ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

NEUMANN JÁNOS
FACULTY OF INFORMATICS

THESIS

OE-NIK Student's name: **Dániel Tóth**
2021 Student's registration number: **T/006099/FI12904/N**

Óbudai University
John von Neumann Faculty of Informatics
Institute for Cyber-physical Systems

THESIS WORK SPECIFICATION

Name of the student:	**Dániel Tóth**
Identification number of the student:	T/006099/FI12904/N
Neptun's code:	[redacted]

Title of the thesis:

Blockchain-based evoting system
Blokklánc-alapú elektronikus választási rendszer

Internal supervisor	Ernő Rigó
External supervisor:	
Deadline:	15 December 2021
Subjects of the final exam:	Computer Architectures Cloud service technologies and IT security specialization

The task:

The rise of Bitcoin and other cryptocurrencies have changed the landscape of the financial markets. However, the technology behind these elements is not only capable to represent monetary assets, but can be used for various fields in life, such as IoT, healthcare, e-governance and so on. The aim of the thesis is to explore possibilities of developing an electric voting system based on blockchain technology. Characteristics, such as decentralization, transparency, security and efficiency make this approach a good fit and are crucial to eliminate several concerns over digitalized elections as well as improving election turnout by making collective decision making more accessible. The goal of this task is to identify the pros and cons of a digitalized election system compared to the traditional methods and to create and test an example electric voting system that tackles existing issues using blockchain technology.

The thesis must contain:

- results of the literature research on traditional and modern electronic electoral systems,
- results of research on blockchain based technologies, focusing on application in the target environment,
- identification of electoral challenges that could be solved using blockchain technology, including analysis of suggested solutions,
- requirements and implementation plan for a digitized voting system based on blockchain technology, including test criteria, test methods and expected results,
- detailed description of the implementation and evaluation of test results,
- summary of lessons learned and identification of possible improvements.

Place of stamp

.....
Dr. Rita Fleiner
head of institute

This specification is valid until: **15 December 2023**
(According to OE TVSz 55.§)

I consider the thesis suitable for submission:

.....
external supervisor

.....
internal supervisor

STUDENT'S DECLARATION

I the undersigned student hereby declare that this degree project / thesis is the result of my own work; I have disclosed the references and tools used in an identifiable manner. The results indicated in my degree project / thesis completed may be used by the university and the institution announcing the task for their own purposes free of charge.

Dated: Budapest, 13.05. 2021.

Tóth Dániel

.....

student's signature

CONSULTATION LOG

Student's name: Tóth Dániel

Neptun code: [redacted]

Specialty: Full time training

Phone number: [redacted]

Mailing address (e.g. domicile): dantoth55@icloud.com

Degree project / thesis[1] title in Hungarian:

Blokklánc-alapú elektronikus választási rendszer

Degree project / thesis[2] title in English:

Blockchain-based evoting system

Institutional supervisor: Rigó Ernő

External supervisor: -

Please write the data in printed capital letters!

Occ.	Date	Content	Signature
1.	02.23.2021	DISCUSSION OF THESIS TOPIC AND REQUIREMENTS	
2.	03.10.2021	DISCUSSION OF THEORETICAL ASPECTS OF THE PROJECT	
3.	04.14.2021	DISCUSSION OF TECHNICAL ASPECTS OF THE PROJECT	
4.	05.05.2021	STATUS UPDATE AND DISCUSSION OF POSSIBLE IMPROVEMENTS	

The Consultation log is required to be countersigned by either supervisor on a total of 4 occasions of consultation.

The student has complied with the requirements of the subject titled Degree project I / Degree project II (BSc) or Thesis 1 / Thesis 2 / Thesis 3 / Thesis 4[3], and is allowed to proceed for reporting / defense[4].

Dated: Budapest, 05.13.2021

.....
institutional supervisor

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Faculty of Informatics

CONSULTATION LOG

Student's name:	Neptun code:	Specialty:
Tóth Dániel	[redacted]	Full time training
Phone number:	Mailing address (e.g. domicile):	
[redacted]	dantoth55@icloud.com	

Degree project / thesis[1] title in Hungarian:

Blokklánc-alapú elektronikus választási rendszer

Degree project / thesis[2] title in English:

Blockchain-based evoting system

Institutional supervisor:	External supervisor:
Rigó Ernő	-

Please write the data in printed capital letters!

Occ.	Date	Content	Signature
1.	09.17.2021	DISCUSSION OF THE CURRENT STATE OF THE THESIS AND PLANNING THE TECHNICAL DEVELOPMENT	
2.	10.09.2021	DISCUSSION ABOUT THE FRONT-END AND BACK-END CONNECTIONS	
3.	11.06.2021	STATUS UPDATE AND DISCUSSING TESTING METHODS	
4.	12.01.2021	FINAL INTERNAL EVALUATION AND POSSIBLE IMPROVEMENTS	

The Consultation log is required to be countersigned by either supervisor on a total of 4 occasions of consultation.

The student has complied with the requirements of the subject titled Degree project I / Degree project II (BSc) or Thesis 1 / Thesis 2 / Thesis 3 / Thesis 4[3], and is allowed to proceed for reporting / defense[4].

Dated: Budapest, 12.06.2021

.....
institutional supervisor

Contents

1 Introduction

1.1 Issues and challenges in current electoral systems

Democracy has been the most successful form of government in human history, but this system also has its flaws. In 2021, there are 195 countries in the world, of which 193 are members of the United Nations. As the so-called Democracy Index [1] indicates - which is a study compiled by the Economist Intelligence Unit (EIU) every year, measuring the state of democracy in 167 countries - only 23 of them can be categorized as ”full democracies”, 52 are described as ”flawed democracies”, 35 as ”hybrid regimes” and 57 countries belong to the ”authoritarian regimes” group. This research is based on 60 indicators grouped in five different categories, measuring pluralism, civil liberties, and political culture. Since this index was made by a UK-based private company, the results should be taken with a grain of salt, but it is safe to say that the majority of the world's population have met with some kind of elections in their lives, whether it was a general election, a referendum or any other kind of occasion where the people had the authority to decide.

The campaign methods and the freedom of the press differ hugely between states. Lack of open political debate can lead to poorly informed voters - this is an issue that is often noted for countries in the ”flawed democracies” group. Foreign interference and gerrymandering (the practice of changing boundaries of electoral districts to gain an unfair political advantage) are also often repeated phrases when it comes to lower-level democracies [2]. Elections may use different methodologies to help the decision-making process, but almost all of them are prone to flaws such as electoral fraud or the high cost of operation. Most common electoral frauds are based on human nature, something that systems barely can counter. These issues are happening mostly before the actual election process begins. Notable examples are vote-buying (in which a party or politician seeks the support of a voter in exchange for money, goods, or services), artificial migration (in which a large number of voters move into a different area temporarily in order to support a local candidate).

There are also systematic issues [3] that are still happening even in modern societies, such as misleading ballot papers (purposely badly designed papers could lead voters to vote for the wrong candidate, supporting the other one), misrecording of votes (corrupting ballots using correction fluid, allowing duplicate, unsigned or unverified votes or altering the voting machines so that the vote intended for one candidate is given for another one), intentional destruction of ballots (it can be done only in small numbers since many invalid ballots could draw attention, but in case of a close race between candidates it could change the results) or simply tampering with electronic voting systems (through infecting machines with malicious code to favor a candidate or man-in-the-middle attack executed between the polling place and the vote-counting authority while transmitting data on the internet).

1.2 Research question and goal of the study

The foundation of democracy is transparency, perhaps it is crucial to ensure the integrity and the security of an election since it is a matter of national security. The focus of this study is to develop an e-voting system and conclude if a theoretical, functioning democracy, with a system working similarly to the current Hungarian parliamentary election system, could be improved through digitalization using blockchain technology? The goal is to eliminate issues during the voting and the vote-counting process by decreasing human factors and centralization.

1.3 Recommendations to address existing issues

The strength of the rule of law is a crucial factor to ensure legitimacy and meet international standards when it comes to free and fair elections. Incumbent governments ruled by dictators can use their powers of the executive to keep their power even against popular opinion. Entities can also interfere with elections using physical force, intimidation which can result in fake results. Even worse, if the regime has total control over the government (via supermajority or through military power), sham elections could be held - a show which has no significant political choice or impact whatsoever. They are concluded in order to appear to be the legitimate ruler of a state. There were examples of these practices in the 1929 and 1934 elections in Fascist Italy or even nowadays in North Korea. Ballots may contain only one candidate or option, and even if they had more choices, people who went against the will of the regime could face persecution. These are issues that are nearly impossible to counter with a machine or software.
This research mainly focuses on developed democracies, which intend to improve their current systems and ensure the legitimacy of future elections. General elections tend to be very costly by nature: the whole organization process, human resources, rental of polling stations, and election equipment are all expenses to be paid by the government - hence the taxpayers. There are existing solutions for digitalized voting, but still, the vast majority of votes are handled by pen and paper. On the 43rd General Election of Canada [4] - a country known to be one of the most open societies and ranked among the best full democracies of the world - held on 21st of October, 2019 the estimated cost was $502 million or approximately $18.35 for each registered elector. These numbers are seemingly high for an advanced democracy with little to no corruption. Most of these processes could be substituted for a fully automated mechanism while increasing transparency, security, and efficiency of the election. The recommended solution is to use distributed ledger technology - in this case, Ethereum, which is a well-established open-source blockchain that allows deploying automatically executing custom scripts called smart contracts. This system would require basically no hardware to upkeep, as it is a publicly run environment. The ways this new system shall be integrated, and if it's worth

changing existing procedures, be concluded later in this study.

2 Foundations of modern democracies

2.1 Origins and characteristics

The roots of democracy lie deep in human history. The word itself originates from the Greek language, namely built up from 'demos' (people) and 'kratos' (rule) words, but it wasn't ancient Greece where this decision-making structure first appeared [5]. Its first forms were identified by anthropologists from the age of hunter-gatherers, who lived before the first known agrarian establishments. These groups or sedentary societies are called proto-democracies, commonly identified as tribalism. Generally, 50-100 individuals formed small communities, consisting of closely tied families. Decisions in important questions were often reached by consensus or majority without any involvement of a tribal chief [6]. This system could only work to a certain point. Later on, seeing more complex societies forging and the higher the population grew, the more could other forms of rules - such as monarchy, aristocracy, and other authoritarian systems - emerge to the politics. Even in modern times, there is no generally accepted definition for democracy, but each and every article one can find will state that it means a type of government in which the supreme power is originated from the support of the people. It is a set of ideas and principles about freedom in an institutionalized way. It is important to point out that democracy comes in many shapes. One can differentiate between direct and representative democracies (differing in the decision-making process), constitutional and non-constitutional democracies (differing on popular sovereignty and the strength of constitutional rules), federal and unitary democracies (differing in the division of power), and presidential and parliamentary democracy (differing in the executive and legislative branching) [7]. All of these ideas share the same core characteristics [8]:

- All adult citizens can exercise their power and civic responsibilities directly or through their elected representatives.
- Democracy is built upon the principles of majority rule and individual rights. These rights shall be protected against absolute-power central governments, meaning that all levels of government must be accessible and responsive to the people.
- Basic human rights - such as freedom of speech and religion, right to equal protection, and the opportunity to organize and participate fully in the political, economic, and cultural life of society - must be protected.
- Free and fair elections must be conducted for the citizens of voting age.

2.2 Historic implementations

The first known historical examples of democracies are originated from the land between the Euphrates and Tigris rivers, **Mesopotamia** [9]. The political history of this empire shows that the government system that was used is very similar to today's democracy. This specific government system that was prevalent in Mesopotamia is known as the "primitive democracy". The primitive democratic government is considered a very loose power structure. The government system of the early Sumer was a king-like power structure, and the rulers of Mesopotamia continued with the same power system. But the power system of autocratic power was not used by the ancient Sumer rulers, which started in Mesopotamia later on.

Democracy, which was prevalent in Mesopotamia, is mainly used in the tribalism and smaller societies of the world. In the primitive democratic power system, the main authority remains in the major city-states, and there were the councils of the elders for making important decisions related to the specific area and specific problem. These councils consisted of the young men who used to make all the important decisions under the supervision of the king. In this government, there was an assembly of the elective peoples, and these people were elected by the people through the vote. The opinion of those elected people was very important as they used to represent the people of their areas. King had to consider the opinion of those elected people while making decisions.

The laws of the country are made by the government and other representatives according to the prevailed government type in that country. In Mesopotamia, the laws were made by the king of the empire, and every individual had to obey the orders of the king. In every city-state, the royal families were present, and there were separate military and assemblies for each city-state in that ruling system. Moreover, every city-state had its own kings, which were subordinate under the power of the main king of the empire. The written law system was first introduced here as well (The Code of Hammurabi).

For the next example, we have to skip a couple of centuries. As mentioned before, the word democracy came from the Greek language. It is safe to say that **Greece** is considered the father of democracy. This democratic system was a little different from the modern democratic ruling systems, but Greece's philosophies and politics are the basis of modern democracy. In ancient Greece, there was a city-state system in which every city-state had its king and representatives to run the assembly. All these city-states were under the supervision of one king. In most cases, these city-states used to fight against one another. Athens and Sparta were prominent city-states that used to fight against one another in ancient Greece.

There were four different types of government systems in the ancient Greek government [10]. The democratic system in which the ruling was made through the male people. Monarchy system in which the power was inherited. The third one was the oligarchy, in which the group of peoples was chosen for ruling the state. But one of the best sys-

tems in ancient Greece was the Democracy system. Ancient Greece democracy has also influenced modern democracy. In the ruling system of ancient Greece, young and adult citizens were required to take part in all government activities. In terminology, this type of system is known as direct democracy.

In a direct democracy, all people take part in building important laws for the country through direct voting. In the ancient Greece political system, every citizen had an equal chance to take part in economic decisions and to become an official in any department of the country. The main purpose of this system was to promote equality in all things. Even for making the army generals, voting was done. According to the rules of the country, only the nationals could take part in the voting. In this system, the main government bodies were the assembly and court. There were a total of 500 members in the assembly who were elected through voting. The courts were used for judge and jury of public issues. For a public lawsuit jury, 201 people were required, and for a public lawsuit jury, this requirement is 501 people.

Another important phase comes from the western neighbor of Greece across the Mediterranean, **Rome** [11]. There was also a senate along with the assembly in the roman democracy system. The members of the senate were the aristocratic people. Once a member became a member of the senate, He became for his whole life. But the main requirement for becoming a member the first time was to be an official. Due to these assembly and senate systems, there were some conflicts between both the representatives. Even it was a democratic government, but there was some dictatorship in the country because the king had the authority to choose his favorite people as the members of the assembly and senate. The king had the authority to announce an emergency in the country that is why this system was entirely not democratic.

During the democratic era, an official was chosen by the plebeian group who had some conflicts with commoners over many issues. This selected official favored the military instead of the democratic system. As a result, the power of the military in the roman empire increased, and it affected the democratic ruling system very badly. But both the commoners and plebeians made many improvements in the ruling systems to make democracy strong. The assembly system was made by the commoners in 471 BCE, and this step had much importance in roman democratic history. The democratic ruling system allowed the plebeians to choose officials through democracy for making important laws and passing the legislation. Judiciary and legislation systems were very similar to the modern democratic systems in the Roman empire.

The ruling system, which was prevalent in the **middle ages**, is called feudalism [12]. This system was used from 9 to 15 centuries. This system is a combination of various systems like the economic system, military system, cultural system. This system started after the fall of the Roman empire. This system was the combination of various subsystems which worked under the supervision of the king. The king had the authority to punish anybody

according to his own will. All the rules were made by the king, and the opinion of other representatives had no importance. But in some cases, the king used to ask for the opinion of the representatives of the people. The final decision was made by the king himself. The king had the authority to decide according to his will in any matter. This system was not the actual form of democracy. But the democratic ideas were followed in this system because more people were following Christianity. Christianity teaches the values of equality and freedom of speech. That is why many democratic ideas were followed by this ruling system. The feudalism system started broken down at the end of the 14th century in some parts of this empire.
In the feudalism system, only men had the right to become lords. These lords owned the lands and extravagant homes. People were the subservience under the specific landlord in this system. The middle ages era was the start of the evolution of democracy after the 15th century. With the passage of time, the trend of democracy increased after the 15th century, and the feudalism system was gradually converted to the actual form of democracy until the mid of 18th century. Thus era is the actual start of modern democracy. In England and many European countries, the democracy system started after the civil war, ideology, and belief in equality and freedom. After the 18th century, the first time the power of the king was reduced. Then in some areas of Europe, more rights were given to the parliament. In Europe, Poland was the first country in which parliament got more rights, and the power of kings was reduced. It was the result of some wars due to which local power got much importance in the middle ages.

2.3 Western democratic governments in the modern-era

Democratic governance is categorically characterized by freedom of expression and opinion. But lately, a drastic threat to modern democracies has been observed even in the western world that tends to suppress the masses, especially in the European Union. The major factors that further enhance the intensity of such threats are increased authoritarianism and populism. Democratic societies in the western world are typically characterized by independent media that act as a mouthpiece to public opinion, no matter even if it tends to challenge the potential authorities.
We see digital media changing the whole picture of democracy by being the easiest way to communicate and express for the masses. Reforms in the electoral process tend to be the most important factor in democratizing the western world. The elections themselves are a visible representation of democracy in the western world, which lets the citizens play a vital role by expressing their ideas about how they want to be governed. That very fact makes the EU focus even more keenly on the electoral rights of citizens.

2.3.1 The European Instrument For Democracy and Human Rights

EIDHR is a tool that ensures democracy, fundamental rights, and human rights, empowering the civilians with democratic rights in the area of politics [13]. Civil society ultimately becomes a vital force in all regards. EIDHR is unique in regards to its matchless features playing a vital role in various other assistance tools designed by the European Union in order to ensure democracy and human rights. It will not be wrong to say that it is a valuable addition to EU policy structures.
EIDHR has a scope on the global level, is equipped with the potential power to be able to address critical issues such as torture, restriction of speech, death penalties, and a lot more. To be precise, it is mainly aimed at the following objectives:

- Back the human rights defenders up in their course of service to provide human rights and democracy. Moreover, to get them all covered up in threatening situations.
- To support the basic democratic system and ensure its implementation in the governance, fighting off public oppression at all steps.
- To keenly focus on the electoral systems through European Union Election Observation Mission enabling the masses to elect their government.
- Supporting all other national and regional instruments designed for the maintenance of a stronger Democratic system and human rights.

2.4 Electoral systems in the 21st century

The Presidential elections in a state call for a crucial event with huge public interests, especially if it is a presidential form of government. In this section, I analyze the presidential elections of three different states. French elections differ quite significantly in regards to the procedure from the USA elections and Hungarian elections.

2.4.1 United States of America

Who can become a President in the US, and what is the election procedure? The eligibility criteria for an individual who aspires to serve as the president of the United States of America is quite clearly defined in Article 2 of the US constitution. According to this provision, any individual at the age of 35, an American national (naturally born citizen), and residing in any of the states of America for at least 14 years can be a candidate for presidential elections.
Starting a campaign does not require being exactly 35 years old as far as the candidate reaches the required age as by the Inauguration day. Another important point to remember

is the convention that later popped up as the 22nd Amendment to the constitution that limits the number of terms of a president to two. The USA President is not directly elected by the people but through an electoral college. The following part describes the steps of the procedure:

1. Primary and Caucus: 34 out of 50 states in the USA conduct primary, a state-level election where the parties elect the candidate who can best represent them in the general election. These elected candidates then stand as opposites in the general elections. The rest of the 16 states undergo another process called the caucus. We might define the caucus as a local meeting before selecting delegates from the political parties to the national party convention. It takes place in the respective towns or cities.

2. National Convention: The national convention comes up with the party nomination for the president, which takes place as people directly vote for delegates, and then the elected delegates vote for any of the party candidates of their choice. The national convention finishes here and comes up with the beginning of the general election procedure.

3. General Elections: General elections usually take place in November every five years. American citizens are basically the members of the electoral college and not the president. These electors then vote for the president.

   Electing these members is like authorizing them to elect the president on behalf of public opinion. People from all states across the USA take part in the voting to vote for a President and a Vice President.

   An institution called the electoral college comprises these elected members who are now constitutionally authorized by the public to elect the president.

   There is no such thing as a popular vote in the USA constitution. This means that even if a candidate wins the maximum number of votes if it is not more than 270, the candidate does not secure his position in such a case. The House of Representatives steps in if that is the case. Through voting by the members of the house of representatives, one of the top 3 candidates is elected to be the president. This happened once only in American history in 1824 when the House of Representatives elected John Quincy Adams.

4. More About the Electoral college: The president in the USA is elected through the electoral college. According to the constitution of the USA, the candidate with the maximum number of votes from the members of the electoral college serves as the president for the next five years. We presume that the framers of the constitution wanted to nominate a wisely polished group of people who would ultimately reflect public opinion to elect the president.

Based on representation in Congress, each state is granted a certain number of voters. For example, California, being the most densely populated state, has 55 electoral votes. The candidate securing more than half of the electoral votes, i.e., 270 out of 538, holds the office as president in the USA for a 5-years term.

2.4.2 France

France has a presidential form of government too, and each presidential election helped determine the president of France for the next five years, which was formerly seven. The presidential elections always take place on Sundays. So far, since the establishment of the Fifth Republic in 1958, 11 presidential elections have taken place in France. The president was not elected directly but through an electoral college that comprises parliamentarians, the general councils, the elected members of municipal councils, and last but definitely not least, the assemblies of the overseas territories. This makes a sum of 80,000 locally elected councilors in total.

President De Gaulle reformed the structure of presidential elections in France through the Constitutional Act of 6th November 1962. This Act introduced the two-round election system through which the president was to be elected directly by the people instead of an electoral college.

From the establishment of the Fifth Republic, 1958, till 24th September 2000, the presidential elections used to take place every seven years, which changed to a period of five years. The referendum proved to be a triumph, and thus, reduction of the term took place through a Constitutional referendum on 24th September 2000. Jacques Chirac, the president elected after September 2000 referendum in 2002, enjoyed a term five years long. Furthermore, the next elections were scheduled to be held in 2007 rather than 2009 as per history.

But how does the two-round election work? The candidates, to secure their position on the ballot, have to secure 500 signatures from officials like the members of the parliament and mayors who were elected as well. According to Article 7 of the French Constitution, the two-round election system was introduced in 1962 through an amendment according to which if all the candidates fail to secure an absolute majority of votes during the first round of elections, a second-round is held right after two weeks, in which the candidates with the maximum number of votes take part, and this round determines that who wins the presidential elections. The people vote for one of these two candidates. The first round is quite simple, the people directly vote for any officially eligible candidate; have secured 500 signatures of elected officials. The number of candidates settled somewhere between 6 to 10 or 12 every time since the establishment of the 2 round election system in 1965. Since 1965, all elections require a second round in order to deduce the results as no candidate has ever been successful in securing an absolute majority vote in French history.

2.4.3 Hungary

Indirect Presidential elections take place in Hungary every five years. The latest presidential elections were held on 23 March 2017, which resulted in János Áder was being elected as the president of Hungary for a second time for a term of 5 years.
The existence of a parliamentary form of government in Hungary makes the Prime Minister the state's sole power. The maximum power lies in the Prime Minister, who is elected by the national assembly of Hungary. Parlamentary elections take place in Hungary every four years. The Prime Minister is considered as the head of the government and thus exercises all the executive powers to the maximum extent. He has to be a member of the majority party of the Parliament, having the right of dismissal of the cabinet ministers as well. The Parliamentary form of a government undeniably suggests the merely ceremonial role of the president. So, the constitution of Hungary clearly defines the ceremonial role of the president of Hungary. He is deprived of maximum power. The period for a president cannot exceed two terms. The members of the National Assembly elect the president. It is suggested that the president of Hungary, after completing his two terms, leave his political party. Moreover, that is to ensure that he is not impartial or prejudiced towards his party. This very act builds up a sense of unity rather than an impartial political attitude. The members of the national assembly are then elected through two procedures. There are 199 members of the national assembly, to be precise. These 199 members ultimately elect the president. 106 members out of 199 are elected through the system of first past the post voting that refers to the voting procedure in which the voters directly vote for the candidates and the one with maximum votes is considered as the winner. The rest of the 93 members are elected through the proportional method in which the candidates require a 50% majority in order to secure their position. The first 106 members are elected in single-member constituencies, while the latter is from a single nationwide constituency. For a coalition of the parties during the elections, the electoral threshold is up to 15%, where it is generally only 5% and 10% in the case of two parties. Moreover, the D'Hondt Method [14] comes to help while the allocation of seats.

2.5 Conclusions

In this section, the study has covered the definition and characteristics as well as the origins of democracy. It was essential to understand these concepts since the research focuses on improving its core element, the electoral system, which allows people to practice their right to vote. The comparison of three developed western states' methods has shown that there are significant differences between systems, and they were briefly analyzed. Since the problems in the current electoral processes were identified, this study will continue with an overview of the technical aspects that will be the backbone of the proposed new electoral system.

3 Overview of Blockchain Technology Concepts

3.1 Cryptography

In this era of information, threats like hacking, data leaking, and data-stealing are at their peaks. According to the Peter Parker principle originated from Spider-man comics: ”With great power comes great responsibility”. Perhaps it makes sense that there should be some sort of system that will let us protect our data so that none other than the intended person can read it. This is why the term ”cryptography” is trending again. Specifically, in the world of blockchain-based technologies such as cryptocurrencies, cryptography is helping in improving digital storage and money.
Cryptography is the method used to protect information and data using complex codes that encrypt the information so that only the intended person can decipher and read it. It is more of a vault for information. This word also originates from Ancient Greek, the term ”kryptós” means hidden, and the term ”graphein” means to write. When we talk about cryptography in the Computer Science methodology, it simply means secure information or algorithms that are derived from complex mathematical concepts. Cryptography is used in areas like web browsing, online transactions, email, and areas where you will want to protect your privacy or to ensure that sensitive data is transmitted securely between a server and a client. We differentiate between three different types:

1. Symmetric-Key Cryptography: As the name suggests, this encryption method incorporates a single key. The same key is responsible for encrypting and decrypting. Symmetric-Key Cryptography is fast and efficient for decrypting large amounts of data.

2. Asymmetric-Key Cryptography: This encryption method uses two keys. An encryption and decryption key. Moreover, it is also called Public and Private Key. This type of Cryptography is also known as Public Key Cryptography.

3. Hash Functions: The only Cryptography that does not incorporate any type of keys. Hash Functions have a specific Hash Value in the form of plain text. Hash Function Cryptography takes random data and generates an enciphered text, also known as ”Hash.” Therefore, the Hash itself becomes the password that a user can then use to verify the credentials.

The primary need for cryptography occurred when the importance of security increased. Hence, it is responsible for preventing sensitive data from being read/stolen by people who are not intended to see it, as we all know that data is practically everywhere. From schools, hospitals, software houses to universities and the military, data is everywhere. There are hundreds of reasons why the world would want their data to be secured. In some cases, the threats can reach national or international levels. For example, the nuclear launching

code can lead to the next world war. It is hard to estimate the exact consequences of a data breach, but they are extreme in some cases.
Cryptography can be applied in many ways. It might sound surprising that this important concept of computer science is far from being a modern idea: its origin was way back in 2000. B.C. When Egyptians used to practice hieroglyphics (basically incomprehensible symbols), it was a great way to protect valuable and sensitive information without giving it to the enemies [15]. For example, a more often seen way of use in the past was rearranging letters and then deciphering them onwards. This is the basic use and concept of cryptography. Moving back to the modern era, cryptography nowadays is getting its power from complex mathematical algorithms and computers. These new possibilities and the security it might mean have become a challenge for the world's most famous computer scientists and mathematicians. This unique ability to make data incomprehensible is not only useful in our everyday lives. However, the main significance of cryptography comes in wars, too, and it was especially visible under World War II, thinking of the significance of the Enigma cipher and the successful efforts of its codebreaking, just to mention one. Even though cryptography is an old concept, it is timeless, and most likely, it will be around humanity until we exist.

3.2 History of blockchain technology

The popularity of this technology has been undoubtedly one of the big stories in the past decade. However surprising it may sound, the history of blockchain dates back to the early 1990s. The underlying methodology has been created by W. Scott Stronetta, and Stuart Harber in joint research work on a cryptographically secured chain of blocks that ensured no outsider could modify the timestamp of documents. Gradually the system was upgraded to include Merkle trees to enhance efficiency, allowing storing multiple documents on a single block.
The world had to wait until October 31, 2008, to see a breakthrough: that is when a so-called "Satoshi Nakamoto" has released the whitepaper of Bitcoin, calling it a peer-to-peer electronic cash system. It is unknown if Satoshi is a person or a group of people that worked on this project, but, indeed, this was the first successful conceptualization and application of digital ledger technology. Before we advance with this section, one must understand the differences between digital ledger technology and blockchain because there is a common misconception hearing these words. Blockchain is just a type of distributed ledger - technically a subset of it - but includes a sequence of blocks as well as proof of work and better scaling. It is designed to record transactions or digital interactions and bring better-defined attributes for its users. Distributed ledger technology does not necessarily require having a data structure in blocks but is merely a type of database that spreads across multiple regions or participants.
Ever since the release of the first whitepaper, we have seen a gradual increase in the ad-

aptation of the technology as well as the value of specific cryptocurrencies. Nowadays, we differentiate between three eras: Blockchain 1.0, the genesis of bitcoin, aiming to bring transparency and public access to an instant and secure global financial system. Developers started experimenting with the possibilities of the distributed ledger. This era was mainly focused on the creation of cryptocurrencies, but it is an essential stage of growth, as it was the first time in the world's financial history to see monetary transactions go completely decentralized, thus raising alarms for governments and other financial organizations. Throughout this era, blockchain has advanced staggeringly.
We mark the introduction of smart contract capabilities as the second big step, marching into the Blockchain 2.0 era. We mark the beginnings to November 2013, when Vitalik Buterin has described potential scripting language implementation for application development on the blockchain, perhaps proposing the development of Etherum. After successful crowdfunding in 2014, the network went live on July 30, 2015. Gaining instantaneous popularity, developers started working on creating more decentralized applications (DApps) and decentralized autonomous organizations (DAO). The history and evolution do not stop with Bitcoin and Ethereum: thousands of projects have emerged to introduce this new methodology into every single industry in the world economy.
Reasonably, Blockchain 3.0 is the era that will see significant institutional and enterprise adoption of this tech. This marks the final stage, as the growth will make blockchain technology widely accepted as an industry standard for internal, external operations and finances as well. Some argue that 3.0 is the last step of this evolution, as most of the projects in this era, such as EOS, were unsatisfactory solutions because of scalability-safety issues, lack of business-level infrastructure, and high cost of entry. The ultimate goal that could mark the 4.0 era is indeed a business-friendly and high-performance public chain that is capable of executing real-world use cases and applications while providing an open, decentralized platform for organizations of any size and type.

3.3 Features of blockchain technology

As previously mentioned, the introduction of this technology has indeed caused a social and financial earthquake, mainly attributed to the following features and advantages:

- Decentralization: In general, this term means that the transactions/interactions are happening between the participants without any governing authority or controlling individual. This might be the most important feature that caused the emergence of this idea. Rather than using central actors, a group of nodes or the participants themselves upkeep the system. This makes blockchain less prone to a general failure, gives control to its users to interact of their own will and produces a consistent, faultless result as it does not depend on human calculations. No third-party intervention decreases risk and increases trust.

- Immutability: A feature that is responsible for creating a corruption-free environment. The word itself means that something - in this case, data - cannot be changed or altered. Simply saying, it means that once a piece of information is recorded on the blockchain, they are time- and date stamped, acting as a permanent record that cannot be changed or deleted afterward. This is achieved through nodes operating in the system since all of them have a copy of the ledger. Transaction validation runs through these nodes, and if the majority approves its integrity, then it is added to the ledger.

- Security: Obviously, without a central ruling power over the network, no one is capable of simply changing any characteristics of the network. Moreover, since it is using encryption, it just lays another security wall called cryptography. This complex mathematical algorithm acts as a firewall for incoming attacks. Every single piece of information on the blockchain is hashed, perhaps hidden from the malicious eyes. The input algorithm produces different kinds of values of the same length and also initializes a method in the ledger that contains the hash of the previous block, so reversing its content is a hard nut to crack, impossible so to say. This is why private keys are used along the public keys to make transactions.

- Transparency and Privacy: While those two words may seem distinct at first, they are perfectly fit together in this world. Since almost all blockchains are publicly available (some are not public, Monero, for example), every single interaction can be tracked, validated. It is the transparent and accurate end-to-end tracking that provides trust between the participants in a blockchain. Every bitcoin wallet is technically available for the curious eyes (the balance, transactions, etc.), yet the owner's identity of this account is not public, and the network requires no identifications whatsoever. The control of the data or their balance is entirely through the private and public keys. This is an important feature when it comes to healthcare use-case, for example, ensuring patient privacy.

- Cost-efficiency: Blockchains are able to reduce manual tasks, creating more efficient solutions for institutions. Moreover, eliminating intermediaries from the process - or a third-party institution or service in this case - also helps cost-cutting.

- Speed: With no intermediaries and the transactions fully automated, and blockchain is capable of handling transactions significantly faster than the traditional banking system, users can initiate or receive transactions within seconds, no matter the distance between the two counterparts. This incredible pace assists more than just the financial use-cases and has been implemented in the biggest USA-based grocery store chain, Walmart. They have used blockchain to track food supply-chain, namely mango slices in the US and pork in China, with incredible results. In the

US, the time needed to trace the origin of mangos went from 7 days down to only 2.2 seconds.

These are the main qualities that could help in achieving the goal of this thesis: creating a transparent, reliable, and rigid general election system that ensures integrity and improves the current mechanisms significantly while upkeeping the very dear anonymity of its participants.

3.4 Use-cases

3.4.1 Supply chain

Blockchain technology proves to be quite an effective tool to manage supply chain projects in regards to recording certification, dates, quality, location, and others. To be the market leader in responsible manufacturing, one needs to ensure increased traceability, lower losses from the gray market, potentially enhanced visibility, and compliance over outsourced manufacturing. All this comes in hand with convenient access to critical information. This brings a handful of benefits like reduced risks, supply chain transparency, enhanced efficiency in management, thus ultimately helping you add on the business value tremendously.
Blockchain makes it practically easy to track the supply chain accurately so that end-to-end tracking is at your fingertips. You can track the physical assets from production to use by the end-user. Organization in a sequential manner tends to decentralize complete records of all the transactions. In the long run, it helps build a greater transparency extent to increase the visibility for the consumer as well. Potential benefits are:

- A supply chain project-driven through blockchain technology is potentially exposed to lesser risks as well as an overall reduced cost.
- Corporate standards of quality are easily approachable by the convenient and effective traceability of the material supply chain.
- Lower potential threats to losses from the counterfeit or gray market.
- A drastic decrease in the administrative cost by reducing the paperwork.
- Blockchain technology leads to greater transparency which in turn leads to increased transparency that develops a strong corporate reputation.
- Improvement of the credibility levels.
- Makes public relations safer.

Improved traceability means improved credibility and better sales. Blockchain technology is a source of increasing visibility and authenticity in order to win consumers' trust. On the other hand, consumers want a clearer picture of the businesses, insights, and traceable information. Not just that consumers are not ready to compromise on transparency, but also they are ready to pay premium prices for products that are more likely to be authentic due to visibility. A 2018 NielsenIQ [16] research suggests how 49% of the buyers will not mind going out of their way to buy products from companies that have greater visibility and traceability. Other big names like Walmart have been considering focusing on blockchain traceability solutions to ensure their supply chain visibility on both ends i.e., consumers' end as well as producers' end [17].

3.4.2 Financial services

Many well-known companies like Jaguar, Land Rover, Verizon, JetBlue, AirBnB, Daimler, and many others have been showing their keen interests in blockchain technology and then making partnerships with blockchain technology service providers in 2016 and 2017. Furthermore, this investment completely reflects how significantly effective blockchain technology is from the financial perspective.

Be it supply chain finance, project finance, management of treasury, any bank-related transactions typically that of investments or international payments, blockchain technology has been playing an efficient role in providing safer and easier channels transforming the concepts of transactions at the grass-root level. Supporting cryptocurrency is just one part. Blockchain technology has been revolutionizing mainstream banking as well, providing a clearer picture of all the financial details. And not that alone, blockchain technology tends to cut down various stress situations and hassles regarding financial transactions.

Royal Bank Of Canada has been seen investing in blockchain technology for financial transactions across the USA and Canada [18]. And this fact is something that makes the credibility levels of blockchain technology higher, making it even more appealing to be widespread across the globe. Moreover, experienced financial analysts presume that blockchain technology finds its easiest and most effective application in financial projects. Moreover, that is quite clear by hundreds of investment examples, such as the American Securities Exchange that had announced the investments in implementation strategies of blockchain in 2018.

The accurate history maintenance of transactions typically characterizes blockchain technology. Any unauthorized party cannot hack or alter the records, as all the records are sequentially arranged on a ledger, where hacking one part requires hacking the whole ledger, which requires about thousands of computers working together, which is practically quite impossible for the "unauthorized party". Such a fact might not sound impressive to somebody unaware of the technical complexities of financial transactions. However,

this is one of the biggest factors that makes blockchain technology immutable in a literal sense.
Blockchain technology finds its application in bank transactions to receive foreign remittances. Various international businesses involve huge financial transactions every year, which, when made through the traditional way, are quite expensive. Although bitcoin is being used as an alternative, remittances are moved through blockchain technology with is way more effective and secure as well as hassle-free. Many banks establish partnerships with various service providers for blockchain technology solutions to facilitate large amounts of international payments. Blockchain technology ensures saving your time as well as money. Traditional bank transfer for international transactions has to wait longer as well as pay a fee of 7% to 10%, while on the other hand, the same thing through blockchain technology takes a few clicks on your cell phone or desktop wallet application.

3.4.3 Smart contracts

Smart contracts might be defined as a contract that is self-executive, in which all the terms and conditions of the agreement decided by the buyers and sellers are written directly in codes. Nick Szabo, who is a first-generation Hungarian born in the US working as a computer scientist, first introduced the concept of smart contracts in 1994 [19]. He is also known for his contribution to the finance world by designing the mechanism of a decentralized digital currency he called "bit gold" in 1998.
The legal status of smart contracts is still debated. Implementation of the Decree on Development of Digital Economy in 2017 makes Belarus the first country that legitimizes smart contracts. US Senate too legitimized the smart contracts in 2018. Smart contracts, although they sound like something different, liabilities applied in the case of small contracts are typically similar to those applied on regular contracts under the contract law. Legislations on smart contracts have also found their way into legislatures of many American states such as Arizona and Nevada. However, what features make smart contracts beneficial?

- Efficient and accurate dealings: Being automated and digital makes smart contracts the fastest, most efficient, and accurate. Once the buyers and sellers are done with their dealing, the execution of the contract takes place automatically without any hassle of time-consuming paperwork and reconciling of errors that are very likely to happen in the manual handling of documentation.

- Transparency of Dealings: Smart contracts are end-to-end encrypted to ensure transparency and security of the content so that it might not be altered by any of the parties for any personal privilege. Transaction records are safe from all threats of involvement of any third party. So, trust issues are just out of the question in the case of smart contracts.

- Security Assurance: Security is something uncompromisable, and smart contracts make sure you do not have to compromise. The encryption of blockchain records ensures that the records never get leaked or altered. Being in a consecutive sequential chain makes each record safer, as the hacker would have to hack a whole chain in order to make even the slightest of a change in the respective data.

- Cost-cutting: Smart contracts go an extra mile saving money by cutting down unnecessary intermediate expenses such as the person hired in order to look after transactions and other manual operations that are automatically executed in case of a smart contract.

3.4.4 Cryptocurrencies

Cryptocurrency is a digital money-like asset that is based on blockchain technology. It allows users to safely and almost instantly transfer or receive funds without a middleman involved. Moreover, these transactions are completed with minimal processing fees, allowing parties to avoid higher fees charged by banks and financial institutions for wire transfers [20]. Notable, and well-known examples are Bitcoin, Ethereum, or Tether (a fixture stablecoin, which is backed by fiat money to create valuations stable). They are generally not issued by any central authority (government, central bank, etc.), making them practically immune to outside political interference. This also concerns people who tend to criticize cryptocurrencies for their use for illegal activities, high volatility, and underlying infrastructure vulnerabilities.
But why does this word contain the ”crypto” part? The main application of cryptography comes in when the transactions get validated by the users or miners with the help of cryptography. In other words, cryptocurrencies use cryptography to handle the following things:

- To make the transactions secured

- To make sure that the transaction was successful (verification)

- To rule out doubles-spend or counterfeits

The use of public-key cryptography achieves all this. The method provides two keys for the user: a public key and a private key. These are just random numbers that are around numbers or even letters. In essence, a public key is - as its name provisions - responsible for identification on a public blockchain. People usually use this address to receive funds. Moreover, the private key combined with the public key enables/authorizes the user to unlock their ”wallet” and freely initiate transactions.

3.5 Mining

Mining - in the sense of cryptocurrencies - is a crucial concept of Proof of Work (PoW) coins. PoW is a decentralized consensus mechanism that needs the participants to put in an effort (in this case, hardware resources) to solve a mathematical puzzle that prevents disruption in the network from people with malicious intentions [21]. This methodology was firstly used in Bitcoin for transaction validation and mining new coins/tokens. This made secure peer-to-peer cryptocurrency transactions possible without the need for a trusted third party, perhaps giving way to the decentralized revolution we are seeing nowadays. The amount of effort needed is scaled programmatically or by the number of miners joining the network.
As analyzed in previous sections, these systems are running on a distributed ledger, which contains a record of every single transaction of a specific cryptocurrency, arranged in sequenced blocks. Since this data is distributed, tampering is impossible since it will be rejected by the other users. The effort needed for Bitcoin, for example, is used for iterations of the SHA-256 hashing function, which is an irreversible way to generate one hash from a long string of numbers. Its only use is to check that the data that generated the hash matches the original data. Bitcoin network also sets an increasing difficulty, adjusting in a way that each new block needs approximately 10 minutes to get mined. The ”winner” of the hashing of the block - that is randomly selected chosen proportional to the work done - will receive a block reward - it is what makes mining profitable and keeps Bitcoin alive. Mining is a competitive market by nature and compared to the beginnings in 2011, and nowadays, it is nearly impossible to be the one who mines the block, so most people mine by joining ”mining pools” to increase their chances of mining blocks. In case of success, the block reward will be proportionally distributed between the pool members.

3.6 Bitcoin

3.6.1 Introduction

Satoshi Nakamoto, an anonymous user individual or group, developed Bitcoin in a white paper published in 2008. It is a basic but enticing idea: Bitcoin is a virtual currency that enables safe online peer-to-peer payments. With the exception of online financial companies like Venmo and PayPal that depend on the old banking sector for authorization to move funds as well as on current debit/credit accounts, Bitcoin is decentralized: anyone, anywhere in the globe, may transfer Bitcoin to anyone else, without any middleman. Thousands of other cryptocurrencies have been developed after Bitcoin’s inception, but Bitcoin is the most valuable in terms of global value and market cap.
Bitcoin is an Internet-based currency. As government-issued commodities such as the dollar or euro, Bitcoin permits internet transactions without the use of an intermediary

such as an institution or payment facilitator. The absence of those intermediaries opens up hundreds of new options, such as the ability for cash to travel more swiftly and inexpensively over the internet", as well as enabling people to have complete ownership over their own resources. Using, holding, and trading Bitcoin is acceptable, and it may be used for anything from a vacation to generous causes. It has been employed as a means of trade, a measure of wealth, and a piece of accounting, all of which are qualities of the currency. Bitcoin can be used for a variety of purposes, depending on your objectives:

- A type of investment product
- A method of transferring value around the globe
- Or maybe just a way to learn about new technology.

Unlike credit card companies, Bitcoin is not controlled by a person or a firm. Bitcoin seems to be the world's largest truly open payment system, accessible to anybody with an internet service. Bitcoin was created to be utilized online and does not rely on institutions or other businesses to complete transactions. The blockchain is among the most significant aspects of cryptocurrency, as it records who possesses what, comparable to how a bank monitors resources. The Bitcoin blockchain differs from a bank's record in that it is decentralized, which means that anybody can see it, and no single organization has control over it.

3.6.2 Economic aspects

Bitcoin proponents frequently point out that the currency is unaffected by inflation. They bring awareness to the reality that Bitcoin is restricted in supply, contrasting this with the traditional money system, in which central banks can theoretically bring a limitless quantity of money into the economy. While this does provide information on the amount of Bitcoin, it does not provide information about the degree of inflation, which is evaluated based on the price changes instead of the amount of cash. As a result, the scenario provides little insight into inflation. To establish any assertions about inflation in the Cryptocurrency market, you would have to know exactly which products and services were actually exchanged in Bitcoin internationally, how significant a proportion of sales in Bitcoin each particular commodity has, and how the value of every item has changed over a period. Only then can a pricing tag for Bitcoin be created to track its evolution over a period. However, that data does not really exist and would not be made public. Since that would necessitate widespread visibility throughout the Cryptocurrency market, it would jeopardize Bitcoin's core concept, which prioritizes anonymity and pseudonymity over openness. As a result, the idea that Bitcoin is unaffected by inflation is false.
Cryptocurrencies also provide prospects in developing nations. Depending on a review of the financial challenges, cryptocurrencies have the ability to promote growth in a vari-

ety of industries. Innovations and breakthroughs are crucial answers for emerging nations' catch-up processes. To profit from cryptocurrency monetary system improvements, users must have internet connectivity, as only those with internet connectivity may market cryptocurrency. As a result, the significant rise in internet consumption in developing nations over the last decade is both positive and necessary.

3.7 Ethereum

3.7.1 Introduction

Ethereum is among dozens of digital currencies that have popped up in the last decade but are marked as the pioneer of significant development of blockchain technology. Ethereum debuted in 2015, being the product of eight co-founders, led by Vitalik Buterin. Ethereum is the name of the cryptocurrency and network, and Ether is the name of the single component. Ethereum is also managed and tracked using a decentralized computer system, or global log, known as a blockchain.
It is helpful to think of a blockchain as a continuous record of all cryptocurrency transactions. The operations are verified, and the information's authenticity is ensured by devices in the network. Ethereum, as well as other cryptocurrencies, are appealing because of its decentralized system. Individuals can transfer currency without the necessity for a centralized middleman like an institution, and the currency is practically independent due to the unavailability of a banking system. Even if the transfer is generally visible on the network, Ethereum enables individuals to conduct deals practically anonymously. It may be used to support a variety of applications that perform tasks slightly more extensive than Bitcoin does:

- Currency: Anyone can own or transfer Ether with an ERC-20[1] supported wallet, or use it to spend on products and goods if the virtual currency is approved. Some services, like Ledger or Trezor, also enable you to store your money in a physical wallet, which theoretically makes them less vulnerable to hackers.
- Smart contracts: These are a type of permission-less application which operates instantly after the contract's requirements have been fulfilled.
- Decentralized applications (dApps): These are digital applications that exist on a blockchain (or P2P[2]), enabling individuals to do things like play video games, trade, transfer cash, maintain an investment strategy, and keep up with social networking.

[1] ERC-20 is the technical standard of Ethereum acting as a list of rules applied to the functions of every single smart contract on its network.
[2] Peer-to-Peer network, in which individuals interact directly with each other, without intermediation by a third party, acting both as a client and a server at the same time.

- Non-fungible tokens (NFTs): These tokens, which are based on Ethereum, enable artists and many others to trade paintings or other products straight to customers via smart contracts.
- Decentralized finance (DeFi): A strictly software-based system designed to remove intermediaries between transacting parties. Financial products can be openly used on a decentralized network, making it possible for buyers/sellers or lenders/borrowers to interact [22].

Another important concept to remember is the way Ethereum calculates the transaction fees. In case someone wants to send Etheruem or any different kind of ERC-20 tokens to another wallet address, so-called ”Gas” will be required to conduct a transaction or contract deployment successfully. It is priced in a small fraction of Ether, commonly called gwei. The exact price is market-based (supply/demand) between the miners and the queue of transactions waiting to be confirmed. Gwei is a configurable cost, but if set too low, miners can decline to process the transaction, and the other way around, if set high, it will act as a ”priority” transaction and will be processed sooner. The minimum amount of gas required to process a transaction is 21,000, and to get the final fee, you must multiply that number by the average gas cost noted in gwei.

3.7.2 Smart contracts using Solidity

Solidity is an object-oriented programming language developed by several former Ethereum core contributors, most notably Christian Reitwiessner and Alex Beregszaszi. It is statically typed and was heavily influenced by Javascript, C++, and Python. A smart contract is a self-contained program generated in Solidity, converted into JSON, and distributed to a specified blockchain account. Broadly said, a ”smart contract” is a technology that executes on Ethereum’s blockchain. It is a set of software (its operations) and data (its configuration) that lives on the Ethereum platform at a single location.
Ethereum accounts come in the form of smart contracts. This indicates that they will have a deposit and are able to conduct payments across the system. However, they really are not managed by a user; alternatively, they are distributed to the system and operate according to a set of instructions. User profiles can, however, engage with a smart contract by sending payments or interacting with functions that cause the smart contract to perform a task. Smart contracts, like conventional agreements, can make guidelines and have them enforced automatically through programming. Smart contracts cannot be canceled by default, and their exchanges are permanent. This immutability and reliability are perhaps the main reason this thesis research development is conducted using Solidity.

3.7.3 The initial coin offering boom in the 2010s

Initial coin offers (ICOs) are purchases of virtual tokens centered on the blockchain that is linked to particular networks or assets. These were made possible with the introduction of Ethereum's smart contract feature. Since 2014, initial coin offerings (ICOs) have developed as a new type of financing, having some similarities to Initial public offerings and venture funding. With 5728 ICOs that raised over $65 billion as per the estimations of ICOBench as of 2021 [23], we investigate the connection among issuer attributes and metrics of achievement, with a concentration on stability.

- Initial coin offerings are indeed a common financing mechanism for entrepreneurs that want to sell goods and services in the virtual currency and blockchain sector.
- Initial coin offerings are comparable to shares, but they can also be used to fund computer products or services.
- Some initial coin offerings have resulted in significant profits for participants. Many others have been exposed as frauds, have collapsed, or have fared horribly.
- In order to engage in an ICO, you will have to initially buy a virtual currency and also have a general knowledge of how to use crypto accounts and markets.
- Because ICOs are largely uncontrolled, investors must proceed with extreme care and diligence while evaluating and investing in them.

3.7.4 The DAO event and 51% attacks

Smart contracts indeed do mean reliability and ease of mind in the long term. However, just as with any other software, human error still can be a negative factor that has to be considered. If a system has a logical error or perhaps a loophole that can be attacked or taken advantage of, it will eventually raise the attention of hackers. Carelessly planned and tested smart contracts are undoubtedly easy targets, as most of the smart contracts are publicly available. The first painful lesson was the so-called DAO event. DAO - a short version of decentralized autonomous organization-, has raised $150 million worth of Ether in 2016 through a public sale, with the goal of forming an investor-directed capital fund, where the decisions are made by the members weighted by the equity of the tokens instead of central management. The objective of creating a new decentralized business model has failed miserably after one-third of its funds have been stolen due to an error in its smart contract. This project was the biggest of its time with more than 11000 investors. Some of them started to spot vulnerabilities in the codebase. The funders have tried to fix the issue in time, but an attacker succeeded. This was a turning point in the history of Etherum because this issue did not only mean financial loss for the investors but heavily undermined the trust in it, since DAO had become such heavily invested, at

that point, 14% of all Ether in circulation has belonged to that project's wallet. After a controversial decision of the community, a hard fork was executed that effectively rolled back the network's history to the point before the attack. It has raised ethical issues since this step has countered the idea of immutability and central governance, but it was a collective decision in order to restore the funds to the investors. This resulted in the creation of Ethereum as we know it today, but the pre-fork blockchain is still in use these days, renamed Ethereum Classic.
Other than the programming flaws in such systems, there is another issue that was fundamentally concerning about blockchain-based currencies and applications: the infamous 51% attack. It is an event where a group of miners controls more than half of the network's mining hash power, gaining the ability to be able to halt, deny or revert new transactions, effectively giving the possibility of double-spending coins [24]. The most vulnerable ones are smaller projects running with less mining computing power, but this issue has happened with known coins too. When these attacker groups gain power over the network, the idea of collective validation and rejection of altered blocks cease to exist. Even though changing historical blocks are nearly impossible, a 51% attack proved to be devastating for currencies. Ethereum based currencies such as Krypton and Shift have seen multiple attacks, but such can happen to different blockchains as well. For example, an attack has happened to Bitcoin hard fork, Bitcoin Gold, in 2018, the 26th largest currency at the time. The orchestrators of the attack have been able to double-spend for days, stealing more than $18 million in total. Bitcoin Gold has not been able to recover nor the trust of investors nor its previous value.

3.7.5 Ethereum 2.0

Ethereum 2.0 will be an expansion to the Ethereum network that now exists. Its goal is to improve the network's performance, reliability, and sustainability, allowing it to resolve blockages and boost transaction volume (increasing from 30 transactions per second to 100,000 per second). Contrary to the beginning, Ethereum nowadays is considered to be a big pollution source since it became the number one currency mined. Ethereum 2.0 is also known as Eth2 or Serenity. In comparison to the old generation, it features several significant structural and design modifications. Proof of Work will be abandoned, and Proof of Stake[3] will take its place, which will technically eliminate the current energy-intensive method.

[3]Proof of Stake (PoS) is a concept in which the mining power or the number of validated transactions are dependants on the number of coins owned. More than just an energy-efficient alternative of Proof of Work (PoW), this algorithm carries less risk and is less prone to potential 51% attacks.

3.8 Summary and Conclusions

In this section, the background of blockchain technology has been researched, through its history and development, the core concepts and features have been identified. After the introduction of the two biggest cryptocurrencies on the market as of 2021, namely Bitcoin and Ethereum, it is clear that the ability to create an immutable but transparent smart contract makes Ethereum and its ERC-20 network a great fit for an application supporting decision-making, perhaps developing an advanced election system is favorable. In the following section, perhaps, using Solidity and existing web development concepts, an example experiment of a working voting platform that takes into consideration the flaws of the currently existing election systems and utilizes the strengths of blockchain technology will be introduced in a hypothetical scenario.

4 Implementation of a blockchain-based evoting system

4.1 Development plan

4.1.1 Hypothetical Scenario

Extensive planning before software development is crucial. One important element to consider in this process is understanding the environment and the end-users, where the topic of this thesis research will be implemented. In this case, the subject is an imaginary country with its imaginary story, the Republic of Sunshine. This nation is considered to be a full democracy according to the Democracy Index and is about to face its 18th Presidential Elections, using a new, blockchain-based evoting system for the first time.
Each citizen has an ID card with a unique verification number. The electoral system is mostly mimicking the Hungarian Parlamentary elections. Voters will have two different matters to decide about - who should be the next President and who should be elected to the National Assembly, representing their local issues? There are three contestants for the President position from three different parties, and there are five different regions that divide the country into five constituencies, of which each party will have its contestants. People will be able to vote for their local representative based on their address, and the winner of each region will represent it in the National Assembly. For the sake of a successful test, later on, the population will be ”limited” to a lower number, but the system must be easily scalable. Before the elections, a database must be set up with the citizens’ personal information and a generated Ethereum address key pair and supply a small amount of Ether for each wallet to cover the costs. Every eligible citizen will get a notification, through traditional mail or a national gateway, with their own private (secret) key included. This will be their own identifier, and no one else will be able to authenticate with it.

4.1.2 System Plan

Our goal is to create a system that is easy to handle, can be accessed through most devices, and is reliable enough to support the whole election process. The entire platform will be web-based because, with proper coding, it could work just a well on mobile phones as it would work on personal computers, providing the necessary flexibility we need. This would practically eliminate the use of voting stations since everyone could be able to express their opinions from the comfort of their homes, possibly providing a much higher voting turnout than usual. The logic needs to be separated into multiple elements:

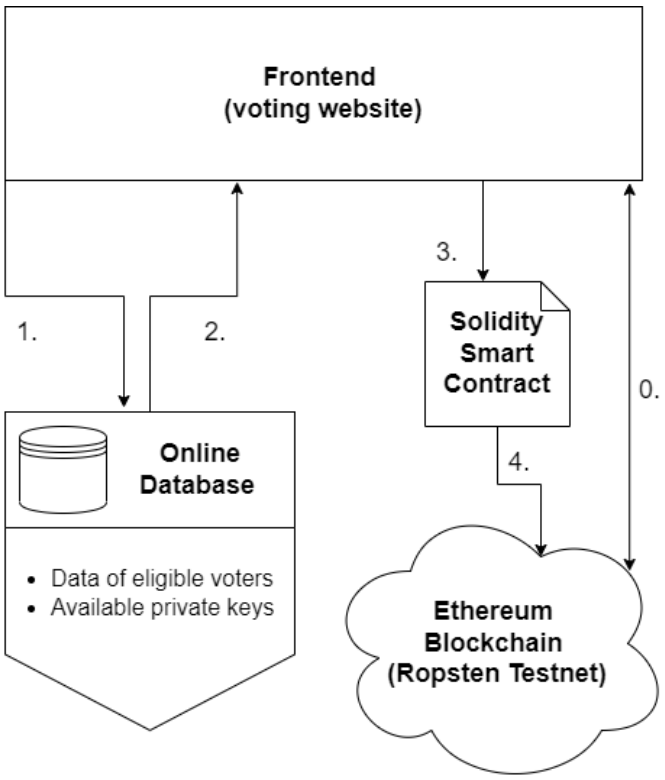

Figure 4-1: System Design and Workflow

1. Front-end: The graphic design interface, in which the citizen can navigate, learn more about the process, and vote.

2. Back-end: One of the backbones of the project that is responsible for handling the input data, can securely retrieve from or store data to the network or databases.

3. Database: The constantly accessible storage that is used to verify the citizens before allowing them to vote.

4. Smart Contract: The Solidity-based core support of the voting process that accelerates and controls the steps transparently on Ethereum blockchain.

5. Blockchain: The distributed ledger itself that stores the current standings of the election and does so while providing privacy for the citizens. Its data should be displayed by the front-end.

It is also crucial to plan carefully and think about the userbase that will use the system. It is done so by creating use cases, which in terms of systems engineering is a scenario analytics method to plot every situation that an end-user can face and every interaction that it could have with our software's user interface, which is the point of human-computer interaction and communication in a device [25].

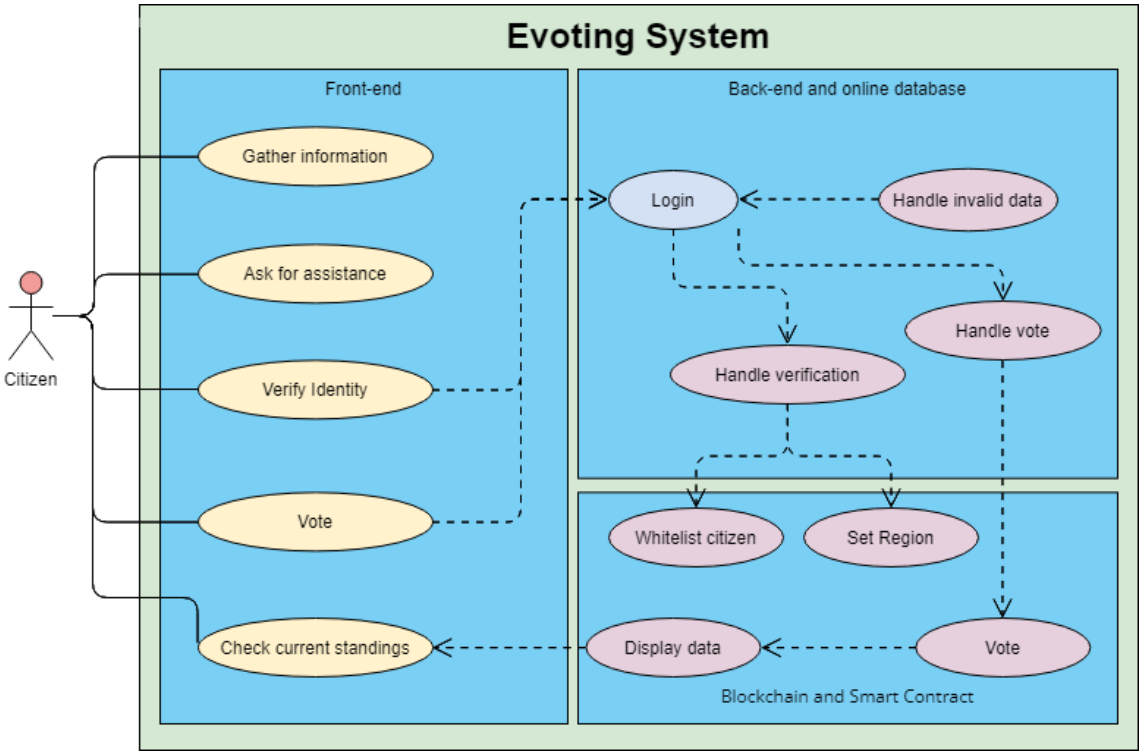

Figure 4-2: System Use Case

It is also worth noting that there are three kinds of front-end displayed information that must be separated, depending on the source.

- Static information: The non-changeable information, such as contact details, help section, video explanation, falls in this category.
- Server produced or local database-stored information: Certain data is stored in the database, gathered from national resources, such as the citizens' personal information. This is used to compare the input data during the identity verification to make sure there will be no unauthorized access, as well as used during the voting process to display the appropriate regional candidates according to the address of the potential voter.

- Blockchain-stored information: These are the statistics that are gathered directly from the network. These are publicly accessible, and the server will request these data straight from the Ethereum blockchain without requiring any interaction with locally stored data or processes. This means that the platform will provide up-to-date temporary results even for those not authenticated.

The smart contract's task is to provide blockchain deployed functions that are only accessible for the administrator or an organization responsible for handling the elections. Once these data objects and functions are deployed, they cannot be changed anymore.

4.1.3 Data Storage Plan

Since the structure has been set, the next step is to figure out, what are the necessary information that we need to store in both data sets. The online database should consist the personal data since this database is only used for the verification process. We assume that the Republic of Sunshine owns a national database of its people. A distributed ledger could support these data elements. Still, it is not recommended, as personal details could change over time, so they will be stored in a MariaDB-backed online database. MariaDB is a truly open-source advanced fork of the MYSQL relational database management system, designed for support, reliability, and ease of use. It uses a client/server model and is almost entirely compatible with MYSQL [26]. The data pairs that have to be compared in order to identify the citizen are their own national ID number and the private key they have got previously. Since the rest of the data will be stored on the blockchain, we will not need more than one data table.

Table 4-1: Online database table structure plan

ID	Name	Type	Comment
1	ID	integer	Unique number for identifying each entry
2	name	text	Full name of the citizen
3	nationalID	varchar(7)	Unique 7 character long personal ID number of citizen
4	regionID	integer	A number from 1 to 5, indicating the region the citizen is living
5	publicKey	text	The public key pre-assigned to the citizen
6	privateKey	text	Encoded private key pair, that is sent to the citizen for the identification process

For security reasons - in case of a data breach event - the private key must be encrypted. This will make sure that only the owner of the key will be able to verify their identity using it because with good encryption, it will be impossible to revert the data, but the back-end would still be able to make the appropriate comparison. Luckily we do not have to be concerned with the security related to the smart contract-assisted data. By the nature of blockchain technology, the data stored on the network will be secured unless we leave loopholes in the contract's code.
The data stored on the network, however, has a different structure compared to a MariaDB table because they act as a collection of objects. Similar to strongly typed programming languages, Solidity requires the type of data we would like to work with, as well as gives the possibility to hide functions or objects using the ”private” modifier - and to do the opposite with ”public”. So in this particular case, two collections of objects will be used, one public for the candidates - so that the vote count will be visible - and one private voter so that the citizen can practice their democratic rights while ensuring their anonymity.

Table 4-2: Private voters collection on the blockchain

ID	**Name**	**Type**	**Comment**
1	ID	integer	Autogenerated unique number for identifying each entry
2	autorizedToVote	bool	False by default, each address is blocked from casting a vote unless it passes the verification process and gets whitelisted by the smart contract
3	regionToVote	uint	Null by default, after the verification process, the smart contract sets the appropriate regionID, so that the citizens can only vote on contestants in their region
4	voted	bool	False by default, after the whitelisted citizen votes, the smart contract sets this attribute to true, eliminating duplicate votes
5	generalVote	uint	The ID number of the selected prime-minister candidate
6	regionVote	uint	The ID number of the selected candidate in the constituency/regional elections

The data fields are not used at the same time, some of them have significance in the authorization process, and the rest are the ones that are responsible for the actual voting. No one can retrieve this information, nor citizens, or any government-related personnel. This object collection's only goal is to assist the functions. Apart from these data, each object will be mapped/associated with one public key that is stored in the MariaDB table, providing a layer of security in case of an error occurs.

Table 4-3: Public candidates collection on the blockchain

ID	Name	Type	Comment
1	ID	integer	Autogenerated unique number for identifying each entry
2	name	string	The name of the candidate
3	regionID	uint	The region where the candidate fights for a mandate
4	numOfVotes	uint	Total number of votes received

The public "candidates" collection and its objects are a different story. These ones have to be publicly accessible to retrieve each person's actual number of votes and to deliver it to the front-end. The regionID will be used to compare it to the voter object's regionToVote attribute to filter erroneous or malicious voting attempts.

4.2 Front-end

4.2.1 Wireframe and Planning

Before the actual front-end graphical designing begins, it is recommended to do a process so-called wireframing. This is a planning process in which the developer produces a two-dimensional illustration of the user interfaces, focusing on the module and space allocation, prioritizes the content and the functionalities in an attempt to form a good base for templating and improving usability. Usually, very few or no colors and images are used and only schemes an idea on which a well-structured application can be built to produce the best possible user experience. The idea was to provide accurate and on-point information for the potential voters so that even the older generation would not have any problem understanding the manner of verification and choosing their preferred politician. My first idea was to create a menu/navbar that serves as the container of available menu options. That menu can also contain the flag of the Republic of Sunshine and the title of the event. It must be "sticky", meaning that even after scrolling down to visit other content on the website, it should remain on top so that users can find their desired information as quickly as possible. The next row should display the most important data

about the election, perhaps some kind of graphic flowchart helping in the voting steps or an explainer video that assists the citizens.

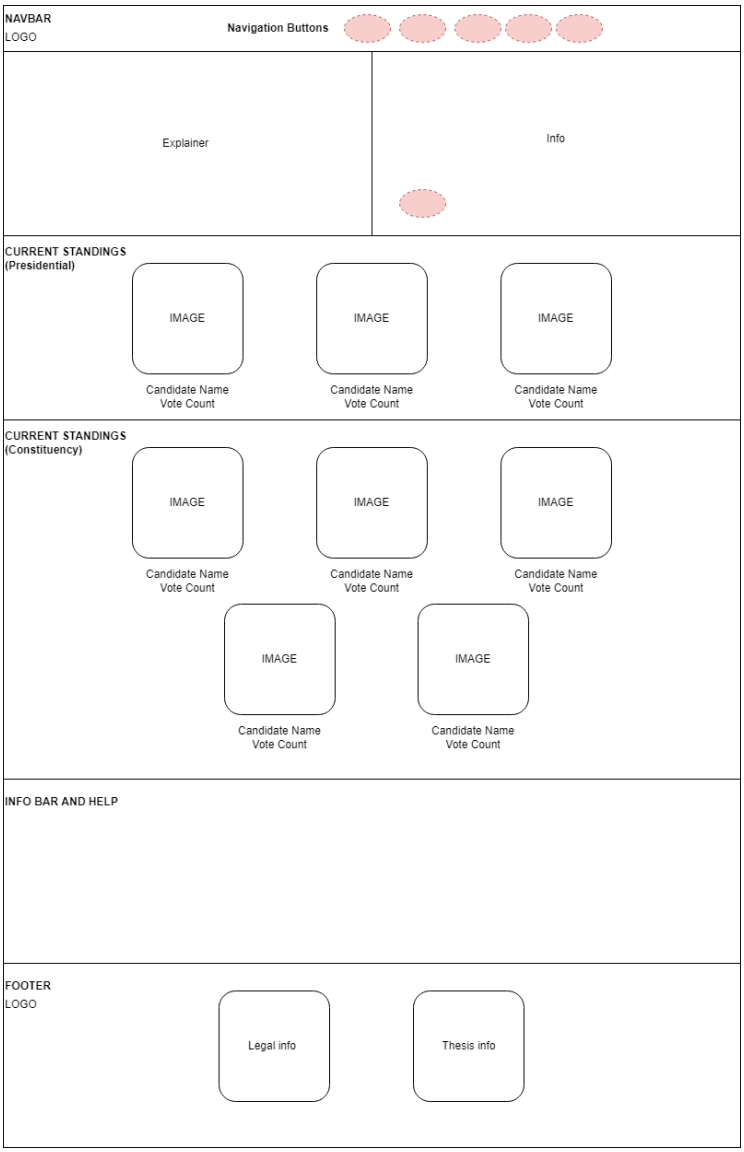

Figure 4-3: Index Front-end Wireframe

As of the right side, there should be the title of the event (in this case, Presidential Elections), some basic facts, and a button to forward the voter to the identification phase. The next block is about the statistical display of the most important question, the presidential candidates. There are a couple of fields that should be displayed here, for example, the image, the name, the party of the contestant, and the current vote count. The other section would technically work the same, but with constituency elections, and divided into five parts of the five regions (western, northern, central, eastern, southern). For now, the numbers displayed on the HTML file are dummy data, but they are the ones that will require back-end support to download them from the blockchain. The last two remaining sections

are for assisting the voters in case they get stuck. There should be a help section with a detailed explanation, including contact details if someone needs real-time assistance, and there should be a footer that also offers some fields of additional information display, but mainly for aesthetic reasons. There were also important usability principles to take into consideration.
Effectivity, the first and the most important rule because an application should be able to provide efficient, suitable functionality for the users to complete their tasks. The website must not overload the voter with unnecessary information to fulfill this principle because each additional information distracts the user from the important steps. Careful attention also needs to be paid to the optimization of efficiency, meaning that the citizen should be able to vote in minimal time successfully. The second important rule is **controllability**, meaning that the system should regard the voters' authority within the system, providing control over their actions. They may be able to cancel, pause or resume their action at a later point in time, doing so transparently. The third principle is **consistency**. The control of the platform should align with the expectations of the voter in every aspect. With the consistent usage of terms, icons, styles in the same uniform way, the user will be able to memorize and reuse a behavior pattern once learned. The fourth principle is **design and layout comprehensibility**. The layout of the user interface elements and the used colors should support the voters with recognizing buttons and easily readable pieces of information. The fifth rule is **language**, meaning that the application should be in line with the target user's language and way of thinking. The labels, text elements, button names should be verbalized clearly with the audience's vocabulary. The sixth rule is **feedback**, and the system should react to the voter's input at any time and inform about the current situation. In case of an error (for example, wrong personal ID input), it should be clear for the end-user what the issue was with their request. As for the seventh principle, **error tolerance** should be considered. This means that user errors will most likely happen, so the platform should try to avoid any misunderstandings and logical loopholes. And even if an error happens, the system should "forgive" the user and provide guidance accordingly. Under no circumstances do user faults should lead to data loss or even a system crash. And the eighth and last principle is **user experience (UX)**. It is an overall, complete experience the voters have with the application. They may come from previous experiences with other systems. This principle results from all the above and is characterized by giving a good impression to the end-users. If a good UX is achieved, the voters will have a sense of security and reliability, understand the purpose of the evoting system and know the requirements to proceed with expressing their choise.

4.2.2 Designing the User Interface

Multiple different technologies and programming languages need to be composed into one working product to reach the planning goals. Responsive web design is a concept

that allows completely functional user interfaces across various devices (mobile, desktop, tablet, and other portable devices). It suggests design should respond to the user's behavior based on the size of their screen, platforms, and orientation [27]. Flexible grids are foundational elements of responsive design. This plays a crucial part because if the website does not work or has design issues on mobile phones, for example, a big chunk of potential voters can be discouraged. The used technologies in the front-end are the following:

- HTML: HTML or, in full-term, hypertext markup language, is an "ancient" formatting method for content displayed in a web browser during browsing on the internet. It was first released in 1993, but the development started way earlier, in the 1980s, by a CERN contractor, Tim Berners-Lee. It is the standard barebone of a website and describes the structure semantically, effectively acting as building blocks built upon each other limited by a set of rules. HTML provides a wide range of functional elements, such as headings, paragraphs, lists, links, as well as constructs, images, forms, and other possibilities. These elements are separated using tags written in angle brackets. HTML also supports embedding scripting language written programs, for example, JavaScript, which adds more dynamic possibilities to the otherwise relatively static HTML. But HTML itself does not provide graphical design elements. For advanced styling, it needs to have CSS implemented.

- CSS: CSS stands for cascading style sheets. It is a language used to describe the graphical presentation of web pages and other media. It is considered just as important a cornerstone of the internet as HTML and Javascript. The technology was also suggested by CERN engineer Hakon Wium Lie in 1994 in hopes of improving the quality and user experience of content published. Two years later, it got its initial release. In web development terms, CSS simplifies the process of creating web pages user-friendly and presentable, handling the look and feel of it. CSS can be either inline in an HTML bracket or included from a different .css file, in which using different terms, the inheritable design rules can be set for classes, thus saving time for developers. CSS can control colors, the style of fonts, spacing between elements, column sizes, background images, layout designs, effects, but can also apply different rules for different devices and screen sizes. It has a steep learning curve, but designing with pure CSS is a rare concept nowadays. In general, pages load faster if included .css was used, and it also means easier maintenance due to global changes that would apply to any pages where that specific CSS rules were applied.

- JavaScript: JavaScript is a scripting language that allows the implementation of complex features on a website. It is part of the "three musketeers" of the early web, created by Brendan Eich, a Netscape Communications engineer, in 1995. Ini-

tially, it was called LiveScript but eventually renamed to position it as a companion of Java language created by their partner, Sun Microsystems [28]. Apart from the name similarities, though, it is in no way related to Java itself. The main use of this language in web programming is to display dynamic content that otherwise would be nearly impossible with just HTML and CSS. Almost every time, if a site has content that gets automatically updated, or when a map with direction is shown, 2D/3D animations appear, it is almost certain that JavaScript is involved. It provides an additional layer allowing developers to access APIs [4], store values inside variables, do string or integer operations or run code based on certain events occurring on the page, among many others. In 2019, 95% of all websites had JavaScript [29] implemented in their code, and the majority of websites are run using improved JavaScript-based frameworks, such as React.js, jQuery, Express, Angular, Vue.js, and other members on the list.

These core technologies still rule the web as of today, but creating complicated platforms would be too much of a hassle and not too efficient timewise. Dozens of front-end frameworks popped up in the past decade exactly for that reason: they provide the necessary tools and code base for faster and more secure development. This is the reason why Bootstrap is the one to use in this project. Bootstrap's initial release has dated back to 2011. It was originally named Twitter Blueprint as its developers, Mark Otto and Jacob Thornton was worked at Twitter, the popular social media, at that time. It is a free, open-source front-end framework focusing on responsive design. Its main content is CSS, but optionally JavaScript-based templates, such as types, forms, buttons, and other interface components, can be integrated with ease. With Bootstrap, I was able to successfully design the user interface, following the usability principles and the planned wireframe. It was not an easy task to make sure that the responsibility was on point, but the built-in grid system worked wonders. It served as a base for the two additional pages in the voting process: the authentication form and the actual voting page with the candidates; they just needed a small twitch by adding a form, in which the inputs will be handled by the back-end and - if necessary - sent to the smart contract.

4.3 Smart contract

4.3.1 Setting up the environment

This section will cover the required steps of an Ethereum ERC-20 supported Solidity smart contract creation, including the setup of the development environment and a detailed explanation of the functions and objects assisting the election process. The front-end is now ready, which is functioning as our first layer. The smart contract will mean

[4] API is the shortened term for application programming interface is a software intermediary that assists communication between applications.

the third layer meaning that the effective communication between them will demand back-end support. Ethereum, as of December 2021, has five different networks: Mainnet, Görli, Kovan, Rinkeby, and Ropsten. Deployment is possible on all chains, but they serve other purposes. The first one, Mainnet, is the ”live” network, which is used as a currency and live dApps. Görli, Kovan, and Rinkeby are proof-of-authority test networks, differing in the clients that can access them. In this thesis project, the used network will be Ropsten since it is a multi-purpose proof-of-work test net, the closest in technical terms of the Mainnet. The deployment of an election system does not necessarily require to be on the Mainnet. Most of the smart contracts serve financial purposes there, and considering the extremely high deployment costs at the moment, that can reach up to $8.000. It would not serve the purpose of this research, and it's not focused on creating monetary value. Perhaps Ropsten is a perfect choice to simulate an electoral system.
There are various tools to use for development, but the most popular one is called Remix IDE. It is a JavaScript-written open-source web and desktop environment that supports fast development cycle, provides easy plugin integration, and, most importantly, can be used from sandbox experimenting to actual deployment. It has modules for testing, debugging, and much more, making it a perfect choice for beginners and experts. Remix-IDE is available at https://remix.ethereum.org.
To complete our set of tools in this step, installing MetaMask is highly recommended. MetaMask is a cryptocurrency wallet software that interacts with any arbitrary Ethereum blockchain. MetaMask can only be installed as a web browser extension or mobile application. Here, a master wallet is created, which will serve as the ”owner” of the smart contract. Remix-IDE can connect to your wallet and assist with the deployment right away.

4.3.2 Designing the smart contract

The smart contract will consist of three ”categories” of code: the required tags, the objects and lists to store data, and the functions interacting with them. The back-end will supply accurate data to the functions from the citizen MariaDB.In the first step, we create a new Solidity file in Remix. The file extension of these documents is ”.sol”. The first line is always the one that specifies the Solidity version used throughout the contract, often followed by the contract tags with its name as a parameter. It is also a regular practice to include a public address variable that will display the owner's public key. In this case, I'm adding a string as well that contains the name of this event.

```
1     // Declaring the Solidity version
2     pragma solidity >=0.7.0 <0.9.0;
3     /**
4      * @title ElectionThesis
5      * @dev Smart contract supporting an anonymous general election
6      */
```

```
7     contract ElectionThesis{
8         // The "owner" master address
9         address public ownerAddress;
10        // The name of the election event
11        string public eventsName;
12    }
```

First of all, we have to set a constructor that will set the value of the two fields and will be used only once, in the event of the deployment.

```
1         // Initial setup of the contract, naming the event
2         constructor(string memory _eventsName){
3             ownerAddress = msg.sender;
4             eventsName = _eventsName;
5         }
```

After that, using the previously created data storage plan Data Storage Plan, the objects and their list containers should be designated.

```
1         // Object containing information of the candidate
2         struct Candidate {
3             string name;
4             uint regionId;
5             uint numOfVotes;
6         }
7
8         // An object containing only technical information of the voter
9         struct Voter {
10            bool authorizedToVote;
11            uint regionToVote;
12            bool voted;
13            uint generalVote;
14            uint regionVote;
15        }
16        // Distinguishing each voter by its address
17        mapping(address => Voter) private voters;
18        // Collection of all candidates
19        Candidate[] public candidates;
```

Now that the objects are ready, the next step is to design the functions using them. For security reasons, there must be a function that limits the usage of other functions. It will be called ownerOnly, and this will make sure that only the master address has access to specific functions.

```
1         // Snippet to ensure certain functions are only available for
              the "owner" address
2         modifier ownerOnly(){
3             require(msg.sender == ownerAddress);
4             _;
5         }
```

Our goal is to make the system as flexible as possible, perhaps the candidates will not be set at the deployment a contract, but they can be added afterward. This will be a function only accessible from the master address.

```
1        // Possibility to add more candidates
2        function addCandidate (string memory _name, uint _regionId)
             ownerOnly public{
3            candidates.push(Candidate(_name, _regionId));
4        }
```

From the voter's point of view, the first step is an authorization. We need to "whitelist" those addresses who have successfully proved their identity. This function will set the authorizedToVote boolean to true and set the region where the person will be able to choose their constituency candidate. This is also a function that must be limited to the master address - or in this case, government or Central Electoral Commission - so that no outsider will be able to change address status with malicious intent.

```
1        // Authorize citizens to vote and set their constituency
2        function authorizeVoter(address _person, uint _regionVotable)
             ownerOnly public{
3            voters[_person].authorizedToVote = true;
4            voters[_person].regionToVote = _regionVotable;
5        }
```

And last but not least, the public vote process function is needed. A totalVotes integer will also be supplied, so that it can be displayed on the front-end as an extra piece of data.

```
1         // Counting the total number of votes
2        uint public totalVotes;
3
4        // The voting function, checking if the citizen has already
             voted, checks if they are allowed to vote and if they have
             selected an appropriate regional candidate
5        function vote(uint _voteIndexGeneral, uint _voteIndexRegional)
             public{
6            require(!voters[msg.sender].voted);
7            require(voters[msg.sender].authorizedToVote);
8            require(voters[msg.sender].regionToVote == candidates[
                 _voteIndexRegional].regionId);
9
10           voters[msg.sender].generalVote = _voteIndexGeneral;
11           voters[msg.sender].regionVote = _voteIndexRegional;
12           voters[msg.sender].voted = true;
13
14           candidates[_voteIndexGeneral].numOfVotes += 1;
15           candidates[_voteIndexRegional].numOfVotes += 1;
16
17           totalVotes += 1;
18       }
```

This concludes the creation of the smart contract that will process the incoming requests acting as a constant listener. The contract has been tested in RemixIDE to make sure no bugs or loopholes were left. Since the test was successful, I have set up a master address in MetaMask (Check on Etherscan), set the network to Ropsten Test Network. The deployment and contract transactions also require gas, the same way as on the Mainnet, so I have requested test Ether from publicly available faucets - such as `https://faucet.ropsten.be` - for the master account. After selecting the Injected Web3 deployment mode in the RemixIDE, I have connected it to the MetaMask and successfully deployed the smart contract (Check on Etherscan).

4.3.3 Front-end and back-end connection

In this section, the second layer, the back-end, will be described. These scripts are mainly responsible for data transmission from and to the front-end, handling either local database operations or requests sent to the smart contract. The primary back-end languages used were:

- PHP: Hypertext preprocessor is a widely-used general-purpose, open-source server-side scripting language that was created for web development. Initially, it was created by Rasmus Lerdorf in 1994. Most of the time, PHP snippets are embedded in HTML. PHP is processed on a web server by an interpreter implemented as a Common Gateway Interface (CGI). It is used to handle dynamic content, sessions, and databases, among many others. As of April 2021, 79.2% of all the websites whose server-side programming language is public uses PHP [30]. To be able to run these scripts flawlessly - since the feedback is vital for the overall user experience - another concept was needed to be implemented since PHP supports no asynchronous processing.

- AJAX: Asynchronous Javascript and XML is a set of web development techniques that use various existing client-side technologies to create asynchronous web applications. Using AJAX, web applications can send and revieve data from the server in the background without interfering with the behavior of the page. The significance of AJAX in this research is that it allows front-end to PHP communication in the background, so in case there is an error in the process, for example, incorrect authorization details are given by the user, the system will be able to handle the request and return instructions to raise attention and guide the voter to the solution.

PHP and AJAX are more than enough to communicate flawlessly with our MariaDB citizen table and to show server responses to the end-users in the form of an unskippable browser alert message. However, additional libraries will be required to communicate with the election's smart contract. The workflow of the authorization is the following:

1. Handle input data, check if data was supplied at all. If so, check if the personal ID number and secret key provided by the voter exist in the online database. In case any of these turn out to be false, display an alert accordingly.

2. Gather data from the table and send an authorization request to the smart contract acting as the master wallet.

3. Set session variables to store variables from the table, and redirect to the voting page.

These server-side sessions [5] will handle the rights of a website visitor: if they gained authorization already, they could visit the actual voting page. If not, they will be redirected to the index page if they try to access it. The session will also decide certain form elements shown on the voting page, most importantly, the regional candidates. The workflow of the voting page will work similarly to the authorization, but in this case, it will follow these steps:

1. After successful authorization, display the appropriate candidates on the front-end.

2. In case the citizen has decided to whom they support and send the form, handle the request. In case they have not made any choice, alert the user. Otherwise, send a request to the smart contract using the citizen's wallet details and the selection they have made.

3. Destroy existing session variables to log out the voter and redirect to the home page.

Importing libraries require an additional software called Composer. It is a dependency management tool in PHP that allows users to declare libraries a project will depend on and it will install/update them. PHP does not have any core functions to work with blockchain-based applications. For this purpose, an open-source library called Web3PHP has to be used. It is a PHP interface for interacting with the Ethereum blockchain and ecosystem. Using Web3PHP's built-in functions, PHP calls can be sent to the smart contract in case a node provider is available. So the last thing to consider was to find a way to communicate with the Ropsten Test Network. One solution is to host a node, but it is a more complicated process. On the other hand, it would provide better security. For this research, Infura was used. Infura is a service provider platform that gives tools and infrastructure for developers to easily access Etherum blockchain and deploy dApps. Infura requires registration and to request a project API key but has a limited free use package that allows 100.000 requests through their API. Each and every Web3PHP call towards the election smart contract will run through Infura.

[5] Session variables are server stored data about one single user that can be accessed on all pages in one application.

4.3.4 Setting up the hosting

In case every layer, from the front-end to the blockchain connection, is ready, a publicly accessible server is required so that the potential voters will be able to reach the platform. When selecting the hosting solutions, it is crucial to proceed with one that supports the used technologies and runs them the most efficient way. My choice was to host the evoting system from a Linux-based resource that applies Apache 2.4 [6] as its web provider.
Thousands of hosting companies offer these servers, and after my positive experiences with Magyar Hosting, I have rented a server from them and registered a domain where this research website is publicly available. This service also comes with cPanel, which is a graphical interface that allows simplified control over website and server management. cPanel provides numerous integrated functions. For example, database management is through phpMyAdmin, which is an open-source administration tool for both MYSQL and MariaDB databases. This tool helps to set up the online database where the citizen table would be filled with mock data and wallet details. The access details, such as database user and password, had to be changed in the PHP files at that point to be able to communicate with our table.
The project folder that contains the pages with front-end and back-end, the style, and imported libraries can be uploaded to the server using either the built-in File Manager of the cPanel or via an FTP [7] client, such as Filezilla. All the files have to be in the public_html folder on the server to make it publicly accessible.
For the last step of the setup process, a free TLS certificate was installed, which is also an integrated function of cPanel. TLS is the successor of SSL (Secure Sockets Layer) and stands for Transport Layer Security. It is a standard cryptographic protocol used to secure server-to-client transactions (for example, voters' secret key sent through the form). This secure data transfer has to be enforced by using HTTPS protocol instead of HTTP. For this reason, a configured .htaccess file has to be uploaded into the public_html folder. After everything had been set up, the product of this research, a working blockchain-based evoting system, was ready to go to the next phase. The connected domain, where this election system is up and running is `www.icje2sthesis.hu`.

[6] Apache, an open-source web server that was created by Rober McCool. It is responsible for accepting directory (HTTP) requests from Internet users and sending them their desired information in the form of files and Web pages.
[7] File Transfer Protocol is a network protocol used to transmit files between computers over transmission control protocol/internet protocol (TCP/IP).

5 Testing the system

5.1 Test plan

Software testing is a process of reviewing software applications and products for bugs and errors to guarantee their efficiency. It is a fundamental process of designing reliable and usable products. The testing of this election system was conducted in two notable steps. In the first phase, internal tests were focused on the responsivity of the front-end and the consistency and security of the back-end and the smart contract. These were conducted without the involvement of outsiders. The responsivity test was carried out using ResponsiveTestTool, a publicly available platform that allows setting dozens of different screen sizes to conclude if the front-end CSS was correctly set, while the back-end and smart contract testing was through setting up test scripts to see if the communication was established. After the successful internal tests, it was time to get feedback from external sources and to see if the platform was ready to handle more significant traffic.
Before the second phase, there were several steps to be done that were needed for the launch. First of all, the citizen database was empty, so two external tools assisted me to generate a mock database: Mockaroo in generating fake personal data for the citizens, and Heliowallet's wallet generator tool for mass-creating Ropsten Test Network addresses that will represent the public key and the private (secret) key that was provided to the citizens before the voting for identification and authorization purposes. This time, I had a list of the private keys and the citizen's IDs to work with because, in the online MariaDB table, they are encrypted using the default PHP encryption method, bcrypt, so they are impossible to retrieve once the unencrypted private keys are lost. All the newly generated Ethereum wallets had to get "funds" so that they would cover the gas fees when interacting with the smart contract. For this purpose, I used EthereumICO's Token Multisender, which allows Web3 connection to a MetaMask wallet and mass token transfer to specified addresses. During the first testing phase, I came to the conclusion that 0.05 Ether would be more than enough supply to each citizen's wallet because the vote function cost an average of 0.03 Ether but never went over the 0.05 Ether limit. At that point, everything was set to proceed with involving volunteers in the process.
The plan was to request people to participate in the election anonymously - as the goal of this research was to ensure voters' privacy. Before the survey, I asked each and every participant in a form to consent to collecting their data for research purposes. The document did not state any use case or specify the steps required to vote. The goal was to see if an average user could deal with the system. Every pre-survey form had a personal ID and secret key pair printed, unique for each form. After the participant had finished the test, I asked them to fill a feedback form to answer the following questions:

1. What age group do you belong to? (18-24, 25-34, 35-59, 60+)

2. What device did you use? (PC/Laptop, Phone, Tablet)
3. How would you rate your IT skills? (1-5 scale, 1 is the worst, 5 is the best)
4. How would you rate your knowledge of blockchain technology? (1-5 scale, 1 is never heard of it, 5 is the expert)
5. Did you successfully vote? (Yes/No)
6. How hard did you find it to navigate on the website? (1-5 scale, 1 is the very hard, 5 is very easily)
7. Have you used any help displayed on the website? If so, which one?
8. Have you encountered any issues? If so, what happened?
9. Do you have any suggestions?
10. Would you use a platform like this instead of the current election systems? (Yes/No)

5.2 Test results

During the phase two process, a grand total of 22 people have participated in the research and provided a filled feedback form. The experiment went according to the plan, and no technical issues have occurred. The results were the following:
For the first question regarding the age groups, 9 participants were between 18-24 years, 5 in between 25-34 years, 6 in between 35-59, and only two above 60 years of age. Perhaps the pool mainly was consisting a younger audience. Out of the 22 people, 15 of them used either a PC or a Laptop to vote, 7 of them used phones, and none of them had used tablets. Sadly none of them have used tablets, so I cannot draw any conclusions about the usability on that platform. They have rated their IT skills to an average of 3.09 points, with 2 people claiming they are on an elementary level, 4 saying they are below average, 8 claiming to be an intermediate user, 6 saying they believe they are more skilled than the average and 2 claimed themselves to be experts. The answers related to their knowledge about blockchain technology, however, showed a different picture, with a low average of 2.04 points. 6 people have claimed they never heard of blockchain, generally from the older age groups, 9 claimed they have very little knowledge, 4 said they have an average understanding of it, 2 said they are well aware of the technology and its features, and 1 claimed to be an expert on the field. It is clearly visible that while cryptocurrencies gain continuous fame, the underlying technology is not yet understood by the general public. Only 1 person was not able to vote, while 21 people succeeded without any assistance needed, suggesting a 95.05% efficiency rate. The one person who failed has claimed that they couldn't get through the authorization process, which was due

to a banal error, a misunderstood 'O' character, and typed a zero number. Most likely, it was caused by wrong, confusing font usage on my side when delivering the first form for the participant. Luckily, our voters found it easy to understand and navigate the website, gathering an average of 4.04 points, with only one rating - the person who could not vote - lower than the average, that got selected by 6 people, 5 claimed to be easy to get along, and 10 said it was very easy to get through the process. Most people (13) claimed that they progressed intuitively and did not need any assistance to progress. 7 claimed they had read the information displayed on the website to understand what was happening. Only 1 person said they had watched the video as well, and 1 person said the help was inadequate and they could not vote in the end. Apart from the one person who could not get through the authorization, several people (5) claimed that the website loaded slowly initially. There was only one known responsibility issue. A person noted that the website looked weird on his screen. One person suggested that maybe a map should be displayed on the front-end showing the current standings with a chart or other visual graphics instead of pure text. The last question focused on the opinion of the participants if they would use a similar evoting system instead of their own respective election system currently used, 14 claimed they would, and 10 preferred to remain using traditional methods.

5.3 Possible improvements

There were a couple of ideas gathered from the testing feedback, as well as insights I have gained during the test and realizations I made after the test. This system is not perfect, and there are numerous ways to make it more efficient or more suitable for future use:

1. Display current voting percentages of each contestant on the front-end.
2. Create a cron job [8] to gather the current number of votes instead of calling the smart contract on each visit to speed the website up and make less traffic through the Web3 provider.
3. Set up multiple addresses that can handle the election as a master to decrease the workload of each address.
4. Add more functions to make editing or removing contestants possible (for example, in case they step back or get disqualified for some reason).
5. Add more advanced ID & KYC Verification [9] instead of using personal ID and secret key combination for the authorization (but it could potentially significantly slow down the entire process).

[8] Cron Job is a Linux job scheduler, and it allows the developers to run specific commands or scripts on the server to automatically complete repetitive tasks.

[9] KYC (Know Your Customer) is a process of identifying and verifying a person's identity, mostly used nowadays to enforce banks' anti-money laundering (AML) policy.

6. Create a script to randomize the order of the contestants in order to eliminate the psychological bias that a fixed order might mean.

7. Improve data visualization by using graphs to display the results instead of pure text.

8. Improve the user experience on older displays using smaller resolution (1024x768 or under) by paying more attention to design blocks margins and by decreasing menu element sizes to counter overflowing.

9. Add website security components, such as Cloudflare content delivery network to eliminate DDoS [10] threats.

10. Allow voters to abstain and not to support anyone. For example, in the regional elections, they vote, but they do not prefer anyone out of the presidential candidates.

11. Make it possible to re-authorize within the allowed timeframe in case the user has not cast their votes.

6 Conclusions

6.1 Research question and reflection

After a summary of the current state of democracies in the world, its issues, and possible improvements, and e-voting system was successfully developed, deployed, and tested during this study. The research question was about figuring out if a blockchain-supported digital system could decrease the chance of electoral fraud and help in other aspects as well. During this development, the positives of digital ledgers have been identified, and using a current, more advanced crypto network, Ethereum made it possible to successfully substitute the traditional vote-counting process to a reliable, immutable, fraud-proof system. The front-end, back-end, and Ropsten test network connections were successfully established, the working example is publicly available. The flexibility of Solidity and other existing client and server-side programming languages has been demonstrated since multiple platforms can easily access a web-based application. The only requirement is a web browsing capable device and internet connection. Thus, possible improvements and changes according to the local environment, including the electoral system, are easily doable.
During the front-end development, I focused intensely on achieving high usability to make it easier to understand how the platform works and minimize the chance of getting lost on

[10] DDoS (distributed denial-of-service attack) is a malicious attempt to disrupt the traffic of a server by overwhelming its underlying infrastructure with a flood of internet traffic.

the user interface since the population consists of people with a wide range of technological knowledge. Scaling up this system is also possible. With slight twitches in the smart contract and the validation process, it would not fail under higher stress if the necessary server resources had been allocated and proper security measures had been made. Analyzing the feedback from the participants of the anonymous testing, it is clear that most of the people had no problem casting a vote even without direct assistance or personal guidance. This proves that the usability analysis was concluded and its rules have been implemented just right, and there was adequate information displayed on the front-end (help section, video explanation). The system did not once fail during the test, proving to be a reliable solution for decentralized decision-making. Numerous human elements that have been the weak chain in the current practices have been ruled out from the steps.The system provided an easier way for citizens to vote, possibly increasing the turnout while keeping their identity completely transparent with no chance of misrecording votes, destruction of ballots, tampering with the electronic system, voter impersonation, and other organized fraudulent activities.
Considering the observations, I can convincingly conclude that blockchain technology could be a great help in revolutionizing the current electoral processes and could mean a technological leap in reaching next-level democracy, in which people gain more trust in the process and could be more incentivized to express their opinion.

6.2 Ending thoughts

There are specific sources and past experiences I have had in the world of cryptocurrencies and the blockchain technology itself that I can not cite or can not cite only once during this thesis research. In this minor footnote, I would like to thank the unknown Mr. Satoshi Nakamoto for releasing the whitepaper of Bitcoin [31], from which this whole technological revolution has started. The core concepts and rules set in that document still give a direction for all projects implementing a distributed ledger. Perhaps its significance is undoubted and gives the possibility of a more advanced democracy in the future.
I would like to thank IBM for releasing the Blockchain for Dummies book for the 3rd editorial version already [32]. It had played a significant role in my obsession with this world and provided a good starting point back in 2017 when I got really close to this technology. This book has also helped me in this research and proved to be substantial assistance if I got stuck.
Last but not least, I would like to thank everyone that was part of my sadly failed blockchain project, Blockfollow, in 2018. All the team members, investors, and the community who assisted in translating our whitepaper [33] to over ten languages, the ones that made our project one of the most awaited in those times [34]. The idea of creating a social trading platform that rewards information and provides a lowered barrier of entry is still relevant these days. Although we did not reach our goals [35], it is a sorrowful but still

cherished memory of mine: I have met many great people and got to learn something new each day. It is a constantly evolving environment, full of excitement. I have had much time reaching my personal conclusions. Sometimes multiple failures can lay heavy on someone, but not giving up is the key. I had not left crypto, and I am delighted to conduct this research and leave a little mark on the world, showing the limitless possibilities and future blockchain may have in the hope of reaching its ultimate goal: giving the incorruptible and undisruptable power to the people.

References

[1] Wikipedia, "Democracy index." Available at https://en.wikipedia.org/wiki/Democracy_Index (2021/03/22).

[2] Wikipedia, "Election." Available at https://en.wikipedia.org/wiki/Election (2021/03/22).

[3] Wikipedia, "Electoral fraud." Available at https://en.wikipedia.org/wiki/Electoral_fraud (2021/03/24).

[4] Unknown, "Estimated cost of the 43rd general election." Available at https://www.elections.ca/content.aspx?section=res&dir=rep/off/cou&document=index43&lang=e (2021/03/26).

[5] Wikipedia, "Democracy." Available at https://en.wikipedia.org/wiki/Democracy (2021/04/02).

[6] Wikipedia, "History of democracy." Available at https://en.wikipedia.org/wiki/History_of_democracy (2021/04/04).

[7] M. Coleman, "The meaning of democracy." Available at https://dlc.dcccd.edu/usgov1-1/the-meaning-of-democracy (2021/05/04).

[8] U. E. . C. in the Republic of Korea, "Democracy in brief." Available at https://kr.usembassy.gov/wp-content/uploads/sites/75/2017/04/Democracy-in-Brief_kor-1.pdf (2021/05/12).

[9] L. . D. Donn, "The unusual government of ancient mesopotamia - mesopotamia for kids." Available at https://mesopotamia.mrdonn.org/government.html (2021/04/05).

[10] Ducksters, "Ancient greece for kids: Government." Available at https://www.ducksters.com/history/ancient_greek_government.php (2021/04/07).

[11] Wikipedia, "History of democracy - rome." Available at https://en.wikipedia.org/wiki/History_of_democracy#Rome (2021/04/06).

[12] Medievaltimes.com, "Government - the medieval era." Available at https://www.medievaltimes.com/teachers-students/materials/medieval-era/government.html (2021/04/03).

[13] E. Union, "European instrument for democracy and human rights." Available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/568332/EPRS_BRI(2015)568332_EN.pdf (2021/04/04).

[14] S. Kotanidis, "Understanding the d'hondt method: Allocation of parliamentary seats and leadership positions." Available at https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2019)637966 (2021/09/20).

[15] C. Ellison, "Cryptography timeline." Available at https://theworld.com/~cme/html/timeline.html (2021/04/14).

[16] NielsenIQ, "Unpacking the sustainability landscape." Available at https://www.nielseniq.com/global/en/insights/analysis/2018/unpacking-the-sustainability-landscape/ (2021/04/02).

[17] N. Gagliordi, "Walmart implements ibm's blockchain for food traceability." Available at https://www.zdnet.com/article/walmart-implements-ibms-blockchain-for-food-traceability/ (2021/04/02).

[18] M. Scuffham, "Exclusive: Royal bank of canada using blockchain for u.s./canada payments - executive." Available at https://reut.rs/3lbPhmz (2021/04/17).

[19] Ábrahám Vass, "Nick szabo – a hungarian behind bitcoin?." Available at https://hungarytoday.hu/nick-szabo-hungarian-behind-bitcoin-48359/ (2021/05/02).

[20] J. Frankenfield, "Cryptocurrency definition." Available at https://www.investopedia.com/terms/c/cryptocurrency.asp (2021/05/02).

[21] J. Frankenfield, "Proof of work (pow)." Available at https://www.investopedia.com/terms/p/proof-work.asp (2021/11/25).

[22] R. Sharma, "Decentralized finance (defi) definition." Available at https://www.investopedia.com/decentralized-finance-defi-5113835 (2021/11/20).

[23] ICOBench, "Stats and facts." Available at https://icobench.com/stats (2021/11/26).

[24] P. Nahar, "What are 51% attacks in cryptocurrencies?." Available at https://economictimes.indiatimes.com/markets/cryptocurrency/

what-are-51-attacks-in-cryptocurrencies/articleshow/85802504.cms (2021/11/28).

[25] F. Churchville, "user interface (ui)." Available at https://searchapparchitecture.techtarget.com/definition/user-interface-UI (2021/12/03).

[26] B. Forta, *MariaDB Crash Course*. Addison Wesley, 2011.

[27] N. Babich, "Responsive web design tutorial and best practices." Available at https://xd.adobe.com/ideas/principles/web-design/responsive-web-design-2/ (2021/12/02).

[28] LaunchSchool, "An introduction to javascript programming and the history of javascript.." Available at https://launchschool.com/books/javascript/read/introduction (2021/12/02).

[29] E. Elliott, "How popular is javascript in 2019?." Available at https://medium.com/javascript-scene/how-popular-is-javascript-in-2019-823712f7c4b1 (2021/12/02).

[30] W3Techs, "Usage statistics of php for websites." Available at https://w3techs.com/technologies/details/pl-php (2021/11/26).

[31] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008.

[32] M. Gupta, *Blockchain For Dummies, 3rd IBM Limited Edition*. John Wiley and Sons, Inc., 2020.

[33] D. Tóth, "Blockfollow network whitepaper." Available at https://icje2sthesis.hu/cite/whitepaper.pdf (2021/12/04).

[34] Cryptometrics, "Top10 ico gainers of the week." Available at https://icje2sthesis.hu/cite/statistics.png (2021/12/04).

[35] D. Tóth, "Blockfollow network onepager." Available at https://icje2sthesis.hu/cite/onepager.pdf (2021/12/04).

List of Figures

List of Tables