SECTION 16.
INFORMATION TECHNOLOGIES AND SYSTEMS

Лещенко Юлія Ярославівна
здобувач вищої освіти факультету комп'ютерних систем і автоматизації
Вінницький національний технічний університет, Україна

Мороз Ігор Ігорович
здобувач вищої освіти факультету комп'ютерних систем і автоматизації
Вінницький національний технічний університет, Україна

Юхимчук Марія Сергіївна
проф. кафедри комп'ютерних систем управління
Вінницький національний технічний університет, Україна

FUSION CHAIN: ЗАСТОСУВАННЯ ДЕЦЕНТРАЛІЗОВАНОГО БЛОКЧЕЙНУ

Анотація. *У цій статті представлено огляд існуючих і нових технологій блокчейну та їх можливості для впровадження в системах Інтернету речей (IoT) для забезпечення безпеки та надійності зберігання та обробки даних. Огляд основних проблем існуючих архітектур для IoT, які часто є причиною атак зловмисників і витоку конфіденційних даних. Запропоновано методи вирішення цих проблем за допомогою блокчейну. Порівнюється придатність різних блокчейн-платформ, таких як Bitcoin, Ethereum і Hyperledger Fabric, для IoT, враховуючи масштабованість, вимоги до обчислювальних ресурсів і рівні безпеки. Узагальнено переваги технології блокчейн у забезпеченні децентралізованого зберігання даних, захисті від DDoS-атак і підвищенні загальної безпеки систем IoT.*

IoT (інтернет речей) – це технологія, яка під’єднує до інтернету все: від невеликих комунікаційних об’єктів, таких як вбудовані датчики в вимикачах світла, до великих та технічно складних пристроїв, таких як транспортні засоби, промислове устаткування тощо. Очікується, що кількість IoT пристроїв збільшиться з 30.73 мільярдів у 2020 році до 75,44 мільярдів у 2025 році [1]. Зі збільшенням використання сфера застосування пристроїв інтернету речей широко розповсюдилася на різні галузі, серед яких виробництва, транспорт, енергетика, торгівля, охорона здоров’я, логістика, будівництво тощо [2]. Загальний обсяг даних, який генеруватимуть пристрої IoT у 2025 оцінюється в 79.4 ЗБ (зетабайт) [3]. Враховуючи це постає питання безпеки інтернету речей, оскільки пристрої та девайси збирають та обробляють великі обсяги конфіденційних даних, таких як персональні бібліометричні дані, зображення, фотографії, голоси та геолокації [4]. Однак існуючі пристрої інтернету речей використовують централізовану архітектуру для обробки та зберігання даних. Збираючи і передаючи велику кількість даних на центральний сервер, вони спричиняють проблему монополізації прав на дані, тим самим дають можливість реалізовувати різноманітні схеми зловмисників, такі як метод ботнету Mirai, які атакують центральний сервер, заражаючи пристрої IoT, використовуючи вразливість центральної мережі IoT. Такі атаки зловмисників фактично зламали 500 000 серверів, домашніх роутерів та пристроїв IoT, в т.ч. були випадки витоку паролів користувачів, які зберігались на центральному сервері [5].

Технологія криптографії, що використовується для забезпечення безпеки існуючої централізованої архітектури, не може гарантувати надійність даних, тому що довірена третя сторона відповідає за запобігання підробки даних. Технологія блокчейн розглядається як ефективне вирішення цієї проблеми. Блокчейн має всі ті ж переваги розподілених систем, але базуючись на алгоритмі консенсусу, вузли мережі можуть гарантувати надійність даних і запобігати їх підробці, тим самим ефективно вирішуючи проблеми описані вище. Основна ідея полягає в тому, що мережа блокчейн використовує децентралізований метод, заснований на P2P (peer to peer) мережі, вузли якої можуть брати участь в вже існуючих системах без зміни або додаткового обладнання. Блоки мережі блокчейн розподіляються та зберігаються в кожному вузлі з однаковими даними, тому, навіть якщо проблема виникає в деяких вузлах, на загальну систему це має менший вплив. Завдяки цим особливостям, мережі на основі блокчейн мають деякі переваги. По-перше, дані зберігаються для кожного вузла мережі блокчейн, що ускладнює маніпулювання та підміну даних зловмисниками. По-друге, мережа блокчейн ефективно захищає від атак на сервери, таких як DDoS, завдяки децентралізованій структурі мережі [6]. По-третє, навіть в випадку проблеми з'єднань між деякими пристроями в системі, ця проблема має менший вплив на роботу загальної мережі.

Тим не менш, існуюча технологія блокчейн має обмеження при використанні в IoT системах:

1. Блоки в мережі блокчейн з часом збільшуються і вимагають великого обсягу пам'яті. Для пітримки нового вузла розмір блоку в мережі Ethereum на сьогоднішній день досяг 308 ГБ, у випадку з Bitcoin – 271 ГБ [7].

2. Обчислювальна потужність пристроїв IoT не дає змогу використовувати їх для участі в найбільш розповсюдженому алгоритмі консенсусу технології блокчейн – PoW (proof of work). Даний алгоритм вимагає великих обчислювальних потужностей для забезпечення швидкодії системи (в т.ч. використання графічних процесорів з великою кількістю обчислюваних ядер).

3. Зі збільшенням використання пристроїв IoT на них зберігається конфіденційна інформація, така як фотографії та зображення, медична інформація і це стає серйозною проблемою конфіденційності, коли вони витікають в результаті хакерських атак. У випадку з TRENDnet, компанією, яка виробляє і продає SecurView, через проблеми з безпекою її IoT-продуктів хакери отримали доступ до великої кількості зображень в будинках приблизно 700 домогосподарств [8].

У цій науковій статті здійснено аналіз основних блокчейн-платформ, у тому числі тих, які використовуються в системах Інтернету речей (IoT). Проведено порівняльну оцінку їхніх характеристик, включаючи рівень захищеності, швидкість взаємодії та обсяг необхідної пам'яті. Дослідження розкриває різноманітність підходів до імплементації блокчейн-технологій у сфері IoT і дозволяє ідентифікувати ключові переваги та недоліки кожної з розглянутих платформ. Аналізуються також важливі аспекти, такі як масштабованість, ефективність консенсус-протоколів та можливість взаємодії з існуючими інфраструктурами IoT.

У роботі Sensor-chain [9] було запропоновано полегшене рішення для належного використання пристроїв IoT у блокчейні. Було використано просторовий блокчейн, який розділяє блокчейн на просторові одиниці, та функцію менеджера міграції в поєднанні з міграцією в часі. Кожен вузол володіє блокчейном відповідно до свого простору, а вміст даних блокчейну агрегується в один блок, розмір блокчейну зменшується, починаючи з цього блоку.

У статті IPFS for Smart Contract було запропоновано рішення з використанням IPFS для зменшення ваги блокчейну Ethereum. У цій роботі загальний розмір Ethereum був зменшений за рахунок завантаження коду смарт-контракту в Ethereum і не займати місце

за рахунок непотрібних або невикористовуваних смарт-контрактів, а також завантаження коду смарт-контракту в IPFS і зберігання тільки хешу IPFS. Цей метод підходить тільки для Ethereum і дозволяє зменшити розмір коду смарт-контракту, що зберігається в блокчейні Ethereum.

Таблиця 1

Порівняльна таблиця Blockchain платформ:

Платформа	Розширюваність	Алгоритм консенсусу	Тип вузла	Створення блоку	Валідація блоку	Створення / Підтвердження транзакції	Накладні витрати CPU/GPU
Bitcoin	Так	PoW	Повний вузол	Так	Так	Так	Високі
			Легкий вузол	Ні	Ні	Так	Низькі
Ethereum	Так	PoW	Повний вузол	Так	Так	Так	Високі
			Легкий вузол	Ні	Ні	Так	Низькі
Hyperledger Fabric	Ні	Kafka, Raft, Solo	Рівноправний	Ні	Так	Так	Низькі
			Впорядкований	Так	Ні	Ні	Низькі
Fusion Chain	Так	PBFT	-	Так	Так	Так	Низькі

Біткойн – онлайн криптовалюта, заснована на технології блокчейн. Була розроблена для того, щоб дозволити людям вільно здійснювати фінансові транзакції в режимі P2P, без центральної установи, такої як банк. У мережі Біткоїн доступні два типи вузлів: повний вузол та легкий вузол. Повний вузол Біткоїну синхронізує всі дані блокчейну мережі Біткоїн і бере участь у процесі консенсусу, оскільки зберігає всі дані блоку від генезисного блоку до теперішнього часу.

Полегшений вузол Біткоїна бере участь у блокчейні і виконує транзакції. Він запитує дані у повного вузла для перевірки окремих транзакцій. Цей вузол не володіє всіма даними блоку, як повний вузол, а лише підсумовує і зберігає важливі дані в дереві Меркла в заголовку блоку. Ці вузли можуть перевіряти і створювати транзакції, але не можуть брати участь в процесі консенсусу.

Ethereum – розподілена обчислювальна платформа для реалізації смарт-контрактів на основі технології блокчейн. Вона забезпечує розширюваність для роботи різних додатків зі смарт-контрактами. Повний вузол Ethereum зберігає всі дані блокчейну і перевіряє нові транзакції та отримані блоки, а також бере участь у процесі консенсусу. Як і Біткоїн, Ефір адаптує PoW як базовий алгоритм консенсусу і вимагає високі обчислювальні потужності для майнінгу блоків.

Аналогічно з Біткоїном, полегшений вузол Ефіру зберігає не всі дані блокчейну, а лише частину інформації про блокчейн. При зберіганні блоків для зменшення ваги використовується деревоподібна структура Меркла-Патрісії в заголовку блоку. Не можуть брати участь в процесі консенсусу PoW.

Fusion Chain – це інноваційна блокчейн-архітектура, спеціально розроблена для Інтернету речей (IoT). Вона використовує алгоритм консенсусу PBFT (Practical Byzantine Fault Tolerance) для забезпечення високої надійності та швидкості транзакцій. Для децентралізованого зберігання даних Fusion Chain інтегрує IPFS (InterPlanetary File System), що дозволяє ефективно керувати великими обсягами інформації.

Архітектура Fusion Chain:

Відображено всю архітектуру Fusion Chain, а також процес створення блоку в Fusion Chain (рис. 1).

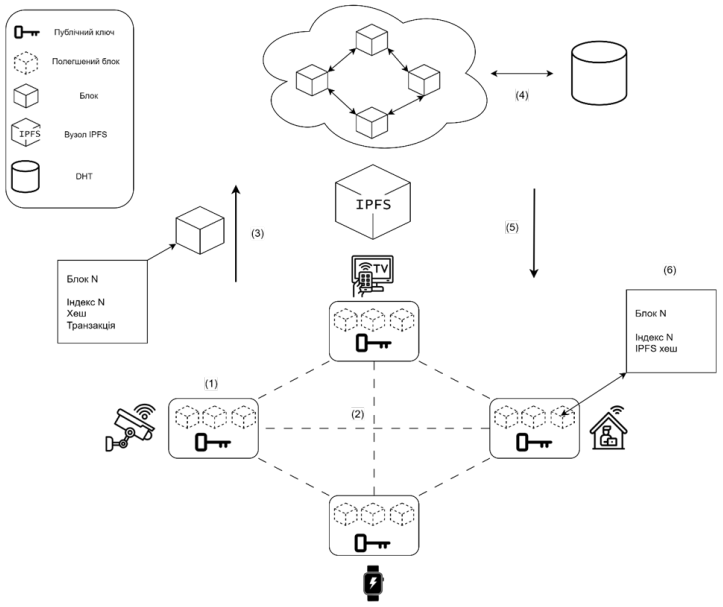

Рис. 1. **Архітектура системи Fusion Chain**

1. Перший крок. Пристрій IoT фіксує та збирає дані за допомогою датчиків і шифрує їх використовуючи свій відкритий ключ. Після чого створює транзакцію і передає її іншим учасникам мережі.

2. Другий крок. Всі вузли мережі Fusion Chain використовують консенсус PBFT. Якщо консенсус знайдено, створюється новий блок, який включає в себе транзакцію з першого кроку.

3. Третій крок. Створений блок завантажується в IPFS.

4. Четвертий крок. Завантажений блок зберігається в розподіленій хеш-таблиці (DHT) мережі IPFS.

5. П’ятий крок. Коли блоки розподілені і зберігаються в мережі IPFS, хеш IPFS повертається в Fusion Chain.

6. Шостий крок. Вузол Fusion Chain створює полегшений блок, який зберігає індекс і хеш IPFS блоку в блоці, після чого зберігає його в блокчейні.

У мережі блокчейн з переданої транзакції створюється блок, який перевіряється за допомогою алгоритму консенсусу PBFT. В IPFS перевірений блок розподіляється і зберігається в IPFS, і повертається тільки хеш IPFS. В мережі блокчейн в блоці зберігається тільки індекс і хеш IPFS.

Fusion Chain використовує IPFS для зменшення накладних витрат на зберігання даних блокчейну у вузлі IoT. IPFS зберігає файли, так як фотографії, текстові файли та відео, поширені в інтернеті і може швидко завантажувати розподілені дані за допомогою унікальних хеш-значень. За допомогою унікального хеш-значення можна швидо та ефективно завантажувати файли великого обсягу. Таким чином, його можна використовувати для зберігання великих файлів. У Fusion Chain блоки зберігаються в IPFS, блокчейн Fusion Chain зберігає лише хеш-значення блоку. Розподілена хеш таблиця (DHT) дозволяє вузлам, що беруть участь в мережі IPFS, керувати хеш-таблицями індивідуально і зберігати дані без сервера. DHT використовується при пошуку файлу, використовуючи метод зіставлення імені файлу зі значенням у хеш-таблиці, що зберігається у кожному вузлі блокчейну, без використання центрального сервера. IPFS використовує метод пошуку імені файлу (CID) в таблиці DHT за допомогою даних, адресованих за вмістом. Сам метод використовує файл як адресу, за якою в подальшому знаходяться вузли, які розповсюдили фрагменти файлу. Коли IPFS поширює файли, він перетворює всі файли в мережі у формат орієнтованого ациклічного графа Меркла (DAG). Для кожного вузла в Merkle-DAG

використовується CID та хеш вмісту вузла. Використовуючи Merkle-DAG, IPFS може адресувати вміст, запобігати несанкціонованому доступу та дублюванню. IPFS працює шляхом пошуку та обміну об'єктами IPFS. Об'єкти IPFS зберігають вміст файлу лише у двійковому форматі, якщо вміст оригінального файлу менший за 256 КБ, і зберігають файли частинами, якщо вміст оригінального файлу більший за 256 КБ.

Приведена схема того, як зберігаються блоки в IPFS у Fusion Chain (рис. 2).

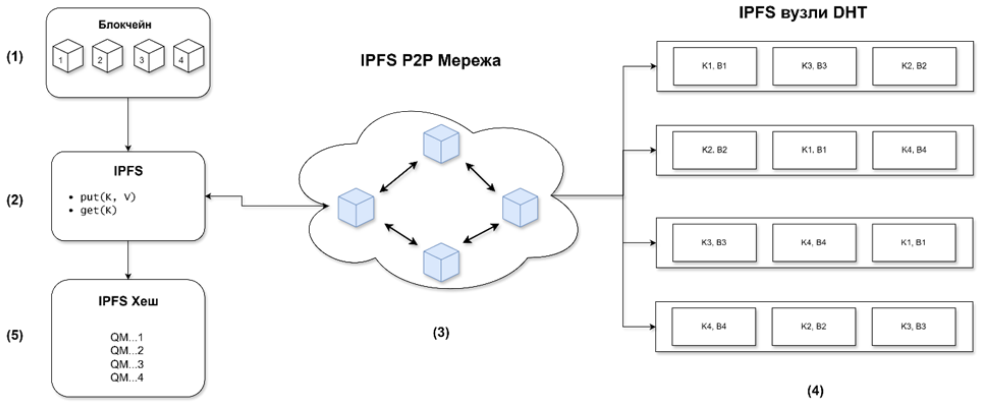

Рис. 2. **Зберігання блоків DHT**

Метод зберігання полягає в наступному:

1. Перший крок. Блоки створюються в мережі блокчейн у вигляді файлів.
2. Другий крок. Створений блок завантажується в IPFS.
3. Третій крок. Файли блоків розподіляються між вузлами в IPFS P2P мережі.
4. Четвертий крок. Розділені файли зберігаються в DHT вузлів IPFS. При збереженні вони розподіляються і зберігаються у вигляді ключ-значення.
5. П'ятий крок. Після завантаження в IPFS повертається хеш IPFS, і значення хешу зберігається в блокчейні.

Зображена порівняльна діаграма структури Fusion Chain та Ethereum (рис. 3). Оскільки Fusion Chain орієнтований на пристрої IoT, він зберігає основні дані в блоці: індекс і хеш IPFS. Дані, що зберігаються в IPFS, містять індекс, хеш, попередній хеш, мітку часу та дані. Таким чином, блок Fusion Chain є доволі легким. На противагу цьому, блок Ethereum містить майже 20 полів даних у блоці, що призводить до великих додаткових витрат на зберігання інформації.

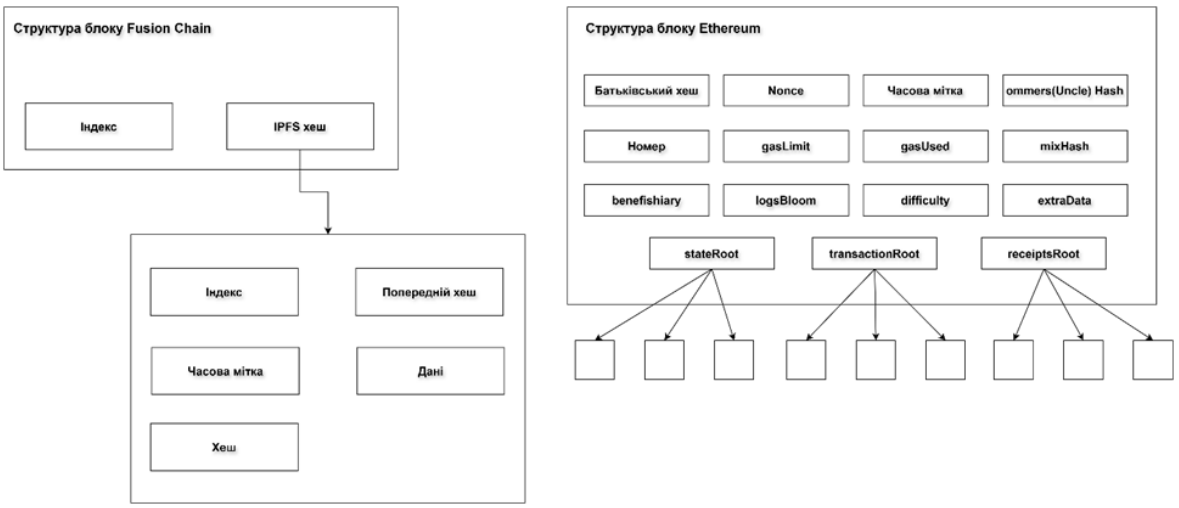

Рис. 3. **Порівняння структури блоків Fusion Chain та Ethereum**

Вузли мережі блокчейн Fusion Chain надсилають та отримують повідомлення під час процесу консенсусу PBFT. У мережі Fusion Chain вузол PBFT, який згенерував транзакцію, стає вузлом лідером, і після генерації блоку, він поширюється на всі інші вузли, після чого починається процес превотування.

Тестування блокчейн системи на трьох Малинках

Експеримент проводився з використанням трьох RaspberryPi 4 B (System on Chip: Broadcom BCM2711, Quad core Cortex-A72 (ARM v8) 64-bit SoC @ 1.5 GHz, Memory: 4 GB LPDDR4-3200 SDRAM, OS: Raspbian GNU Linux 10) [23]. Ланцюг злиття був реалізований за допомогою Node.js, а Ethereum - за допомогою Geth. Node.js використовувався версії 10.15.3, а Geth - версії 1.9.6. Geth - це офіційна golang-реалізація протоколу Ethereum.

Для експерименту використовувались чотири типи наборів даних для пристроїв Інтернету речей: текстовий файл, зображення, аудіо та відео. Представлений опис кожного виду файлів (табл. 2). Розмір кожного набору даних визначався на основі середнього розміру файлів txt, jpg, wav та mp4.

Таблиця 2

Датасет для IoT пристроїв

Тип даних	**Розмір**	**Формат**
Лог	1 КБ	txt
Зображення	10 КБ	jpg
Аудіо	100 КБ	wav
Відео	1 МБ	mp4

Підтримка низького навантаження на процесор і пам'ять є важливою вимогою для пристроїв IoT. Щоб протестувати навантаження на процесор і пам'ять, було виміряно використання процесора і пам'яті під час операцій майнінгу для Fusion Chain і Ethereum. Спочатку алгоритм консенсусу Fusion Chain за замовчуванням був PBFT. Крім того, окремо був використаний алгоритм консенсусу PoW в Fusion Chain для справедливого порівняння з Ethereum, оскільки він підтримує тільки PoW.

Показано використання процесора при роботі алгоритмів консенсусу Fusion Chain та Ethereum (рис. 4). Алгоритм консенсусу PBFT показав дуже низьке використання процесора (близько 6%) у порівнянні з PoW. Алгоритм PBFT досягає консенсусу за допомогою мережевого зв'язку між вузлами-учасниками. Таким чином, обчислення на центральному процесорі майже не виконуються. В результаті, алгоритм консенсусу Fusion Chain майже в 16 разів легший за алгоритм консенсусу Ethereum.

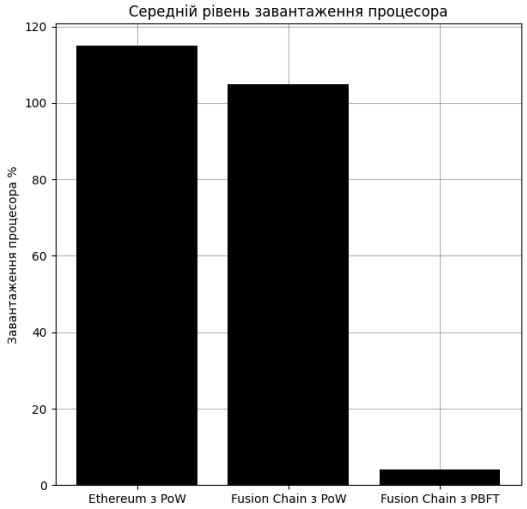

Рис. 4. **Завантаження процесора при роботі алгоритмів консенсусу**

Показано використання пам’яті при виконанні алгоритму консенсусу для мереж Fusion Chain та Ethereum (рис. 5). У порівнянні з алгоритмом консенсусу PBFT, PoW повинен підтримувати пул транзакцій для зберігання транзакцій в пам’яті. Через це алгоритм PBFT займає в середньому 49.6 МБ, а PoW – 64.4 МБ, тобто використовує в середньому на 30% більше пам’яті, ніж PBFT. У випадку з Ethereum в процесі майнінгу використовується в середньому 2.1 ГБ пам’яті.

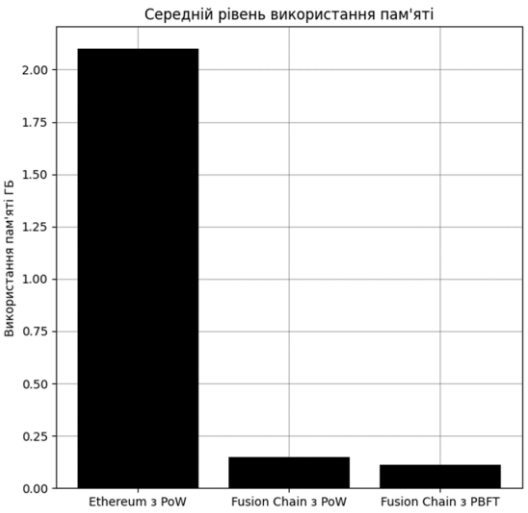

Рис. 5. **Використання пам’яті для різних алгоритмів консенсусу**

Висновок. Узагальнюючи результати дослідження, можна стверджувати, що технологія блокчейн здатна суттєво підвищити рівень безпеки та надійності IoT систем завдяки своїй децентралізованій природі й використанню алгоритмів консенсусу. Використання архітектури Fusion Chain, яка базується на алгоритмі консенсусу PBFT та системі зберігання даних IPFS, дозволяє ефективно обробляти і зберігати великі обсяги даних IoT, забезпечуючи високу швидкість транзакцій та низькі витрати на зберігання.

Попри всі переваги, існують певні технічні виклики, які потребують подальших досліджень і розробок. Це, зокрема, високі вимоги до обчислювальних потужностей та обсягів пам'яті для підтримки блокчейн мережі, що може обмежувати його використання у пристроях з обмеженими ресурсами. Розв’язання цих проблем можливо через оптимізацію алгоритмів консенсусу та впровадження нових методів компресії даних.

Таким чином, подальші наукові дослідження та інноваційні розробки в області блокчейн технологій мають великий потенціал для розширення застосування цієї технології в IoT системах, що сприятиме підвищенню рівня безпеки, надійності та ефективності їх функціонування.

Список використаних джерел:

1. Vailshery L. S. Topic: Internet of Things (IoT). Statista. Вилучено з: https://www.statista.com/topics/2637/internet-of-things/#topicOverview.
2. Blockchain IoT Market Size & Share, Trends Report, [Latest]. MarketsandMarkets. Вилучено з: https://www.marketsandmarkets.com/Market-Reports/blockchain-iot-market-168941858.html.
3. Hojlo J. Future of Industry Ecosystems: Shared Insights & Data | IDC Blog. IDC Blog | Global Market Intelligence. Вилучено з: https://blogs.idc.com/2021/01/06/future-of-industry-ecosystems-shared-data-and-insights/.
4. IoT Security: Needed now more than ever. CISO MAG | Cyber Security Magazine. Вилучено з: https://cisomag.com/iot-security-needed-now-more-than-ever/.
5. Cimpanu C. Hacker leaks passwords for more than 500,000 servers, routers, and IoT devices. ZDNET. Вилучено з: https://www.zdnet.com/article/hacker-leaks-passwords-for-more-than-500000-servers-routers-and-iot-devices/.

6. Shafi Q., Basit A. DDoS Botnet Prevention using Blockchain in Software Defined Internet of Things. IEEE Xplore. Вилучено з: https://ieeexplore.ieee.org/abstract/document/8667147.
7. Phillips D. Ethereum archive nodes now take up 4 terabytes of space - Decrypt. Decrypt. Вилучено з: https://decrypt.co/24779/ethereum-archive-nodes-now-take-up-4-terabytes-of-space.
8. Kerr D. FTC and TrendNet settle claim over hacked security cameras. CNET. Вилучено з: https://www.cnet.com/news/privacy/ftc-and-trendnet-settle-claim-over-hacked-security-cameras/.
9. Shahid A., Pissinou N., Kwan R. Sensor-Chain: A Lightweight Scalable Blockchain Framework for Internet of Things. IEEE Xplore. Вилучено з: https://ieeexplore.ieee.org/document/8875416.
10. Norvill R., State R., Cullen A. IPFS for Reduction of Chain Size in Ethereum. IEEE Xplore. Вилучено з: https://ieeexplore.ieee.org/abstract/document/8726794.