Blockchain Based e-Voting System

BBM 443 Fundamentals of Blockchain Term Project

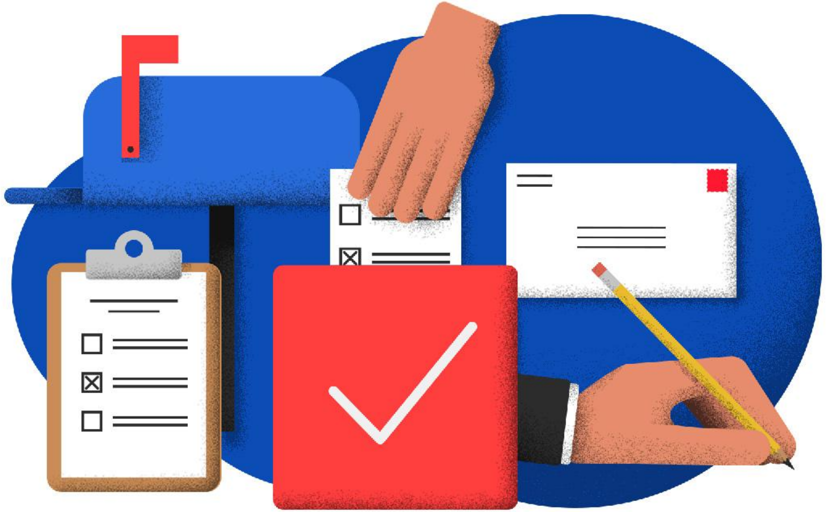
- Gökhan Özeloğlu - 21627557
- Burak Yılmaz - 21627868
- Dilara İşeri - 21783561
- Fatma Usalan - 21727829
- Necati Berk Özgür - 21785229

INTRODUCTION

- Voting is the foundation of democracy. In order for democracy to function properly and in accordance with its principles, voting must also be done correctly and effectively. No matter what choice is made, its basic rule is that it should be reliable.

- Although paper based voting continues to be used today, there are many vulnerabilities that threaten the reliability of voting, the security of votes, and the privacy of voters.

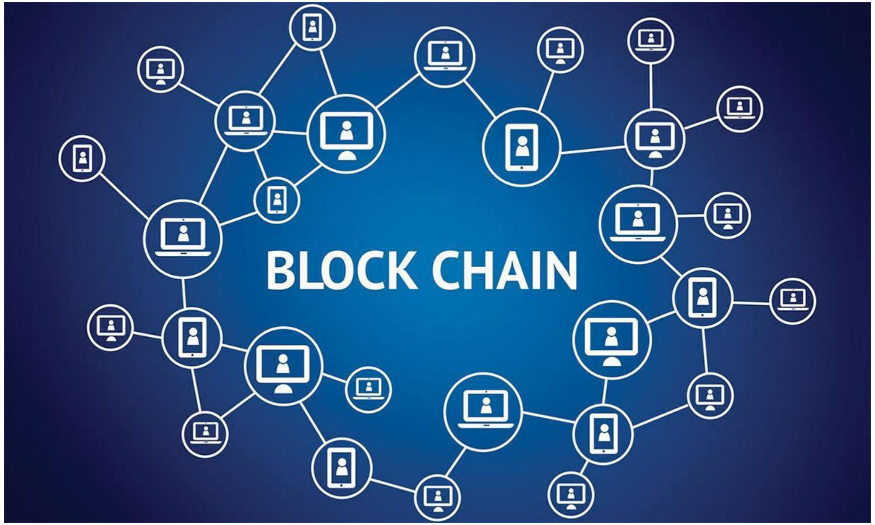
- Traditional voting is a centralized application. Centralized voting means that the voting process is carried out and managed by a center. In traditional voting, voting is done with paper ballot papers in certain centers. At the end of the voting, the votes are counted by certain persons and the results are announced to the public after all the votes are counted.



Paper Based Voting System

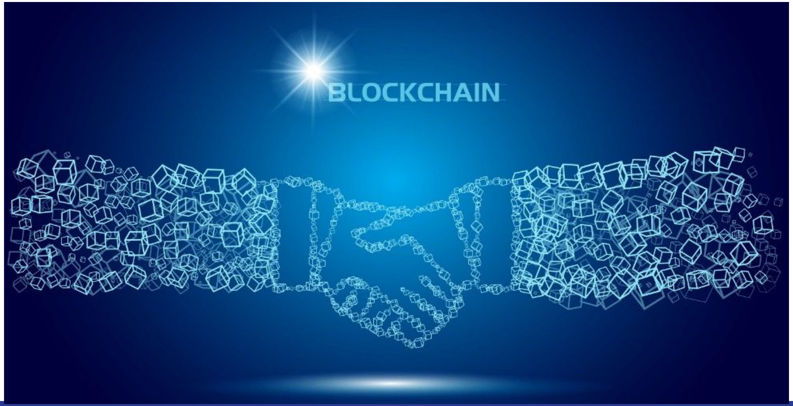
- Not trustworthy enough.
- Waste of resources: money, effort, time...
- Low participation.
- Accessibility problems.
- Lots of error of fact.

- Technology is developing rapidly today. However, new technologies are entering our lives every day that will make our lives easier. Blockchain, which is a new technology, is one of them.

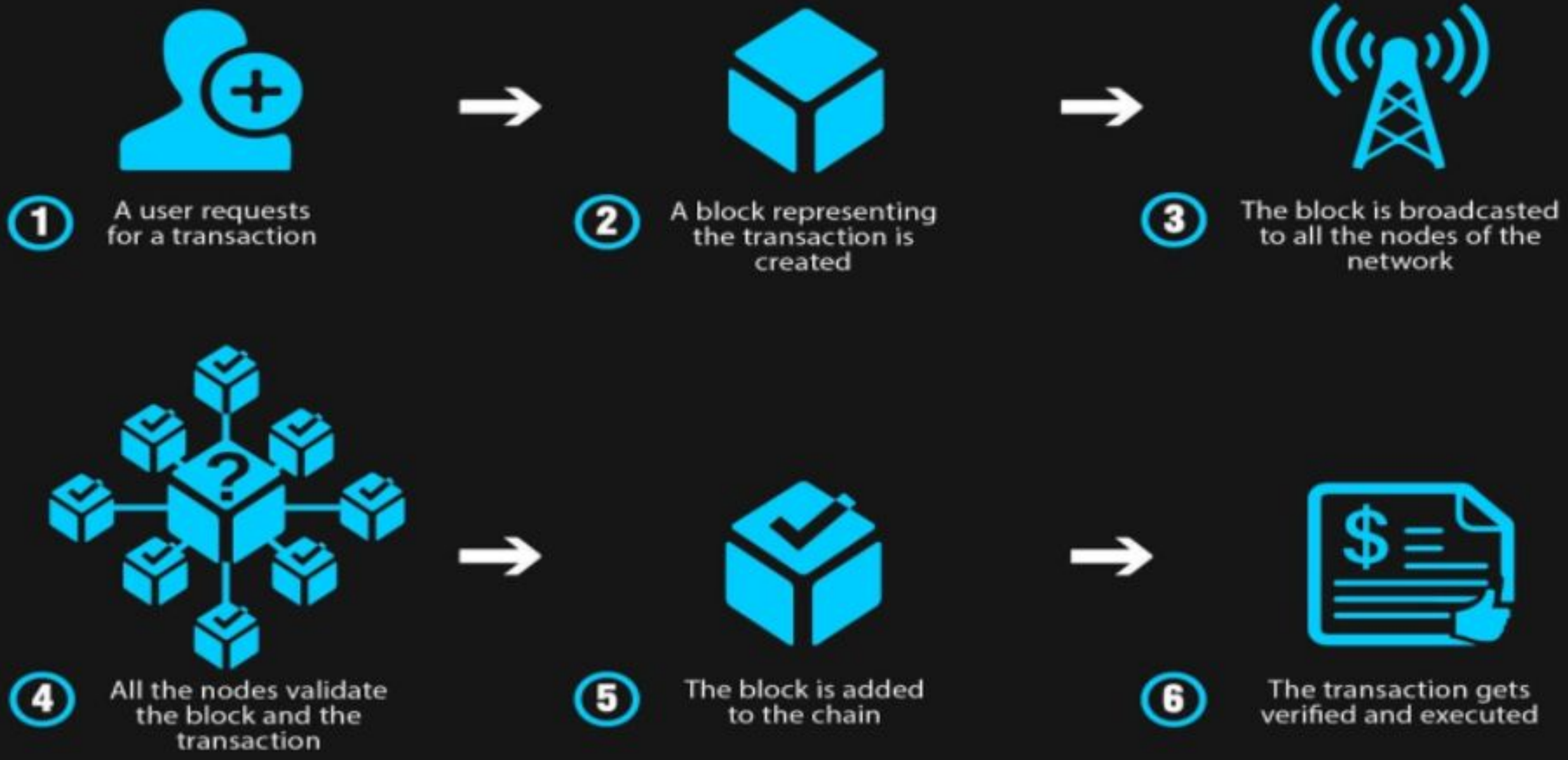


What is Blockchain ?

- Transparency, security and a decentralized structure form the basis of blockchain technology. Blockchain has a public ledger where all transactions are recorded, seen by everyone, but no one can change it. All blocks in the chain keep a copy of this ledger. In other words, when a record in any block is changed, this situation can be easily detected by the ledgers in the other blocks. This makes it almost impossible to change data.



How Does a Blockchain Work: A Step-by-Step View



1. A user requests for a transaction

2. A block representing the transaction is created

3. The block is broadcasted to all the nodes of the network

4. All the nodes validate the block and the transaction

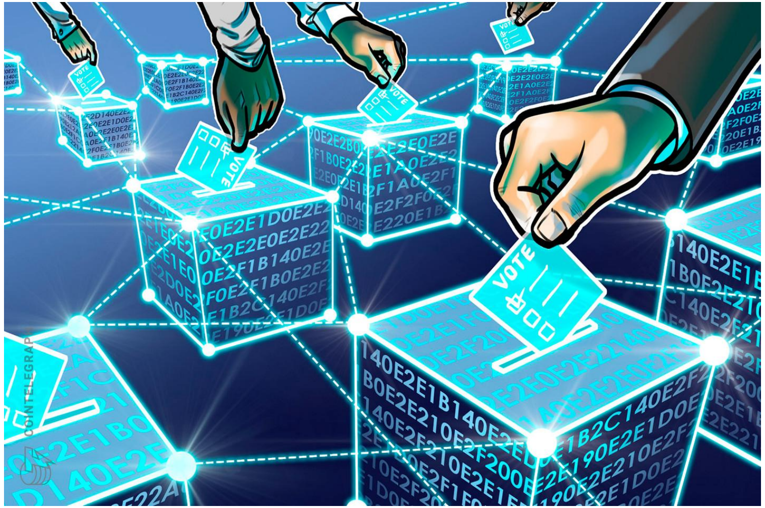
5. The block is added to the chain

6. The transaction gets verified and executed

101 Blockchains
Created by 101blockchains.com

Blockchain Based E-Voting System

- Thanks to this security and decentralized structure that blockchain offers, it can be an almost perfect alternative to the voting system.



- The general purpose of the blockchain-based e-voting system is to perform the voting process on a blockchain chain. Thus, thanks to the security provided by the blockchain, the invariance and security of the votes are ensured and the need for a central authority is eliminated. At the same time, blockchain can significantly reduce the process of counting votes and announcing results.

In this project, we aimed to examine and bring together the researches on the blockchain-based e-voting system, to address the advantages and disadvantages of this system, and to offer a solution that can be an alternative to existing applications. In the Related work part of the project, the existing research and solutions found so far have been examined. The features of the solution we propose are explained in our propose section.

State of Art

Although the blockchain based e-voting system is not common today, it has started to be developed and implemented in some countries. Until now, a lot of research and studies have been done on digital voting around the world like Germany, Netherlands, Estonia, Japan, Norway... Some of these are:

Sierra Leone

Sierra Leone conducted a Blockchain-based voting system on March 7 and it was the first country to become this. Leonardo Gammar of the Agora provided instant access to election results by keeping the votes in a uniformly distributed ledger.

State of Art

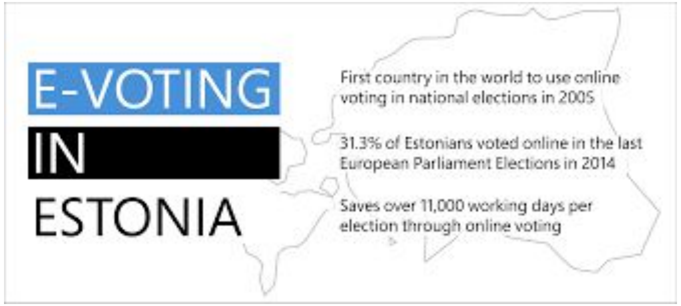
Russia

Moscow authorities planned and launched a blockchain-based electronic voting system pilot project in June 2019. The project was carried out in partnership with the Moscow City Election Commission and the Moscow Information Technology Department (DIT). They provided the necessary support to test the project.

State of Art

Estonia implemented the European Union's first country-wide internet voting system in 2005. Their systems are based on the national ID card that all of the Estonian citizens are given. These id’s consist of encrypted files which uniquely identify the owner. First of all voters must enter their card into the card reader and must access the voting website of the connected computer. They may also use their mobile phone. After that they use their pin number to see if they are eligible to vote. If they are eligible to vote they can cast/change their vote up until four days before election day. When the voter submits his/her vote, the vote is sent to the vote server which is publicly accessible. Votes reside there until the voting timeline is done.

When this voting period is over all votes are transferred by a DVD to the vote counting server after each of the votes are cleaned identifying information. Each of these votes are decrypted and counted by the server then outputs the result.



First country in the world to use online voting in national elections in 2005

31.3% of Estonians voted online in the last European Parliament Elections in 2014

Saves over 11,000 working days per election through online voting

Some Problems may occur as follows:

Client side machines can contain malware and this can cause some serious problems like changing the original vote of the voter.

There can be a malware on the DVD and it may affect the servers so that the election becomes untrustful and corrupted

Our Model

- Our model provides many features. Some of these features can be listed as follows:
  - Registration/Authentication/Eligibility : System should allow voters to vote for only once, only for the people who have registered the system before the election and which are eligible to vote
  - Anonymity : Any information that may reveal the identity of the voter should be confidential and not monitored by anyone
  - Accuracy : Every vote must be counted correctly and not changed by someone else
  - Security : Security will be provided by encryption mechanisms such as public-private keys hash functions
- Voters can vote in a 2 way either by using online platforms or in polling centers.
  - The voters indicate whether they want to cast a vote in online platforms or polling centers.

Our Model

- Our model is not fully decentralized.
- It is not so easy to make fully decentralized, because the government is necessary during the registration.
- Our model has a layered structure to increase speed of the synchronization.
  - The country is divided into regions.
  - Firstly, the ballots become synchronized in their region.
  - Then, these regions become synchronized across the country.

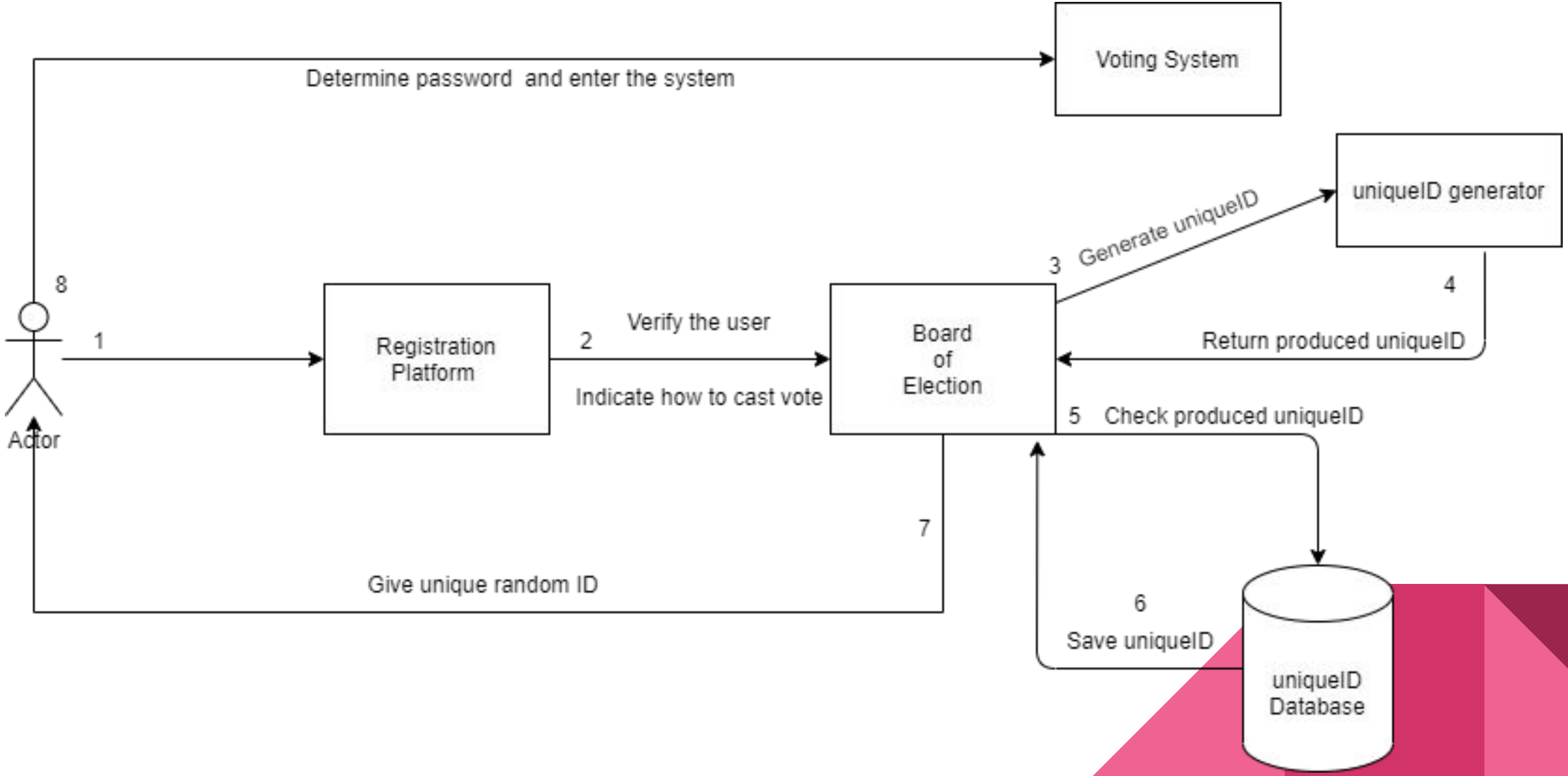
Registration

- Eligible people are determined by the institution.
  - E.g. YSK in Turkey, Board of Election in US.
- The election rules are determined and announced through the people by institution.
- People should be registered to system by using online platforms or going to institution.
  - E.g. Online platform: e-devlet in Turkey, IRS in US
- People can us citizenship number or passport to verify themselves.
- The system produces the random unique ID for eligible people.
- The unique ID is stored in a database to satisfy uniqueness.
  - No other information except password is saved in database to satisfy anonymity.

Registration

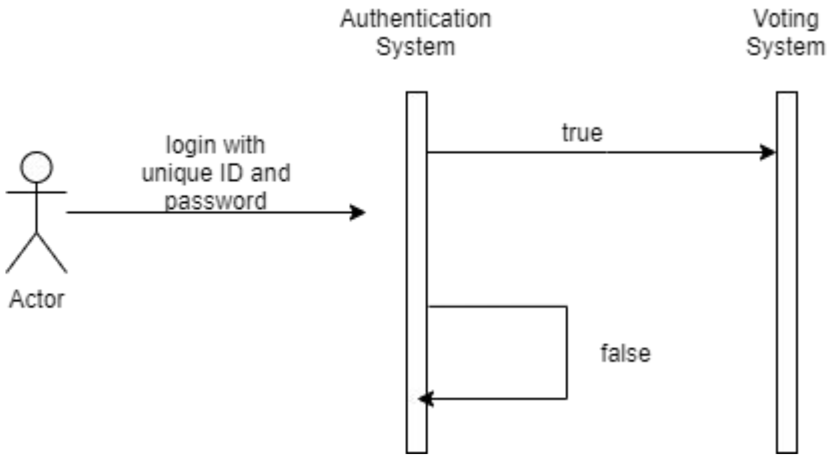
- The voter is marked as received in separate database after receiving the unique ID.
  - Prevents to receiving second unique ID from the voter.
- The first 2 digits indicate the region that the voter cast a vote.
  - Prevents to cast a vote for another region.
- The voter indicates whether cast a vote in online platform or polling center during the registration.
- The voter determines a password after receiving the unique ID.
  - The password is mapped with unique ID.
  - Increases the election’s security if the voter forgets or loses the unique ID.

Registration



Authorization

- Enters the unique ID and password in order to enter the system
    - Do not forget your ID or password otherwise you cannot access the system and use your vote

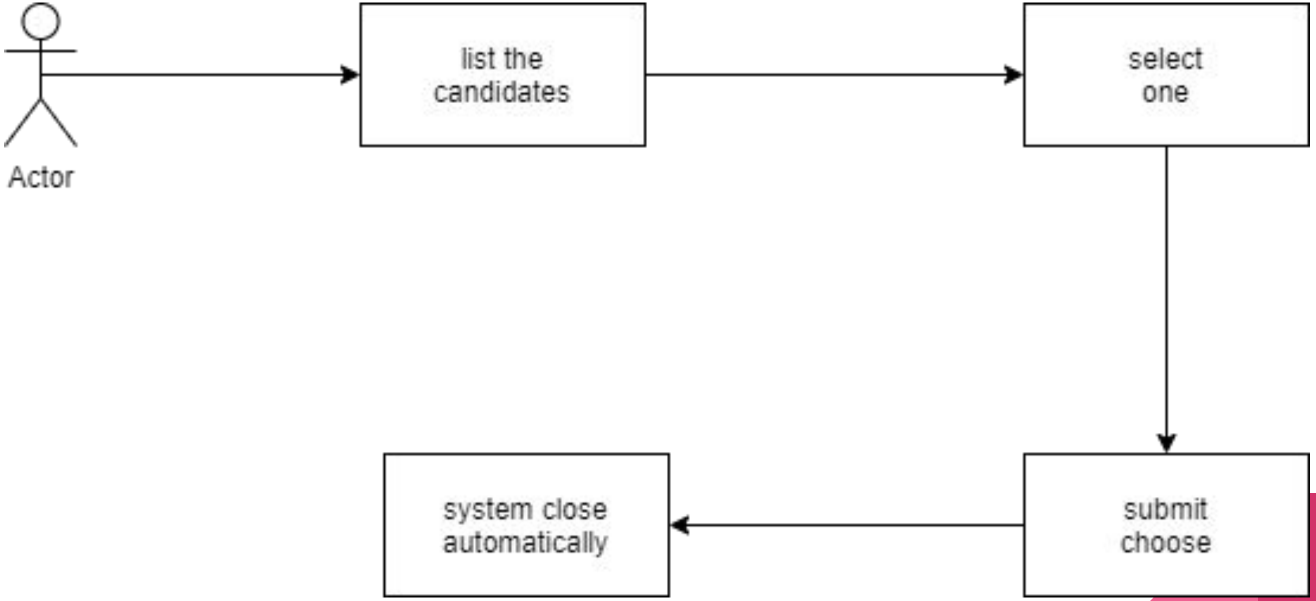


Authorization

Casting Vote

- The voter has 5 minutes to cast a vote.
  - Time can vary with respect to election rules.
  - Prevents the density in the system.
  - The voter can enter the system until casting a vote.
- Candidates appear in the system.
- The voter casts a vote a candidate.
- The system closed after casting vote and will not allow any other access to the system.
  - Prevents the double-casting.

Casting Vote



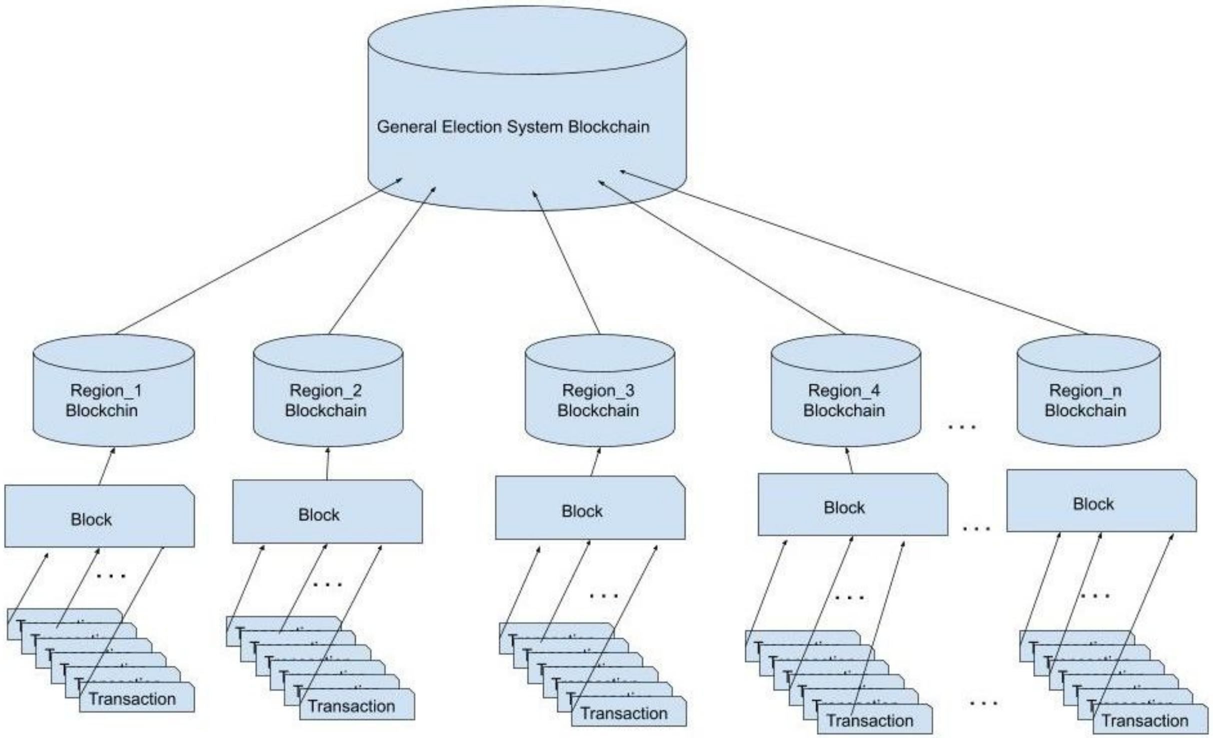
Voting Process and Architecture

- Synchronization is one of the most important problem especially for big countries.
- The system can have delays while adding transactions to election system.
- We proposed a layered-structure system.
- There are 2 layers which the first one is the region and the second one is the general.
- Firstly, the votes are combined in the region.
- Then, the regions are combined in the system.
- Periodically, the regions’ blocks are added to the system.
  - The system is being closed to cast a vote during this period.
  - The synchronization period can take approximately 10-15 minutes by vote count.

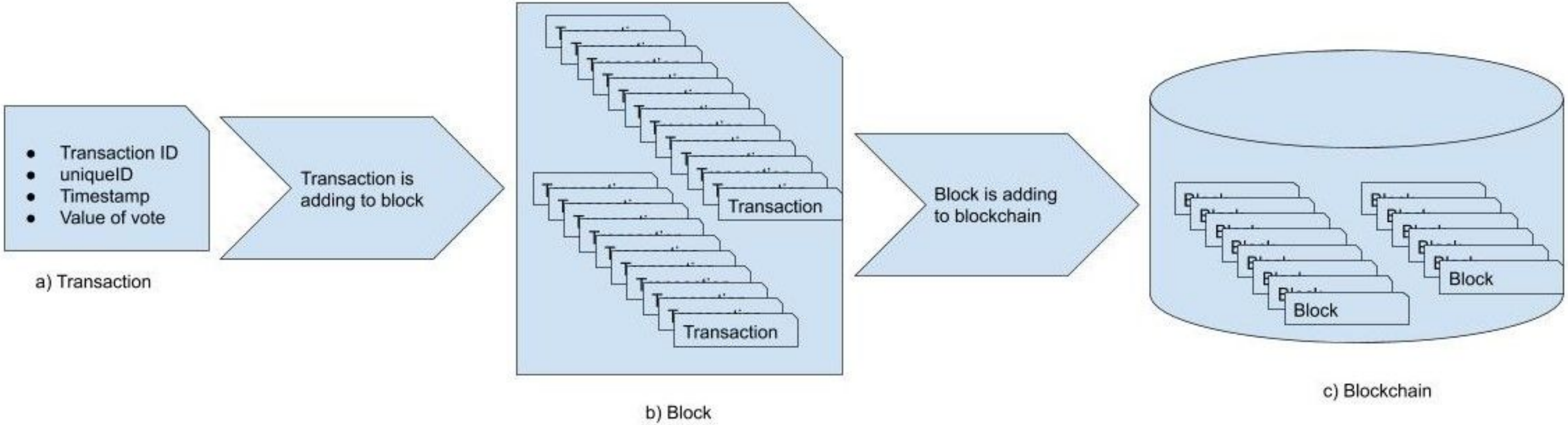
Voting Process and Architecture

- The transaction includes {transaction ID, unique ID, timestamp}, and{value of the vote}
- System will look the first two digit of unique ID and finds the corresponding public key of the region and after that encrypt the transaction with this public key so that only corresponding institution can decrypt and verify the transaction by using its private key
- It is important to note that this transaction information is not revealing any information about voters identity because unique ID does not correspond to any information about voters identity in the database.(Anonymity provided)
- After that transaction will be added to the block.

Voting Process and Architecture



Voting Process and Architecture



- Transaction ID
- uniqueID
- Timestamp
- Value of vote

a) Transaction

Transaction is adding to block

Transaction

Transaction

b) Block

Block is adding to blockchain

Block

Block

c) Blockchain

Counting Votes

- Votes will be started to count while the voters continue to cast a vote.
- Votes are counted during the voting process.
- When the final region blocks are added, the last votes count and the result will be announced shortly.
- Results will become available to everyone after the voting time has elapsed

Our Model Overview and Problems

- Forgetting the unique ID or password on the election day. Voter cannot enter the system so that voter won't be able to cast a vote on that election. In addition we said that eligible voter can get a unique ID for only once for a specific election, in this case if unique ID get stolen or if the voter forgets it there is no way for the voter to use its vote on that election. Securing its unique ID and password is under voter responsibility.
- Viruses, trojans,worms or malicious software on client side hosts.
- DDoS attack which targets the government institutions but it is also government institutions responsibility to provide their security.

Our Model Overview and Problems

- Stolen private-public key pairs of the region institution.If the institution’s private keys are stolen, the votes can be manipulated by attackers.
- The voter cannot track the vote.
    - This can be seen as a problem or lack of the system, but it is not also possible in paper-based elections.

Conclusion

- In the face of cyber threats, the deployment of reliable electronic services systems becomes an important task.
- The analysis showed that blockchain technology can be useful for this purpose. Particularly, for developing electronic voting systems.
- Classical systems do not meet all desired requirements for voting systems (for example, a voter cannot check whether his voice is correctly taken into account and, if necessary, inform the authorized bodies about this).

Conclusion

- In our model, it was developed as a solution to the problems of classical electronic voting systems and to the problems of legacy voting systems.
- By offering two different ways to vote, an alternative was created for users who could not adapt to the new systems.

Who did what?

- Gökhan Özeloğlu: Wrote proposed model and state of art, prepared slide, drawing some schemas.
- Burak Yılmaz: Wrote proposed model and state of art, prepared slide, drew some schemas.
- Dilara İşeri: Wrote introduction part and state of art part of paper , prepared slide.
- Necati Berk Özgür: Wrote traditional Voting vs. E-Voting
- Fatma Usalan: Wrote conclusion part, drew some schemas.

THANKS FOR LISTENING