UDC: 342.8

SIMPLE BLOCKCHAIN-BASED E-VOTE APPLICATION

[1]Valerii Yalanetskyi, [2]Andrii Fedorko, [3]Lev Lashyn, [4]Petro Shevchuk

[1,2,3,4] National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: [1] https://orcid.org/0000-0001-6163-0258
E-mail: [1]v.yalanetskyi@gmail.com, [2]andrii.fedorko01@gmail.com, [3]lashin.lev13@gmail.com, [4]p.sheva5409@gmail.com

DOI: 10.15673/atbp.v%vi%i.2498

Abstract. *This paper describes a blockchain-enabled e-voting system that uses digital wallets to represent voter credentials, with each voter receiving a single "coin" to cast their vote. The voting process includes steps for voter registration and identification, as well as the casting of votes using encryption or hashing algorithms. The authors discuss various methods for voter identification, including the use of private and public key pairs, ID documents, and biometric data. They also mention the use of the SHA-256 hashing algorithm for added security. The goal of the project is to develop a flexible system that can be used in any institution and that guarantees maximum security against fraud. The system is built using Rust, a new experimental programming language developed by Mozilla, and makes use of "task trees" to manage the voting process. Consideration of various methods for voter identification, including the use of private and public key pairs, ID documents, and biometric data, shows a commitment to providing a flexible solution that can be adapted to meet the needs of different institutions and voting scenarios. The use of the SHA-256 hashing algorithm also adds an extra layer of security to the system, making it more difficult for malicious actors to manipulate or tamper with the voting process. The use of Rust and "task trees" to manage the voting process also indicates a focus on developing a robust and efficient system that can handle the complexities of large-scale voting. Rust's emphasis on safety and memory management can help prevent common programming errors that can lead to security vulnerabilities, while task trees can provide a structured approach to managing multiple concurrent voting processes. Overall, the blockchain-enabled e-voting system described in this paper presents an interesting approach to addressing the challenges of secure and transparent voting processes. However, as with any new technology, it will be important to thoroughly test and evaluate the system to ensure its reliability and effectiveness before it can be widely adopted*

Keywords: *blockchain, smart contract, election, e-voting.*

1. Introduction

A blockchain-based e-vote application is a digital platform that allows individuals to cast their votes electronically using blockchain technology. The use of blockchain ensures that the vote-casting process is secure, transparent, and immutable. With a blockchain-based e-vote system, voters can cast their ballots from anywhere with an internet connection, eliminating the need to physically visit polling stations. This makes it easier for voters to participate in elections and can also increase voter turnout.

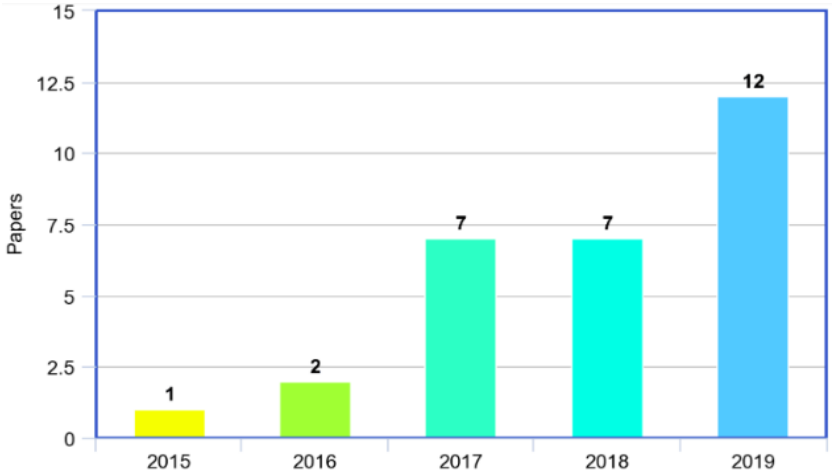

Fig. 1 – Number of relevant papers by year

Additionally, a blockchain-based e-vote system can help to reduce the potential for fraud and errors that may occur during the voting process. Overall, a blockchain-based e-vote application offers a convenient and secure way for individuals to exercise their democratic rights and have their voices heard [1]. Interest in the relevant topic grows over years (Fig. 1) [2].

One of the key features of a blockchain-based e-vote system is the use of decentralized technology. This means that the voting process is not controlled by a single entity, such as a government or election commission. Instead, the voting process is distributed across a network of computers, known as nodes. Each node maintains a copy of the blockchain, which is a digital ledger that records every vote cast in the election. This ensures that the voting process is transparent, as all votes are recorded publicly on the blockchain.

Another advantage of a blockchain-based e-vote system is the increased security it provides. The use of cryptography and decentralized technology makes it virtually impossible for hackers to manipulate the voting process or alter the results. This helps to ensure that the outcome of an election is accurate and reflects the will of the voters [3]. Overall, a blockchain-based e-vote system offers numerous benefits over traditional voting methods. It provides a convenient, secure, and transparent way for individuals to cast their ballots and have their voices heard in the democratic process.

Election Integrity in the 21st Century: The Need for Robust Fraud Prevention Measures. Paper ballot voting, in which voters cast their votes on physical paper ballots that are manually counted, has been a widely used method of voting for centuries. However, it's important for election officials to have robust processes in place to detect and prevent ballot fraud, and to ensure that the outcome of an election accurately reflects the will of the voters. This is particularly relevant in today's political climate, where there is often intense scrutiny of the electoral process and heightened concern about the integrity of elections.

Electoral fraud, which refers to the act of manipulating or tampering with the electoral process in order to change the outcome of an election, has been a concern in many countries. Some examples of electoral fraud that have occurred in these countries include allegations of voter intimidation and vote-buying, as well as reports of ballot stuffing and irregularities in the vote-counting process. It is important for election officials to have robust processes in place to detect and prevent fraud, and to ensure that the outcome of an election accurately reflects the will of the voters [4]. It is important to note that these are just a few examples, and electoral fraud has been a concern in many other countries as well. It is important for election officials to have robust processes in place to detect and prevent fraud, and to ensure that the outcome of an election accurately reflects the will of the voters.

It is important to raise awareness about the potential benefits and uses of smart contracts in order to facilitate their widespread adoption and integration into various industries. By educating the public and industry leaders about the capabilities of smart contracts, and how they can be used to increase efficiency, transparency, and trust, it will be easier for individuals and organizations to understand and see the value of implementing them in their own operations. Fortunately, the Ukrainian government has launched free courses to teach web3 [5]. War veterans which cannot fight anymore are the target audience.

Estonia first country in the world to introduce internet voting. In general, the cost of the voting process includes expenses related to voter registration, voter education, ballot printing and distribution, polling station setup and operation, vote counting and tabulation, and any other necessary expenses. It can also include costs related to the management and oversight of the electoral process, such as the salaries and expenses of election officials and the costs of conducting audits or investigations into any allegations of fraud or irregularities. Electronic voting, which refers to the use of electronic devices such as computers, tablets, or smartphones to cast and count votes, has the potential to improve the efficiency, accessibility, and transparency of the voting process. However, there are also a number of challenges and issues that need to be addressed in order to fully realize the benefits of electronic voting. Some possible areas for improvement include:

1. Security: One of the main concerns with electronic voting is the potential for hacking or other types of cyber attacks that could compromise the integrity of the voting process. To address this issue, it is important to ensure that electronic voting systems are designed with strong security measures in place, such as encryption and secure authentication protocols.
2. Reliability: Electronic voting systems need to be reliable in order to ensure that they can handle the demands of a high-volume voting environment. This includes ensuring that the systems are able to function properly without disruptions or malfunctions, as well as having adequate backup systems in place in case of any technical issues.
3. Accessibility: Electronic voting systems should be designed to be accessible to all voters, regardless of their physical abilities or technological literacy. This includes providing assistive technologies for voters with disabilities, as well as clear instructions and support for those who may not be familiar with electronic voting systems.
4. Transparency: Electronic voting systems should be transparent in order to ensure that voters have confidence in the integrity of the voting process. This includes providing a clear audit trail that allows for the verification of votes, as well as making the system's code and design open and available for review by experts.

Overall, there are many ways in which electronic voting systems can be improved in order to better serve the needs of voters and ensure the integrity of the electoral process. Smart contracts on blockchain naturally solve issues of security, reliability, and transparency, with accessibility being the hardest to address due to the lack of knowledge in a major part of the population.

One of the issues with voting machines in the USA is their vulnerability to hacking and manipulation. Smart contracts, which are self-executing contracts with the terms of the agreement between parties being directly written into lines of code, can help to mitigate these issues by providing a secure and transparent way to record and verify votes. Smart

contracts can also be programmed to automatically trigger actions, such as counting votes and to ensure that only authorized parties have access to the voting data. Additionally, smart contracts can be used to create tamper-proof and immutable voting records, which can help to increase public trust in the electoral process.

Currently, surveys in universities are done using Google Forms. A single responsible person has access to the spreadsheet. The pitfall of the data structure is that this table can be tempered. Results are not known until an admin publishes them. Ordinary voters don't see nor do they know who hides behind the administrative tasks. We would like to introduce voting on blockchain because it serves as a read-only ledger (or roughly speaking a read-only database).

2. Literature Analysis

2.1. Used implementation

There are a huge number of similiar ideas about how to choose a structure case and build appropriate service. The idea in blockchain-enabled e-voting (BEV) is simple. To use a digital-currency analogy, BEV issues each voter a "wallet" containing a user credential. Each voter gets a single "coin" representing one opportunity to vote. Casting a vote transfers the voter's coin to a candidate's wallet. A voter can spend his or her coin only once. However, voters can change their vote before a preset deadline.

The different blockchain-based e-voting applications in general have a similar structure of voting, from voter registration to the announcement of the result. So, this section will show the most popular ways to develop the voting process.

Steps of the E-voting process [6]:

1. Initialization: during this phase, the smart contracts are initialized with the voting rules, also the process of approving nominees as eligible candidates. In many papers, registration is not required because a central authority sends its keys to all voters. Another one requires confirmation.
2. Identification phase: before voting required this step to confirm your personality. There are different platforms to register voters, especially a dedicated app or website.
3. Voting: the voter chooses one or several candidates according to the voting rules. The vote is then encrypted using an encryption algorithm or hashed using a hash function Which will add to blockchain. There are many ways to set up the voting process including the possibility to absent the vote, or create two-round voting, where the second one modifies the first one.
4. Counting: when the end of the election is declared, it becomes impossible to change or add votes. The possibility of recounting needs be considered as well, since it is one of the required properties.
5. Results: through a secure channel, the results are announced in detail and declared to all.

2.2. Voter identification methods

Actually, identification methods are native-born problems to provide data safety, to be sure they won't be stolen or something else.

There are the most popular methods:

1. Authentication thanks to the validity of credentials: match between private key and public key.
2. Authentication with a scan copy of an ID document or Passport.
3. Biometric authentication: it uses the fingerprint, or Face ID check.

Also, this list does not have methods connected with personal cell phone, otherwise these peoples couldn't vote [7]:

1. The most common authentication method in blockchain-based e-voting applications is the matching of a private and public key pair. The main problem is the loss of the password. If a voter loses his password, it is very complicated to assign another one securely [6]. However, a public key cannot be directly associated with voter's identity, otherwise anonymity of electors would be not guaranteed clearly, anonymity is one of the main properties we need to satisfy (if not "the" property). A hacker could change the user's password without his knowledge, which would be very problematic [8].
2. The most popular and understandable method to us is the method via ID documents. Concerning authentication with an ID document poses security and scalability problems. Indeed, it is necessary for the system to quickly process the scanned copies of millions of users and verify that the identity documents correspond to each user. If this verification is automated, it can be very complicated to implement at large scale. In addition, the scanned copy would have to be taken instantly to ensure that it is not a fraud.
3. The fingerprint or iris photo of the eye forms a user specific hash key that is much more secure than an emailed code. This chiefly reduces the risk of fraud and ensures that a user who votes is who he claims to be. Nevertheless, the major problem remains the logistics that this requires on a large scale: each voter would have to have a device that allows the transmission of his biometric data, which seems difficult to achieve now. At the same time this method prevents us from disadvantages of previous methods.

2.3. Hashing as e-voting security

Hashing is the method of adjusting the arbitrary and variable input size to a fixed output size. There are various functions which perform different levels of hashing. But we used the most widespread method of hashing. We have implemented security by using SHA-256. SHA-256 is one of the SHA-1 (collectively referred to as SHA-2) successor hash functions and is one of the strongest hash functions available. SHA-256 is not much more difficult to code than SHA-1 and is in no way corrupted yet [6]. The 256-bit key makes AES a good partner feature which is a symmetrical key encryption cipher, meaning that the same key is used for encryption and decryption. Unlike its other predecessors, the algorithm's versatility is that it embraces any input length and produces an arbitrary output length, whilst all other

algorithms generate a set output length. The advantage of this algorithm is that it accepts any input length and produces an arbitrary output length, whereas most other algorithms produce a fixed output length and doesn`t have collisions.

3. Object, Subject, And Methods Of Research

Honesty in business relationships plays a very important role. In business, it is generally accepted that honesty has no place in business relationships: the opinion is widespread: “Why should I be honest if others profit from deceit?”. In fact, deceit in any form is unacceptable from the point of view of morality. With regard to relations with partners, the duty of the firm is to be honest in the execution of contracts. Honesty in contract enforcement is essential to the viability of the system. Without integrity, contracts simply won't be awarded or renewed. Unfair contracts entail inefficient and unproductive transaction costs, with which each party will try to protect itself from the consequences of the expected injustice. The alternative of forcing a deal entails the undermining of long-term deals, as parties who feel they have been unfairly disadvantaged take every measure available to them to resist the injustice or terminate the deal. Integrity covers a wide range of issues, from fair compensation for damages, the truthfulness of advertising to ensuring the high quality of the goods or services offered. It is for this reason that we have begun developing a product that will allow you to maintain a trusting business relationship between the state or business and the people with whom they interact.

The result of the analysis and research of competitors was our project. We have developed a flexible system that can be used in any institution as it guarantees maximum security against fraud. Our system is written in the Rust programming language using the Near blockchain.

Rust is incredibly fast and memory efficient: with no runtime or garbage collector, it can run performance-critical services, run on embedded devices, and integrate easily with other languages. Rust's rich type system and ownership model guarantees thread and memory safety, and allows you to eliminate many classes of errors at compile time. Rust is a new experimental programming language being developed by Mozilla. The language is compiled and multi-paradigm, positioned as an alternative to C / C ++, which is interesting in itself, since there are not so many contenders for competition. You can think of Walter Bright's D or Google's Go. Rust supports functional [9], parallel, procedural, and object-oriented programming, i.e. almost the entire spectrum of paradigms actually used in applied programming. A Rust program consists of a "task tree". Each task has an entry function, its own stack, means of interaction with other tasks - channels for outgoing information and ports for incoming information, and owns some part of the objects in the dynamic heap. Many Rust tasks can exist within a single operating system process. Rust tasks are "lightweight": each task consumes less memory than an OS process, and switching between them is faster than switching between OS processes.

A typical algorithm of the e-voting system is shown in the Fig 2.

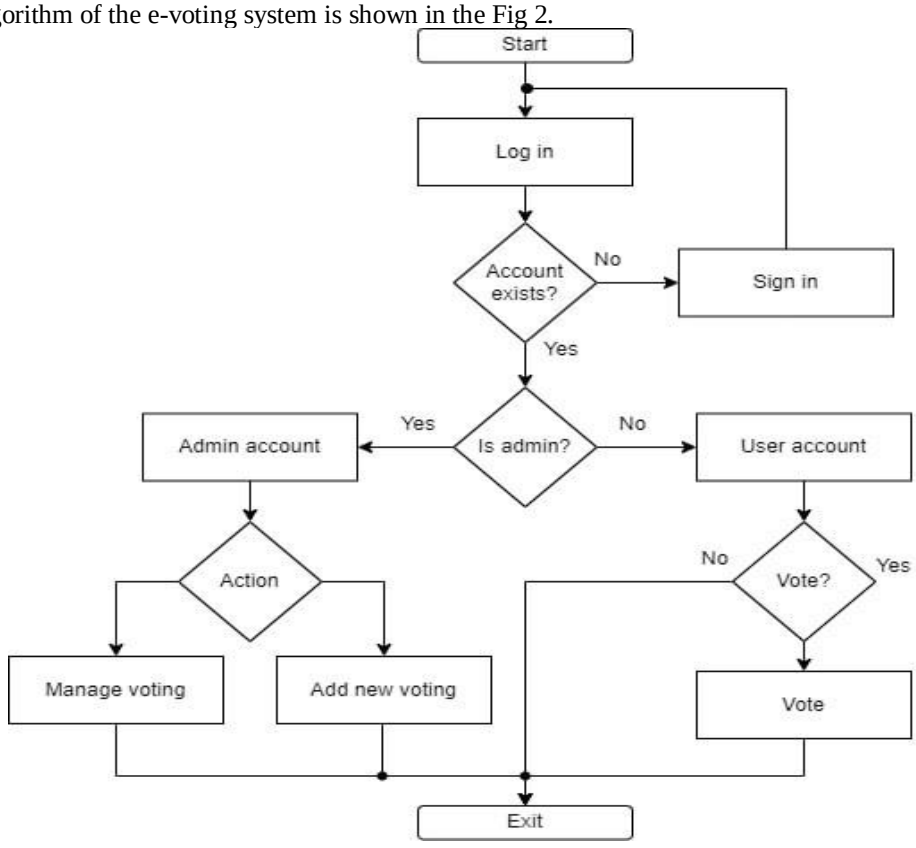

Fig. 2 – User flow diagram e-voting application

Near is a Proof-of-Stake blockchain that launched its mainnet in 2020. It is a decentralized development platform designed to provide an ideal environment for dApps (decentralized applications) by overcoming some of the limitations

of competing systems (such as low bandwidth, low speed, and poor cross-compatibility). A developer-friendly blockchain that includes a number of innovations to increase scalability and reduce costs for developers and end users. According to the creators, the application on Near can be launched in just 5 minutes. Near is open source, anyone can start contributing to its development. Near uses a delegated Proof-of-Stake (PoS) blockchain with support for smart contracts. It uses sharding for maximum efficiency and is run by holders of its own NEAR token. Near [10] also interacts with Ethereum via the Rainbow Bridge, a secure bridge that allows assets such as ERC20 and NFT tokens to be transferred between Ethereum and NEAR. Eventually, it is even possible to interact with smart contracts and dApps on both sides using the Rainbow Bridge. In terms of architecture, it uses a sharding mechanism called Nightshade. Instead of creating multiple edge parachains like the Polkadot blockchain, the Near chains are modeled as a single blockchain. Simply put, each block created on Near contains snapshots of transactions occurring on each segment of the other chain.

When logging in, the user will need to be authorized. Each person will have a unique account associated with their personal data, which will avoid the creation of a large number of fake credentials. In his profile, each voter will have tokens that he can spend on voting, everyone will be able to vote only once. It will also be possible to create an administrator account to manage voting. The administrator will be able to create, configure, start and stop voting.

4. Conclusions

There is a big risk when it comes to electoral fraud; it is a highly popular crime with rewards of up to $500 million per US campaign cycle. Unfortunately, no government has yet put in place a system that effectively prevents this kind of thing from happening. This is because election fraud is incredibly difficult to pull off - you need many criminals to work together effectively and anonymously.

Secure e-voting systems [11] make electoral decisions more reliable because they reduce the risks associated with questionable election results. In addition, they promote greater voter participation by preventing invalid votes from discouraging people from voting at all. Ultimately, implementing secure e-voting systems is a great path to global peace and prosperity!

So, as a result, we studied all analogues of competitors and came to the conclusion that our solution is innovative and will perfectly fit into the modern state system. For example, it can be implemented in the e-voting system on the Ukrainian state platform "Diya" due to which it will increase the system's resistance to hacking and will not give attackers the opportunity to influence the results. Also, in the near future, we are considering the introduction of our product into the education, healthcare, and economy systems, as well as offering it as a turnkey solution for private businesses, which will allow them to effectively optimize many processes.

Companies can use our system to collect data about their products and services to increase their success. Marketing teams can use them to conduct market research and collect data for business plans and advertising. Consumer researchers can use them to collect data on consumer attitudes and buying habits. In addition, surveyors can use the data they collect to train new surveyors or provide feedback to clients on revised designs.

5. References

[1]. S. A. Wright, “Towards a Blockchain Voting Roadmap”, 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, 2021, pp. 121-128, DOI: 10.1109/BRAINS52497.2021.9569826.

[2]. M. Dengo, F. P. Milani, “Blockchain Voting: A Systematic Literature Review”, Bachelor’s Thesis ed., 2020, Vol. 9 ECTS). Tartu. [Online]. Available: https://comserv.cs.ut.ee/home/files/dengo_informaatika_2020.pdf?study=ATILoputoo&reference=8732933CBBE5DB165A0DE9EE3F97B7FD377C5D16. [Accessed Dec. 12, 2022].

[3]. M. Musharraf. “What is the Blockchain Trilemma?”, Ledger Academy. October 22, 2022. [Online]. Available: https://www.ledger.com/academy/what-is-the-blockchain-trilemma. [Accessed Dec. 12, 2022].

[4]. S. Perera, S. Nanayakkara, M.N.N. Rodrigo, S. Senaratne, R. Weinand, “Blockchain technology: Is it hype or real in the construction industry?”, Journal of Industrial Information Integration, Volume 17(100125), 2020, ISSN 2452-414X, DOI: https://doi.org/10.1016/j.jii.2020.100125.

[5]. Kyiv Tech Summit is a WEB3 Hackathon focused on using the power of technology to solve real on-the-ground issues in Ukraine, September 6–9, 2022, [Online]. Available: https://kyiv-tech-summit.devpost.com/. [Accessed Dec. 12, 2022].

[6]. A. Shah, N. Sodhia, S. Saha, S. Banerjee, M. Chavan. “Blockchain Enabled Online-Voting System”, ITM Web Conf., 32 (2020) 03018. DOI: https://doi.org/10.1051/itmconf/20203203018.

[7]. A. Benabdallah, A. Audras, L. Coudert, “Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review”. HAL open science, 2022. [Online]. Available: https://hal.science/hal-03717773/document.

[8]. S. Bistarelli, M. Mantilacci, P. Santancini, F. Santini. “An end-to-end voting-system based on bitcoin”, SAC '17: Proceedings of the Symposium on Applied Computing, April 2017, Pages 1836–1841. DOI: https://doi.org/10.1145/3019612.3019841.

[9]. Rust Programming Language. [Online]. Available: https://www.rust-lang.org/. [Accessed Dec. 12, 2022].

[10]. NEAR Protocol. Create without limits. [Online]. Available: https://near.org/. [Accessed Dec. 12, 2022].

[11]. H. Yi. (2019, May 28). “Securing e-voting based on blockchain in P2P network”, EURASIP Journal on Wireless Communications and Networking. Vol. 137 (2019), [Online]. Available: https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-019-1473-6. [Accessed Dec. 12, 2022].