

CHAPTER ONE

INTRODUCTION

CHAPTER I

INTRODUCTION

1.1 Background

Elections allow the populace to choose their representatives and express their preferences for how they will be governed. A voting system must preserve the anonymity of a voter's ballot, must be tamper-resistant, and be comprehensible to and usable by the entire voting population. In traditional elections, voters go to their home precinct and prove that they are allowed to vote there, by presenting an ID card. After this, the voter is given a validated envelope that allows them to approach a voting booth, choose a piece of paper, make a mark in a preprinted paper or similar for their candidates of choice, save the paper in the official envelope and close it. Later, in presence of voting authorities, the voter put the envelope in a box[1]. When the contest time expired, a handmade count and tabulate vote process must be done in each precinct. Later, the communication of results to a central general office (sometimes a hierarchical path) will produce a preliminary final score subject to a recounting process. Different types of voting equipment are used to speed up the ballot emission and counting process, but the technologies implemented do not capture the power of the information revolution. There have been several studies on voting systems using computer technologies especially the Internet. These studies caution against the security risks in tasks of election process: voters authentication, ballot secrecy, communications confidence [1] .

The emerging Information Society has enabled people in the developed countries to perform several activities in a direct, electronically automated and efficient way. To keep up with the need to provide citizens with the ability to benefit from services over networks, as well as to reduce the cost and bureaucracy of public administration, governments are striving to transfer an increasing number of their activities to the new medium[1].

1.2 Research Motivation

Elections are the essential part of every democratic society and organization. Hence it is very important to hold up as many elections as possible. Unfortunately, elections come with big administrative efforts and costs.

In order to circumvent the drawbacks of conventional physical elections, a studies of people suggested the use of cheaper online voting systems. Today a lot of alternative e-voting systems have been proposed. Some of them are already used. Unfortunately most of them do not even fulfill the most basic security requirements, whereas other systems are provably secure, but completely impractical. Furthermore a few E-voting scandals destroyed the peoples trust into these voting schemes. As a result, thesis a need for a new easy to use, practical, secure and transparent online voting scheme, that can not only convince experts but also citizen and lawyers. In this thesis such a new easy to use, secure and transparent online voting system is proposed, we are going to leverage the open source Block chain technology to propose a design for a new electronic voting system that could be used in local or national elections. The Block chain based system will be secure, reliable , and anonymous , and will help increase the number of voters as well as the trust of people in their governments.

1.3 Problem Statement

Traditional elections satisfy neither citizens nor political authorities in recent years. They are not fully secure since it is easy to attack votes. It threatens also privacy and transparency of voters. Additionally, it takes too much time to count the votes. This thesis propose a solution using Block chain to eliminate all disadvantages of conventional elections. Security and data integrity of votes is absolutely provided theoretically. Voter privacy is another requirement that is ensured in the system.

1.4 Objective

The main objectives of this study are :

1. To Enhance the Electronic voting system from the security perspective.
2. To Evaluates the use of block chain in Ethereum platforms to implement Electronic voting system.
3. To make E-voting system more reliable used biometric authentication in block chain.

1.5 Research Methodology

The proposed model for an electronic voting system, using algorithms (AES and SHA-256) to encode and decode the vote, as well as using a fingerprint to verify if the voting person is the same person with a national number as well as using block chain technology to achieve CIA coding (confidentiality, integrity and availability) , As well As the use of DFD technology and UML for analytical purposes.

1.6 Research Important

Empowering the prevailing democracy while ensuring the preservation of the electoral process by making the electronic voting system secure , more transparent , and provides high availability , verification and integrity .

1. **High Availability means:** Completely distributed with many nodes storing the complete database.
2. **Verifiability means :** Each block contains the hash of its previous block and is appended to the block chain. Everyone can calculate the hash and verify them.
3. **Integrity means :** It is hard to alter an older value in the chain, since all following blocks have to be re-calculated, which needs much computational power due to the proof-of-work .

1.7 Thesis Layout

This thesis consists of five chapters , Chapter one is the introduction that present the problem and the solutions. Chapter two describes the literature review and related work of e-voting schemes . Chapter three Methodology the proposed e-voting scheme. Chapter four discusses implementation security analysis and results of the proposed scheme. Finally Chapter five gives the Conclusions and Recommendation.

CHAPTER TWO

LITERATURE REVIEW

CHAPTER II

LITERATURE REVIEW AND RELATED WORK

2.1 Introduction

In a democratic country public opinion is the most important determinant to establish a government and voting is the process through which people display their opinion and help to setup a democratic government. So the voting system should be reliable, accurate and it must be transparent. Traditionally, the process of voting is quite cumbersome because voter must come in person to vote. This problem results in the low participation rate of voting. Vote by mail can cater for certain voters such as those who live in sparsely populated areas and who work far away from the voting centers. However, this method is time consuming and cumbersome for the authority to manage since it requires extra work to send , collect and count the ballots manually electronic voting system or Electronic Voting System (EVS) can overcome those problems. EVS is expected to make our modern social life more convenient, efficient and inexpensive. By using EVS in national election, a voter can vote from his home or office. EVS must meet security requirements such as confidentiality, integrity, authentication, and verifiability. This is because EVS is more vulnerable than traditional voting due to the nature of digital processing of election data which can be easily manipulated, hence may result in widespread fraud and corruption. This research, implemented a prototype of an EVS, called E-Voting, that satisfies four security requirements for a safe election. This is achieved by designing some protocols that guarantee those requirements. We believe that E-Voting can reduce human error in voting process by providing easy-to-use user interface[2].

2.1.1 Internet

Internet was invented by the department of defense, United States of America in 1960s as a communication network for defense research purposes, no one could have foreseen how it would transform society three decades later. Today, the internet has become a part of the daily life of many people around the world. Explosive growth in Internet usage and rapid development of e-commerce in the private sector have put growing pressure on the public sector to serve citizens electronically, which is often known as the e-government and this initiative is taken to provide public services and to empower citizens and communities through information technology, especially through internet. The use of Internet for mission critical transactions must provide solutions to ensure that only authorized government officials have access the sensitive data. It must also address concerns about reliability, origin and integrity. In addition to the security issues, the use of Internet for critical government services must provide trust and integrity in both the data and the transactions[3].

2.1.2 E- Government

E-government applies concepts of electronic commerce (e.g. information and marketing through web sites, selling to customers online) to government operations.

E-Government is simply defined as the use of information and communication technology (ICT) to improve the process of government. In a narrow sense it is sometime define as citizens' services, re-engineered with the technology, or procurement over the Internet. Digital (electronic) government is about transforming government service delivery through the use of technology. United nation (UN) world report on public sector says that 90 percent of member countries have operational government websites[3]. E-Government is the use of technology to enhance the access to and delivery of government services to benefit citizens, business partners and employees .Users (Citizens) expect the same level of services from government as they have from the private sector and the government itself expects more effective, productive and improved services as the private sector is. Having this all in common the E-Government still differs in its uniqueness of its interaction between government and its users[3].

2.1.3 E-Services

The use of electronic delivery for government information, programs, strategies and services can named as E-services. These are available online 24h/7 days. It also refers to Electronic Service delivery (ESD) and such expression as one stop service centers. The latter describes situation in which citizen needs are met through a single contact with the government. In many cases it assumes a modernized front office but not necessarily redesigned back office capacity. At the same time, E-services emphasize innovative forms of citizen involvement and offer services that demonstrate serious valuation of citizens as customer of administration. The strategic challenge is to deliver services to members of public along with dimensions such as quality, convenience and cost[3].

2.2 The Importance of Voting

The E-Voting gives you the power to decide how the Countries is run. If you have a complaint about the way the country is being run, voting is a way simple you can make a change. You can choose a candidate to suit to your views and they can represent your views at a national and local level. It's not the only way to participate but it's the quickest and easiest way[3].

2.2.1 Traditional Voting System in Sudan

1. Registration phase

The basic component of a credible electoral is voter registration in accurate and comprehensive manner. This phase starts with determining the eligibility of voters:

1. Voter registration determines, prior to polling date, who is eligible to vote and who is not. Ineligible voters will not be authorized to register. Only those persons whose names are found in the register are allowed to vote.
2. This phase has many benefits. For instance, some of the questions that can be answered are: how many polling centers, their location and consequently the number of staff and materials needed. Thus determining the eligibility of voters facilitates operational planning. Another benefit of this phase is make it easier (or voters to know the location of polling centers on Election Day as most registration centers will become polling centers on Election Day) [4].

2. Sudanese Registration Process Principle

Registration is personal and proxy registration is not allowed. Anyone who wishes to register should come in person for registration. No proxy can represent another person in registration. Registration occurs only once. A person can only register once. Registration by the same person in more than one registration center is not permitted. If the voter has a house in more than one constituency, he/she must choose only one location to register and it must be where he/she was residing during the three months preceding the registration period. Registration is a prerequisite for voting in elections Inclusion In the voters register is a prerequisite for exercising the right to vote. Inclusiveness. Voting is a constitutional right for all eligible citizens. The voters' Register must include as many eligible voters as possible and registration must be accessible to all eligible citizens who are willing to participate in the elections[4].

Registration is public. Registration is conducted in public which will allow monitoring by national and international observers, party agents and representatives of the media as per the rules and procedures set forth by The National Elections Commission (NEC).Registration centers are polling centers. In general, registration centers will become polling centers on the Election Day. Voters should go to the same center where they registered[4].

Head of registration center team determines a person's eligibility to register. The head of the registration center team has the final say to determine whether the person is eligible to register or not. A person deemed ineligible has the right to lodge a complaint. Registration is preliminary and can be challenged during the exhibition period. After the close of the registration process, the preliminary voters register will be publicly displayed. Registered voters can check their names and request corrections on any inaccurate information. Registered voters can object to the inclusion of those they deem ineligible to vote [4].

3. Who Can Register And Vote

Anyone who meets all the requirements below has the right to be registered[4]:

1. To be a Sudanese National.
2. 18 years of age or above.
3. To be mentally fit.
4. Resident of The geographical constituency where he/she wishes to register for at least three months before the registration closing date.
5. Not to be registered in any other geographical constituency.

4. Electoral Period

Political parties and/or individuals submit to Election Management Body (EMB), which is responsible for planning, organizing and managing elections in the Sudan), names of candidates for the elections. This is done through a formal procedure called Nomination of Candidates. The EMB verifies that the candidates meet the criteria specified in the Electoral Law and that there are no public objections to their nomination before placing their names on the ballot. On the day of the election, each voter goes to the polling center which they did their registration if they intend to vote. As it mentioned it is not possible to register in one polling center and vote in another. The highlight of most elections is when people go to the polls to cast their votes[4].

For an election to be free and fair, the polling must follow democratic principles (freedom of expression and movement, secrecy of the vote, etc.). Polling sites should be safe, accessible and neutral. The ballots used should reinforce the integrity of the process by providing safeguards against fraud. At polling stations, trained workers are present to ensure that voting takes place in compliance with the electoral law.

Party agents and independent observers can help detect Potential problems, such as discrimination, intimidation and fraud. Vote counting. It is one of the most crucial stages in the election process. Failure to complete the count and transmit results in a transparent and accurate manner can jeopardize public confidence in the elections and will directly affect whether candidates and political parties accept the final results[4].

In Sudan, party/candidate agents and observers are entitled to watch the counting process. Rules established by National Elections Commission(NEC) will also provide for the recording of any complaints about the counting Process. The responsibility and authority to announce election results rests with the Election Management Body(EMB). When counting has been completed, NEC will declare preliminary results of the election. Candidates or political parties participating in Sudan's elections have the right to appeal those results to the Court. According to Sudan's electoral law, NEC shall immediately after the appeals process, prepare and declare final election results within 30 days of polling. The results will be published in the official Gazette and in the media.

2.2.2 Some of The Problems Facing Traditional Voting [5]

1. traditional voting, makes voters go to a specific place at a specific time in order to vote.
2. more physical infrastructure: When running on a traditional voting. You need of paper, printing, physical urns or staff may, therefore, lead to a lower monetary investment.
3. Slow and difficult votes tally: Since the tally in traditional voting is tally by human counting that it will in most cases run slower than a count carried out by machines, so the results of your election will be not available sooner.
4. Vote may be vote more than once.
5. Modifying vote totals.

2.2.3 Electronic Voting System

E-voting systems include three actors : voter, registration authorities and tallying authorities.

1. Voters: have the right for voting.
2. registration authorities: register eligible voters before the "election day". These authorities ensure that only registered voters can vote and they vote only once on the election's day.
3. Tallying authorities: collect the cast votes and tally the results of the election. They may be counter, collector and /or tallies [6] .

E-voting system should also involve four phases : Voters register themselves to registration authorities and the list of eligible voters is compiled before the Election Day. On the Election Day registered voters request ballot or voting privilege from the registration authorities and the registration authorities check the credentials of those attempting to vote and only allow those who are eligible and registered before. Voters casts their vote and finally the tallying authorities count the votes and announce the election result[6].

1. Benefits of Electronic Voting Systems

E-voting system is a specific case of remote electronic voting , whereby the vote takes place over the Internet such as via a web site or voting applet. Sometimes also used synonymously with Remote Electronic Voting . That usage is however deprecated and it will be used instead as a strict subset of remote electronic voting.

In this work, we use the term E-voting with the specific meaning of Internet voting. If we use it as a general term, then we specify the meaning. They could lead to increased voter turnout [6] , thus supporting democratic process.

1. They could give elections new potential (by providing ballots in multiple languages, accommodating lengthy ballots, facilitate early and absentee voting, etc.)thus enhancing democratic process.
2. They could open a new market, thus supporting the commerce and the employment.

2. Problem of Electronic Voting Systems [6]

Despite the privileges and benefits of the electronic voting program, there are difficulties and gaps facing the electronic voting program , which is:

1. Technological gap: Disparity between expectations from software/hardware and the performance being delivered (security flaws, etc.).
2. Socio technical gap: Difference between social policies (laws, codes, etc.) and computer policies (procedures, functionalities, etc.) .
3. Social gap: Difference between social policies and human behavior (equipment misuse).

2.2.4 Block Chain In E-Voting System

Block chain is a distributed , immutable , incontrovertible , public ledger. This new technology has three main features : [7]

1. **Immutability:** Any proposed "new block" to the ledger must reference the previous version of the ledger. This creates an immutable chain, which is where the Block chain gets its name from, and prevents tampering with the integrity of the previous entries.
2. **Verifiability:** The ledger is decentralized, replicated and distributed over multiple locations. This ensures high availability (by eliminating a single point of failure) and provides third-party verifiability as all nodes maintain the consensus version of the ledger.
3. **Distributed Consensus:** A distributed consensus protocol to determine who can append the next new transaction to the ledger. A majority of the network nodes must reach a consensus before any new proposed block of entries becomes a permanent part of the ledger.

2.3 Block Chain Explained

Distributed ledger technology (DLT), the technology that started the various Crypto currencies in circulation today, has created quite a buzz in many areas in the last few years. Putting it simply, a DLT is a decentralized system for recording transactions with mechanisms for processing, validating and authorizing transactions that are then recorded on an immutable ledger. Block chain is one implementation of DLT. It is also referred to as an “Internet of value”, meaning a secure way to store and transact value anything from currency, stocks, contracts and even votes from one entity to another. It is also the underlying technology powering crypto currencies such as Bitcoin and Ether[6] .

2.3.1 Block Chain History

The first Block chain was conceptualized by Satoshi Nakamoto in 2008. Nakamoto improved the design in an important way using a Hash cash-like method to timestamp blocks without requiring them to be signed by a trusted party and to reduce speed with which blocks are added to the chain. The design was implemented the following year by Nakamoto as a core component of the crypto currency bitcoin, where it serves as the public ledger for all transactions on the network. In August 2014, the bitcoin block chain file size, containing records of all transactions that have occurred on the network, reached 20 GB (gigabytes). In January 2015, the size had grown to almost 30 GB, and from January 2016 to January 2017, the bitcoin block chain grew from 50 GB to 100 GB in size[7].

The words block and chain were used separately in Satoshi Nakamoto's original paper, but were eventually popularized as a single word, block chain, by 2016[7].

Smart contracts that run on a block chain, for example, ones that "create [e] invoices that pay themselves when a shipment arrives or share certificates that automatically send their owners dividends if profits reach a certain level". Require an off-chain oracle to access any "external data or events based on time or market conditions [that need] to interact with the block chain"[7].

According to Accenture, an application of the diffusion of innovations theory suggests that block chains attained a 13.5% adoption rate within financial services in 2016, therefore reaching the early adopters phase. Industry trade groups joined to create the Global Block chain Forum in 2016, an initiative of the Chamber of Digital Commerce[8].

In May 2018, Gartner found that only 1% of Chief Information Officer (CIO) indicated any kind of block chain adoption within their organizations, and only 8% of CIOs were in the short-term "planning or [looking at] active experimentation with block chain"[8].

2.3.2 Type of Block Chain

Three major types of block chain networks exists , each having their own characteristics are consortium block chain, private block chain and public block chain[9].

1. **Consortium:** A consortium formed by a group of members control this block chain. Verifying and adding records to the block chain is based on a consensus mechanism by a pre-selected set of nodes.

Example: In regulatory related decision-making.

2. **Private** : This is controlled by a centralized entity. Only people with specific authentication and permission can be part of this network and thereby can verify and add records to the block chain. However, the block chain could be publically viewable. Participants in this block chain know and trust each other. Also known as a permissioned ledger.

Example: A permissioned ledger between banks to settle inter-bank fund transfers and supply chain with well-defined roles for all actors.

3. **Public** : Public or permission less block chain are decentralized and are visible to the public, anyone can join or leave the block chain and anyone can verify and append transactions to the block chain. This type of block chain facilitates the dynamic collection of participants who may not know each other. Hence, stringent consensus mechanisms have to be implemented in this system

Examples: Time stamping , cryptocurrencies such as Ethereum and Bitcoin .

2.3.3 Block Chain Components

Block chain is combination of below three technologies (cryptography, Peer To Peer Network and distributed block chain programmer) [9].

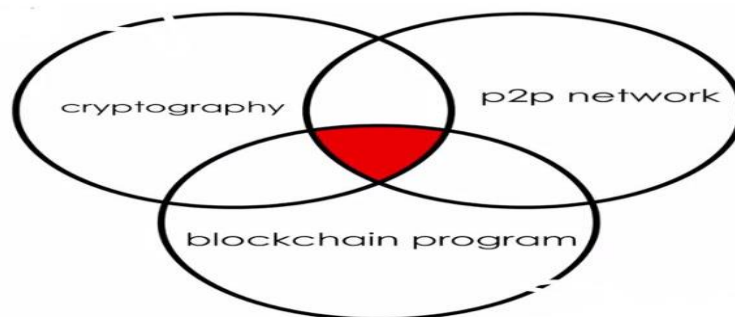


Fig 2.1 Block Chain component [9]

A. Cryptography

1. Public Key Cryptography

In real world E-voting systems, asymmetric cryptography is: heavily used to de/en crypt or sign a ballot ,employing systems such as RSA [10]. With public key encryption, both parties in communication can maintain a public and private key pair. The public key of every party may be known by everyone, whereas the private key must be kept secret. Party 1 may encrypt a message for Party 2 using Party 2's public key, which creates a cipher text which only Party 2 can decrypt. Party 1 can also sign any message using their private key so that Party 2 (or anyone else listening in) can verify that the message is indeed from that Party 1.

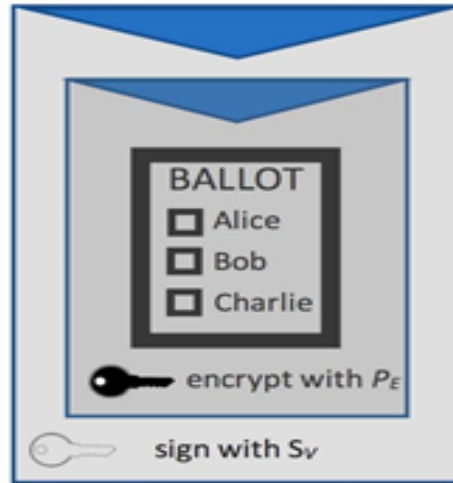


Fig 2.2. Double Envelope a signed and encrypted ballot $E_{S_V}[E_{P_E}[msg]]$, P_E being the public key of the election, and S_V the secret key of the voter [10].

A schematic of double envelope encryption is shown in Fig 2.2. It shows a message sent from a voter to the election server. The ballot is encrypted by election's public key into a cipher text, which becomes one "envelope". After the voter signs the inner envelope with their private key it becomes a "double envelope" which can be sent to the election server [10].

2. Cryptographic Hash Function

A cryptographic hash function is a particular class of hash function that is suitable for use in cryptography. It maps data of arbitrary size to a bit string of fixed size. It is designed to be a one-way function, i.e., irreversible. By making the output string large enough, brute-force attacks (trying every possible input) becomes intractable. Password verification and the proof-of-work used in block chain employs cryptographic hash functions. Fig 2.3 shows the general idea how a cryptographic hash function works[11].

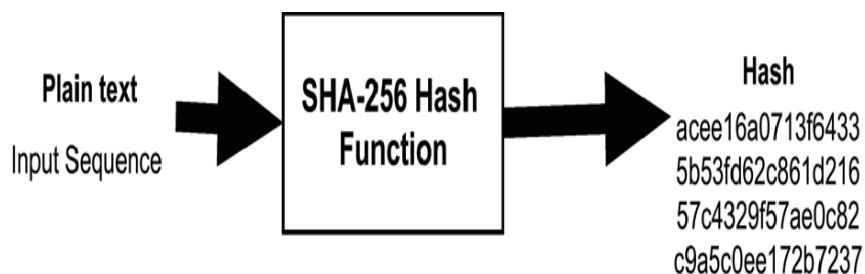


Fig 2.3. Basic Function of the SHA-256 [11]

According to Cryptodex, “a cryptographic hash function should behave as much as possible like a random function while still being deterministic and efficiently computable” [11]. A cryptographic hash function is considered insecure if either of the following is computationally feasible:

1. Finding a previously unseen message that matches a given hash value.
2. Finding collisions, in which two different messages have the same hash value.

B. The Block Chain

1. Block

A block is a bunch of transactions that have been added to the block chain the individual blocks are composed of several components. Roughly these can be differentiated into the head of the block (block header) and his body (block body).



Fig 2. 4. One block (nodes) on the block chain [12]

a. Head of Block

Each header contains information that links a block to its previous block in the chain, which creates a chain linked to the very first block ever created, which is referred to as the foundation. The primary identifier of each block is the encrypted hash in its header. A digital fingerprint that was made combining two types of information: the information concerning the new block created, as well as the previous block in the chain[12].

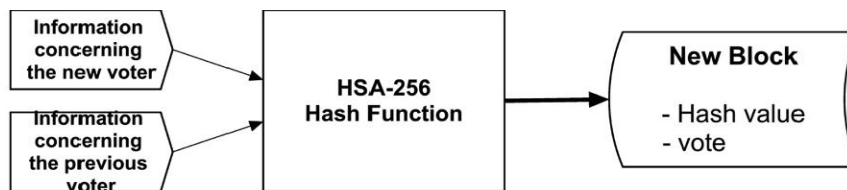


Fig.2. 5. Creation of new Block containing a Hash Value and a Vote [12]

As soon as a block is created, it is sent over to the Block chain. The system will keep an eye on incoming blocks and continuously update the chain when new blocks arrive[12].

b. Body of Block

The block body is conceivable as the loading space of a truck. It contains all transactions that are confirmed with the block. It contains several parts :[13]

1. Magic number # it's four byte long.
2. The hash of the previous block: is, so to speak, the chain of block chains. Because the hash of the previous block is contained in the hash of the new block, the blocks of the block chain all build on each other. Without this component, there would be no connection and chronology between each block.
3. The root hash of the Merkle tree: All transactions contained in a block can be aggregated in a hash. This is the root hash of the Merkle tree.

The Merkle Tree takes its name from the mathematician Ralph Merkle. The discovery was that much information can be represented in a single hash. For this, the data itself is first hashed. Then the hashes are hashed again and merged. Finally, the Merkle Tree is merged into a single hash. This last hash is also called the root hash, the root of the tree. It represents all the information of its “leaves” (individual transactions) and “branches” (hashes of the leaves) in a relatively short string.

Creating the root hash is quick and easy, as long as all branches and leaves are known. We remember the function of a hash function: it works clearly and quickly in one direction and is impossible to break down in the other direction. If the root hash is known, but the transactions are unknown, it is impossible to guess the transactions.

4. The time in seconds: A timestamp in the block itself. The time is given in seconds since 1.1.2020.
5. The goal of the current difficulty: The goal indicates how small the new hash must be to claim validity. In other words, every hash has a size in bits. The lower the goal in bits is, the harder it is to find a matching hash. A hash with many zeros at the beginning is smaller than a hash without zeros. Find out more about the difficulty of the proof of work.
6. The Nonce: The nonce is the variable incremented by the proof of work. In this way, the miner guesses a valid hash, a hash that is smaller than the target.

The screenshot shows a web interface for a 'Blockchain Demo'. At the top, there is a navigation bar with links for 'Hash', 'Block', 'Blockchain', 'Distributed', 'Tokens', and 'Coinbase'. The main content area is titled 'Block' and contains a form with the following fields:

- Block:** # 1
- Nonce:** 72608
- Data:** (empty text area)
- Hash:** 0000f727854b50bb95c054b39c1fe5c92e5ebcf4bcb5dc279f56aa96a365e5a

A blue 'Mine' button is positioned below the hash field.

Fig 2.6. Header and Body on the block [13]

2.3.4 Block Chain Consists

The block chain consists of a set of nodes based on a peer-to-peer network. For each node, it maintains the consistency of the data by performing a consensus algorithm. To specify the mechanism of the block chain, the Bitcoin is a typical representation of the block chain. To specify the block chain, we should have a basic concept of the block. The block is composed of the block header and the main part of the block including a serialized transaction raw[14].

The transaction raw contains the unique identifier(TxID) which is the hash value of the transaction. The identification value of all transactions on each block constitutes each leaf node of the Merkel tree[14].

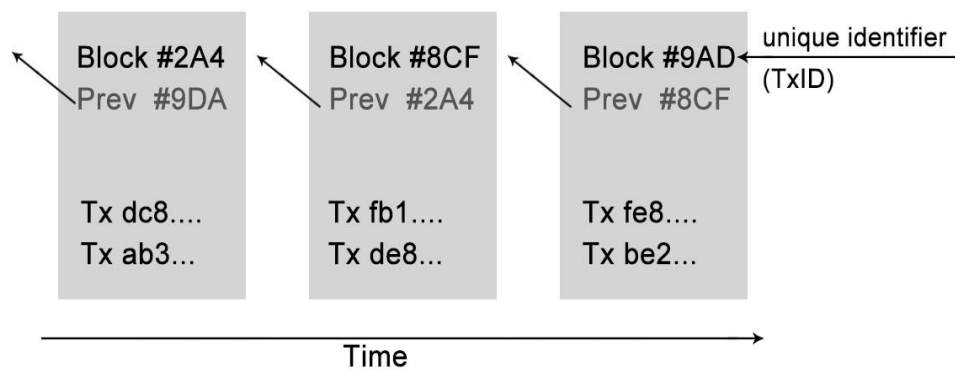


Fig 2.7. Block chain [14]

Fig 2.7 show the Store previous block TxID into the next block, all nodes are linked with the block header which is also called block chain. When creating a new block, the block chain will use consensus algorithm to create a new transaction unique identifier. A new block is generated by the consensus algorithm, which generates a new block by calculating the hash value of the block header. After most nodes accept the new block, it will be added to the block chain[14].

2.3.5 How The Block chain Works

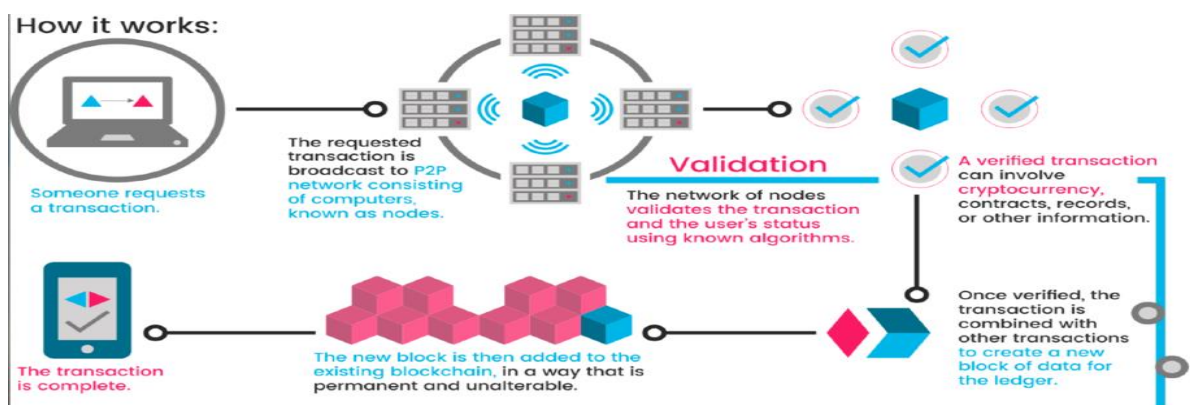


Fig 2. 8. Block Chain Works [15]

Fig 2.8 explain the storing blocks of information that are identical throughout the network, the block chain does not have a single point of failure and cannot be controlled by a single entity, two points that are important when using the block chain for voting. Two additional important properties result from any node being able to download the block chain and verify new data using a block's hash value. The first one is transparency; data on the network is public and can be accessed and checked by anyone making it transparent. Additionally, it would take huge amounts of computing power to alter any unit of information on the block chain making it almost incorruptible. Block chain technology allows for transparent and incorruptible data that cannot have a single point of failure or be controlled by a single entity, making it potentially an ideal platform for digital voting [15].

2.3.6 Benefits of The Block Chain Technology

One of the key advantages of block chain technology is that it allows to simplify the execution of a wide array of transactions that would normally require the intermediation of a third party (e.g. a custodian, a bank, a securities settlement system, broker dealers and a trade repository). In essence, block chain is all about decentralizing trust and enabling decentralized authentication of transactions. Simply , it allows to cut out the "middleman". Also, there are a number of other features like: [15]

1. **Security** : Block chain is considered to be a highly secure system due to its digital signature and encryption. The system is specially designed to be secure , convenient, and tamper proof.
2. **Fraud control** : A system that is based on data stored in a number of places is immune from hackers, it's not that easy to get access to it, and if so, any piece of information can be easily recovered.
3. **Transparency** : Banks, as well as the clients, are immediately notified about the completion of transactions, which is both convenient and trustworthy.
4. **No hidden fees** : As the system is decentralized, there's no need to pay intermediaries.
5. **Access levels** : Users have to choose between public block chain networks available for anyone and the ones requiring permission where each node should be authorized first for the user to enter.
6. **Speed** : Transactions are processed way faster than usual as there is no need to include payment systems, which reduce the cost and increases the processing speed.
7. **Account reconciliation** : The validity of transactions is checked and confirmed by participants, thus, they also confirm their own authenticity.

2.3.7 Block Chain Application And Use Cases

Although we mostly know about block chain due to its application in the financial area, the network is currently implemented in the following spheres:

1. **Healthcare** : Samsung uses block chain in medicine block chain technology is used to share personal medical information . Samsung SDS believes that the network will reduce the workload of medical institutions, reduce waiting times for claims processing and reduce the cost of handling medical claims by up to 70 per cent. In June

this year, Samsung SDS said it had already signed a number of major hospitals on the block chain healthcare network. The list includes Samsung Hospital, Severance Hospital and Korea University Medical Center, while discussions with other institutions were ongoing. The company said at the time that the new system would be introduced in August 2019. The network is built on Next ledger, an enterprise block chain platform originally developed in 2017. Samsung SDS says Next ledger is used to implement 110 block chain projects and has 51 patents[16].

2. **Education** : Now a days , block chain solutions are used for simplifying the process of documents verification in the Californian Holbertson School, and many other institutions are on their way to implement the network[16].
3. **Real Estate** : Bit Property using block chain and smart contracts, Bit Property wants to democratize opportunity and create a decentralized society by allowing anyone anywhere in the world (except the U.S. and Japan due to regulatory concerns) to invest in real estate[16].
4. **Charity**: Bit give this global donation platform leverages Bitcoin and block chain technology to provide greater transparency to donors by sharing real time financial and project information. Save the children, the water project and medic mobile are a few of the charities working with bit give[16].
5. **Government** : Block chain technology is used for a series of political issues, for example, the storage of voting records[16].
6. **Financial Services** : Bitcoin Atom a new fork of Bitcoin that allows everyone to easily exchange crypto currencies without any trading fees and no exchange hacks, making Bitcoin truly decentralized again. The technology is based on atomic swaps an invaluable tool for exchanging one crypto currency with another (e.g. 1000 BTC with 56500 LTC) and no need for a trusted third party. But currently, widespread adoption of atomic swaps has been prevented because they require highly technical skills, something Bitcoin Atom will solve [16].












Name	Symbol	Market Cap ¹²²	Supply limit ¹²³
Bitcoin	 BTC	\$124,969,093,161	21 million
Ethereum	 ETH	\$57,462,517,858	TBD ¹²⁴
Ripple	 XRP	\$23,790,387,789	100 billion
Bitcoin Cash	 BCH	\$17,159,025,225	21 million
Litecoin	 LTC	\$6,704,709,572	84 million
Stellar	 XLM	\$5,128,373,973	100 billion
Cardano	 ADA	\$5,034,129,651	45 billion
IOTA	 MIOTA	\$4,038,240,572	2,779,530,283,277,761
NEO	 NEO	\$3,386,383,000	100 million
Monero	 XMR	\$2,626,586,260	18,4 million
Dash	 DASH	\$2,592,894,544	17.74 – 18.92 million ¹²⁵

Fig 2.9. Block Chain Cryptocurrencies [16]

Fig 2.9 Explain different crypto currencies on the world used block chain technology.

7. **Agriculture** : In the agriculture domain, self-executing smart contracts together with automated payments would be the game changer. The role of smart contracts especially in agricultural insurance, green bonds, and traceability could be very effective. Agricultural insurance built on block chain with key weather incidents and related payouts drafted on a smart contract, linked to mobile wallets with weather data being provided regularly by sensors in the field and correlated by data from proximity weather stations would facilitate immediate payout in the case of a drought or flooding in the field[17] .

2.4 Examples of Countries Using Block Chain In E-Voting System

2.4.1 Estonian E-Voting System

Estonia is the first country in the world to introduce nation-wide Internet voting. The Estonian Internet voting system has been under development since 2002 with the final pilot held at the end of 2004. In 2005 the system was used for the first time for local government council elections [18].

In 2007, for the first time in the world, it was possible to vote online during Estonian parliamentary elections. A total of 30 275 out of 940 000 registered voters used that opportunity and cast their ballots via the Internet. I-voting system is gaining popularity. In 2009, 58 669 voters used I-voting during the European Parliament elections, which is 15% of all the people who voted. In the local government council elections in October 2009, a total of 104 413 persons used I-voting. The percentage of I-votes among all the votes cast was 15.7%. The new record for I-votes was set during the parliamentary elections in March 2011, when 140 846 people cast their votes electronically, which is 24.3% of all the people who voted. In 2014, during the European Parliament elections, a third of voters participated in elections over the Internet – from 98 different countries. Internet voting is meant to supplement, not to replace the traditional methods of voting. The idea is to give voters the opportunity to vote from the location of their choice (home or office) , without the necessity of going to the polling station. Therefore remote voting is used[18].

Estonia takes the security of Internet voting very seriously. Voting over the Internet is as secure as ballot voting. A variety of technical, administrative, legal and other measures are used to safeguard the integrity of the system and most importantly, the security and secrecy of the votes[18].

Electronic voting takes place during advance polls (the tenth to fourth day before Election Day) and government-issued ID-cards are used for voter identification.

If an ID-card is used, the voting procedure is as follows :[18]

1. The voter inserts the ID-card into a card reader and opens the webpage for voting .
2. The voter verifies him/herself using the PIN1 of the ID-card.
3. The server checks if the voter is eligible (using the data from the population register).
4. The voter is shown the candidate list of the appropriate electoral district.

5. The voter makes his/her voting decision, which is encrypted.
6. The voter confirms his/her choice with a digital signature (by inputting the PIN2- code).
7. The voter receives a notice on the computer screen that the vote has been accepted .

During the vote count, the voter's digital signature is removed and at the final stage, the members of the National Electoral Committee can collegially open the anonymous I-votes and count them. Since parliamentary elections in 2011, it is also possible to use a mobile phone to identify oneself for I-voting. This is even more convenient, since then the voter doesn't need an ID-card reader for his/her computer. A mobile phone with the respective SIM card acts as a card and a card reader at the same time. However, one still needs a computer for the voting procedure.

If mobile-ID is used, the voting procedure goes like this in fig.2.10[19]:

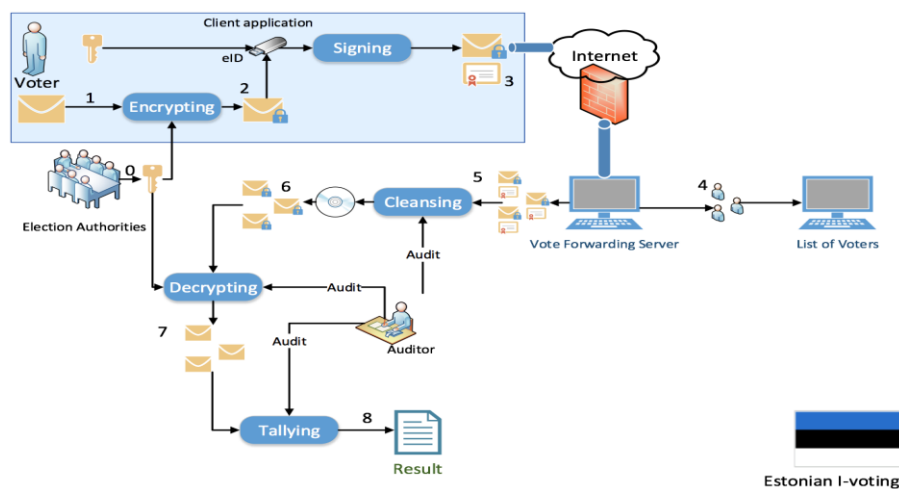


Fig 2.10. Estonian E-voting system [19]

1. The voter opens the webpage for voting.
2. The voter enters his/her mobile number into the computer. After that a control code is sent to the voter's mobile phone by SMS.
3. The voter identifies him/her Self by entering the PIN1 code into the mobile phone.
4. The voter is shown the candidate list of the appropriate electoral district on the computer screen[19].
5. The voter makes his/her voting decision, which is encrypted. A control code is once again sent to the voter's mobile phone by SMS.
6. The voter confirms his/her choice with a digital signature by entering the PIN2- code into the mobile phone[19].
7. The voter receives a notice on the computer screen that the vote has been accepted. There is the possibility of an electronic re vote an I -voter can electronically cast his/her vote again and the previous vote will be deleted. The traditional means of voting (with a paper ballot) is given priority. Should the voter go to a polling station during advance polls and cast a vote, his or her I- vote shall be deleted. On Election Day, the registered i-vote cannot be changed or made void. After Internet voting ends and advance polls close (4 days before Election Day) , the list of voters who have voted electronically is comprised and sent to polling stations. The polling station marks on the voter list that the person has already voted. This prevents them from voting for a second time on Election Day[19].
8. Voters and Candidate show the Results.

2.4.2 Domestic Online Voting System K-Voting (used in Korea)

The online voting system replaces the existing voting method, i.e., visiting the polling place in person, going through the identification process, filling out the voting paper, and putting it in the ballot box, and helps voters use PCs and mobile communication terminals to express their opinions and elect representatives in the web and mobile environment anytime and anywhere . It also makes it possible to hold various ballots , e.g. , general preferential voting and aye and no votes, efficiently and safely so that people’s intentions can be correctly reflected in selection of board members, revision of the articles of incorporation and making decisions on agendas. Like the conventional election method, voters’ basic rights, i.e., the principles of universal suffrage, equal suffrage, direct vote and secret vote, must be guaranteed throughout the voting process[19].

The National Election Commission has been operating the online voting system K-Voting since October 2013, and K-voting is utilized not only to elect the representatives of communities like schools, apartments, villages and cooperatives, but also to gather opinions on certain agendas and make policy decisions. Also, the National Election Commission supports the online voting system in election of representatives of political parties and nomination of presidential candidates. Online voting provides the convenience of voting regardless of time and place, and has a big advantage, i.e., cost reduction. But nevertheless, it is not widely used in Korea yet[19].

2.4.3 Republican Presidential Nomination in Utah , US

The online voting system of the block chain method was used in the process of nominating the presidential candidate for the Libertarian Party in Texas , US and nominating the presidential candidate for the Republican Party in Utah , US in 2016.

It was announced that more Republicans of Utah registered online to exercise their right to vote because of the convenience of the block chain technology. In the past, citizens living overseas, e.g. overseas travelers , missionaries and soldiers , used to receive ballots in the mail, but online voting utilizing the block chain is said to have simplified the registration to vote and the voting process. As for the voting method, voters can visit the polling place to vote as previously, or visit the website of the Republican Party (Utah.gop) and vote between 7:00 am and 11:00 am (local time), and if voters preregister for the online voting system, a unique PIN code will be sent to the voters’ cell phone or e-mail on the day of system election. UK-based Smartmatic , which provides online voting solutions, used end - to - end encryption and the private block chain to provide the online voting infrastructure.

About 10,000 out of 40,000 Utah residents, who voted online on the day of voting, said they had difficulties in the authentication stage. It turned out that most voters received the PIN code as a spam message, or they were not pre-registered properly in the pre- registration stage, but thought they completed pre-registration[19].

2.5 Existing Block Chain Platforms

To choose the right block chain to develop of the decentralized application we review some of the major options available as listed below:

2.5.1 Hyper ledger

Hyper ledger project was published by Linux Foundation in 2015 with the goal of providing a block chain-based open source technology through which companies will be enabled to build robust and industry-specific systems for secure transaction processing. Many different companies collaborate and contribute to the Hyper ledger project and build frameworks. The new version of the Hyper ledger block chain is called Fabric. Hyper ledger is a permissioned block chain and does not provide a crypto currency. However, since the consensus mechanism is based on a plug-in, it is possible to run the system with a crypto currency. Lastly, there is a cryptographic plug-in, as Hyper ledger does not define a specific cryptographic algorithm (like for example the secure hashing algorithm SHA 256 for Bitcoin) and therefore depending on the plug-in, different algorithms are used. Through the open plug-in architecture, the system can be adapted to changes in the future . Fabric is primarily designed for integration projects where a Distributed Ledger Technology is used, offering no user facing services other than an SDK for Node.js, Java and Go. Fabric supports chain code in Go, JavaScript and other languages such as Java that can be accessed by installing corresponding modules. As such it is more flexible than other block chain platforms that only support a closed Smart Contract language[19].

Hyper ledger has a consensus mechanism based on current implementation of practical byzantine fault tolerance (PBFT) . It includes trust anchors to root certificate authorities as an enhancement to the asymmetric cryptography and digital signature features with SHA3 and ECDSA . The permissioned nature of Hyper ledger enhances security of the network by preventing attacks involving unauthorized generation of malicious peers that can potentially take over the network. Also, smart contract implementation in Hyper ledger is based on chain code, which can self-execute conditions or resource transfers among peers in fraction of a second . Thus, by applying smart contracts based on chain code and a unique PBFT implementation which offsets computational overhead for increased networking among peers, Hyper ledger offers a well-rounded platform for applications for Internet-Of-Things[19].

2.5.2 Ethereum

Ethereum is an open source public block chain-based distributed computing platform and operating system on which smart contracts can be deployed . Ethereum was first developed by Vitalik Buttering in 2013 and launched in 2015 after an online crowd sale that took place in 2014 . Ethereum currently works on the proof-of-work mechanism like bitcoin and Ether is the crypto currency generated. Ethereum began as an alternative crypto currency solution to compete Bitcoin but further on things have changed. It has some special characteristics, as it is an adaptable block chain implementation with an implementation of smart contracts and a derivative of proof-of-work consensus known as Ethash. This also applies to directed acyclic graphs to manage probabilistic hash generation in matters that will prevent potential abuse from specialized hardware where other proof-of-work algorithms are vulnerable to .

Ethereum contracts are executed on the Ethereum Virtual Machine (EVM), a decentralized virtual machine. EVM can execute contracts using an external network of public nodes. The virtual machine's instruction set is Turing-complete which makes it much more usable in the real world without elaborate restrictions. A small fee called "Gas" is charged per transaction to mitigate spam and allocate resources on the network.

In addition to implementing smart contracts, Ethereum transactions can also store custom data. This allows use of Ethereum for several applications beyond crypto currency transactions. Due to Ethash being based upon proof-of-work, Ethereum is very fast compared to Bit coin's Proof-of-Work and may require between 10 to 20 seconds to produce a block. Still high frequency and time sensitive IOT device operations may not support such delays.

While Ethash prevents abuses from potential specialized hardware, it does not necessarily enhance fault tolerance. At scale, IOT devices would need to rely on trusted and computationally powerful peers to ensure fault handling. Storage also presents another problem, as Ethereum requires all peers to store a block chain that is tens of gigabytes larger. IoT devices that normally do not have such storage capacity, will either need to intercommunicate with a proxy server that will act as a peer in the Ethereum network or accommodate large storage. Ethereum, as it is used longer than most distributed ledger implementations, has IOT prototypes, such as handling tokens and contracts for electronic lock sharing and supply chain assurance prototypes .

To keep the increasing number of users and applications sustainable on Ethereum and to improve transaction speed Ethereum 2.0 is being developed. It aims to introduce a proof-of-stake consensus mechanism, which will eliminate the need for expensive proof-of-work mining. Also, Ethereum 2.0 plans to introduce sharding, which will improve the speed and throughput of ETH transactions [19].

2.5.3 Stellar

Stellar features a public block chain with its own consensus algorithm which is like Practical Byzantine Fault Tolerance (PBFT) but uses elements from Social network modeling. The difference is that a node agrees on a transaction if the nodes in its neighborhood agree. Nodes in the neighborhood are more trustworthy than the others. When the transaction has been accepted by a threshold number of nodes in the network, a cascading effect ensues due to homophily and the transaction will be confirmed by the entire network with a high degree of certainty. As such, this protocol requires much less computing power, as it does not require solving of cryptographic puzzles. Unlike Ethereum, there is no specific language for smart contracts; it is still possible to assemble some transactions and write them atomically within the block chain. Stellar also features special accounts called multi-signature which essentially lets several owners handle a single account. To perform operations from these accounts, a minimum level of consensus must be reached among the owners. Transaction chaining and multi-signature accounts can be combined to make more complex contracts[19] .

2.5.4 Comparison of Block chain Platforms

After considering and reviewing some of the popular block chain platforms available we can list and compare their main difference in Figure 2.11

Features/Characteristics	Hyperledger Fabric	Ethereum	Stellar
Blockchain Type	Public	Public	Public
Privacy	Private	Public/Private	Public
Permission Restrictions	Permissioned	Permissionless	Permissionless
Average Transaction fee	N/A	\$2.50	0.00001 XLM
Node Scalability	Low	High	N/A
Performance Scalability	High	Low	N/A
Consensus Mechanism	PBFT	PoW	Stellar
Turing Complete	Yes	Yes	No
Contract Language	Go	Solidity	JavaScript, Go
Encryption of Transaction data	Yes	No	N/A

Fig. 2.11. Comparison of features in popular block chain platforms [19]

2.6 Smart Contract Technology

As conceptualized by Nick Szabo[20] , a smart contract is a computerized transaction protocol that executes the terms of a contract . The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs . While the idea was conceptualized in 1994, it was not until the invention of block chain that such contracts could execute in a truly decentralized and autonomous manner. Unlike legal contracts which are meant to be referred to and act as a guideline for execution, Smart contracts perform the execution of contract terms themselves while ensuring it meets all the terms agreed upon to begin with . Vending machines can be used as an analogy to understand Smart Contracts. They are like smart contracts in that the machine operates based on pre-written software code. When the required amount of coins is deposited in the machine and a selection of items made, the vending machine dispenses this item along with any change that needs to be returned. Smart contracts work in a similar fashion and perform tasks of contract only after ensuring conditions of contract are met. This ensures trust and reliability as once the contract terms are agreed upon and coded, neither party will have the ability to change the way it functions. Furthermore, smart contracts on a block chain provide even more security and trust as terms of the contract code are always available to the public for scrutiny and all transactions are recorded permanently and cannot be changed[20] .

2.6.1 Working of Smart Contract

Smart contracts are executable programs . They are usually written in high-level computer programming languages in order to represent business logic or predefined criteria to trigger transfer of values. For a smart contracts engine to be effective in supporting a wide range of use cases, the language needs to be Turing complete, that it can solve any computation problem. Therefore, even though Bitcoin has its own scripting language, it is not considered to have smart contracts. On the other hand, Ethereum smart contracts are Turing complete and have been used to solve some of the most challenging problems in real-world [20].

When a user submits transactions, smart contracts gets executed by the block chain nodes to process transactions. A block chain transaction has a designated target smart contract function, a payload that contains input values to the function call and is always signed by the submitter. A transaction can be submitted to any node in the block chain network, which broadcasts it to the entire network so all the nodes will see the transaction. At some point, the transaction gets processed by each individual node using the executable program in the target smart contract. If the transaction execution is successful, the internal state of the block chain will be updated. A smart contract may also consider the input to be invalid and reject the transaction as failed, in which case the state is not affected[20].

Smart contracts must be executed by a set of block chain nodes independently. Unlike traditional databases , block chains are decentralized. As such, every node assumes others are potentially malicious and never trusts states maintained by other nodes within the network. Instead each node executes the transactions themselves using the smart contract code and maintains its own state. Since all nodes have the identical beginning state, same input values and therefore the same execution logic. If all three parts are identical, the top state is sure to be identical. The chain of blocks with the linked hashes each representing the total list of transactions input and therefore the starting state, play a critical role in forming consensus among the block chain nodes. To ensure the correct smart contract code is executed to process the transaction, Ethereum smart contract code stores a copy of itself on the block chain directly as state. In Hyper ledger Fabric and Corda, contract code is stored off-chain, and an on-chain hash is used to identify the correct version of the contract. The main purpose of smart contracts is to take care of program states. State is an arbitrary piece of knowledge that gets updated by executing a transaction. So, a block chain can be conceptualized as a database, although it is designed for data consistency and immutability and not for speed of performance of queries. Most of the block chain protocols are designed to follow a state transfer conceptual model where each smart contract maintains its own set of states. Most transactions submitted to a block chain involve a contract, except for pure value transfers that do not involve smart contracts. Whenever a transaction is executed, the state of the target smart contract is updated. Good contracts can call another smart contract and question the downstream contract's state or update it. Smart contracts may be thought of as program functions: there are inputs, logic to process the inputs, and output. Execution of smart contracts often ends up in updated states[20].

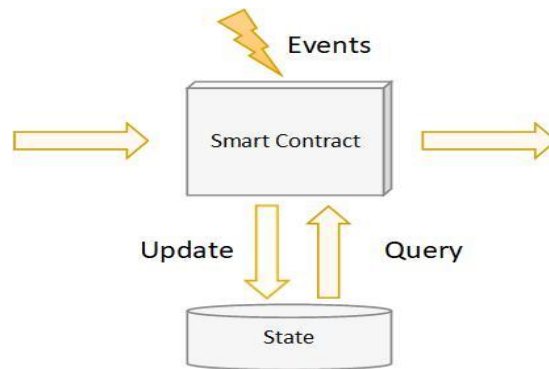


Fig 2.12. Working of Smart contracts [20]

When smart contracts are executed only valid transactions will result in updated states. Invalid transactions resulting from exceptions thrown by the smart contract are rejected by the network or included as failed depending on the block chain platform.

Smart contracts can also publish events that send notifications to the outside world when the block containing the transaction gets committed to the block chain on the node [20].

A smart contract may have multiple public functions that can be called by any transaction. These functions could either result in a state change or simply return the latest state after performing internal calculations. Some of common functions that update states are:

Transfer (to, amount)

Approve (delegate, amount)

Transfer From(from, to, amount)

Mint (to, amount)

Burn (from, amount)

Functions that only query the latest states for information and do not result in a state change: Balance Of (account)

If a transaction calls a function that requires a state change, then it must be handled by a consensus mechanism, so that the system ensures all the copies maintained by the block chain network's participating nodes have identical records.

On the other hand, querying the latest state and retrieving information without updating state can be done with the help of just one node. Since the consensus mechanism ensures all nodes have the same information it does not matter which single node we query. Hence, we can conclude that write operations on a block chain are far more expensive than read only operations [20].

2.6.2 Advantages and disadvantages

Smart contracts offer several advantages over traditional contracts, some of which are listed below[20]:

1. **Lower cost:** Even though each transaction requires a small fee, applications using smart contracts require much less manual handling or verification and as such will reduce overall costs/financial charges by a significant amount.
2. **High Accuracy:** Since these transactions are processed automatically without manual intervention at any point, there are fewer errors resulting from human error.
3. **Increased Speed:** as smart contracts are essentially software codes that automate complex tasks involving decision making, they can increase the speed of transactions as well as the entire business process.
4. **Lower Risk:** Since smart contracts are stored and executed on the block chain, an immutable and permanent record of transactions are stored, it would be virtually impossible to manipulate or cheat the system which reduces the overall risk associated with doing business.
5. **No Middlemen:** Since smart contracts can function autonomously in a reliable manner, it is often used to remove third party intermediaries whose sole purpose is to be a bridge between two untrusting parties.

While Smart contracts provide many advantages, they are not without their fair share of disadvantages as well :

1. **Privacy:** Since smart contracts are executed on a block chain, every transaction that needs to be added to the block chain needs to be broadcasted to the network of nodes to reach consensus. So, any node participating in the block chain can essentially deduce all the information regarding any transaction. As such privacy is never guaranteed even when some amount of information can be obfuscated.
2. **Limited Scope:** While many contracts existing today, particularly those relating to business transactions are well suited to be converted to a smart contract, there are many others that may include ethical and social issues that may be hard to do so.
3. **Performance issue:** Most block chains have a high latency or low transaction speed depending on the consensus mechanism used. This makes it inapplicable to many applications that require instantaneous confirmation of transactions.
4. **Governance:** If block chains are to be sustainable in the long run, serious consideration should be given to ethics and framework for governance models. Nascency of the technology coupled with pseudonymity of account holders and complexity of underlying concepts make it prone to deception and fraud.

2.6.3 Vulnerabilities with Smart contracts [20]

There are many known vulnerabilities in Smart contracts that can be exploited to perform certain attacks that are provided below.

1. Out-of-gas: When a function is trying to transfer ether to another account, it is possible to encounter an out-of-gas exception if the sender does not have sufficient gas to cover the transaction. This may result in contract execution if not handled appropriately.
2. Invalid transfer: When sending ether, recipient address must be specified accurately. If some ether is sent to an incorrect address, it could be lost forever. Even if the incorrect address is valid and someone else did receive the ether, it may be hard to get it back. As such it is important that the correct recipient addresses are used especially when retrieving these from an array or other complex data types.
3. Exception handling: Solidity raises an exception when one the execution runs out of gas; the call stack reaches its limit or when the command throw is executed. However, the way Solidity handles different exceptions is not uniform and developers should be careful on how these will be handled.
4. Reentrancy: Unlike some other programming languages, it is not guaranteed that when a non-recursive function is invoked, it cannot be reentered before its termination. Due to the fallback mechanism an attacker may be able to re-enter the caller function. This could cause unexpected behaviors and loops which might end up draining all the gas before coming to stop throwing an out-of-gas exception.
5. Private fields: Again, unlike some common programming languages, privacy of private fields is not guaranteed. Since every transaction is sent to miners and broadcasted on the block chain, elements of the transactions are available for anyone to inspect.
6. Call stack depth limit: Whenever a contract invokes another contract, the call stack associated with the transaction increases by one frame. Since the call stack is limited to 1024 frames, an exception is thrown when an invocation is made beyond this limit. As such it is highly recommended to avoid using recursive functions.
7. State: The state of a contract is determined by the value of its fields and balance. In general, when a user sends a transaction to the network in order to invoke some contract, he cannot be sure that the transaction will run at the same state as the contract was at the time of sending that transaction. This may happen because, in the meanwhile, other transactions have changed the contract state. Even if the user was fast enough to be the first one to send.
8. transaction, it is not guaranteed that such a transaction will be the first to run. Indeed, when miners group transactions into blocks, they are not required to preserve any order; they could also choose not to include some transactions.
9. Timestamp dependency: Timestamps should be avoided in critical parts of the code as the miners can manipulate the timestamps. Solidity also provides a list of known bugs with their corresponding severity level.

2.6.4 Potential Countermeasures

It is suggested that known vulnerabilities in smart contracts can be prevented and risk mitigated by using tools such as listed below:

1. **ZeppelinOS**: is an operating system for smart contract applications developed by Zeppelin Solutions that enables development of smart contracts by using already developed and secure smart contracts[21].
2. **HackThisContract**: is a crowdsourcing experimental website where smart contracts uploaded will be attacked and tried to be exploited for potential vulnerabilities by other developers. This helps eliminate a lot of common issues and makes the smart contract more secure before deployment.
3. **Hard Fork**: It is always recommended to upgrade the Ethereum platform adding functionalities that can improve operational semantics and face security issues such as: guarded transactions to deal with transaction ordering dependence (TOD), deterministic timestamp and exception handling[21].
4. **Oyente**: This tool extracts the control flow graph from EVM byte code of a smart contract and executes it symbolically to detect vulnerability patterns. This tool identifies vulnerabilities arising due to non-handling of possible exceptions such as not checking the return code of call or issues with reentrancy.
5. **Remix**: is a web-based IDE that allows users to write, deploy and run Solidity smart contracts. Remix includes an integrated debugger and a test-block chain network. It can be used to analyze the Solidity code and reduce coding mistakes by performing a security analysis using deductive program verification and theorem provers.
6. **Town Crier**: TC acts as a high-trust bridge between existing HTTPS websites and the Ethereum block chain. It scrapes website data and delivers it to contracts on the block chain as concise pieces of data called datagrams. TC uses a combination of Software Guard Extensions, Intel's recently released trusted hardware capability, and a smart-contract front end. It executes its core functionality as a trusted piece of code in an SGX enclave that can prove to remote clients that it is interacting with a legitimate, SGXbacked instance of the TC code[21].

2.7 Block chain As a services on E-voting system

Defining a smart contract includes identifying the roles that are involved in the agreement (the election agreement in our case) and the different components and transactions in the agreement process. We start by explaining the election roles followed by the election process[22].

1. **Election Roles** : As can be seen in Figure 2.13, elections in our thesis enable participation of individuals or institutions in the following roles. Where multiple institutions and individuals can be enrolled to the same role[22].

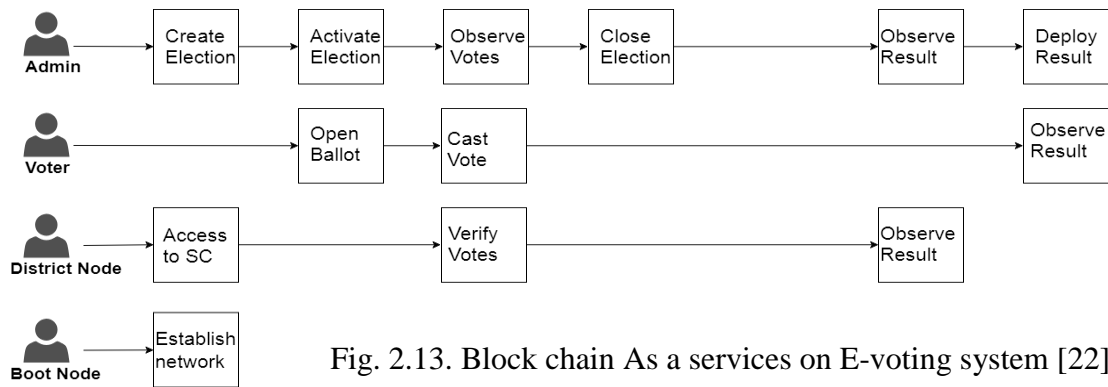


Fig. 2.13. Block chain As a services on E-voting system [22]

- i. Election administrators: Manage the lifecycle of an election. Multiple trusted institutions and companies are enrolled with this role. The election administrators specify the election type and create aforementioned election, configurator ballots, register voters, decide the lifetime of the election and assign permissioned nodes.
- ii. Voters: For elections to which they are eligible for, voters can authenticate themselves, load election ballots, cast their vote and verify their vote after an election is over. Voters can be rewarded for voting with tokens when they cast their vote in an election in the near future, which could be integrated with a smart city project.
- iii. District nodes: When the election administrators create an election, each ballot smart contracts, representing each voting district, are deployed onto the block chain. When the ballot smart contracts are created, each of the corresponding district nodes are given permission to interact with their corresponding ballot smart contract. When an individual voter casts his vote from his corresponding smart contract, the vote data is verified by all of the corresponding district nodes and every vote they agree on are appended onto the block chain when block time has been reached.
- iv. Boot nodes : Each institution, with permissioned access to the network, host a boot node. A boot node helps the district nodes to discover each other and communicate. The boot nodes do not keep any state of the block chain and is ran on a static IP so that district nodes find its peers faster[22].

2. **Election Process** : In our work, each election process is represented by a set of smart contracts, which are instantiated on the block chain by the election administrators.

A smart contract is defined for each of the voting districts of the election so multiple smart contracts are involved in an election. For each voter with its corresponding voting district location, defined in the voters registration phase, the smart contract with the corresponding location will be prompted to the voter after the user authenticates himself when voting[22].

2.8 Block chain As A Services On E-Voting System Using Ethereum

With an intention to make E-voting more open , transparent and independently auditable, we have used the block chain technology on the Ethereum platform using solidity programming language. Block chain creates an immutable ledger, every time a transaction takes place. Once a vote is casted, it cannot be tampered. To make this into a decentralized application, we have written smart contracts in Solidity specifying the various conditions of the election[23].

Our smart contracts are responsible for communicating with the local block chain and running the election. After successfully running our smart contract, we were able to create an application for conducting elections with the help of ganache, which is our local block chain. It is user-friendly and an important advantage is that a voter can cast their vote from any location, thus increasing the overall participation. One account on block chain is associated with only one voter, who can cast only once, thus ensuring that there are no duplicate votes. The election results are displayed after the voter has finished voting, which guarantees complete confidentiality[23].

2.8.1 Dependencies Involved

To deploy smart contracts on an Ethereum block chain we need different application and software programmed for examples :

1. Solidity is an object-oriented programming language for writing smart contracts. It is used for implementing smart contracts on various block chain platforms but majorly Ethereum[23].
2. Geth: Go-Ethereum or Geth is one of three original implementations of the Ethereum protocol and it runs smart contract applications exactly as programmed without possibility of downtime, censorship, fraud or third party interference . This framework supports development beyond the Geth protocol, and is the most developer-friendly framework of the frameworks we evaluated. The transaction per second(transaction rate) is dependent on whether the block chain is implemented as a public or private network. Because of these capabilities, Geth was the framework we chose to base our work on, any similar block chain framework with the same capabilities as Geth should be considered for such systems[23].
3. Truffle Framework Truffle is a development environment testing framework and an important asset timeline for Ethereum. Truffle boxes are helpful boiler plates that allow you to focus on what makes a decentralized application unique. They also consist of other useful modules such as solidity libraries and front-end views, which help to complete the decentralized application. We have used the Truffle pet shop box in particular

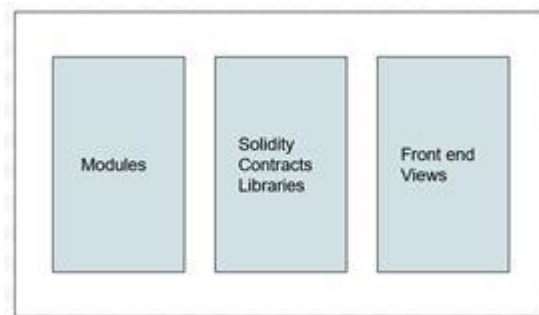


Fig. 2.14. Representation of Truffle Framework [23]

4. Ganache is a personal Ethereum block chain which mimics the characteristics of the main block chain. It can be used to run tests, execute commands and inspect state, while controlling how the chain operates[23].
5. Metamask gives the liberty to run Ethereum decentralized app (D-Apps) , right in your browser without running a full Ethereum node. A web browser can be converted into a

block chain browser by installing Metamask extension. It aids in managing our personal account that we need to pay for transactions.

6. Web3.js is a JavaScript library and the front-end module for our proposed system. It helps the clients to interact with the Ethereum block chain by performing actions like sending ether from one account to another, read and write data from smart contracts and also create new smart contracts[23].

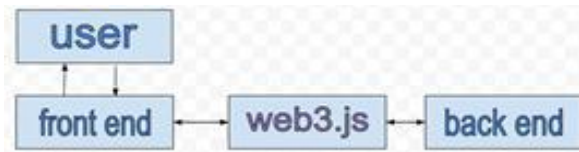


Fig 2.15. Overview of Web3.js [23]

7. Smart Contracts are the building blocks used to create the block chain. They are programs that we can write with source code and deploy to the block chain. They are written in Solidity programming language. Smart contract becomes the public ledge agreed upon the parties involved[23].

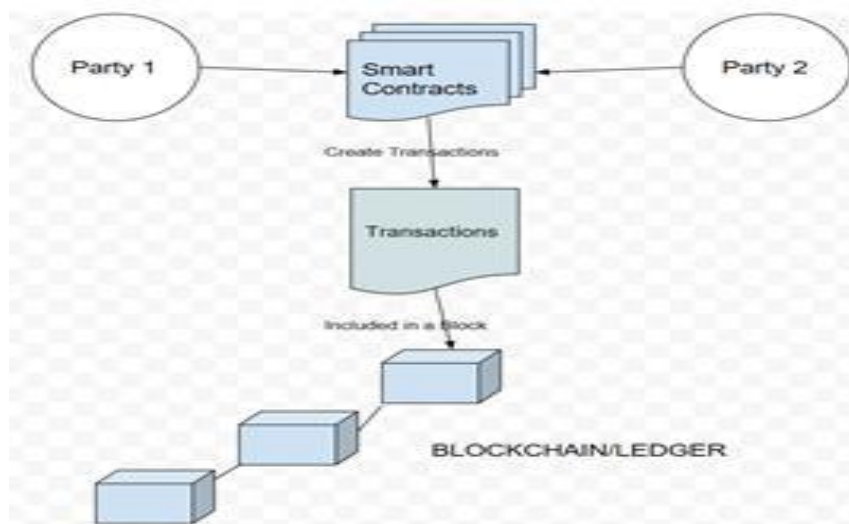


Fig 2.16. Illustration of client side application using smart contracts between two parties [23]

2.9 E-voting System Related Works

For a long time, many researchers are devoting to design a secure and efficient e-voting protocol. The first thesis related to cryptographic e-voting protocol was published by Chaum in 1981 and he used an anonymous commutation channel to encrypt the ballot [17]. With the developing of cryptography, a lot of protocols with its own properties had been proposed. In 1982, Richard A. DeMillo proposed a protocol requires all voters must participate and encrypt the ballot of each voter and at the end

cast the ballots [17]. The protocol encrypts the ballot by using homomorphism theorem and the government will release the tally result.

Yifan had Present a paper. The aim of this paper is to present design implemented a new web voting system software through PHP and JavaScript programming languages. A security analysis, software performance analysis and evaluation .On account of the pseudonymous of Bitcoin address and the openness of the block chain, which is consistent with part of e-voting requirement. This paper proposed an e-voting protocol based on block chain by using the ring signature algorithm. The requirements can be satisfied with ballot-privacy, individual verifiability, eligibility, completeness, uniqueness, robustness, and coercion[17].

In some cases, a trusted third party (TTP) is involved to make E-voting systems more easily implemented and controlled. However, a powerful TTP may also become the vulnerable spot of the whole system. A few efforts have been made to combine an e-voting protocol with the block chain paradigm to design a voting protocol without a TTP, which provides anonymity and verifiability as well [18].

Zhao and Chan proposed a voting protocol in 2015, which introduces a reward/penalty scheme for correct or incorrect behaviors of voters. Although the protocol has some limitations, this is the first attempt to combine E-voting with block chain [18].

Later in 2016, Lee, James, Ejeta and Kim proposed an e-voting protocol, which involves a TTP into block chain to preserve voters' choices. Very recently, using Bitcoin , Bistarelli, Mantilacci, Santancini and Santini proposed another e-voting protocol .This protocol divides the organizer of elections into two different parts - the Authentication Server (AS) and the Token Distribution Server (TDS), to protect voters' privacy. However, there remain some problems in this protocol, for example, it is difficult to inspect these two parts' behaviors, and it limits the extension of the voting scheme[18] .

2.10 Related Work Applications

The research of E-voting system is widely used nowadays. Some partial practices are listed as follows [14].

In 2000, E-voting has been used in US Election. Although it is an experiment in some area of Florida, it was a milestone in the development of E-voting [14].

In 2002, United Kingdom tried out an electronic voting system. 16 public authorities were awarded to build the e-voting system. After 1 year, more than 18 authorities were award[14].

In 2004, US election used an electronic voting system DRE for the first time. India uses this system for parliamentary elections on a national scale.

In 2007, France UMP party made a history of internet based voting. More than 31,000 voters vote in UMP to in 2007 French Presidential election. This was the first mass E-voting activity in history[14].

In 2009, China used electronic voting for the election of the grass-roots organization in Hangzhou. There were 3122 residents enrolled this voting activity with an electronic touch screen.

In 2014, the election of Ministry of National Education(France) received 1,760,000 ballots , it took the lead in legal and security network voting, thus popularized the channels of network voting[14].

Table 2.1 provides a brief overview of the systems that are in use throughout the world [14].

Table 2.1 Comparison Table E-Voting Systems Deployed All Over the World [14]

E-Voting Systems Deployed All Over the World								
Country	E-Voting	Company	Election Type	Electoral System	Introduced Year	Year Used	Software Used	Hardware Used
India	668 million	BHEL	State	FPP	2001	2009 2004 2003 2001	EPROM	EVM
Belgium	3.2 million	Steria	General & Municipal	Open PR-List	1994	1999	Digivote, Jites, Stesud	DEVS
Brazil	66 million	UniSys & Diebold	All Govt. Level		1996	1996 1998 2000 2002	GEMS	GX-1 integrated processor
Australia	218000	Software Improve	ACT federal	PR-STV	2001	2001	eVACS	PCs
UK	1.5 million	SVS	Local Govt.	FPP	2000	2000 2003	AVC	DRE
Spain	3000	Indra	Municipal	PR-List	2002	2003	SIRE	SIRE System
Canada	98000	Can Vote	Municipal	FPP	2002	2003	Can Vote On Linux	Can Vote On Internet

CHAPTER THREE

METHODOLOGY

CHAPTER III

METHODOLOGY

3.1 Introduction

A block chain is a distributed database , where the complete data is shared among all participants in the network. Data , which is supposed to be stored in this database, is packed into blocks with a defined maximum size and verified with a specific hash.

3.2 Block Chain E-voting System Requirements

The first transaction added to the block will be a special transaction that represents the candidate. When this transaction is created it will include the candidate's name and will serve as the foundation block, with every vote for that specific candidate placed on top of it. Unlike the other transactions, the foundation will not count as a vote, and it will only contain the name of the candidate. Our e-Voting system will allow a protest vote, where the voter may return a blank vote to demonstrate dissatisfaction with all candidates or a refusal of the current political system and/or election. Every time a person votes the transaction gets will be recorded and the Block chain will be updated[24].

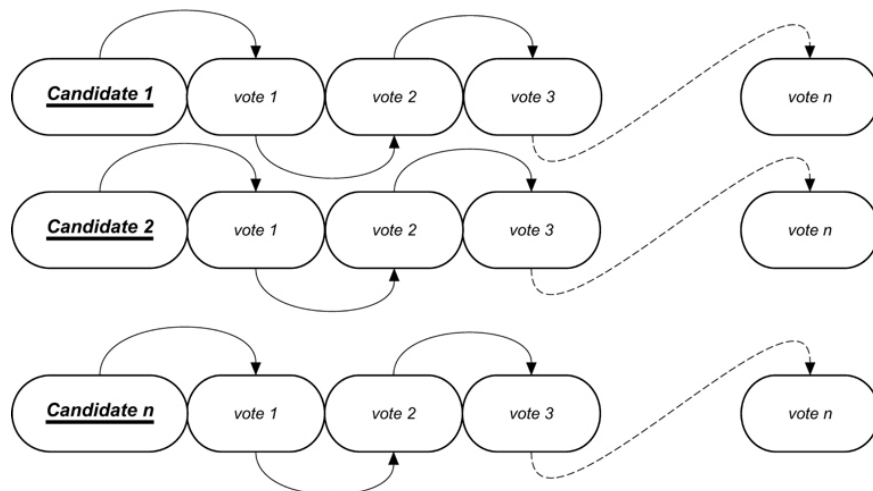


Fig 3.1. A simple Requirement of the Block chain Structure of each Candidate [24]

Fig 3.1 explain To ensure that the system is secure, the block will contain the previous voter's information. If any of the blocks were compromised, then it would be easy to find out since all blocks are connected to each other. The Block chain is decentralized and cannot be corrupted; no single point of failure exists. The Block chain is where the actual voting takes place. The user's vote gets sent to one of the nodes on the system, and the node then adds the vote to the Block chain. The voting system will have a node in each district to ensure the system is decentralized[24].

3.3 Representation of The E-voting System

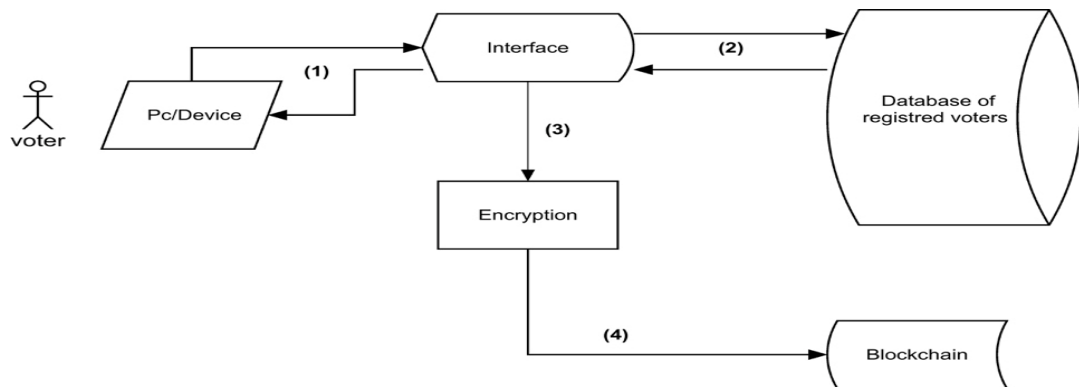


Fig. 3.2. A Simple Representation of the Block chain Structure of each Candidate

1. **Requesting to vote** : The user will have to log in to the voting system using his credentials in this case, the E-voting system will use his Social Security Number his address, and the voting confirmation numbers provided to registered voters by the local authorities. The system will check all information entered and, if matched with a valid voter, the user will be authorized to cast a vote. Our E-voting system will not allow participants to generate their own identities and register to vote. Systems that allow identities to be arbitrarily generated are usually vulnerable to the Sybil attack , where attackers claim a large number of fake identities and stuff the ballot box with illegitimate votes[24].
2. **Casting a vote** : Voters will have to choose to either vote for one of the candidates or cast a protest vote. Casting the vote will be done through a friendly user interface.
3. **Encrypting votes**: After the user casts his vote, the system will generate an input that contains the voter identification number followed by the complete name of the voter as well as the hash of the previous vote. This way each input will be unique and ensure that the encrypted output will be unique as well. The encrypted information will be recorded in the block header of each vote cast. The information related to each vote will be encrypted using SHA-256, which is a one-way hash function that has no known reverse to it. The only theoretically possible way to reverse the hash would be to guess the seed data and the encryption method and then hash it to see if the results match. This way of hashing votes makes it nearly impossible to reverse engineer, therefore there would be no way voters' information could be retrieved[24].
4. **Adding the vote to the Block chain**: After a block is created, and depending on the candidate selected, the information is recorded in the corresponding Block chain. Each block gets linked to the previously cast vote[24].

3.4 Mechanisms of E-Voting System

In this thesis we use block chain technology in the Ethereum platform. The power of smart contracts provides a wide range of use cases. Ethereum has a huge open source community that contains large types of software that can be used together to build a secure distributor app. Given the basic security that Ethereum provides from digital signatures to hashing, it is difficult to change the source code for the specific program. The election process takes place in three stages: the registration stage for the election, the polling stage, the stage of sorting results

First: The registration stage for the elections: in which the parties participating in the elections are registered according to the conditions provided by the Sudanese National Elections Commission, and the candidates are registered for election. Also, the voters are registered according to the geographical constituency of each voter and he is given a special code from the program that he uses in the voting phase.

Second: The voting stage: In this stage, the transaction between the voter and the server is encrypted using block chain technology.

Third: The stage of sorting the results: In this stage, the audio is coded using the AES algorithm and decoding.

3.5 Block Chain E-Voting System Architecture

The electronic voting system relies on the use of block chain technology, the national number and the fingerprint of the voter to verify non-tampering and fraud in the three stages of the system (registration stage, polling stage and results stage).

1. Registration Stage of The Election

The voter registration is done according to the geographical constituency, and the system administrator opens the registration stage for a specified period of time so that every person who has successfully completed the registration process can cast his vote in the voting stage. At this stage, the voter information and access to it is verified and approved by the fingerprint and the national number obtained from the civil registry. After that, the system gives the voter a special code that is considered a special registration number, such as the password used at the polling stage. The system sends the voter a SMS message on the phone previously entered in the registration process that contains his registration number.

After the end of the period specified for registration in the system, each voter gets his national number and his own registration number. There is a copy of the national number and the private registration number on the server. We have a fixed block chain that includes the numbers of all those who successfully complete the registration process. Voting according to the vote of each voter.

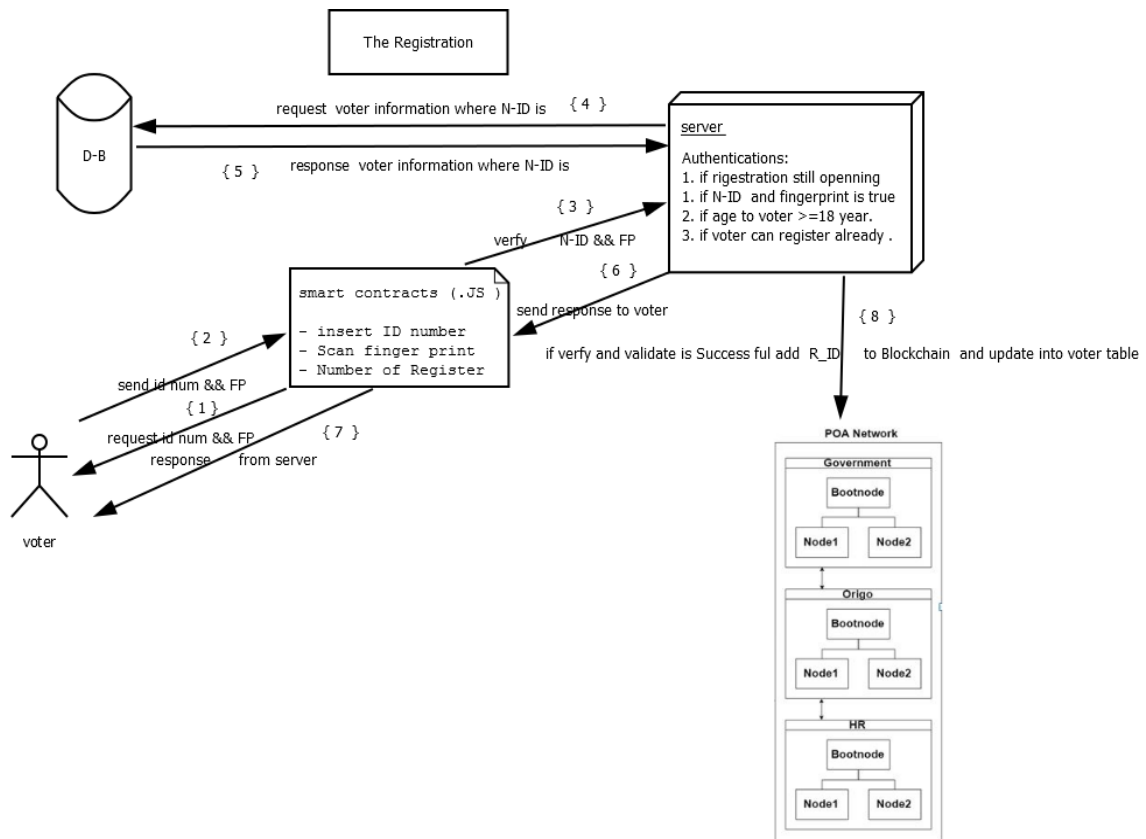


Fig 3.3. Registration phase

The system architecture contains two main constituents and a server shown in Figure 3.3

Voters:

- Step 1: Enter the national number and scan fingerprint.
- Step 2: Enter phone number and Choose the geographic circle.
- Step 3: save private number (Reg_num) .

Server:

- Step 1 : The voter is asked to enter the national number and his/her fingerprint .
- Step 2 : Request voter data from civil registry databases based on the national number.
- Step 3 : Verify and authorize the voter data, the correctness of the national number, the fingerprint, and the voter age is at least 18 years old, that he has not performed the registration process in advance and that the registration phase is still available and has not ended.
- Step 4 : sending a response to the voter according to the registration conditions .
- Step 5 : Save the national number and private number from voter in server and Give him the registration number (private number) if all conditions are met send SMS message to voter .
- Step 6 : Added voter data to the Block chain .

Create Block Chain

The chain of blocks that are present with each of the peers is the same since we are dealing with the same distributed ledger, block (n+1) is connected to the block (n) which is the block before it is using the hash of the previous block this is hash(n).

Hash of a block is a function of :

Hash (block (n+1)) = f (timestamp+ hash(block(n)) + payload+ version of the software + hash (Merkel root) + target+ Nonce).

So , if block(n) is tampered with, its hash changes, which means hash (block(n+1)) changes and then hash(block(n+2)) will also change and so on and so forth. This means that all the blocks after the modified block will have to change and each peer should calculate this individually which is compute intensive process so hence block tampering is not possible in such an infrastructure. Target is the difficulty value that is specified in the genesis file which specifies how difficult the puzzle is going to be for the peers to mine. Nonce is the random number that will be generated by the peers during mining. Whichever peer is able to generate the correct nonce will be rewarded. This is a part of the puzzle that peers solve. This is used for adding new blocks in the block chain. The block contents can be seen by using its hash as the identifier as a hash of one block is unique in a block chain. The contents of one block consists of the following information:

1. **Block hash:** This is the hash generated using the information about the hash of the previous block, the timestamp, the version of the software used, the Merkel root or the binary hashing of all the transactions that are present inside the blocks of the block chain, the difficulty value that is specified in the genesis file and the nonce or the random number that is generated in the mining process.
2. **Block Number:** This is the next consecutive number in the block chain.
3. **From:** This refers to the public key of the voter who has performed the transaction which is the vote in this case. As discussed, every voter is associated with a set of public, private keys.
4. **Gas Used:** This refers to the amount of gas or ethers used to complete this transaction. This is supplied by the voter who has performed transaction.
5. **Status:** This field gives information about whether the transaction is successful or not, status 1 stands for a successful transaction and 0 if unsuccessful.
6. **To:** This is the public address of the smart contract to which the transaction is submitted to.
7. **Transaction Hash:** It is an identifier that uniquely identifies a particular transaction.

2. The Pallot Phase For Election

Candidate registration in The ballot phase is conducted by the election administrators. When an election is created the election administrators must define a deterministic list of eligible voters. This might require a component for a government identity verification service to securely authenticate and authorize eligible individuals. Using such a service is necessary to satisfy the requirement of secure authentication as this is not guaranteed, by default, when using a block chain infrastructure. In our work, for each eligible voter, a corresponding identity wallet would be generated. A unique wallet is generated for each voter for each election that the voter is eligible to participate in. Verifying votes In the voting transaction, each voter receives the transaction ID of his vote. In our e-voting system, voters can use this transaction ID and go to an official election site (or authority) using a block chain explorer and (after authenticating themselves using their electronic identification) locate the transaction with the corresponding transaction ID on the block chain. Voters can, therefore, see their votes on the block chain, and verify that the votes were listed and counted correctly. This type of verification satisfies the transparency requirements while preventing traceability of votes.

Voting transaction: Each voter interacts with a ballot smart contract for her corresponding voting district. This smart contract interacts with the block chain via the corresponding district node, which appends the vote to the block chain. Each individual voter receives the transaction ID for their vote for verification purposes. Every vote that is agreed upon, by the majority of the corresponding district nodes, is recorded as a transaction and then appended on the block chain. Figure 3.2 is a visual representation of this process. A transaction in our proposed system (see Table 3.1) has information on :

1. the transaction ID.
2. the block which the transaction is located at.
3. to which smart contract the transaction was sent which indicates from which voting district the vote was cast.
4. The value of the transaction, i.e. the vote, indicating which entity (party) the voter voted for.

A voting transaction in our system, therefore, reveals no information about the individual voter who cast any particular vote.

table. 3.1 Example of an transaction in our system

TxHash	Block	To	Num of vote
0xdeadbeef...	1337	Person 1	2
0xG1345edf...	1330	Person 3	6

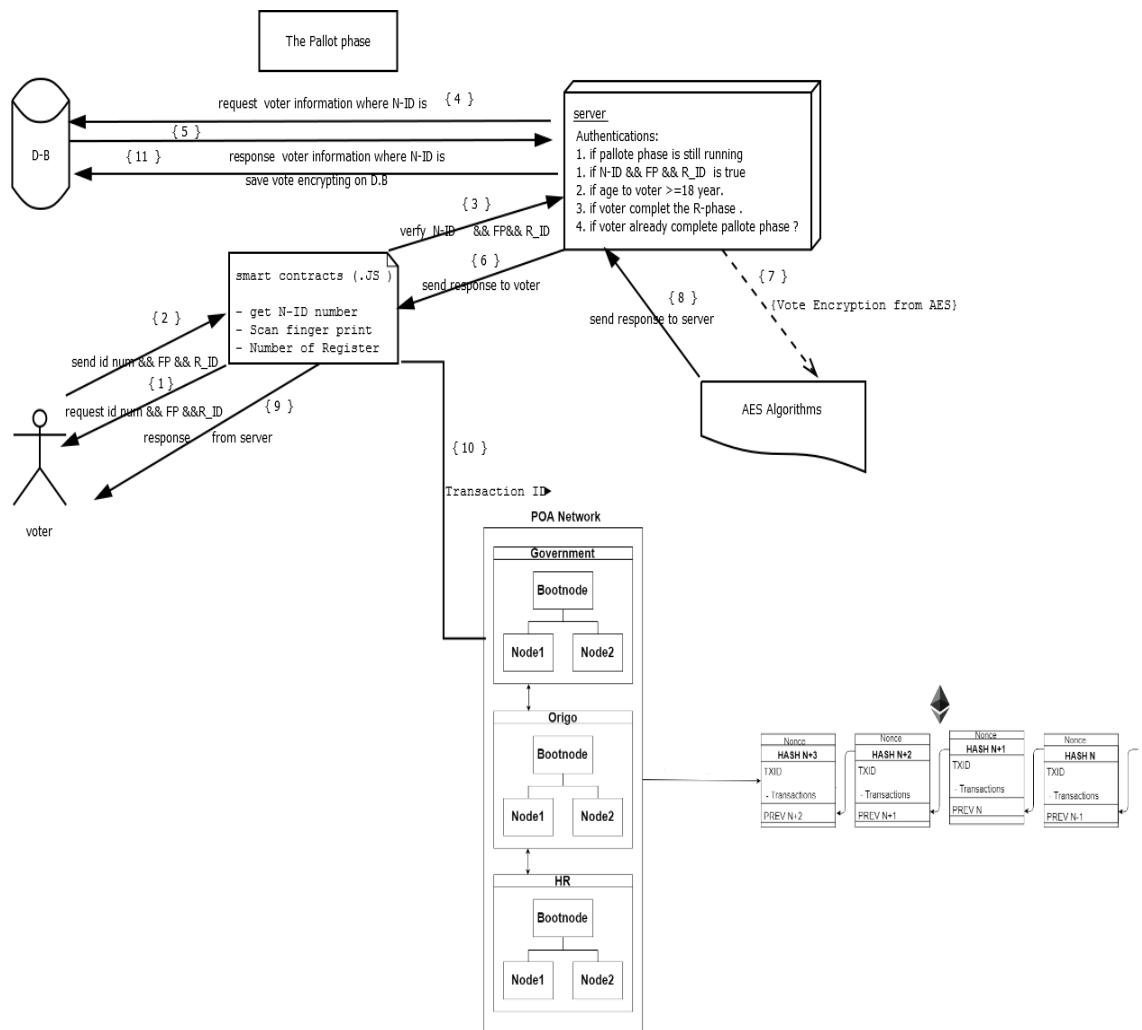


fig 3.4. Pallote phase

The following are the main activities in the election process show figure 3.4:

Voter :

- Step 1: Enter the national number and Scan finger print.
- Step 2: Enter the private number (Reg_num) .
- Step 3: Choose favorite candidate and vote for him/ her .

Server :

- Step1: The voter is asked to enter the national number, his / her fingerprint and his / her registration number.
- Step 2 : Request voter data from civil registry databases based on the national number.
- Step 3: Verify and authorize the voter data, validity of the national number, fingerprint, and voter age of at least 18 years, that he/she has successfully completed the registration phase and that the voting stage is still available and the time period has not ended.

- Step 4: Requesting the list of candidates from the results table on data base.
- Step 5 : Show the candidate list to the voter so that he can choose his candidate.
- Step 6: Receive the voter nomination and send it to the AES algorithm .
- Step 7: Receive the encoded filter from the encryption AES algorithm.
- Step 8: The voter nomination is saved in an encrypted form in the database.

Update The Block Chain

All transactions which were received and verified in the ongoing block time are deployed onto the block chain after the block time has reached its time limit . With each new block added to the block chain, each district node updates his copy of the ledger.

Vote transaction When an individual votes at a voting district, the voter interacts with a ballot smart contract with the same voting district as is defined for any individual voter. This smart contract interacts with the block chain via the corresponding district node, which appends the vote to the block chain if consensus is reached between the majority of the corresponding district nodes. Each vote is stored as a transaction on the block chain whereas each individual voter receives the transaction ID for their vote for verifying purposes . Each transaction on the block chain holds information about whom was voted for, and the location of aforementioned vote. Each vote is appended onto the block chain by its corresponding ballot smart contract, if and only if all corresponding district nodes agree on the verification of the vote data. When a voter casts his vote, the weight of their wallet is decreased by 1, therefore not enabling them to vote more than once per election. A single transaction on the public Ethereum block chain includes the transaction ID, the block which the transaction is located, the age of the transaction, the wallet which sent the transaction and who received it, the total value which was sent and the transaction fees[27].

Mining and generating of voting Block

Mining and generation of voting blocks All votes in the block chain are cryptographically linked block by block. Many secure hash algorithms can be applied to solve the problem of condensing the message in the current block to produce a message digest, such asSHA-256.New block is generated by users from the P2P network .The new block generation is based on POW algorithm. When a new vote is submitted and verified, miner generates a new block with the information of vote and broadcasts the new blocks to the network. If new block shave the same timestamp, the block with a higher value of signature is selected over others.[27]

Advance Encryption Standard (AES) Algorithms

Encryption Process [28]

1. At a time it takes a plain text and divides it into sub-blocks, these sub-blocks are the inputs for the first round of the algorithm. If the size of plain text is 128 bits, it will be divided into 16 bytes sub-block.
2. For 128 bits key the encryption process is executed in 10 rounds.
3. The 16 Byte sub-block are substituted by a fixed table (S-box). The result comes out in a matrix of four rows and four columns.
4. In this stage Shift Rows phases of AES, each row of the 128-bit internal state of the cipher is shifted. The rows in this stage refer to the standard representation of the internal state in AES, which is a 4x4 matrix and cell contains a byte. Bytes of the internal state are placed in the matrix across rows from left to right and down columns. In the Shift Rows operation, each of these rows is shifted to the left by a set amount. Their row number starting with zero. The top row is not shifted at all; the next row is shifted by one and so on. The result is a new matrix consisting of the same 16 Bytes.
5. The Mix Columns stage provides diffusion by mixing the input around. A mathematical function is using transform each column of four bytes. This function takes as input the four Byte of one column and outputs four completely new bytes, which replace the original column. The result is a new matrix consisting of the same 16 new Bytes. These rounds perform the 10 times and output produced is ciphertext consisting of 128 bits.
6. The Round key stage, The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Decryption Process [29]

The decryption process is the same as the reverse order of the encryption process. It's every round consider four process reverse order of the encryption process.

1. Round key
2. Mix columns
3. Shift rows
4. Byte substitution

Above mention, sub-process is reverse order of the encryption process and its process converted cipher text to plain text.

3.6 Data Flow diagram

Figure No. (3.5 and 3.6) shows the sequence of electronic voting operations.

3.6.1 Registration phase

In this stage, the voter enters the national number and takes action. Fingerprint scanning The system verifies that the voter is the same person who holds the national number and fingerprint through his statement from the civil registry if the result is correct and meets all registration requirements. If the data are correct, the system sends the voter a special number that is considered as a code or registration number, after which the system sends the voter a text message with the special registration number and creates a block chain for voter registration. Allow the voter to enter and complete the registration process. If one of the conditions is violated, the system sends SMS message and stops the process. If the voter loses his registration number (the private number), he can enter the national number and the geographical district in which he was registered, in addition to his fingerprint before the registration period ends. Both systems can return its registration number to it.

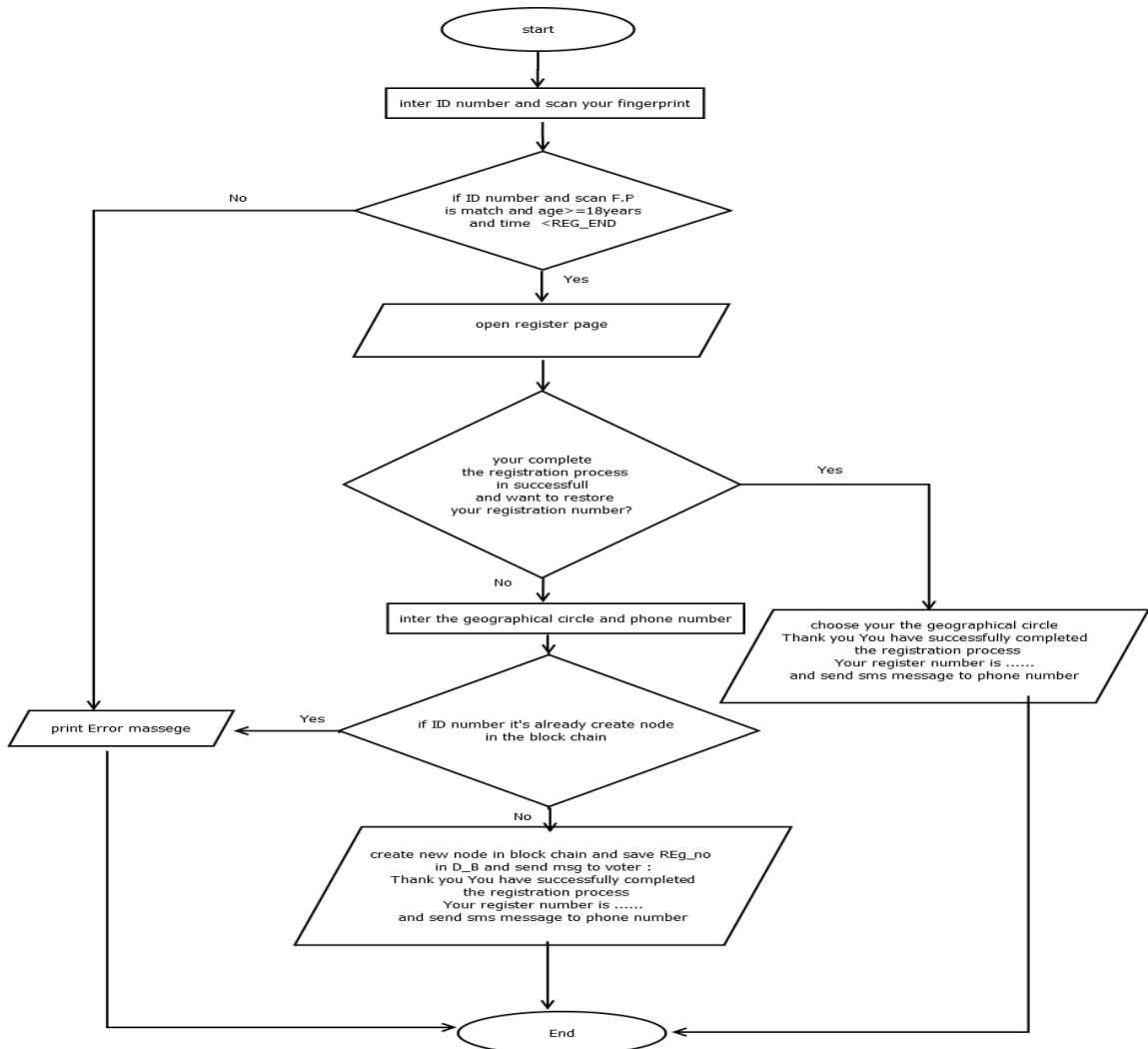


fig. 3.5. DFD register phase

3.6.2 Polling phase:

At this point, the voter enters the national number. Then the system requires the voter to enter a fingerprint to verify that the voter is the same person who carries the national number, then enter his own registration number (a special code) in the first stage if the result is correct to allow the voter to enter and complete the voting process. In the event that one of the conditions is violated, the system sends a message and stops the process. The system provides the voters with a list of candidates so that the voter can choose after the voter selects his candidate. A situation in which he does not want to vote for any of the candidates present, either to cancel the entire process or to pressure a neutral candidate from the list. The system then updates the block chain for candidates and voters and saves the filtering result in an encrypted vote used by the AES algorithms within the database so that it is not tampered with.

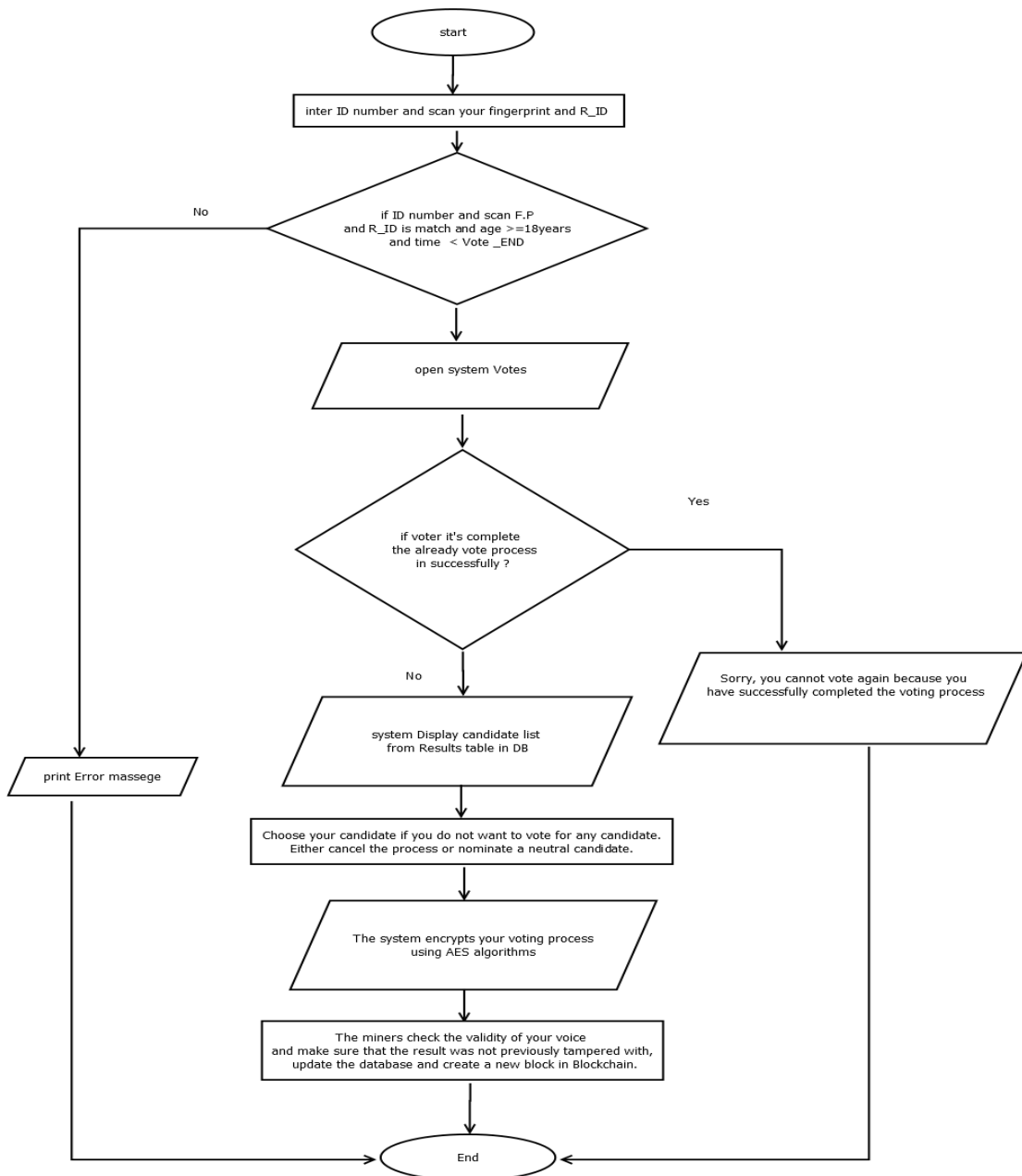


fig 3.6. DFD Polling phase

3.7 Unified Modeling Language (UML) Analysis

In this section discuss the analysis process of the proposed model (electronic voting). The analysis process performed by the Unified Modeling Language in two parts: use case diagram and sequence diagram.

3.7.1 Use Case Diagrams

Figure (3.7) shows the voter as actor takes the simple steps listed above and shows them as actions the voter might perform. These procedures are the process of registration, entry , voting and show results.

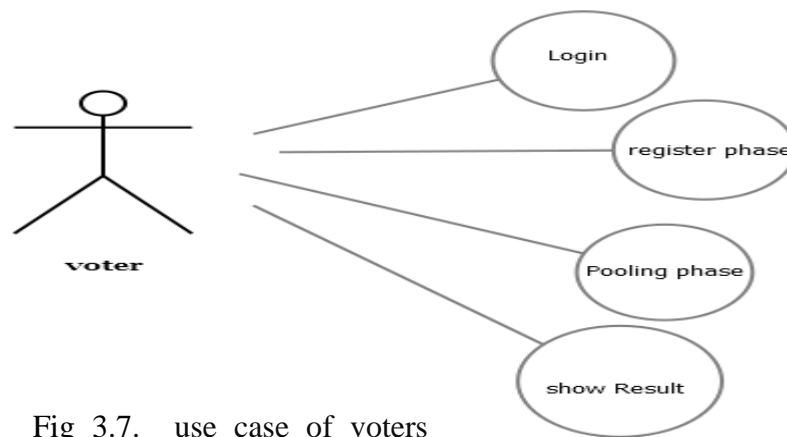


Fig 3.7. use case of voters

Figure (3.8) shows the supervisor as an actor. The graph takes the simple steps listed above and displays them as actions that the supervisor may take. These procedures are controlling the beginning and end of the registration phase in the system, the beginning and end of the polling phase in the system, managing the voters page from entering data, updating and deleting, managing the candidates page, managing the states page, managing the parties page, controlling the electoral process results table and adding candidates to Result table , and (CRUD) create, read, update and delete operations on system pages.

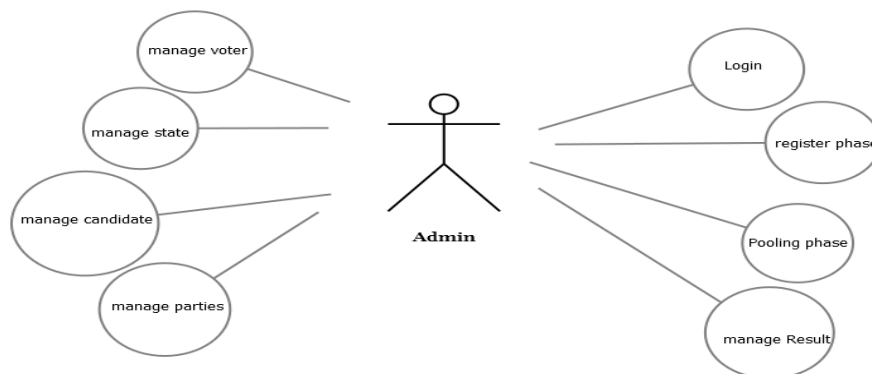


Fig 3.8. use case of admins process

3.7.2 Sequence Diagrams

Sequence diagrams demonstrate the behavior of objects in a use case by describing the objects and the messages they pass. The diagrams are read left to right and descending. The example below shows an object of class 1 start the behavior by sending a message to an object of class 2 . Messages pass between the different objects to the object of class 1 receives the final message.

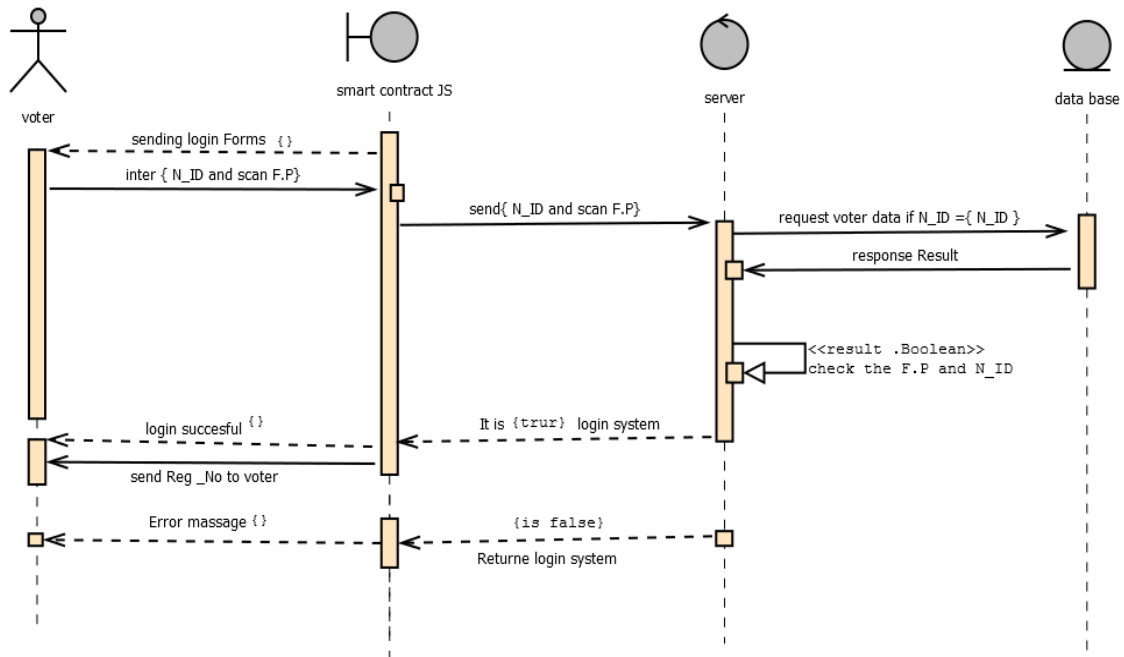


Fig 3.9. sequence of login voter

Figure (3.9) shows the voter login process:

1. The Smart Contract (SC) sends the registration form to voters.
2. The voter enters the national number and scan fingerprint.
3. (SC) sends voter data to the server to validate voter data.
4. The server requested the database to give it all the information of the voter.
5. The database sends response the voter data to the server.
6. The server verifies the voter data with the following: (Sudanese, 18 years or older, N_ID and F.P it is true , and the registration period did not end).
7. The server checks whether the voter has performed the registration process before or not, it is first time.
8. The response is sent to the (SC), which is, according to the following result from the server.
9. If the result is correct that he has registered before, you send the user that he has completed the registration process before.
10. If the login is valid and he did not register before, you send the voter a thank you. You have successfully completed the registration process and your registration number is and send SMS message to voter .

11. If there is an error in its entered data and the entry is not sent to the voter an error message.
12. The server update REG_NO (private number) from voter where N_ID = N_ID

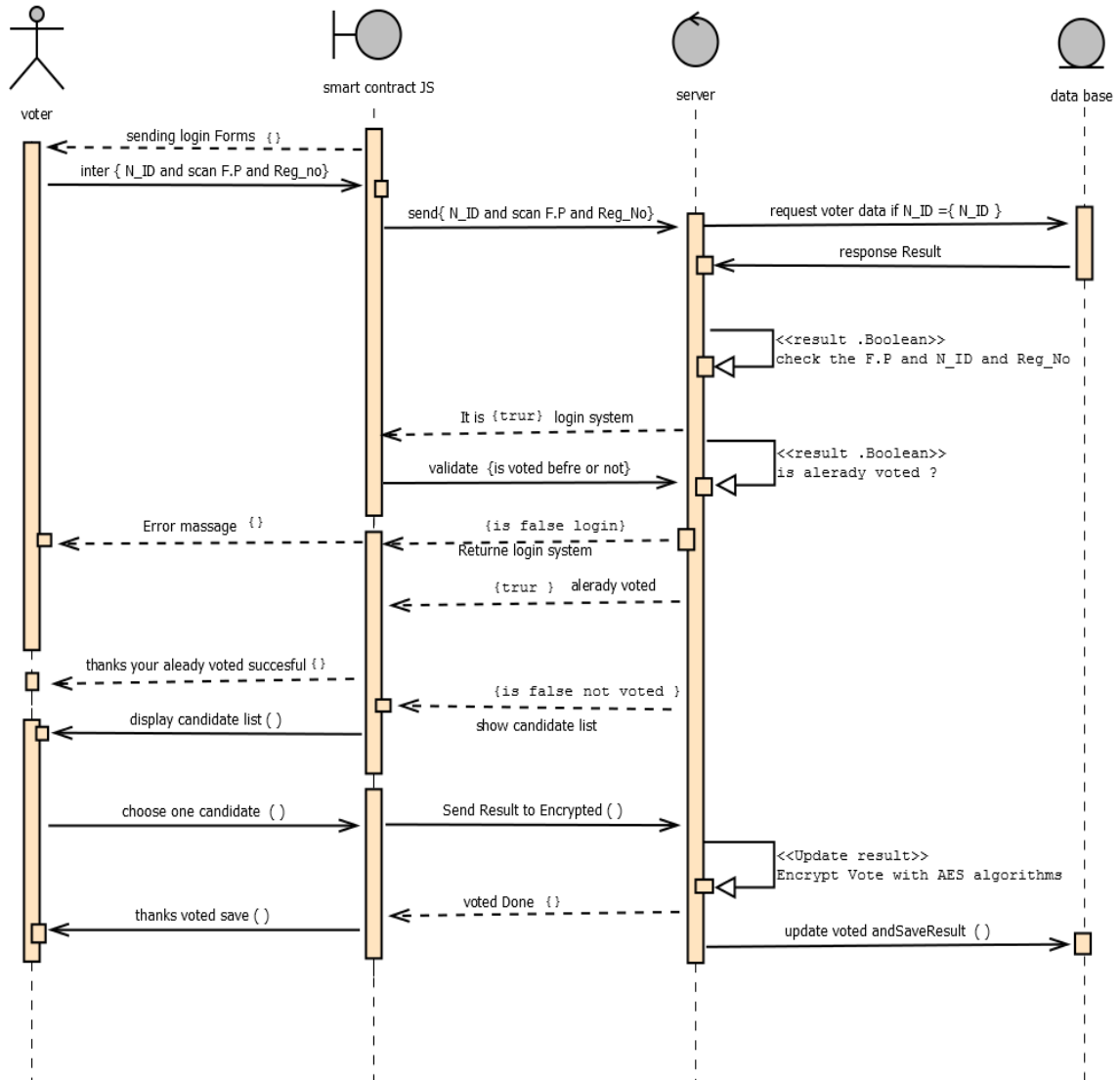


Fig. 3.10. sequence voting process

Figure (3.10) explains the polling phase. The voter enters the national number, and scan fingerprint and registration number, then sends data to the system. The system must verify that the voter has already been registered at the registration stage. If it is not registered, the system sends an error message to the voter. If he registered, the system submits the list of candidates so that the voter can vote. If the voter votes before this time, the system prevents him from voting again. Finally, the system encrypts the vote (AES) algorithms and saves it in the database and sends a message to the voter stating that the vote was successful.

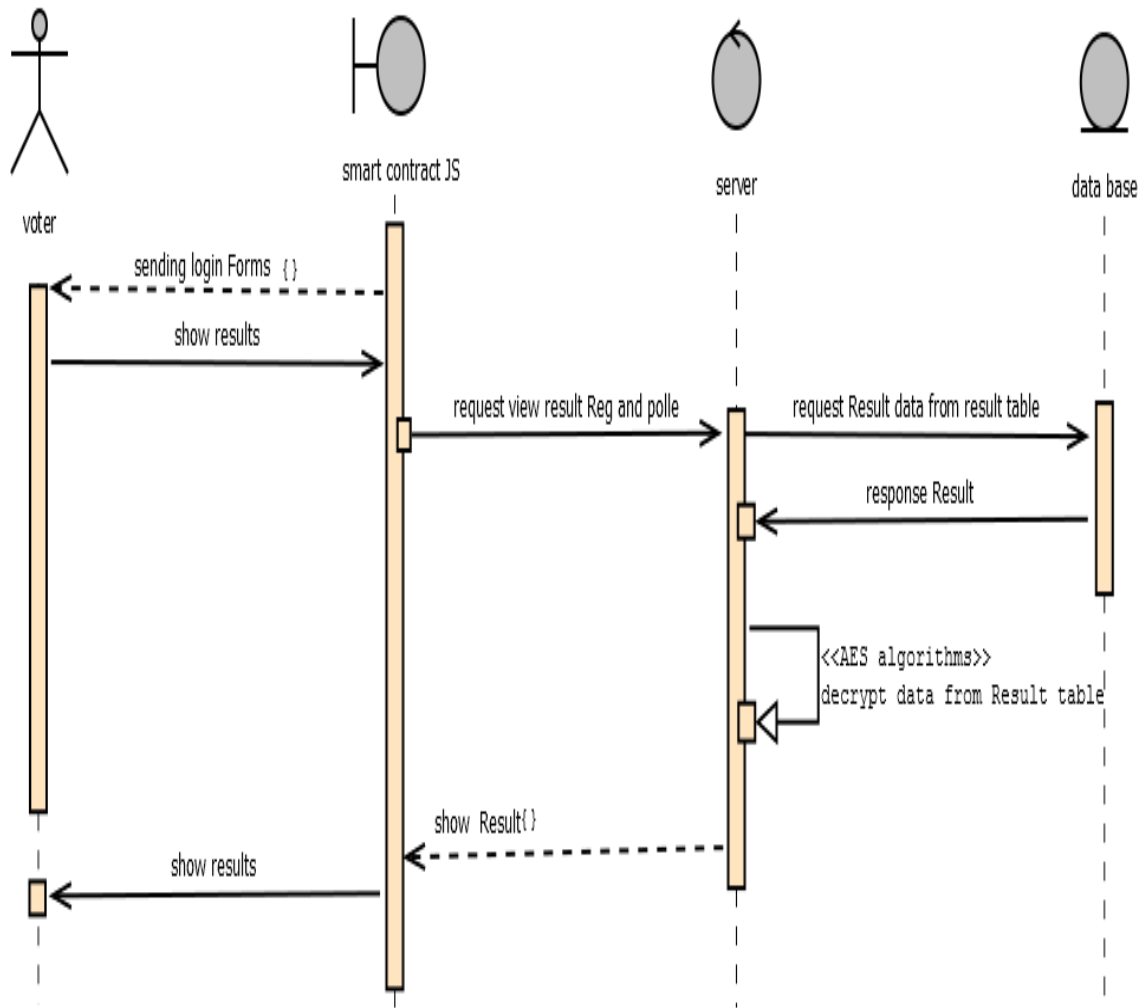


Fig 3.11. sequence of election result process

Figure (3.11) Explanation of the result stage, whereby the system displays the results to the voter, the candidate, and everyone who wishes to see the results of the voting and registration results.

The voter requests the display of results from the smart contract and sends the request to the server, who then requests the databases to display the results table and the response comes from the database with the result encoding, then the server decodes the results(AES) algorithms and sends them to the voter to view them.

3.8 Designing Stage

Design is to build a logical model for the developed system that shows how the system works and the interaction of the system parts with each other. Therefore, the design is concerned with how to find the solution, that is, how to achieve the basic functions of the system and the design stage includes choosing the techniques used in building the system such as (language of the language, protocols, and systems Databases and others) because these technologies affect how the solution will be found by the system.

1. Input And Output Design Process

The entrance to the design process is the diagrams of the entities in the analysis and the output at this stage is:

1. Database design.
2. Design categories diagram.

3.8.1 Create Tables Inside The New Database

Before we start creating spreadsheets, we must create the database via phpMyAdmin using the xampp dashboard and create the database with the name bac Then we create tables. The electronic voting system using fingerprint and block chain technology must contain 6 tables. These tables are:

1. candidate Table

Table 3.2 .Candidate table

Column	Type	Null	Default	Extra	Links to
c_no	int(5)	No		auto_increment	-> voter.v_no
c_name	varchar(255)	No			
c_age	varchar(30)	No			
c_address	Text	No			
c_pa_no	int(3)	No			
c_type	int(11)	No			
c_state	int(3)	No			-> parties.pa_no
visible	int(11)	No	1		
c_edu_degree	varchar(50)	Yes	NULL		
c_job	varchar(50)	Yes	NULL		
c_phone	varchar(20)	Yes	NULL		
c_email	varchar(50)	Yes	NULL		
c_photo	varchar(255)	No	unknown.png		
image	Text	No			

2. Parties Table

Table 3.3. parties table

Column	Type	Null	Default	Extra
pa_no	int(3)	No		auto_increment
pa_name	varchar(255)	No		
visible	int(11)	No	0	

3. Result Table

Table 3.4. Result table

Column	Type	Null	Default	Link to
c_id	int(11)	No		
c_votes	varchar(255)	No	0	-> candidate.c_no
voter_date	Datetime	No		

4. State Table

Table 3.5. State table

Column	Type	Null	Default	Extra
st_no	int(3)	No		auto_increment
st_name	varchar(255)	No		
visible	int(11)	No	1	

5. Users Table

Table 3.6. Users table

Column	Type	Null	Default	Extra
id	int(22)	No		auto_increment
username	varchar(255)	No		
password	varchar(255)	No		
firstname	varchar(255)	No		
lastname	varchar(255)	No		
email	varchar(255)	No		
date	datetime	No	CURRENT_TIMESTAMP	

6. Voter Table

Table 3.7. voter table

Column	Type	Null	Default	Extra	Links to
v_no	int(11)	No		auto_increment	
v_name	varchar(255)	No			
v_nat_no	varchar(15)	No			
v_state	int(3)	No	1		-> state.st_no
v_address	Text	No			
v_age	int(3)	No			
v_reg	int(3)	No	0		
status	int(11)	No	0		
v_gender	int(15)	No	1		
v_den	varchar(255)	No			
v_job	varchar(255)	No			
v_phone	varchar(255)	No			
v_email	varchar(255)	No			
v_reg_loc	varchar(255)	No	موطن خلا		
date	Datetime	No	CURRENT_TIMESTAMP		
v_photo	varchar(255)	No			
fingerprint	Text	No			
v_date	Datetime	No			

3.8.2 Design Category Diagram

1. Candidate page

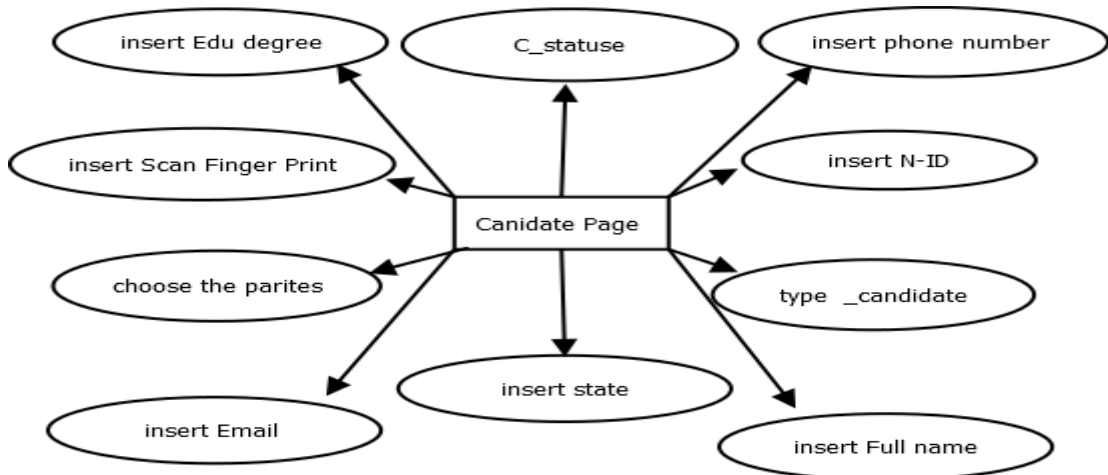


Fig 3.12 manage from candidate page

2. Parties page

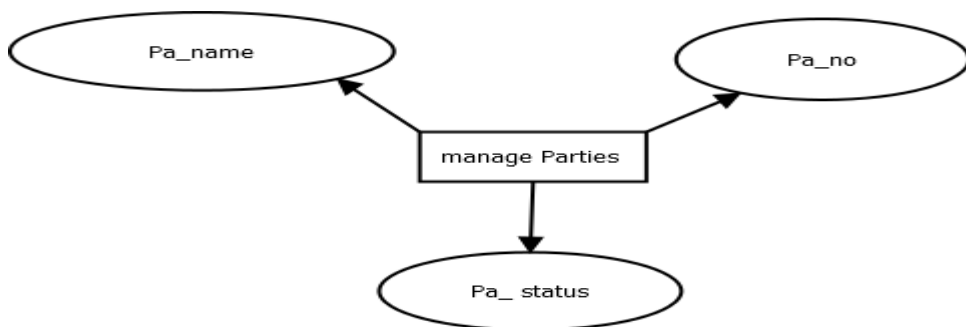


Fig 3.13 manage from parties page

3. State page

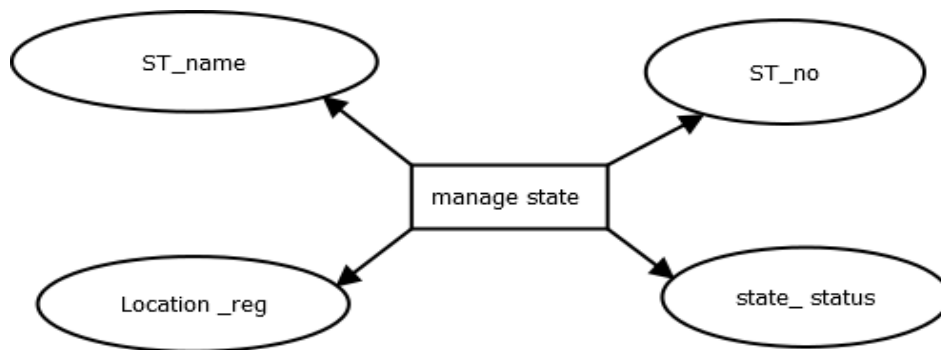


Fig 3.14 manage from state page

4. Voter page

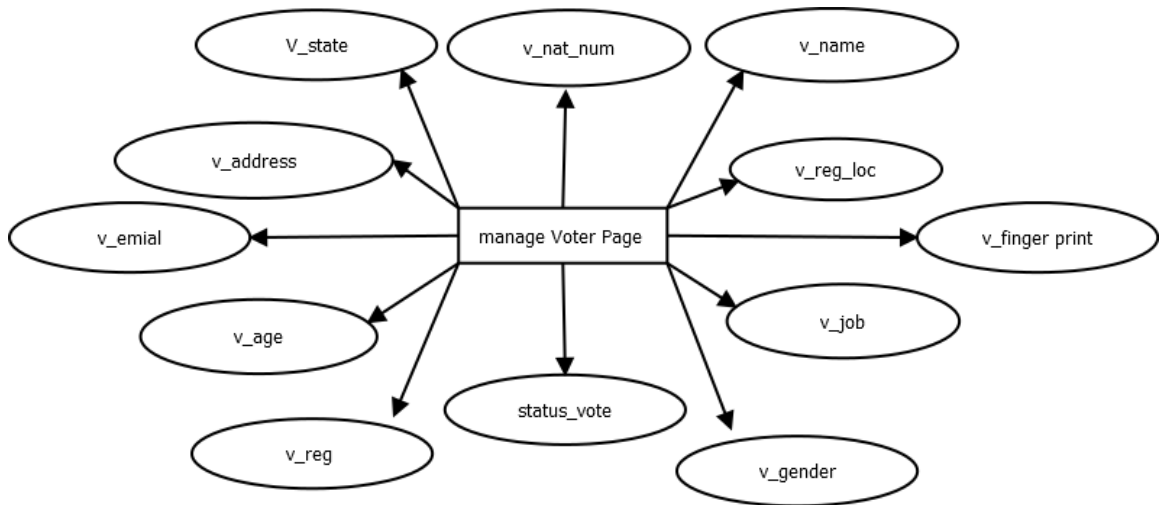


Fig 3.15 manage from voter page

5. Login Admin page

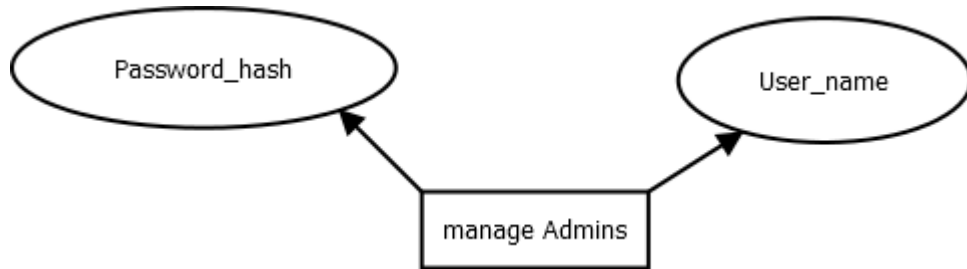


Fig 3.16 manage Admin login

6. Register phase voter

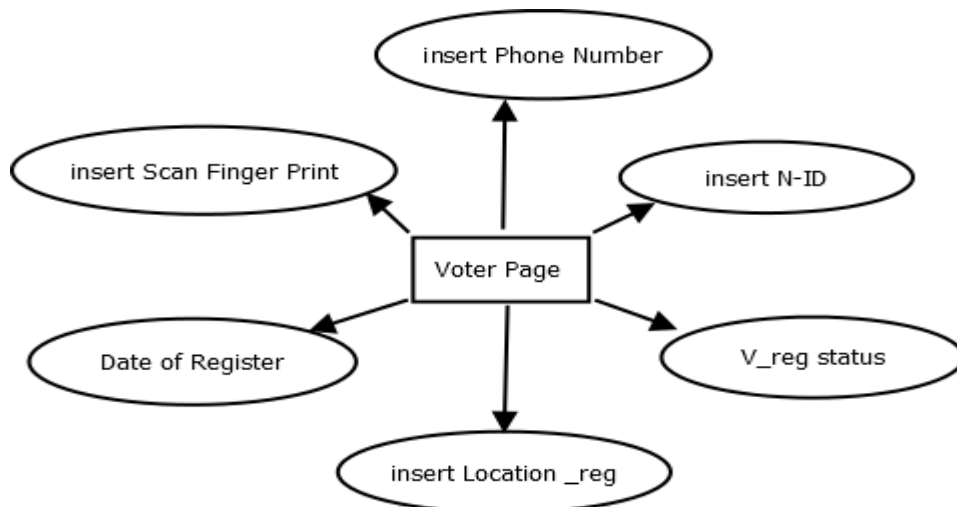


Fig 3.17 manage Admin register phase

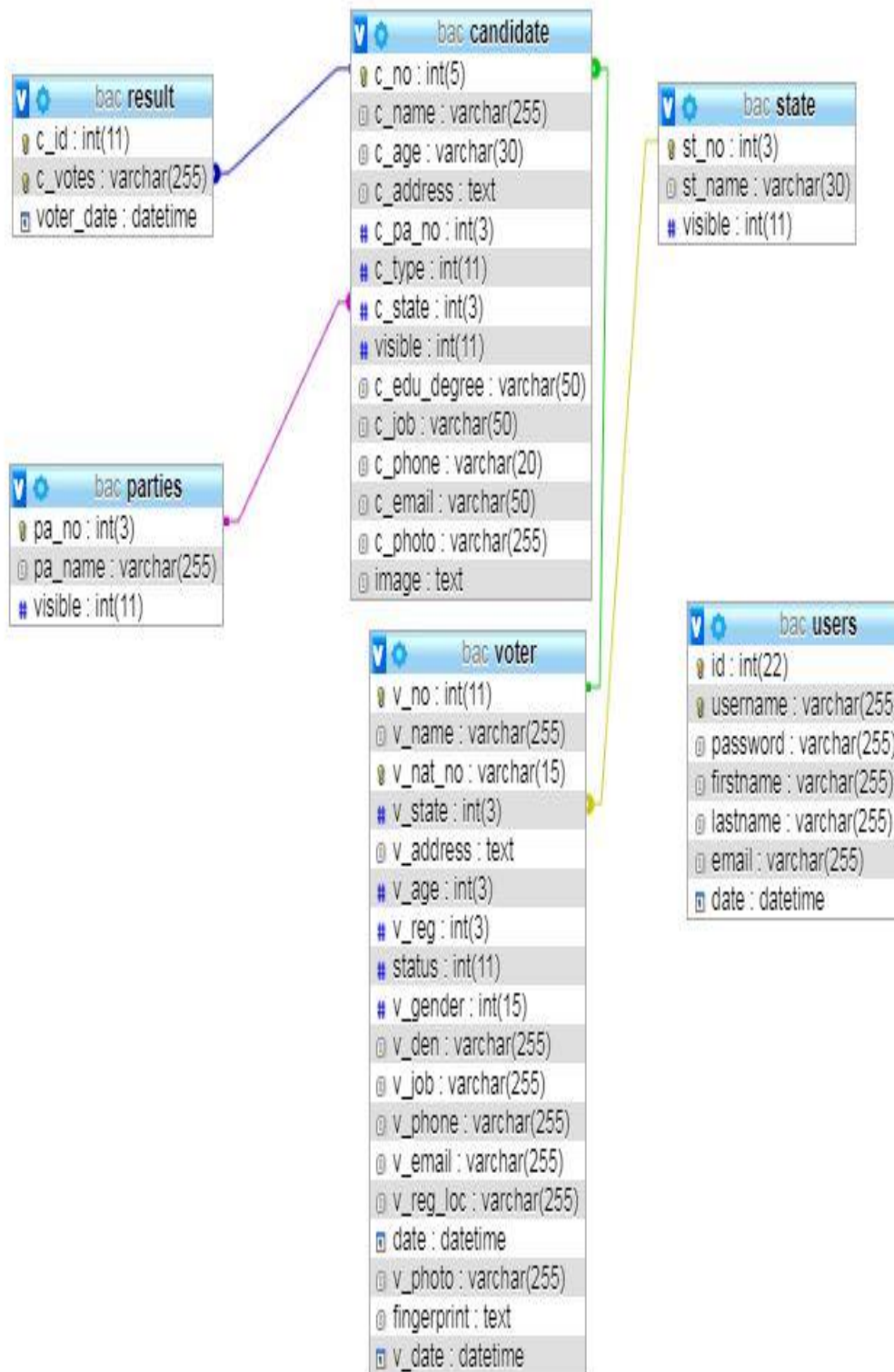


Fig 3.18 Relational schema tables

CHAPTER FOUR

IMPLEMENTATION

CHAPTER IV

IMPLEMENTATION

4.1 Introduction

This chapter displays implementation and security analysis. The first section shows the sequence of screens and the function of each screen in the system and the second section displays the attacks and the test whether this system has achieved security and integrity and confidentiality and enjoys the security analysis.

This system was applied to the Sudanese National Elections Commission in the presidential elections in all the localities of Khartoum State. The system was divided into three phases (registration, voting and the results counting phase). In the registration phase, each of the candidates and parties that want to participate in the elections and the voter registration are registered according to the geographic constituency for each one and the system then gives the voter a special registration number (code), in the form of a text message, and at the end of the registration phase, it is used in the voting stage. It can never be modified and the number of votes is stored in encrypted form using the AES algorithm in the databases, decoding it again and displaying the vote results whenever requested.

4.2 Overview of The Secure Electronic Voting Using Block Chain Technology

This section does a high level overview of the voting scheme. The process is divided into two main Phases:

1. Registration Phase.
2. Voting Phase, and the Tallying Phase.
3. Admin pages and Control of system .
4. Result Phase .

4.2.1 Registration Phase

As we mentioned at the beginning of this chapter, an accurate and comprehensive voter registry is an essential component of a reliable election. The first problem is how to perform the validation online because the proposal solution offers a complete online voting system.

There is a lot of research and methodology in online authentication such as fingerprint, voice recognition, or special devices granted to the authorized user. All of these procedures require special hardware and require more cost to implement, so there is a

need for another method to do the registration and corresponding authentication in a fully reliable way. The solution to the proposal is to separate the registration stage in a special system that is implemented in the registration center. The voters' data are verified by the national number and fingerprint through the civil registry. If the data in the registry matches what has been entered, the registration page opens and the voter completes the registration process and the system then sends to the voter A text message containing the voter's registration number. This number is used at the polling stage. If the voter loses his registration number, he can retrieve the number according to the data entered by the voter, the phone number and the geographical constituency.

Registration System

Create a complete registry system that is well implemented in the registration center. In this system the following procedures are performed:

1. At the beginning of the electronic registration stage, the voter enters his national number and fingerprint, and the registration authority (RA), which is the civil registry, checks the entered voter data to verify whether the voter is eligible.
2. After RA verifies eligibility, the voter now enters the registration system and completes the registration process and enters his / her geographical area and phone number by going to the nearest Public Service Center.
3. The voter then obtains a special registration number (code), which will be a unique code to log into the voting system.
4. After completing the electronic registration phase, the voters' data is saved in a series of blocks and databases that are divided according to the type of the voter and his geographical distance. The system sends the voter a text message containing his registration number.

Figure (4.1) and (4.2) The system requires the voter to enter the national number and fingerprint to verify his age based on the civil registry data stored in the databases and then pass it to the server.



Fig 4.1 Registration login



Fig 4.2 insert ID_Num and scan Finger print

Figure (4.3) The system verifies the national number and fingerprint, and whether the voter has the authority to enter the registration system or not, in the event that the voter has previously conducted the registration process in violation of any of the registration conditions, an error message appears.

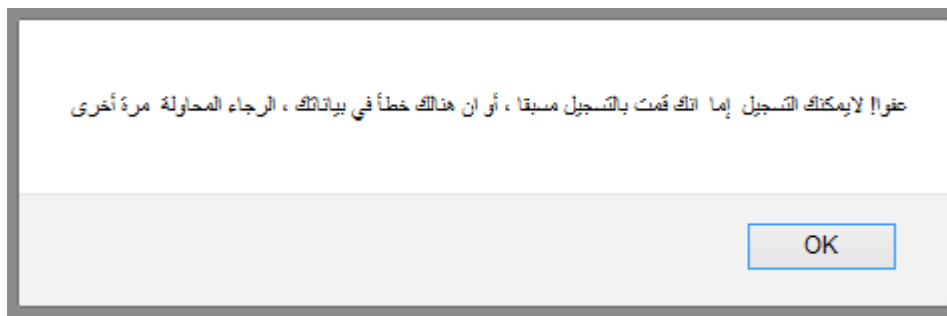


Fig 4.3 The system verify information

Figure (4.4) and (4.5) The system verifies the national number and fingerprint, and whether the voter has the authority to enter the registration system or not, in the event that the voter has passed the conditions, the voter's data appears in conformity with the civil registry data and the system gives the voter a special registration number as his private key.

جمهورية السودان
المفوضية القومية للإنتخابات

بيانات الناخب :
هذه البيانات مأخوذة من السجل المدني ، لاى تعديل في هذه المعلومات الرجاء التوجه الى أقرب مركز لخدمات المقيوم

البيانات الأساسية :

الاسم : محمد الفتح حيدر صالح

تاريخ التوثيق : 11/17/2006

العنوان : الخرطوم

العمر : 18

رقم الهاتف : 092078213

محافظة الانتخاب : الخرطوم

البريد الإلكتروني : m7mes@gmail.com

Fig. 4.4 information of voter

جمهورية السودان
المفوضية القومية للإنتخابات

معلومة مهمة :

يجب عليك حفظ رقم التصويت لكي تتمكن من التصويت
مرحبا بك : محمد الفتح حيدر صالح
رقم التصويت الخاص هو : 2

التصويت الإلكتروني © Show Results 2020

Fig. 4.5 system give voter Reg_num (code)
and Send sms message to voter

Figure (4.6) and (4.7) In the event that the voter has forgotten his registration number, he can press the button to restore the registration number, after which a slot appears in which he enters the voter's data from his fingerprint, the national number, the phone number and the geographical constituency.

لاستعادة رقم التسجيل الخاص بك الرجاء ادخال

الرقم الوطني

قم بإختيار بصمة الاصبع التي أدخلتها

No file selected.

رقم الهاتف

الدائرة الجغرافية التي سجلت بها

اختر اسم المنطقة

لاستعادة رقم التسجيل الخاص بك الرجاء ادخال

11617306662

قم بإختيار بصمة الاصبع التي أدخلتها

2.jpg

●●●●●●●●

الدائرة الجغرافية التي سجلت بها

محلية كرري

Fig 4.6 and Fig 4.7 recovery Reg_num

Figure (4.8) In the event that the voter entered his data and was approved by the system, the system gives the voter his registration number and send sms message to voter the reg_num is before the end of the specified registration period.



Fig. 4.8 system give voter Reg_num again and send SMS message to phone number

Figure (4.9) In the event that the voter has entered his data and has been approved by the system, the system sends an error message to the voter

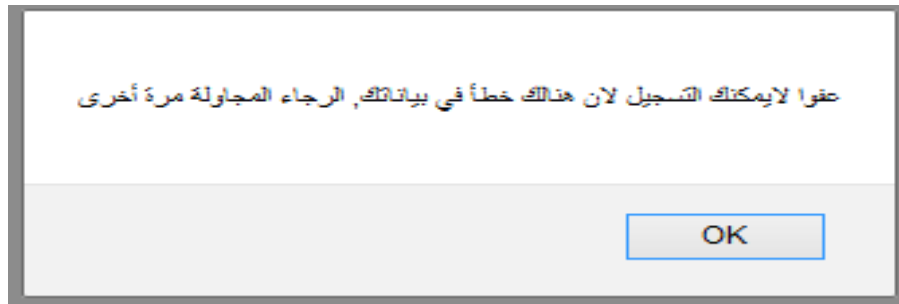


Fig 4.9 Error message from system to voter

4.2.2 Voting Phase

Create another system for voting which involve:

1. Authentication process.
2. Voting phase.

1. Authentication Process

After the voter complete the registration process, and get his/her token he/she is now allow to vote in any time and any place accessing online voting system and perform authentication process:

1. Administrator server send login interface to the voter.
2. Voter proved his/her token (National number, Reg_num and finger print).
3. Administrator server check and verify token.
4. Administrator Add candidate list to block chain .
5. Show list candidate to voter .

Figure (4.10) system requires the voter to enter his national number , code (Reg_num) and scan finger print , so that the system can present the candidates to the voter and allow him to choose the candidate and vote for him.

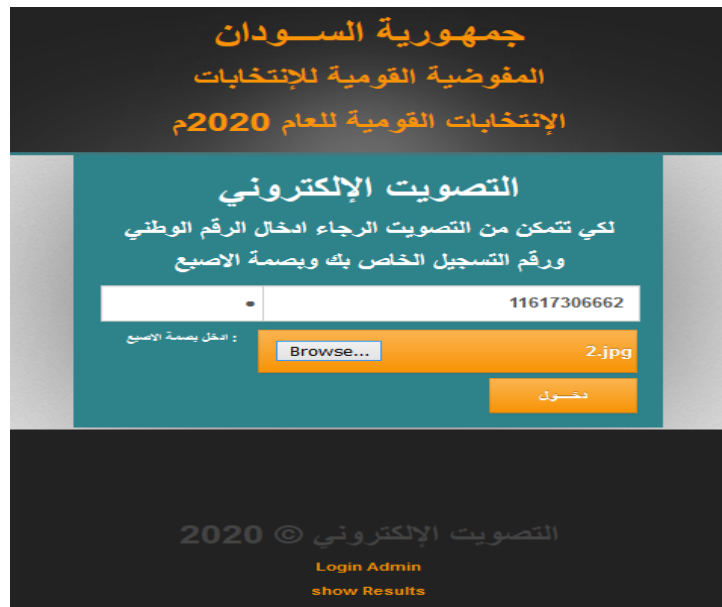


Fig. 4.10 voting login page

Figure (4.11) The system send error message to the voter in the event that the fingerprint, national number, or registration number does not match the data in the database, or if one of the voting conditions is not met.



Fig 4.11 voting login page

Figure (4.12) and (4.13) of the candidates is displayed, and the voter chooses the best candidate and casts his vote. The system uses the AES algorithm so that the voters' vote is encrypted and stored in the database and with every vote, the voter's vote is added to the blockchain.



Fig 4.12 vote page

الرؤساء

ابحث عن ..





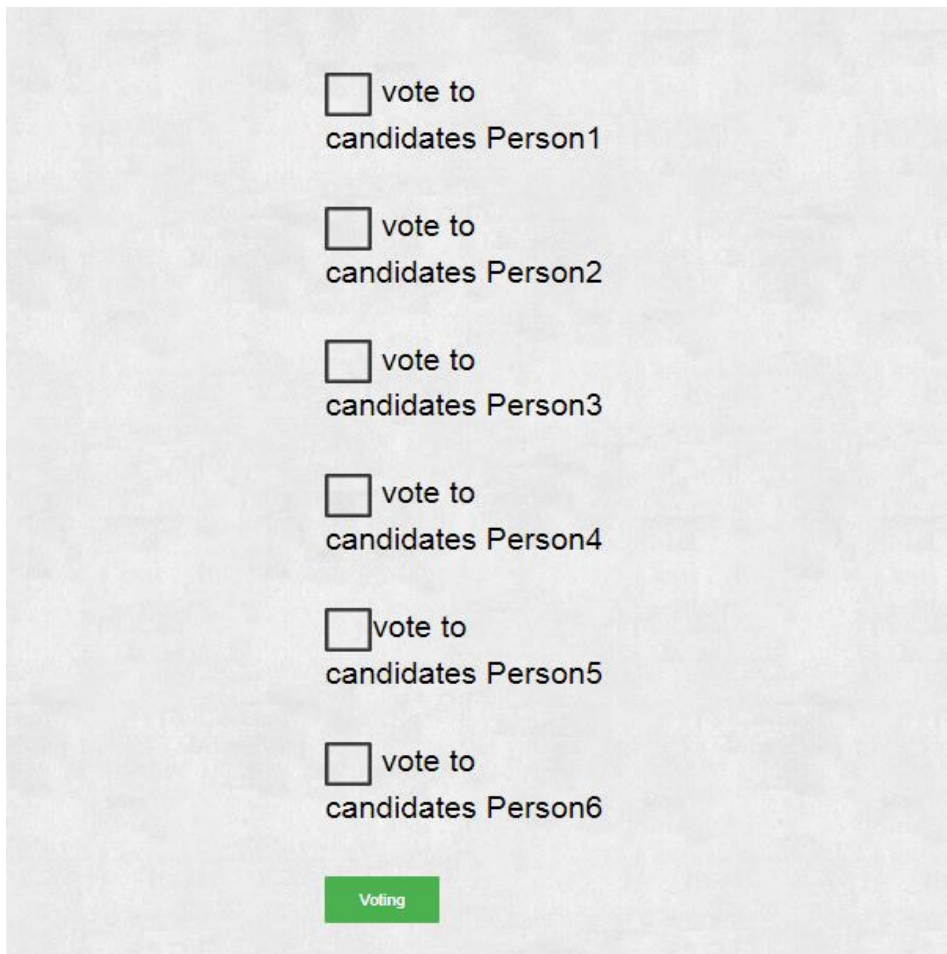
<p>محاييد رئاسي</p> <p>محاييد</p> <p>محاييد</p>		<input type="radio"/>
<p>طلال عمر عباس</p> <p>د</p> <p>ولاية الخرطوم</p>		<input type="radio"/>
<p>صفا مختار حامد</p> <p>ب</p> <p>ولاية الشمالية</p>		<input type="radio"/>
<p>محمد القاتح حيدر صالح حسين</p> <p>أ</p> <p>ولاية الخرطوم</p>		<input type="radio"/>

Fig 4.13 vote page

2. Voting Phase

After administrator verify and validate token, provide list of candidate. In this process the following actions are carried out:

1. Voter Select his/her Candidate.
2. The block is generated based on the filter number and encrypt vote SHA 256 algorithms.
3. The block is verified and then added to the block chain.
4. The voting in the blockchain is updated and saved encoded in the databases by the AES algorithms .



The image shows a voting interface with six candidates listed vertically. Each candidate has a checkbox to its left and the text "vote to candidates PersonX" to its right, where X is the candidate number. At the bottom of the list is a green button labeled "Voting".

- vote to candidates Person1
- vote to candidates Person2
- vote to candidates Person3
- vote to candidates Person4
- vote to candidates Person5
- vote to candidates Person6

Voting

Fig. 4.14 choose candidate and click voting button

Figure (4.15) and (4.16) are show the voting process for the candidates and the voter chooses the best candidate and casts his vote, the voter vote is added to the block chain.

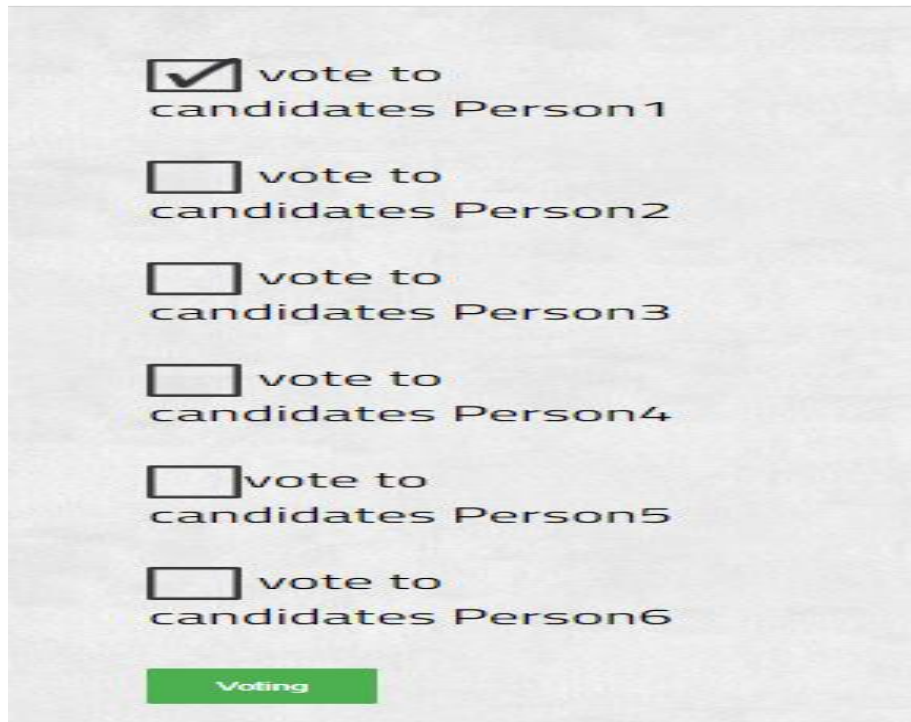


Fig 4.15 voter choose candidate1 and click voting button

```

BLOCK MINED:
02420627167bd10da6b53598f71cca08f75b2825d7e45d6f100135d030eaf1d6
Block successfully mined!
Voting Counter: Person One has 1 Votes Person Two has 0 Votes Person Three has 0 Votes Person
Four has 0 Votes Person Five has 0 Votes Person Six has 0 Votes Blockchain: { "previousHash":
"0", "timestamp": 1594339200000, "votes": [], "hash":
"1928291c038b61569f78a03e0483e9aa89da9c7c37fc0bd083199a5e1ac82927", "nonce": 0 }
{"previousHash": "1928291c038b61569f78a03e0483e9aa89da9c7c37fc0bd083199a5e1ac82927",
"timestamp": 1598324329481, "votes": [ { "personOne": 1, "personTwo": 0, "personThree": 0,
"personFour": 0, "personFive": 0, "personSix": 0 } ], "hash":
"02420627167bd10da6b53598f71cca08f75b2825d7e45d6f100135d030eaf1d6", "nonce": 20 }

```

Fig. 4.16 Block chain and hash transaction of process one

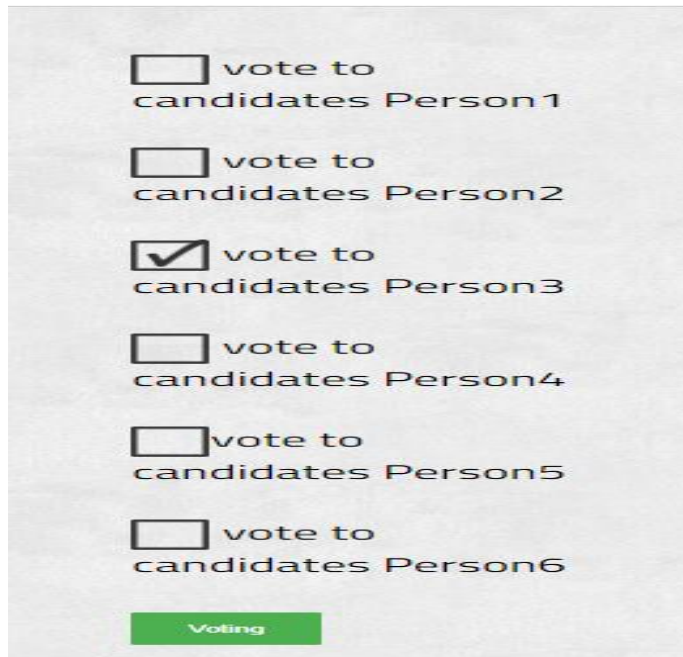


Fig 4.17 voter choose candidate3 and click voting button

```

BLOCK MINED:
02081a784610e41d4d3d340cc96a85e1fadd785bd740e06af23067cc8f6284f
Block successfully mined!
Voting Counter: Person One has 1 Votes Person Two has 0 Votes Person Three has 1 Votes
Person Four has 0 Votes Person Five has 0 Votes Person Six has 0 Votes Blockchain: {
"previousHash": "0", "timestamp": 1594339200000, "votes": [], "hash":
"1928291c038b61569f78a03e0483e9aa89da9c7c37fc0bd083199a5e1ac82927", "nonce": 0 }
{"previousHash":
"1928291c038b61569f78a03e0483e9aa89da9c7c37fc0bd083199a5e1ac82927", "timestamp":
1598324329481, "votes": [ { "personOne": 1, "personTwo": 0, "personThree": 0, "personFour":
0, "personFive": 0, "personSix": 0 } ], "hash":
"02420627167bd10da6b53598f71cca08f75b2825d7e45d6f100135d030eaf1d6", "nonce": 20 }
{"previousHash":
"02420627167bd10da6b53598f71cca08f75b2825d7e45d6f100135d030eaf1d6", "timestamp":
1598324342326, "votes": [ { "personOne": 0, "personTwo": 0, "personThree": 1, "personFour":
0, "personFive": 0, "personSix": 0 } ], "hash":
"02081a784610e41d4d3d340cc96a85e1fadd785bd740e06af23067cc8f6284f", "nonce": 17 }

```

Fig 4.18 Block chain and hash transaction of process two

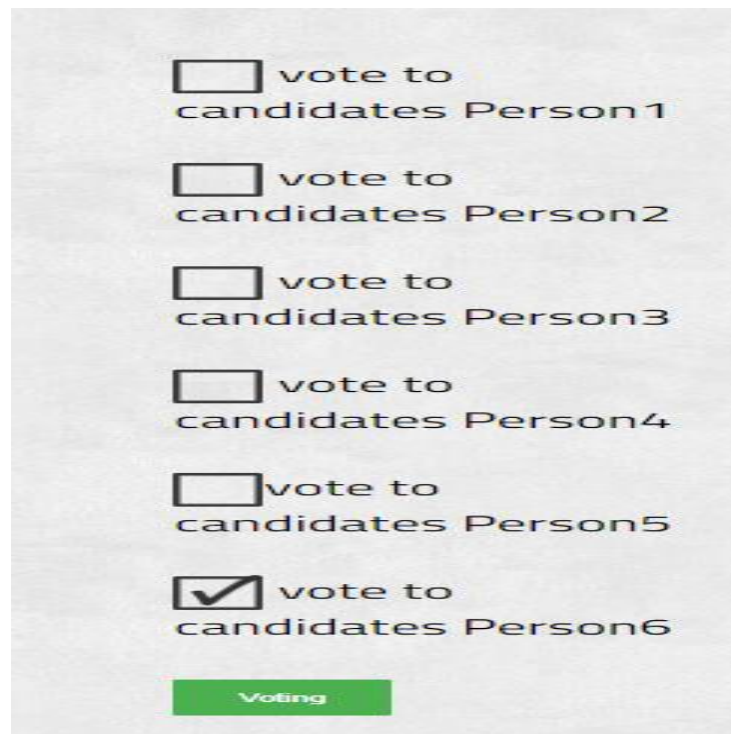


Fig 4.19 voter choose candidate6 and click voting button

```

BLOCK MINED:
08d7f05b3209c3259cd91b02191c5f3c3d48d7e494bca7e0ec2f2c000db922f8
Block successfully mined!
Voting Counter: Person One has 1 Votes Person Two has 0 Votes Person Three has 1 Votes Person
Four has 0 Votes Person Five has 0 Votes Person Six has 1 Votes Blockchain: { "previousHash": "0",
"timestamp":1594339200000,"votes":[], "hash":
"1928291c038b61569f78a03e0483e9aa89da9c7c37fc0bd083199a5e1ac82927", "nonce": 0 }
{"previousHash": "1928291c038b61569f78a03e0483e9aa89da9c7c37fc0bd083199a5e1ac82927",
"timestamp": 1598324329481, "votes": [ { "personOne": 1, "personTwo": 0, "personThree": 0,
"personFour": 0, "personFive": 0, "personSix": 0 } ], "hash":
"02420627167bd10da6b53598f71cca08f75b2825d7e45d6f100135d030eaf1d6", "nonce": 20 }
{"previousHash": "02420627167bd10da6b53598f71cca08f75b2825d7e45d6f100135d030eaf1d6",
"timestamp": 1598324342326, "votes": [ { "personOne": 0, "personTwo": 0, "personThree": 1,
"personFour": 0, "personFive": 0, "personSix": 0 } ], "hash":
"02081a784610e41d4d3d340cc96a85e1fadd785bd740e06af23067cc8f6284f", "nonce": 17 }
{ "previousHash":
"02081a784610e41d4d3d340cc96a85e1fadd785bd740e06af23067cc8f6284f", "timestamp":
1598324842508, "votes": [ { "personOne": 0, "personTwo": 0, "personThree": 0, "personFour": 0,
"personFive": 0, "personSix": 1 } ], "hash":
"08d7f05b3209c3259cd91b02191c5f3c3d48d7e494bca7e0ec2f2c000db922f8", "nonce": 31 }

```

Fig. 4.20 Block chain and hash transaction of process three

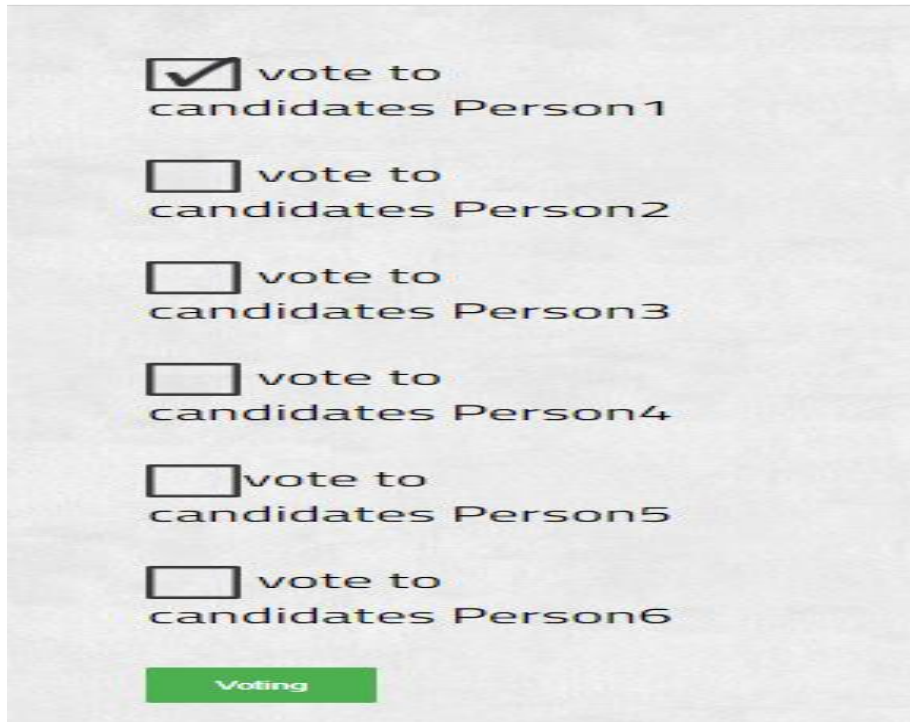


Fig. 4.21 voter choose candidate1 and click voting button

```

BLOCK MINED:
04b4e253cc05c8ba7c8eebdad2d554408ffa14168731d43226a198dd12c7c68c
Block successfully mined!
Voting Counter: Person One has 2 Votes Person Two has 0 Votes Person Three has 1 Votes Person
Four has 0 Votes Person Five has 0 Votes Person Six has 1 Votes Blockchain: { "previousHash": "0",
"timestamp": 1594339200000, "votes": [], "hash":
"1928291c038b61569f78a03e0483e9aa89da9c7c37fc0bd083199a5e1ac82927", "nonce": 0 } {
"previousHash": "1928291c038b61569f78a03e0483e9aa89da9c7c37fc0bd083199a5e1ac82927",
"timestamp": 1598507864327, "votes": [ { "personOne": 1, "personTwo": 0, "personThree": 0,
"personFour": 0, "personFive": 0, "personSix": 0 } ], "hash":
"06b412db2dfa271ed9b9c77080f87b255eaecdc816abeadee949fac3fea714ee", "nonce": 33 } {
"previousHash": "06b412db2dfa271ed9b9c77080f87b255eaecdc816abeadee949fac3fea714ee",
"timestamp": 1598507954745, "votes": [ { "personOne": 0, "personTwo": 0, "personThree": 1,
"personFour": 0, "personFive": 0, "personSix": 0 } ], "hash":
"0b37328ded3934cd16c294f4895db94cca82b0a2dd6902f4f5da0d7cf8203024", "nonce": 11 } {
"previousHash": "0b37328ded3934cd16c294f4895db94cca82b0a2dd6902f4f5da0d7cf8203024",
"timestamp": 1598507990456, "votes": [ { "personOne": 0, "personTwo": 0, "personThree": 0,
"personFour": 0, "personFive": 0, "personSix": 1 } ], "hash":
"01afa8653695db55f25629748d8ca5a5a69b1052129eea3be4e0a11ec023fa28", "nonce": 15 } {
"previousHash": "01afa8653695db55f25629748d8ca5a5a69b1052129eea3be4e0a11ec023fa28",
"timestamp": 1598508008123, "votes": [ { "personOne": 1, "personTwo": 0, "personThree": 0,
"personFour": 0, "personFive": 0, "personSix": 0 } ], "hash":
"04b4e253cc05c8ba7c8eebdad2d554408ffa14168731d43226a198dd12c7c68c", "nonce": 25 }

```

Fig. 4.22 Block chain and hash transaction of process four

Figure (4.23) screen appears after the voter completes the voting process successfully



Fig 4.23 successful vote page

Figure (4.24) screen appears if the voter who has already voted before the vote tries again.



Fig. 4.24 validation page

Figure (4.25) result of the vote and is encrypted in the database the encrypt data using Advance Encryption Standard (AES), which is symmetric block cipher using 128 block size .

		c_id	c_votes	voter_date
<input type="checkbox"/>	Edit Copy Delete	1	JAGXKhShRF+M	2020-08-25 07:26:44
<input type="checkbox"/>	Edit Copy Delete	2	rgA+7dqgRF+r	2020-08-25 07:25:46
<input type="checkbox"/>	Edit Copy Delete	3	QwG6WxShRF+R	2020-08-25 07:26:44
<input type="checkbox"/>	Edit Copy Delete	4	9AFw5mmgRF8A	2020-08-25 07:23:53
<input type="checkbox"/>	Edit Copy Delete	5	6AEav6ufRF8d	2020-08-25 07:20:43
<input type="checkbox"/>	Edit Copy Delete	6	ewHNPDOfRF8v	2020-08-25 07:18:43
<input type="checkbox"/>	Edit Copy Delete	7	tAD6k9qgRF9p	2020-08-25 07:25:46
<input type="checkbox"/>	Edit Copy Delete	8	+gFkDWmgRF+I	2020-08-25 07:23:53
<input type="checkbox"/>	Edit Copy Delete	9	7AFo76ufRF9J	2020-08-25 07:20:43
<input type="checkbox"/>	Edit Copy Delete	10	qAB/hdqgRF9H	2020-08-25 07:25:46
<input type="checkbox"/>	Edit Copy Delete	11	MQENlxShRF8J	2020-08-25 07:26:44
<input type="checkbox"/>	Edit Copy Delete	12	wwG0ke6eRF8d	2020-08-25 07:17:34

Fig. 4.25 AES algorithms Result in DB

Figure (4.26) screen appears if the voting period is over and the voter decides to enter after the voting period because the system adheres to a fixed time for voting, where the voter can press the display button and the system displays the result to the voter .



Fig 4.26 End of vote phase

4.2.3 Admins page

The system administrator is the cornerstone of the system. The administrator governs the start and end times of the registration and polling phases and controls the different pages of the system.

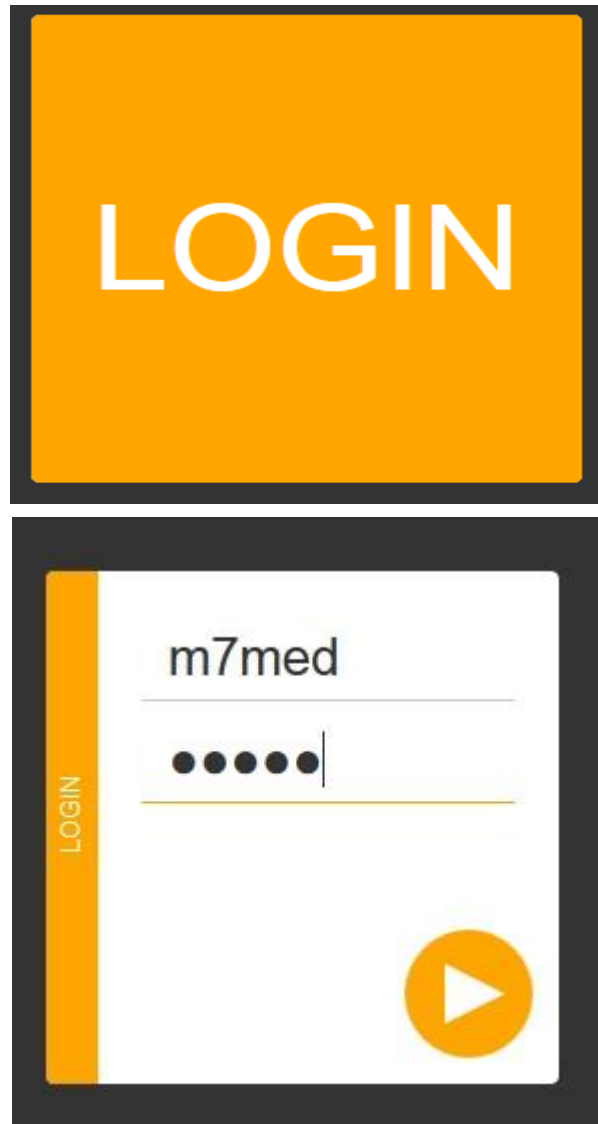


Fig. 4.27 Admin login

Figure (4.28) The screen of displays the system administrator’s work in monitoring the voting system and controlling the various system screens and the start and end times of the registration and voting stages.

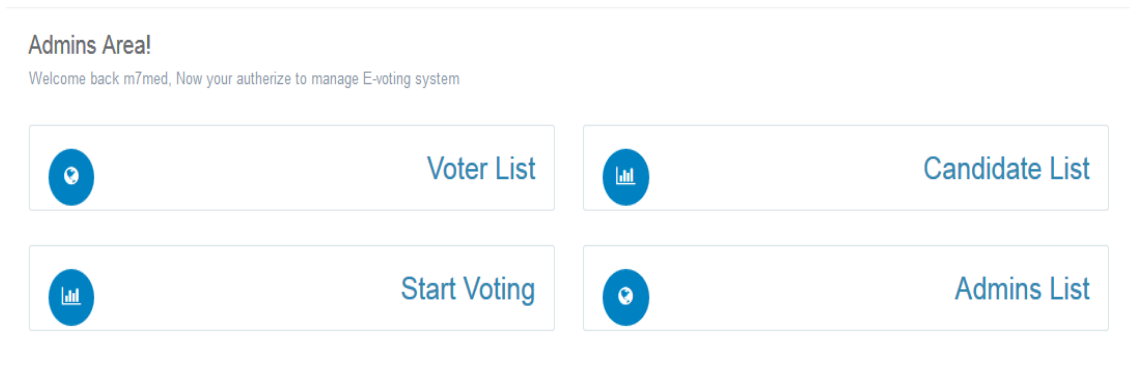


Fig. 4.28 Admin main page

Manage Admins Area Figure (4.29) all admins information on database

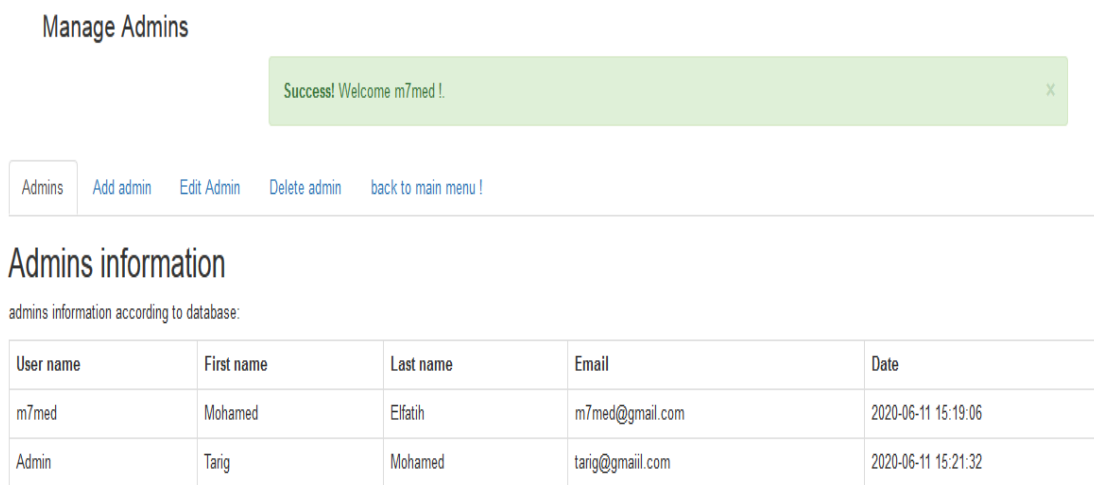


Fig 4.29 Admin list

Manage Admins Area Figure (4.30) Add Admins information on database

Manage Admins

Admins Add admin Edit Admin Delete admin back to main menu !

First name:

Last name:

Username:

Password:

Email address:

Submit

Fig. 4.30 Add Admin information

Manage Admins

Admins Add admin Edit Admin Delete admin back to main menu !

m7med

Admin

First name:

Last name:

Username:

Password:

Email address:

Submit

Fig. 4.31 Edit Admin information

Manage Admins

Admins Add admin Edit Admin Delete admin back to main menu !

Admins Delete

This area to delete admins :

User name	First name	Last name	Email	Date	
m7med	Mohamed	Elfatih	m7med@gmail.com	2020-06-11 15:19:06	Delete
Admin	Tarig	Mohamed	tarig@gmail.com	2020-06-11 15:21:32	Delete

Fig. 4.32 Delete Admin information

Manage Admins Area Figure (4.33) control Candidate information page

معلومات المرشحين

هذه المعلومات مأخوذة من بيانات المرشح في السجل المدني الرجاء الإنتباه قبل اجراء اي عملية :

الرقم	اسم المرشح	اسم الحزب	اسم الولاية	العمر	الغنوان	الوظيفة	رقم الهاتف	تأكيد الترشيح	البريد الالكتروني
1	محايد رئيسي	محايد	محايد	20	لا يوجد	لا يوجد	0	1	0.0@0
2	محايد ولائي	محايد	محايد	20	لا يوجد	لا يوجد	0	1	0.0@0
3	محايد عضو برلمان	محايد	محايد	20	لا يوجد	لا يوجد	0	1	0.0@0
4	محمد الفاتح حيدر صالح حسين	حزب المؤتمر الوطني	ولاية الخرطوم	25	امدرمان	موظف	0926078213	1	m7med@gmail.com
5	محمد الحسن احمد	حزب الأمة القومي	ولاية الشمالية	30	الدامر	موظف	0912398585887	1	moh58@hotmail.com
6	ملاط عمر عباس	الحزب الشيوعي	ولاية الخرطوم	25	المعمورة	محاسب	0928826343	1	orten1994@gmail.com
7	امنة سمير عثمان	مستقل	ولاية الخرطوم	30	الجريرف غرب	موظفة	099876542322	1	nona@gmail.com
8	العز المبارك محمد عبدالدافع	حزب المؤتمر الشعبي	ولاية شمال كردفان	30	امدرمان ،ال	موظف	0907700345	1	elmoiz@gmail.com
9	احمد علي عثمان	حزب البعث السوداني	ولاية النيل الازرق	31	سنار	موظف	091229875455	1	ahmed@yahoo.com
10	الصفا مختار حامد	مستقل	ولاية الخرطوم	28	امدرمان	معلمة	0908203229	1	alsafamukhtar@gmail.com

Fig. 4.34 candidate information list

اسم المرشح

الاسم

العمر

صورة المرشح

No file selected. Browse

الولاية

اختار الولاية

الغنوان

الجنس

الهاتف

phone number +249

المرجحة التعليمية

اختار المرجح التعليمي

الحزب

اختار الحزب

نوع المرشح

اختار النوع

الوظيفة

الولاية

البريد الإلكتروني

تأكيد

Fig. 4.35 Add candidate information

محايد رئيسي

محايد ولائي

محايد عضو برلمان

محمد الفتاح حيدر صالح حسين

محمد الحسن احمد

طلال عمر عباس

امنة سمير عثمان

المعز المبارك محمد عبدالدافع

احمد علي عثمان

الصفا مختار حامد

حيدر صالح حسين محمد

:candidate name
محمد الحسن احمد

:age
30

address
الداير

:job
موظف

:phone
0912398585887

No Yes : Visible to vote system

:Email address
moh58@hotmail.com

: parties
حزب الأمة القومي

نوع المرشح
رئيس

الولاية
ولاية الخرطوم

الدرجة العلمية
بكالوريوس

تأكيد

Fig. 4.36 Edit candidate information

* candidate information according to database !

Remove all data from result table

* Add OR Remove candidate into result table before the Votting proceses :

search for candidate name:

candidate_no	candidate_name		
1	محايد رئيسي	upload	Delete
2	محايد ولائي	upload	Delete
3	محايد عضو برلمان	upload	Delete
4	محمد الفتاح حيدر صالح حسين	upload	Delete
5	محمد الحسن احمد	upload	Delete
6	طلال عمر عباس	upload	Delete
7	امنة سمير عثمان	upload	Delete
8	المعز المبارك محمد عبدالدافع	upload	Delete

Fig. 4.37 Add candidate information to block chain

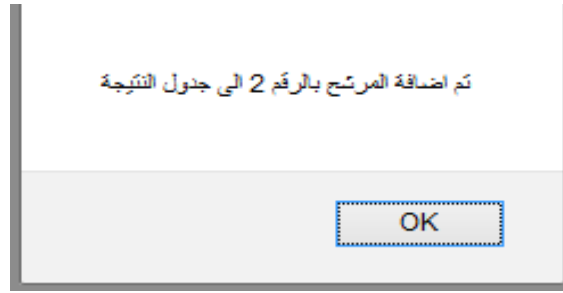


Fig. 4.38 upload candidate to result table

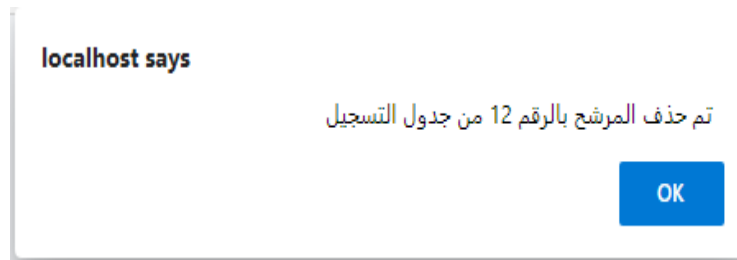


Fig. 4.40 Delete candidate From result table

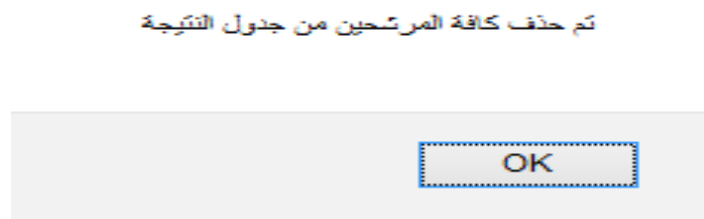


Fig. 4.41 Delete all candidate in result table

Manage Admins Area Figure (4.42) control Voter list page

معلومات الناخبين

هذه المعلومات مأخوذة من قاعدة بيانات السجل المدني الرجاء الانتباه في عمليات التعديل :

.....:search for voter name

الرقم	اسم الناخب	الرقم الوطني	العنوان	العمر	الجنس	الديانة	الوظيفة	رقم الهاتف	البريد الالكتروني	الدائرة الجغرافية	تاريخ التسجيل
1	عبدالله محمد سر الختم علي	98765432155	الخرطوم	45	1	مسلم	تاجر	0926078213	m7med.963@gmail.com	كرري	2020-06-13 12:06:24
2	محمد الفلاح جابر صالح	11617306662	أمدرمان	18	1	مسلم	موظف	0926078213	m7med@gmail.com	كرري	2020-06-13 12:43:17
3	نسي جابر صالح حسين	98764	أمدرمان الواحة	15	0	مسيحية	طالبة	0995684378	nada@gmail.com	أمدرمان	2020-06-13 13:07:12
4	الصفاء مختار حامد	987654321	الخرطوم	45	0	مسيحية	موظفة	0908203229	a@a.com	جل أولياء	2020-06-13 14:00:36
5	امنية جابر صالح	12345645678910	أمدرمان ، الواحة	23	0	مسيحية	طالبة	0901980990	omnia@yahoo.com	بحري	2020-06-13 15:05:20
6	جابر صالح حسين	112233445566	بحري	61	1	مسلم	موظف	0912139899	hayder@gmail.com	أمبدة	2020-06-13 15:08:27
7	احمد جابر صالح	98765432107812	أمدرمان ، الواحة مربع 10	20	1	مسلم	طالب	0904994277	a@gmail.com	الخرطوم	2020-06-14 06:32:53

Fig. 4.42 voter information list

الاسم

الرقم الوطني

يجب ان يتكون على 12 اقله

الولاية

اللقب الوظيفي

العنوان

العمر

الجنس female male

الديانة

الديانة

رقم الهاتف

phone number +249

صورة بصمة الاصبع

No file selected.

الدائرة الجغرافية

اختار اسم المنطقة

البريد الإلكتروني

Fig. 4.43 Add voter information

معلومات الناخبين

هذه المعلومات مأخوذة من قاعدة بيانات السجل المدني الرجاء الانتباه في عمليات التعديل :

الرقم	اسم الناخب	الرقم الوطني	العنوان	العمر	الجنس	الديانة	الوظيفة	رقم الهاتف	البريد الالكتروني	الدائرة الجغرافية	تاريخ التسجيل
1	عبدالله محمد سر الحكم طي	98765432155	الفرطوم	45	1	مسلم	تاجر	0926078213	m7med963@gmail.com	كرري	12:06:24 2020-06-13
2	محمد الفلاح حيدر صالح	11617306662	امدرمان	18	1	مسلم	موظف	0926078213	m7med@gmail.com	كرري	12:43:17 2020-06-13
3	شذى حيدر صالح حسين	98764	امدرمان الواحة	15	0	مسلمة	طالبة	0995684378	nada@gmail.com	امدرمان	13:07:12 2020-06-13
4	الصفاء مختار حامد	987654321	الفرطوم	45	0	مسلمة	موظفة	0908203229	a@a.com	جل أولياء	14:00:36 2020-06-13
5	امينة حيدر صالح	12345645678910	امدرمان ، الواحة	23	0	مسلمة	طالبة	0901980990	omnia@yahoo.com	بحري	15:05:20 2020-06-13
6	حيدر صالح حسين	112233445566	بحري	61	1	مسلم	موظف	0912139899	hayder@gmail.com	أهبيد	15:08:27 2020-06-13
7	احمد حيدر صالح	98765432107812	امدرمان ، الواحة مربع 10	20	1	مسلم	طالب	0904994277	a@gmail.com	الفرطوم	06:32:53 2020-06-14
8	ريهام امير حسين عباس	118278965432011	امدرمان الواحة	25	0	مسلمة	موظفة	0909307090	reham2@gmail.com	كرري	15:08:26 2020-06-16
9	المنعم المبارك محمد عبدالقادر	987654535446146	امدرمان ، الواحة	30	1	مسلم	موظف	0907700345	elmoiz@gmail.com	شرق النيل	13:41:53 2020-06-29
10	خليل عمر عباس	198976565735536	المعجورة	25	1	مسلم	موظف	0928826343	orten1994@gmail.com	الفرطوم	22:00:33 2020-06-30
11	خديجة مهدي عبدالعالم محمد	118788999837636	الحاج يوسف	30	0	مسلمة	موظفة	09978475478	hadeel@hotmail.com	شرق النيل	22:02:20 2020-06-30
12	احمد امير حسين	998177237888973	امدرمان ، الواحة	20	1	مسلم	طالب	0968755455448	a@gmail.com	بحري	22:04:00 2020-06-30

Fig. 4.44 Delete voter information

الاسم

الرقم الوطني

العنوان:

صورة بصمة الاصبع

العمر

رقم الهاتف

الدائرة الجغرافية

البريد الالكتروني

Fig. 4.45 Edit voter information

4.2.4 Result phase

Any person, voter, candidate, party, or any governmental or media agency and international organizations has the right to see the results of the registration and polling stages even without the need for powers to enter the system. Once the person clicks on the results tab, a list of current results appears for him, and this electronic stage is more flexible It is credible and transparent and cannot be rigged by any party for the purpose of manipulating the electoral process.

The results can be viewed even before the polling stage ends. This list is updated periodically until the successful completion of the voting process.

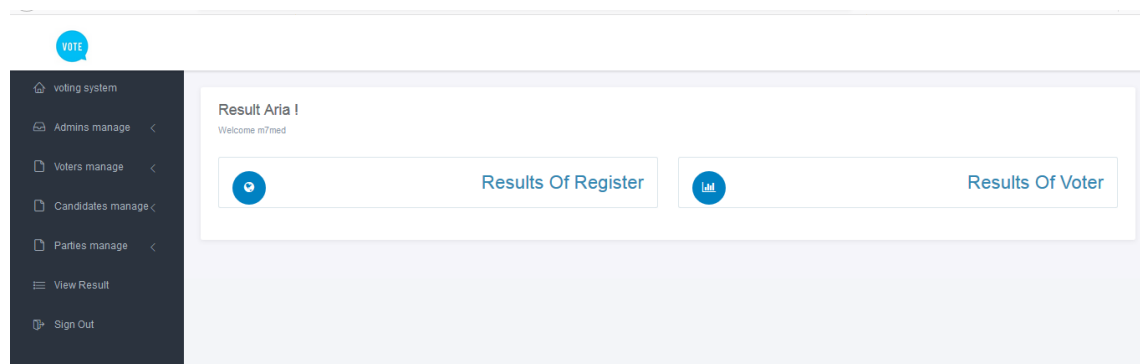


Fig. 4.46 Result page

Figure (4.47) result appears after the election period ends and after decoding the votes

المرشحين للرئاسة		الأحزاب	
#	الإسم	إجمالي المرشحين بالحزب	إسم الحزب
1	محمد الفاتح حيدر صالح حسين	3	محايد
2	محايد رئاسي	2	أ
3	طلال عمر عباس	2	و
4	الصفا مختار حامد	2	مستقل
		1	ب
		1	د
		1	ز
		0	ج

Fig. 4.47 Result of voter

الأحزاب

#	إسم الحزب	اجمالي المرشحين بالحزب
1	محايد	3
2	أ	2
3	ب	2
4	و	2
5	د	1
6	ز	1
7	مستقل	1
8	ج	0

Fig. 4.48 Result of parties and candidate

المرشحين للرئاسة

#	الإسم	الحزب	عدد الأصوات
1	محمد الفاتح حيدر صالح حسين	أ	3
2	محايد رئاسي	محايد	3
3	طلال عمر عباس	د	1
4	صفا مختار حامد	ب	3

Fig. 4.49 Result candidate president

Figure (4.50) The screen of displays the result of the regestration phase.

عدد الذكور والاناث في الدائرة الجغرافية				تقارير التسجيل حسب الدائرة الجغرافية			
الاناث	الذكور	اجمالي المسجلين	اسم الدائرة الجغرافية	#	اجمالي المسجلين	اسم الدائرة الجغرافية	#
1	2	3	كرري	1	3	كرري	1
0	0	0	أمدرمان	2	0	أمدرمان	2
1	0	1	جبل أولياء	3	1	جبل أولياء	3
0	1	1	أميدة	4	1	أميدة	4
0	1	1	الخرطوم	5	1	الخرطوم	5
1	0	1	بحري	6	1	بحري	6
0	1	1	شرق النيل	7	1	شرق النيل	7

اكملو عملية التسجيل والانتخاب			
اكملو عملية الانتخاب بنجاح	اكملو عملية التسجيل بنجاح	اسم الدائرة الجغرافية	#
3	3	كرري	1
0	0	أمدرمان	2
0	1	جبل أولياء	3
1	1	أميدة	4

Fig. 4.51 Result of the Registration phase

تقارير التسجيل حسب الدائرة الجغرافية		
اجمالي المسجلين	اسم الدائرة الجغرافية	#
3	كرري	1
0	أمدرمان	2
1	جبل أولياء	3
1	أميدة	4
1	الخرطوم	5
1	بحري	6
1	شرق النيل	7

Fig. 4.52 Result of voter accordion to Geographical circle

عدد الذكور والاناث في الدائرة الجغرافية

#	اسم الدائرة الجغرافية	اجمالي المسجلين	الذكور	الاناث
1	كرري	3	2	1
2	أمدرمان	0	0	0
3	جبل أولياء	1	0	1
4	أمبدة	1	1	0
5	الخرطوم	1	1	0
6	بحري	1	0	1
7	شرق النيل	1	1	0

Fig. 4.53 Result of voter according to Gender

اكملو عملية التسجيل والانتخاب

#	اسم الدائرة الجغرافية	اكملو عملية التسجيل بتجاح	أكملو عملية الانتخاب بتجاح
1	كرري	3	3
2	أمدرمان	0	0
3	جبل أولياء	1	0
4	أمبدة	1	1
5	الخرطوم	1	1
6	بحري	1	1
7	شرق النيل	1	1

Fig. 4.54 All Result of voter in two stages

4.3 Security Analysis And Results

4.3.1 Potential Attacks

1. Spoofing And Man-in-the-Middle Attacks

In man-in-the-middle attacks the adversary interposes itself between legitimate communicating parties and simulates each party to the other. To simplify the discussion in the context of this research, focused primarily on ways that a man-in-the-middle attack can subvert voter privacy, although the same general technique can be used for other attacks, such as vote buying. The use of Security Socket Layer (SSL) does little to mitigate man-in-the-middle attacks on privacy[30].

Any man-in-the-middle could act as an SSL gateway, forwarding application data between the voter and the vote server unaltered. The attacker could see all of the traffic by decrypting and re-encrypting as communications pass between the two. In effect, the attacker would communicate using two SSL sessions, one between itself and the voter, and the other between itself and the vote server, and neither would know that there was a problem. These attacks are possible because the voter's browser does not verify that it is talking to the real server web server only that it is talking to someone in possession of a valid SSL certificate (who could be an attacker). Man-in-the-middle attacks also could be used to disenfranchise voters by spoofing the entire interaction with the voter. server has some safeguards in place, but they assume the voter knows exactly what to expect from the voting experience, it is likely that an attacker could create a voting experience the voter would believe is real. Similarly, voters could be led to believe they registered successfully, when in fact they were communicating directly with an adversary instead of the legitimate registration server. The voters would discover when attempting to vote that they were not registered, but at that point there might be nothing they could do to resolve the situation. Perhaps the most serious consequence of man-in-the-middle attacks is that attackers could engage in election fraud by spoofing the voting server and observing how a particular voter votes. If the vote is to the attacker's liking, the voter is redirected to server's legitimate voting site. If the attacker does not like the vote, then the entire voting session is spoofed; in this case, the user thinks he or she has voted, but in fact the vote will not be received or counted by server[30].

The proposed system (Electronic Voting System Based on block chain technology) faced the center man's attack with several procedures. One of these procedures is that the system requires the voter to enter the private key and scan finger print in Figure (4.2) password screen this password is not entered by anyone except the voter and the system manipulate password by using hash algorithm. The second procedure is that the system encrypts the voting process in in Figure (4.25) by using AES algorithm and saves it in the database and also add to the chain of block as in the figure(4.22) .

2. Distributed Denial Of Service Attacks

DDOS : for a successful DDOS distributed system like As we suggested, a DDOS attacker must reach one bootnode in private network. The individual or the organization Immediately if that happens. Each node is executed using a Byzantine error tolerance algorithm, This helps in locating the failed nodes in the system.

3. Vulnerability Of Authentication Phase:

Each individual is identified and authenticated by the system by electronically submitting the national ID number corresponding to the 12-digit PIN and scanning a fingerprint and private key in the voting booth. Without supervision, and thus an individual cannot vote for several people, if the individual has knowledge of the personal identification number for each electronic identity and obtains the password of the other voter, he cannot match the fingerprint of the person and thus the proposed system achieves sufficient security in the authentication process and guarantees the integrity of each vote in the process Electoral.

4.3.2 Results

In our proposed system there are two types of encryption have been combined in order to exploit the advantages of each one to build a high security system. AES is used to encrypt sent data, exploiting its high encryption speed and its low RAM requirements. Block chain and SHA256 are used to protect the encrypted vote or the data. The vote and encrypted data are sent to the receiver and get decrypted by using the AES algorithm. Comparing with system in the proposed system is simple and fast with low computational requirements and provides reasonable system security the research proposal to define and implement a new e-voting system concept. This system is called Crypto-voting and it is based on permissioned blockchain technology. the elements of innovation, compared to the state of the art, consist in the approach, in the technology and in the use of tools such as Smart Contracts.

Smart contracts will be responsible for managing voting procedures and results. Our system increases the efficiency of the validation phase and of the assignment of the candidate's vote. In addition, the proposed technology covers aspects not currently treated, such as a safe timing of voting abroad, the automatic management of electoral lists, integration of the identification process with that of voting secrecy advanced, and automatic and reliable mechanisms to guarantee the security of voting. The nature of this research proposal is itself of directed towards the wide circulation of results in the research community and in the e-government sectors. Considering the vastness of the proposal, research results could interest several research institutions, which can enrich results by means an audience of experts more articulated than that of the proponents. In the same way, it is essential the public actors involvement in order to verify if the ambition related to the project could effectively find an application feedback.

CHAPTER FIVE
CONCLUSION AND
RECOMMENDATION

CHAPTER V

CONCLUSION AND RECOMMENDATION

5.1 Conclusion

This research , presented a unique block chain-based electronic voting system that uses smart contracts to enable safe and cost-effective elections while ensuring voter privacy. Compared to previous work, block chain technology has been shown to offer a new possibility for democratic countries to progress from a pen-and-paper election scheme, to a more cost- and time-efficient election scheme , while increasing security measures in the present-day scheme and introducing new possibilities for transparency. With Ethereum private block chain, it is possible to send hundreds of transactions per second to the block chain, using every aspect of a smart contract to ease the load on the block chain.

Based on the design and the research results conducted, it can be concluded that the system is successfully operating in registering a Block chain technology based electronic voting system. The block chain permission protocol used is a distributed recordkeeping system run by well-known entities, in other words it has the means to define which nodes can control and update data together to achieve participants' trust goals. A known entity in this system is any node that was registered before the process was run, and the public key in each node is owned by all nodes in the system. Any data that is broadcast by the node that gets a turn is always verified and its data updated by the recipient. The verification system performed by all receiving nodes can determine if there are prior hashes and / or public keys not registered in the database. The counter time system becomes a parameter when there are nodes that have an overlap acting according to the design. Interfering nodes can perform manual data, or system broadcasts can be repeated to refresh the data when the operation reaches the last hop node. Each previous hash used by the block in the system has demonstrated the same hash value in the calculation results using the data in the previous block. Each hash value in the previous block was included in the computation of hash values by the block that plays its role in the system, which makes anyone wanting to change data in the database will have difficulty because if one data is changed, then they must make changes to the data in the other blocks.

5.2 Recommendation

1. Implementing block chain technology in the electronic government of Sudan and making use of it in various fields such as agriculture, industry , commerce , health , education , mining and oil , public interests , and others.
2. Dealing with decentralized database systems instead of centralizing databases and exchanging information between different databases according to the powers needed by each of the electronic government systems.
3. We have all seen the uproar caused by the Corona virus (Covid-19) pandemic around the world and how the world has benefited from advanced technologies in preventing this disaster and mitigating its effects. Among the technologies is block chain technology, which is a scientific breakthrough in the field of technology. By linking the health field record with the civil registry, knowing the patient and his family's data, and providing the necessary information to him as soon as possible.
4. In the electronic voting system, we used a fingerprint and the national number for the authentication. Other types such as eye print or face print can also be used with block chain technology.
5. The magnetic national card can be used and inserted into a device to complete the voting process electronically, after verifying the voter's powers and matching the entered fingerprint with the databases.

REFERENCES

References

- [1] F. P. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtýsson, "Blockchain-based e-voting system," in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 2018, pp. 983-986.
- [2] F. Fusco, M. I. Lunesu, F. E. Pani, and A. Pinna, "Crypto-voting, a Blockchain based e-Voting System," in *KMIS*, 2018, pp. 221-225.
- [3] F. S. Hardwick, A. Gioulis, R. N. Akram, and K. Markantonakis, "E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy," in *2018 IEEE International Conference 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)*, 2018, pp. 1561-1567.
- [4] B. Wang, J. Sun, Y. He, D. Pang and N. Lu, "Large-scale Election Based On Blockchain", *Procedia Computer Science*, vol. 129, pp. 234-237, 2018.
- [6] P. Tarasov and H. Tewari, "THE FUTURE OF E-VOTING," *IADIS International Journal on Computer Science & Information Systems*, vol. 12, 2017.
- [7] Y. L. a. Q. Wang, D. o. C. S. a. Engineering, S. Southern University of Science and Technology, China, and w. s. e. c. liuy7@mail.sustc.edu.cn, "An E-voting Protocol Based on Blockchain," 2017.
- [8] R. H. (Author), S. o. E. E. a. Informatics, B. I. o. Technology, W. J. Bandung, Indonesia, and rifahani@students.itb.ac.id, "Blockchain Based E-Voting Recording System Design," 2017.
- [9] C.-H. Roh and I.-Y. Lee, "A Study on Electronic Voting System Using Private Blockchain," *Journal of Information Processing Systems*, vol. 16, 2020.
- [10] A. Poniszewska-Marańda, M. Pawlak, and J. Guziur, "Auditable blockchain voting system-the blockchain technology toward the electronic voting process," *International Journal of Web and Grid Services*, vol. 16, pp. 1-21, 2020.
- [11] M. I. L. Francesco Fusco¹, Filippo Eros Pani² and Andrea Pinna² and V. M. 1NET SERVICE SPA, 4/d Bologna Italy, "Crypto-Voting, a blockchain based e-voting system," 2019.
- [12] K. Isirova, A. Kiian, M. Rodinko, and A. Kuznetsov, "Decentralized electronic voting system based on blockchain technology developing principals," in *CMIS*, 2020, pp. 211-223.
- [13] K. Srivathshan, S. Elamathi, and P. R. Saleh, "The SecureElect-Blockchain based Electronic Voting System to Enable Online," *Probyto Journal of AI Research*, vol. 1, 2020.
- [14] TechCrunch, (2018). Liquid democracy uses blockchain to fix politics, and now you can vote for it. Available at: <https://techcrunch.com/2018/02/24/liquid-democracy-uses-blockchain/>.
- [15] T. Roopak and R. Sumathi, "Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology," in *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, 2020, pp. 71-75.
- [16] Quinn, A. (2018) Are online music platforms undermining the principles of copyright law? *Journal of Intellectual Property Law & Practice*, Volume 13, Issue 1, 1 January 2018, Pages 49-60 <https://doi.org/10.1093/jiplp/jpx148>
- [17] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Applied Innovation*, vol. 2, p. 71, 2016.
- [18] Raskin, M. (2017) The Law and Legality of Smart Contracts (September 22, 2016). 1 *Georgetown Law Technology Review* 304(2017). Available at SSRN: <http://dx.doi.org/10.2139/ssrn.2842258>

- [19] Sharma, P., Singh, S., Jeong, Y., Park, J.H. (2017) DistBlockNet: ADistributed Blockchains-Based Secure SDN Architecture for IoT Networks, *Communications Magazine IEEE*, vol. 55, pp. 78-85,2017.
- [20] C. K. Adiputra, R. Hjort, and H. Sato, "A proposal of blockchain-based electronic voting system," in *2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, 2018, pp. 22-27.
- [21] Dagher, Gaby G., Praneeth Babu Marella, Matea Milojkovic, and Jordan Mohler. "BroncoVote: Secure Voting System Using Ethereum'sBlockchain." (2018).
- [22] I. L. Awalu, P. H. Kook, and J. S. Lim, "Development of a Distributed Blockchain eVoting System," in *Proceedings of the 2019 10th International Conference on E-business, Management and Economics*, 2019, pp. 207-216.
- [23] Geth.ethereum.org. (2018). Go Ethereum. Available at: <https://geth.ethereum.org/>
- [24] K. Isirova, A. Kiian, M. Rodinko, and A. Kuznetsov, "Decentralized electronic voting system based on blockchain technology developing principals," in *CMIS*, 2020, pp. 211-223.
- [25] C.-H. Roh and I.-Y. Lee, "A Study on Electronic Voting System Using Private Blockchain," *Journal of Information Processing Systems*, vol. 16, 2020.
- [26] T. Roopak and R. Sumathi, "Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology," in *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, 2020, pp. 71-75.
- [27] A. Poniszewska-Marańda, M. Pawlak, and J. Guziur, "Auditable blockchain voting system-the blockchain technology toward the electronic voting process," *International Journal of Web and Grid Services*, vol. 16, pp. 1-21, 2020.
- [28] R. Hanifatunnisa and B. Rahardjo, "Blockchain based e-voting recording system design," in *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, 2017, pp. 1-6.s
- [29] Ajit Kulkarni, (2018), "How To Choose Between Public And Permis-sioned Blockchain For Your Project", *Chronicle*, 2018.
- [30] B. D. S. S. 1M.Sudhakar and I. Y. M. T. 1Professor in ECE, "Secure E-voting System using Symmetric Encryption," 2018.