УДК 004.75

ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ДАНИХ В МЕРЕЖІ ІНТЕРНЕТ РЕЧЕЙ НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Яцків В.В. [1)], Барилко А.В.[2)], Верцімага Ю.О. [3)]
Тернопільський національний економічний університет
[1)] д.т.н., доцент;[2-3)] магістрант

I. Постановка проблеми

Останнім часом постійно зростає кількість випадків несанкціонованих дій (підробка, копіювання, видаляння або змінювання), щодо даних компаній та фізичних осіб. Незалежно від того, випадково або зловмисно, як хакери так і співробітники можуть порушити цілісність і достовірність даних, що призводить до фінансових втрат [1, 2]. Дані, які зберігаються в хмарі, можуть бути вразливими до порушення цілісності та конфіденційності. Ця основна проблема безпеки завадила деяким галузям промисловості, зокрема тих, що значною мірою потребують зберігання конфіденційних даних - від переміщення даних у хмару.

З використанням мережі дешевих сенсорів і з'єднаних між собою речей, збір інформації про навколишнє середовище можна реалізувати з високим ступенем деталізації. Наявність детальної і точної інформації дозволить підвищити ефективність і забезпечити додаткові послуги в різних галузях.

Потенційними галузями для застосування Інтернет речей (Internet of Things, IoT) є сільське господарство, моніторинг навколишнього середовища, моніторинг здоров'я, смарт- виробництво, інтелектуальні міста та інші [3]. Проте, збільшення пристроїв збору, та обробки даних підключених до мережі Інтернет, призводить до виникнення серйозних проблем, пов'язаних з безпекою даних, зокрема з конфіденційністю, анонімністю, стійкістю та зберіганням даних. Деякі з цих ризиків відомі, інші потребують досліджень. Приділення недостатньої уваги проблемі безпеки в середовищі IoT може призвести, наприклад, до атак на секретність і аутентифікацію, цілісність обслуговування або атак відмови в обслуговуванні (DoS) [4].

Широке впровадження Інтернету речей (IoT) ускладняється необхідністю забезпечити цілісність а інколи і конфіденційність даних, що надходять на пристрої IoT та з них. Організації витрачають значну кількість ресурсів для захисту та підтвердження цілісності своїх даних. За даними Інституту SANS, 63% організацій стверджують, що захист даних є головним чинником витрат на безпеку. Отже забезпечення цілісності ділових та особистих даних є актуальною задачею.

II. Мета роботи

Метою дослідження є розробка структури системи забезпечення цілісності даних в середовищі Інтернет речей із використанням технології блокчейн.

III. Забезпечення цілісності даних в мережі Інтернет речей

В даний час ведуться дослідження та здійснюється реалізація ряду проектів з використанням технології блокчейн в різних секторах економіки.

За своєю конструкцією, технологія блокчейн забезпечує стійкість до модифікації даних. Це означає, що після додавання даних або транзакції запис про ці зміни не може бути змінений або видалений.

Дані в блокчейн зберігаються в блоках, які є хронологічно упорядкованою структурою даних транзакцій. Кожен блок ланцюга містить два елементи заголовок: 1) мітки часу, задачі складності PoW, хеш-значення попереднього блоку, корінь дерева Merkle, nonce, який необхідний для вирішення задачі PoW; 2) блок даних: він містить всі входи та виходи кожної транзакції. Вхідні дані містять вивід попередніх транзакцій і поле, що містить підпис із приватним ключем власника. Це підтвердження права власності на актив. Виходи містять актив, який необхідно надіслати та адресу одержувача (відкритий ключ одержувача). Одержувач буде єдиним користувачем, який зможе витратити цей актив, оскільки лише його приватний ключ може підтвердити право власності на актив.

Таким чином, прості слова, щоразу, коли група транзакцій затверджується, яка підключається до попереднього блоку через хеш, унікальна та незмінна марка, яка забезпечує гарантію, що ніхто не може втрутитися в записані дані.

Єдиний спосіб змінити блок полягає в тому, щоб отримати 51% обчислювальної потужності всієї мережі, яка діє на блок. Отже, людині неможливо зробити зміни в блокчейн. Це фундаментальний елемент, що робить децентралізований блокчейн захищеним та розподіленим до того ж, така децентралізація дозволяє ліквідувати будь-яку центральний орган, спираючись, натомість, на "демократію обчислювальної влади", яку забезпечують тисячі учасників мережі блокчейн. Структурна схема роботи мережі IoT на основі блокчейн приведена на рисунку 1.

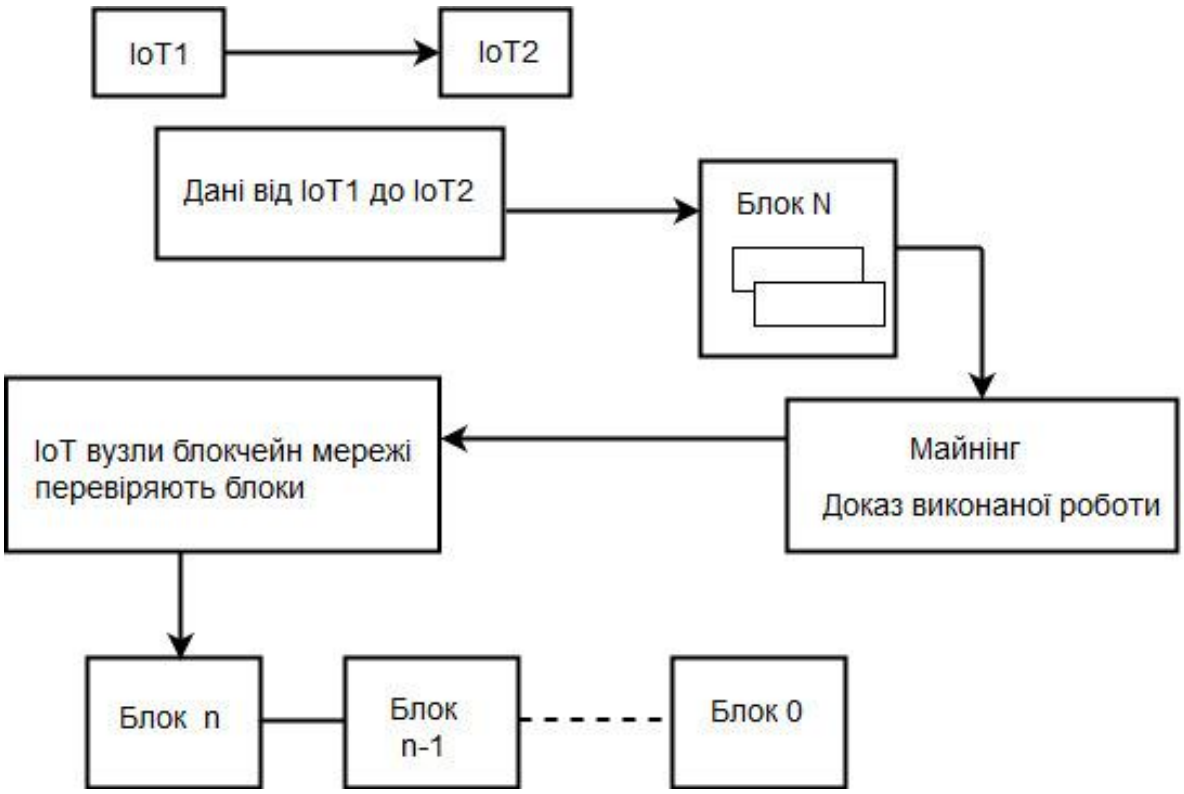

Рисунок 1 – Структурна схема роботи мережі IoT на основі блокчейн

З даних, які надходять від пристроїв IoT формується блок (Блок N). В блоці Майнінг відбувається виконання складної обчислювальної задачі, яка полягає в знаходженні значення хеш функції, яка починається із наданої кількості нулів. Сформований блок даних додається до раніше сформованих блоків. Всі IoT вузли блокчейн мережі можуть перевірити цілісність даних в будь-якому блоці.

Висновок

У роботі розроблено структуру системи забезпечення цілісності даних в мережах Інтернет речей з використанням технології блокчейн. Технології блокчейн гарантує цілісність даних в середовищі де отримувачі інформації не довіряють один одному.

Список використаних джерел

1. Novo, O. Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Int. Things J. 2018, 5, pp.1184–1195.
2. Samaniego, M.,Deters, R. Blockchain as a Service for IoT. In Proceedings of the 9th IEEE International Conference on Internet of Things, Chengdu, China, 15–18 December 2016; pp. 433–436.
3. Яцків Н.Г., Яцків С.В. Перспективи використання технології блокчейн в мережі Інтернет речей. Науковий вісник НЛТУ України. - 2016. - Вип. 26.8. – С. 381-387.
4. Яцків Н.Г., Яцків С.В. Типи атак на Інтернет речей. Захист інформації і безпека інформаційних систем: матеріали VI Міжнародної наукової технічної конференції. – Львів: Видавництво Львівської політехніки, 2017 р. – С.162-163.