Blockchain Based e-Voting System

Gökhan Özeloğlu
Hacettepe University
Ankara, Turkey
b21627557@cs.hacettepe.edu.tr

Burak Yılmaz
Hacettepe University
Ankara, Turkey
b21627868@cs.hacettepe.edu.tr

Dilara İşeri
Hacettepe University
Ankara, Turkey
b21783561@cs.hacettepe.edu.tr

Necati Berk Özgür
Hacettepe University
Ankara, Turkey
b21785229@cs.hacettepe.edu.tr

Fatma Usalan
Hacettepe University
Ankara, Turkey
b21727829@cs.hacettepe.edu.tr

ABSTRACT

Election process is of great importance for all countries. Traditional elections are behind the age and have been insufficient with the rapid development of technology recently. There are problems with traditional election, such as attacks on votes, privacy of the voters and transparency of the process. When the problem of taking too much time for the voting and counting process is added to this, it becomes necessary to develop a new method. Nowadays, people try to do everything in the easiest, fastest, safest and most effective way to keep up with the times. That's why we designed a model that solves the existing problems of the traditional voting system with blockchain technology. Blockchain, which is a new technology for the whole world, solves many problems in the traditional voting system such as security of votes, privacy of the voters, and waste of time.

1 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. Elections play a decisive role in the future of countries and the lives of their citizens. No matter what kind of choice is made, the basic rule is that it is reliable. Traditional voting is a centralized application. Centralized voting means that the voting process is carried out and managed by a center. The traditional voting or paper-based voting process is as follows. State-authorized election boards in the countries determine the voters who can participate and vote and send a paper ballot to the voters. Voters vote by going to the election centers written on the ballot papers. The votes are collected at the ballot boxes in the election centers and at the end of the election, the ballot boxes are opened and the votes are counted. This process can take a long time depending on the size of the selection and the population of the country. 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.

Technology is developing rapidly today. However, new technologies, new applications and systems are entering our lives every day, which will make our lives easier. These technologies aim to make our lives easier, as well as solve the problems in our current systems. Blockchain, which is a new technology , is one of these technologies. Transparency, security and a decentralized structure form the basis of blockchain technology. Blockchain has a public ledger where all transactions are recorded, visible to everyone, but no one can easily change. 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. In addition, losing data in a block does not harm the existence of data, since the data is not stored only in one center. Because the copy of the data already exists in other blocks. In this way, the blockchain ensures the security of the data by keeping all data in all blocks. Thanks to this trust, the need for a central authority is eliminated.

Thanks to this security and decentralized structure that blockchain offers, it can be an almost perfect alternative to the voting system. In addition, one of the negative aspects of traditional voting is that it takes a very long time to count votes and announce the result. In fact, the time that passes until the announcement of these voting results causes voters to doubt the accuracy of the results or the possible attack on the votes. Blockchain also solves this time problem due to its nature.

Blockchain-based e-voting system is generally as follows: Voting is done on a blockchain chain. When Voters vote, this vote is added to the chain. In this way, the votes can be seen easily by everyone. In this way, votes cannot be changed. However, there is no personal information about voters in the chain. Only voters have addresses determined by the system. Thus, the privacy of voters is ensured. Although the blockchain based e-voting system is not common today, it has begun to be developed and implemented in some countries. But of course there are some problems brought about by this system.

This paper aims to review and bring together the researches on the blockchain-based e-voting system in general, to address the advantages and disadvantages of this system, as well as to offer a solution that can be an alternative to existing applications. This paper also includes the problems caused by traditional voting and the solutions that can be brought to these problems with blockchain. In the Related work section of the Paper, the existing research and

solutions found so far have been examined. The features of the solution we propose are explained in our propose section.

2 RELATED WORK

Until now, a lot of research and studies have been done on digital voting around the world. Some countries like Germany, Netherlands, Estonia, Japan, Norway, Sweden, Switzerland tried e-voting but they quickly went back to paper based elections because of shortcomings in the areas of security, transparency and privacy. Considering all of these works and researches that has been done so far, we we will mention the related work that has been done so far and the e-voting systems have been used until now in this section.

In one study [1] it supports self counting of votes with maximum voter privacy was proposed. It tested an election with small scale, in this case it was 40 participants. In [2] e-voting is tested in Iceland. Ethereum blockchain was used with an ID authentication company to make sure about the voter's identity to prevent fraudulent people. On that paper authors claimed that the system supports cost-efficient elections while preserving the privacy of the voter. In contrast, Iceland is a small sized country with a small population so in this case that study may not be convenient for countries with a big population such as USA, China ...

In [3], it is designed for national scale e-voting by protecting voters privacy. Voterum supports robustness, ballot privacy, individual verifiability, and universal verifiability but it has scalability problems because it relies on ethereum which is a public blockchain and has a huge number of transactions other than those that will come from national election.

In [4], Ques-Chain claims that it can provide authentication during e-voting without damaging confidentiality and the anonymity of voters. Also authors of that paper claims that, system can be used nationwide because of its high security requirements. However it also relies on ethereum, which has a huge amount of transactions other than national e-voting therefore scalability problem is very potential.

In [5], Hyperledger Fabric was used for e-voting. Chain code which implements the smart contracts make it easier to provide security and efficient transaction while protecting the identity and privacy of the voters. However there is not an actual implementation of it.

In [6] TrustedEVoting (TeV) framework is used. It is a mixture of cryptography and permissioned blockchain to make sure the security in a more trusted way. It also provides voter anonymity and voters can check their vote after the election. Unfortunately, there is not an actual implementation of it nationwide.

In [7], A blockchain based e-voting system suggested which uses Elliptic Curve Digital Signature Algorithm. In this paper they authenticate voters by using the fingerprint hardware implementation. They also use hashing to encrypt the data. Authors claim that the system was capable of ensuring election confidentiality and increasing the number of participants.

In [8], Authors suggested an architecture for South Africa by taking the requirements of the stakeholders who take part in the South Africa Election Commission. They claim that researches done for now just did not ask stakeholders about the requirements; they did only domain analysis and general requirements so this paper basically differs in this way from the others. Therefore it targets a specific location, South Africa, not the nationwide. They asked the South African Independent Commission what are the requirements they expect from a blockchain e-voting system. The requirements are trust, transparency, verifiability, auditability, availability, performance, non-coercion of voters, socio-economic influences, socio-political factors. Based on these requirements they proposed a layered architecture which consists of client layer, application layer, blockchain layer, data storage layer. Client layer, has various electronic devices and some systems which users can interact with. These devices are called peer nodes and they interact via smart contracts. There are different types of peers and each of these type of peers have different roles. Application layer consists of some services that e-voting system can contain. In blockchain layer they use hyperledger fabric. Data Storage layer contains databases that store information about registered voters and candidates. In addition to that architecture they use smart cards for authentication to make sure that only eligible voters can vote. These cards will be distributed by the central authority and it will contain the voter's public key and a PIN number. Moreover they agreed to use zero knowledge protocol to provide privacy and anonymity by hiding the identity of the voter and its choice. It is assumed that the casting votes will take place at polling units to make sure that no one has been forced to vote in a certain way by politicians or their agents. Voter uses his smart card to authenticate himself by inserting it to the voting node, if it is successful a digital ballot will be created with candidate public keys and a unique ballot id. Voter chooses one of the candidates and submits the vote, then ballot id is assigned to the candidate which is selected by voter through their public key. Finally the transaction is authenticated by using the digital signature of the private key and sent to all nodes on the blockchain. Considering this solution using smartcards and public-private key encryption enhanced the security. These features provide only eligible voters will vote. Anonymity of the voter can also be supported by using zero knowledge proof. Man-in-the-middle attacks are also prevented by using smart cards. Finally authors of the paper offered to span the election to a few weeks so that everyone can vote in different days and this will minimize the traffic and high volume of transactions per day. However this suggestion can have an impact on reliability, accessibility and security in a dangerous way.

In [9] they examined the Estonian e-voting architecture and based on that examination they propose their own solution. They used two separate blockchains. One for transactions relating to which users have registered and which users still have a vote and the other one to store the contents of vote. By using this approach they claim that voter anonymity is provided by removing threats to associate votes for certain candidates with individual voters while providing the ability to track who was voted and the number of total votes. They use tier architecture and because of this and the encryption mechanism they used it is almost impossible to gain access all the votes without taking the control of entire network. At the end they

publish the private keys of constituency therefore by using that private key, it allows anyone to verify election result by decrypting blocks. One potential risk of this system is if a voter forgets his password, id, or ballot on the day of voting, the voter will be unable to cast the vote. Another possible risk is, in their approach the individual nodes which are selected by the government if they meet the requirements. In this case if a corrupted person who works for the government selects these individuals, election trustiness will fail. The most important problem is actually attackers can directly target the voters own devices and in this case there will be an insecure connection between polling station and voters device. Therefore any possible network attack can cause serious damage on the election.

In the research [12], the benefits and weaknesses of the E-voting system were first mentioned. According to the authors of this paper, the most important weakness of the E-voting system is the lack of transparency and understanding of the system which leads to lack of trust in the solution and undermines its whole sense. The article presents the use of smart agents and multi-agent system concepts for blockchain-based e-voting system. It has been proposed to use blockchain technology to create an e-voting system that can be overseen and verified by voters. This is a delegate-based voting idea. Also in this study primarily aims to meet the transparency and verifiability features that should be found in the e-voting system. In this paper, the researchers explained the previously proposed Auditable Blockchain Voting System (ABVS) to provide a basis for their own ideas. To briefly mention the ABVS system: It is a non-remote and supervised electronic voting system. The AVBS system consists of three components. These are: super-node, trusted nodes, polling stations. The super node is the parent node that reports directly to the National Election Commission. All votes are first transmitted to it and counted there. The chain stored in the super node is considered the most important chain and counts votes accordingly. The task of trusted nodes is to collect votes and create the correct chain using the consensus algorithm. They are the remaining nodes of the blockchain network, approved by the National Election Commission. Trusted nodes provide a backup chain in case the main chain is damaged or lost. Polling stations are voting applications that represent individual voting districts here. They allow voters to vote. All the mentioned above elements of ABVS system communicate within a peer-to-peer network. The five basic components in ABVS are: network of trusted nodes and polling stations, Vote Identification Tokens, ABVS blockchain technology, counting application, voter-verified paper audit trail, vote error notification module. Researchers express their opinions on ABVS. This is the Multi-agent system for ABVS system.

A multi-agent system generally consists of a representative who cooperates by communicating, working in an environment, having different spheres of influence and connected by other organizational relationships. Agents are often used in situations where it is necessary to solve sporadic or computationally complex problems, and these agents pursue and cooperate with common goals.

In the multi-agent system, there is no distributed architecture and no specific central data source. It is difficult to control the entire project with a single representative. The advantage of multi-mediated systems is that they work asynchronously, that is, they are independent. In addition, researchers in [12] believe that a properly constructed system would also be resistant to damage from some agents. The use of smart agents with the solution suggested in this paper significantly increases the safety of the ABVS system. The recommended agent types in this research are: authorization configuration agent and voting agent.

The authorization configuration agent deals with the authorization and configuration of the voting application in individual polling stations. The role of the voting agent is to provide a voting card for the voter, and the timestamp, VIT number, data identifying the voting location, etc. Submit a vote to nodes with all necessary vote metadata, including. The main advantage of the multi-agent based ABVS e-voting solution is to increase voting security by reducing the practice in polling stations to the intermediary between agents who will take over all voter related tasks. Processing and transmission of votes. Agents are thought to be distributed by nodes so that they cannot be changed from outside. Additionally, the researchers in [12] noted that this solution allows computing resources available at voting stations to be used to process votes, thus reducing the load on nodes. The researchers proposed the Ethereum platform and smart contracts for implementation at the end of the paper.

In this research [10], the researchers propose a multi-channel hybrid system based on the blockchain technology of the Crypto-voting system. The purpose of this system is to allow remote voting for voters who live far from membership. The researchers suggested the use of mobile phones or personal computers for the remote voting system. Thanks to this Crypto voting system, the researchers aim to guarantee continuity with traditional voting and accessibility to IT illiterates.

In the paper [10], side-chain technology is suggested to implement Crypto voting. To talk briefly about side-chain technology: side-chain expands the blockchain and allows the creation of new features by both overwriting the main blockchain, reducing costs and risk of failure, and avoiding the need to create a new currency. Also, with side-chain, a system based on the combined use of main blockchain and sub-blockchain communicating with each other can be created. In the crypto voting system, it is aimed to use a permissioned blockchain (i.e. subject to authorization), providing anonymity and privacy requirements. Side chain BitPoll is created in this system. Later, the Crypto-voting blockchain is frozen, eliminating blind scripts by associating them with a hash signed by the trio responsible for the election with their private signature. This process eliminates the following possibilities: Triad reopening the blockchain without complicity, Ex-review nodes changing individual votes without complicity, reconstruction the association of the vote to the voter.

With this recommendation, the researchers in [10] promise to provide truly customizable, integrable, and sufficiently reliable services to their users at the same time. At the end of this paper, the researchers state that in this proposed system, they plan to use the cloud system to realize the virtual voting booth and to examine

the integration of cyber security and privacy tools to protect the blockchain in the cloud system.

The voting system in this article [13] is divided into two parts, which are lower and upper level. For the people who will vote, the identity verification is first made to check whether they are suitable for voting. Later, a new ID is assigned by creating a wallet for these people. Candidates become members of the same system. When voters make their elections, the created token is sent to the candidate's wallet. This token replaces the vote and when the transactions are completed, the vote count is made with the number of tokens.

In this paper [14], writer combine the zcash and voting protocol. Zcash is payment scheme. It provide anonymity and privacy of transaction. Proof of work part is different from bitcoin. Zcash has two types of addresses. These are z-address and t-address. Z-address preserve anonymity in transactions, t-address resembles the bitcoin addresses structure. When sender and receiver use z-address, private transactions occur. Z-address consist of 4 different keys. There is a nullifier for each ZEC (value of Zcash). Nullifier can be considered as a serial number for each ZEC which prevents double-spending of the same ZEC. Ephemeral keys are established for secret value transmission. JoinSplit is part of the transaction. It is for the sender to spend their Zcash.

In another article [15], as in the most other implementation, firstly voters must be registered to system by eliminating citizens who are eligible to vote. After registration step, all voters are given Ethers, and unique keys to vote. On voting day, voter must visit the voting poll and skip verification process to vote. Voting system mentioned in [15] has three layers: front end, application layer and a Blockchain system based on Ethereum. Our topic of interest, Blockchain layer is based on Ethereum Smart Contract. Ethers here should be considered as not votes themselves but as a voting fee.

Paper [16] proposes a solution which considers security in the first place. For example, they propose that cryptographic features of the blockchain system satisfies privacy of votes/voters. Collision resistance property also prevents voter from misuse. Also, to cast a vote, citizens are counted as eligible or not by using their biometric indexes, such as their fingerprints. In article [16], while process is very similar to article [15], application layer differs. In [16], an Access Control Management layer is used to increase security and isolate voter and election authority. As Blockckhain implementation, [16] uses Multi-chain technology.

In [17], the authors mainly proposed a Blockchain-Based e-Voting system for Turkey. Firstly, they mentioned the possible problems of the paper-based elections. Their model is consisting of nodes that can be seen as computers. The eligible voters are checked by e-government. The model's whole voting process can be summarized in three main titles. These are authentication, voting, and counting. Also, the voter who casts a vote is marked in the system, in this way, double-vote is being prevented. Any ballot information is not sent to the system for protecting privacy. As in the other blockchain applications, the ballot is adding to the system after a transaction is created with keeping previous transaction information. That's why manipulation of the ballots is impossible after the transaction is added to the block. There is a chain that contains all ballots so that the election results are announced in a short time. Their model has a layered-structured architecture. In the synchronization periods, the system is closed for a short time. At the lowest level, the blocks store one transaction. At the upper layers, the blocks are combined and stored in a monolith structure.

In [18], SHARVOT means that secret Share-based Voting on the blockchain. They use Shamir's Secret Sharing algorithm. The protocol is based on Shamir's Secret Sharing Scheme and shuffling technique which name is Circle Shuffle. The vote is casting a 64-bytes key. Shuffling and encryption are implemented for de-linking of user's information from their vote.

3 PAPER-BASED ELECTION SYSTEM PROBLEMS

Ballot based voting systems are being used since Ancient Greek democracy. Despite its long history, it still has some problems unresolved.

First of these problems is theft. Since paper based elections are carried out in voting centers such as schools, sports centres or other public places, ballots must be transferred from stations to center. During this transfer period, although maximal security measures are taken, a theft may occur. Blockchain-based elections bring the ultimate solution to this issue since it is impossible to manipulate numbers in blockchain systems.

Another major problem in ballot based is counting. Counting of ballots involves many sub problems. First and most important of these problems is: Error of Fact. Since all votes are counted by humans there can be always shady results or misinterpretations resulting in erroneous results and trust loss. Another negative aspect of counting is the fact that especially in heavily populated countries, counting takes so much time and human effort. As a result of this human effort, counting also causes waste of resource. A well constructed software based election system will resolve all these issues since it will be precise, fast and cheap.

As mentioned above, waste of resource is an important drawback of paper based elections. Not only limited with resources wasted by the people counting votes, but also includes resources for many people who are responsible with managing election centers, paper ballots and transfer of these ballots from/to central election authority. A blockchain based election system is not going to need all this physical environment since it will be software based and easily accessible.

Accessibility of blockchain based voting systems also solves another major problem is participation. Handicapped and elderly voters are mostly unable to go to a voting center. In blockchain based election, voter does not have to go to a voting center to vote since they can vote remotely by their smartphones or computers. Also low participation rates in elections in some countries will be increased by ease of access. Paper based elections uses ballot letters to increase participation rate and ease of access. But this solutions comes with drawbacks such as increasing the time required to complete elections and manipulation or loss of votes. In a blockchain

based voting system, since a vote in a blockchain can be traceable, voters do not need to worry about their vote.

An online voting system will also solve problems faced in voting centers such as long waiting queues and mistakes made during voting, such as voting seals pressed out of box, contagion of ink to other boxes and various other physical issues.

In conclusion, a blockchain based digital election system will resolve many issues coming alone with paper based election systems such as key problems like trustworthiness of current election system, wasteful resource allocations and efforts made by voters and election staff both.

4 OUR MODEL

In this section, we are going to propose our solution for a blockchain-based e-voting election system. In our model, voters can have two options to use their vote either by using online platforms or physically by using voting machines in predetermined election areas. Our model has two options because there might be some people who have disabilities or are not familiar with technology or online platforms. In addition, some people use old phones rather than smartphones. Therefore, these people should also be able to cast a vote in our election system. In order to make this goal successful, we have physical machines that give a chance to these kinds of people to vote easily for that purpose. For the convenience our model is not fully decentralized. In the registration step a government institution will take place to register the people to the system also they should verify the identities. For that reason we thought it is more convenient and easier to verify the identities if we involve a government institution to our model. We will first mention some requirements that our solution supports shortly and after that we go into detail step by step.

(1) **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.

(2) **Anonymity:** The people who cast their votes should be anonymous for the nature of the elections. The votes and voters should not be tracked by other people or the government. For these reasons, any information that may reveal the identity of the voter should be confidential and not monitored by anyone.

(3) **Accuracy:** Every vote must be counted correctly and not changed by someone else. It is the essential part of the elections all over the world. Also, there can be invalid votes because of the people's faults. This will be prevented, so that the accuracy will be increased in our model.

(4) **Security:** We will provide a secure system as much as we can. Security will be provided by encryption mechanisms such as public-private keys hash functions and the architecture that we use which is layered architecture in this case.

We divided our model into steps. There are 5 different steps to cast a vote successfully. Each of them must be accomplished successfully.

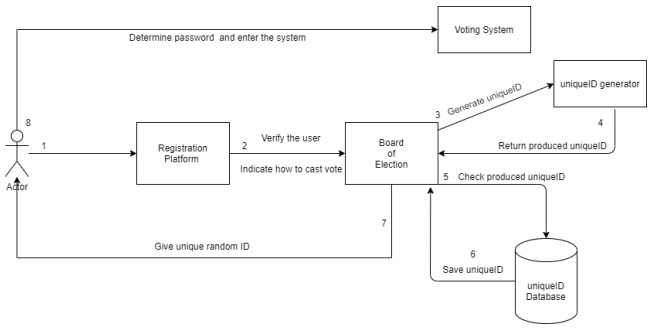

Figure 1: Registration

4.1 Registration

Firstly, eligible people should be determined by an institution. This institution may already exist like YSK in Turkey. The rules for being eligible voters can be changed in countries. That's why these rules should be determined by the government before the election. Once these rules are determined by the government, people should register into the system by using online platforms(e-devlet in Turkey or IRS in the USA) or by physically going to the institution. People should register themselves by using their ID(like TC Kimlik NO in Turkey) or passport so that the government can verify them without any problem. Once the eligibility of the voter is confirmed, the system will produce a random unique ID to the voter in order to access the voting system on election day. The unique ID will be saved on the database anonymously. Any personal information will not be saved in this database to ensure anonymity. The system controls the newly produced unique ID in this database to make sure the new one is unique and stored it by firstly taking a hash of that unique ID. When the voter receives the unique ID, the voter will be marked as received in a separate database without storing the unique ID hence the voter cannot receive a second unique ID. This received ID's first two digits indicates the region(like the plate number) of the voter because each vote should be added to its region's block. Therefore, the voter cannot cast a vote for another region which is not a valid region for the voter. This unique ID should be stored in a secured way by the voter and not announced to nobody. In addition, the voter should determine a password for entering the system. The voter should enter both unique ID and password while entering the system. Finally, the voter should indicate how to cast a vote, by using voting machines on predetermined voting sites or by using online platforms while getting a unique ID.

4.2 Authentication

On the election day, the voter types the unique ID and password to enter the system. Most importantly if the voter forgets his/her password or unique ID the voter cannot enter the system and cast a vote. This responsibility completely belongs to the voter.

4.3 Casting Vote

After entering the system, the candidates will appear. The voter selects a candidate among various options and submits his/her vote. Once the voter submits, the system will be closed for that

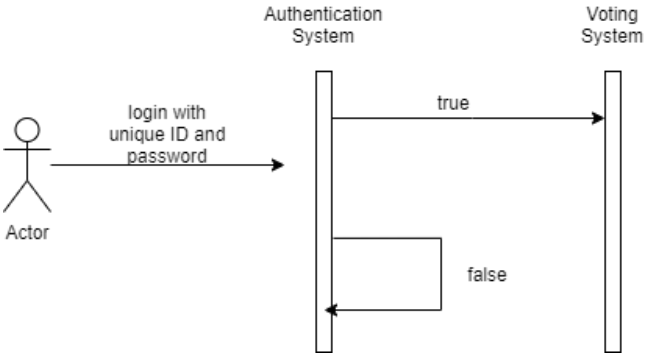

Figure 2: Authorization

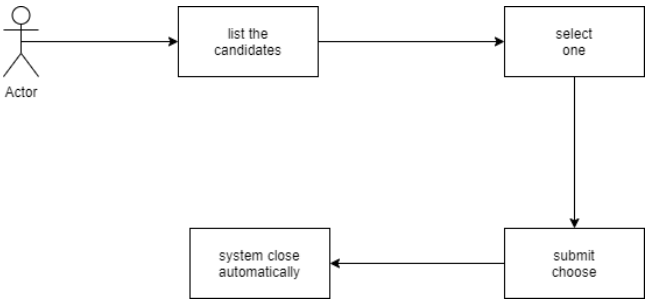

Figure 3: Casting Vote

voter to prevent double voting. After that the transaction part will start.

4.4 Voting Process and Architecture

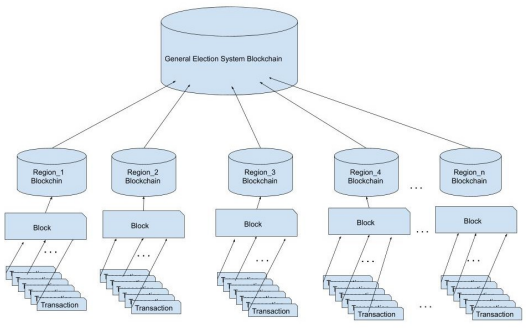

Figure 4: Layered Architecture

Synchronization of the blockchain could be a real problem especially in big countries. While adding transactions to the election system can have delays because of distance between each server. Double-spending or conflict between transactions can occur because of the delays. To solve this problem we propose a layered architecture. In this architecture, the voters will be divided into different groups in terms of their regions. The number of groups will differ depending on the population, area of the country. Transactions will be added

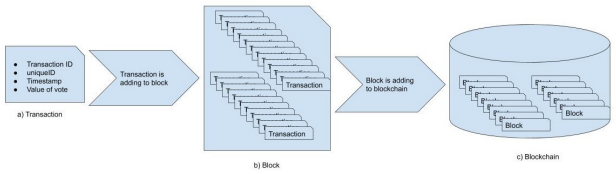

Figure 5: From transaction to blockchain

to its region's block. Periodically, the region's blocks will be added to the general system's block. For example, if the election time is 10 hours, this time can be divided into 5 parts. The region's blocks will be added to the general system's block every 2 hours. While adding the region's blocks to the system's block, the system will stop and nobody can cast a vote at this time. This break time will be a small time like 5-10 minutes that depends on the number of the voter. The synchronization of the system will be protected in this way. Transaction is being produced automatically. The transaction includes **transaction ID, unique ID, timestamp**, and **value of the vote**. We mentioned in the registration process that the unique ID's first two digit is used for indicating the region of the voter system will look this first two digit 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 as we mentioned earlier. In this way anonymity is provided. After that transaction will be added to the block.

4.5 Counting Votes

After the region's blocks are added to the system, the votes will be started to count while the voters continue to cast a vote. The 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. The results will become available to everyone after the voting time has elapsed.

5 OUR MODEL'S PROBLEMS

There might be some problems in our model. The first possible problem is forgetting the unique ID or password. Both of them are essential for entering the system as we discussed before. If the voter forgets or loses the unique ID or password on election day, the voter cannot enter the system so that voter won't be able to cast a vote on that election. We may add a forget password part but due to some network attacks(like network sniffing or hijacking) we don't want to include that part to our system. Another problem might be viruses, trojans, worms or malicious software on client side hosts. In that case there will be an insecure connection between the system and the client so that this can give a serious damage to the election. To prevent this government may force every host to download a secure software but it is costly. Another problem might be a DDOS attack which targets the government institutions in our model however this problem is not rely on our discussion we assume that

institution is responsible to provide its own security. Also there can be a problem with private-public key pairs. If the institution's private keys are stolen, the votes can be manipulated by hackers. Finally, the voter cannot follow the vote. Actually, this situation is the same as the paper-based elections. That's why, not following the votes could not be evaluated as a problem or lack of the system. Nonetheless, not following the votes can be seen as a problem in comparison with the Bitcoin system, but we had to provide the anonymity of the voters. Tracking the vote is a contradiction with anonymity.

6 CONCLUSION

Thanks to the features provided by blockchain technology, more secure and transparent voting systems can be created. It has proven to be more useful than systems that require trust in the center. In this article, we mentioned that many negative features can be solved. It not only solves the problems of old voting systems, but also provides solutions to problems encountered in other electronic voting systems. In this article, we examined the voting system model we created with blockchain in 5 steps. The first step is the registration step. In this step, those who will vote are registered to the system and how they will be cast is selected. Two options are offered as voting method, one by using applied devices at physically determined addresses, and the other by using voters' own devices. Also, at this stage, a unique ID is determined by the system for voter and creates a voter password. The second step is the authentication step. In this step, the person logs into the system with the unique ID and password given at the registration stage. The third step is the voting step. In this step, after successful login to the system, voter sees the list of candidates on the screen and confirms the candidate he wants. The steps up to this point were related to the registration and voting of voters. The last two steps in our model definition are about the inclusion and counting of votes in the counting process. In order to avoid double spending or conflict, the process of adding votes to blocks can be resolved by making the process of adding the votes to the blocks at certain hours and stopping the voting process during these hours. Counting of votes can also be performed while adding blocks. In this way, confidence in the voting process can be increased. Because it is not possible to make a wrong count or change the votes. As a result, we can say that voting systems developed with blockchain are more reliable and transparent. The financial and time loss that occurs in traditional voting methods is also prevented. Besides these advantages, it is questionable whether societies are ready for this or not. Apart from the problems of trust in new technologies, it is okay to trust voting with blockchain. The main purpose of presenting two different voting options in the model we have created is to avoid victimizing the segment that cannot keep up with new technologies. The provision of devices that will physically count the voting must be provided by the state. This means bringing a new cost to this process. However, the advantage of the created model at this point is that it can offer an alternative to the segment that will not adapt to the electronic voting process. Therefore, we can look at the model as usable in the transition to electronic voting systems.

7 REFERENCES

[1] McCorry, P.; Shahandashti, S.; Hao, F. *A Smart Contract for Boardroom Voting with Maximum Voter Privacy.* In International Conference on Financial Cryptography and Data Security; Springer Science and Business Media LLC: Cham, Switzerland, 2017; pp. 357–375.

[2] Hjalmarsson, F.P.; Hreioarsson, G.K.; Hamdaqa, M.; Hjalmtysson, G. *Blockchain-Based E-Voting System.* In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2–7 July 2018; pp. 983–986.

[3] Thuy, L.V.-C.-; Cao-Minh, K.; Dang-Le-Bao, C.; Nguyen, T.A. *Votereum: An Ethereum-Based E-Voting* System. In Proceedings of the 2019 IEEE-RIVF International Conference on Computing and Communication

[4] Zhang, Q.; Xu, B.; Jing, H.; Zhang, S.; Zheng, Z. Ques-Chain: *An Ethereum Based E-Voting System.* In Proceedings of the 9th International Conference on Computer Science and Information Technology (CCSIT 2019), Sydney, Australia, 29–30 June 2019.

[5] Kirillov, D.; Korkhov, V.; Petrunin, V.; Makarov, M.; Khamitov, I.M.; Dostov, V. *Implementation of an E-Voting Scheme Using Hyperledger Fabric Permissioned Blockchain. In Proceedings of the Applications of Evolutionary Computation*; Springer Science and Business Media LLC: Cham, Switzerland, 2019; pp. 509–521.

[6] Verwer, M.B.; Dionysiou, I.; Gjermundrod, H. TrustedEVoting (TeV) a *Secure, Anonymous and Verifiable Blockchain-Based e-Voting Framework.* In Proceedings of the Education and Technology in Sciences; Springer Science and Business Media LLC: Cham, Switzerland, 2019; pp. 129–143.

[7] Nimje, R.; Bhalerao, *D.M. Blockchain Based Electronic Voting System Using Biometric. In Proceedings of the Lecture Notes on Data Engineering and Communications Technologies*; Springer Science and Business

[8] Olawande Daramola, Darren Thebus, *Architecture-Centric Evaluation of Blockchain-Based Smart Contract E-Voting for National Elections*

[9] Plymouth University Andrew Barnes, Christopher Brake and Thomas Perry *Digital Voting with the use of Blockchain Technology*

[10] Fusco, Francesco, et al. "Crypto-voting, a Blockchain based e-Voting System." KMIS. 2018.

[11] Taş, Ruhi, and Ömer Özgür Tanrıöver. "A systematic review of challenges and opportunities of blockchain for E-voting." Symmetry 12.8 (2020): 1328.

[12] Pawlak, Michał, Aneta Poniszewska-Marańda, and Natalia Kryvinska. "Towards the intelligent agents for blockchain e-voting system." Procedia Computer Science 141 (2018): 239-246.

[13]K. Isirova, A. Kiian, M. Rodinko and A. Kuznetsov, "Decentralized Electronic Voting System Based on Blockchain Technology Developing Principals" *V. N. Karazin Kharkiv National University, 4 Svobody Sq. Kharkiv, 61022, Ukraine*

[14] Hitesh Tewari, Pavel Tarasov, "Future of E-Voting", *School of Computer Science and Statistics, Trinity College Dublin, University of Dublin, Ireland*

[15] Benny, Albin, *Blockchain based E-voting System* (July 11, 2020). Available at SSRN: https://ssrn.com/abstract=3648870

[16] Mehboob, Kashif Arshad, Junaid & Khan, Muhammad. (2018). Secure Digital Voting System Based on Blockchain Technology. International Journal of Electronic Government Research. 14. 53-62. 10.4018/IJEGR.2018010103.

[17] R. Bulut, A. Kantarcı, S. Keskin and Ş. Bahtiyar, "Blockchain-Based Electronic Voting System for Elections in Turkey" *2019 4th International Conference on Computer Science and Engineering (UBMK)*, Samsun, Turkey, 2019, pp. 183-188, doi: 10.1109/UBMK.2019.8907102.

[18] S. Bartolucci, P. Bernat, and D. Joseph, "SHARVOT: Secret SHARebased VOTing on the blockchain," 2018, *arXiv:1803.04861*. [Online]. Available: https://arxiv.org/abs/1803.04861