DEMOCRATIC AND POPULAR REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

UNIVERSITY OF MOHAMMED SEDDIK BENYAHIA JIJEL
FACULTY OF EXACT AND COMPUTER SCIENCES
COMPUTER SCIENCE DEPARTMENT

Master's thesis
Presented to obtain the Master's diploma

Option: *Computer forensics and multimedia*

Theme

BlockTree based voting system

Presented by :

MOUSSAOUI Redouane

Supervised by:

ZENNIR Med Nadjib

To my dear parents

Acknowledgements

I would like to thank first of all God who gave me the strength, the will and and courage to accomplish this modest work.

I would like to thank Mr. Zennir Med Nadjib in particular for the trust he placed in me by agreeing to direct this master's thesis. It is thanks to his help and his precious advice that this work could see the light of day. I will always be grateful to you.

My thanks also go to the members of the jury for having accepted to judge and examine this work,

And finally, thank you to all those who have contributed to the realization of this thesis.

Abstract

The integrity of traditional voting systems has always been questionable and most of the voting methods in place are unreliable, vulnerable and slow to count the results. In this work, we propose a solution to this problem with the BlockTree, a variant of the Blockchain, which is a distributed ledger technology, to build a platform for voters accessible to everyone everywhere. BlockTree offers multiple advatages over Blockchain, like increased speed and throughput. This platform is secure and unaltered by nature, every vote is counted correctly, and no fraud can be possible. This system solves the problem of lack of trust and transparency.

Keywords : *Voting, Elections, Blockchain, BlockTree, Ledger.*

Résumé

L'intégrité des systèmes de vote traditionnels a toujours été remise en question et la plupart des méthodes de vote en place sont peu fiables, vulnérables et lentes à comptabiliser les résultats. Dans ce travail, nous proposons une solution à ce problème avec la BlockTree, une variante de la Blockchain, qui est une technologie de registre distribué, pour construire une plateforme pour les électeurs accessible à tous et partout. La BlockTree offre de multiples avantages par rapport à Blockchain, comme une vitesse et un débit accrus. Cette plateforme est sécurisée et inaltérable par nature, chaque vote est compté correctement, et aucune fraude n'est possible. Ce système résout le problème du manque de confiance et de transparence.

***Mots-clés**: Vote, Elections, Blockchain, BlockTree.*

CONTENTS

LIST OF FIGURES

GENERAL INTRODUCTION

Introduction

In contrast to the conventional web, which is built on centralized servers, blockchain is essentially a decentralized database that also doubles as a decentralized network in which all nodes and devices can connect with one another directly. We have chosen to build our voting application on a Blockchain due to these two key benefits. Thus, we can guarantee the impartiality of any central body that may have an impact on the outcome of an electronic vote, as well as the openness, security, and, most importantly, the immutability of the outcome.

Issue

Traditional elections necessitate substantial material, human, and financial resources (offices in each town hall, thousands of volunteers to sort the votes, hundreds of controllers, paperwork, and vote centralization), as well as a significant amount of time. Not to mention that neither the traceability nor the integrity of the vote calculations are guaranteed, because this process involves intermediate authorities who can alter the calculations and the result.
Traditional web-based electronic elections reduce voting procedures but do not ensure data transparency and integrity. Because the entire process is centralized in a server managed by a third party, the data can be easily altered without anyone knowing.
Despite the web 2.0 technology that has reduced procedures, time, human and financial resources, the problem of data integrity and transparency of results is not guaranteed.In any voting system, no matter how simple or complicated it is, the following principles are expected to be upheld [30]:

- **Universality**: All eligible voters have the right and ability to cast their votes using that system
- **Equality**: Each eligible voter has the same number of votes, usually one ballot each
- **Freedom** of choice: Each voter has the right to cast his votes in a free manner without threats or undue influence

- **Anonymity**: Each voter has the right to cast his vote secretly, and no one should be able to relate a voter to his vote
- **Security**: No one should be able to change or remove the voter's ballot, or add votes not cast by legitimate voters
- **Directness**: Votes should be recorded as intended by the voter, and the results of the poll shall be determined by the votes cast by the voters
- **Trust**: The eligible voters must trust the system and believe that these principles were met

Goal

In traditional voting schemes the integrity has always been questionable, but Blockchain has emerged as reliable and robust technology in contrast to traditional server oriented Architectures. The security and immutability of Blockchain allows us to keep track of every account that sent a transaction during the vote. Each vote goes to the chosen candidate without possibility of corruption. Every transaction is permanently and immutably recorded on all nodes of the Blockchain network. To increase throughput, instead of using a conventional blockchain, we opted for a BlockTtree, our system must be able to:

- Define the period of each phase (registration, voting, final result).
- Define the controls and data verification during registration.
- Encrypt every vote with a shared Master key until the end.
- Limit the number of registrations to 1 for each user.
- Limit the number of votes to 1 for each voter.
- Calculate the votes at the end of the voting period.
- Deliberate the final result.

This thesis is structured in four chapters. In what follows, we detail the contents of the different chapters. Chapter 1 presents the social choice theory and the different electoral systems in place. Chapter 2 presents the Blockchain technology. In chapter 3, we describe our proposed voting system. Chapter 4 is dedicated to the implementation of the system, source code and GUI captures.

CHAPTER 1

SOCIAL CHOICE THEORY

1 History & Definition

The study of collective decision-making processes and procedures is known as social choice theory[29]. Its main focus is on how to translate the preferences of individuals (such as votes, preferences, judgments, and welfare) into the preferences of a group (e.g., collective decisions, preferences, judgments, welfare) .Its goal is to provide answers to some questions, such as :

- How can a group of individuals choose a winning outcome (e.g., policy, electoral candidate) from a given set of options?
- What are the properties of different voting systems?
- When is a voting system democratic?
- How can a collective (e.g., electorate, legislature, collegial court, expert panel, or committee) arrive at coherent collective preferences or judgments on some issues, on the basis of its members' individual preferences or judgments?
- How can we rank different social alternatives in an order of social welfare?

Social-choice theory explains how a certain way of choosing a legislature affects the stability of a parliamentary administration and the number of parties with realistic possibilities of winning seats (Duverger's law). However, the relevance of a stable administration (and the desired level of stability), as well as the desirability of a small or large number of such parties is a purely political one [17].

Nicolas de Condorcet and Jean-Charles de Borda pioneered social choice theory in the 18th century, and Charles Dodgson in the 19th century. But it only took off in the 20th century with the works of Kenneth Arrow, Amartya Sen and Duncan Black[29].Social choice theory has an impact on economics, political science, philosophy, mathematics, and, more recently, computer science and biology. Aside from improving our knowledge of collective decision procedures, social choice theory has implications in institutional design, welfare economics, and social epistemology.

Condorcet proposed in his Essay on the Application of Analysis to the Probability of Majority Decisions (1785), a specific voting method, pairwise majority voting, and highlighted his two most important insights.
The first, known as Condorcet's jury theorem, states that if each member of a jury has an equal and independent chance of being correct on whether a defendant is guilty (or on some other factual proposition), The majority of jurors is more likely to be accurate than each individual juror, and as jury number grows, the chance of a correct majority ruling approaches one. Thus, under certain conditions, majority rule is good at 'tracking the truth' (e.g., Grofman, Owen, and Feld 1983; List and Goodin 2001).[29]

Condorcet's second insight, frequently referred to as the Condorcet paradox, is that majority preferences can be 'irrational' (specifically, intransitive) even when individual preferences are 'rational' (specifically, transitive). Assume that one-third of a group chooses alternative x to y to z, another third prefers y to z to x, and the other third prefers z to x to y. Then there are two-thirds majorities for x against y, y against z, and z against x: a 'cycle' that defies transitivity. Furthermore, no alternative is a Condorcet winner, that is, an alternative that beats or ties every other alternative in pairwise majority contests. Condorcet foresaw a crucial feature in modern social choice theory: majority rule is both a viable form of collective decision-making and a source of unexpected challenges. One of the central goals of social choice theory is resolving or avoiding these issues. [29]

Election results can change depending on how elections are conducted, as demonstrated by Kenneth Arrow (1950). Furthermore, when there are more than two voters and three candidates for a single position, it is impossible [15] to design a voting system that meets all five of the rationality and fairness criteria he proposes:

- The vote must assign all candidates the same rank no matter how votes are counted.
- Each vote should have equal weight.
- Every [serious] candidate should have a chance to win.
- A voter should not be able to hurt one candidate by promoting another.
- If every voter prefers a certain candidate, so must the result.

As a result, there is no single perfect system for conducting a fair vote.This helps to explain why multiple major stems and variants have emerged, each with its own set of strengths and weaknesses. (Brams 1982, Nurmi 1987; Saul and Johnson 2017).

2 Computational social choice

Since the 1980s, the field of social choice has been invested in computer science (especially theoretical computer science, artificial intelligence and operations research) with the aim of using computational concepts and algorithmic techniques to solve complex collective decision problems. [13]

The first works focused on computational social choice were initiated by Bartholdi III et al (1989) and by Hudry (1989) [13]. They use algorithmic techniques to better analyze

the mechanisms of social choice, in particular the voting rules that can serve as a barrier against the strategic manipulation of an election.

Some domains of artificial intelligence such as learning, reasoning under uncertainty or knowledge representation, have been applied to social choice with the same goal [8]. The applications are varied and concern voting as well as the fair sharing of resources (aggregation procedures for the classification of web pages) or consensus building (judgment aggregation).

Today, research in computational social choice has two main thrusts. First, researchers seek to apply computational paradigms and techniques to provide a better analysis of social choice mechanisms, and to construct new ones. Leveraging the theory of computer science, we see applications of computational complexity theory and approximation algorithms to social choice. Subfields of artificial intelligence, such as machine learning, reasoning with uncertainty, knowledge representation, search, and constraint reasoning, have also been applied to the same end.
Second, researchers are studying the application of social choice theory to computational environments. For example, it has been suggested that social choice theory can provide tools for making joint decisions in multiagent systems populated by heterogeneous, possibly selfish, software agents. Moreover, it is finding applications in group recommendation systems, information retrieval, and crowdsourcing. Although it is difficult to change a political voting system, such low-stake environments allow the designer to freely switch between choice mechanisms, and therefore they provide an ideal test bed for ideas coming from social choice theory.[13]

3 Elections

The election is the designation, by the vote of voters, of representatives (a person, a group, a political party) intended to represent them or to occupy a function on their behalf.
The population concerned transfers by the vote of its majority to the chosen representatives or principals, the legitimacy required to exercise the attributed power (a function supposedly defined and oriented by means of a political program).
There are several stages or phases involved in the implementation of a single election. in modern democracies, the electoral process comprises of the following phases:

3.1 Pre-election Phase

This is, unsurprisingly, a period of intense preparation. Unfortunately, despite the numerous "lessons learned" from previous elections that underline its importance, this is frequently the period that is most overlooked. [31] These are the key steps in this phase :

- Establishing an election management body to organize the elections .
- Elaborating a legal framework to trace the rules that define the regulations and major parameters of the electoral boundaries and electoral lists.
- Determining who is competent to vote and how much weight should be given to each voter. One most common rule is : one person = one vote.

- Determining the electoral system to be used.
- Voters registration and the preparation of the voters' lists that will be used in the polling stations on election day.
- Candidates registration for citizens that meet the requirements for becoming a candidate
- Civic and Electoral Education Campaign to increase awareness about the electoral process.

3.2 Election phase

The electoral phase is the period during which the election takes place where citizens exercise their right to vote . There are a multitude of elements that could impact the vote as it goes, of course. Voter turnout is a crucial topic, as high or low turnouts are thought to favor one party or the other. It's not uncommon for reporting turnout to be restricted in some way.

3.3 Post-election phase

This phase includes the centralization of the results and the validation of the collected data. Then, the count period can last anywhere from a few hours to several days or even weeks, depending on the circumstances and processes of an election. The announcement of the results by the election management body marks the end of the electoral process.

4 Electoral systems

A country's electoral system is its sets of laws, regulations, procedures and modalities that govern the elections of its head of state and representatives to its legislature, local or traditional councils. Electoral systems are the detailed constitutional arrangements and voting systems that convert the vote into a political decision[33]

Most systems can be categorized as either proportional, majoritarian or mixed. Among the proportional systems, the most commonly used are party-list proportional representation (list PR) systems, among majoritarian are First Past the Post electoral systems (plurality, also known as relative majority) and absolute majority. Mixed systems combine elements of both proportional and majoritarian methods, with some typically producing results closer to the former (mixed-member proportional) or the other (e.g. parallel voting). Many countries have growing electoral reform movements, which advocate systems such as approval voting, single transferable vote, instant runoff voting or a Condorcet method.

Some electoral systems elect a single winner to a unique position, such as prime minister, president or governor, while others elect multiple winners, such as members of parliament or boards of directors. When electing a legislature, voters may be divided into constituencies with one or more representatives, and may vote directly for individual candidates or for a list of candidates put forward by a political party or alliance.

One of the most critical areas of the democratic electoral process is the choice of an electoral system for a country. It is even more challenging in a country's transition from colonial rule to nationhood, from a one-party system to a pluralistic democratic system, from a military dictatorship to constitutional rule and from an apartheid system to a multiracial participatory democracy.[33]

4.1 Type of elections

4.1.1 Plurality systems

Plurality voting is a method in which the candidate(s) with the most votes wins, regardless of whether they receive a majority of votes or not. In cases where there is a single position to be filled, it is known as first-past-the-post; this is the second most common electoral system for national legislatures, with 58 countries using it to elect their legislatures, the vast majority of which are current or former British or American colonies or territories. It is also the second most common system used for presidential elections, being used in 19 countries.[45]

4.1.2 Majoritarian systems

Majoritarian voting is a voting system in which candidates must earn a majority of votes in order to be elected, either in a runoff election or in the final round. (although in some cases only a plurality is required in the last round of voting if no candidate can achieve a majority).There are two primary types of majoritarian systems: one that uses ranked voting in a single election and the other that uses numerous elections to reduce the field of candidates. Both are commonly used in single-member districts.

The other main form of majoritarian system is the two-round system, which is the most common system used for presidential elections around the world, being used in 88 countries. It is also used in 20 countries for electing the legislature. [45] If no candidate achieves a majority of votes in the first round of voting, a second round is held to determine the winner. In most cases the second round is limited to the top two candidates from the first round, although in some elections more than two candidates may choose to contest the second round; in these cases the second round is decided by plurality voting.

4.1.3 Proportional systems

The most widely used electoral system for national legislatures is Proportional representation , with over eighty countries' parliaments elected using various forms of the system.

Party-list proportional representation is the most widely used election system, with 80 nations using it. It involves people voting for a list of candidates nominated by a party. Voters in closed list systems have no control over the candidates put forth by the party, but voters in open list systems can vote for the party list as well as affect the order in which candidates are assigned seats. In some countries,like the Netherlands, elections are carried out using 'pure' proportional representation, with the votes tallied on a national level before assigning seats to parties. However, in most cases several multi-member constituencies are used rather than a single nationwide constituency, giving an element of geographical representation; but this can result in the distribution of seats not reflecting

the national vote totals. As a result, some countries have leveling seats to award to parties whose seat totals are lower than their proportion of the national vote.

4.1.4 Mixed systems

Mixed systems are used to elect legislators in a number of countries. These include parallel voting (also known as mixed-member majoritarian) and mixed-member proportional representation.

In non-compensatory, parallel voting systems, which are used in 20 countries [45], members of a legislature are elected in two ways: one by plurality or majority vote in single-member constituencies, and the other by proportional representation. The results of the constituency vote have no effect on the outcome of the proportional vote.

In compensatory mixed-member representation the results of the proportional vote are adjusted to balance the seats won in the constituency vote. In mixed-member proportional systems, in use in eight countries, there is enough compensation in order to ensure that parties have a number of seats proportional to their vote share.[45]

Mixed single vote systems are also compensatory, however they usually use a vote transfer mechanism unlike the seat linkage (top-up) method of MMP and may or may not be able to achieve proportional representation. An unusual form of mixed-member compensatory representation using negative vote transfer, Scorporo, was used in Italy from 1993 until 2006.

4.1.5 Condorcet method

The Condorcet method (also called Condorcet ballot or Condorcet vote) is a system of voting that obeys Condorcet's principle, which states: "If one choice is preferred to any other by a majority or another, then that choice must be elected." The winner, if there is one, is the candidate who, compared to each of the other candidates in turn, proves to be the preferred candidate each time. In other words, he or she beats all the others in a duel. Such a candidate is called the Condorcet winner.

Nothing guarantees the presence of a candidate satisfying this criterion of victory: this is the Condorcet paradox. Thus, any voting system based on the Condorcet method must provide a way to solve the votes for which this ideal candidate does not exist.

Randomized Condorcet voting is one way to solve the paradox. It is a Condorcet method, which means that it elects the Condorcet winners, when they exist. Otherwise, this voting system solves Condorcet's paradox by choosing the elected person according to a probability law among a subset of leading candidates.

This system has several interesting properties from the point of view of social choice theory in general [27] and in particular with respect to the question of strategic voting by voters [22], which make it a particularly robust method to strategic voting and a majority voting method in that it designates the Condorcet winner when there is one. The simplest case of the paradox is the following. Among the set of candidates, there exists a trio A, B, and C such that A is preferred to B, B is preferred to C, and C is preferred to A, and this trio is preferred to all other candidates. In this case, the randomized Condorcet vote [34] will choose the winner at random among A B and C with the same probabilities: (1 / 3 , 1 / 3 , 1 / 3).

5 Voting

5.1 Definition

Voting is the act of declaring a choice among a number of alternative options in the process of reaching a group decision on a particular matter. In politics, this mostly concerns the selection of a person for a specific position, such as a mayor or a member of parliament. The right to vote in elections is widely considered the most fundamental political right of citizens. In any country, democratic voting is the most important event that allows its citizens to exercise their power by electing their representatives. To protect this right of the citizens, conducting fair elections is the basic prerequisite for any country.

In smaller organizations, voting can occur in different ways. Formally via ballot to elect others for example within a workplace, to elect members of political associations or to choose roles for others. Informally voting could occur as a spoken agreement or as a verbal gesture like a raised hand or electronically.

5.2 Voting methods

5.2.1 Paper-based method

The most common voting method uses paper ballots on which voters mark their preferences. This may involve marking their support for a candidate or party listed on the ballot, or a write-in, where they write out the name of their preferred candidate if it is not listed.

The main advantage of paper ballot [5] is the transparency of the elections. All processes of handling and counting ballots are completely open to public scrutiny in transparent elections. Nothing is hidden, with the exception of individual voting choices, which cannot be revealed in order to ensure the voter's safety when voting against a malevolent candidate and to prevent voters from selling their votes.

Another advantage of the Paper ballot is the simplicity. For example, elderly voters are more likely to successfully cast their votes using a paper ballot instead of advanced touch screen systems [10].

Even when utilizing simple paper ballots, such as those used in the Minnesota Senate race in 2008, calculating votes correctly can be difficult [5]. Paper ballots were used by 2,920,214 voters; unlike the presidential election, in which Democrat Barack Obama defeated Republican John McCain by nearly ten percentage points, the Senate race was decided by a razor-thin margin of less than 0.0075 percent. Senator Norm Coleman, a Republican who has served in the Senate since 2002, defeated Democrat Al Franklin by 215 votes in the first round of voting. [47].

Due to the close margin, an automatic recount was triggered. Many people were concerned about the high number of challenged ballots. Both campaigns disputed more than 6,500 ballots. When the margin of victory is less than 0.0075 percent, each ballot is important and must be counted. Unfortunately, the canvassing board was unsure about the voter's purpose in more than 6,000 situations.

Some of the actual challenged ballots are displayed below (Figure 1.1, Figure 1.2, Figure 1.3) [47].

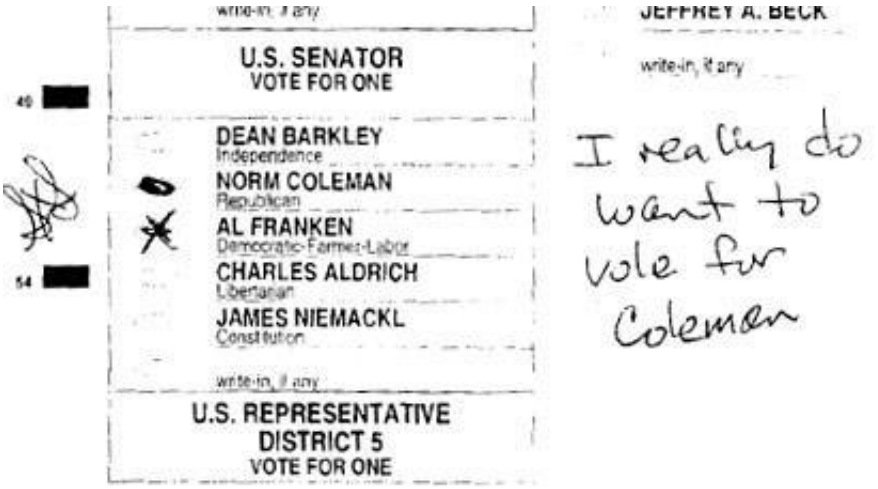

Figure 1.1: Both campaigns challenged this Hennepin County ballot with the Coleman camp saying the voter's intent is clear and the Franken camp saying what appear to be initials constitute an identifying mark on the ballot [47].

Figure 1.2: The ballot was challenged and considered Overvote [47].

On June 30, 2009, the state's Supreme Court declared Franken the winner by 312 votes, giving the Democrats the majority in the senate, putting an end to a recounting process that lasted almost eight months. The huge number of challenged ballots points out one of the shortcomings of the Paper Ballot system. The use of paper ballots allows voters to overvote and mark or sign their ballots. The use of e-voting could have minimized or even eliminated the challenged ballots; as a result, the recounting process would have been accomplished faster.

5.2.2 Postal voting

Postal voting works in the same way as statewide absentee voting does. Registered voters receive ballots in the mail, which they fill out at their own convenience and either mail back or drop them off at authorized locations. Punch cards or optical scan ballots are used for these ballots. An identification number ensures that a person votes only once, while maintaining the secrecy of the vote.

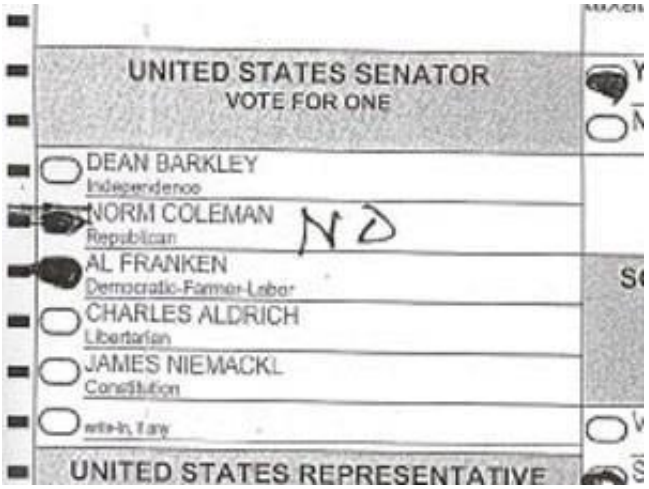

Figure 1.3: This ballot was challenged in Dakota County because two ovals were filled in. Minnesota law says a ballot is valid if election officials can determine the voter's intent [47].

The counting of the ballot envelopes then takes place in two stages: the opening of the envelope containing the voter's identification card by the municipal administration, and then at the close of the ballot, the opening of the closed envelopes containing the ballots by the electoral office.

In an election, postal votes may be available on demand or limited to individuals meeting certain criteria [5], such as a proven inability to travel to a designated polling place. Most electors are required to apply for a postal vote, although some may receive one by default.

Postal voting also allows for early voting by voters who can cast their ballots one or more days before the date set for the election. The procedure can be conducted by mail or physically at special polling places. The purpose of postal and early voting is to increase participation by allowing people who are prevented from voting by personal circumstances to vote, and to reduce crowds on election day. Special reasons for inability to vote may be required (participation in the organization of the election, professional or medical reasons).

Absentee voting can also be used to commit electoral fraud, for example by stealing envelopes from mailboxes or by concealing the use of ghost voters.

5.2.3 Machine voting

Citing all the negative reviews from ballot paper, many countries upgraded their voting mechanism with advancement in embedded technology with machines called Electronic Voting Machines (EVM).

EVMs are electronic devices that are only programmed once during production. The software is written into the chip, and it cannot be reprogrammed. EVMs are made up of two parts. There is a control unit where the voter is given the option of voting for any of the candidates. There is a button that corresponds to the candidate's name. Another embedded device, the Electronic Balloting Unit, is connected to this device by a 5-meter wire and collects all of the electronic votes.

EVMs do not require an external power supply because they are powered by a battery. They're light, portable, and simple to set up in any situation. Then, when a voter presses any button corresponding to the candidate for whom he wishes to vote, the machine will light an LED light corresponding to the choice, allowing the voter to be confident that the vote was correctly recorded. As a result, the machine locks itself. It can now only be unlocked by a new ballot number, which the person in charge will enter again when a new voter votes. This will prevent multiple votes from the same person.
It's small, portable, and runs on a 6 volt battery. So, it can be taken to a location where there is no electricity.

The votes are stored electronically, reducing paper waste and speeding up the counting process.
The most criminal thing that can happen in a ballot paper is that the entire ballot box is captured. Those votes are wasted anyway. This is a simple problem to solve. In the case of EVMs, however, if anyone gains access to the device, he can manipulate it by replacing the chip and commit a more sophisticated crime that may not even be detected.
Because the votes are electronically stored, if the balloting machine fails, all of the votes may be lost. The embedded device memory can be corrupted in a variety of ways.

5.2.4 Online voting

Online voting is a specific case of remote electronic voting, whereby the vote takes place over the Internet such as via a web site or mobile application. It has a few advantages :

- Increase elections' activity by facilitating the casting of votes by voters;
- Reduce elections' and referendums' expenses;
- Accelerate vote counting and the delivery of voting results;
- Enable voters to cast their votes from different places, not from only a particular polling station.

But does not come without some downsides :

- malicious software, firmware, or hardware that can change, fabricate, or delete votes, deceive the user in myriad ways including modifying the ballot presentation, leaking information about votes to enable voter coercion, preventing or discouraging voting
- denial of service attacks from networks of compromised computers (called "bot-nets"), causing messages to be misrouted, and many other kinds of attacks
- undetected changes to votes not only by outsiders, but also by insiders such as equipment manufacturers, technicians, system administrators, and election officials who have legitimate access to election software and data;

6 Online voting

In this section, we will take a deeper look at the feasibility of electronic voting. Any discussion of Internet voting inevitably returns to one topic: security. All of the main

reports on Internet voting have praised its virtues. But according to these reports, regardless of how advantageous the Internet may be as a voting method, the potential costs—specifically, the security risks—outweigh the benefits. The chance of the system being hacked, targeted by terrorists or rogue states, infected with computer viruses, or hijacked by political groups intent on committing vote fraud is viewed as a hurdle that is now too difficult to overcome.[3]

We do not deny that there are risks associated with using the Internet for voting. Any system that is as complex as the Internet, operating with as many different component parts—including different hardware, software, and interfaces—is going to face the possibility of failure. However, no voting system is foolproof, including current voter registration, poll site voting, and absentee voting systems. Elections today are fraught with risks: voting machines that fail to work, ballots that are cast but not counted, polls that never open or open late, long lines, tabulation systems that have been tampered with or that simply have been programmed incorrectly, and allegations of vote fraud. Given that current voting systems are not foolproof, there is no reason to think that Internet voting will be completely foolproof either.[3] In most ways, the risks associated with Internet voting are not much different from the risks associated with voting in other domains.
Garfinkel and Spafford, [20], argue that Internet security is a three-fold problem:

- securing central web servers and the data that reside on them.
- securing information as it travels between web servers and users.
- securing the user's computer.

Any Internet transaction, from buying goods to voting, gives a high potential for tampering. A person with unauthorized access to a central web server can record and alter key information about a transaction; the person could also access information in transit between the user and the server.Furthermore, before a transaction, malware might be installed on a computer to monitor or change data being communicated in either direction. As a result, any significant Internet transaction necessitates rigorous scrutiny of security.

Given the huge stakes associated with commercial transactions on the Internet, a great deal of progress has been made in trying to mitigate the risks. The use of high-level encryption, with software firewalls on both user and web servers that monitor and block unauthorized access, makes it virtually impossible for information to be captured or altered in transit, and hardware firewalls and strong physical security systems make it difficult to gain unauthorized access, electronic or physical, to central web servers.

The important point to make here is that maintaining the security of an Internet voting system is quite similar and perhaps identical to maintaining the security of any other voting system. Anyone who has witnessed good polling place operations on election day understands how much time, effort, and resources are committed by local election officials to guaranteeing the security of ballots and voting equipment. .[20]

One reason that computer security is such an important issue is popular perception. Many people have experienced computer failure. Their computer has crashed while they were working on something important, or it contracted a virus that rendered something they were working on useless. They have been kicked off a website or off the Internet

entirely by their Internet service provider. They have read about people attacking the Department of Defense website and Microsoft's corporate network and about hackers stealing credit card numbers from online companies. They have, of course, also heard of widespread virus attacks like the Code Red worm. If the website of a cybersecurity company is not secure, what is?[3]

Every system faces threats that have to be minimized, and the threats to Internet voting are not so great that they cannot be surmounted. Our goal is to create an Internet voting system that is at least as effective as traditional voting systems, especially in regard to their accessibility and security. However, there are in fact reasons to think that Internet voting will be better. One key component in achieving it is Blockchain technology.

CHAPTER 2

BLOCKCHAINS & BLOCKTREES

1 Introduction

There are three architectural approaches for a system to follow [6] : Centralized, decentralized and distributed.
Centralized systems share information in a network and rely on a single entity which handles all major data processing[14]. This entity fully controls the network. This conventional client-server system is the most commonly used type of system in many organizations. The majority of online service providers, including Google, Amazon, eBay, and Apple's App Store, use this conventional model to deliver services.[9]
Even though such systems are simple,consistent and cost-effective for small businesses,they nonetheless are vulnerable , the requirement for a central node and the potential for the system to collapse always exists as central node failure causes the entire system to fail. Not to mention the limited scalability the more the system grows[14].

Decentralized systems can be split into two or more nodes working and sharing workloads with each other without being dependent on a single entity. As a result, the whole network can continue to function without disruption even if one node fails or is compromised, because the others can continue to function properly. Although this kind of system has excellent flexibility, scalability, and performance, it comes at a greater maintenance cost and occasionally has coordination issues amongst its nodes.[14]

In a distributed system, data and computation are distributed across multiple nodes. [9], These nodes are independent computers located at various locations that collaborate and communicate with one another to appear to the end-user as a single entity. By offering several nodes to its users while hiding their specifics, the distributed system strives to make resources accessible to all nodes while achieving transparency. Distributed systems have many benefits like scalability , speed, fault tolerance and enhanced transparency. But there are some drawbacks, one challenge is security, especially in public networks, where an intruder can attack to leak any confidential information. Another one is coordination between nodes, as the data is being transferred between nodes simultaneously, which can overburden the system and also can be the reason for data loss in a network without any coordination [46].

2 Blockchain overview

Blockchains are distributed, tamper-resistant digital ledgers that operate without a centralized authority. They allow users to record transactions in a shared ledger in a way that once they are published, no transaction can be modified. Every network user has access to the history of all transactions .[48] .

A block is the fundamental building element of a blockchain. It contains some or all of the transactions that take place over a time period [43]. Every transaction ever performed is stored on the blockchain. It is impossible to alter, remove, or tamper with a transaction after it has been added to the blockchain. This is one of the critical aspects of blockchain technology. Blockchain confirmation is required for transactions to be effectively led. These confirmations are carried out by consensus mechanisms.[9]

Because it enables transactions to be made without a central entity, Blockchain-based applications are developing rapidly across a wide range of industries, including financial services such as digital assets and online payments [38] [18], smart contracts [24], public services [2], Internet of Things [49] , reputation management [42], and security services [37].

These industries benefit from blockchain in a variety of ways. To begin with, blockchain is unchangeable. Once a transaction is stored in the blockchain, it cannot be altered. Blockchain can be used to attract customers for businesses that require high reliability and honesty.

Furthermore, because blockchain is distributed, it can avoid the single point of failure situation. Smart contracts, on the other hand, could be executed automatically by miners once they are deployed on the blockchain. [50]

3 Background and history

In the late 1980s and early 1990s, the fundamental concepts of blockchain technology first surfaced. Leslie Lamport created the Paxos protocol in 1989 [28] as a consensus model for determining a result in a computer network when the computers or network itself may not be dependable. Instead of a digital currency system, Haber and Stornetta [21] suggested a technique for securely timestamping digital documents.The purpose of timestamping is to provide an approximation of the creation date of a document. A more significant benefit of timestamping is that it precisely reflects the order in which every document was created; if one was created before the other, the timestamps will reflect that. The security property demands that the timestamp on a document cannot be altered after the fact.There is a timestamping service in Haber and Stornetta's scheme to which clients send documents to timestamp. When the server receives a document, it signs it along with the current time and a link or pointer to the previous document. Instead of a location, this pointer refers to a piece of data. That is, if the data in question changes, the pointer becomes invalid. [36]

These concepts were combined and applied to electronic cash in 2008 and described in the paper, Bitcoin: A Peer to Peer Electronic Cash System [35], which was published pseudonymously by Satoshi Nakamoto. The Bitcoin network was launched in 2009, [50] the first of many modern cryptocurrencies. Nakamoto's paper contained the blueprint

that most modern cryptocurrency schemes follow. Bitcoin was just the first of many blockchain applications. [48]

The blockchain in Bitcoin made it possible for users to utilize pseudonyms, users are thus anonymous, but account identities are not. In addition, all transactions are open to the public. Because accounts can be formed without any identifying or authorization steps, Bitcoin can effectively provide pseudo-anonymity.

Due to this pseudonymity, it is essential to have mechanisms to create trust in an environment where users could not be easily identified. Prior to the use of blockchain technology, this trust was typically delivered through intermediaries trusted by both parties.

Without trusted intermediaries, four key characteristics of blockchain technology enable the required trust within a blockchain network [48]:

- **Ledger** : To provide complete transaction history, the technology employs an append-only ledger. In contrast to traditional databases, transactions and values in a blockchain cannot be changed.
- **Secure** : Because blockchains are cryptographically secure, they guarantee that the data on the ledger hasn't been altered and that it is verifiable.
- **Shared** : the ledger is shared amongst every participants.As a result, the blockchain network's node participants are transparent to one another.
- **Distributed** : Blockchain technology is distributed. This makes it possible to scale the number of nodes in a blockchain network, increasing its resistance to attacks from malicious parties. A malicious actor's capacity to influence the blockchain's consensus protocol is diminished by increasing the number of nodes.

Several attempts were made in the 1990s to develop a digital form of currency : [9]

- **Digicash** (David Chaum, 1989)4
- **Mondex** (National Westminster bank, 1993)
- **Cybercash** (Lynch, Melton, Crocker & Winston, 1994)
- **E-gold** (Gold and Silver reserve, 1996)
- **Hashcash** (Adam Black, 1997)
- **Bit Gold** (Nick Szabo, 1998)
- **B-Money** (Wei Dai, 1998)
- **Lucre** (Ben Laurie, 1999)

Even if not directly, the aforementioned technologies helped Bitcoin develop in some way and their work is relevant to the issue that Bitcoin addressed. The problem of preventing double spending in a completely trustless or permissionless environment remained unsolved despite the success of all prior attempts to create anonymous and decentralized digital currency. The Bitcoin blockchain, which introduced the Bitcoin cryptocurrency, finally delivered a solution to this issue. [9]

4 Technical definition

Blockchain is a peer-to-peer distributed ledger that is cryptographically secure, append-only, immutable , and updateable only via consensus or agreement among peers.

- A peer-to-peer network is a decentralized system in which each party can interact with any other on the same level, without a central controller. A peer-to-peer network is like a web, where every user is both an author and reader of information.
- A distributed ledger is a database that is shared by multiple parties on computer networks.
- Cryptographically secure means that the data can't be hacked or changed by another party. The blockchain uses cryptography to ensure the safety and security of data stored within.
- The blockchain is "append-only," which means that new data can be added to the blockchain, but old data cannot be erased.
- This is the most critical attribute of a blockchain. A consensus has to be reached among all participating nodes in order to make any updates to the ledger.
- The structure of a generic blockchain can be visualized with the help of the following diagram (Figure 2.1):

5 Blockchain structure

The figure 2.1 shows the Blockchain structure.

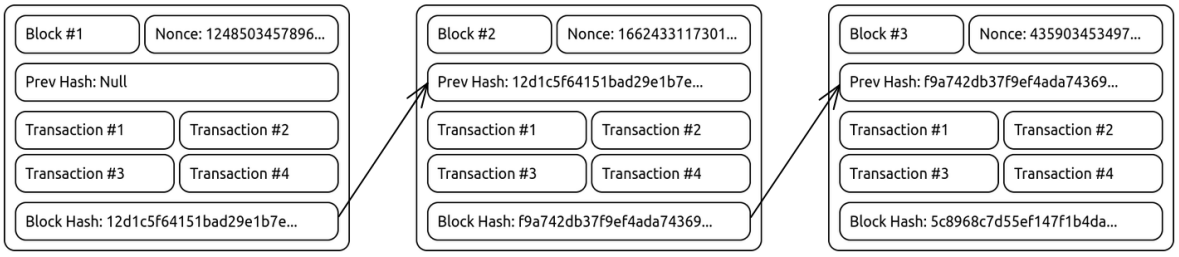

Figure 2.1: Block chaining

5.1 Addresses

Addresses are unique identifiers used in blockchain transactions to identify senders and recipients. An address is typically a public key or derived from one.

5.2 Transaction

The basic building block of a blockchain is a transaction. A transaction is the movement of money from one address to another.

5.3 Block

A block is a group of transactions that have been logically organized together [9]. It consists of the block header and the block body, the block header includes [50] :

- **Block version**: indicates which set of block validation rules to follow.
- **Merkle tree root hash**: the hash value of all the transactions in the block.
- **Timestamp**: is the creation time of the block.
- **nBits** : target threshold of a valid block hash.
- **Nonce**: an 4-byte field, which usually starts with 0 and increases for every hash calculation, it's used in PoW consensus algorithms.
- **Parent block hash**: a 256-bit hash value that points to the previous block , unless it's a genesis block (first block in the blockchain).

6 Types of Blocks in Blockchain Network

Blocks in the blockchain network can be classified as follows [46]:

- **Genesis Block** The initial block of any blockchain network is known as the genesis block. In 2009, the Genesis Block of the Bitcoin blockchain was created.
- **Valid Block** Valid blocks are already mined blocks by the miners added to the blocks in the blockchain. It means blocks have been appended to the blockchain by satisfying the criteria of the consensus mechanism.
- **Orphan Block** According to the consensus, if all the nodes in the network agree to the addition of a new block, then they are the valid blocks, but the rest of the blocks are orphan blocks. Since miners are competing to validate blocks simultaneously , the blockchain only accepts the valid block or the longest chain of blocks, as shown in figure 2.2.

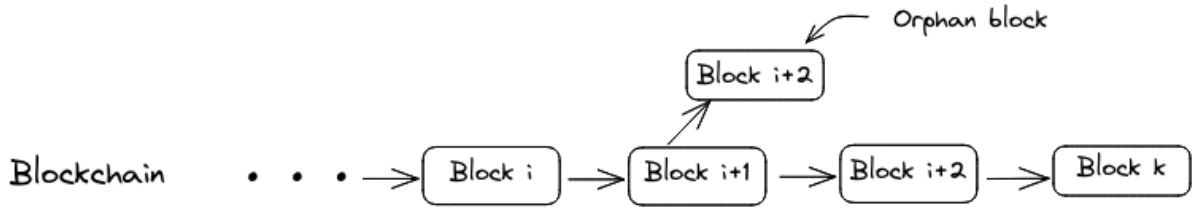

Figure 2.2: Orphan block

7 How blockchain works

This section show us how the blockchain works.

- **Transaction definition**
  The "Sender" creates a transaction and transmits it to the network. The transaction message includes details of the Receiver's public address,the value of the transaction. The transaction needs to be authenticated using digital signature and encryption techniques using the sender's private key. The figure 2.3 shows how the transaction is defined.[19]

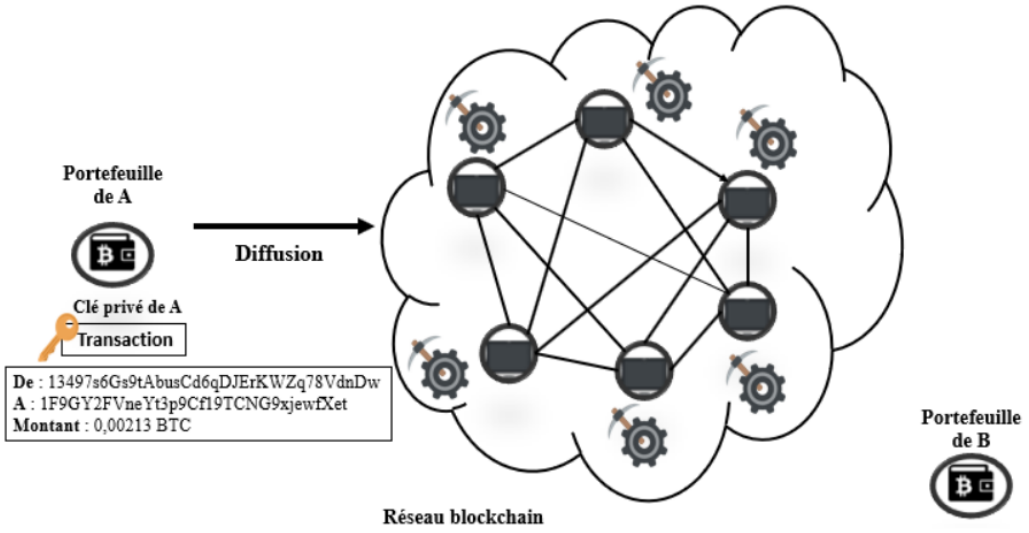

Figure 2.3: Transaction definition
[1]

- **Transaction authentication**
  A transaction is propagated (broadcast) usually by using data-dissemination protocols, such as Gossip protocol [46].. The nodes (computers/users) of the network receive the message and authenticate the validity of the message by decrypting the digital signature. The authenticated transaction is placed in a 'pool' of pending transactions as shown in the figure 2.4.[19]

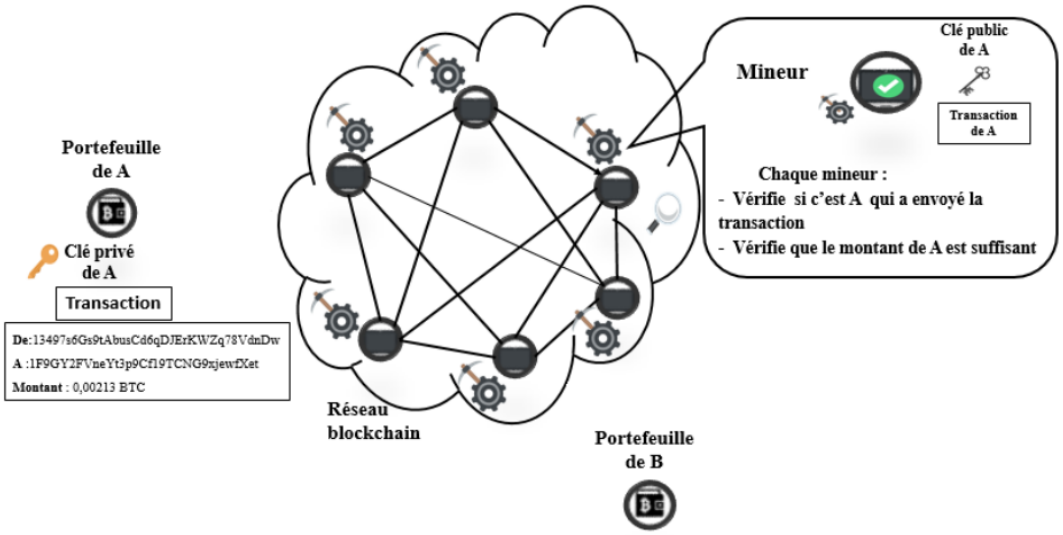

Figure 2.4: Transaction authentication
[1]

- **Block creation**
  These pending transactions are put together in an updated version of the ledger, called a block, by one of the nodes in the network. As shown in the figure 2.5, at a specific time interval, the node broadcasts the block to the network for validation. [19]

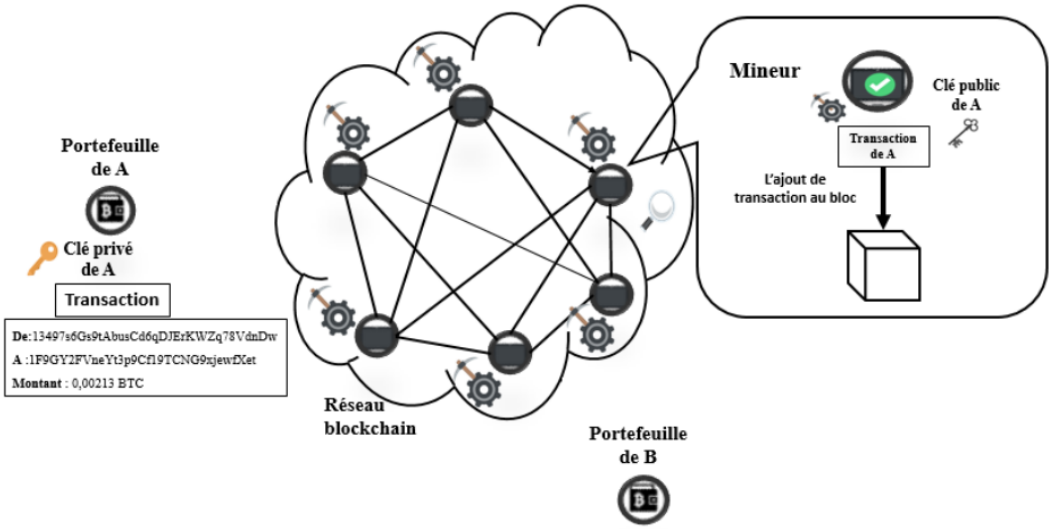

Figure 2.5: Block creation
[1]

- **Block validation**
  Once a miner fulfills the requirements of the consensus mechanism, the block is considered "found". At this point, the transaction is considered confirmed. Usually, in cryptocurrency blockchains such as Bitcoin, the miner who solves the mathematical

puzzle is also rewarded with a certain number of coins as an incentive for their effort and the resources they spent in the mining process. The figure 2.6 shows the process of the bloc validation.[46]

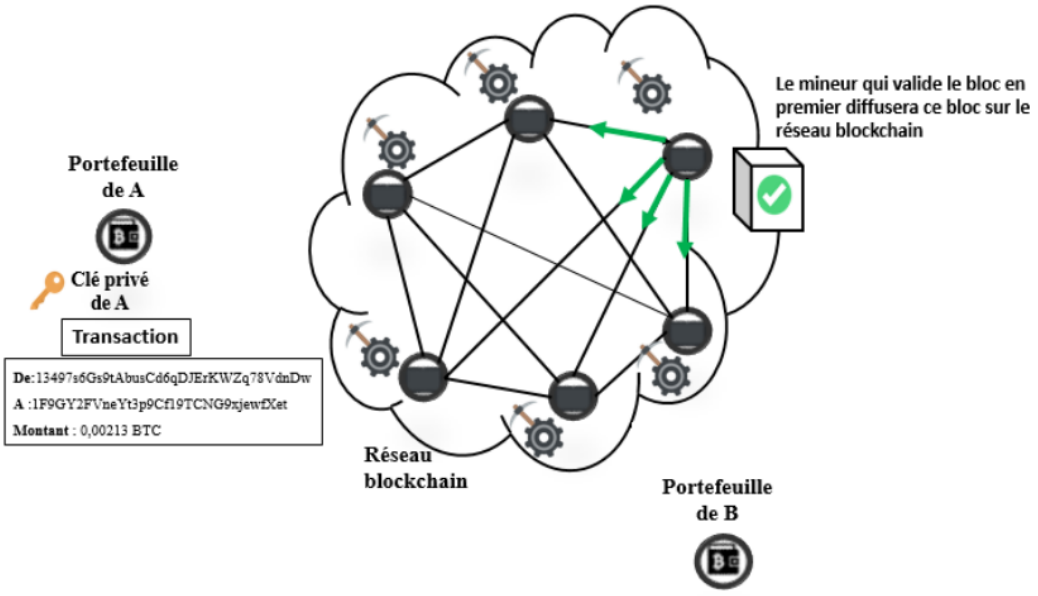

Figure 2.6
[1]

- **Block chaining**
  The newly created block is validated, and all the participants of the network have to come to an agreement regarding which block is "chained" into the blockchain, and the new state of the ledger is broadcast to the network. As shown in the figure 2.7.[19]

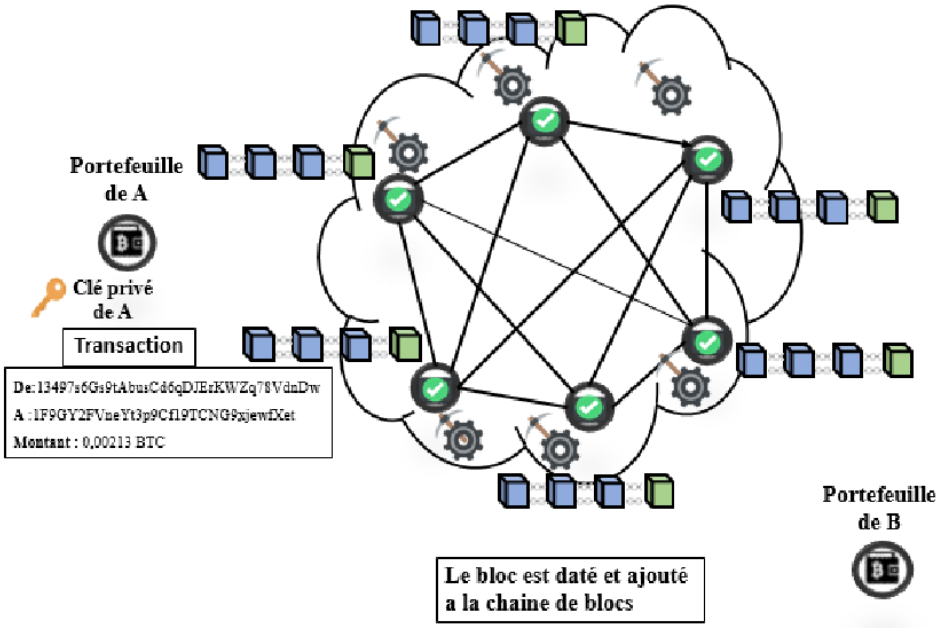

Figure 2.7: Block chaining
[1]

When an attacker tries to modify a transaction in a block, he still needs to find a way to make the modified chain accepted by all network nodes before his attack is successful. The only way is to make a longer chain than the genuine one. This is so-called the "longest chain rule": If there are two or more valid chains, always use the longest one. Unless the attacker controls over half of the power on the network, he will never win the race to create the longest chain (Figure 2.8).

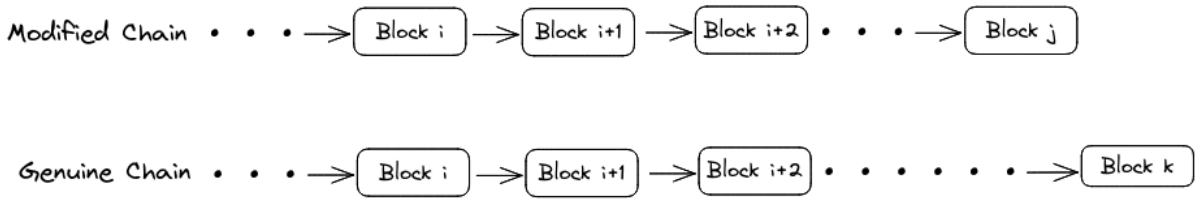

Figure 2.8: Nodes accept longest chain in blockchain

8 Benefits of Blockchain

Numerous advantages of blockchain technology have been discussed in many industries . The notable ones are [9] :

8.1 Decentralization

This is a fundamental idea and advantage of blockchain. Instead of relying on a trusted third party or intermediary, a consensus process is employed to determine whether transactions are genuine.

8.2 Immutability

It is quite challenging to alter data back once it has been posted to the blockchain.Although it is not truly immutable it is considered advantageous because altering data is extremely difficult and practically impossible.

8.3 Transparency and trust

The system can be transparent since blockchains are shared and everyone can see what is on them.Consequently, trust is built.

8.4 High availability

The system becomes extremely available due to the fact that it is built upon thousands of peer-to-peer nodes and that the data is replicated and updated on each node. The network as a whole keeps operating even if some nodes depart or are rendered inoperable, making it highly available. High availability is the outcome of this redundancy.

8.5 Highly secure

To ensure network integrity, all transactions in a blockchain are cryptographically secured. A predetermined set of rules is used to verify any transactions that are posted from nodes on the blockchain. For inclusion in a block, only valid transactions are chosen.

8.6 Faster dealings

Blockchain technology has the potential to be extremely valuable in the financial sector, particularly in post-trade settlement services. Because there is already a single version of the agreed-upon data available on a shared ledger between financial entities, blockchain does not necessitate a drawn-out process of verification, reconciliation, and clearance.

8.7 Cost-saving

The blockchain concept does not require a trusted third party or clearing house, which can significantly reduce overhead expenses in the form of the fees paid to such intermediaries.

8.8 Platform for smart contracts

A blockchain is a computing platform where applications can run and carry out business logic on behalf of users. Although not all blockchains offer a method to execute smart contracts, this is a very valuable feature and one that is often desired. It is accessible on more recent blockchain platforms like MultiChain and Ethereum but not on Bitcoin.

9 Challenges and limitations of blockchain

As with any technology, some issues must be resolved in order to make a system more reliable, practical, and usable.Blockchain technology is no different. In fact considerable

effort is being devoted in order to address the issues that blockchain technology raises. The most sensitive blockchain problems are:

9.1 Scalability

The blockchain grows larger every day as a result of the rising transaction volume. Additionally, the Bitcoin blockchain can only process about 7 transactions per second due to the original restriction on block size and the time interval utilized to generate a new block, which does not meet the need of processing millions of transactions in real-time. Since the capacity of blocks is so low, many minor transactions could experience delays since miners favor those with high transaction fees.

9.2 Adoption

Blockchain is frequently viewed as a developing technology. Even while this viewpoint is quickly shifting, there is still a long way to go before this technology is widely used. The difficulty in this situation is making blockchain networks simpler to use so that acceptance can rise. There are also a number of additional issues, such scalability, that must be resolved in order to boost adoption.

9.3 Regulation

Regulation on blockchain is incredibly difficult because of its decentralized nature. This is frequently viewed as a hurdle to adoption since, historically, customers have had some degree of faith that, if something goes wrong, they can hold someone accountable thanks to the existence of regulatory authorities. Blockchain networks, however, lack such governmental authority and oversight, which is a deterrent for many customers.

9.4 Privacy and confidentiality

Through the use of a public key cryptography, blockchain can maintain a certain level of privacy. [50] Users conduct transactions using their keypairs without having to disclose their identities. However, Since all transaction values and balances for each public key are made available to the public, it is demonstrated in [32] and [24] that blockchain cannot ensure transactional privacy. Additionally, a recent study [7] has demonstrated that links between a user's Bitcoin transactions can be used to reveal the user's information. Moreover, Biryukov et al. [11] presented a method to link user pseudonyms to IP addresses even when users are behind Network Address Translation (NAT) or firewalls.

9.5 Selfish mining

Blockchain is vulnerable to attacks from selfish, complicit miners. Eyal and Sirer [16] in particular demonstrated how the network is weak even if only a small amount of the hashing power is used for fraud.Selfish miners hold their mined blocks without broadcasting them, and the public is only made aware of the secret branch if certain conditions are met. All miners would accept it because the private branch is longer than the current public

chain. Prior to the publication of the private blockchain, honest miners were wasting their resources on a useless branch, while selfish miners were mining their private chain without competition. As a result, selfish miners tend to earn more money.

10 Key Technologies of Blockchain

Several technologies are linked to the blockchain in order to securely add transactions to the network. As previously stated, blockchain allows for the secure storage of transaction records in a decentralized and secure manner. However, in order to achieve this immutability in the network, we must consider several blockchain-related technologies.

10.1 Cryptographic Hash Functions

Bitcoin uses the SHA-256 hashing algorithm [35]. SHA is an acronym for Secure Hash Algorithm, it was created by the National Institute of Standards (NIST). Blockchain, in general, uses cryptographic hash functions to preserve and secure transaction storage and sharing in the network. It means the generated hash of the data has to pass through a cryptographic hash algorithm to yield an output that cannot be altered or tampered with by any malicious activity, which leads to a process known as hashing. Hashing takes variable length data of the block as input and produces the different hashes of the fixed size. So, if there is any modification in the input, change will be reflected in the hash value, which is known as the avalanche effect. Cryptographic hash functions need to satisfy several characteristics to ensure the security in the blockchain network [46] :

- **Deterministic** No matter how many times the input data for a block has been run through the cryptographic hash function, the output in the form of a hash value should always be the same due to the hash function's deterministic property.
- **Fast Computation** In order to apply the cryptographic hash function efficiently for the security of the blockchain network, the entire hashing process must be quick enough to produce the desired hash value of the input data.
- **Feasibility** According to the hash function's feasibility property, no one can determine the original data using the output hash value once the hash value of the data has been retrieved from the input data.

10.2 Digital Signature

A set of private and public keys are owned by each user. The transactions are signed using the private key, which must be kept secret. The transactions that have been digitally signed are broadcasted across the whole network. The signing phase and the verification phase are the two stages of a typical digital signature. For instance, user Alice wants to communicate with user Bob. Alice uses her private key to encrypt the data she wants to sign, then she gives Bob both the encrypted data and the original data. Bob checks the value with Alice's public key during the verification stage. Bob could then quickly determine whether the data has been altered.

10.3 Consensus Mechanism

Since there is no single entity in charge of verifying or approving transactions, it offers immutability, transparency, security, and privacy thanks to consensus algorithms which refers to the method through which each network node agrees on which transactions are legitimate and should be recorded on the blockchain. Blockchains are vulnerable to a number of assaults if the consensus techniques used are insufficient.

10.3.1 Proof of Work

The Bitcoin network employs proof of work as a kind of consensus. It takes a lot of work to demonstrate that a node is unlikely to attack the network before it can publish a block of transactions. Calculations using a computer are typically part of the process. Each node of the PoW network determines a block header hash value. A nonce is contained in the block header, and miners frequently change the nonce to obtain various hash values. The calculated value must match or be less than a specified value, according to the consensus. When a node reaches the desired value, it broadcasts the block to all other nodes, who then have to mutually verify that the hash value is accurate. Other miners would add this new block to their respective blockchains if the block is validated. In Bitcoin, nodes that perform the PoW are known as miners, and the process itself is known as mining. [50]

10.3.2 Proof of Stake

The most frequent replacement for Proof of Work is Proof of Stake [40]. In PoS, the validator invests in coins rather than spending money on expensive hardware to solve mathematical challenges. As stakes, they lock some of their coins. Randomization is used to choose who gets to create the next block. The odds of creating the next block are typically higher for those with the largest stake. How long the coin has been staked is another consideration. In this case, transaction fees are given as payment in full or in part for the work. Due to the high cost and increased energy efficiency of PoS over POW, consumers benefit from more anonymity and data protection. [46]

11 Types of Blockchain

This section presents the types of the blockchain

11.1 Permissionless Blockchain

These types of blockchains are open and transparent, anyone can review them at any given point of time. They are also known as public blockchains and they power up most of the digital currency in the market.[44]

What characterizes the permissionless ledgers is that there is no gating or authorizing process to enroll into the transactions scheme. Everyone is free to download a copy of the blockchain ledger, and they are able to join as anonymous validators by performing computationally intensive proof-of-works [19]. Anyone can run a node, mining software.

Anyone can access a wallet, write data onto the transactions as long as they are following rules of the blockchain.[44] Public blockchains are secure even though they are open and public. It has also been argued that these public ledgers are practical for primarily on-chain assets, meaning assets that are endogenous and created on the ledger (e.g Bitcoin). This argument is based on the fact that off-chain assets are not controllable by the validators in the same way as the native assets, and any conflicts in a transaction would need to be solved by an outside party or legal entity. [19] Bitcoin is the best example describing Permissionless blockchain

11.2 Permissioned Blockchain

They are also known as private blockchains. They act as a closed ecosystem [44] where only pre chosen entities can join the network. The network is centralized, and the central authority is responsible for giving permissions for writing transactions and who can read the particular transaction. The central authority also determines mining rights, which can be overridden or modified [46]. The administrator can give or revoke the permissions granted to a user. The consensus mechanism may be the same as public blockchain or some other may be used.[19] The main benefits offered by employing a permissioned ledger approach over a permissionless have been suggested to be: cheaper energy cost for transactions, greater privacy, and a faster validation process

11.3 Consortium Blockchain

Consortium blockchains are a hybrid blockchain that combines public and private blockchains. [9]. The private section is run by a small group of people, whereas the public section is open to anyone. Some nodes can participate in transactions, while others control the consensus process. The network, like the private blockchain, is centralized, with a single point of failure. Control is not in the hands of a single authority, but of a small group of authenticated users. Control is not completely centralized; rather, it is a hybrid of centralization and decentralization. Some nodes need to sign off each transaction, while others require network approval. Consortium blockchains mimic the advantages of private blockchains by enhancing efficiency and transaction privacy. [46]

12 BlockTree

Implementations of blockchains are frequently created with a particular goal or function in mind. Cryptocurrencies, smart contracts, and distributed ledger systems between businesses are a few examples of these goals. Blockchain technology has seen a steady stream of advancements, and as new platforms are routinely introduced, the landscape is always shifting. [48]
Variants of blockchain technology do exist, such as : BlockTree. A blockchain that follows a tree structure figure 2.9. Simply put, BlockTree is a blockchain with branches that offers better and improved consensus delay and throughput. This comes in handy with our implementation of the voting system.

In traditional Blockchains, branches do exist. But only the longest branch is accepted by all the nodes. All the blocks in those branches are discarded. This is a huge waste of

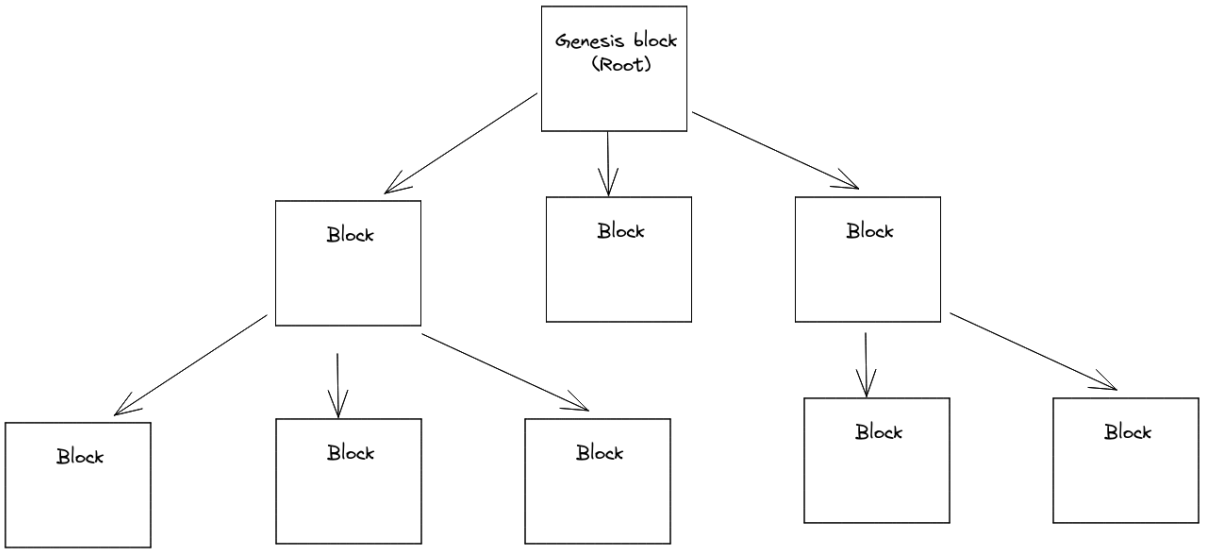

Figure 2.9: BlockTree

time, calculation power and energy. By accepting these branches, things drastically improve, since accepting multiple blocks at the same time increases throughput and reduces delay.

CHAPTER 3

REALIZATION & IMPLEMENTATION

1 Introduction

Online voting is a delicate matter, and stringent rules and requirements have to be met in order to create a trusted voting system. Blockchain technology offers a secure and trustworthy platform to build our system on top of. but it has a major downside : speed.

In this chapter, we present our voting system based on blockctree while explaining why BlockTree technology could be the perfect solution for this type of voting. This chapter also contains a part for the description of our system and another one illustrates its implementation

2 Why BlockTree ?

Traditional Blockchains discard branches to avoid duplicate transactions from appearing in different blocks on different branches. This is a major problem to face when implementing a BlockTree like this. But due to the nature of voting, each eligible citizen can only cast one vote, (one transaction). So By allowing only one transaction per block, and using mechanisms to prevent citizens from voting multiple times, this problem is easily solved. And if, by any means, multiple blocks with the same vote by the same person do end up in the BlockTree, all we have to do is count it only once.
Another important aspect is mining, or more precisely, the lack of it. Since every registered citizen is already allowed to vote once, it is as if they have one *coin* to spend. Validating a transaction is then reduced to two simple verifications :

- Ensure the electronic signature is valid.
- Ensure the uniqueness of this electronic signature.

Other implementations of Blockchain based voting systems that require mining (or any other consensus mechanism) impose a transaction fee, which means you have to pay to be able to vote. With our implementation, voting is free.

3 Why MasterKey ?

One of our goals in this work is to hide the state of the vote until the end. No one should know who is winning during the voting period, to avoid certain types of vote manipulation that may occur in situations where a candidate is winning in the morning, for example, which may discourage other citizens from voting for another candidate, thinking he already lost, but in reality, if they do cast their vote, their candidate may be able to win.
To achieve this, every citizen uses a shared public key, called the MasterKey, to encrypt their vote. The corresponding private key is hidden from every one, and is calculated at the end to decrypt the votes in order to count them. This process is further explained in 4.1.2.

4 System description

Like we saw in chapter 1, we have three election phases :

4.1 Pre-election phase

Before anyone can vote, it is important to have certain elements in place for the system to work properly. A consortium is established to manage and organize the elections. This consortium shares a Master key that will be used to encrypt every vote during the voting period. It is responsible for :

- Supervising the citizen enrollment process.
- Managing candidates
- Starting/stopping the vote
- Decrypting the votes in order to calculate the results.

4.1.1 Consortium creation

In this step, the consortium members are designated. Ideally, multiple representatives of each candidate are chosen. Other members can also be chosen amongst citizens. This consortium will take care of the citizen enrolment process. Each member is presented with an interface to generate a keypair (public and private key), which will be used for authentication and signing transactions. This consists of scanning a QRcode with a mobile phone. The generated private key stays in the consortium member's device, while the public key is transmitted to the blockTree.

The use of a QRcode allows us to facilitate the registration process. Upon scanning, the system does the following, as shown in figure 3.1 :

- Verifies that the code was generated on the BlockTree.
- Verifies that the code wasn't used before.
- If the first two conditions are verified, it generates a key pair on the user's device.

- Sends the the public key and the address(derived from the public key) to the BlockTree
- Show error message if one of the first two conditions aren't verified.

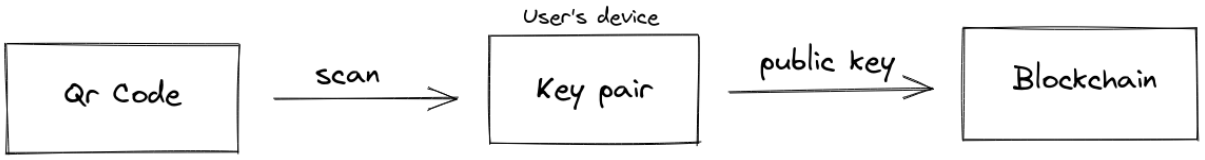

Figure 3.1: Keypair generation

The government provides a document to the consortium members containing a list of citizens eligible to vote, along with the hash value of this document to prevent anyone from tampering with it.

4.1.2 Master Key Generation

The master key is then generated. The public part will be used by every citizen to encrypt their ballot in order to hide the state of the vote until the end. The private part needs to be hidden as well, it is split amongst the consortium members before the voting period, and recalculated after the voting period ends. Splitting the Private key in a traditional fashion will prevent recalculating it if one of the consortium members is unable to provide his part. We need a way to split it between N consortium members, and be able to recalculate it successfully with the data provided by a majority $K = \frac{N}{2+1}$ of consortium members, this aims to avoid a strategic blocking from other members.

We propose a method to achieve that, by using a system of equations. The necessity of n equations to resolve an n variable system. For example, a one variable system needs a one variable equation : $A = Bx + C$. It is a well-known formula from algebra. The reasoning behind it is quite simple: in order to find the unknown solution x , we subtract C from both sides of the equation to yield $A - C = Bx$, and then divide each side by B to yield : $(A - C)/B = X$. This problem has been solved using this formula for centuries now, with no known new discoveries or innovations ever popping up.

To solve a multi-variable equation (e .g) $\begin{matrix} x + 2 = 10 \\ y - 3 = 8 \end{matrix}$, the goal is to find a system of two equations that satisfy both equations simultaneously. To do this, we will use an algebraic method called "algebraic reduction" which allows us to replace the multi-variable equation with a single linear equation and then pair the equations. Our method consists of generating a system of N equations with K variables, so that K equations will be sufficient to solve the system.

Based on that, we follow these steps for every character in the base64 encoded private key :

- Get the ASCII number of the current character.
- This number is then split into a sum of K numbers $(k_1, k_2 \dots)$.
- A line equation is generated $Y = k_1 * x_1 + k_2 * x_2 \dots$

- For each consortium member, assign randomly generated numbers for $(x_1, x_2 \dots)$ and the equivalent Y.

To avoid generating equivalent equations for multiple members, we make sure to generate at least one different prime number for each equation.To recalculate the private key, we solve the equation system for each character by finding $k_1, k_2 \dots$.

Example for $N = 5$ members, $K = 3$:
Let's say the first character in the base64 encoded private key is : M. The ASCII value of M is 77. We randomly generate 3 numbers that add up to 77 : $k_1 = 10, k_2 = 120, k_3 = -53$. So $Y = 10x_1 + 120x_2 - 53x_3$.

$$10 * 2 + 120 * 3 - 53 * 6 = 62 \Rightarrow (x_1 : 2, x_2 : 3, x_3 : 6, Y : 62) \tag{3.1}$$

$$10 * -3 + 120 * 1 - 53 * -4 = 302 \Rightarrow (x_1 : -3, x_2 : 1, x_3 : -4, Y : 302) \tag{3.2}$$

$$10 * -2 + 120 * 1 - 53 * 3 = -59 \Rightarrow (x_1 : -2, x_2 : 1, x_3 : 3, Y : -59) \tag{3.3}$$

$$10 * 2 + 120 * 2 - 53 * 3 = 61 \Rightarrow (x_1 : 2, x_2 : 2, x_3 : 3, Y : 61) \tag{3.4}$$

$$10 * 6 + 120 * -2 - 53 * -3 = -21 \Rightarrow (x_1 : 6, x_2 : -2, x_3 : -3, Y : -21) \tag{3.5}$$

To retrieve the original letter in our example, we need at least three sets of data equations, let's use the 1st,3d and 5th :

$$\begin{cases} k_1 * 2 + k_2 * 3 + k_3 * 6 = 62 \\ k_1 * -2 + k_2 * 1 + k_3 * 3 = -59 \\ k_1 * 6 + k_2 * -2 + k_3 * -3 = -21 \end{cases} \tag{3.6}$$

$$\begin{cases} k_1 * 2 = 62 - (k_2 * 3 + k_3 * 6) \end{cases} \tag{3.7}$$

$$\begin{cases} -62 + k_2 * 3 + k_3 * 6 + k_2 + k_3 * 3 = -59 \\ 4 * k_2 + 9 * k_3 = 3 \Rightarrow k_2 = \frac{(3 - 9 * k_3)}{4} \\ 3 * (62 - 3 * k_2 + 6 * k_3) - 2 * k_2 - 3 * k_3 = -21 \\ 186 - 9 * k_2 - 18 * k_3 - 2 * k_2 - 3 * k_3 = -21 \\ 11 * k_2 + 21 * k_3 = \frac{33}{4} - \frac{99 * k_3}{4} + 21 * k_3 207 \end{cases} \tag{3.8}$$

$$\begin{cases} -99 * k_3 + 21 * k_3 = 795 \Rightarrow \mathbf{k_3 = -53} \\ k_2 = \frac{(3 - 9 * -53)}{4} \Rightarrow \mathbf{k_2 = 120} \\ k_1 * 2 = 62 - (120 * 3 - 53 * 6) = 20 \Rightarrow \mathbf{k_1 = 10} \end{cases} \tag{3.9}$$

The originale character is the sum of k_1, k_2 and k_3:

$$10 + 120 - 53 = 77.$$

The ASCII value of 77 is M.

The machine's memory on which the master key is generated should be wiped after the key is distributed amongst the consortium, a virtual machine with no access to the host system should suffice.

4.1.3 citizen enrolment process

The same method as in 4.1.1 is applied, the only difference is the generated keys are used to authenticate citizens and digitally sign the timestamp of the casted vote. The hash of the base64 encoded public key is used to represent the citizen's address on the BlockTree. Each citizen presents his identity card to the consortium to prove he is authorized to vote, by matching his data to the document provided by the government. It is worth mentioning that no organization has the power to manipulate this process. Even if they provide a document with extra fake entries to make fake votes, the consortium keeps track of every citizen that shows up for registration, and only those who registered successfully will have the authorization to cast a vote. Each citizen will have to cast his vote with the same phone he registered with, since the private key is stored only on that device.

4.2 Election phase

The Election phase is divided into two parts which are mentioned below.

4.2.1 Authentication

Electronic signature - figure 3.2 - is used to authenticate citizens on the BlockTree. Whenvere one tries to connect, a message signed with his private key is sent to the BlockTree for verifications, if the signature is verified, he is authorized to vote. The BlockTree then responds with a success message, the public master key and the hash of the last block on the BlockTree.

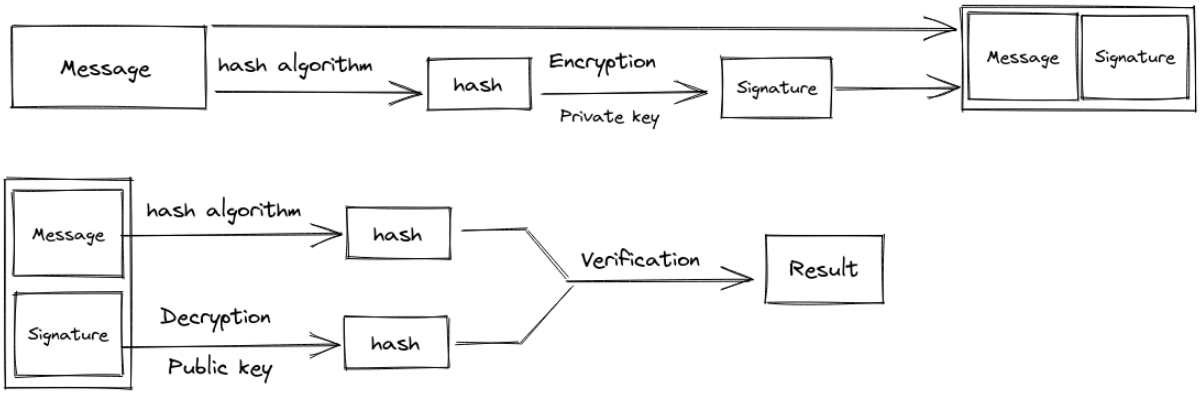

Figure 3.2: Electronic signature

4.2.2 Voting

When a citizen makes his choice and casts his vote, the following is transmitted to the BlockTree :

- His address
- His choice, encrypted with the Master Key.
- The current timestamp.
- The previous hash.
- The current timestamp and the previous hash, signed with his private key.

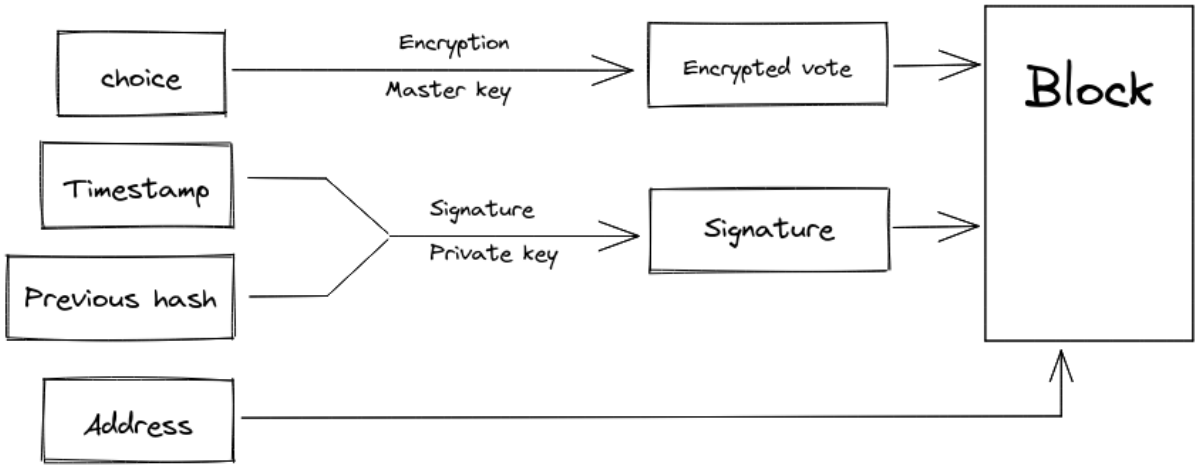

Figure 3.3: Block creation

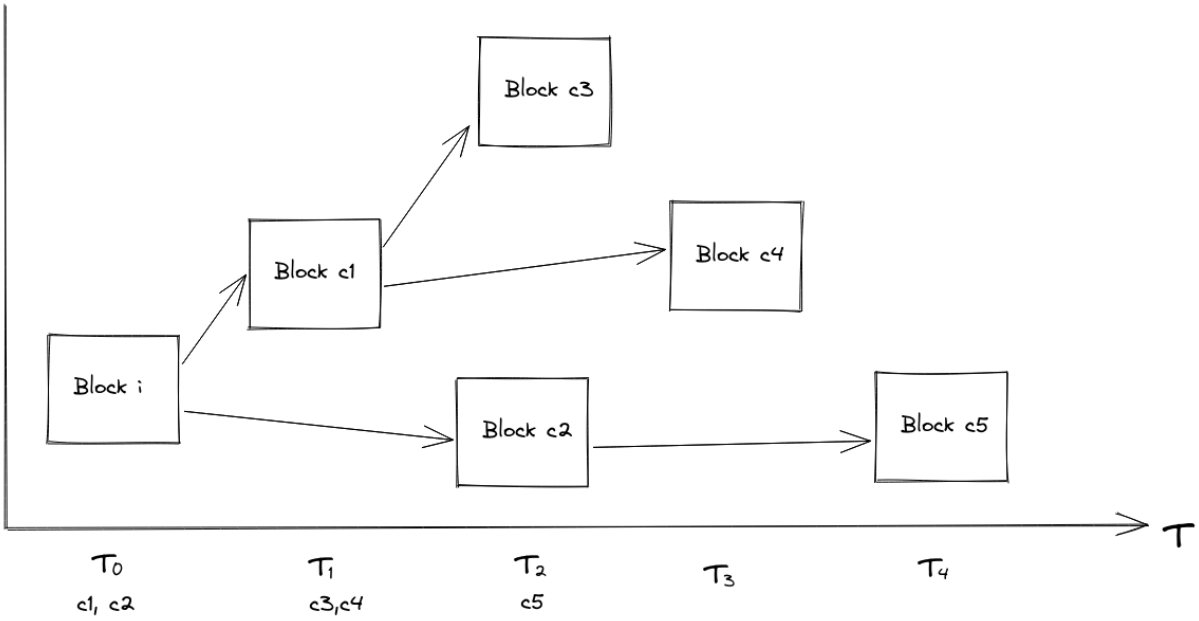

Figure 3.4: Chaining of blocks over time

For example, over time, five citizens (c1-c5) connect to the blocktree and cast their votes, whenever one logs in successfully , he receives the hash of the last block on the BlockTree. Figure 3.4 shows how a tree is created :

- At T0, c1 and c2 received the hash of the last block i.
- At T1, c1 emitted his block chained to block i, c3 and c4 received the hash of the block c1.
- At T2, c2 emitted his block chained to block i, c5 received the hash of the block c2, c3 emitted his block chained to block c1.
- At T3, c4 emitted his block chained to block c1.
- AT t4, c5 emitted his block chained to block c2.

4.3 Post Election phase

In this phase, the consortium members provide their data to recalculate the master key. Every citizen has access to the entire blocktree and calculate the results.
If more than half of the members refuse or are unable to provide their data, there will be no way to get the results and the entire vote is canceled.

5 Design Flow Diagrams

In this section, we will define the requirements analysis of our application through use case diagrams.

5.1 General Use Case Diagram

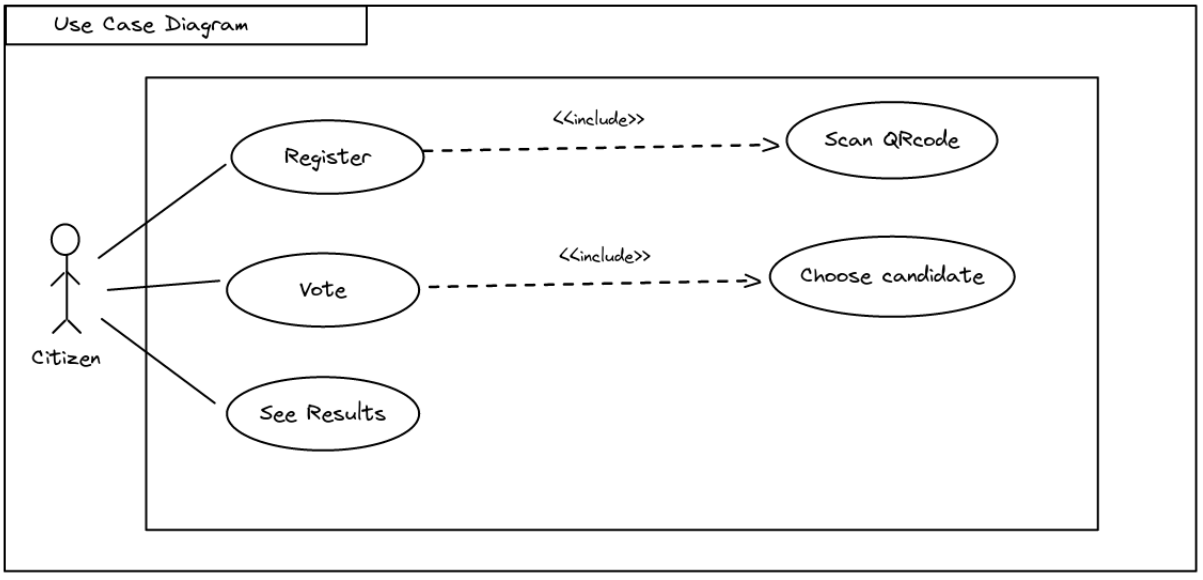

Figure 3.5: General use case diagram

Authentication is required for citizens to access the voting interface. To register, citizens have a limited amount of time to visit a registration center supervised by the consortium. They provide documents to prove they are eligible to vote. If this operation is successful, they are presented with a computer screen with a button to generate a QRcode. When visiting the interface during this period, citizens are presented with the option to scan that QRcode, the system does some verifications as mentioned in 4.1.1, a unique key pair is generated on the citizen's device, and the public key is transmitted to the BlockTree.

5.2 Voting Use Case Diagram

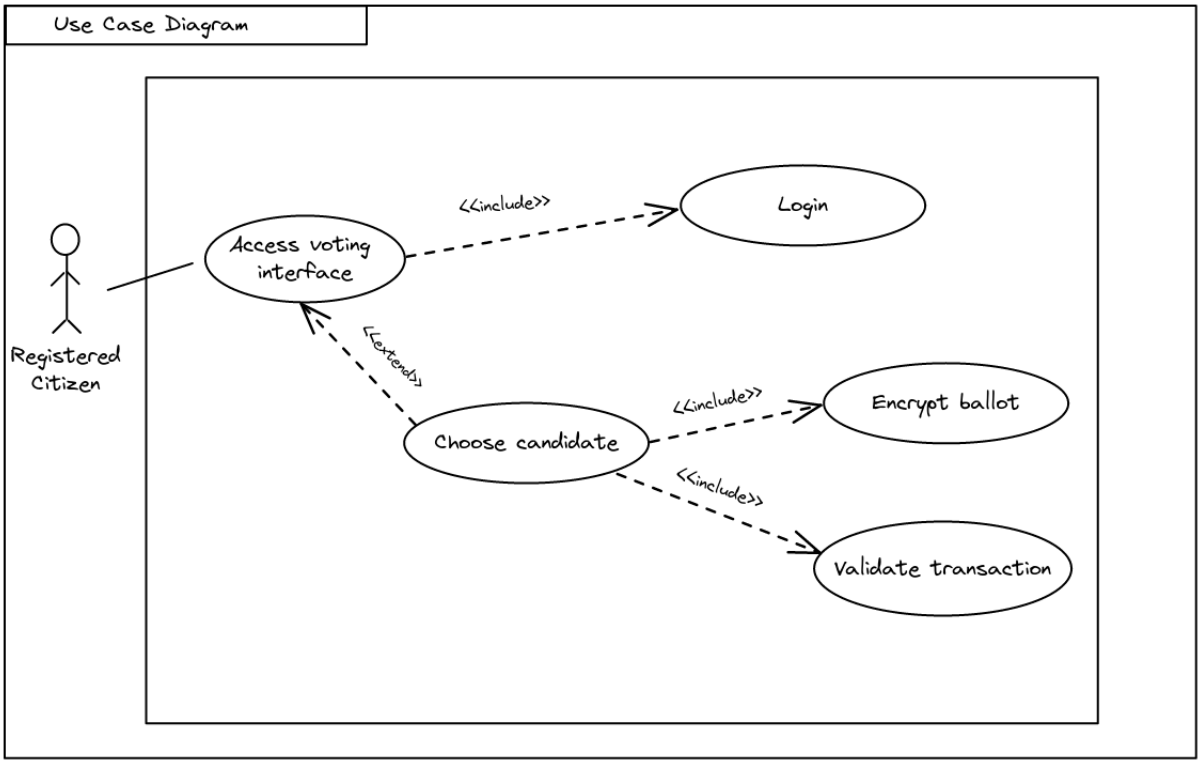

Figure 3.6: Voting use case diagram

A registered citizen is authorized to access the voting interface. During the voting period, electronic signature is used to log citizens in. They are then presented with the list of candidates and a button to confirm their choice. The figure 3.6 shows the details of the voting use case. A message is displayed according to every situation the citizen might be in :

- Already registered (If the citizen already registered and the voting period didn't start yet).
- Not authorized to vote (If the citizen didn't register to vote).
- Already voted (If the citizen already made their vote).

- Any other error that might occur.

5.3 Consortium Use Case Diagram

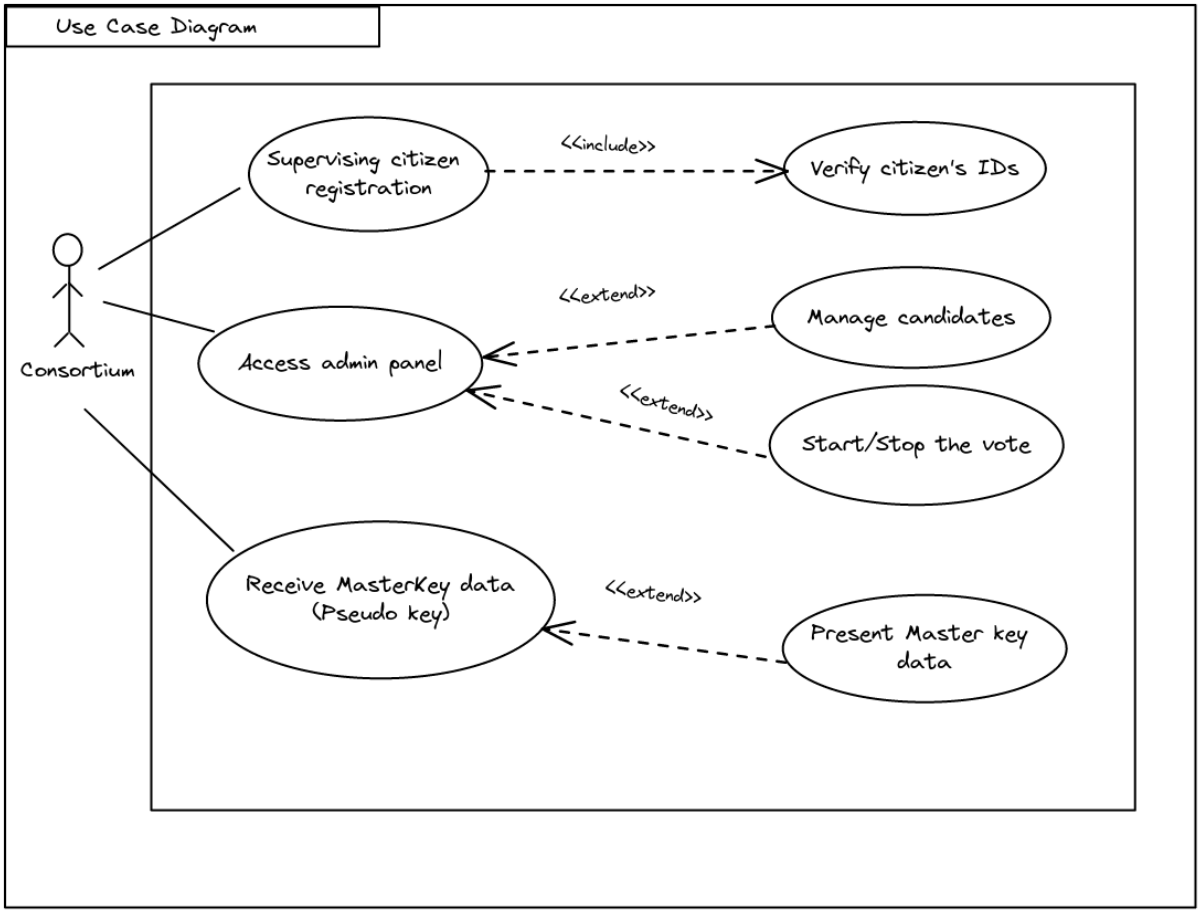

Figure 3.7: Consortium use case diagram

Whenever a citizen visits the registration center and presents his ID, consortium members check that information with the official document of eligible voters provided by the government. If the information is valid, the citizen can move along with the registration process.
The MasterKey is split between consortium members right after its creation, and only at the end of the vote, they can present their part to recalculate it.
Consortium members have access to an admin panel where they can add or remove candidates. Candidates can only be added before the voting period starts. They can also start and stopping this vote.3.7

6 Implementation

In this section, we will present our application in greater details, along with some tests and results. This project consists of several components that interact with each other :

- The blocktree itself.
- A graphical interface connected to the Blocktree to generate QRCodes and manage registrations.
- A PWA (Progressive Web App) for smartphones to register, authenticate, vote and display the results.
- An admin panel to manage candidates and start / stop the voting period.

6.1 BlockTree

To create our blocktree, we used Python as a programming language, and the SocketIO module for managing sockets. First we define a Block class :

```
class Block:
   def __init__(self,prevHash,transaction,timestamp,
                signedTimestamp):
       self.previousHash = previousHash
       self.transaction = transaction
       self.timestamp = timestamp
       self.signedTimestamp = signedTimestamp
       self.hash = self.blockHash()
```

Listing 3.1: Block class

We initialize the block with the required parameters :

- The previous hash.
- The transaction in the shape : address => encrypted choice.
- The current timestamp.
- The signature of the previous hash and the current timestamp

Then, we calculate the hash of the block using the hashlib module. A block only contains one transaction.
Next , we define a Node class as a tree structure to store the block, and an array of its children in order to form a tree.

```
class Node:
   def __init__(self, block):
       self.block = block
       self.next = []
```

Listing 3.2: Node Class

The BlockTree class is just a reference to the first node. The genesis block is created when the BlockTree is initialized. In order to add a block given a hash, we need to crawl the Blocktree until we find the corresponding block, and then we append the new block to its children. We also keep track of the last block added in the BlockTree.

```
class BlockTree:
   def __init__(self):
       self.blocktree = Node(Block("", "",
       str(int(round(time.time() * 1000))), ""))
       self.last = self.blocktree

   def findNode(self, root, hash):
       if root == []:
           return None
       else:
           for el in root:
               if el.block.hash == hash:
                   return el
               tmp = self.findNode(el.next, hash)
               if tmp is not None:
                   return tmp
           return None

   def addBlock(self,transaction,timestamp,hash,signedTimestamp):
       new_node = Node(Block(hash, transaction,
       timestamp, signedTimestamp))
       if self.blocktree.next == []:

           self.blocktree.next.append(new_node)
           self.last = new_node
       else:
           root = self.blocktree.next
           node = self.findNode(root, hash)
           if node is None:
               print("ERROR, block not found")
           else:

               node.next.append(new_node)
               self.last = new_node
```

Listing 3.3: Python BlockTree class

The Socketio module provides an easy way to serve static files like html, css , and javascript. We used it to serve the client application in the public folder that connects to the BlockTree in a peer to peer way.

```
sio = socketio.AsyncServer(async_mode="asgi")
app = socketio.ASGIApp(sio, static_files={"/": "./public/"})
```

Listing 3.4: SocketIO ASGI Server

When a citizen visits the served website, it automatically connects to the BlockTree:

```
store.connexion.on("connect", () => {
   console.log("connected ");
});
store.connexion.on("disconnect", () => {
   console.log("disconnected ");
});
```

Listing 3.5: Javascript SocketIO events

The BlockTree listens for new connections

```
@sio.event
async def connect(sid, env):
   print(sid, "connected")
@sio.event
async def disconnect(sid):
   print(sid, "disconnected")
```

Listing 3.6: Python SocketIO events

6.2 QRcode generator

As explained in 4.1.1, the registration process relies on QRcodes, which are image representations of passwords that can only be scanned once, as shown in figure 3.9.

This component is made with python, GTK 3 for the Graphical interface - figure 3.8 -. It accepts some command line arguments :

- -c : Consortium members registration.
- -t : Citizen registration.

Figure 3.8: QRcode generator interface

Figure 3.9: QRcode generated

6.3 PWA

A progressive web app with html, css and javascript, with Vue.js as the javascript framework, Vue.js offers a lot of benefits over regular javascript :

- Support for PWA's by default.
- Provides modules for accessing the camera.
- Provides an easy way to write reusable components.
- Very fast build times.
- Easy to maintain and update.

The registration page for consortium members, as shown in figure 3.10 , presents two functionalities :

- Registering as a consortium member.
- requesting the Master key data.

The latter is only possible when the former is successful.
A message is displayed - figure 3.12 - to indicate whether the registration operation is successful or not. The registration fails for example, when one scans an already used QRcode.
This operation requires camera access - figure 3.11 -. The Master key data can only be requested once, and only if it has been generated.

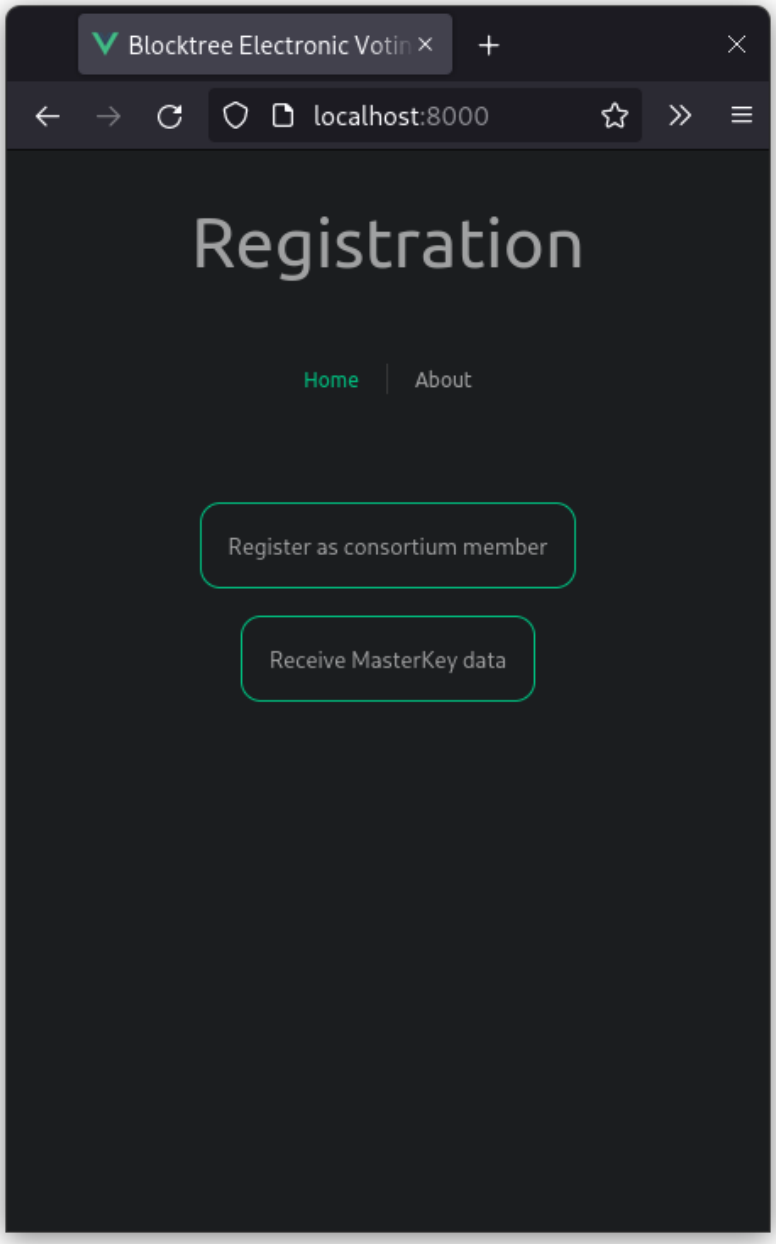

Figure 3.10: Consortium registration page.

When a QRcode is scanned, the system verifies that the QRcode is valid (generated by the app) and that it is not already used.

Figure 3.11: QRcode scanning

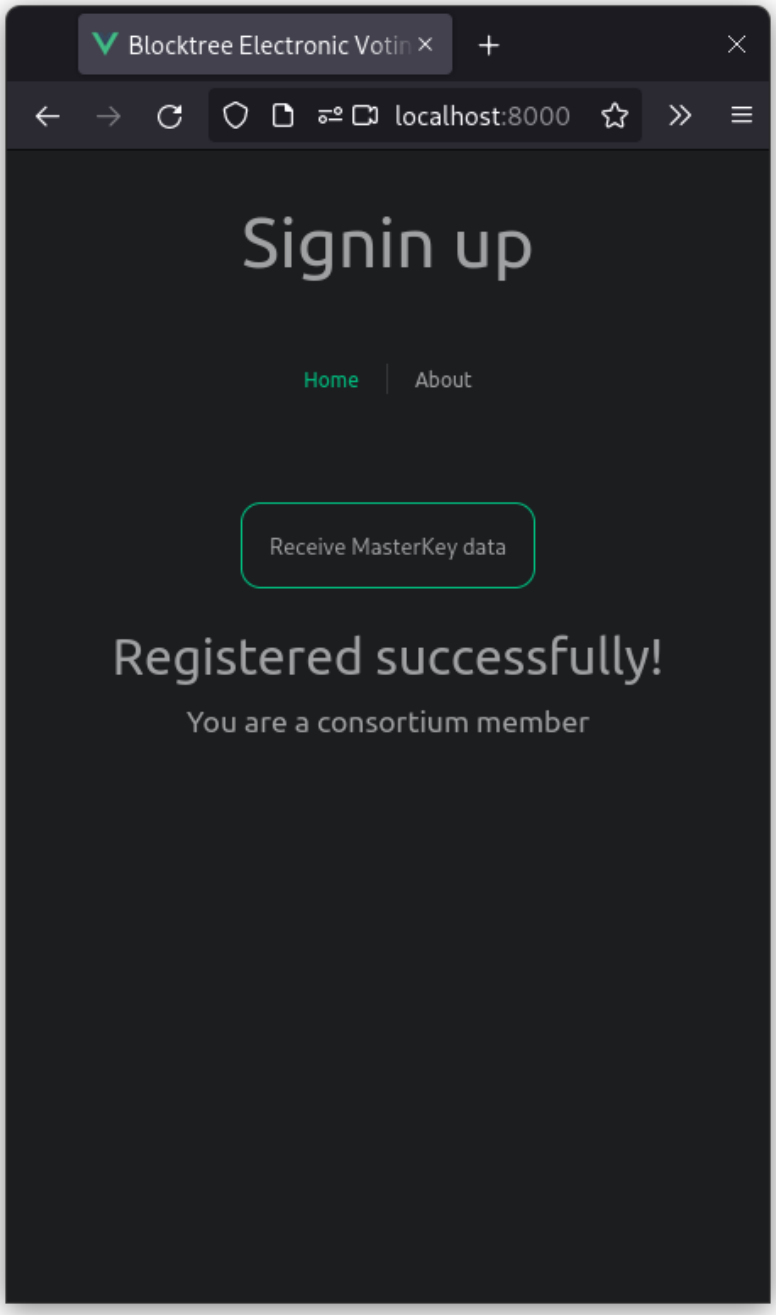

Figure 3.12: Successful registration

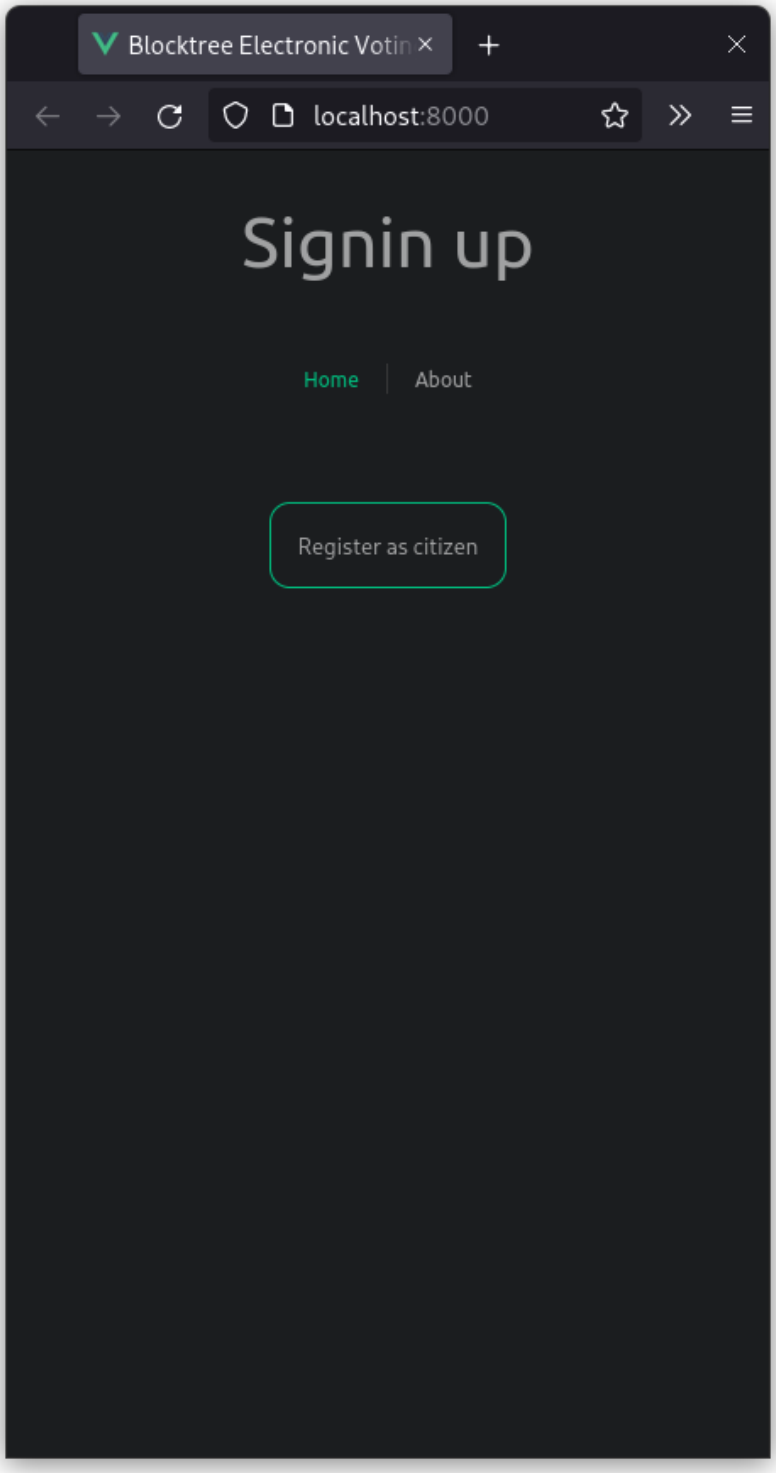

Figure 3.13: Citizen registration

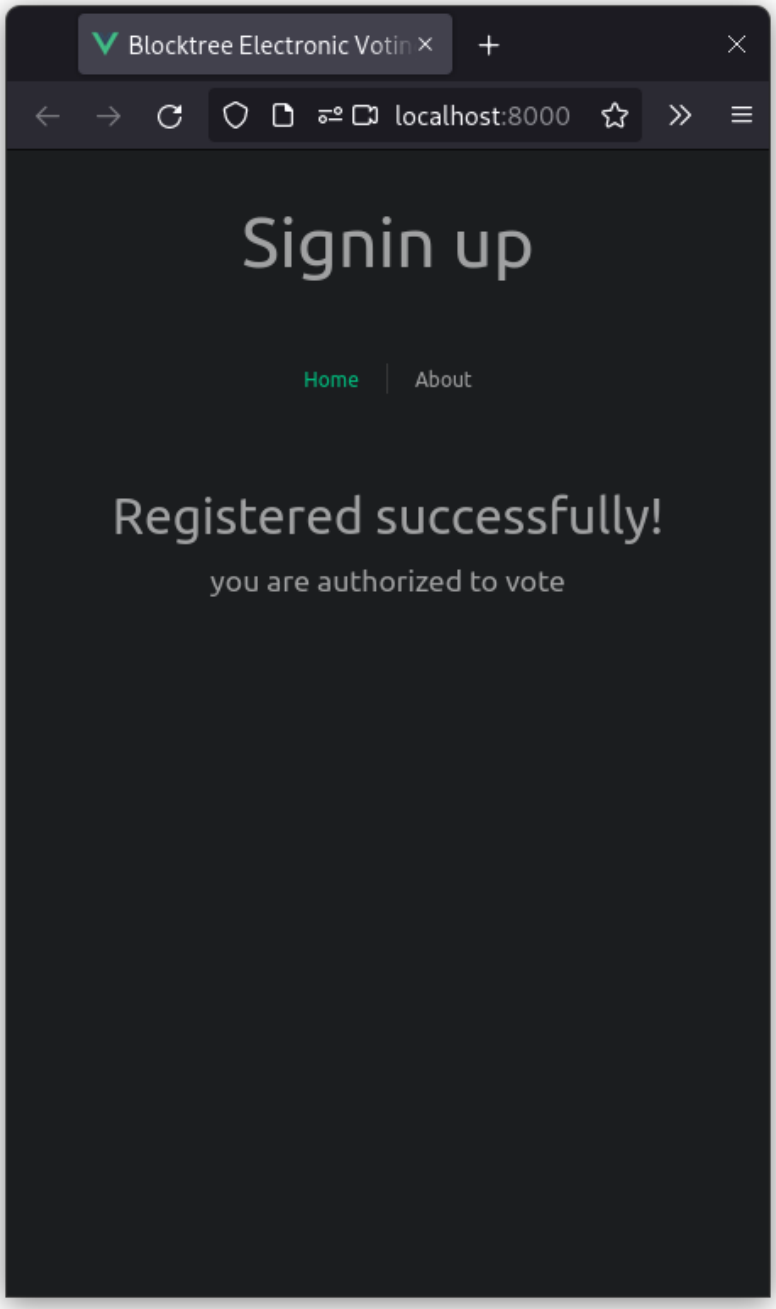

Figure 3.14: Citizen registration success.

6.4 MasterKey generator

This Master key must be generated only after the consortium registration step.

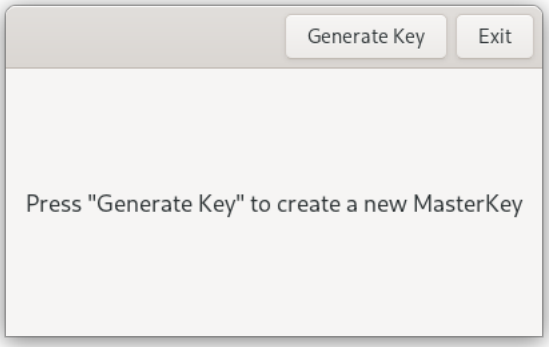

Figure 3.15: Master key generator UI

We used OpenSSL to generate the MasterKey, we store the public part in an sqlite file and then we use our previously described method in 4.1.2 to split the private part amongst the consortium members.

```
def generate_consortium_key(self, *data):
    os.system("openssl genpkey -out masterkey.pem\
            -algorithm RSA -pkeyopt rsa_keygen_bits:2048")
    os.system("openssl pkey -in masterkey.pem -pubout\
            -out masterkeyPub.pem")
    with open("masterkeyPub.pem", "r") as f:
        pempubkey = f.read()
    conn = sqlite3.connect("../database.db")
    c = conn.cursor()
    c.execute("""INSERT INTO MASTERKEY
            VALUES ("{}")""".format(pempubkey))
    c.execute("select * from MASTERKEY")
    data = c.fetchone()
    print("Public master key : ", data)
    c.execute("select * from CONSORTIUM")
    n = len(c.fetchall())
    print("number of consortium members :", n)
    conn.commit()
    conn.close()

    with open("masterkey.pem", "r") as f: pemkey = f.read()
    genHiddenKeys(pemkey, n)
```

Listing 3.7: Python method for generating the Master Key

A message is displayed when a member successfully receives his part of the Master Key data -figure 3.16.

When the voting period is on, the interface looks like in figure 3.17. Every citizen must log in before he is able to vote. The login function signs a message with the citizens private key, and sends it to the blockchain for verification with the corresponding public key. If the verification is successful, he is redirected to the voting page - figure 3.18 -.

Casting a vote is simple, the citizen selects his choice amongst the available candidats, and then presses “Vote”, a block is then transmitted to the BlockTree, there, it is verified that:

- The citizen signature is authentic.
- The block’s signature is authentic.

A message is displayed to confirm that the vote has successfully been casted - figure 3.19 -.

Consortium members are presented with a button to present their Master key data at the end of the vote - figure 3.20.

When enough members present their data, the Master key is recalculated and the results are immediately available to everyone -figure 3.21.

Consortium members also have access to an admin panel - figure 3.22. It allows them to add candidates before the voting period. And to start and stop the vote.

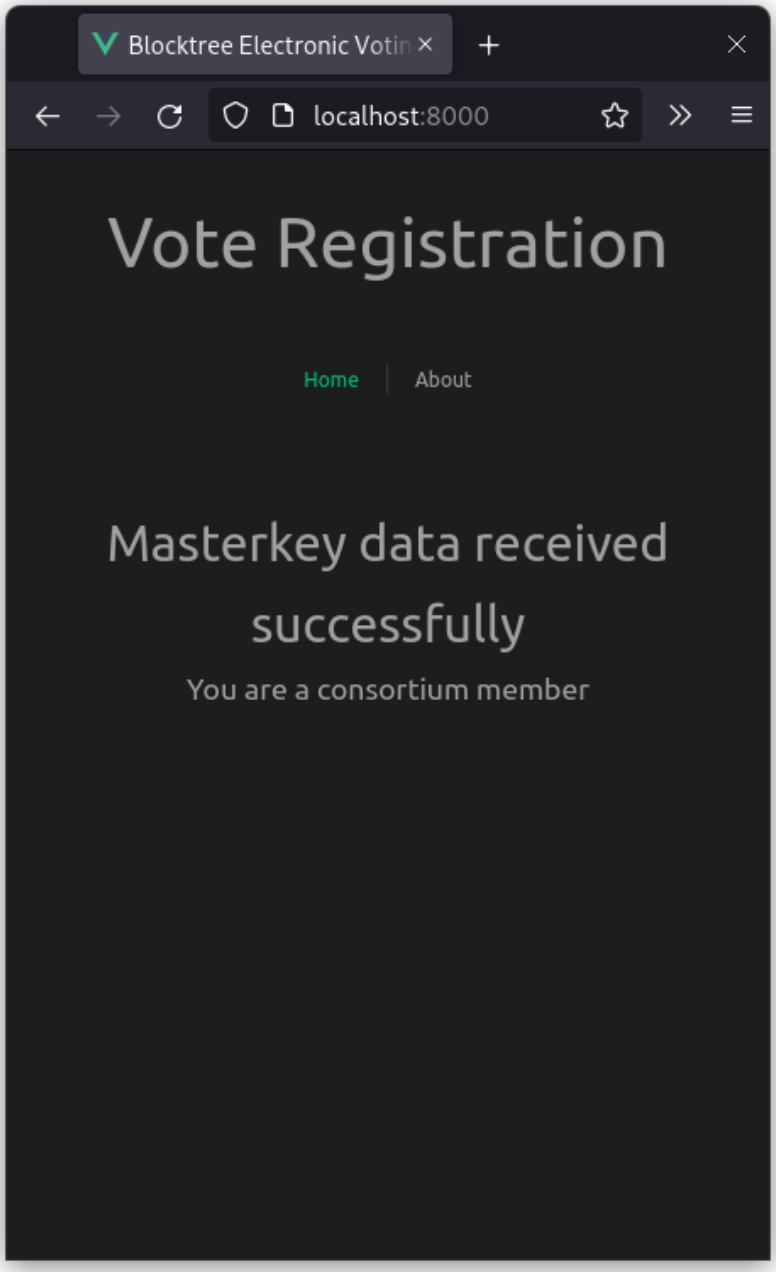

Figure 3.16: Receiving Master Key data

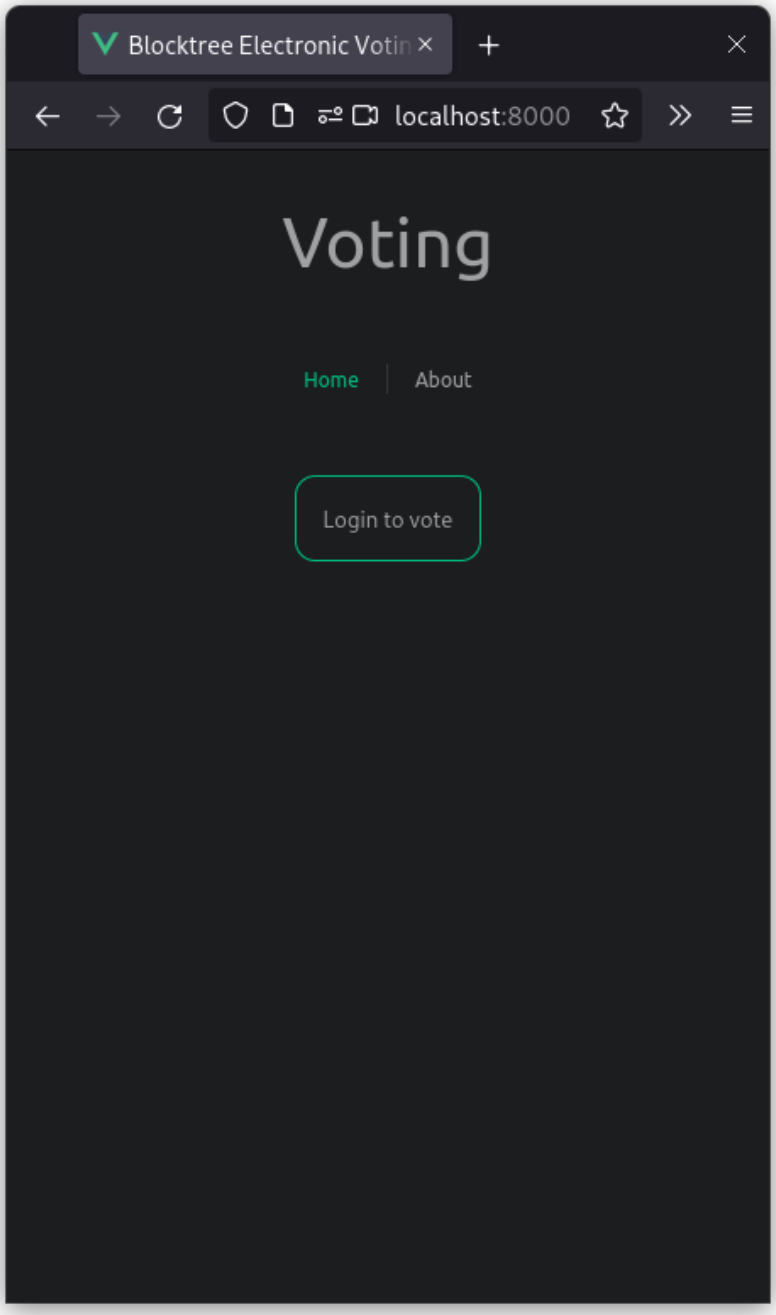

Figure 3.17: Login page.

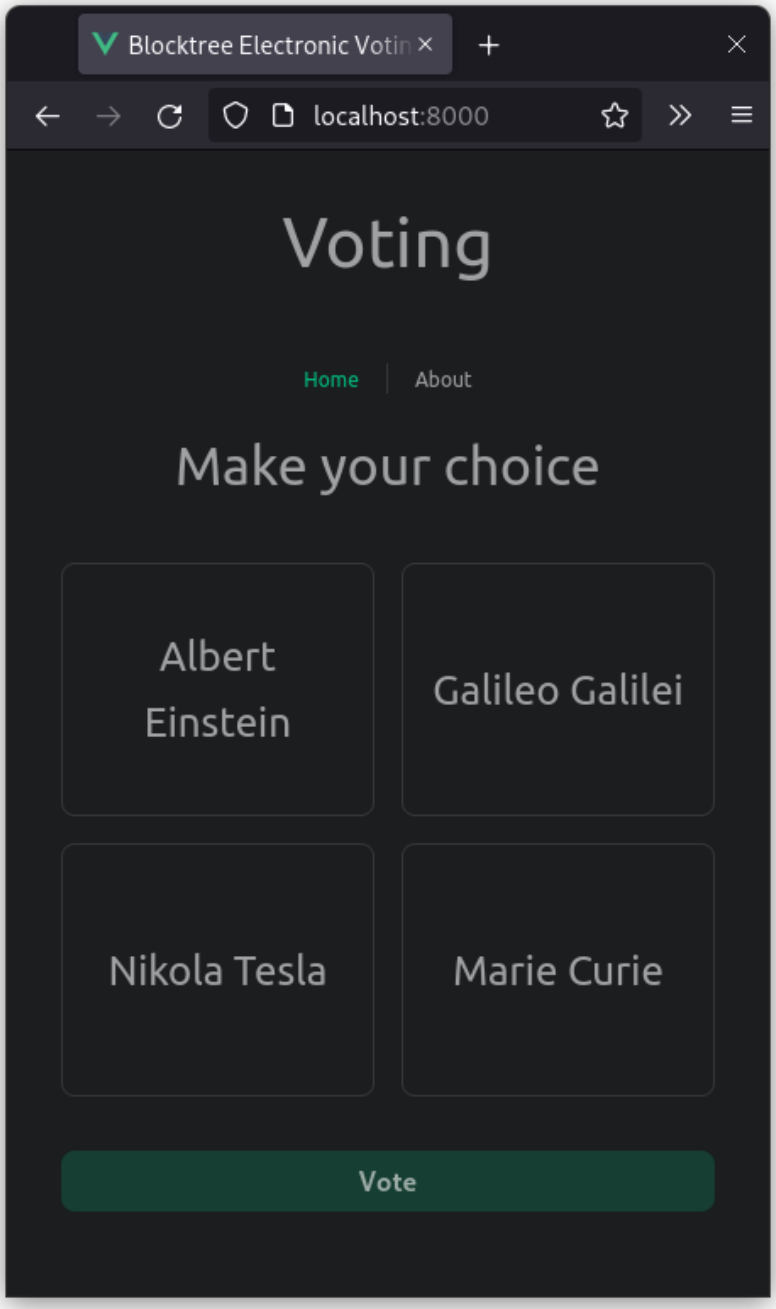

Figure 3.18: Voting interface.

Figure 3.19: Voting success.

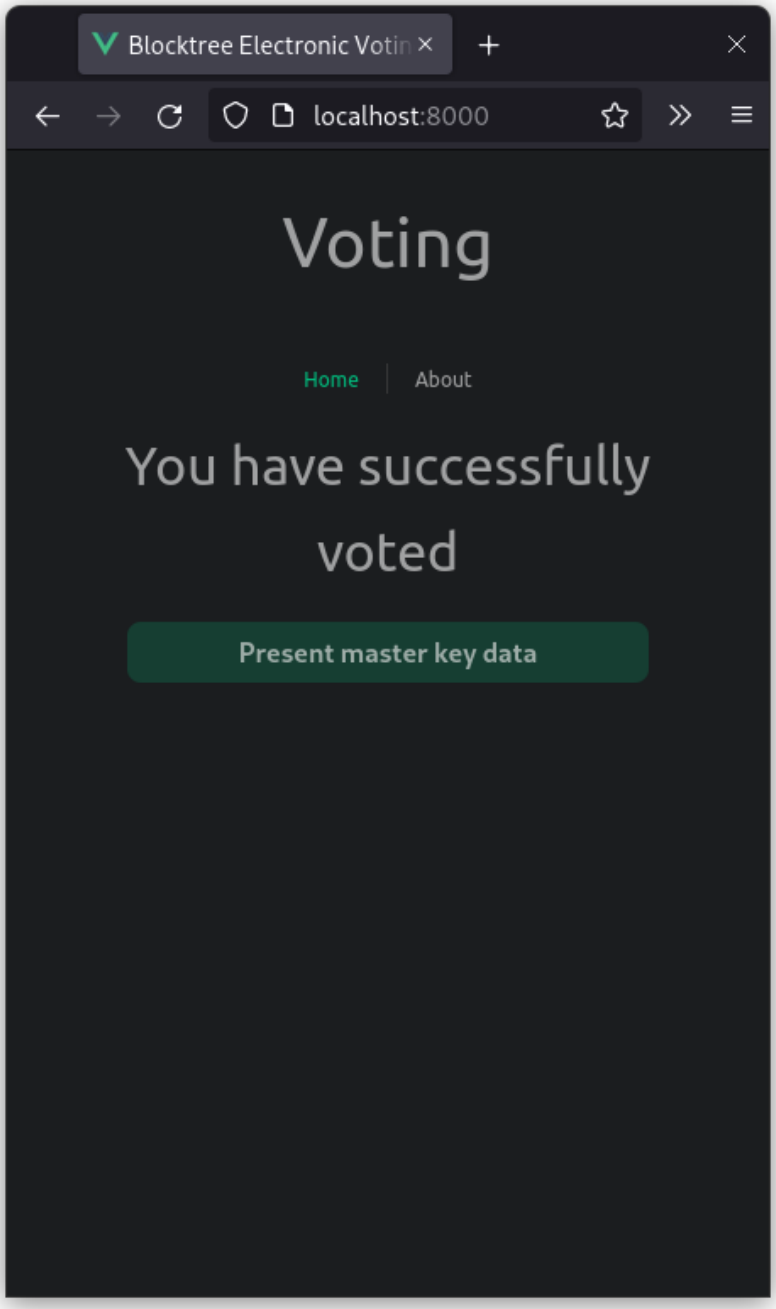

Figure 3.20: Presenting Master Key data.

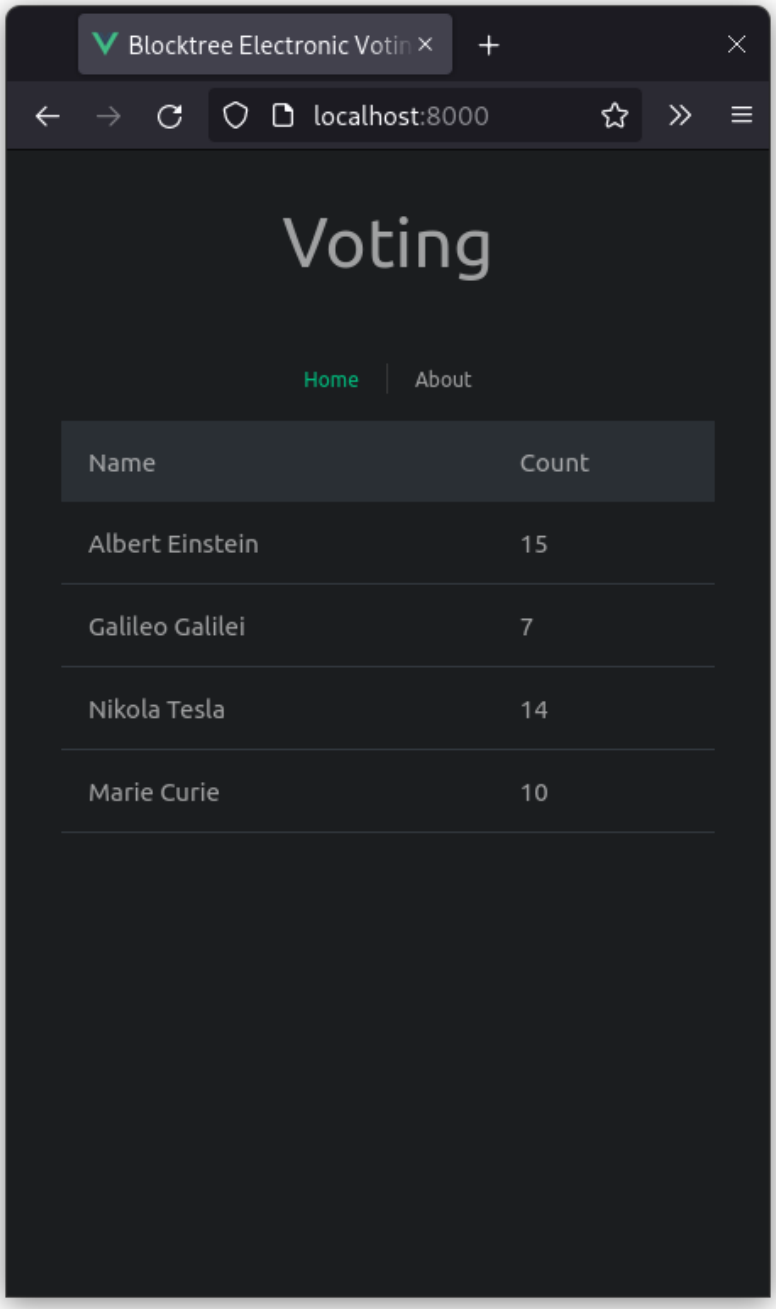

Figure 3.21: Results.

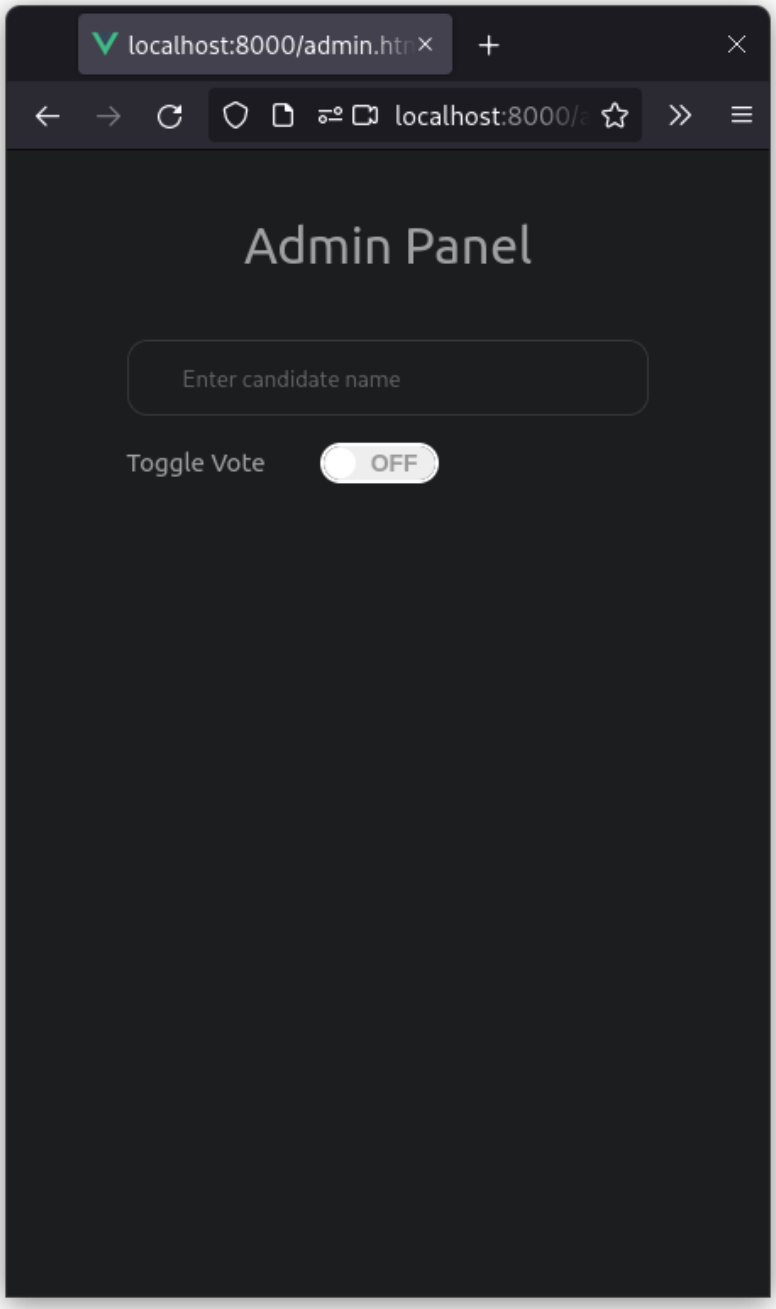

Figure 3.22: Admin panel.

7 System analysis

We have developed a robust Blocktree based voting system that olves the problem of lack of trust and transparency.

7.1 System properties

Our work respects the seven main requirements for voting systems [30]:

- **Universality**: Every eligible voter that follows the citizen's enrollment process has the ability to cast his vote wherever he is.
- **Equality**: Every vote counts as one, and every voter can only cast one vote.
- **Freedom** of choice: Voters can securely and safely cast their votes from their device.
- **Anonymity**: There is no link between a vote and its original caster.
- **Security**: No vote can be modified once made, and no fake vote can be introduced by malicious actors.
- **Directness**: Votes go directly to their chosen candidate.
- **Trust**: This system is trustworthy and all the previous conditions are met.

One other feature of our system is its resistance to strategic manipulations. It achieves this by hiding the advancement of the vote during the entire voting period, using a MasterKey. Every vote is encrypted on the voter's device and only decrypted at the very end. The decryption key is split amongst the consortium members in a special way : it can be recalculated when more than half the members are present.

8 Conclusion

In this work, we have proposed a voting system based on BlockTree technology that is robust, trustworthy and is applicable in many voting scenarios, from small community voting to large scale elections.
An improvement to this voting system would be the implementation of a better vote counting method, like the Randomized Condorcet method.

GENERAL CONCLUSION

In many different application fields around the world, blockchain has demonstrated its efficiency in the areas of security and decentralization. It has introduced a number of novel concepts and ideas to the research community by putting forth a fresh way of thinking about things without the need for a central authority. It relies on cryptography to keep the system secure and consistent across all network nodes that share a copy of the Blockchain.
In this work, we have developed a decentralized e-voting platform built on BlockTree technology. By encrypting every vote with a Master Key, we ensure the results are hidden until the end of the voting period. It is a compelling goal in contemporary society for these decentralized voting systems to increase the public political process's security, affordability, speed, simplicity, and transparency. This technique encourages a more open and transparent democracy by making it simple for voters to cast their ballots with only a click of a button. Through the internet, voters may confirm that their votes have been counted from anywhere in the world. With the help of this platform, it will be possible to hold an election without interference from a third party. It helps to save money and time while ensuring the integrity of the election and is more dependable and stronger than the traditional pen and paper ballot system.

BIBLIOGRAPHY

[1] CHELAGHMA Abdessamad. “Primitives Cryptographiques dans la blockchain”. In: (2021).

[2] Benjamin W Akins, Jennifer L Chapman, and Jason M Gordon. “A whole new world: Income tax considerations of the Bitcoin economy”. In: *Pitt. Tax Rev.* 12 (2014), pp. 1–25.

[3] R Michael Alvarez and Thad E Hall. *Point, click, and vote: The future of Internet voting*. Brookings Institution Press, 2003.

[4] Nafie Asfour. “Role of blockchain and smart contracts in transforming social contracts”. MA thesis. İbn Haldun Üniversitesi, Lisansüstü Eğitim Enstitüsü, 2019.

[5] Mohammed Awad and Ernst L Leiss. “The evolution of voting: analysis of conventional and electronic voting systems”. In: *International Journal of Applied Engineering Research* 11.12 (2016), pp. 7888–7896.

[6] Paul Baran. “On distributed communications networks”. In: *IEEE transactions on Communications Systems* 12.1 (1964), pp. 1–9.

[7] Jaume Barcelo. “User privacy in the public bitcoin blockchain”. In: *URL: http://www. dtic. upf. edu/jbarcelo/papers/20140704 User Privacy in the Public Bitcoin Blockc hain/paper. pdf (Accessed 09/05/2016)* (2014).

[8] Nathanaël Barrot. “Sur les aspects computationnels du vote par approbation”. PhD thesis. Université Paris sciences et lettres, 2016.

[9] Imran Bashir. *Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more*. Packt Publishing Ltd, 2020.

[10] Benjamin B Bederson et al. “Electronic voting system usability issues”. In: *Proceedings of the SIGCHI conference on Human factors in computing systems*. 2003, pp. 145–152.

[11] Alex Biryukov, Dmitry Khovratovich, and Ivan Pustogarov. “Deanonymisation of clients in Bitcoin P2P network”. In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. 2014, pp. 15–29.

[12] Denis Bouyssou, Thierry Marchant, and Patrice Perny. “Théorie du choix social et aide multicritère à la décision”. In: *Concepts et méthodes pour l'aidea la décision* 3 (2005), pp. 235–270.

[13] Felix Brandt et al. *Handbook of computational social choice*. Cambridge University Press, 2016.

[14] *Centralized, Decentralized and Distributed Networks*. July 12, 2021. URL: https://www.gemini.com/cryptopedia/blockchain-network-decentralized-distributed-centralized.

[15] David Churchman. “Voting Systems”. In: *The Palgrave Encyclopedia of Peace and Conflict Studies*. Cham: Springer International Publishing, 2019, pp. 1–6. ISBN: 978-3-030-11795-5. DOI: 10.1007/978-3-030-11795-5_62-1. URL: https://doi.org/10.1007/978-3-030-11795-5_62-1.

[16] Ittay Eyal and Emin Gün Sirer. “Majority is not enough: Bitcoin mining is vulnerable”. In: *International conference on financial cryptography and data security*. Springer. 2014, pp. 436–454.

[17] Dan S Felsenthal and Moshé Machover. *Electoral systems: Paradoxes, assumptions, and procedures*. Springer Science & Business Media, 2012.

[18] George Foroglou and Anna-Lali Tsilidou. “Further applications of the blockchain”. In: *12th student conference on managerial science and technology*. Vol. 9. 2015.

[19] Peter Froystad and Jarle Holm. “Blockchain: powering the internet of value”. In: *Evry Labs* (2016).

[20] Simson Garfinkel and Gene Spafford. *Web security, privacy & commerce*. " O'Reilly Media, Inc.", 2002.

[21] Stuart Haber and W Scott Stornetta. “How to time-stamp a digital document”. In: *Conference on the Theory and Application of Cryptography*. Springer. 1990, pp. 437–455.

[22] Lê Nguyên Hoang. “Strategy-proofness of the randomized Condorcet voting system”. In: *Social Choice and Welfare* 48.3 (2017), pp. 679–701.

[23] Jerry S Kelly. *Social choice theory: An introduction*. Springer Science & Business Media, 2013.

[24] Ahmed Kosba et al. “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts”. In: *2016 IEEE symposium on security and privacy (SP)*. IEEE. 2016, pp. 839–858.

[25] Germain Kreweras. “Aggregation of preference orderings”. In: *Mathematics and Social Sciences I: Proceedings of the seminars of Menthon-Saint-Bernard, France (1–27 July 1960) and of Gösing, Austria (3–27 July 1962)*. 1965, pp. 73–79.

[26] Gilbert Laffond, Jean-Francois Laslier, and Michel Le Breton. “The bipartisan set of a tournament game”. In: *Games and Economic Behavior* 5.1 (1993), pp. 182–201.

[27] Jean-François Laslier. *Tournament solutions and majority voting*. 7. Springer, 1997.

[28] L Leslie. “The part-time parliament”. In: *ACM Transactions on Computer Systems* 16.2 (1998), pp. 133–169.

[29] Christian List. “Social Choice Theory”. In: *The Stanford Encyclopedia of Philosophy*. Ed. by Edward N. Zalta. Spring 2022. Metaphysics Research Lab, Stanford University, 2022.

[30] Margaret McGaley. “E-voting: an Immature Technology in a Critical Context”. PhD thesis. National University of Ireland Maynooth, 2008.

[31] *Media And Elections*. 2012. URL: https://aceproject.org/ace-en/topics/me/med/med04/med06/default.

[32] Sarah Meiklejohn et al. “A fistful of bitcoins: characterizing payments among men with no names”. In: *Proceedings of the 2013 conference on Internet measurement conference*. 2013, pp. 127–140.

[33] Hilary Miezah. *Elections in African Developing Democracies*. Springer, 2017.

[34] Roger B Myerson et al. “Fundamentals of social choice theory”. In: *Quarterly Journal of Political Science* 8.3 (2013), pp. 305–337.

[35] Satoshi Nakamoto. “Bitcoin: A peer-to-peer electronic cash system”. In: *Decentralized Business Review* (2008).

[36] Arvind Narayanan et al. “Bitcoin and cryptocurrency technologies”. In: *Curso Elaborado Pela* (2021).

[37] Charles Noyes. “Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning”. In: *arXiv preprint arXiv:1601.01405* (2016).

[38] Gareth W Peters, Efstathios Panayi, and Ariane Chapelle. “Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective”. In: *arXiv preprint arXiv:1508.04364* (2015).

[39] Jonne Saajos. “Guide to Blockchain Technology”. In: (2022).

[40] Fahad Saleh. “Blockchain without waste: Proof-of-stake”. In: *The Review of financial studies* 34.3 (2021), pp. 1156–1190.

[41] Bruce Schneier. *Secrets and lies: digital security in a networked world*. John Wiley & Sons, 2015.

[42] Mike Sharples and John Domingue. “The blockchain and kudos: A distributed system for educational record, reputation and reward”. In: *European conference on technology enhanced learning*. Springer. 2016, pp. 490–496.

[43] Meng Shen, Liehuang Zhu, and Ke Xu. *Blockchain: empowering secure data sharing*. Springer, 2020.

[44] Harsh Sheth and Janvi Dattani. “Overview of blockchain technology”. In: *Asian Journal For Convergence In Technology (AJCT) ISSN-2350-1146* (2019).

[45] *Table of Electoral Systems Worldwide*. May 23, 2017. URL: https://web.archive.org/web/20170523184045/http://www.oldsite.idea.int/esd/world.cfm.

[46] Sudeep Tanwar. *Blockchain Technology: From Theory to Practice*. Springer Nature, 2022.

[47] T Tibbetts and S Mullis. “MPR: Challenged ballots: You be the judge”. In: *Minnesota Public Radio. Retrieved December* 15 (2008), p. 2008.

[48] Dylan Yaga et al. “Blockchain technology overview”. In: *arXiv preprint arXiv:1906.11078* (2019).

[49] Yu Zhang and Jiangtao Wen. “An IoT electric business model based on the protocol of bitcoin”. In: *2015 18th international conference on intelligence in next generation networks*. IEEE. 2015, pp. 184–191.

[50] Zibin Zheng et al. “An overview of blockchain technology: Architecture, consensus, and future trends”. In: *2017 IEEE international congress on big data (BigData congress)*. Ieee. 2017, pp. 557–564.