IMPLEMENTATION OF A NEW E-VOTING SYSTEM BASED ON BLOCKCHAIN USING ECDSA WITH BLIND SIGNATURES

Lina Lumburovska, Vesna Dimitrova, Aleksandra Popovska-Mitrovikj

Ss. Cyril and Methodius University of Skopje, Faculty of Computer Science and Engineering, Skopje, North Macedonia

ABSTRACT

The latest research shows the benefits, the impact, and the usage of Blockchain and decentralized systems with a high confidence. Its popularity becomes even higher with the electronic voting systems based on the technology itself. In this paper we propose a new implementation of an electronic voting system based on Blockchain using ECDSA with blind signatures. Additionally, the system is compared with other electronic voting systems based on Blockchain technology. Mainly these types of systems hardly ever fulfill the scalability. Nevertheless, our system has an advantage in comparison with the other systems. Since the idea of the Blockchain technology is to show the flexibility and equal privileges to all nodes, this implementation with Angular and Spring Boot shows that, so everyone can track the chain. To sum up, this implementation can have a good usage in smaller departments, because of the performances and all mathematical operations.

KEYWORDS

Blockchain technology, ECDSA, e-voting, blind signatures

1. INTRODUCTION

The rapid development of the digitalization and technology increases the need for replacing many processes of everyday life from their traditional way of working to an electronic version of it. The motivation for building an electronic voting system steam from this replacement and can be stated as a direct consequence. On the other side, the popularity of decentralization was the idea behind the Blockchain technology [1] and that is how the centralized systems were also replaced. Having one central node that operates the entire process in one system is not the best approach because in the history there were examples where the data has been changed or abused. Replacing the traditional system with a decentralized system where all elements have the same privileges to it is the main structure of the Blockchain systems [2, 3].

Building an electronic voting system based on Blockchain is definitely a great example how this technology can be used in practice and how the decentralized systems are constructed. In this certain example each vote in the election can be represented as one block in the system. The Blockchain technology is consisted of four elements: peer-to-peer network, cryptography, consensus algorithm and punishment or reward. As soon as these requirements are fulfilled, the system can be created [4].

In the peer-to-peer network all elements are called nodes and they have the same role in the system, where they can asynchronously communicate from different places and time zones. The

David C. Wyld et al. (Eds): MLSC, ITCSS, ACSTY, SOFE, NATP, BDAB - 2023
pp. 145-152, 2023. CS & IT - CSCP 2023 DOI: 10.5121/csit.2023.130211

choice of the cryptography has a major part in the security of the system, so choosing a right cryptographic algorithm has a huge impact on the behavior of the system. Every new node that wants to join the system must prove that it is valid and valuable to the system by solving a given problem. The consensus algorithm can be of different types, but the most used is the proof of work. Based on this third element, the new node can get a reward or punishment if the problem is solved or not [5]. Having these elements in mind, the Blockchain technology can be implemented and used in practice. The Blockchain technology can be used in different sectors such as: medicine, law, IoT (Internet of things), artificial intelligence, cyber security, electronic voting etc. For this paper, the last usage of the above listed is researched.

The last usage of the Blockchain technology can contribute a lot in time when voting is happening [6], since the counting of the votes is not done physically, but instead it is automated. The counting of the votes is done in real time, and the admin can see the statistics over the whole voting process. The hardest part in this case is obtaining the anonymity, so there is no way how the admin or the other users can see which user voted for which candidate. It is important to notice that when we are talking about voting, we do not think always about political voting but instead it is more meant as part of one organization such as: dean elections at the faculty, choosing the project manager within one department and so on.

Implementing an electronic voting system based on Blockchain is a modern topic that professionals work on in the last years. The hardest part in this implementation is keeping the anonymity of the voters, where there is no way how the admin or the other users in the system can find which user voted for which candidate and the vote is still counted in the main statistics. For that purpose, the implementation of the electronic voting system based on Blockchain is done using ECDSA (Elliptic Curve Digital Signature Algorithm) with blind signatures. Additionally, interactive zero-knowledge proof is used to prove the security of this algorithm. There are many electronic voting systems, and this system is also compared with other electronic voting systems based on Blockchain. The main problem that most of these systems have is the problem with the scalability [7]. Our newly proposed system is compared with different systems that are made by companies and individuals. Based on our roles, we are comparing the system in the second group, and we concluded that the system has a huge advantage that the other systems do not have. Since Blockchain technology is everything about equal roles and privileges, we decided to include the chain in the application, so the users can see the flow of the voting process. We believe that the UX changes in the application can contribute to the usage of the system. Apart from that, the ECDSA with blind signatures fulfills the security issues for the system and the main disadvantage is the performance, due to the long-lasting mathematical operations. For that purpose, we limit the usage of our system in smaller organizations and departments.

The structure of the paper starts with the introduction to the topic, followed by a section for explaining the implementation into technical details (the technologies behind it, the ECDSA algorithm itself, different types of zero-knowledge proof). The third section is focused on the comparison of this system and other systems that are build using the Blockchain technology (some of the systems are created by companies and some of them are created by individuals). The paper ends with a conclusion an acknowledgment of the authors.

2. TECHNICAL IMPLEMENTATION OF ELECTRONIC VOTING SYSTEM BASED ON BLOCKCHAIN USING ECDSA WITH BLING SIGNATURES

2.1. Technology in Use

The system is implemented as a web application which is made using Angular and Java (Spring Boot). The front-end of the system is implemented in Angular [8] which is a modern Typescript framework and uses Bootstrap library for a beautiful styling. On the other side, the back-end is implemented in Java with Spring Boot [9]. The database used in this system is a relational H2 base where the data is queries using SQL language. In these cases, the usage of Spring Boot reduces the need for SQL queries, so the basic CRUD (Create-Read-Update-Delete) operations are already implemented using the Repository of Spring Boot with no additional code. The anonymity implementation for hiding the voter's choice is calculated in the back-end. Basically, the combination of ECDSA with blind signature is not that straight forward and does not work without any additional changes. This combination only works with a modified Paillier cryptosystem. ECDSA uses SHA256 as a cryptographic hash function and this is used as the second element of the Blockchain technology. One of the reasons why Angular is chosen for the front-end is the increase scalability that provides this framework which covers to some extend the disadvantages of the electronic voting systems on a global level. Spring Boot is mainly used for microservices and in this case is also a good solution because the module for the ECDSA is implemented separately of the application [10].

2.2. Architecture of the System

The architecture of the whole application is separated into three parts: the front-end, the back-end and the module for the ECDSA (which is also part of the back-end). Each of these must be initialized separately. The front-end architecture is based on the principle of lazy loading which means that not all modules are loaded together and, on every page, but as the user navigates through the page, only the needed/necessary modules for that specific page are loaded. Another part of the architecture is one of the best practices in Angular: separation of the code into components, modules, pages, views, and services which helps into the code maintenance. Additionally, the code shows an example where the same code is used on two places (only with different content) and instead of coping the code, a shared component is used where a dynamic parameter is sent. The components on the front-end have three parts: template (an html file that shows the structure of the page), style (a sass file that has the classes for the style) and logic (a typescript file that contains the logic for the component) [11, 12].

Every service in the front-end is connected with a controller on the back-end, which also helps in the code maintenance and best practices. For example, the Typescript file that represents the service for the candidate (candidate.service.ts) has the functions that are connected with the controller for it (CandidateController.java) and so on. Each entity from the back-end is directly connected with the interface on the front-end where both have the same fields with the same types [13, 14].

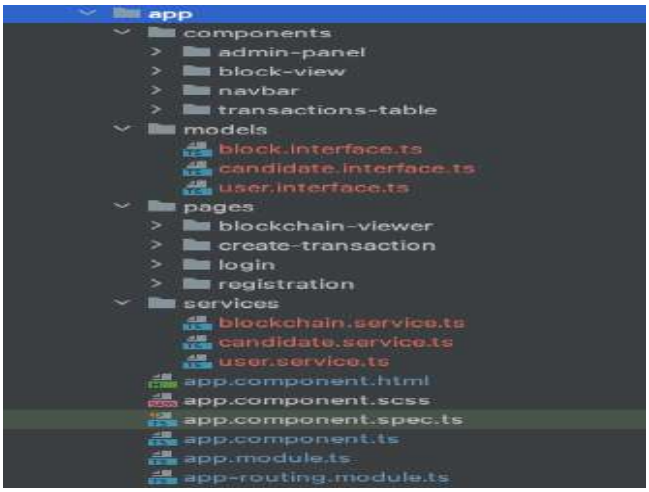

Figure 1. Architecture of the front-end

The above-described architecture is shown on Figure 1, where the core of the application is built on separate modules. On the other side, Figure 2 gives an example how the back-end architecture is structured.

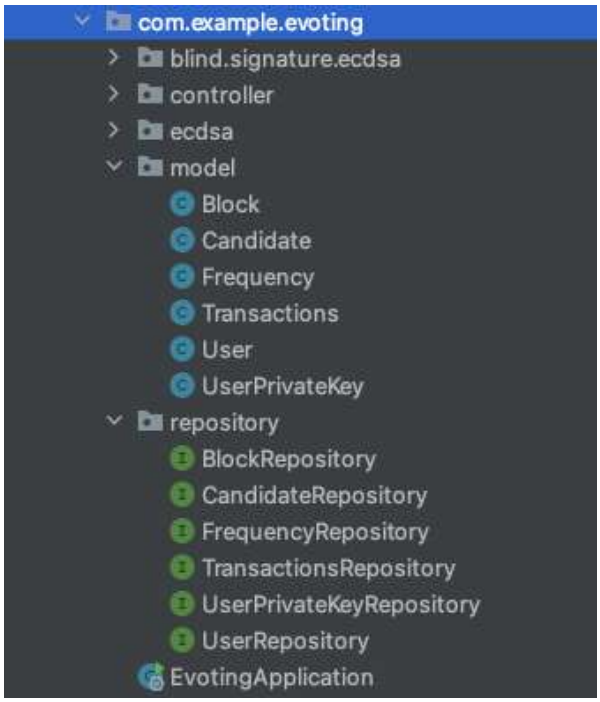

Figure 2. Architecture of the back-end

The application has two roles: user and admin and both have different view of it. The admin is already an existing entity that is created with the creation of the database and the user must be registered first via the registration form. The admin can add, delete, edit the users, and can see the frequency per candidates (only number of votes and nothing else for the voting). The user has the screen with the list of candidates, but he can only click on the vote button (no operations for the candidates). Once the user clicks on the button, he gets a confirmation modal. On this page the

user not only chooses which candidates he wants to vote for, but he can also see the chain of the blocks in the current Blockchain.

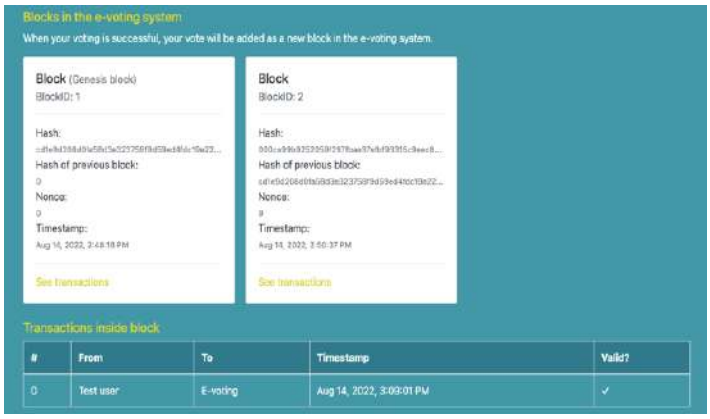

Figure 3. User panel with blocks and transactions

This is a really good view, because the users enjoy the benefits of the Blockchain technology and their contribution to the system is equal. By clicking on the blocks, the user can see the transactions of each block. Figure 3 show the chain of the blocks with the transactions (this is only part of the page, the table with the users is omitted in this figure). The other part of the voting is done on the second page where the user adds a transaction that is sent to the admin panel. First, the user must enter his private key and once it is done, the user can perform his voting. When the user comes to this step the ECDSA with blind signatures is calculated and he clicks on the 'Sign Vote and Confirm' button.

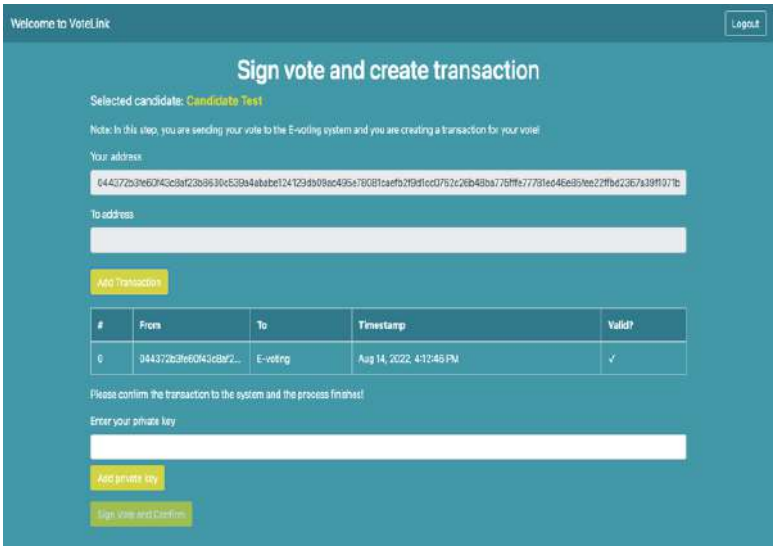

Figure 4. Form for submitting the vote

Figure 4 shows the last part of the user panel where the user enters the private key and starts the sign and verify process with ECDSA and blind signatures.

2.3. ECDSA with Blind Signatures

The definition of a digital signature may be listed as an electronic, encrypted stamp that is used for authentication of digital information where the integrity of the information is being fulfilled. The module of the ECDSA implementation consists of the following elements: Point (one point on the elliptic curve that is defined with the coordinates x and y), Curve (the curve that is defined with the equation:

$$y^2 = x^3 + A * x + B(\mathrm{mod}\, P)$$

where *A, B,* and *P* are parameters. The curve has the order and the group of the curve. The class Math contains the functions for executing mathematical operations such as: the sum of two points of the curve and others. The private and the public key are known and used elements for every cryptography. The class Signature is calculated based on the mathematical equations of ECDSA algorithm but for the purpose of this paper, those equations are omitted. Those equations give the modified Paillier cryptosystem [15] that has the sign and verification processes. All these elements together are the core of the ECDSA algorithm with blind signatures. The definition of a blind signatures comes directly from its name and shows that the message is blinded before it is signed.

Another advantage of this system is that it uses additional check if the message is created correctly. Using zero-knowledge proof the processes of signing and verifying can be checked if they have been constructed correctly. There are two ways how to do this: interactive and non-interactive zero-knowledge proof. The current implementation of the system uses the interactive version because of the birthday attack. The interactive version requires two parts to make an interaction to prove this and the non-interaction requires only one way to execute the calculations. The main problem for choosing the interactive zero-knowledge proof is the possibility of a birthday attack. The non-interactive zero-knowledge is done using another hash function and with the birthday attack a duplicate may be found. If this happens, the system loose its security and with that the electronic voting will fail. On the other hand, the performances with the non-interactive zero-knowledge proof will be better since there is no waiting time from the opposite side. In this paper, the focus is on security and that is why the interactive zero-knowledge proof is used [16].

3. COMPARISON TO OTHER SYSTEMS FOR ELECTRONIC VOTING

There are many electronic voting systems that does the same function, but they are implemented on different ways. There is no right or wrong way how to do this, but it depends on many factors. The most meaningful characteristics for comparison of the systems are anonymity, audit, integrity, accessibility, scalability and so on. The systems can be implemented by companies or independent individuals. The most famous systems that are created by companies are: Follow My Vote, Voatz, Polyas, Luxoft, Polys, Agora and others. These are systems that are mainly stable, tested and used for years in practice. The research has shown that these systems have one disadvantage and that is the scalability (and the programming language). Our new system needs to be compared with the group of systems built from individuals. One of the most famous systems in this group are: Schema OVN, Schema DATE and the Schema BES. The anonymity, audit, verification by voter, accessibility and affordability are positive for all systems and that is something very important. On the other hand, accuracy and scalability are characteristics that are not fulfilled for none of the systems [17]

The new system for electronic voting, proposed in this paper, shows a characteristic that is not common for the other systems and that is the “block-chain”. Since the Blockchain technology put the emphasis on the equal nodes and privileges, none of the systems shows this in the user interface. That is what our system shows, and the users can see visually how the whole chain is structured. Nevertheless, this has technical issues and one of them is the DOM tree which now is constructed with so many elements. This can be optimized by implementing a pagination with only *n* elements per request or implementing a search filter that will only focus on filtering the elements by certain parameter.

4. CONCLUSIONS

Blockchain technology and decentralized system shows that every node in the chain have the same privileges and role. According to its structure, the technology does not have one central unit and with this modification the changes for abuse and changing data is not the case anymore. Most of the electronic voting system suffer from the scalability, and this is even the case with the bigger companies. Building electronic voting system can have various of advantages and disadvantages, but in the end the most important parts that every system must have are obtaining the security and keeping the vote as anonymous.

In this paper, we propose a new system of electronic voting based on Blockchain, which represents a stable system with a good architecture and high code maintenance. After some modifications, the ECDSA with blind signatures can be used with zero-knowledge proof and together they build a secure chain that users can use to vote easily. The analysis of this system shows that due to limited resources and performance issues, the best practice where to use this system is on smaller target group and that is how also the technical issues may occur less. The system has an easy-to-use user interface and shows some hints for the user. The implementation with Angular and Spring Boot has detailed and structured architecture which uses the best practices. When the system is compared to other systems, it shows that our system has an advantage that is not present in the others. The advantage is that our system shows the user how the chain of the voting is constructed and that is exactly one of the benefits of the Blockchain. This comes with a disadvantage in the DOM tree of the application, but we propose a way with using pagination to solve the issue.

In the end, we can conclude that the Blockchain technology has a positive impact in the world of technology and the advantages of it can be used to build helpful systems for the whole environment.

ACKNOWLEDGEMENTS

This research was partially supported by Faculty of Computer Science and Engineering at "Ss Cyril and Methodius" University in Skopje.

REFERENCES

[1] Easttom, C, (2015) “Modern cryptography”, Applied mathematics for encryption and information security. McGraw-Hill Publishing.
[2] Yaga, D., Mell, P., Roby, N. & Scarfone, K, (2019) “Blockchain technology overview”, arXiv preprint arXiv:1906.11078.
[3] Jafar, U., Aziz, M. J. A. & Shukur, Z, (2021) “Blockchain for electronic voting system—review and open research challenges”, Sensors, Vol. 21, No. 17, pp5874.
[4] Joshi, A. P., Han, M. & Wang, Y, (2018) “A survey on security and privacy issues of Blockchain technology”, Mathematical foundations of computing, Vol. 1, No. 2, pp121.

[5] Zheng, Z., Xie, S., Dai, H., Chen, X. & Wang, H, (2017) “An overview of Blockchain technology: Architecture, consensus, and future trends“, In 2017 IEEE international congress on big data (BigData congress), pp557-564.
[6] Kohno, T., Stubblefield, A., Rubin, A. D. & Wallach, D. S, (2004) "Analysis of an electronic voting system", In IEEE Symposium on Security and Privacy, 2004, Proceedings. 2004, pp27-40.
[7] Song, J. G., Moon, S. J. & Jang, J. W, (2021) “A scalable implementation of anonymous voting over Ethereum blockchain”, Sensors, Vol. 21, No. 12, pp 3958.
[8] https://www.edureka.co/blog/advantages-and-disadvantages-of-angular/#AdvantagesDisadvantages accessed: 10.11.2022
[9] https://bambooagile.eu/insights/pros-and-cons-of-using-spring-boot/ accessed: 10.11.2022
[10] Rajesh, R. V, (2016) “Spring Microservices”, Packt Publishing Ltd.
[11] https://angular.io accessed: 10.11.2022
[12] Gutierrez, F, (2021) “Spring Boot. In Spring Cloud Data Flow“, Apress, Berkeley, CA, pp9-31.
[13] Moiseev, A. & Fain, Y, (2018) “Angular Development with TypeScript”, Simon and Schuster.
[14] https://spring.io/projects/spring-boot accessed: 10.11.2022
[15] Yi, X. & Lam, K. Y, (2019) “A new blind ECDSA scheme for bitcoin transaction anonymity", In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, pp613-620.
[16] Dumas, J. G., Lafourcade, P., Miyahara, D., Mizuki, T., Sasaki, T. & Sone, H, (2019) “Interactive physical zero-knowledge proof for Norinori”, In International Computing and Combinatorics Conference, Springer, pp166-177.
[17] Enguehard, C, (2008). “Transparency in electronic voting: the great challenge. In IPSA International Political Science Association RC 10 on Electronic Democracy”, Conference on “E-democracy-State of the art and future agenda”, pp.édition-électronique.

AUTHORS

Vesna Dimitrova, is a professor at the Faculty of Computer Science and Engineering, Ss. Cyril and Methodius University in Skopje. She obtained the Ph.D. in 2010. She participated/coordinated more than 30 projects. She was a chair of one International Conference and a member of program/scientific committee at more than 40 conferences. She has published over 70 scientific papers. Her research areas are cryptography, information security and application of ML, DL and NLP in security, cryptography and cryptanalysis.

Aleksandra Popovska-Mitrovikj, is an associate professor at the Faculty of Computer Science and Engineering, Ss. Cyril and Methodius University in Skopje. She obtained the Ph.D. in 2014. She participated in several scientific research projects, many international scientific conferences, and is a co-author of many scientific research papers published in journals and proceedings of international conferences. Her research areas are coding theory, cryptography and application of ML in security, blockchain technology.

Lina Lumburovska is a Master student at the Faculty of Computer Science and Engineering, Ss. Cyril and Methodius University of Skopje. She is currently finishing her Master thesis in the field of cryptography, coding, and security. She has been author and co-author of 8 scientific papers in national and international conferences. She works as a full-stack developer in kern.ai (a start-up that builds an open-source data-centric IDE for NLP).