УДК 681.3 **doi: 10.26906/SUNZ.2022.1.057**

Д. Ю. Голубничий[1], О. В. Коломійцев[2], В. Ф. Третяк[3], Я. О. Ключка[2], А. О. Рибальченко[2]

[1] Харківський національний економічний університет імені Семена Кузнеця, Харків, Україна
[2] Національний технічний університет "Харківський політехнічний університет", Харків, Україна
[3] Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна

АРХІТЕКТУРА СИСТЕМИ ОБМІНУ МЕДИЧНИМИ ДАНИМИ ПАЦІЄНТІВ З ЛІКАРЯМИ НА ОСНОВІ IOTA

Анотація. Обмін медичною інформацією дозволяє здійснювати електронне переміщення медичних даних між різними інформаційними системами охорони здоров'я. На відміну від традиційних паперових документів, електронні дозволяють постачальникам медичних послуг отримувати доступ до важливої медичної інформації та обмінюватися нею. Проте, існуючі системи охорони здоров'я для обміну медичними даними громадянин, зіткнулися з низкою проблем, зокрема: конфіденційність, безпека та відсутність контролю з боку пацієнтів. Враховуючи все вищесказане, запропоновано використовувати технологію розподіленого реєстру, оскільки вона може кардинально змінити спосіб зберігання медичної інформації, забезпечуючи безпечні способи обміну даними. У статті розглядається технологія розподіленого реєстру для Інтернету речей (Internet Of Things, IoT), яка називається IOTA. Блокчейн вже використовується в багатьох системах охорони здоров'я, оскільки він вирішує серйозні проблеми охорони здоров'я, що пов'язані з конфіденційністю та безпекою. Однак, залишаються питання, що пов'язані з масштабованістю та продуктивністю блокчейну. IOTA вирішує ці проблеми, оскільки використовує структуру даних DAG (directed acyclic graph), яка дозволяє додавати транзакції паралельно. Це скорочує час, що потрібний на підтвердження транзакцій, а кількість одночасно оброблюваних транзакцій може бути необмеженою. Протокол Masked Authenticated Messaging (MAM) дозволяє безпечно передавати зашифровані потоки даних як транзакції. Тому, система, що пропонується, використовує IOTA для безпечного обміну медичними даними. Процес створення та надсилання медичних даних в IOTA проілюстровано на конкретному прикладі. Розглянуто застосування протоколу MAM на прикладі передачі медичних даних пацієнта лікарю.

Ключові слова: спрямований ациклічний граф, обмін медичними даними, технологія розподіленого реєстру, Masked authenticated messaging.

Вступ

Щороку у сферу охорони здоров'я впроваджуються нові технології для вирішення однієї з найбільших проблем галузі – обмін даними. Обмін медичними даними між інформаційними системами різних медичних закладів покращить якість медичної допомоги громадянам. Однак, медичні установи використовують власні інформаційні системи, які здебільшого не можуть спілкуватися з іншими системами. Відсутність функціональної сумісності знижує якість медичної допомоги громадянам, оскільки медичні працівники не мають доступу до необхідної інформації пацієнта. Функціональна сумісність – це здатність медичних інформаційних систем безпечно обмінюватися електронними медичними даними для покращення здоров'я як окремого пацієнта, так і всього населення в цілому (громадян). Таким чином, для надання якісної медичної допомоги пацієнтам дуже важливо налагодити функціональну сумісність [1 - 2].

Ще однією проблемою охорони здоров'я є фрагментація даних. Дані пацієнтів, зазвичай, зберігаються в різних медичних закладах. Ці численні сховища даних перешкоджають повноцінному обміну та повторному використанню даних, а також обмежують якість медичної допомоги пацієнтам [3]. Крім цього, не так давно, усі медичні дані були схоронені на папері. І хоча електронні медичні картки вже замінили паперові, заповнення цих карток відбувається повільно. Крім того, інформація, що міститься у цих медичних картках, часто буває неповною або зовсім відсутня. Отже, незважаючи на те, що життєво важливі медичні дані стали доступнішими, є ще багато роботи для створення цілісної екосистеми даних [2].

Використання технології розподіленого реєстру, зокрема IOTA, для безпечного обміну медичними даними викликало неабиякий інтерес. IOTA – це інноваційний тип технології розподіленого реєстру, який дозволяє безпечно обмінюватись даними та цінностями між користувачами мережі. Тому, важливо проаналізувати використання IOTA у сфері охорони здоров'я громадян для забезпечення безпечного обміну медичними даними пацієнтів. Оскільки IOTA можна використовувати для передачі даних пацієнтів між закладами охорони здоров'я. А протокол MAM дозволить передавати потоки зашифрованих медичних даних, які можуть містити як окремі дані пацієнта, так і всю медичну карту [3].

Літературний огляд. У цьому розділі наведено детальний огляд літератури, у якому описується застосування технології блокчейн та IOTA у сфері охорони здоров'я.

У роботі [4] пропонується нова спільна система охорони здоров'я для забезпечення ефективного та широкомасштабного обміну медичними даними пацієнтів (громадян). Метою якої є об'єднання різних медичних закладів в єдину національну систему охорони здоров'я громадян, що забезпечує швидкий, безпечний обмін та зберігання медичних даних пацієнтів. Запропонована система MEdgeChain використовує граничні обчислення та технологію блокчейн для забезпечення безпечної передачі великих обсягів медичних даних пацієнтів, які генеруються різними медичними установами.

Автори роботи [5] також розробили систему EdgeMediChain для безпечного обміну медичними даними пацієнтів. Запропонована архітектура використовує як граничні обчислення, так і блокчейн, щоб полегшити та забезпечити необхідні вимоги до екосистеми охорони здоров'я громадян з точки зору масштабованості, безпеки та конфіденційності даних.

У роботі [6] представлено нову, безпечну і ефективну схему, що заснована на технології блокчейн та шифруванні на основі атрибутів. Запропонована схема MedSBA призначена для запису та зберігання медичних даних пацієнтів. Вона захищає конфіденційність та дозволяє точно контролювати доступ до медичних даних пацієнтів.

У роботі [7] для боротьби з епідемічними захворюваннями пацієнтів використовуються технології IOTA та QR-коду. CoviReader – це децентралізована система управління охороною здоров'я громадян, яка анонімно передає дані пацієнтів. Система побудована на платформі IOTA та надає пацієнтам (користувачам) детальний, незмінний та легкий доступ до їх особистої інформації. Користувачі взаємодіють з IOTA через мобільний додаток.

Також, технологія IOTA, зокрема протокол MAM, використовується в роботі [8] для безпечного обміну даними в системі охорони здоров'я громадян.

Система безпечного обміну даними про рівень глюкози в крові пацієнта була запропонована в роботі [9]. Враховуючи відсутність ідеальної схеми обміну даними між пацієнтом та медичним працівником на основі DLT, автори запропонували два варіанти системи. Один варіант заснований виключно на IOTA, а інший використовує IOTA в поєднанні з приватним кластером IPFS (InterPlanetary File System).

У роботі [10] також пропонується система обміну медичними даними на основі IOTA. Дані генеруються пристроями IoT та передаються за допомогою IOTA. MAM використовується для полегшення обміну даними між різними сторонами.

MedShare [11] – це децентралізована платформа для безпечного обміну електронними медичними записами. Вона використовує розумні контракти для створення надійного середовища, де медичні установи можуть обмінюватися своїми зашифрованими медичними записами.

Обмін медичними даними відіграє вирішальну роль у сучасній сфері охорони здоров'я громадян. Тому, забезпечення безпеки, конфіденційності та цілісності медичних даних пацієнтів є першочерговим пріоритетним завданням.

Таким чином, використання технології розподіленого реєстру, зокрема IOTA, забезпечить надійний обмін даними між медичним працівником та пацієнтом.

Мета та завдання дослідження. Метою дослідження є розробка системи обміну медичними даними між пацієнтами та лікарями, закладами, установами і організаціями системи охорони здоров'я громадян з використанням IOTA.

Для досягнення цієї мети вирішуються наступні завдання:

– здійснення огляду IOTA, а також протоколу передачі даних MAM;

– визначення загальної схеми передачі медичних даних пацієнтів за допомогою IOTA;

– визначення застосовності протоколу MAM для безпечного обміну медичних даних пацієнтів.

Виклад основного матеріалу

Відомо, що IOTA – це технологія розподіленого реєстру, яка забезпечує безпечний обмін даними між різними пристроями IoT. IOTA використовує DAG замість традиційного блокчейну, який отримав назву Tangle (рис. 1). Завдяки цьому, IOTA вирішує типові задачі блокчейну – комісія за транзакції та масштабованість. Тобто, IOTA не використовує концепцію блоків та майнерів для підтвердження транзакцій. Натомість вузли, що створюють нові транзакції, повинні схвалити дві попередні транзакції [12]. Тому, є можливість здійснювати операції без комісій, що відкриває ще одну важливу особливість Tangle – мікротранзакції. Крім того, мережа IOTA спроектована як легка та енергоефективна. Це дозволяє використовувати IOTA на різноманітних пристроях та комп'ютерах (персональних) з різними висvмогами до енергоспоживання.

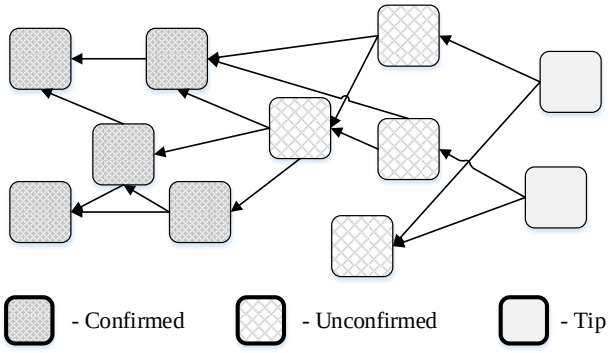

Рис. 1. Tangle

Масштабованість – головна проблема технології блокчейн. У Bitcoin блок видобувається приблизно кожні 10 хвилин з максимальним розміром блоку 1 МБ, що обмежує швидкість транзакцій Bitcoin від 3 до 7 транзакцій в секунду. За умови, якщо транзакції будуть надходить дуже швидко, то блоки додаватимуться повільно. Оскільки усі блоки послідовно з'єднуються один з одним, утворюючи безперервний послідовний ланцюжок блоків. IOTA дозволяє додавати транзакції паралельно, що забезпечує більш швидке підтвердження транзакцій, на відміну від блокчейну [13].

Ще однією ключовою особливістю IOTA є протокол MAM.

MAM – це протокол передачі даних, який дозволяє користувачеві публікувати потоки зашифрованих даних у вигляді транзакцій. Використання MAM є кращим рішенням, ніж просто надсилати транзакції з даними на одну адресу. Для цього, користувач створює канал та транслює на нього повідомлення.

Інші користувачі мережі можуть підписатися на канал, щоб отримувати повідомлення, використовуючи адресу транзакції. Кожна транзакція має вказівник на наступну транзакцію, відому як *next root*, який є коренем дерева Меркла наступної транзакції. Тому, якщо користувач отримав доступ до каналу, він не може переглядати минулі транзакції через пряме зв'язування транзакцій [12 - 14].

Існує три режими конфіденційності (рис. 2): загальнодоступний, обмежений та приватний.

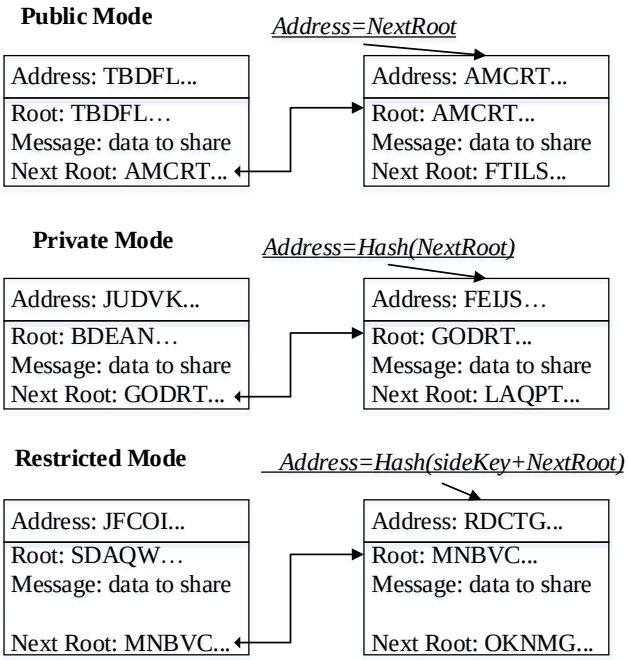

Рис. 2. Режими MAM

У загальнодоступному режимі *root* (корінь дерева Мерекла) використовується як адреса транзакції MAM, так і ключ каналу. Таким чином, весь вміст ланцюга повідомлень може прочитати будь-хто у мережі. У приватному режимі, у якості адреси використовується хеш кореня (*address = hash(root)*), а повідомлення розшифровується за допомогою *root*, що не дозволяє випадковим користувачам розшифрувати повідомлення, оскільки вони не можуть отримати *root* з хешу. Дана обставина робить потік MAM доступним для читання лише тим, кому надано *root*. У обмеженому режимі, у якості адреси використовується хеш кореня та *sideKey* (*address=hash(sideKey + root)*). *sideKey* – це ключ авторизації, який використовується для шифрування та дешифрування, що дозволяє розробнику (власнику) каналу у будь-який час скасувати доступ до свого каналу для майбутніх повідомлень [15-16].

Обмін медичними даними за допомогою Tangle

Сьогодні отримати медичні дані пацієнта дуже важко. Оскільки дані фрагментовані і розподілені між різними медичними установами та знаходяться у розрізнених сховищах. Кожен медичний заклад використовує власну медичну інформаційну систему для обробки та зберігання даних громадян. І здебільшого ці системи не сумісні одна з одною. Це створює ряд труднощів, що пов'язані з отриманням медичної інформації пацієнтів.

Для вирішення даного наукового завдання пропонується створити систему передачі медичних даних пацієнтів із використанням IOTA.

На рис. 3 представлена система передачі медичних даних пацієнтів за допомогою IOTA.

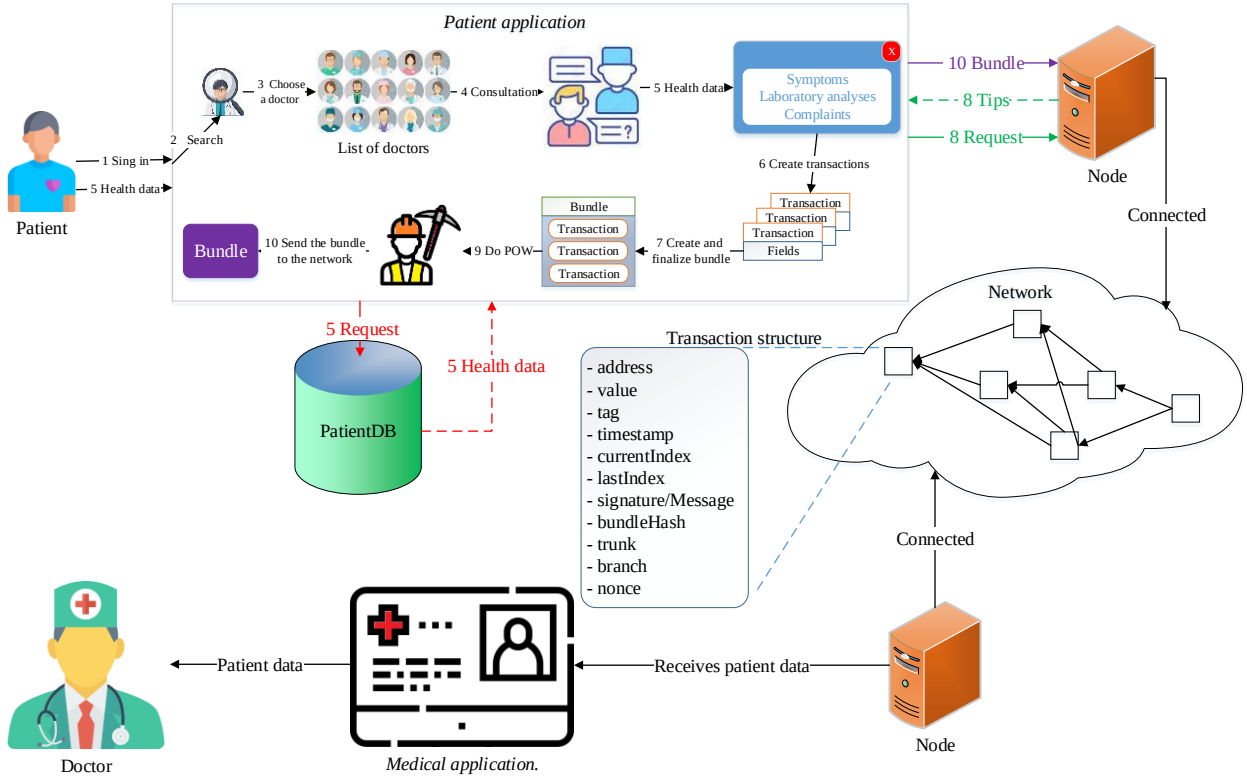

Рис. 3. Архітектура системи обміну медичними даними пацієнтів на основі IOTA

Перш за все, пацієнт вводить відповідні дані для авторизації. Потім, пацієнт здійснює пошук лікаря за відповідною спеціальністю. З отриманого списку пацієнт обирає лікаря за необхідними критеріями. Обравши лікаря, пацієнт записується на консультацію.

У відповідне вікно пацієнт заносить симптоми захворювання, скарги на стан здоров'я (які його турбують). Пацієнт також може отримати необхідні дані з бази даних. На основі цих даних створюються транзакції, які поміщаються в *bundle*. Наступним кроком є підтвердження двох непідтверджених транзакцій. Відповідний запит надсилається на вузол, а у відповідь отримуємо хеші необхідних транзакцій. Далі обчислюється POW відповідно до MWM (minimum weight magnitude). І, нарешті, *bundle* транслюється у мережу.

Пацієнт та лікар можуть обмінюватися повідомленнями за допомогою протоколу MAM.

На рис. 4 схематично представлено процес обміну медичними даними пацієнта із лікарем за допомогою MAM.

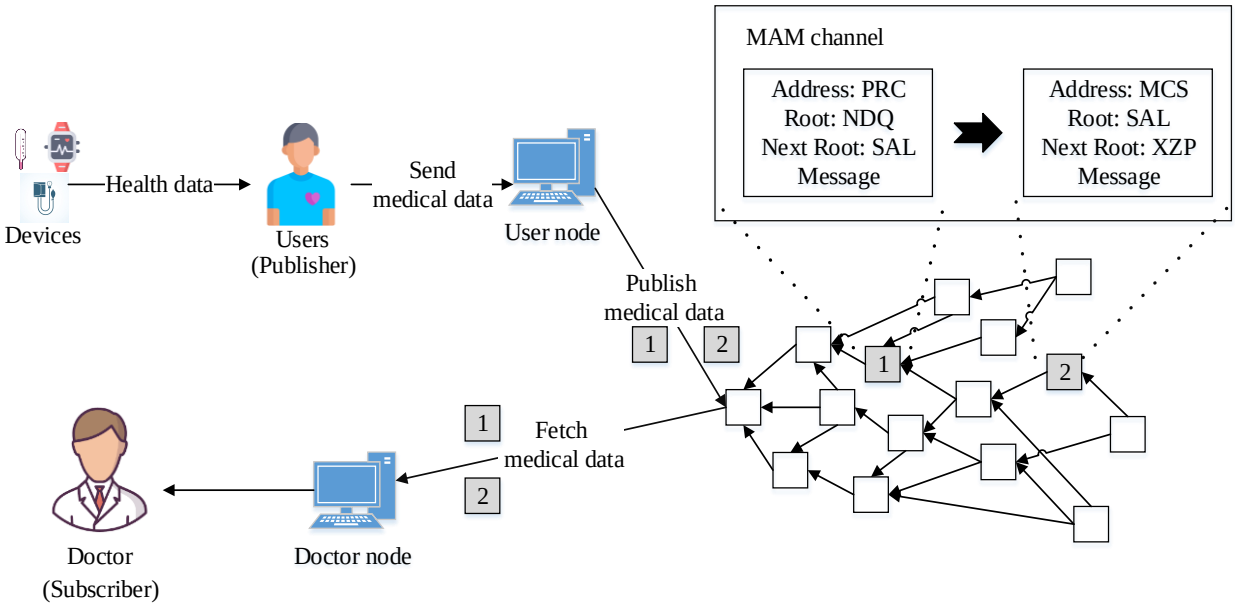

Рис. 4. Процес обміну медичними даними пацієнта із лікарем за допомогою MAM

Пацієнт вводить список скарг на здоров'я, з якими хоче звернутися до лікаря.

Щоб опублікувати ці дані в Tangle, створюється канал MAM.

Оскільки система використовує обмежений режим, генерується ключ авторизації (*sideKey*). Пацієнт формує *bundle* з відповідними транзакціями та відправляє його у мережу.

Постачальники медичних послуг підписуються на канал для перегляду опублікованих даних. Дані потім будуть розшифровані за допомогою ключа авторизації.

Завдяки MAM пацієнт та лікар можуть безпечно обмінюватися даними через Tangle, підписавшись на канал один до одного.

Результати дослідження. Медичні дані пацієнта страждають від фрагментації, закритих інформаційних систем та сховищ даних. А це, на жаль, створює певні труднощі, які пов'язані із доступом та обміном необхідною інформацією. Пацієнт може відвідувати багатьох лікарів, які можуть мати власні ізольовані медичні записи. Отримати доступ до цих даних неможливо. Крім того, обмін цими даними між постачальниками медичних послуг не завжди безпечний.

У статті запропоновано використання IOTA, яка дозволить здійснювати безпечний обмін медичними даними між пацієнтом та лікарем з гарантіями їх цілісності, враховуючи величезну кількість інформації, якою обмінюються медичні організації. Використання IOTA може прискорити обмін медичними даними пацієнтів.

Завдяки застосування структури Tangle забезпечується висока масштабованість. До того ж, IOTA дозволяє проводити транзакції з нульовими комісіями і без фіксованого обмеження на кількість транзакцій, які можна підтвердити у секунду. Крім того, MAM дозволяє передавати потоки зашифрованих даних між користувачами, а обмежений режим дозволить пацієнту контролювати доступ до своїх медичних даних. Пацієнт може будь-коли змінити *sideKey*, що анулює доступ до даних. Запропонована система дозволить лікарям та пацієнтам обмінюватися медичною інформацією безпечним, прозорим та децентралізованим способом.

Висновки

Таким чином, проведено огляд технології IOTA, яка завдяки своїй структурі дозволить медичним працівникам (лікарям) та пацієнтам обмінюватися медичними даними надійним і швидким способом, порівняно з існуючими методами та схемами. Протокол MAM надає додаткові функції, такі як керований контроль доступу до медичних даних пацієнта та їх шифрування, які покращують безпеку та конфіденційність.

Представлено загальну схему передачі медичних даних пацієнта до лікаря за допомогою IOTA.

Детально розглянуто процес пошуку лікаря за необхідною спеціальністю, а також описано процес створення і відправлення транзакцій у Tangle. Переваги використання Tangle проілюстровані на конкретному прикладі.

Розглянуто протокол MAM, який дозволяє пацієнту та лікарю публікувати потоки зашифрованих даних у вигляді транзакцій.

Здатність MAM забезпечувати цілісність медичних даних пацієнта та контролювати доступ до даних є ключовим фактором у використанні даного протоколу у системах охорони здоров'я громадян.

СПИСОК ЛІТЕРАТУРИ

1. HIMSS. Interoperability in Healthcare. Available at: https://www.himss.org/resources/interoperability-healthcare.
2. IBM. What is interoperability in healthcare? Available at: https://www.ibm.com/in-en/topics/interoperability-in-healthcare.
3. IOTA Beginners Guide. eHealth. Available at: https://iota-beginners-guide.com/use-cases/ehealth/.
4. Abdellatif, A. A., Samara, L., Mohamed, A., Erbad, A., Chiasserini, C. F., Guizani, M., O'Connor, M. D., Laughton, J. (2021). MEdge-chain: leveraging edge computing and blockchain for efficient medical data exchange. IEEE Internet of Things Journal, pp 15762-15775. doi: 10.1109/JIOT.2021.3052910.
5. Akkaoui, R., Hei, X., Cheng, W. (2020). EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange. IEEE Access, 8, pp 113467-113486. doi: 10.1109/ACCESS.2020.3003575.
6. Pournaghi, S. M., Bayat, M., Farjami, Y. (2020). MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption. Journal of Ambient Intelligence and Humanized Computing, 11(5). doi: 10.1007/s12652-020-01710-y.
7. Cisneros, B., Ye, J., Park, C. H., Kim, Y. (2021). CoviReader: Using IOTA and QR Code Technology to Control Epidemic Diseases across the US. 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC). doi: 10.1109/CCWC51732.2021.9376093.
8. Abdullah, S., Arshad, J., Khan, M. M., Alazab, M., Salah, K. (2022). PRISED tangle: a privacy-aware framework for smart healthcare data sharing using IOTA tangle. Complex & Intelligent Systems. doi: 10.1007/s40747-021-00610-8.
9. Hawig, D., Zhou, C., Fuhrhop, S., Fialho A. S., Ramachandran, N. (2019). Designing a distributed ledger technology system for interoperable and general data protection regulation–compliant health data exchange: a use case in blood glucose data. Journal of Medical Internet Research, 21 (6), pp. e13665. doi: 10.2196/13665.
10. Zheng, X., Sun, S., Mukkamala, R. R., Vatrapu, R., Ordieres-Meré, J. (2019). Accelerating Health Data Sharing: A Solution Based on the Internet of Things and Distributed Ledger Technologies. Journal of Medical Internet Research, 21(6), p 13583. doi: 10.2196/13583.
11. Wang, M., Guo, Y., Zhang, C., Wang, C., Huang, H., Jia, X. (2021). MedShare: A Privacy-Preserving Medical Data Sharing System by Using Blockchain. IEEE Transactions on Services Computing. doi: 10.1109/TSC.2021.3114719.
12. Brogan, J., Baskaran, I., Ramachandrana, N. (2018). Authenticating health activity data using distributed ledger technologies, Comput Struct Biotechnol J., 16, pp 257-266. doi: 10.1016/j.csbj.2018.06.004.
13. Ключка Я. О., Шматко О. В. 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. doi: 10.20998/2079-0023.2020.01.18.
14. Gangwani, P., Perez-Pons, A., Bhardwaj, T., Upadhyay, H., Joshi, S., Lagos, L. (2021). Securing Environmental IoT Data Using Masked Authentication Messaging Protocol in a DAG-Based Blockchain: IOTA Tangle, Future Internet, 13 (12). doi: 10.3390/fi13120312.
15. ABmushi. (2018). IOTA: MAM Eloquently Explained. Available at: https://medium.com/coinmonks/iota-mam-eloquently-explained-d7505863b413.
16. 1OTA Foundation Blog. Introducing Masked Authenticated Messaging. Available at: https://blog.iota.org/introducing-masked-authenticated-messaging-e55c1822d50e/.

Received (Надійшла) 14.12.2021
Accepted for publication (Прийнята до друку) 26.01.2022

Architecture of the system of exchange of medical data of patients with doctors on the basis of IOTA

D. Golubnychy, O. Kolomiytsev, V. Tretyak, Ya. Kliuchka, A. Rybalchenko

Abstract. The exchange of medical information allows the electronic movement of medical data between different health information systems. Unlike traditional paper documents, electronic ones allow healthcare providers to access and share important medical information. However, existing health systems for the exchange of medical data have faced a number of issues, including confidentiality, security, and lack of patient control. Given all the above, it is proposed to use distributed registry technology, as it can dramatically change the way medical information is stored, providing secure ways to share data. The article discusses the technology of a distributed registry for the Internet of Things (IoT), called IOTA. Blockchain is already used in many healthcare systems as it addresses serious health and privacy issues. However, questions remain about the scalability and performance of the blockchain. IOTA solves these problems by using the DAG (directed acyclic graph) data structure, which allows you to add transactions in parallel. This reduces the time required to confirm transactions, and the number of transactions processed simultaneously can be unlimited. Masked Authenticated Messaging (MAM) allows you to securely transmit encrypted data streams as transactions. Therefore, the proposed system uses IOTA for the secure exchange of medical data. The process of creating and sending medical data to IOTA is illustrated by a specific example. The application of the IAM protocol on the example of transferring medical data from a patient to a doctor is considered.

Keywords: directed acyclic graph, medical data exchange, distributed registry technology, Masked authenticated messaging.