Organization of a Digital Voting System Based on Blockchain Technology for the Faculty Council

Mirko Köhler, Miljenko Švarcmajer(✉), Ivica Lukić, and Tomislav Stipanić

Faculty of Electrical Engineering, Computer Science and Information Technology Osijek, 31000 Osijek, Croatia
miljenko.svarcmajer@ferit.hr

Abstract. Digital/online voting has great potential to decrease organizational costs and increase voter turnout because voters do not need to be present during meetings to cast a vote, they can vote from wherever there is an Internet connection. Despite obvious benefits, digital voting solutions are viewed with a great deal of caution because a single vulnerability can lead to distrust in the results of voting and the organization itself. Blockchain technology offers decentralized nodes with pear-to-pear verification advantages, security protection characteristics, non-repudiation and digital signatures. In the paper organization of the Faculty Council session, roles of its members, and the current ways of decision-making are described. This paper proposes using Blockchain to replace the existing voting system using e-mail. Security and data integrity of votes is absolutely provided theoretically. The organization of such a voting system is given in this paper. Voting application and resulting session report is proposed.

Keywords: Blockchain · Smart contract · Digital voting

1 Introduction

When it comes to democracy, as well as a democratic society, people immediately think of voting. Although it is already well into the 21st century, paper balloting is still considered the most reliable and certain way to make sure a person has fully exercised their right to vote [1]. In this paper, the concept of organizing a digital voting based on blockchain technology is presented, using a relatively small body such as the Faculty Council voting system. The Faculty Council is a faculty body that makes important decisions and whose work is described in detail by the faculty statute. A more detailed description of the Faculty Council role will be given in Chap. 2. Previously, all Faculty Council sessions were organized physically, at the same location. However, the COVID-19 pandemic has shown that this will not always be possible and a more modern solution was needed without physical contact. As a logical step, in a time when it was impossible to physically meet, e-mail sessions and video conferences were conducted, but there are more modern solutions using blockchain technology which will be presented in this paper.

D. Blažević et al. (Eds.): OTO 2022, LNNS 592, pp. 25–36, 2023.
https://doi.org/10.1007/978-3-031-21429-5_3

The following chapters will describe the organization of the Faculty Council session, roles of its members, and the current ways of decision-making. This is followed by an introduction to blockchain technology, smart contracts and a proposal for the concept of using this technology in decision-making by the faculty council is given. The described concept would enable a free, accessible and transparent way of voting, as well as full confidence in the results with blockchain traceability. However, although modern methods are generally considered to have advantages, they will be accompanied by possible disadvantages that will be discussed.

2 Organization of the Faculty Council Session

The Faculty of Electrical Engineering, Computer Science, and Information Technology Osijek (FERIT) has the Statute. A statute is a collection of rules and regulations used by different companies or institutions. A faculty statute regulates the internal structure, management issues and decision-making [2], and it is the most important document of an institution. According to the Statute of FERIT [3], the two most important bodies of the FERIT are the Dean and the Faculty Council.

2.1 Dean

Among a lot of other responsibilities, Dean has a crucial role in Faculty Council Sessions. The Dean chairs the sessions of the Faculty Council and has the following rights and duties:

- convenes and conducts sessions,
- proposes the session agenda and makes sure that the session takes place as determined agenda,
- maintains order at the session and gives the floor to the speakers,
- refers to the discussion and decision-making of the Faculty Council, prepares proposals, reports, opinions, analyses and other items within the competence of the Faculty Council,
- determines and publishes the voting results,
- takes care of keeping the minutes of the session,
- ensures that the work of the Faculty Council respects the provisions of the Law, the Statute and the general acts of the University and the Faculty,
- signs decisions and general acts adopted by the Faculty Council,
- performs other tasks in accordance with the Law, the Statute of the University and the Faculty, general acts of the University and the Faculty and these Rules of Procedure.

2.2 Faculty Council

According to [3] The Faculty Council consists of all full professor with tenure, full professors, associate professors, assistant professors, two representatives of lecturers elected to teaching positions, two representatives of associates elected to associate titles, one representative of other employees who have a contract of employment with the

Faculty, and student representatives who make up at least 15% of the total number of members of the Faculty Council. The work of the Faculty Council and the manner of decision making, in addition to the Statute, are determined in more detail by the Rules of Procedure of the Council [4]. By default, Dean is a member of the Faculty Council.

The Faculty Council of FERIT is organized according to the rules written in the Statute of FERIT. The main role of Faculty Council members is to attend sessions of the Faculty Council. At them, Faculty Council members participate in discussions and vote on items proposed by the Dean. Responsibilities of the Faculty Council are:

- vote on proposed items,
- makes decisions on academic, scientific, and professional issues,
- elects and dismisses deans and vice-deans,
- adopts the Statute and other general acts at the proposal of the Dean,
- initiates and conducts part of the selection procedure for scientific titles,
- initiates and conducts the procedure of election to scientific-teaching, teaching, associate and professional titles and appropriate positions,
- organizes postgraduate university studies,
- organizes postgraduate specialist study,
- determines the structure of the Faculty,
- decides on the establishment of new organizational units of the Faculty,
- appoints and dismisses heads of institutes,
- proposes to the Dean the Rulebook on the organization of jobs.

The Faculty Council decisions are made by public voting by a majority vote of the members present, except in cases where the Law, the Statute of the University, the Statute of the FERIT or another general act stipulates otherwise. In those cases, the decision must be made by a majority of the total number of members and/or by secret vote.

2.3 Session of Faculty Council

There are four types of Faculty Council Sessions. They can be regular, extraordinary, elective and ceremonial. Elective and ceremonial sessions are not in the interest of this paper. There is no voting at ceremonial sessions, and elective sessions must be held in public. Regular sessions of the Faculty Council are held as a rule once a month and extraordinary sessions of the Faculty Council are held based on the indicated need or justified reason.

As stated before, the Dean proposes the agenda of proposed items to be discussed at the session. The Faculty Council makes decisions by public vote and by a majority vote of the members present, except in cases where the Law, the Statute of the University, the Statute of the FERIT or another general act stipulates otherwise. In those cases, the decision must be made by a majority of the total number of members and/or by secret vote.

An electronic session of the Faculty Council may be convened by the Dean in urgent and justified cases. For valid decision-making at the electronic session, the Dean must submit a decision proposal by e-mail and set a deadline by which voting is not shorter than 24 h, within a working day. The present members of the electronic session are those members who voted in the electronic session and decisions must be made by a majority of all members of the Faculty Council. Voting is done using the official e-mail address assigned to the Faculty Council member by FERIT. After an individual member of the Faculty Council receives a proposed item's, by e-mail, he should vote on them in specific way. The ordinal number of the proposed item should be given first and then after that one of the decisions: “FOR”, “AGAINST” or “ABSTAINED” [4]. Electronic session of the Faculty Council does not have an oral discussion. All documents related to the individual decision proposal, as well as the invitation to the session with the agenda, are submitted as attachments in e-mail. That is why it is very important that decisions that could provoke controversy or require discussion are not put on the agenda of electronic sessions.

After the vote, the dean determines whether the individual decision received the required majority of votes and announces the result of the vote. Previously made decisions may be revoked, annulled, or changed by the Faculty Council at one of the next sessions if a new factual situation related to the decision-making is established.

Each new session begins with the adoption of the written Report from the previous session of the Faculty Council. Report of the electronic session of the Faculty Council must be accompanied by a printout of all e-mails sent by members of the Faculty Council containing their votes.

3 Blockchain Based Voting

As explained in the previous chapter, there is a need for electronic sessions and digital voting. Whether it is case of an emergency, or some other justified cases like in last years it was even forbidden to hold public gatherings due to measures introduced in the fight against the COVID-19 pandemic.

The current voting system for electronic sessions takes place via e-mail. Traceability of such voting is less than desirable, messages can end up in spam or some other mail folders, as well as replies to them. As proof of voting, it is necessary to print out all the responses sent by the Faculty Council members and archive them. Messages can be accidentally deleted or forwarded to the wrong address. Voting must be done from an official email given by the faculty in order to be valid.

This paper will present the organization of digital voting using blockchain technology. In order to better explain this proposed voting solution, it is necessary to explain used technologies. To understand why blockchain is used in the voting system at all, it is necessary to explain its basics and advantages like traceability, trust and transparency.

3.1 Distributed Ledger Technologies

Distributed Ledger Technologies (DLT) offers a way to increase trust, traceability, and collaboration within one or more institutions. Most known DLT is a blockchain [5]. Blockchain is a growing record of data in a slightly unique way than with standard databases. Various security mechanisms are also used in blockchain. Every record is stored in the block and when the block is full, it gets its timestamp and a hash of the previous block. The timestamp is proof that the date stored in the blockchain existed when the block was published. While the hash is a mathematical function that turns an arbitrary-length input into a fixed-length encrypted output. As a result, its unique hash will always be the same size, regardless of the original quantity of data or file size involved. Furthermore, because hash functions are "one-way," they cannot be utilized to "reverse-engineer" the input from the hashed result. Even yet, if you perform the same function on the same data, the hash will be the same, allowing you to verify that the data is the same [6]. The main use of blockchain, in the beginning, was cryptocurrencies, but very quickly blockchain attracted the attention of various business sectors. The blockchain is used in supply chain management, healthcare, identity management, and conventual financial services as shown in Fig. 1.

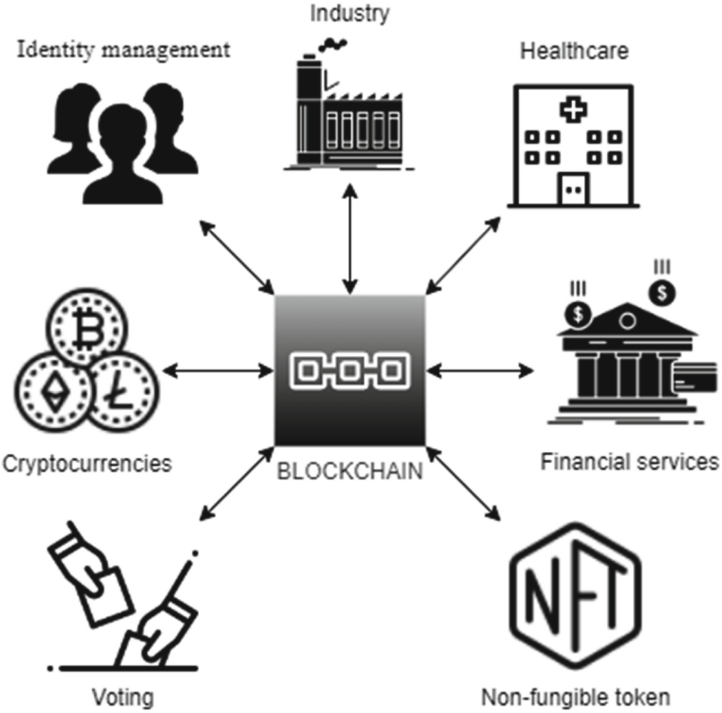

Fig. 1. Blockchain use cases.

3.2 Blockchain Voting

To put it simply, blockchain voting is a variant of electronic voting that adds digital (cryptographic) signatures to make it more difficult to forge votes, due the hashing and distributed consensus to keep votes secure are used. Computer networks use software to agree on the data's arrangement and content. As previously stated, such software is public and accessible to everybody. As the software attempts to check and link received data using hash algorithms that prohibit data modification, users upload fresh data as well as digital cryptographic signatures. As a result, previous data is preserved, unaltered, and available to all users. It is critical to highlight the following qualities in the context of voting:

(1) **The consensus protocol** is a set of rules used by nodes in a network, which leads to the conclusion that is best for the entire network. Although there is no central body for validation and verification, it is considered that every transaction in the chain is fully secured and verified. A consensus or protocol that allows any computer to connect and participate in a network is called a permissionless protocol. The blockchain which uses permissionless protocol is called public and has been used in most of the currently most popular blockchains (Bitcoin, Ethereum, Litecoin, Cardano, etc.). The advent of the permissionless protocol has forced many to reconsider distributed databases where the set of participants is predetermined and limited. These protocols improve error tolerance and may even tolerate some malicious nodes. Such a protocol is called a permission protocol, and the blockchain that uses it becomes private.

(2) **Authentication**. There is no traditional user identity in the blockchain system, the only thing that represents the user is the private key with which he performs digital signing. The user is solely responsible for managing and storing his private key. In case the private key is stolen or lost, the user loses his "identity" on the blockchain.

(3) **Smart contracts**. A smart contract is computer code that is automatically executed at defined conditional events described within the contract. In this way, it is possible to perform much more complex actions on the blockchain than just transferring values from one address to another. With smart contracts, it is possible to create applications such as markets, computer games and various decentralized financial applications.

(4) **Secrecy of transactions**. All transactions on the blockchain are public, at least in most cases. This is one of the key features, that all transactions are transparent and verifiable. In a private blockchain, it is possible to restrict access to read data, which can be useful to limit data leakage but those without access cannot participate and check the blockchain. Some systems use "zero-knowledge proof" to hide details of transactions, participants and amounts. Proof of zero-knowledge reliably shows that a statement is true without revealing why that statement is true [7].

Most research related to blockchain-based electronic voting is related to voting in public elections where anonymity is particularly important [8, 9].

Blockchain-based electronic voting usually looks like this. The electorate, which conducts the election and has a list of all voters, creates a pair of keys, public and private, that will represent that voter. In addition to the voting question and candidates, the period within which they will be able to vote is defined. Voters send their votes signed with their private key before the deadline, after which the election closes and the votes are counted.

Blockchain-based voting scenario schematics, as shown in Fig. 2, is consisting of:

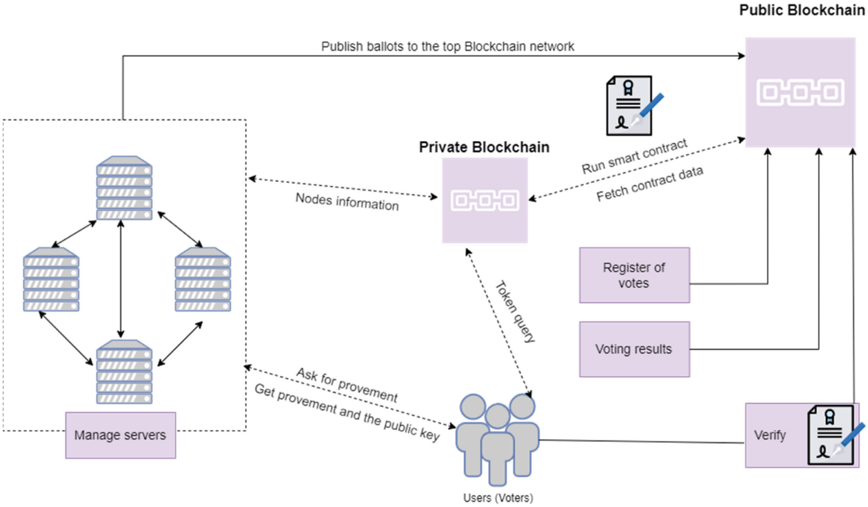

Fig. 2. Blockchain-based voting scenario.

Manage servers: Its purpose is to store node information in the lower blockchain network, broadcast it to the higher blockchain network, and issue certificates to nodes. This enables node authentication as well as the usage of user credentials to access the system.

Blockchain network: The blockchain network in the proposed scenario is made up of many blockchains that work in tandem. This structure enables parallel execution, which boosts the system's overall performance and scalability. Because each node in the private chains has a local blockchain that holds the privacy-sensitive data, the private chains are used to store node information and the voter identity register. After certain voters successfully agree on the transactions, the public blockchain (such as Ethereum) serves to record independent blockchain states across all voters and concurrently process transactions. The transactions that are recorded in the public blockchain are trusted and unchangeable.

Users (Voters): Users are both voters and members of the election committee; they can authenticate and access their wallets using their identity ID. Voters are given a digital token that enables them to cast their ballots. As a result, smart contracts are deployed in the blockchain's public section (Ethereum blockchain).

Smart contract: In the proposed decentralized system, smart contracts are self-executing pieces of code. The contract agreements that allow transactions in the public blockchain network to be tracked are defined by the functions encoded in smart contracts. Each node in the blockchain network can independently run the smart contract to obtain consensus in the proposed scenario, resulting in the establishment of a modular cryptosystem for voting systems [10].

4 The Organization of a Faculty Council Voting System

In this chapter, the organizational structure of the electronic session of the Faculty Council and the voting itself, on the proposed decisions, will be presented. The roles of the system will be presented first and then the components of the smart contracts will be explained. Also, the system architecture will be proposed, and a description of voting applications will be given. One of the most significant differences between the voting presented here and the solutions presented so far in the article lies in the fact that there is no anonymity in this voting system. Voting in political (parliamentary or presidential) elections must be by a secret vote. This is one of the principles of democratic systems. However, in this example, it is required that the vote be public and that it can be determined exactly who voted how.

4.1 Roles

There are three roles in this system. The two, most important roles, we have already explained: Dean and Faculty Council members. The third role in the system is the Secretary of the Faculty (Secretary). The role of the Secretary, within the sessions of Faculty Council, is to perform organizational, professional-administrative, legal, technical, and other general tasks. Secretary interprets the law and other regulations, performs other tasks determined by the Statute, the Law, other regulations, and general acts of the Faculty. The Secretary participates in the work of the Faculty Council, without the right to vote. Its role in this organizational solution is for the session to take place under the rules of the Statute.

4.2 Smart Contracts

There are two types of smart contracts in the organization of electronic sessions. The first smart contract is the session itself. The Dean creates a new event called the Faculty Council Session. This smart contract consists of these attributes:

- full name of the Faculty
- ordinal number of the session
- date of the session
- time of the beginning of the session
- duration of the session
- number of proposed points
- list of all faculty council members.

The list of all faculty council members is just a list of public keys of individual members. Every employee will generate their own private key, with the help of the IT department, when he is employed, and there can be lots of lists. List of all employees, list of members of each department, list of members of some special committee, etc. It is proposed that the Secretary oversee creating and updating the lists.

This smart contract must have a method for creating session report and requires the same number of second type of smart contract as there is number of proposed points to vote on. So, the second type of smart contract is a proposed item. It was also created by the Dean and consists of these attributes:

- hash of session smart contract
- ordinal number
- title
- brief description
- link to documentation
- hash of documentation
- the question of accepting the item.

This smart contract must have a method for voting and returning the voting result. The properties title and description are part of every point. Each proposed point has the attributes of title and description, regardless of whether it is an electronic or regular session. The documentation, which usually consists of one or more documents, is published on the Faculty's website, and its hash is property of a smart contract to ensure traceability. In case the documentation contains more than one document, it is suggested that all documents be compressed into a.zip document and then the hash of that document be published in smart contract.

4.3 Blockchain Platform

There are various blockchain platforms that support smart contracts. Ethereum [11], Hyperledger [12], Tezos [13], Algorand [14], Solana [15] just to name a few. They are different by execution environment, smart contract language, permission type, consensus, etc. For this application, it is proposed to use the European Blockchain Services Infrastructure (EBSI) architecture, or in more detail CroBSI, the Croatian national blockchain infrastructure, that is subdomain of EBSI. It is important to state that EBSI is based on the Proof of Authority consensus.

The organization of holding and voting in the electronic session presented here is just one of the use cases and as such goes through four steps of development according to EBSI rules. EBSI documentation [16] gives these steps for Use Case Lifecycle:

1. Identification and selection
2. Design and development
3. Testing and piloting
4. Deployment in production.

By the time of drafting this article, there are four EBSI services:

- The Self-Sovereign Identity Use Case
- The Diploma Use Case
- The European Social Security Pass Use Case
- The Document traceability Use Case.

There are also plans to deploy more services like: Document Traceability, Trust Data Sharing, SME Financing and Asylum Process Management [17]. Illustration of EBSI layers interactions based on a simple blockchain transaction flow is presented in Fig. 3.

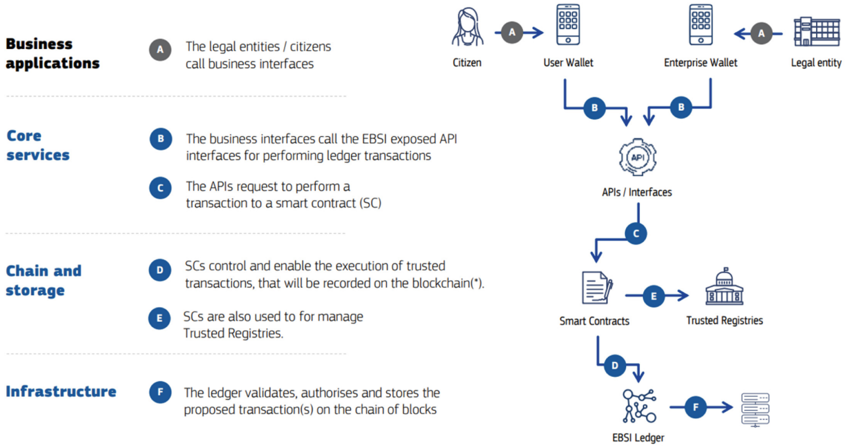
Business applications
A The legal entities / citizens call business interfaces
Citizen
A
User Wallet
Enterprise Wallet
A
Legal entity
B
B
Core services
B The business interfaces call the EBSI exposed API interfaces for performing ledger transactions
C The APIs request to perform a transaction to a smart contract (SC)
API
APIs / Interfaces
C
Chain and storage
D SCs control and enable the execution of trusted transactions, that will be recorded on the blockchain(*).
E SCs are also used to for manage Trusted Registries.
Smart Contracts
E
Trusted Registries
D
Infrastructure
F The ledger validates, authorises and stores the proposed transaction(s) on the chain of blocks
EBSI Ledger
F

Fig. 3. EBSI layers interactions [16].

4.4 Voting Application

The application architecture itself is not the subject of this article. The application, by which Faculty Council members vote in sessions, must be created as a wallet library. Wallets are used for key management, signing blockchain transactions and reference implementations. Wallets can be installed on smart phones or other electronic devices (laptops, desktops, tablets, etc.), and they allow the user to access electronic sessions and vote at individual points. To activate the wallet user needs to enter the private key that he was given by a state administration body or after employment at the Faculty.

Current sessions will be visible in the wallet, on the day of the session, from the time set as the beginning, and voting on each item will be possible until the duration of the session expires. Within each proposed item, the member will be able to read all proposed item attributes, choose one of the offered answers (“FOR”, “AGAINST” or “ABSTAINED”) to the asked question, and submit the ballot. After selecting the answer and submitting the ballot, he will no longer be able to change his answer. After member casts vote on each item, the session will automatically close, and he will be able to see it under archive activities.

4.5 Session Report

After all members have voted on all proposed points or after the end of the session, the Secretary may request that the Session report be downloaded. That report must contain all attributes of the session smart contract, and for each smart contract of the proposed items must, in addition to all the attributes, fetch the results of the vote. It is understood that hash pointers to these blockchain transactions are seen in all parts of the report.

5 Conclusion

The current organization of voting in electronic sessions of the Faculty Council of FERIT has shortcomings in the organization and implementation. Using e-mail as a medium to deliver the agenda of the session as well as all the necessary attachments is not that as big of the problem like, voting on proposed points via e-mail. Agreeing or disagreeing with the proposed item is done by writhing a string of text. That string is prone to errors and is not entirely secure way of voting.

The proposed DLT technology is tested and offers unambiguity of each session and each proposed item. Using smart contracts that will automatically save the data in blockchain and create a report is the best way to prove voting transparency. Using smart contracts offer additional options, such as automatic cancellation of the session if 50% of the council members did not vote. Also, after the session expires or after all members have voted the session could be automatically closed. It offers the possibility of verifying the authenticity of published documents that are attached to the proposed items and so on.

Although the advantages of this method of voting are clear, there are certain disadvantages. Voting by e-mail requires only a username and password to login. Because email is used for a number of other purposes, people rarely lose or forget their username and/or password. In the case of blockchain voting, a person is much more likely to lose private key. On the other hand, remembering is not even an option. Thus, losing the key equals losing the ability to vote within a given time period.

Using the same organization, smart contracts can be made for voting at other sessions held at FERIT, such as voting by members of each department, and voting by members of various committees. In these cases, it would be necessary to make new lists of members and give the Presidents, of department and committee, the power to create sessions.

References

1. Epstein, J.: Are all types of internet voting unsafe? IEEE Secur. Priv. **11** (2013)
2. D. Uršić, Izrada akata u visokom obrazovanju s posebnim osvrtom na statut. In: Proceedings of 6th International Conference "Vallis Aurea" Focus on: Research & Innovation Požega: Veleučilište u Požegi; DAAAM International Vienna (2018). https://urn.nsk.hr/urn:nbn:hr:112:478386
3. Statut Fakultetskog Vijeća Fakulteta Elektrotehnike, Računarstva I Informacijskih Tehnologija Osijek, Osijek (2021) [Online]. https://docs.google.com/viewerng/viewer?url=https://www.ferit.unios.hr/2021/./dokumenti/429/Statut+FERIT+pro%C4%8Di%C5%A1%C4%87eni+tekst-o%C5%BEujak+2022.pdf. Last Visited: 10 June 2022
4. Poslovnik O Radu Fakultetskog Vijeća Fakulteta Elektrotehnike, Računarstva I Informacijskih Tehnologija Osijek, Osijek (2019) [Online]. https://docs.google.com/viewerng/viewer?url=https://www.ferit.unios.hr/2021/./dokumenti/70/Poslovnik+o+radu+Fakultetskog+vije%C4%87a+FERIT-a.pdf. Last Visited: 10 June 2022

5. Li, J., Kassem, M.: Applications of distributed ledger technology (DLT) and Blockchain-enabled smart contracts in construction. Autom. Constr. **132**, 103955 (2021)
6. Williams, S.P.: Blockchain: the next everything. Scribner (2019)
7. Park, S., Specter, M., Narula, N., Rivest, R.L.: Going from bad to worse: from Internet voting to blockchain voting. J. Cybersecur. **7**(1), tyaa025 (2021). https://doi.org/10.1093/cybsec/tyaa025
8. Jafar, U., Aziz, M.J.A., Shukur, Z.: Blockchain for electronic voting system—review and open research challenges. Sensors **21**, 5874 (2021). https://doi.org/10.3390/s21175874
9. Bulut, R., Kantarcı, A., Keskin, S., Bahtiyar, Ş.: Blockchain-based electronic voting system for elections in Turkey. In: 2019 4th International Conference on Computer Science and Engineering (UBMK), pp. 183–188 (2019). https://doi.org/10.1109/UBMK.2019.8907102
10. Abuidris, Y.: Secure large-scale e-voting system based on blockchain contract using a hybrid consensus model combined with sharding. ETRI J. **43** (2020). https://doi.org/10.4218/etrij.2019-0362
11. Ethereum Development Documentation [Online]: https://ethereum.org/en/developers/docs/. Last Visited: 10 June 2022
12. A Blockchain Platform for the Enterprise [Online]: https://hyperledger-fabric.readthedocs.io/en/release-2.2/. Last Visited: 10 June 2022
13. Welcome to the Tezos Developer Documentation! [Online]: https://tezos.gitlab.io/. Last Visited: 10 June 2022
14. Algorand Developer Docs [Online]: https://developer.algorand.org/docs/. Last Visited: 10 June 2022
15. Developer Resources [Online]. https://solana.com/developers. Last Visited: 10 June 2022
16. CEF Digital—EBSI Architecture, explained. Final draft 10 June 2021
17. Discover EBSI's USE CASES [Online]: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Use+cases. Last Visited 10 June 2022