УДК 004.4

В.А.Коцюбняк
В.С.Магуран
О.В.Романюк

АНАЛІЗ СУЧАСНОГО ВИКОРИСТАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ ТА НАПРЯМКИ ЇХНЬОГО РОЗВИТКУ У МАЙБУТНЬОМУ

Вінницький національний технічний університет

***Анотація*:**
Розглянуто сучасне використання блокчейн-технологій для забезпечення безпеки даних задля покращення фінансової грамотності у суспільстві, проведено аналіз їхніх переваг та недоліків і визначено розвиток цієї системи в майбутньому.
Ключові слова: *блокчейн, кібербезпека, Microsoft, безпека даних, KSI.*

***Abstract*:**
The article considers the modern use of blockchain technologies to ensure data security and improve financial literacy in society, analyzes their advantages and disadvantages, and determines the development of this system in the future.
Keywords: *blockchain, cybersecurity, Microsoft, data security, KSI*.

Вступ

Зі зростанням попиту на використання цифрових технологій, питання конфіденційності, цілісності та доступності даних стає надто важливим завданням.

Почавши як підґрунтя криптовалют, зокрема Bitcoin, блокчейн-технологія проявила свій потенціал для вирішення проблем безпеки даних [1]. Вона дозволяє створювати розподілені бази даних, що не підлягають змінам та не залежать від централізованих управлінських органів, можуть бути підтверджені й автентифіковані великою кількістю учасників мережі.

Використання блокчейн-технологій забезпечує незмінність даних, захист від фальсифікації та незаконного доступу. Крім того, розподілені блокчейн-мережі дозволяють уникнути централізованої вразливої точки, що забезпечує вищий рівень безпеки. Тому аналіз сучасних способів використання блокчейн-технологій для захисту даних є досить актуальною задачею.

Аналіз сучасного використання блокчейн-технологій

Упродовж останніх років відбулося значне число досліджень у сфері використання блокчейн-технологій для забезпечення безпеки даних. Один із прикладів цього дослідження був опублікований у відомому журналі "IEEE Transactions on Dependable and Secure Computing"[2]. В проаналізованій публікації наголошується, що блокчейн може бути застосований для створення безпечних децентралізованих систем управління доступом до даних.

Для підтвердження впровадження блокчейн-систем в реальних компаніях, було проведено аналіз двох популярних прикладів: Microsoft і Guardtime.

Компанія Microsoft користується блокчейном для покращення кібербезпеки через свої рішення та платформи, що надають засоби для створення безпечних та надійних додатків та сервісів. Ця компанія використовує декілька видів блокчейнів [3], а саме:

1.Azure Blockchain Workbench: Microsoft надає платформу Azure Blockchain Workbench, яка дозволяє розробникам створювати додатки на основі блокчейну з вбудованою кібербезпекою. Ця платформа допомагає створити розподілену систему, яка забезпечує недоторканість даних, автентифікацію учасників та моніторинг транзакцій.

2. Azure Blockchain Service: Microsoft також надає Azure Blockchain Service, який дозволяє створювати приватні блокчейн мережі з використанням різних протоколів. Цей сервіс дозволяє організаціям забезпечити захист від кібератак шляхом створення децентралізованої і недоторканої інфраструктури з контролем доступу до даних.

3. Microsoft Authenticator: Microsoft Authenticator є мобільним застосунком для багатофакторної аутентифікації. Він базується на блокчейн технології для забезпечення безпеки та надійності процесу аутентифікації. Застосунок генерує одноразові паролі, які підписуються за допомогою приватного ключа, що зберігається на пристрої користувача, тим самим зменшуючи ризик кібератак та фішингу.

4. Confidential Consortium Framework (CCF): Microsoft розробила Confidential Consortium Framework, що базується на технології блокчейн, для створення конфіденційних і безпечних застосунків. Цей фреймворк дозволяє розробникам створювати децентралізовані системи з обмеженим доступом, де дані зашифровуються та захищаються від несанкціонованого доступу.

Guardtime – це компанія, яка використовує блокчейни для забезпечення безпеки даних. Основна їх розробка – Keyless Signature Infrastructure (KSI) [4]. Основні компоненти цього блокчейну є такими:

1. KSI-реєстр: це розподілений реєстр блокчейн, який забезпечує безпечне зберігання журналу транзакцій. Інформація про кожну транзакцію, включаючи час, документи та цифрові підписи, записується в блокчейн.

2. KSI-сервер: це центральна інфраструктура, яка керує процесом створення та перевірки підписів. KSI-сервер генерує унікальний ідентифікатор для кожної транзакції та підписує його за допомогою приватного ключа. Цей підпис потім записується в KSI-реєстр.

3. KSI-клієнт: це програмне забезпечення, яке використовується користувачами для перевірки цілісності даних. Клієнт може перевірити підпис та ідентифікатор транзакції, використовуючи публічний ключ, що знаходиться в KSI-реєстрі.

Напрямки покращення блокчейн-технологій у сфері безпеки даних

На основі проведеного аналізу було виявлено, що однією з основних проблем, яка існує в Україні, є недостатня популярність блокчейн-технологій. Цей факт може бути пояснений декількома чинниками [5-6].

По-перше, через недосвідченість, адже це є відносно новим поняттям. У багатьох осіб, урядовців і бізнес спільнот може бути недостатньо розуміння потенціалу та потужності цієї технології. Така ситуація може призводити до недовіри та меншого використання. Рішенням цієї проблеми може слугувати тільки вихід більшості українських компаній на європейський рівень, де в них буде можливість самостійно побачити її в роботі.

По-друге, відсутність придатної інфраструктури. Блокчейн системи потребують так надійний інтернет-зв'язок, так і високу обчислювальну потужність, і надійні системи зберігання даних. Можливо потрібно просто підняти зацікавленість іноземних інвесторів у вкладення грошей в нові стартапи, що пов'язані з розвитком інфраструктури блокчейну.

Висновки

У результаті дослідження, було проаналізовано кілька сучасних компаній, що активно використовують блокчейн-технології. Крім того, були визначені шляхи для подальшого удосконалення та вирішення основних проблем. Зокрема, такими шляхами можуть бути популяризація блокчейну в Україні, приділення більшої уваги співпраці з європейськими компаніями та привернення іноземних інвесторів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1.What is Blockchain Security? [Електорний ресурс] — Режим доступу до ресурсу: https://www.ibm.com/topics/blockchain-security.

2.A comprehensive review of blockchain: From fundamentals to current implementation and future trends. [Електорний ресурс] — Режим доступу до ресурсу: https://ieeexplore.ieee.org/abstract/document/8250109.

3.Microsoft takes another stab at a Blockchain-powered ledger service [Електорний ресурс] — Режим доступу до ресурсу: https://www.zdnet.com/finance/blockchain/microsoft-takes-another-stab-at-a-blockchain-powered-ledger-service/.

4.Technology - Guardtime [Електорний ресурс] — Режим доступу до ресурсу: https://guardtime.com/technology.

5.N-iX Blockchain solutions designed by Ukrainian developers [Електорний ресурс] — 2019. — Режим доступу до ресурсу: https://medium.com/@N_iX/blockchain-solutions-designed-by-ukrainian-developers-2c1d3c29f152.

6.Bachynskyy T.,Roman [Електорний ресурс] / AKJournals. — 2019. — Режим доступу до ресурсу: https://akjournals.com/view/journals/2052/60/1/article-p3.xml.

Коцюбняк В'ячеслав Андрійович — студент групи 1Пі-21б, Факультет інформаційних технологій та комп'ютерної інженерії, Віницький національний технічний університет, м. Вінниця, e-mail: kocubnakv@gmail.com.

Магуран Володимир Сергійович **—** студент групи 1Пі-21б, Факультет інформаційних технологій та комп'ютерної інженерії, Віницький національний технічний університет, м. Вінниця, e-mail: vovchukmah@gmail.com.

Романюк Оксана Володимирівна **—** доцент кафедри програмного забезпечення, Віницький національний технічний університет, м. Вінниця, e-mail: oroman@vntu.edu.ua.

Viacheslav Kotsiubniak — student of group 1Pi-21b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, city of Vinnytsia, e-mail: kocubnakv@gmail.com.

Volodymyr Mahuran **—** student of group 1Pi-21b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, city of Vinnytsia, e-mail: vovchukmah@gmail.com.

Oksana Romaniuk **—** Associate Professor, Department of Software, Vinnytsia National Technical University, city of Vinnytsia, e-mail: oroman@vntu.edu.ua.