



People's Democratic Republic of Algeria
Ministry Of Higher Education And Scientific Research
University Of Larbi Tébessi -Tébessa



Faculty Of Exact Sciences And Sciences Of Nature and life
Department Of Mathematics And computer science

Final thesis
For obtaining the MASTER diploma
Specialty: Computer science
Option: RSI

Presented By Tayeb Guergah
On: June 27th, 2020

Election Management System Based On Blockchain

Before the Jury:

<i>President</i>	<i>M.R.Laouar</i>	<i>Pr</i>	<i>U. Larbi Tébessi University, Tébessa</i>
<i>Examiner</i>	<i>S. Merzoug</i>	<i>MAB</i>	<i>U. Larbi Tébessi University, Tébessa</i>
<i>Supervisor</i>	<i>T. Mekhaznia</i>	<i>MCA</i>	<i>U. Larbi Tébessi University, Tébessa</i>

Acknowledgement

Before everyone, I want to thank my supervisor Dr. MEKHAZANIA TAHAR for his agreement to be my thesis supervisor and for consistent support, encouragement, patience and guidance during the work on this project.

I would also thank all members of the jury : Pr.LAOUAR MED RIDDA and DR MERZOUG SOULTANE for taking a time to examine my work

Then I thank Dr.DARDOUR MAKHLOUF the RSI speciality headmaster, and all the mathematics And computer science department team, teachers and workers.

I would finally thank my family and all my friends and colleagues of Larbi Tebessi university for their great support.

Dedication

To my genesis block, Jaz BMK...
To my wise buddy, Houssame BD...

المخلص

التصويت الإلكتروني هو علامة على الديمقراطية الحديثة. ومع ذلك عندما يتعلق الأمر بالأمن والشفافية، فقد واجهت أنظمة التصويت الإلكتروني العديد من المشاكل في السنوات القليلة الماضية. ان تقنيات السجل الموزع تنمو بسرعة كبيرة مؤخرًا ، مثل البلوكتشين وتطبيقها الأكثر شهرة المسمى بالبيتكوين، والذي يوفر مستوى عالٍ من الشفافية والقبالية للتحقق من جميع المعاملات الفردية. الهدف من هذه الدراسة هو شرح مفهوم البلوك تشين ، ومحاولة تطبيق فكرة استخدام البلوك تشين في التصويت الإلكتروني بالاعتماد على لغتي البرمجة نود و جافا سكريبت .

الكلمات المفتاحية: التصويت الإلكتروني، البلوك تشين، البيت كوين ،المفتاح العمومي، المفتاح السري، المحفظة الالكترونية.

Abstract

E-voting is a sign of modern democracy. However, when it comes to security and transparency, e-voting systems had many breaks in the past few years.

Distributed ledger technologies had been growing up too fast lately, such as Blockchain, and its most famous application called Bitcoin which offers a high level of transparency and verifiability for all individual transactions.

The goal of this study is to explain the notion of Blockchain, and try to implement the idea of using Blockchain in electronic voting. This implemented web-application for voting would adopt Node and JavaScript programming languages

Key words: E-voting, Blockchain, Bitcoin, Public key, Private key, E-wallet.

Resumé :

Le vote électronique est un signe de démocratie moderne. Cependant, en matière de sécurité et de transparence, les systèmes de vote électronique ont connu de nombreuses ruptures ces dernières années.

Recemment les technologies du registre distribué se sont développées trop rapidement, comme la Blockchain, et sa plus célèbre application appelée Bitcoin, qui offre un haut niveau de transparence et de vérifiabilité pour toutes les transactions individuelles.

Le but de cette étude est d'expliquer la notion de la Blockchain, et d'essayer de mettre en œuvre l'idée d'utiliser la blockchain dans le vote électronique. Cette application Web mise en œuvre pour le vote adopterait les langages de programmation Node et JavaScript

Mots clés : vote électronique, Blockchain, Bitcoin, Clé publique, Clé privée, Portefeuille électronique.

Table Of Contents

1	Blockchain	3
1.1	Introduction	3
1.2	Definition	3
1.3	The Three Main Properties of Blockchain Technology	3
1.3.1	Decentralization	3
1.3.2	Transparency	4
1.3.3	Immutability	4
1.4	Components of Blockchain	4
1.5	Types of Blockchain	5
1.5.1	Public Blockchain	5
1.5.2	Private Blockchain	5
1.5.3	Consortium Blockchain	5
1.6	Cryptographic Hashing	5
1.7	Areas of use of Blockchain technology	6
1.8	Blockchain Data Structure	7
1.8.1	Block	7
1.8.2	Chain	8
1.8.3	Network	8
1.9	How Blockchain work	8
1.9.1	Proof of Work	8
1.9.2	Nonce	10
1.10	Security of Blockchain	10
1.10.1	Blockchain wallet	10
1.10.2	Blockchain keys	11
1.11	Example of how Blockchain works	11
1.12	Conclusion	13
2	Blockchain and Election	14
2.1	Introduction	14
2.2	Background	14
2.2.1	Direct recording electronic (DRE) voting machines	14
2.2.2	Optical mark recognition systems	15
2.2.3	Electronic ballot printers	15
2.2.4	Internet voting systems	15
2.3	Problems	15
2.4	Opportunities	16

2.5	State of art	16
2.5.1	E-Voting on the Blockchain	16
2.5.2	E-Voting Blockchain Projects	17
2.5.3	VoteChain	18
2.6	Conclusion	18
3	VoteChain:An e-voting Web-Application system	19
3.1	Introduction	19
3.2	VoteChain : How was it build ?	21
3.2.1	Building steps and main functions	21
3.2.2	Database	24
3.3	Soft environment	27
3.3.1	Node JS	27
3.3.2	Express	27
3.4	Hard environment	28
3.5	Results	28
3.5.1	Presentation of VoteChain	28
3.5.2	VoteChain in test	33
3.6	Conclusion	33
4	Future prospects	35
4.1	Introduction	35
4.2	e-voting around the world	35
4.2.1	Countries uses e-voting	35
4.2.2	Countries uses e-voting partially	35
4.2.3	Countries put e-voting on test	36
4.2.4	Countries are no longer using e-voting	36
4.3	Renowned e-voting systems	36
4.4	e-voting : pro and conn	37
4.5	Algeria and e-voting	38
4.6	Conclusion	38

List of Figures

1.1	Structure of block[23]	7
1.2	Architecture diagram of a basic Blockchain[18]	8
1.3	Genesis Block[2]	11
1.4	How blocks linked together [2]	12
1.5	Invalid block [2]	12
1.6	Using nonce to get target hash [2]	12
3.1	General architecture	20
3.2	Detailed architecture	20
3.3	block Structure implementation (schema or DB model)	21
3.4	Implementation of block Structure in the application	21
3.5	Hashing the block	22
3.6	get last block	22
3.7	creation of new block and save it to the DB	22
3.8	Implementation of Blockchain	23
3.9	a block stored in mangodb	23
3.10	Creation of wallets and storing in DB	24
3.11	Vote Function	24
3.12	voters model	25
3.13	voter wallet model	26
3.14	candidate model	26
3.15	Blockchain model	26
3.16	Node js single thread execution [5]	27
3.17	VoteChain Welcome Interface	29
3.18	Register and Login	29
3.19	Password recover	30
3.20	Admin Home Page	30
3.21	List of voters	31
3.22	Voter home page before and after election event started	31
3.23	Get my wallet page	32
3.24	Results Page	32
3.25	Blockchain page	33
3.26	Duration to check the existance of block	33
4.1	E-voting around the world	36

List of acronyms

PoW Proof-of-Work

DRE Direct recording electronic

OMR Optical mark recognition

EBP Electronic ballot printers

VVPAT Voter verified paper audit trail

General Introduction

When we talk about democracy, protecting elections is a matter of national security. Governments have studied the possibilities of electronic voting systems to reduce the costs, and at the same time to put more legitimacy on the results. The traditional election system can be manipulated easily, so by replacing it with a new electronic voting system we can reduce fraud. Moreover, we can also trace and verify the voting process.

Electronic voting machines didn't look like a good idea for security reasons because anyone who can access to such machine can damage it or put a malicious code in it, so this will affect all the votes casted on that machine.

Another option is using Blockchain. Blockchain is a technology that distribute digital information to all parts of the network instead of copying it. That means each individual part of data belong to one owner [19]. So by using Blockchain features, we can guarantee the transparency and legitimacy of the results because the information can be accessible to everyone and unchangeable.

Our goal in this study is to create a voting web application that uses the power of Blockchain to protect the voting process and the results.

Chapter 1

Blockchain

1.1 Introduction

In this chapter, we will talk first about Blockchain definition, its properties, its components, its different types, and the most known area of use of it. In the main part of the chapter, we will talk about the data structure of Blockchain starting with block to the chain and the network. Then, we will talk about how Blockchain works by explaining the concept of proof of work and the nonce. After that, the security of Blockchain and finally, we example of how Blockchain works.

1.2 Definition

Blockchain is an accessible, transparent technology that allow users to transfer cryptocurrencies by using encryption keys and proof of work methods. Blockchain is a decentralized network. It has no owner and it don't belong to any authority. Its first and most famous application is Bitcoin [8].

1.3 The Three Main Properties of Blockchain Technology

Blockchain is known worldwide with its great reputation. Millions around the world count on it to protect them while exchanging cryptocurrency that worth thousands of dollars for each. Its benefits made it the worlds hot topic, and made a lot of individuals and organizations start adopting it due to the goods that it offers to the industry. The main reasons behind the Blockchain success are decentralization, transparency, and immutability.

1.3.1 Decentralization

Centralized means that all the data is stored in one entity, so to access the information we have to interact with that entity. Best example of centralized systems is the client-server model which

World Wide Web is based on, that was helpful for sometime. However, centralized systems have some vulnerabilities[9].

- Data being stored in one entity make it more vulnerable to hackers .
- Freezing the whole system every time we upgrade the centralized system .
- If something happened to the centralized entity and shut it down , the information will be inaccessible to all users.
- All data in the system will be compromised if the centralized entity gets hacked.

The decentralized system has solved all those problems. There is no centralized entity. Every entity within the network owns the information. So, when an entity wants to communicate with another one, it doesn't have to go through a centralized entity like servers in centralized systems[9].

1.3.2 Transparency

Transparency is one of main concepts in Blockchain . Each user is represented with his public address while his id is hidden by complex cryptography. All transactions made by that address can be seen by everyone who knows it. This level of transparency is what forced big companies to be honest because all their transactions are shown to everyone[9].

1.3.3 Immutability

Immutability means that the data entered the Blockchain can't be manipulated or changed. Blockchain gets this advantage because of the cryptographic hash function. It's what makes the blocks linked to each other, so any attempt to change a block will change the whole chain, which is impossible[9].

1.4 Components of Blockchain

Blockchain architecture contains the following components:

Node each user that is connected the Blockchain network.

Transaction Each operation between to nodes within the network that is recorded in a block.

Block a data structure for recording transactions that is distributed in all the network.

Chain a group of blocks linked in a specific order.

Miners specific nodes in the network that are responsible for verifying blocks.

Consensus rules and arrangements that made to execute Blockchain operations

1.5 Types of Blockchain

There are three categories of Blockchain structures:

- Public Blockchain
- Private Blockchain
- Consortium Blockchain

1.5.1 Public Blockchain

It's open source. Everyone can participate in it. All the transactions in it are transparent, which means that everyone can access the transactions details. It's not fully controlled by anyone. This is what makes the data secured because it can't be manipulated by a single person. The main use of the public Blockchain is cryptocurrencies like Ethereum, Litecoin, and Bitcoin[4].

1.5.2 Private Blockchain

Also called permissioned Blockchain. Only limited entities chosen by the respective authority can access and participate in it. The Blockchain developers gave permission to access to them during building the Blockchain application. If it has to give permission to a new user or revoke permissions from another, the Network Administrator is allowed to do it[4].

The main use of Private Blockchain is in private organizations to save sensitive data that should be available only to specific people[4].

1.5.3 Consortium Blockchain

Consortium Blockchain is a combination of private and public Blockchain. It used a group of parties with similar authorities as validators instead of letting anyone validate the transactions like in public Blockchains. Consortium Blockchain is used by groups of powerful companies like a group of banks [4].

1.6 Cryptographic Hashing

Hashing means producing a fixed length output out of an input string of any length[10]. Cryptographic Hashing is one of the main pieces in Blockchain technology. Its functions contain the following important properties:

Deterministic Same input always produce same output .

Irreversible It is impossible to find an input using the output of the function.

Collision resistance two inputs can't have the same output

One important feature of cryptographic hash functions is any small change of data in the input will change the whole output[10]. Blockchain uses cryptographic hash function to encrypt the data stored in each block. The block contains its own hash code and the previous hash code, so each block is linked to the previous block and the block that comes after, which makes data in Blockchain immutable[10].

1.7 Areas of use of Blockchain technology

Blockchain is becoming more and more Important for small and big businesses. Its features are so useful. These are some areas in which it got real advantage comparing to other existing technologies :

Digital currency

The first and the main application of Blockchain is creating cryptocurrency like Bitcoin, as well as transferring it without the third part[1]. It's use for :

- Payments
- Exchanges

Financial sphere

Blockchain infrastructure offering superior to current systems, security guarantees, speed, efficiency, programmability, disintermediation, and assets' automation can make a great upgrade to the financial system. Blockchain is the excellent financial protocol because of the transparency's level that the systems guarantee. In the financial sphere[1],It's use for:

- Automating financial system
- electronic properties markets

Crowdfunding and Fundraising

Blockchain Token can raise capital for existing companies and fund new businesses more effectively. The Token leads the businesses to international investment. Moreover, it helps collecting investors for new companies[1].It's use for:

- Financing new projects.
- Capital raising

Certification and Copyright

When using Blockchain to certificate data. It records it in an immutable block which gives the owner a proof that this data is exist. It can be used to prove the ownership of physical and digital properties[1].

1.8 Blockchain Data Structure

Blockchains are composed of three parts:

1.8.1 Block

Block is list of transactions recorded into a ledger in a known period [22] , a block consists of the block header and the block body [23], the block header contain :

Block version it decides which block validation rules to use[23].

Hash the hash value of the block contents[23].

Timestamp Exact time of the block creation[23].

Target Hash Specific number that the hash of the new block must be equal or less then it[23].

Nonce A random number added to the block to modify its hash to meet with the target hash[23].

Previous bloc hash The hash value of the previous block[23].

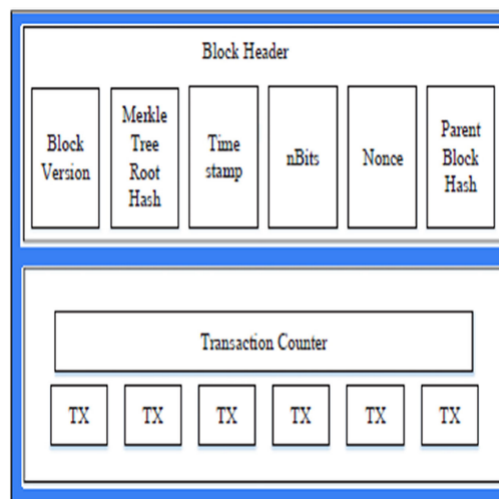


Figure 1.1: Structure of block[23]

The body of the block contains the transactions and its counters. The number of transactions is depending on the size of each transaction and the size of the whole block. Each transaction get validated and authenticated using an asymmetric cryptography[23].

1.8.2 Chain

The Blocks are chained to each other with hash function. The hash of a block is the previous hash of the next block [22]. Any attempt of messing with content of a block will change its hash, and it will no longer be equal to the next block previous hash. Then the whole chain breaks. The next figure shows how the blocks are linked together.

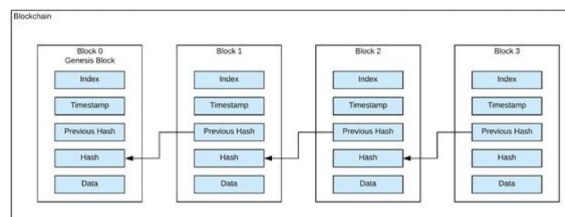


Figure 1.2: Architecture diagram of a basic Blockchain[18]

The first block is called genesis block. It is special because it is the only block that has no previous hash or data. [18]. The other blocks contain the data of all transactions.

1.8.3 Network

The network is composed of nodes. All nodes contain records of all the transactions in that Blockchain, the nodes are located all around the world. Everyone can participate within the network and become a node. However, participating as a full node is expensive and consume a lot of computing power. Therefore people who do that earn cryptocurrencies as a reward from Blockchain[22].

1.9 How Blockchain work

1.9.1 Proof of Work

Proof of Work is the algorithm used by Blockchain network in order to validate transactions and create new blocks. Miners use this algorithm to confirm transactions. The first one who finish the validation get the right to create the block and get reward[26].

How it work

Proof of work got two main principals which are a complicated mathematical puzzle and a possibility to easily prove the solution [26]. Blockchain give this complicated puzzle to miners in order to valid transaction, and they try to solve it with hush function , who ever got the right solution share it with the other nodes, they will check if the calculations are correct, if it's correct, he create the block. It's a competition so only the first one who find the right solution get reworted.

Applications of Proof-of-Work

The first and main implementation of proof of work in Blockchain technology is Bitcoin. It's used to validate transaction for creating new blocks. The PoW algorithm changes the difficulty of the puzzle considering the power of the network in order to keep the average time of creating blocks on 10 minutes max [26].

Benefits of Proof-of-Work

Proof-of-Work is mainly used to prevent DoS attacks. Dos need a lot of calculation time and computing power, so there is no use of such attacks because the time of creating blocks is so short. Another benefit is control mining by making it hard to solve the puzzles. Miners will need a lot of computing power to solve it in very short time, so it won't be any time to mess with the transaction, or make large profits from mining because only one miner creates the block each time[26].

Disadvantage of Proof-of-Work

First disadvantage of PoW is that it's so expensive. Since mining requires high performing hardware, only special machines are capable of doing it. These machines consume so much power, which make mining very expensive and that threats the decentralization of the system[26].

Another disadvantage is that miners use a very expensive hardware to solve puzzles and create blocks. This hardware is useless outside this field[26].

The last con of Pow is the 51 percent attack, which is an attack happen when a group of users control the majority of mining power. They can Monopoly creating new blocks and get all the rewards because they can stop other miners from completing creation of the blocks. However, this attack is not a wise option because it needs a huge mining power and once it's exposed the price of the cryptocurrency will drop down[26].

1.9.2 Nonce

Nonce or "number only used once" is a random number added to a block to change its hash in order to get the target hash. The miners keep changing the value of Nonce in order to create the new block and be rewarded[20].

The use of nonce

There is a certain set of requirements in the hash of the new block to be accepted and validated which is called target hash. A target hash is a number that the value of the new block must be equal or less than it in order for a new block to be accepted and created [21]. In order to create a hash value that meets with the hash target, miners keep changing the value of the nonce and check if the new block hash suits the target hash target. Whoever finds it first gets rewarded and that's what we call mining. So, mining is trying to guess the right value of nonce to get the target hash.

1.10 Security of Blockchain

1.10.1 Blockchain wallet

Definition

Blockchain wallet is an e-wallet mainly designed for fast and secure online payments management [17]. It allows its owners to monitor and control cryptocurrency. Each wallet has a public and private key. Sender of cryptocurrency needs the receiver public key to send it. When he sends it, the address of the cryptocurrency will change from the owner to the receiver. Each owner needs the private key to access his or her wallet, so the private key should stay hidden.

Types of Blockchain wallets

there are four main types :

Software wallets : It is a software that user install on his computer or mobile device to fully control his crypto currencies [17].

Web hosted wallets : It is more easy to use because it is similar to web applications. It is hosted by a third part so the user must check its security level before using it [17].

Hardware wallets : Its a physical USB devise that stores the private key of the wallet. its owner use it by insert it in an internet connected devise then enter his pin code [17].

Paper wallets : The wallet keys are generated by a software then printed on a paper with a QR code that used during each transaction[17].

How do Blockchain wallets secure online payments?

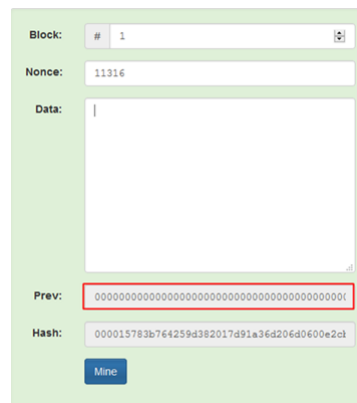
Each time a user make an online payment using his wallet. The wallet interact with the Blockchain network to validate the transaction to allow user to buy, sell or trade cryptocurrencies [17].

1.10.2 Blockchain keys

The public and private keys used to confirm that the transaction is really happed between the owner of the cryptocurrencies and the receiver. Public and private keys are not just about Blockchain and cryptocurrencies, it belongs to a larger cryptography field called Asymmetric Encryption [7].

1.11 Example of how Blockchain works

First Block in the Blockchain called the genesis Block , it's the beginning of the chain so it don't have a previous hash.



The image shows a web-based interface for mining a blockchain block. It features several input fields and a button:

- Block:** A dropdown menu showing the number '1'.
- Nonce:** A text input field containing the value '11316'.
- Data:** A large, empty text area for entering transaction data.
- Prev:** A text input field containing a long string of zeros followed by a '1', representing the previous block's hash. This field is highlighted with a red border.
- Hash:** A text input field containing the resulting hash: '000015783b764259d382017d91a36d206d060e2d1'.
- Mine:** A blue button at the bottom.

Figure 1.3: Genesis Block[2]

The hash of the block will be the next block previous hash as the next figure shows.

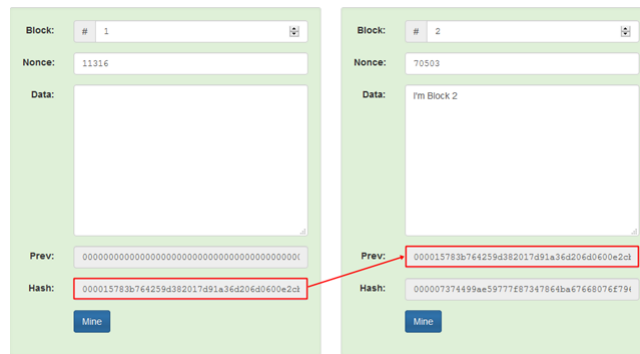


Figure 1.4: How blocks linked together [2]

The hash of the block that will be created rarely met with the target hash which is that it start with four zeros .

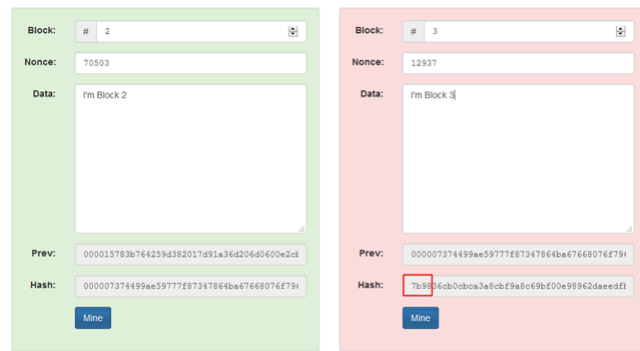


Figure 1.5: Invalid block [2]

To get a hash that meet with target hash , miners keep changing the value of the nonce and test if the hash is valid, who ever guess it first get reward and create the block .

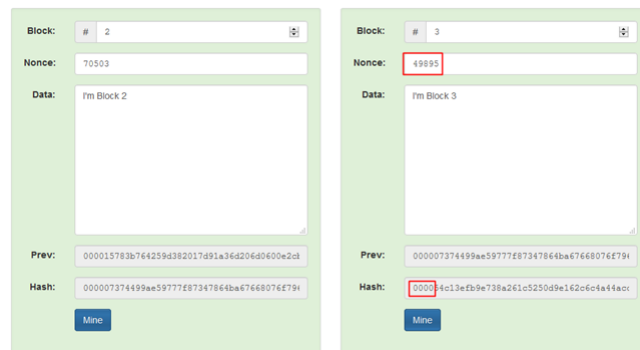


Figure 1.6: Using nonce to get target hash [2]

1.12 Conclusion

In this chapter, we've seen an overview of Blockchain, including the definition, its properties, its components, different types, and the most known area of use of it. Moreover, we discussed the data structure of Blockchain, how it really works, and how it secures transactions. Finally, we showed a practical example of it.

Chapter 2

Blockchain and Election

2.1 Introduction

In this chapter, we will see how e-voting starts followed by its different types . After that, the problems that it faces will be explained. Then we will mention the status of e-voting around the world. Finally, we will discuss a future vision of how e-voting will become.

2.2 Background

Electronic voting system is a big challenge. It is considered as one of the hardest upgrades because this will involve all parts of the electoral process : the casting and counting of votes. E-voting is used to decrease direct human control and effect in the process of election.

There are a number of e-voting systems that proved to be a way to reduce the costs, improve the voting methods, and resist electoral malpractice.

2.2.1 Direct recording electronic (DRE) voting machines

DRE is a system that offers electronic devices such as touch screen, keyboard, mouse or electronic pen to allow voters to enter their choices. It's also a non-remote system used with supervision in polling stations. The machine, then, saves the voters' choices in the memory chip. After election time is done, the data saved in each DRE machine will be transmitted to the counting center by internet or manual way which is printing the results and sending it. Then the center counts all votes and announces the results. Each DRE machine may or may not have a feature called VVPAT or voter verified paper audit trail which is a paper record that allow each voter to verify his choice after voting so people usually are more comfortable to use it because it offers more transparency [14].

2.2.2 Optical mark recognition systems

OMR systems are a combination of paper ballot and electronic counting. The voter marks his choice with a pen or pencil on a given ballot paper, then puts that paper on OMR machine that can read it. The machine counts the votes using marks made by the voters in the paper ballot. OMR systems are a great choice because they cost much less than DRE machines, but a lot of factors can affect the counting process such as ink type, or paper thickness [14].

2.2.3 Electronic ballot printers

EBP machines are similar to DREs. Both take the voter choice using electronic devices. The difference is that EBPs don't store vote data, instead, it prints a token with the voter choice. Then the voter puts that token in an electronic ballot box which counts the votes automatically. EBPs are composed of two machines, one for taking the voter choice and the other one for recording it [14].

EBP is easy to use and understand for everyone, especially the old ones, because it's similar to the traditional way. So, it's a good choice to enter the world of e-voting for countries that have never used it before [14].

2.2.4 Internet voting systems

An internet voting system is a remote unsupervised system that allows each voter to cast a vote any time anywhere he wants with any device with internet access. This makes it the most comfortable system for all users. However, such systems require a great care of authentication to avoid frauds. There're also a lot of concerns about security of ballots and of the whole system. Pirates could hack into the system to affect the results. That's what makes it not the first choice for governments [14].

2.3 Problems

The biggest challenge that the electronic voting systems is facing is its security and privacy. Protecting the whole process of election is the most important thing. An e-voting system doesn't look like a good idea because of three main reasons : software error, impossibility to get votes back in case its lost without VVPAT, and the opportunities of fraud is much more than ever.

There's no perfect system. No one knows how to build such thing so software errors must happen somehow. E-voting software is so complicated, and the more complicated the software is, the harder it is to find the errors and fix it. Errors may cause a loss of votes like the case in

2004 in North Carolina USA, 4438 votes were lost because of system errors. Also in Florida at the same year, 134 votes were gone [6].

Another problem that the e-voting system is facing is that there's no way for the voter to trace his vote or to know if it's recorded correctly or not. For example in DRE machines, after the voter cast his vote, if for any reason the machine didn't count his vote or didn't get it correctly, he or she will not know. And it may happen to many voters. And when the election event ends, the results printed from the machine would be wrong and no one would even know.

2.4 Opportunities

The election result data is elaborate, and the total voting process is also delicate. In addition, security is also an important key to the fair elections. Each ballot needs to be respected. However, in reality, it does not be like how it is supposed to be. So, the opportunities of using Blockchain technology are higher to solve those concerns.

Interestingly, the Blockchain technology has more potential advantages than the traditional election methods because of the huge technological upgrades from how the current elections are arranged. Many national elections still use the paper system or electronic voting machines which causes big problems in security leak and corruption.

The transparency of Blockchain allows the votes to be followed, counted, and calculated from many different sources. Consequently, we can say that Blockchain can make a great upgrade to e-voting that can fix all its problems.

2.5 State of art

2.5.1 E-Voting on the Blockchain

E-voting can be one of the best application of Blockchain. Blockchain distributes votes through thousands of nodes to make it impossible to edit or delete it. This will make election more secure and transparent which increase citizens trust in their government. This trust come from the idea of that each voter own his data. Such platforms will allow voters to cast their votes through smartphone applications or websites instead of staying in long lines in pooling stations. this will change the central nature of traditional election to make it decentralised and owned by citizens instead of government and it will guarantee integrity and trust which is the hardest things to guard in election[16]. A Blockchain implimentation must offer:

Public Verifiability: All voters can see and verify the voting process[16].

Individual Verifiability: Each voter can verify that his vote recorded correctly[16].

Auditability: Election results must be verifiable after election ends by public[16].

Anonymity: Votes are not related to voters[16].

Transparency: Blockchain allows all public to scrutinize the whole process[16].

2.5.2 E-Voting Blockchain Projects

Some great communities and IT service providers are trying to implement Blockchain for e-voting. The following are some of the project they work on:

Luxoft

Luxoft Holding is known worldwide with the IT services that it provides. It plans to deliver the first e-voting system that is based on Blockchain in the city of Zug in Switzerland. It team up with organizations that work on government services that uses Blockchain to finish this project together. Luxoft idea is to use strong encryption technology to hide voters identity and use proof of work method as temper proof and make to whole process auditable, and make it decentralized by distributing the data in three data centres, two of them in Switzerland and one in Ireland[16].

IIT Bandung

IIT Bandung uses Blockchain to record votes from every election place. The system they made uses nodes with predetermined turn instead of using proof of work like the way in Bitcoin. The idea is that each node generates public and private key before the election event starts. Each node share its public key with all other nodes. When election event starts, the node take the voter choice and wait its turn to create a block. then it create it and distribute to all other nodes. The distributed block will contain the node id, the vote results, the timestamp, the hash and the previous hash[16].

Ethereum Blockchain Trustless Voting

Fernando Lobato create an e-voting system that lives on a smart contract in the Ethereum network. It uses threshold keys and linkable ring signatures to upgrade the transparency and power of the system. Each voter can check his vote while his identity stay hidden. This will minimize the centralization of the system and allow each voter to tall the whole voting process even if he didn't vote yet. the voting smart contract have the the following steps after being deployed on the Blockchain[16].

Setup: Government adds information of election, like starting time, list of candidate and duration[16].

Registration: Voter request his keys from authority[16].

Voting: The voters that they already registered submit their encrypted vote to the contract[16].

Finished Once the voting phase is over all the third parties holding secrets can submit them to the Blockchain. When all the secrets are in the contract, anybody can download and reconstruct the private key[16].

Ready to Tally all the voters can tally and verify the results[16].

Public Votes

PublicVotes is a free voting application build with using the Ethereum Blockchain network to create a trustful and transparent environment to cast their votes. All votes of participants are recorded (by proxy) into the Blockchain for the world to verify. The application is not fully decentralized, since the design goal was to create an application that is easy to use for people outside the Ethereum space. The entire platform is built on Meteor with one smart contract coded in Solidity that is used for placing a poll into the Blockchain and for casting the votes. Anyone with a small amount of Ether can create a poll. At PublicVotes, the creator of the poll pays for the creation of the poll and for all votes[16].

2.5.3 VoteChain

VoteChain is a Blockchain based web application for election, so it's a remote internet voting type. it's a node js application connected with mongodb database. It allows the authority to start a vote after creating candidates. It also allows each voter to cast his vote safely and secure. What makes VoteChain special from other usual voting apps is the implementation of the notion of Blockchain to secure the votes and to put more transparency on the election.

2.6 Conclusion

Innately, e-voting was all about voting machines. Internet voting was not the first option for security concerns, but with years passing, voting machines become more and more vulnerable. So, developers start working to secure online voting because of the evolution in security development. Consequently, in my vision, the future e-voting will be an internet voting based on Blockchain to solve all security and privacy issue for fair and transparent election.

Chapter 3

VoteChain: An e-voting Web-Application system

3.1 Introduction

VoteChain is a Blockchain-based web-application to organize election events. It's designed to fix the weakness of normal internet voting systems by adding features of Blockchain. And also like DRE machines with VVPAT, it adds a good feature which is the ability of tracing votes for each voter.

The idea of VoteChain is that each voter gets a wallet with one token. Candidates get an empty wallet. When an election event starts, voters send the token from their wallets to the wallet of the candidate they want. After the transaction is made, it gets recorded in a block in Blockchain. The winner is the one who gets the most tokens.

VoteChain allows each voter to create an account, and recover password in case of loss. Authority creates candidates and a wallet for each one. It also can check the list of voters and create wallets to all of them. Both users and authority have access to the Blockchain, so everyone can verify the whole voting process.

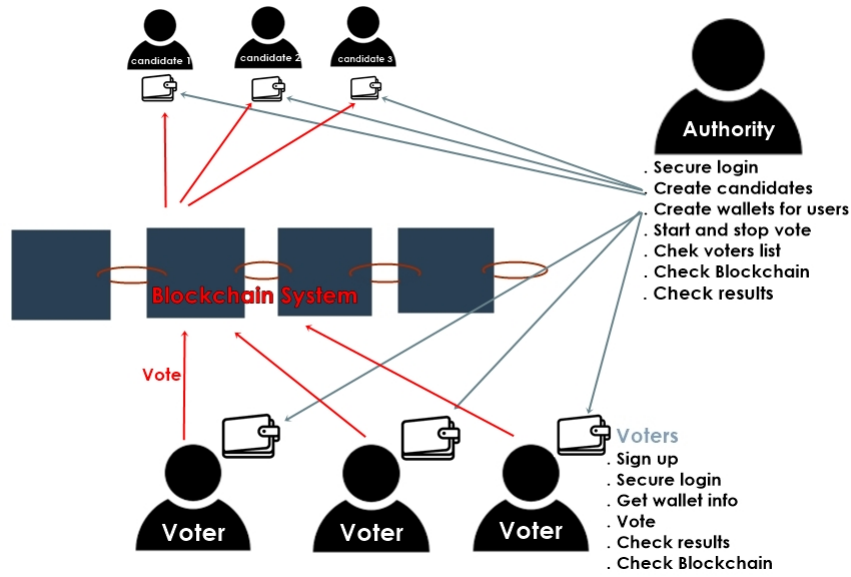


Figure 3.1: General architecture

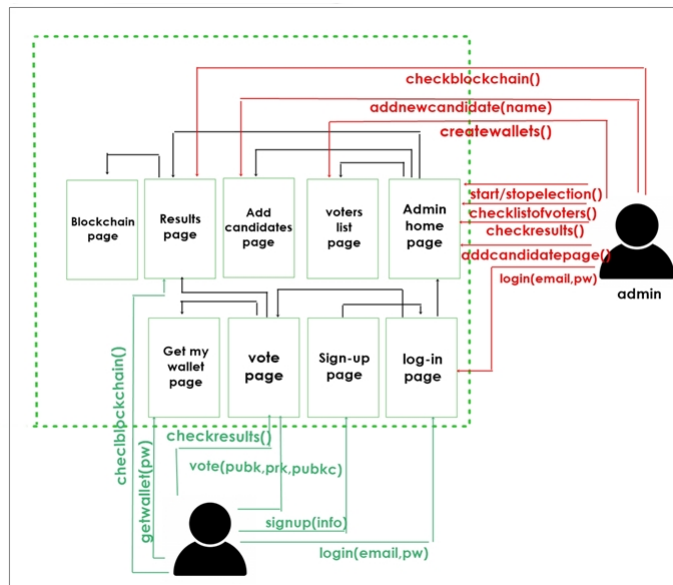


Figure 3.2: Detailed architecture

In this chapter, we will first start talking about the main function of the web application, the database tables and building steps. Then, we will talk about the used environment, starting with the used platform and the database. Finally, we will represent the result and what our application offers.

3.2 VoteChain : How was it build ?

3.2.1 Building steps and main functions

Step one : block structure

Transactions are saved permanently in a structure called blocks. Blocks are linked to each other to create what we know as Blockchain. Each block records the recent transactions, along with other things such as timestamps. And it refers to the block that comes just before it. It also contains the answer to a very hard-solved puzzle (proof of work) which is the only way to create new blocks (mining).

```

1  const mongoose = require("mongoose");
2  const BlockChainSchema = new mongoose.Schema({
3  ▾  index: {
4     required: true,
5     type: Number
6  },
7  ▾  timestamp: {
8     required: true,
9     type: Date,
10    default: Date.now()
11  },
12  ▾  transactions: {
13     required: true,
14     type: Array
15  },
16  ▾  prevHash: {
17     required: false,
18     type: String
19  },
20
21  ▾  hash: {
22     required: true,
23     type: String
24  }

```

Figure 3.3: block Structure implementation (schema or DB model)

index	timestamp	Hash	Previous Hash	Transactions
1	Sat May 09 2020 15:12:34 GMT+0000 (GMT)	3ef450db23b9743ea4613d21727883b0df7ad51b		Voter : 1JH78p1v2SVUVEc5j9pQ5kia6y7PLUAkK Candidate : 16aoekrxW4kbDkxBFkXQeJ4yktMfRbD1z7 Ammount : 1

Figure 3.4: Implementation of block Structure in the application

Step two : Hash

In order to keep the integrity of Blockchain data, each block needs to be hashed. That's what links the blocks to each other. The algorithm used is the hash function (also known as SHA256). The hash function takes any size of data and it gives a fixed size string. Each time we enter the same data we get the same result. And it's impossible to find the entered data through the output.


```

1 let hash1 = require("object-hash");

block.hash = hash1(block);

```

Figure 3.5: Hashing the block

Step three : Coherence of blocks

In order to create a new block, we must know the hash of the previous block, so each change on the data inside the block will change the block hash. The next block's previous hash will not be equal to that new hash. And the whole chain breaks and becomes invalid. This is the code to get the last block from the database in order to get the previous hash .

```

//Get last block from Database
getLastBlock(callback) {
  return BlockChain.findOne(
    {},
    null,
    { sort: { _id: -1 }, limit: 1 },
    (err, block) => {
      if (err) return console.error("Cannot get last block ", err.message);
      return callback(block);
    }
  );
}

```

Figure 3.6: get last block

After getting the last block, it will be easy to generate a new block using the previous block hash. This is the code how to generate a new block and save it to the database.

```

addNewBlock(prevHash) {
  let block = {
    timestamp: Date.now(),
    transactions: this.curr_transactions,
    prevHash: prevHash,
  };
  //when get the target hash (the right nonce)
  if (validator.proofOfWork() == TARGET_HASH) {
    //get last block from database
    this.getLastBlock((lastBlock) => {
      if (lastBlock) {
        block.prevHash = lastBlock.hash;
        block.index = lastBlock.index+1;
      }
      block.hash = hash1(block);
      var index = block.index;
      var timestamp = block.timestamp;
      var transactions = block.transactions;
      var prevHash = block.prevHash;
      var hash = block.hash;
      //save the block in the
      const newBlock= new BlockChain(
        {index,
        timestamp,
        transactions,
        prevHash,
        hash
        });
      newBlock.save((err) => {
        if (err)
          return console.log("Cannot save Block to DB ", err.message);
        console.log("Block Saved on the DB");
      });
      //Add to Chain
      this
        .chain
        .push(block);
      this.curr_transactions = [];
      return block;
    });
  }
}

```

Figure 3.7: creation of new block and save it to the DB

index	timestamp	Hash	Previous Hash	Transactions
1	Sat May 09 2020 15:12:34 GMT+0000 (GMT)	3ef450db23b9743ea4613d21727883b0df7ad51b		Voter : 1JH78p1v25VUVEc5j9pQ5kia6y7PLUAktk Candidate : 16aoekrxW4kbDkx8FKXQeJ4yktMRbD1z7 Ammount : 1
2	Sat May 09 2020 16:50:32 GMT+0000 (GMT)	f806dba0c0e20c70f5fd200449c6c04aeaf73f2e	3ef450db23b9743ea4613d21727883b0df7ad51b	Voter : 13Hh83D1E24dAIApPHkgBVno7Qp2FF23kc Candidate : 1QBfEshyB5itRmTiqD6KEe3wg5W4vmih Ammount : 1
3	Sat May 09 2020 21:48:28 GMT+0000 (GMT)	4efe82d207dce55ec070c56f4835eb59643d955f	f806dba0c0e20c70f5fd200449c6c04aeaf73f2e	Voter : 14nD6AgbWV3iNwdyc3DTknw4PbRgVkmMgm Candidate : 16aoekrxW4kbDkx8FKXQeJ4yktMRbD1z7 Ammount : 1
4	Sun May 10 2020 13:11:52 GMT+0000 (GMT)	779488e8a8ee81b30305ac0cd1b6d9162b68a0f0	4efe82d207dce55ec070c56f4835eb59643d955f	Voter : 1BSWUL2dmxF8aAkJDsRk5v87yS9MnGzcf Candidate : 16aoekrxW4kbDkx8FKXQeJ4yktMRbD1z7 Ammount : 1

Figure 3.8: Implementation of Blockchain

Step four : Storing blocks

The Blockchain is stored and it's accessible to each node in the network. If a node is not working, this won't affect the Blockchain at all. we've stored it in Mangodb database. Each user can access it, but no one can change it.

```

QUERY RESULTS 1-4 OF 4

  _id: ObjectId("5eb6c86589ac876143c2474e5")
  timestamp: 2020-05-09T15:12:34.525+00:00
  > transactions: Array
    index: "1"
    prevHash: null
    hash: "3ef450db23b9743ea4613d21727883b0df7ad51b"
    
```

Figure 3.9: a block stored in mangodb

Step five : Creating wallets

The authority creates a wallet for each candidate and each voter. The candidates' wallets are empty, but other voters' wallets contain one token which is enough to vote just once. I used a library called "bitcore-lib" for creating wallets, which gives us wallets starting from a string. The string I used is the email because it's unique. This piece of code is for creating and storing Wallets keys and amounts in the database.

```

users.forEach(function(user) {
  email[i] = user.email;
  name[i] = user.name;

  var nn = new Buffer.from(email[i] );
  var hash =bitcore.crypto.Hash.sha256(nn);
  var bn = bitcore.crypto.BN.fromBuffer(hash);
  var prk = new bitcore.PrivateKey(bn).toWIF();
  var pubk = new bitcore.PrivateKey(bn).toAddress().toString();
  var owner = name[i];
  var email = email[i];

  Wallet.findOneAndUpdate({ email: email[i] }, {pubk:pubk,prk:prk,ammount:1}, { new: true }, (err, doc) =>{
    if (!err) { console.log("done");}
    else {
      console.log('Error during record update : ' + err);
    }
  });
  i++;
});

```

Figure 3.10: Creation of wallets and storing in DB

Step six : Cast a vote

Vote function works as this : when a voter casts a vote. He sends his public and private key, and the candidate's public key. Vote function searches for that wallet in the table of wallets in the database, also searches for the candidate wallet. Then it minuses from the amount of voters' wallets, and adds it to the candidate wallet. Then it puts those users as already voted. After all of this, the transaction (voter, candidate, amount sent) will be saved in the database. This piece of code contains that function.

```

function vote(voteremail,voter,candidate,pk) {
  Wallet.findOne({email: voteremail}).then(wallet => {
    if (!wallet) {
      console.log("vote address wrong");
    }
    else{
      if(voter==wallet.pubk){
        if (pk==wallet.prk) {

          CandidateWallet.findOne({pubk: candidate}).then(CandidateWallet => {
            if (!CandidateWallet) {
              console.log("no such address for any candidate");
            }
            else{
              Wallet.findOneAndUpdate({ pubk: voter }, {$inc: {ammount:-1}}, { new: true }, (err, doc) =>{
                if (!err) { console.log("done"); }
                else {
                  console.log('Error during record update : ' + err);
                }
              });
              User.findOneAndUpdate({ email: voteremail }, {votedyet:true}, { new: true }, (err, doc) =>{
                if (!err) { console.log("done"); }
                else {
                  console.log('Error during record update : ' + err);
                }
              });
              CandidateWallet.findOneAndUpdate({ pubk: candidate }, {$inc:{ammount:1}}, { new: true }, (err, doc) =>{
                if (!err) { console.log("done"); }
                else {
                  console.log('Error during record update : ' + err);
                }
              });
            }
          });
          blockchain.addNewTransaction(voter, candidate, 1);
          blockchain.addNewBlock(null);
        }
      }
    }
  });
}

```

Figure 3.11: Vote Function

3.2.2 Database

VoteChain used a scalable and flexible document database called mongodb. This Database is composed of a set of documents. It stores the data with no limitations of the format and

structure unlike the old method that stores data in the relational databases. The document is able to contain floats, numbers, strings, and even objects and arrays. It makes working on the database fast and simple. MongoDB supports many operations, such as querying for the documents, inserting new documents, editing and deleting existing documents[25].

What makes MongoDB special is the ability of storing dynamic data. we can find different properties for documents of the same collection. So unlike the other relational databases, It can store different structured data. Storing all the data in a single document will speed up the operations more than relational databases because it will avoid joining many tables to get the data[25].

Mongoose

It is a schema-based solution that was made to model the application data. It creates different key value pares for the different data types that the app use. It is used to build a structure for the data to make the applications work correctly. Mongoose allows the developers to model the data inside Mangodb within the code [25].

Database architecture

By using the Mongoddb database, we've created the tables, or as Mongoddb calls it "collections". The first collection is for the users, it contains the information about each user and stores email and password for each one.

```
const UserSchema = new mongoose.Schema({
  name: {
    type: String,
    required: true
  },
  email: {
    type: String,
    required: true
  },
  password: {
    type: String,
    required: true
  },
  secquestion: {
    type: String,
    required: true
  },
  answer: {
    type: String,
    required: true
  },
  idcard: {
    type: Number,
    required: true
  },
  date: {
    type: Date,
    default: Date.now
  },
  type: {
    type: String,
    default: 'user'
  },
  votedyet: {
    type: Boolean,
    default: false
  },
  blockchaincopy: {
    type: Array,
    default: []
  }
})
```

Figure 3.12: voters model

Second collection is for voters wallets, each wallet has an owner, email, public key, private key and amount.

```
const WalletSchema = new mongoose.Schema({
  email: {
    type: String,
    required: true
  },
  owner: {
    type: String,
    required: true
  },
  pubk: {
    type: String,
    default: ""
  },
  prk: {
    type: String,
    default: ""
  },
  amount: {
    type: Number,
    required: false
  },
  vote: {
    type: String,
    default: "not voted yet"
  }
});
```

Figure 3.13: voter wallet model

The third collection is for the candidates , it contains information about each candidate and the wallet keys and amount.

```
const CandidateWalletSchema = new mongoose.Schema({
  name: {
    type: String,
    required: true
  },
  pubk: {
    type: String,
    required: true
  },
  prk: {
    type: String,
    required: true
  },
  amount: {
    type: Number,
    required: true
  }
});
```

Figure 3.14: candidate model

The last collection is for the Blockchain. It contains index, timestamp, hash, previous hash, and transactions, as we mention it above in building steps.

```
const BlockchainSchema = new mongoose.Schema({
  index: {
    required: true,
    type: Number
  },
  timestamp: {
    required: true,
    type: Date,
    default: Date.now()
  },
  transactions: {
    required: true,
    type: Array
  },
  prevHash: {
    required: false,
    type: String
  },
  hash: {
    required: true,
    type: String
  }
});
```

Figure 3.15: Blockchain model

3.3 Soft environment

VoteChain consists of three main technologies. We build the application by using Node js, Express MongoDB.

The reason why we chose those technologies is because voting web-application will get big traffic from voters, that can slow it down or even block it. So in order to avoid that, we use node js instead of php. Node js's non-blocking nature will make the web-application fast.

3.3.1 Node JS

Node js is a free open source platform that uses asynchronous programming. It is a non-blocking platform that is designed to build scalable network applications which make it a great choice to build real-time web applications [24].

Node js create his own server by using the HTTP module, This server connects to the database, takes requests, handles it, validates inputs, and returns results by rendering an html page or as a JSON file [24].

What makes Node js fast is his non-blocking nature, and that comes from his way of handling requests. It creates a loop to take all requests in the same thread, so it doesn't wait for an API to complete to start the next one. The next figure shows how the execution works [24].

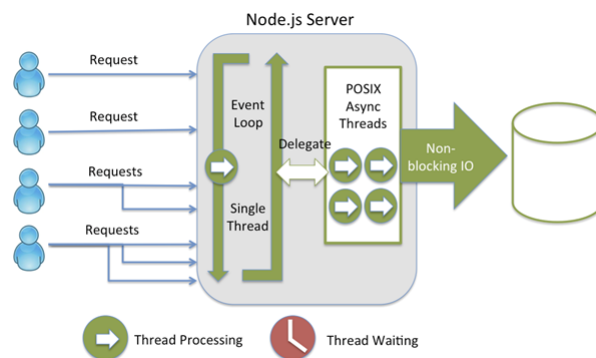


Figure 3.16: Node js single thread execution [5]

3.3.2 Express

Express is a very popular routing framework that was made upon Node js. Its flexibility offers many powerful tools and features to make building node apps more easy and fast[3].

Express middleware is a combination of functions that get executed during the cycle of a request sent to the express server. Each middleware or function can access to the HTTP request and response that it's linked to. The middleware takes the request then execute the code inside it and change the objects of the request and response then pass it again to the next middleware[25]. Express application can access to five types of middleware which are:

Application-level middleware It is related to app object by using two functions which are “app.method()” and ” app.use()”[25].

The router-level middleware Same as application level middleware but it's related to an instance of the express router instead of the app object[25].

Error-handling middleware It is linked to the app object. And it takes four arguments which are :the request, the response, the error and the next object[25].

Built-in middlewares It serves the files in a static way and analyze the incoming request to JSON[25].

Third-party middlewares it log the information about the coming request or it pass the cookies in order to extend the functionality of the express app[25].

3.4 Hard environment

The systems used to build and run VoteChain contain the following properties :

Operating System: Windows 8.1.

Ram: 4 GB.

Disk Space: 156 MO.

3.5 Results

3.5.1 Presentation of VoteChain

VoteChain web-application starts with a simple interface to let the user choose to sign up or login.

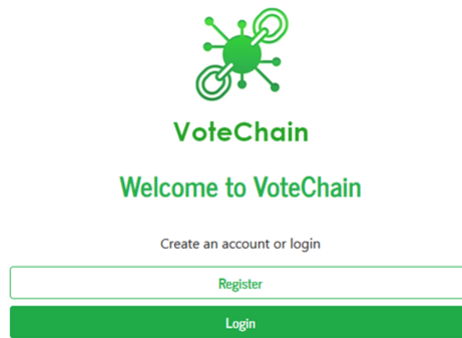


Figure 3.17: VoteChain Welcome Interface

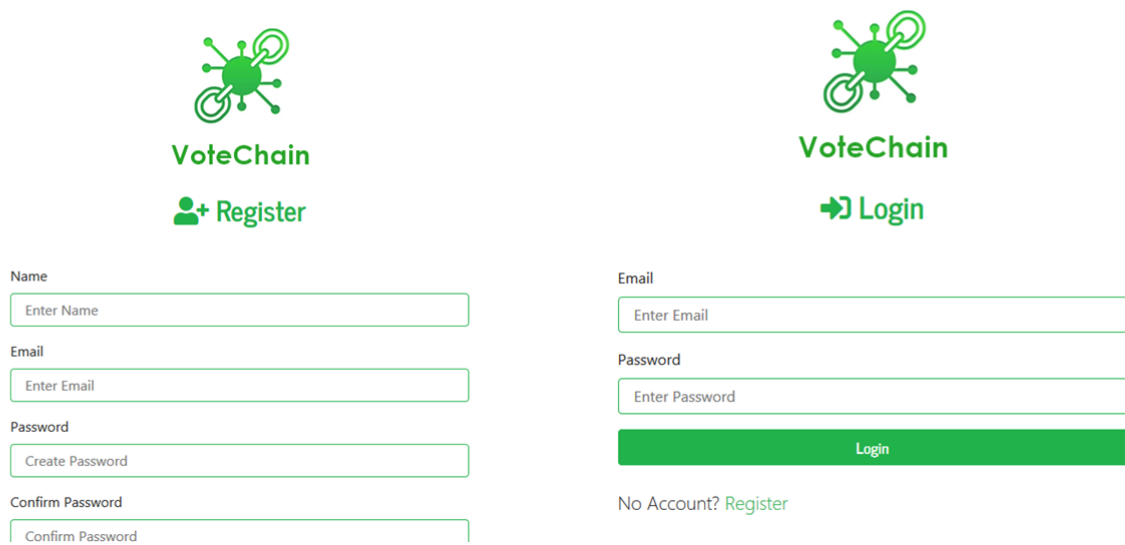



Figure 3.18: Register and Login

In case the user forgets his password, he can choose to recover it.



VoteChain
Forget Password

please choose the right security question and answer it

What's the name of your favorite uncle

Email

Enter Email


Answer

Enter your answer

Get My Password

Figure 3.19: Password recover

After login, the authority (admin side) main page shows the list of candidates that he created. He can choose to add candidates and launch the vote or stop it, and check the list of voters as the following figure shows.



VoteChain
Admin side

[Add Another Candidate](#) or [Check list of voters](#)

Candidate List :

Full Name	Wallet
Nouar Dahem	1HFFB4kYyiRBV4QeVofdNN7sm57515jBFp
Amar Nahal	1KxKizLUTvQTihq7WSUUhSdp2UnjFRJPvM

Start vote

Logout

Figure 3.20: Admin Home Page


When the admin wants to check the list of voters, he gets a list of all registered voters, with their names, emails, status (voted or not yet), and wallet keys in case he created it already. And he can choose to create wallets for all of them at once.

List of voters

Full Name	E-mail	Public key	Private key	Status
Tayeb Guergah	tayeb.guergah.me@gmail.com			not voted yet
Houssame Boudiar	houssame.boudiar@gmail.com			not voted yet
aymen Chihani	aymen.chihani@gmail.com			not voted yet
Maini Rachid Cherif	maini.rachidcherif@gmail.com			not voted yet
Badaoui Youcef Islam	badaoui.toucef@gmail.com			not voted yet
Yasmin Benmabrouk	yasmin.benmabrouk@gmail.com			not voted yet
Amani Zarougui	amani.zarougui@gmail.com			not voted yet
Hadjaj Khawla	khawla.hadjaj@gmail.com			not voted yet
Djadla Mohammed Ibrahim	djedla.moh@gmail.com			not voted yet
Mellaoui Taki Eddine	melloui.taki@gmail.com			not voted yet

Figure 3.21: List of voters

If the voter logs in before the admin starts the election event, he will be moved to a page that tells him that the election event didn't start yet. If it's started, the voter will be moved to his home page where he can find the list of candidates and he can vote.



Welcome Tayeb Guergah

The Election Event didn't start yet , So election home page is not available yet

[Logout](#)

Vote

Welcome Tayeb Guergah

Nouar Dahem

Amar Nahal

Public Key

Private Key

[Vote](#)


Didn't get your walet yet? [Get my wallet](#)

[Check Results](#)

[Logout](#)

Figure 3.22: Voter home page before and after election event started

The voter needs his wallet key to cast a vote, so before he can cast a vote, he has to go to The get my wallet page to get them. When he's on that page, he needs to enter his password to get the wallet keys.



VoteChain

Get my wallet

Welcome Tayeb Guergah

to get your wallet keys rener your password please

Password

[Get My Wallet](#)


Your wallet

your public key is: ***** 17bJbChbqWPDtTF4GT6M9Rdvc4hecYmri *

[Back](#)

Figure 3.23: Get my wallet page

Both admin and voters can access the results and the Blockchain page where all transactions are recorded .



VoteChain

Results

Candidate	Wallet address	Votes
Nouar Dahem	1HFFB4kYyirBY4QeVofdNN7sm57515JBfp	0
Amar Nahal	1KvXizLUTvQtiHq7WSUUhSdP2UnjFRJPvM	0

[Blockchain](#)

[Logout](#)

Figure 3.24: Results Page

The blockchain

index	timestamp	Hash	Previous Hash	Transactions
1	Tue Jun 02 2020 22:14:37 GMT+0100 (GMT+01:00)	5888a5d0dbf282090e692b320b2b75f351d3fc68		Voter : 15XLNHiGTE1bdXVdpAtR9Y1DKAVjRWo4P Candidate : 1HFFB4kYyiRBY4QeVofdNN7sm57515JBfp
2	Tue Jun 02 2020 22:18:34 GMT+0100 (GMT+01:00)	ec07775443aae8191b382dfec98249f4fef45f9d	5888a5d0dbf282090e692b320b2b75f351d3fc68	Voter : 1HCkycSSZuptjSpZZkDpsYA9T7tZaQM14J Candidate : 1KvXizLUTvQTiHq7WSUUhSdP2UnjFRJPvM
3	Tue Jun 02 2020 22:22:19 GMT+0100 (GMT+01:00)	29b9408853a5b8f59a968a6aad73af56858f1967	ec07775443aae8191b382dfec98249f4fef45f9d	Voter : 186Wtxtrkr5PECeP8tkXEGx2FcLfQ54JZ4 Candidate : 1KvXizLUTvQTiHq7WSUUhSdP2UnjFRJPvM

Figure 3.25: Blockchain page

3.5.2 VoteChain in test

We have tested VoteChain by creating two candidates and launching the election event. After that, we checked its performance and we got the following results .

Before creating any block, we must check if the transaction is already in the Blockchain or not. So we must check block by block, starting from the last one created, to check the duration of this process. And we got the results in the following figure .

```
MongoDBConnected...
Duration to check all blocks: 277 ms
Duration to check each block: 55.4 ms
```

Figure 3.26: Duration to check the existence of block

As the figure shows, the rate of duration to check one block is 55 ms. This was on a 2.16 GHz processor speed laptop which is a very slow one. However, with the government's great capabilities, it can get much computing power and we can reduce the checking time much more.

3.6 Conclusion

In this chapter, we talked about how we created the web application "votechain". We have seen the building steps, the main function used, and the database tables. Then, we talked about the environment used : the platform and the database. Finally, we represented the result of our work.

VoteChain is the first step in the way of implementing Blockchain in e-voting. It is not a perfect app yet and there's a lot more to do about it. However, VoteChain works exactly as the real Blockchain. It allows the authority to monetize the whole election process and it gives the voters the ability to check that all votes are counted and recorded correctly. Therefore, VoteChain added more transparency and legitimacy on the whole election event.

Chapter 4

Future prospects

4.1 Introduction

E-voting is used worldwide with all its kinds, so in the chapter, we will talk about the use of it across the world. We will take examples of used systems. We will discuss its advantages and disadvantages. Then, we will talk about how e-voting can improve elections. Finally, we will talk about where Algeria is from e-Voting statistics and how e-voting can be used there.

4.2 e-voting around the world

4.2.1 Countries uses e-voting

E-voting has been used around the world for decades. The most common used way of it is voting machines because internet voting is too risky to use. It started in USA since 1960s until today but not all the states. India started using voting machines in 1998. The Philippines and Mongolia started using it in 2010. In 2014, Namibia used it and become the first country that uses voting machines in Africa. On the other hand, Estonia has used the Internet voting all around the country since 2005, but it got cyber-attack in 2007. Estonia improved it instead of stopping it to be one of the strongest systems today [12].

4.2.2 Countries uses e-voting partially

Some countries are not comfortable yet with using e-voting, so they use it carefully. Canada and Iran use voting machines just in local elections. France and Belgium use it with some districts, but France is trying to end its use. In Russia, 10 percent of polling stations were using voting machines in 2018. Argentina also uses voting machines, but it considers voting machines not secure to be used in all the country [12].

4.2.3 Countries put e-voting on test

Governments are studying the use of e-voting in their countries. Bangladesh tried it in the national election in 2018 by using voting machines. Bulgaria planned to use it in 2017 then decided not to because it didn't get the machines on time. Norway used internet voting during 2011 to 2013 then stopped it for security reasons. [12].

4.2.4 Countries are no longer using e-voting

After using or testing e-voting as voting machines or internet voting, some countries decided to stop it and back to the traditional way. Ireland was one of first three countries that decided to drop off the use of e-voting in 2006, followed by Netherlands in 2007 after discovering that it's hackable and not secure. Germany decided to stop it in 2009 because Constitutional Court decided that it's not transparent enough [12].

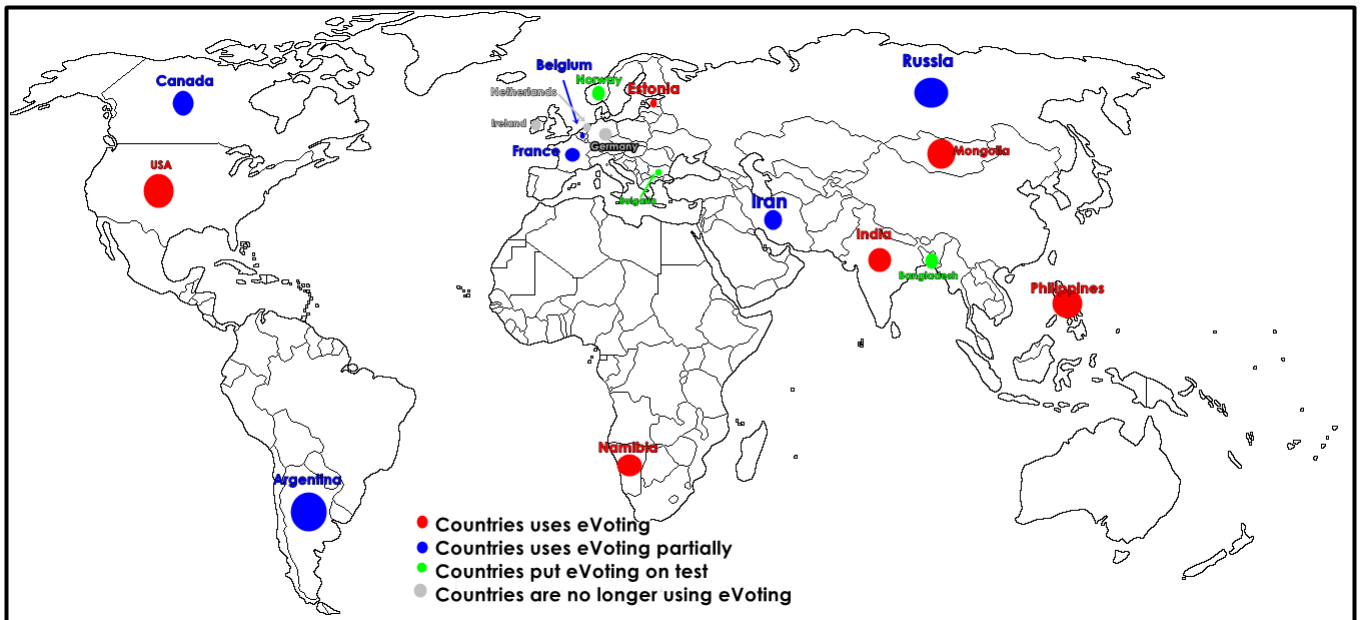


Figure 4.1: E-voting around the world

4.3 Renowned e-voting systems

Apart from voting machines which are considered vulnerable, Internet voting, likewise, is vulnerable too. It may be more vulnerable than voting machines, but the difference is that internet voting can be improved and evolved.

When we talk about internet voting, we must mention Estonian voting system "i-voting". It's an internet voting system started in 2005 and evolved with time after it got hacked in 2007. It

allows voters to cast a vote through any computer with internet connection. All voters have to do is install the voting application, then verify the identity with ID card or mobile ID. After casting the vote, voters can change their votes within a period of time simply by just voting again. Votes then will be encrypted and moved to a central server. Each voter can check if the vote reached the server or not. The key to open the encrypted votes is divided between the members of the national electoral committee, so in order to open the votes, the whole members of the committee have to be together. Such system looks undisputed, but just the idea of centralizing the system makes it vulnerable. If the center server fall somehow, with an earthquake or a lightning or even a terrorist attack, all votes will be gone [13].

Decentralization is the strong point of Blockchain. However, it is the weakness of the systems based on it like VoteChain because results are distributed but the body of the system will be on one central server which means it is still vulnerable. But in case of using a real Blockchain network, all systems will live on a smart contract. And it will be distributed as blocks, so it can't be attacked. Some countries already started working on such systems, for example there is plans to use a Blockchain-based application in USA called "Follow My Vote" in the national elections. Also in USA, there's also another system which is hybrid. It will use the power of Blockchain along with paper ballots that use QR code to make sure that each voter can vote once. The weakness of the Blockchain system is that people don't trust it yet. They are afraid of using it. So before going to Blockchain voting systems, we have to encourage people to use it [11].

4.4 e-voting : pro and conn

There's a big argument whether e-voting is worth or not, it is a big step ahead or backward. To decide if it's good or not, we must first study its benefits and inconvenient.

e-voting is much easier than normal voting. Everyone would like to cast a vote from their home at any time they want rather than going to the polling station. It's also better for people who live outside the country because, in normal voting, their information come often too late, so they won't be able to cast their vote. Another thing is it's more comfortable for younger people who vote less usually, so they would be more likely to use it. By using an e-voting system, we get less invalid votes. Finally, e-voting can reduce the costs of election. Every government has to pay for building the platform and keeping it running, which can be way too less than the cost of a normal election.

On the other hand, there are some reasons that made us think twice before using e-voting. The first reason and most important is security. The security of e-voting is not guaranteed. Second reason is that the result can be manipulated, but the use of Blockchain can solve both problems. Finally, the cost, if we use a normal e-voting system, costs will not be a problem. But if we use

a Blockchain-powered system, the cost can be as much as a normal election because writing data on Blockchain costs cryptocurrency which is too expensive.

After considering both the advantages and disadvantages of using e-voting, in my opinion we should go with e-voting. Although it's more expensive, at least we will guarantee the security of election and transparency of all voting processes.

4.5 Algeria and e-voting

Since independence until now, Algeria has never experienced any kind of electronic voting. It still uses the traditional paper ballot system. So, talking about moving to a new voting system is still too early, but the government should start working on that now, firstly, by supporting developers. So, they can create a hundred percent Algerian voting system by putting a big budget for research. Then, it has to prepare the people for this kind of election by using some trial in local elections, so people will get used to it.

4.6 Conclusion

In this chapter, we've talked about the use of e-voting around the world followed by the most known systems. After that, we compared e-voting with normal voting. Then, we talked about how Algeria can use e-voting in the future.

General conclusion

E-voting is a kind of vote using electronic ways to cast and record votes. It can be done through voting machines or just online vote where you can do it through any internet connected device. E-voting is made to make elections easier and more secure. However, technology keeps evolving, so there're more security concerns. In order to protect the election process, we must use another revolutionary technology that has a great reputation when it comes to security which is Blockchain.

The first successful implementation of Blockchain technology was Bitcoin. After that, the world has found many other useful applications, so why not use it to build an unbreakable E-voting system just by saving all votes in blocks in the Blockchain. The idea is easy but turning it to an actual system is challenging .

VoteChain is my attempt to implement Blockchain in e-voting, it's an online e-voting system that treats each vote as a transaction and records it in a block in its own Blockchain network, the web-application is not connected to the real worldwide Blockchain network, it uses a local network that works as same as the real one.

Building VoteChain was challenging for many reasons like the platform that I used for example, working with node js was very difficult because of its nonblocking nature . Also trying to copy how exactly Blockchain works was never easy.

VoteChain is now on its basic form for now, in the future I'm planning to connect it with the real worldwide Blockchain network using real smart contracts, also I'm planning to add more features to it such as the ability of voter to change the chosen candidate when the voter's not sure yet, or to start more than one vote at once.

Bibliography

- [1] Areas of use of Blockchain technology. <https://www.brightnode.io/en/blog/areas-of-use-of-blockchain-technology/>.
- [2] Blockchain Demo. <https://andersbrownworth.com/blockchain/blockchain>.
- [3] Express - Node.js web application framework. <https://expressjs.com/>.
- [4] Private, Public, and Consortium Blockchains - What's the Difference? <https://www.binance.vision/blockchain/private-public-and-consortium-blockchains-whats-the-difference/>.
- [5] StrongLoop - What Makes Node.js Faster Than Java? strongloop.com/strongblog/node-js-is-faster-than-java.
- [6] Summary of the problem with electronic voting. https://www.verifiedvoting.org/downloads/revised_summary31.pdf. accessed February 7, 2020.
- [7] What Are Public Keys and Private Keys? <https://www.ledger.com/academy/blockchain/what-are-public-keys-and-private-keys/>.
- [8] What is blockchain technology? <http://support.blockchain.com/hc/en-us/articles/211160223-What-is-blockchain-technology-/>.
- [9] What is Blockchain Technology? A Step-by-Step Guide For Beginners. <https://blockgeeks.com/guides/what-is-blockchain-technology/>.
- [10] What Is Hashing? [Step-by-Step Guide-Under Hood Of Blockchain]. <https://blockgeeks.com/guides/what-is-hashing/>.
- [11] Blockchain E-Voting is Real: Where, How, When? <https://irishtechnews.ie/blockchain-e-voting-is-real-where-how-when/>, July 2019.
- [12] E-voting: Which countries use it, where has it failed and why? <https://www.fin24.com/Economy/e-voting-which-countries-use-it-where-has-it-failed-and-why-20190510>, May 2019.

- [13] What's so special about online voting? <https://e-estonia.com/whats-so-special-about-online-voting/>, May 2019.
- [14] apleasant. Common Electronic Voting and Counting Technologies. <https://www.ndi.org/e-voting-guide/common-electronic-voting-and-counting-technologies>, November 2013.
- [15] Elections Canada. A Comparative Assessment of Electronic Voting. <https://www.elections.ca/content.aspx?section=res&dir=rec/tech/ivote/comp&document=benefit&lang=e>.
- [16] Kevin Curran. E-Voting on the Blockchain. *The Journal of the British Blockchain Association*, 1(2):1–6, December 2018.
- [17] Alka Dhingra. How Blockchain Wallet Can Secure Online Payments? <https://www.valuecoders.com/blog/technology-and-apps/how-blockchain-wallet-development-can-secure-online-payments/>, June 2018.
- [18] Rupali Dhongade. Blockchain Technology Basics. <https://www.spheregen.com/blockchain-technology-basics/>, April 2019.
- [19] Paul Dughi. A simple explanation of how blockchain works. <https://medium.com/the-mission/a-simple-explanation-on-how-blockchain-works-e52f75da6e9a/>, March 2018.
- [20] Jake Frankenfield. Nonce Definition. <https://www.investopedia.com/terms/n/nonce.asp/>.
- [21] Jake Frankenfield. Target Hash. <https://www.investopedia.com/terms/t/target-hash.asp/>.
- [22] Tiana Laurence. The structure of blockchains. <https://www.dummies.com/personal-finance/the-structure-of-blockchains/>. accessed February 7, 2020.
- [23] M. Niranjanamurthy, B. N. Nithya, and S. Jagannatha. Analysis of Blockchain technology: pros, cons and SWOT. *Cluster Comput*, 22(S6):14743–14757, November 2019.
- [24] Node.js. Node js. <https://nodejs.org/en/about/>.
- [25] Aashis Rimal. Developing a Web Application on NodeJS and MongoDB using ES6 and Beyond. page 46.
- [26] Andrew Tar. Proof-of-Work, Explained. <https://cointelegraph.com/explained/proof-of-work-explained/>, January 2018.