роботі були розглянуті можливості підвищення рівня протидії таким втручанням, які забезпечуються за допомогою вимог NIST до стійкості та безпековості в умовах постквантового періоду. Для визначення рівня безпековості передачі даних за не-безпечною мережею із забезпеченням приватності, цілісності та автентифікації, було проведено порівняльний аналіз можливостей протоколів передачі інформації. Результати аналізу представлені у вигляді схеми безпеки та стійкості протоколів та алгоритмів, які вийшли у фінал конкурсу NIST. Для забезпечення цілісності та справжності користувачів під час встановлення сеансів зв'язку з вебсайтами рекомендовано використовувати TLS-протоколи. Розроблено схему процесу автентифікованого шифрування та перевірки справжності зашифрованого повідомлення, що пере-дається за допомогою TLS-з'єднання. Розроблено процесну схему автентифікаційного шифрування та розшифрування інформації при встановленні сеансу зв'язку в протоколах TLS. Проведено порівняльний аналіз різних версій протоколів TLS.

Ключові слова: аутентифікація, TLS-протоколи, кіберзагрози, NIST, методи реалізації кіберзагроз.

Alla Havrylova, Senior Lecturer of the cyber security department of National Technical University "Kharkiv Polytechnic Institute".
Гаврилова Алла Андріївна, старший викладач кафедри кібербезпеки Національного технічного університету "Харківський політехнічний інститут".
E-mail: alla.havrylova@khpi.edu.ua.
Orcid ID: 0000-0002-2015-8927.

Yulia Khokhlachova, candidate of technical sciences, associate professor of the department of information technology security of the National Aviation University.
Хохлачова Юлія Євгеніївна, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: yuliiahohlachova@gmail.com.
Orcid ID: 0000-0002-1883-8704.

Andrii Tkachov, candidate of technical sciences, associate professor of the cyber security department of National Technical University "Kharkiv Polytechnic Institute".
Ткачов Андрій Михайлович, кандидат технічних наук, доцент кафедри кібербезпеки Національного технічного університету "Харківський політехнічний інститут".
E-mail: andrii.tkachov@khpi.edu.ua.
Orcid ID: 0000-0003-1428-0173.

Natalia Voropay, PhD in Engineering, associate professor of the cyber security department of National Technical University "Kharkiv Polytechnic Institute".
Воропай Наталія Ігорівна, кандидат технічних наук, доцент кафедри кібербезпеки Національного технічного університету "Харківський політехнічний інститут".
E-mail: voropay.n@gmail.com.
Orcid ID: 0000-0003-1321-7324.

Vladyslav Khvostenko, PhD in Economics, Associate Professor, patent attorney of Ukraine of the cyber security department of National Technical University "Kharkiv Polytechnic Institute".
Хвостенко Владислав Сергійович, кандидат економічних наук, патентний повірений України, доцент кафедри кібербезпеки Національного технічного університету "Харківський політехнічний інститут".
E-mail: vladyslav.khvostenko@khpi.edu.ua.
Orcid ID: 0000-0002-6436-4159.

DOI: 10.18372/2410-7840.25.17594
УДК 004.43

DESIGN AND EVALUATION OF AN IOTA-BASED MEDICAL INFORMATION SYSTEM

Oleksandr Shmatko, Yaroslav Kliuchka, Roman Korolov, Vladyslav Khvostenko, Sergii Dunaiev

The traditional medical information systems are plagued by issues such as data breaches, lack of privacy, and data integrity concerns. This paper presents the design and evaluation of an IOTA-based medical information system aimed at addressing these challenges. In recent years, blockchain technology has emerged as a powerful tool for securing and managing data in a decentralized manner. One area where this technology has the potential to revolutionize the way we do things is in e-medicine. E-medicine, or electronic medicine, refers to the use of technology to deliver healthcare services remotely. This includes telemedicine, online consultations, and remote monitoring of patients' health status. IOTA blockchain technology, in particular, has a lot of potential in e-medicine. IOTA is a distributed ledger technology that uses a directed acyclic graph (DAG) instead of a traditional blockchain. The main ad-vantage of this approach is that it eliminates the need for miners and makes the system more scalable, fast, and energy-efficient. IOTA is also designed

to be feeless, making it an ideal choice for microtransactions. In e-medicine, IOTA can be used in several ways. One potential use case is for secure and decentralized storage of patients' medical records. Medical records are highly sensitive and contain confidential information that needs to be protected from unauthorized access. By using IOTA's tamper-proof and immutable ledger, patients can have more control over their medical records and choose who has access to them. This can be especially useful in situations where patients need to share their medical records with multiple healthcare providers or research institutions. By leveraging the unique features of IOTA, such as its feeless microtransactions, scalability, and distributed ledger technology, the proposed system enhances security, privacy, and interoperability in healthcare information management. The evaluation of the system involves performance tests, and a comparison with existing solutions.

***Keywords**: directed acyclic graph, electronic healthcare system, healthcare data exchange, medical patient data, IOTA.*

INTRODUCTION

Medical information systems play a crucial role in the healthcare industry, as they facilitate the efficient management and sharing of patient data among healthcare providers. However, traditional systems have been plagued by issues such as data breaches, lack of privacy, and data integrity concerns. Moreover, these systems often struggle with interoperability and scalability, which hinder their overall performance and effectiveness.

Because blockchain technology is based on the concept of distributed ledgers, it enables medical records to be easily exchanged between hospitals, doctors, and researchers for a variety of reasons, including maintaining a patient's data [1]. As a result, the healthcare industry is one of the most important industries that stands to benefit from blockchain technology. MedRec is an implementation that is built on Ethereum that keeps and maintains an auditable history and records of medical transaction for providers, regulators, and patients [2]. MedRec was developed by the Ethereum Foundation. As a result of its foundation in Ethereum, miners that verify transactions are eligible for a variety of rewards. They also take into consideration a second incentive strategy that incorporates the participation of medical professionals in the mining process. Now, things get a little more complicated as a result of mining because it boosts both the cost of the gas required to run the function of smart contracts and the possibility of security breaches. [3] Nguyen D. C, and other authors [4] examine the deployment of data sharing through mobile applications that use blockchain. Nevertheless, this implementation does not consider the sharing of data, such as how corporations share information with one another. The exploitation of health data for the sake of research is prevented by the design of this system. In addition, the Hyperledger blockchain and off-chain storage are both utilized by the Medichain system, which was designed specifically for the purpose of archiving data associated with medical care [5, 6].

In addition, the framework that has been developed places an emphasis on providing users with privacy and confidentiality. Yet, it considers Hyperledger Composer but does not consider the results of the implementation. Blockchain technology is being discussed by Patel V. A, and the rest of the team as a potential system and framework for securing and protecting healthcare systems [7]. There is a presentation and discussion of a permission-based blockchain that is presented with authority verification for the purpose of exchanging healthcare data [8]. In [9], with the assistance of a Hyperledger composer, an emergency access control management system (EACMS) is presented. In [10], Tith, D. and his team presented a framework based on Hyperledger that was installed on a local network of four Linux-based computers and served as a user interface for patients and clinicians. In [11], a framework for the administration of electronic health records consent that makes use of the Hyperledger Fabric running on the IBM blockchain platform is described. The analysis included the specifics of the deployments of three different providers (one patient and two providers). CrowdMed overcame the problem of insufficient information-sharing motivation by offering reward tokens to patients who contributed more data for the purposes of research [12], so incentivizing them to share more data with the organization. There has been no discussion regarding the findings of the evaluation of the suggested framework.

METHODS AND MATERIALS

The paper aims to address these challenges by proposing a novel solution that leverages blockchain technology. Blockchain, a decentralized and distributed ledger technology, has shown promising poten-

tial in various industries due to its inherent security, immutability, and transparency features.

In this study, we focus on designing and implementing a permissioned blockchain-based medical information system that allows controlled access to authorized participants. We are integrating IOTA technology to automate and secure various processes, such as patient consent, access control, and data sharing. The evaluation of the system involves performance tests, security analysis, and a comparison with existing solutions.

The primary objectives of the research are:

- to enhance the security and privacy of medical information systems through blockchain technology;
- to ensure data integrity by maintaining an immutable record of data transactions;
- to facilitate efficient and secure data sharing among healthcare providers using smart contracts;
- to improve transparency and auditability within the system;
- to identify and address the challenges of scalability and interoperability in blockchain-based medical information systems.

This paper contributes to the growing body of research on the application of blockchain technology in the healthcare industry. By addressing the key challenges faced by traditional medical information systems, the proposed solution has the potential to revolutionize patient care and transform the way healthcare providers manage and share sensitive medical data.

RESULTS

The architecture of the suggested solution is broken down in great detail in this part of the report. It is structured in such a way that personal information can be stored off-chain in a cloud database, and that the blockchain will only be used to record information relating to consent. The architecture of the new system under consideration is dissected in great detail.

Because personal data cannot be saved on the blockchain, this option was not taken into consideration. Figure 1 presents an illustration of the system's overall architecture [13, 14, 15]. Consumers are able to use blockchain technology to record the specifics of their consent (via blockchain transactions), and they can also use it as an access log, as was shown earlier. Users are able to retain the safety and integrity of their data in the cloud. The users' permission to use their data can be solicited from the organizations that collect it. The administrator is allowed to disclose the user's data if the user has provided necessary approval to the organization. In conclusion, users of a blockchain transaction have the ability to withdraw an organization's access to the ledger at any time.

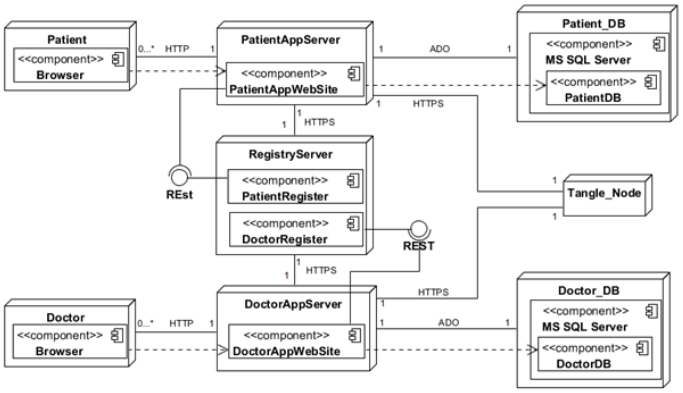

Fig. 1. System's overall architecture

The proposed model of a medical information system (Fig. 1) includes: 2 types of system users (patient and Doctor), 3 web servers on which the corresponding software solutions are deployed, and 2 databases.

To log in, the patient goes through the authorization stage, where they specify the necessary data (last name, first name, patient ID). Thanks to PatientAppWebSite, the patient can search for doctors, view their medical data, and consult with medical professionals. The PatientDB database will store all the necessary medical information of the patient. When logging in to their system at the authorization stage, doctors indicate the doctor's ID issued by the Ministry of health after checking for professional aptitude. However, medical professionals can also log in as a patient. DoctorAppWebSite allows a doctor to advise patients seeking help. The DoctorDB database stores data about all patients who have applied for help, and the data of the doctor himself. PatientRegister and DoctorRegister are suitable solutions that store and provide patients and Doctors With login details.

In the proposed system, node types relative to roles can be classified into:

a. Patient node. This node allows you to perform the following actions:

- fill out the patient's medical card;
- create / view seed and public / private keys;
- view the patient's medical data: tests, medical prescriptions, diagnoses, symptoms;
- view the patient's personal data;
- search for a doctor for further consultation;
- view the data of each doctor (specialty, length of Service, medical skills, etc.);
- send a list of symptoms that are bothering the patient for further consultation;
- view the result of the consultation.

b. Doctor's node. This node allows you to perform the following actions:

- set up a doctor's profile;
- create / view seed and public / private keys;
- view the list of patients who were treated;
- view the patient's medical data: medical prescriptions, diagnoses, etc.;
- view the medical data of patients who have applied for help;
- make a diagnosis and send it to the patient;
- write out a medical prescription and send it to the patient.

c. This is a node that stores all the relevant information that a doctor/patient needs to log in to their system.

Every doctor who wants to use this system must pass professional aptitude. This is necessary so that an incompetent doctor cannot use the system and put human life in trouble. After the check, the doctor receives a special number (DoctorID) that will allow you to log in to the system. All Doctor data and this number are stored on this node. In addition, the data of any patient and their special number (PatientID) are also stored on this node. Therefore, this node allows you to perform the following actions:

- stores the doctor's personal data and DoctorID for authorization in the system;
- stores the patient's personal data and PatientID for authorization in the system.

IOTA is a permissionless, scalable, and feeless distributed ledger technology that utilizes a directed acyclic graph (DAG) called the Tangle. This architecture allows IOTA to achieve high throughput and secure data transactions without the need for mining or transaction fees. In this study, we explore the design and evaluation of an IOTA-based medical information system that leverages the benefits of the Tangle to overcome the challenges faced by traditional systems.

We designed and implemented an IOTA-based medical information system that allows for the secure and efficient management of patient data. The system architecture includes the following components:

– IOTA Tangle: The core infrastructure that underpins the system, enabling secure and feeless data transactions.

– Data Storage and Access Control: Patient data is encrypted and stored on distributed nodes, ensuring data privacy and security. Access to the data is granted to authorized healthcare providers using cryptographic techniques.

The user enters their medical data (body temperature, heart rate, symptoms, laboratory tests, etc.). To send data to the doctor, the patient creates a transaction (transaction). Transactions are broadcast in an envelope called bundle. Next, you will need to sign (signature) transactions with a private key to confirm ownership. Then a bundle hash should be generated. Now you need to calculate the Proof-of-Work for each transaction in the bundle. The POW result is a nonce value that is added to the transaction. The last step is to send the bundle to the network.

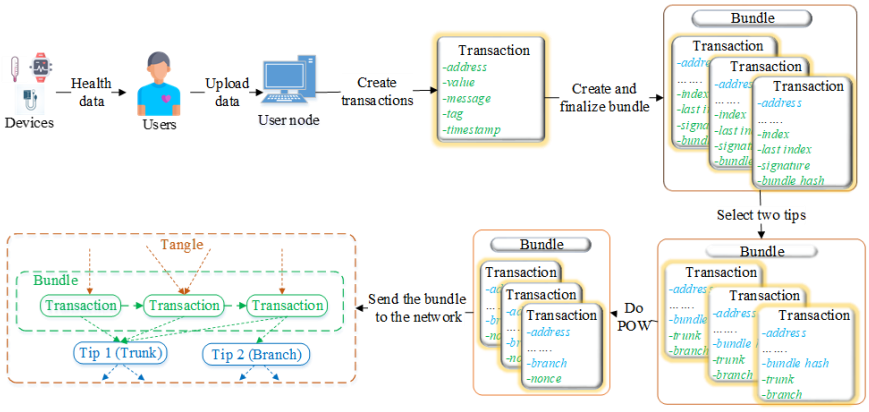

Fig. 2. Transfer of medical records using IOTA Tangle

Experimental Evaluation

When sending a transaction to the IOTA Tangle network, there are 3 main steps that take a lot of time to complete. These main stages are:

- time to search for tips;
- POW execution time;
- total time to create and send the bundle.

For testing, we will take 10 different diseases and their symptoms, which the patient can send to the provider of medical services. We will send the symptoms of these diseases to the doctor's node. We will draw this text 20 times. Figure 3 shows the average execution time for each stage described above and the number of transactions generated during bundle formation.

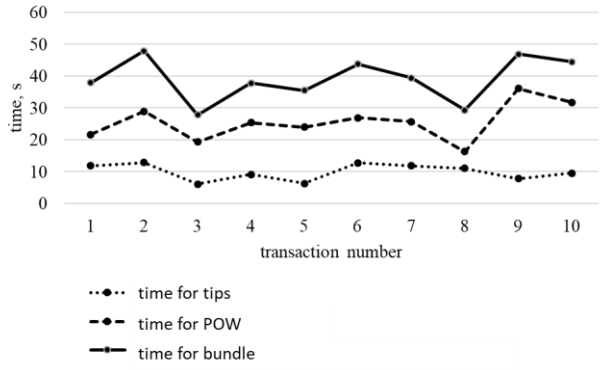

Fig. 3. Average execution time

The graph shows that it takes less than a minute to create and send a bundle to the network. The least time is spent searching for two transactions to confirm. The POW execution time depends on the number of transactions in the bundle, since each transaction calculates its own POW. The more transactions, the more time is spent at this stage. If we draw analogies with the blockchain network, then the transaction time interval depends on the network load. The average transaction time is between ten minutes and an hour, but when the network is overloaded, the transaction time increases.

Performance metrics

Average response time

This is the most important indicator to understand how a website works from the user's point of view. Simply put, the average response time is the time spent passing a specific packet of information sent from the user's browser to the server, and the time spent returning the packet back to the user's computer. The application must be checked under various circumstances (for example, the number of concurrent users, the number of requested transactions). As a rule, this indicator is measured from the beginning of the request to the moment when the last byte is sent.

Other factors, such as the geographical location of the user and the complexity of the requested information, may affect the average response time for users and should be considered when evaluating the overall performance of the application. The researchers call the most acceptable response value 0.5 s. considering geography, this value can be about 1-3 seconds. If the response value is consistently higher than the specified value, then you need to think about changing hosts or optimizing the site [44]. Figure 4 shows the average response time value.

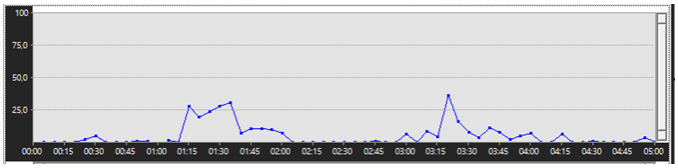

Fig. 4. The average response time value

The figure 4 shows the average Avg value. Response time does not exceed 3 seconds. From this we can conclude that Avg. Response time does not exceed the specified norm. Although the maximum value is 36.8 seconds. To reduce this value, we have changed the methods that are responsible for sending transactions, calculating POW, and searching for confirmation transactions. The Average Response time after the changes decreased by 2.3 times to 15.9 seconds.

One of the most important parameters of any server is its bandwidth, since it is this characteristic that largely determines the speed and loading speed of the entire resource, which in turn affects the number of the users. Bandwidth is the number of records that the server can complete in one second. Band-width is measured in requests per second (RPS).

Figure 5 shows the bandwidth under a load of 25 users. Throughput can be affected by several factors. These include the number of users, the complexity and frequency of user operations, and managing and configuring pages and web parts. Each of these factors can have a significant impact on throughput.

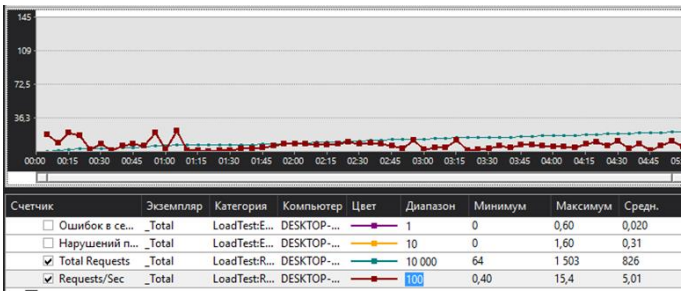

Fig. 5. Bandwidth with a load of 25 users

Figure 5 shows that on average, the server processes 5 requests per second at a constant load of 25 users.

Figure 6 shows the bandwidth under a load of 50 users.

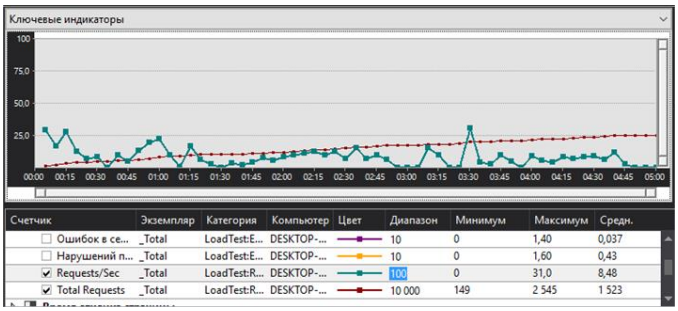

Fig. 6. Bandwidth with a load of 50 users

The IOTA-based medical information system demonstrated significant improvements over traditional systems in several key areas:

1. Security and Privacy: The use of the Tangle, combined with cryptographic techniques, resulted in enhanced security and privacy for patient data.

2. Scalability: IOTA's Tangle architecture allowed for high throughput and scalability, addressing one of the main challenges faced by traditional medical information systems.

3. Interoperability: The system was designed with standardized data formats and communication protocols to ensure seamless interaction with existing healthcare systems.

4. Feeless Transactions: The absence of transaction fees in IOTA enabled the system to carry out microtransactions at no additional cost, which is crucial for large-scale medical data management.

CONCLUSION

The design and evaluation of an IOTA-based medical information system show promising potential for addressing the challenges faced by traditional healthcare systems. By leveraging the unique features of IOTA's Tangle, the proposed system enhances security, privacy, scalability, and interoperability in medical information management. Future research should focus on refining the system architecture, conducting real-world pilot studies, and further exploring the potential benefits of IOTA and other distributed ledger technologies in the healthcare industry.

REFERENCES

[1] McGhin T. et al. Blockchain in healthcare applications: Research challenges and opportunities //Journal of Network and Computer Applications. 2019. T. 135. pp. 62-75.

[2] Ben Fekih R., Lahami M. Application of blockchain technology in healthcare: A comprehensive study //The Impact of Digital Technologies on Public Health in Developed and Developing Countries: 18th International Conference, ICOST 2020, Hammamet, Tunisia, June 24–26, 2020, Proceedings 18. Springer International Publishing, 2020. pp. 268-276.

[3] Sagar V., Kaushik P. Ethereum 2.0 blockchain in healthcare and healthcare-based internet-of-things devices //Proceedings of the International Conference on Paradigms of Computing, Communication and Data Sciences: PCCDS 2020. Springer Singapore, 2021. pp. 225-233.

[4] Nguyen D. C. et al. Blockchain for secure ehrs sharing of mobile cloud-based e-health systems //IEEE access, 2019. T. 7. pp. 66792-66806.

[5] Agarwal A. K. et al. A systematic analysis of applications of blockchain in healthcare //2021 6th International Conference on Signal Processing, Computing and Control (ISPCC). IEEE, 2021. pp. 413-417.

[6] Jagtap S.T. et al. A framework for secure healthcare system using blockchain and smart contracts //2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC). IEEE, 2021. pp. 922-926.

[7] Patel V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus //Health informatics journal, 2019. T. 25. №. 4. pp. 1398-1411.

[8] Al Asad N. et al. Permission-based blockchain with proof of authority for secured healthcare data sharing //2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT). IEEE, 2020. pp. 35-40.

[9] Rajput A. R. et al. EACMS: Emergency access control management system for personal health

record based on blockchain //IEEE Access, 2019. Т. 7. pp. 84304-84317.
[10] Islam M. et al. Distributed Ledger Technology based Integrated Healthcare Solution for Bangladesh //arXiv preprint arXiv:2205. 15416. 2022.
[11] Agbo C. C., Mahmoud Q. H. Design and implementation of a blockchain-based e-health consent management framework //2020 ieee international conference on systems, man, and cybernetics (smc). IEEE, 2020. pp. 812-817.
[12] Shah M. et al. CrowdMed: A blockchain-based approach to consent management for health data sharing //Smart Health: International Conference, ICSH 2019, Shenzhen, China, July 1–2, 2019, Proceedings 7. Springer International Publishing, 2019. pp. 345-356.
[13] Golubnychy D. et al. Архітектура системи обміну медичними даними пацієнтів з лікарями на основі IOTA //Системи управління, навігації та зв'язку. Збірник наукових праць. 2022. Т. 1. №. 67. С. 57-61.
[14] Shmatko O., Kliuchka Y. A novel architecture of a secure medical data storage management system based on tangle //Scientific Collection «InterConf+». 2022. №. 27 (133). С. 361-374.
[15] Kliuchka Y. O., Shmatko O. V. Порівняння технології блокчейн і спрямованого ациклічного графа при зберіганні і обробці даних в розподіленому реєстрі //Вісник Національного технічного університету «ХПІ». Серія: Системний аналіз, управління та інформаційні технології. 2020. №. 1 (3). С. 106-116.

РОЗРОБКА ТА ОЦІНКА МЕДИЧНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА ОСНОВІ IOTA

Традиційні медичні інформаційні системи страждають від таких проблем, як порушення даних, відсутність конфіденційності та проблеми цілісності даних. У цьому документі представлено розробку та оцінку медичної інформаційної системи на базі IOTA, спрямованої на вирішення цих проблем. В останні роки технологія блокчейн перетворилася в потужний інструмент для захисту даних і управління ними децентралізованим чином. Однією з областей, де ця технологія може зробити революцію в тому, як ми працюємо, є електронна медицина. Електронна медицина, або електронна медицина, відноситься до використання технологій для дистанційного надання медичних послуг. Це включає телемедицину, онлайн-консультації та дистанційний моніторинг стану здоров'я пацієнтів. Технологія блокчейну IOTA, зокрема, має великий потенціал в електронній медицині. IOTA-це технологія розподіленого реєстру, яка використовує спрямований ациклічний графік (DAG) замість традиційного блокчейну. Головна перевага такого підходу полягає в тому, що він усуває необхідність в Майнер і робить систему більш масштабованої, швидкої і енергоефективної. IOTA також спроектована так, щоб бути безшумною, що робить її ідеальним вибором для мікротранзакцій. В електронній медицині IOTA можна використовувати кількома способами. Одним із потенційних випадків використання є безпечне та децентралізоване зберігання медичних записів пацієнтів. Медичні записи є високочутливими і містять конфіденційну інформацію, яка повинна бути захищена від несанкціонованого доступу. Використовуючи захищену від несанкціонованого доступу та незмінну книгу IOTA, пацієнти можуть краще контролювати свої медичні записи та вибирати, хто має до них доступ. Це може бути особливо корисним у ситуаціях, коли пацієнтам потрібно поділитися своїми медичними записами з кількома медичними працівниками або науково-дослідними інститутами. Використовуючи унікальні можливості IOTA, такі як її безкоштовні мікротранзакції, масштабованість і технологію розподілених реєстрів, пропонована система підвищує безпеку, конфіденційність і інтероперабельність при управлінні медичною інформацією. Оцінка системи включає тести продуктивності та порівняння з існуючими рішеннями.

Ключові слова: спрямований ациклічний граф, електронна система охорони здоров'я, обмін медичними даними, дані медичного пацієнта, IOTA.

Oleksandr Shmatko, PhD, Associate Professor, Department of Software Engineering and Management Information Technologies**,** National Technical University «Kharkiv Polytechnic Institute».
Шматко Олександр Віталійович, кандидат технічних наук, доцент**,** кафедра програмної інженерії та інформаційних технологій управління, Національний технічний університет «Харківський політехнічний інститут».
E-mail: asu.spios@gmail.com.
Orcid ID: 0000-0002-2426-900X.

Yaroslav Kliuchka, postgraduate student, Department of Software Engineering and Management Information Technologies, National Technical University «Kharkiv Polytechnic Institute».
Ключка Ярослав Олександрович, аспірант, кафедра програмної інженерії та інформаційних технологій управління, Національний технічний університет «Харківський політехнічний інститут».
E-mail: y.kliuchka.kpi@gmail.com.
Orcid ID: 0000-0001-9702-6837.

Roman Korolov, PhD, Associate Professor, Department of Cybersecurity, National Technical University «Kharkiv Polytechnic Institute».
Корольов Роман Володимирович, кандидат технічних наук, доцент, кафедра кібербезпеки, Національний технічний університет «Харківський політехнічний інститут».
E-mail: korolevrv01@ukr.net.
Orcid ID: 0000-0002-7948-5914.

Vladyslav Khvostenko, PhD in Economics, Associate Professor, Department of Cybersecurity, National Technical University «Kharkiv Polytechnic Institute».
Хвостенко Владислав Сергійович, кандидат економічних наук, доцент, кафедра кібербезпеки, Національний технічний університет "Харківський політехнічний інститут".
E-mail: vladyslav.khvostenko@gmail.com.
Orcid ID: 0000-0002-6436-4159.

Sergii Dunaiev, Master's, Department of Cybersecurity, National Technical University «Kharkiv Polytechnic Institute».
Дунаєв Сергій Владиславович, магістр, кафедра кібербезпеки , Національний технічний університет "Харківський політехнічний інститут".
E-mail: serg.dynaev@gmail.com.
Orcid ID: 0000-0001-8736-3602.

DOI: 10.18372/2410-7840.25.17595
УДК 004.43

AN APPROACH TO THE IMPLEMENTATION OF A COMPETENCY-BASED APPROACH IN THE LEARNING MANAGEMENT SYSTEM

Andrii Kopp, Mykyta Parashchych, Herman Zviertsev, Yevhen Motalyhin, Anna Strelnikova

This paper solves the urgent problem of improving the tracking of the process of acquiring competencies by students through the means of analyzing the learning management system data and visualizing the results of the learning process. The object of the study is to track the process of acquiring competencies by students. The subject of the study includes software components for the implementation of a competency-based approach in the learning management system. The purpose of the study is to improve the tracking of the process of acquiring competencies by students by analyzing the data of the Learning Management System (LMS) and visualizing the results of the learning process. Thus, to achieve this goal, we analyzed the technologies for processing learning data from LMS, analyzed the features of modeling the learning process based on Petri nets and BPMN (Business Process Model and Notation), determined a data structure, and proposed an algorithm for building a model and visualizing the learning process data. The developed software components allow processing of learning process data from LMS, building models and visualizations of learning process data, saving the results to data warehouses, depicting the learning process model, and visualizing learning process data for further analytical processing.

Keywords: *competency-based learning, educational process mining, learning management system, process modeling, data visualization.*

INTRODUCTION

E-learning has become an increasingly popular approach to learning thanks to the rapid growth of web technologies. COVID-19 has forced countries to introduce online or hybrid learning to catch up with expected learning targets. However, many countries remain ineffective in the transition to online or hybrid education. In addition, while some countries are succeeding in improving student achievement (e.g., Italy increased student progress with online tutoring by 4.7% compared to traditional instruction), some others are not achieving the same results with online learning. Recently, however, education industry leaders have begun to identify use cases for using process intelligence to improve online learning platforms, teaching methodology, and student learning habits [1].

The Internet and related web technologies offer excellent solutions for presenting, publishing, and sharing learning content and information. This is special software called a Learning Management System (LMS). Learning management systems such as Moodle are a popular tool in higher education. They allow teachers to present their courses virtually. In these virtual courses, they can provide learning objects such as lecture slides or videos, quizzes, or forums where students can interact with each other.