacy *Int. Conf. on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (Ghaziabad: India). https://ieeexplore.ieee.org/document/8777471

[19] Ahmed Ben Ayed 2017 A conceptual secure Blockchain-based electronic voting system *Int. J. of Network Security & Its Applications (IJNSA)* **9**, No.3. https://doi.org/10.5121/ijnsa.2017.9301

[20] Mrs. Harsha V Patil, Mrs. Kanchan G Rathi and Mrs. Malati V Tribhuwan 2018 A study on decentralized e-voting system using Blockchain technology *Int. Research J. of Engineering and Technology (IRJET)* **5** Issue: 11 pp 48- 53. https://www.irjet.net/archives/V5/i11/IRJET-V5I1109.pdf

[21] Gautam Srivastava, Ashutosh Dhar Dwivedi and Rajani Singh 2018 Crypto-democracy: A decentralized voting scheme using Blockchain technology *Int. Conf. on Security and Cryptography* **2** (Porto: Portugal) pp 508-513. https://www.scitepress.org/Link.aspx?doi=10.5220/0006881906740679

[22] Salefu Ngbede Odaudu, Umoh J Imeh and Umar Alfa Abubakar 2019 BIDS: Blockchain based intrusion detection system for electoral process *Int. Conf. on Electronics, Computer and Computation (ICECCO)* (Abuja: Nigeria). https://doi.org/10.1109/ICECCO48375.2019.9043292

[23] Sathya V, Arpan Sarkar , Aritra Paul and Sanchay Mishra 2019 Block chain based cloud computing model on EVM transactions for secure voting *3rd Int. Conf. on Computing Methodologies and Communication (ICCMC*) (Erode: India) pp 1075-1079. https://doi.org/10.1109/ICCMC.2019.8819649

[24] website: investopedia 51% Attack 2019 https://www.investopedia.com/terms/1/51-attack.asp#:~:text=A%2051%25%20attack%20is%20an,other%20miners%20from%20completing%20blocks .