

УДК 004.738.5:004.056.5:004.7

DOI <https://doi.org/10.32782/tnv-tech.2025.1.20>

ДЕЦЕНТРАЛІЗОВАНІ ІОТ-МЕРЕЖІ: БЛОКЧЕЙН ДЛЯ БЕЗПЕКИ ТА АВТОНОМНОСТІ

Сіпко О. М. – кандидат технічних наук, доцент кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченка
ORCID ID: 0000-0003-1385-119X
Scopus-Author ID: 58865476600

У статті досліджено проблеми централізованих IoT-мереж, зокрема соціальних IoT (SIoT)-систем, які стикаються з викликами безпеки, масштабованості та автономності пристроїв. Традиційні SIoT-архітектури покладаються на централізовані сервери для керування взаємодією пристроїв, що створює ризики збоїв, підвищену вразливість до кібератак та обмеження у швидкості обробки запитів у міру зростання кількості підключених пристроїв. Запропоновано новий підхід до побудови довірчих взаємодій між IoT-пристроями, що базується на використанні блокчейну та соціальних зв'язків. Такий підхід дозволяє усунути залежність від централізованого контролю, підвищити рівень безпеки даних та забезпечити пристроям більшу автономність у прийнятті рішень.

У межах дослідження представлено алгоритм децентралізованого управління довірою, який використовує розподілений реєстр для фіксації взаємодій між пристроями, смарт-контракти для автоматизації перевірок і виконання умов довіри, а також механізм динамічної оцінки рівня довіри пристроїв на основі їхньої поведінки, історії попередніх транзакцій та рекомендацій інших вузлів у мережі. Особливу увагу приділено механізму графового консенсусу, який забезпечує ефективну перевірку транзакцій у SIoT без надмірних обчислювальних витрат, що є критично важливим для пристроїв з обмеженими ресурсами.

Запропонована модель дозволяє пристроям автономно оцінювати рівень довіри одне до одного за допомогою поєднання алгоритмів аналізу історичних даних і рекомендацій від довірених вузлів. Це усуває необхідність у централізованих серверах, значно знижує ризики атак, запобігає маніпуляціям з боку злоумисників і створює безпечне, масштабоване та ефективне середовище для функціонування IoT-пристроїв.

Результати дослідження демонструють, що блокчейн у поєднанні з SIoT формує стійку та адаптивну систему управління довірою, яка може бути ефективно застосована у сфері автономного транспорту, розумних міст, охорони здоров'я та критичної інфраструктури. Запропонований підхід забезпечує високу масштабованість мереж, підвищує рівень захисту даних та сприяє автономному функціонуванню пристроїв у децентралізованому середовищі, що відкриває нові можливості для побудови більш безпечних і надійних IoT-екосистем.

Ключові слова: блокчейн, Social IoT, довіра між пристроями, децентралізовані мережі, смарт-контракти, управління довірою.

Sipko O. M. Decentralized IoT networks: blockchain for security and autonomy

The paper explores the challenges of centralized IoT networks, particularly Social IoT (SIoT) systems, which face critical issues related to security, scalability, and device autonomy. Traditional SIoT architectures rely on centralized servers for managing device interactions, leading to risks of failures, increased vulnerability to cyberattacks, and limitations in processing speed as the number of connected devices grows. A novel approach to establishing trusted interactions among IoT devices is proposed, based on blockchain technology and social connections. This approach eliminates dependency on centralized control, enhances data security, and enables greater autonomy in device decision-making.

The study presents an algorithm for decentralized trust management, leveraging a distributed ledger to record interactions, smart contracts to automate authentication and enforce trust conditions, and a dynamic trust evaluation mechanism based on behavioral analysis, historical transactions, and recommendations from trusted nodes. Particular attention is given to the graph-based consensus mechanism, which enables efficient transaction verification in SIoT while minimizing computational overhead, a crucial factor for resource-constrained IoT devices.

The proposed model allows devices to autonomously assess trust levels through a combination of historical data analysis and recommendations from trusted nodes. This eliminates the need for centralized servers, significantly reduces attack risks, prevents malicious manipulations, and creates a secure, scalable, and efficient environment for IoT operations.

The research findings demonstrate that integrating blockchain with SIoT establishes a robust and adaptive trust management system, making it highly suitable for applications in autonomous transportation, smart cities, healthcare, and critical infrastructure. The proposed approach ensures high network scalability, enhances data protection, and facilitates autonomous device operation in a decentralized ecosystem, paving the way for the development of more secure and resilient IoT networks.

Key words: *blockchain, Social IoT, trust management, decentralized networks, smart contracts, trust-based interactions.*

Вступ. Інтернет речей (IoT) відіграє ключову роль у сучасному цифровому світі, сприяючи розвитку розумних міст, автономного транспорту, промислових рішень та медичних технологій [1, с. 618]. Завдяки IoT пристрої можуть взаємодіяти між собою, обмінюватися даними та автоматизувати різноманітні процеси, що значно підвищує ефективність багатьох галузей. Проте стрімке зростання кількості підключених пристроїв несе значні виклики, пов'язані з безпекою, конфіденційністю, масштабованістю та стійкістю систем [2, с. 2292]. Завдяки IoT пристрої можуть взаємодіяти між собою, обмінюватися даними та автоматизувати різноманітні процеси, що значно підвищує ефективність багатьох галузей.

Аналіз останніх досліджень і публікацій. Традиційні IoT-мережі, що базуються на централізованій архітектурі, стикаються з низкою обмежень [3, с. 1184]. Централізовані сервери, які керують пристроями та їх взаємодією, створюють вразливість системи, оскільки відмова головного сервера може призвести до зупинки всієї мережі.

Централізовані SIoT-системи мають низку критичних недоліків, що обмежують їхню ефективність та безпеку [4, с. 251]. Централізовані SIoT-системи схильні до кібератак та порушень конфіденційності [5, с. 2575]. Оскільки всі дані проходять через центральний сервер, він стає основною мішенню для хакерів. Злом такого сервера може призвести до витоку персональної інформації користувачів, компрометації пристроїв та маніпуляції даними. Це особливо критично для галузей, де використовується чутлива інформація, наприклад, у медицині або фінансовому секторі.

Ще одна значна проблема централізованих SIoT-систем – обмежена масштабованість. У міру зростання кількості пристроїв навантаження на центральні сервери збільшується, що може спричиняти затримки у передачі даних, зниження продуктивності та зростання витрат на інфраструктуру. Крім того, централізований контроль зменшує автономність пристроїв, оскільки вони не можуть самостійно приймати рішення та взаємодіяти без посередництва сервера.

Високі експлуатаційні витрати також є суттєвим недоліком централізованих SIoT-систем. Власники таких мереж змушені інвестувати значні кошти у підтримку серверної інфраструктури, забезпечення безпеки та протидію DDoS-атакам. Враховуючи всі ці виклики, децентралізований підхід на основі блокчейну стає перспективним рішенням, яке може суттєво покращити безпеку, масштабованість та автономність SIoT-мереж.

Мета дослідження. Дослідження спрямоване на розробку децентралізованого підходу до управління довірою між IoT-пристроями на основі блокчейну. Основна мета – усунення проблем централізованих SIoT-систем шляхом інтеграції розподіленого реєстру, смарт-контрактів та механізмів графового консенсусу для ефективної взаємодії між пристроями без необхідності центрального контролера.

Виклад основного матеріалу. Блокчейн є перспективною технологією для вирішення проблем централізованих SIoT-систем, оскільки забезпечує децентралізовану архітектуру, підвищену безпеку та автономність пристроїв. Одним із ключових аспектів впровадження блокчейну у SIoT є використання цієї технології для управління довірою між пристроями. Традиційні системи довіри в SIoT покладаються на централізовані сервери, які визначають рівень довіри між пристроями, що ускладнює їхню автономну взаємодію. Інтеграція блокчейну дозволяє впровадити децентралізований механізм довіри, де кожен пристрій самостійно бере участь у прийнятті рішень на основі криптографічно захищених записів про попередні взаємодії.

Блокчейн забезпечує безпеку довірчих відносин за рахунок використання смарт-контрактів, які автоматично виконують перевірки та підтвердження довіри між пристроями без необхідності втручання третіх сторін. Смарт-контракти можуть визначати рівень довіри пристрою на основі його історії взаємодій, що унеможливорює підробку або маніпуляцію даними.

Децентралізація довіри у SIoT також досягається завдяки використанню розподіленого реєстру, у якому всі дії пристроїв записуються та зберігаються у незмінному вигляді. Це означає, що пристрої можуть перевіряти автентичність інших вузлів у мережі без потреби у централізованому сервері. Наприклад, якщо один пристрій раніше взаємодіяв з іншим без порушень, він може автоматично підтвердити його надійність у майбутніх транзакціях.

Додатково, блокчейн дозволяє створити механізм гнучкої адаптації рівня довіри, який змінюється залежно від поведінки пристрою. Якщо пристрій демонструє коректну поведінку протягом тривалого часу, його рівень довіри зростає. Якщо ж виявляється підозріла активність, то рівень довіри знижується, а пристрій може бути виключений з критично важливих операцій у мережі. Такий підхід підвищує загальну безпеку мережі, роблячи її більш стійкою до зловмисних атак та випадкових збоїв.

Таким чином, інтеграція блокчейну в SIoT сприяє створенню безпечного, масштабованого та автономного середовища, в якому пристрої можуть взаємодіяти без посередників, мінімізуючи ризики централізованого управління та підвищуючи довіру між учасниками мережі.

Існуючі підходи до забезпечення довіри між пристроями в SIoT зазвичай спираються на централізовані або гібридні моделі, де певний керуючий сервер або група авторизованих вузлів приймають рішення щодо рівня довіри. Такий підхід має низку обмежень, зокрема високий ризик компрометації централізованого вузла та обмежену адаптивність до змін у мережі. Я пропоную новий підхід, що поєднує механізми SIoT та блокчейну для створення динамічної моделі довіри між пристроями, яка базується на децентралізованих соціальних зв'язках та гнучких механізмах взаємної оцінки.

Ключова ідея нового підходу полягає у формуванні динамічної довірчої мережі, де пристрої будують відносини аналогічно до соціальних мереж людей. Довіра між пристроями не визначається централізованим сервером, а формується на основі таких критеріїв:

- Спільна історія взаємодій – пристрої, які взаємодіють довгий час без порушень, отримують вищий рівень довіри.
- Рекомендації від надійних пристроїв – якщо кілька пристроїв із високим рейтингом довіри підтверджують автентичність нового пристрою, його рівень довіри підвищується.

- Контекстуальна довіра – рівень довіри може змінюватися залежно від сценарію використання (наприклад, у критичних застосуваннях можуть діяти жорсткіші критерії довіри).

Для того, щоб довірчі зв'язки були захищеними від маніпуляцій, вони записуються у блокчейн у вигляді криптографічно підписаних транзакцій. Це забезпечує кілька ключових переваг. По-перше, гарантується прозорість, оскільки всі учасники мережі можуть відстежувати зміни рівня довіри конкретного пристрою, що унеможливорює приховані маніпуляції. По-друге, підrobка стає неможливою, адже пристрій не може штучно підвищити свій рейтинг довіри, оскільки всі зміни фіксуються через механізм консенсусу. Нарешті, система підтримує децентралізовану автентифікацію, що дозволяє пристроям перевіряти рівень довіри один до одного без необхідності централізованого сервера, зменшуючи ризики зловмисного втручання.

Запропонована модель довіри включає адаптивний алгоритм оновлення рейтингу пристроїв, який реагує на їхню поведінку. Основні принципи цього алгоритму:

- Якщо пристрій коректно взаємодіє з іншими вузлами, його рівень довіри зростає поступово.
- Якщо пристрій демонструє підозрілу поведінку (наприклад, передає некоректні дані або раптово змінює ідентифікатор), його рейтинг довіри знижується.
- Пристрій з низьким рівнем довіри може бути тимчасово обмежений у доступі до критичних ресурсів мережі.

Традиційні алгоритми консенсусу (наприклад, Proof of Work) неефективні для IoT через високі обчислювальні витрати. Натомість моя модель довіри використовує графовий консенсус на основі соціальних зв'язків:

- Пристрої з високим рівнем довіри можуть підтверджувати транзакції інших пристроїв.
- Чим більше взаємопов'язаних довірених пристроїв підтвердять дію, тим вища її ймовірність бути прийнятою в мережу.
- Це дозволяє побудувати швидко та енергоефективну модель консенсусу, що не потребує складних обчислень.

Алгоритм поєднання Social IoT та блокчейну з новою моделлю довіри між пристроями виглядає наступним чином:

Етап 1. Ініціалізація мережі.

Крок 1.1. Реєстрація пристроїв. Кожен пристрій отримує унікальний ідентифікатор (IoT-ID) та криптографічну пару ключів (відкритий/закритий ключ). Відкритий ключ додається у блокчейн для подальшої перевірки підписів.

Крок 1.2. Початковий рівень довіри. Пристрої отримують початковий рейтинг довіри TiT_i , який визначається типом пристрою та попередньою історією взаємодій (якщо така є). Нові пристрої мають «нейтральний» рівень довіри, а перевірені пристрої можуть мати вищий початковий рейтинг.

Етап 1. Встановлення довірчих зв'язків між пристроями.

Крок 2.1. Соціальна модель взаємодії. Пристрої створюють динамічні соціальні зв'язки на основі попередніх взаємодій. Формуються типи зв'язків:

- Довготривалі – пристрої, що часто взаємодіють, отримують міцніший зв'язок.
- Тимчасові – зв'язки з пристроями, які рідко контактують, мають нижчу вагу.
- Рекомендовані – пристрій може довіряти іншому на основі довіри до спільного знайомого пристрою.

Крок 2.2. Динамічний граф довіри. Вузли IoT утворюють граф, де ребра – це довірчі зв'язки між пристроями з вагою W_{ij} . Вага W_{ij} змінюється залежно від успішності взаємодій.

Етап 3. Фіксація транзакцій у блокчейні.

Крок 3.1. Формування запису. При кожній взаємодії пристрої обмінюються цифровими підписами та хешем транзакції. Формується блок із записами:

$$(ID_A, ID_B, \text{час}, \text{дія}, \text{результат}, \text{підпис}_A, \text{підпис}_B)$$

Якщо транзакція успішна, пристрої оновлюють рівень довіри один до одного.

Крок 3.2. Запис у блокчейн. Пристрої з високим рівнем довіри підтверджують транзакцію за допомогою графового консенсусу (деталі нижче). Підтверджена транзакція додається до блоку, і пристрої оновлюють свої зв'язки у графі довіри.

Етап 4. Оновлення рівня довіри пристроїв.

Крок 4.1. Адаптивний алгоритм зміни довіри. Рівень довіри пристрою T_i оновлюється за формулою:

$$T_i = T_i + \alpha S_{ij} - \beta P_{ij}$$

де:

S_{ij} – успішні транзакції з пристроєм j ,

P_{ij} – невдалі або підозрілі взаємодії,

α, β – вагові коефіцієнти, які визначають швидкість зміни довіри.

Крок 4.2. Швидке зниження довіри для аномальної поведінки. Якщо пристрій демонструє аномальну активність (наприклад, намагається змінити свій ідентифікатор, маніпулює даними, відмовляється від підписаних транзакцій), рівень його довіри різко знижується.

Етап 5. Графовий механізм консенсусу. Оскільки стандартні алгоритми блокчейну (Proof of Work, Proof of Stake) не підходять для ресурсозалежних IoT-пристроїв, пропонується використання консенсусу на основі графа довіри.

Крок 5.1. Визначення валідаторів. Пристрої з найвищим рівнем довіри формують тимчасову комісію валідаторів. Кількість валідаторів обирається динамічно залежно від кількості пристроїв у мережі.

Крок 5.2. Процес перевірки. Кожен новий блок підтверджується мінімальною кількістю валідаторів V , визначеною за правилом:

$$V = \max(3, \sqrt{N}),$$

де N – загальна кількість пристроїв у мережі.

Пристрої підтверджують транзакції на основі історії довіри та успішних взаємодій.

Крок 5.3. Запобігання змовам. Якщо група валідаторів демонструє аномальні дії (наприклад, завищує рейтинг ненадійних пристроїв), вона виключається з мережі. Нові валідатори обираються на основі адаптивного рейтингу довіри.

Етап 6. Обробка збоїв та захист від атак.

Крок 6.1. Механізм виявлення зловмисників. Використовується система репутації: пристрої, які передають фальшиві або суперечливі дані, отримують штрафні бали. При перевищенні граничного рівня штрафів пристрій може бути тимчасово або назавжди відключений від мережі.

Крок 6.2. Захист від Sybil-атак. Введення нових пристроїв у мережу вимагає схвалення від пристроїв із високим рівнем довіри. Пристрої з недостатньою історією взаємодій отримують обмежені права до накопичення довіри.

Висновки і перспективи подальших досліджень. Запропонований алгоритм забезпечує динамічну адаптацію довіри між IoT-пристроями без необхідності централізованого управління. Запис усіх транзакцій у блокчейн унеможливорює маніпуляції та несанкціоновані зміни, що підвищує безпеку системи. Використання графового консенсусу дозволяє знизити витрати ресурсів, забезпечуючи ефективність роботи мережі. Гнучкість підходу виражається у можливості пристроїв змінювати рівень довіри в реальному часі залежно від їхньої поведінки та взаємодії з іншими вузлами. Автономність системи досягається завдяки тому, що вона не залежить від центрального сервера і може стабільно функціонувати навіть у розподілених IoT-середовищах. Такий алгоритм може бути ефективно застосований у сферах автономного транспорту [4, с. 251], розумних міст [5, с. 2575], безпечних систем охорони здоров'я [1, с. 618] та критичної інфраструктури.

Запропонований підхід до управління довірою між IoT-пристроями на основі блокчейну дозволяє усунути ключові проблеми централізованих SIoT-систем, підвищити рівень безпеки, масштабованості та автономності пристроїв. Використання децентралізованого реєстру та графового консенсусу сприяє ефективній перевірці транзакцій без надмірних обчислювальних витрат.

Подальші дослідження будуть спрямовані на розробку оптимізованих алгоритмів для динамічної адаптації довіри, тестування запропонованої моделі у реальних IoT-системах та оцінку її продуктивності в умовах високого навантаження.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. *IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2017, 618-623.
2. Christidis, K., & Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 2016, 4, 2292-2303.
3. Novo, O. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet of Things Journal*, 2018, 5(2), 1184-1195.
4. Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. Blockchain and IoT Integration: A Systematic Survey. *Sensors*, 2018, 18(8), 2575.
5. Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. Blockchain's adoption in IoT: The challenges, and a way forward. *Journal of Network and Computer Applications*, 2019, 125, 251-279.