ЗАСТОСУВАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ДЛЯ ЗАХИСТУ МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ

Хруслов Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Стрімкий розвиток Інтернету речей (IoT) та експоненціальне зростання кількості підключених пристроїв, що, за прогнозами, значно збільшиться в найближчі роки, створюють фундаментальні виклики для кібербезпеки. Традиційні, переважно централізовані, моделі управління IoT-мережами демонструють значні архітектурні вразливості. Вони покладаються на централізовані сервери для зберігання та обробки даних, що робить їх вразливими до єдиних точок відмови (SPOF), а також до атак типу «відмова в обслуговуванні» (DoS) та «людина посередині» (MITM). Ця проблема значно посилюється через апаратні обмеження та програмну різноманітність мільярдів IoT-пристроїв. Багато сенсорів та виконавчих пристроїв не мають достатньої обчислювальної потужності, пам'яті та енергоресурсів для імплементації складних криптографічних протоколів, що ускладнює впровадження уніфікованих та надійних механізмів захисту [1, 2].

У цьому контексті технологія блокчейн пропонує трансформаційне рішення, здатне кардинально підвищити рівень захищеності розподілених IoT-систем. Впровадження децентралізованого, незмінного та криптографічно захищеного розподіленого реєстру дозволяє вирішити ключові проблеми вразливості, притаманні централізованим підходам. Основні переваги полягають у забезпеченні надійної цілісності даних, оскільки будь-яка спроба модифікації інформації у ланцюгу блоків буде миттєво виявлена. Крім того, децентралізована природа технології усуває єдину точку відмови, підвищуючи загальну відмовостійкість. Важливим аспектом є можливість реалізації новітніх методів управління доступом та ідентифікацією, наприклад, через децентралізовані ідентифікатори та смарт-контракти для автоматизації правил взаємодії пристроїв [3].

Однак, незважаючи на очевидні переваги, практична інтеграція блокчейну в IoT стикається з серйозними викликами, які випливають із фундаментальної невідповідності між ресурсоємною природою блокчейну та апаратними обмеженнями IoT. Для подолання цих суперечностей активно розробляються та досліджуються нові методи та гібридні архітектури. Одним з найбільш перспективних рішень є побудова багаторівневих систем, де кінцеві малопотужні сенсори об'єднуються в локальні «IoT-кластери». У таких архітектурах смарт-контракти можуть використовуватися для автоматизації процесів та управління правилами доступу на рівні кластера, тоді як для обміну даними з кінцевими пристроями застосовуються оптимізовані для мікроконтролерів криптографічні протоколи та бібліотеки [4]. Незважаючи на ефективність гібридних моделей, критичними проблемами залишаються фундаментальні виклики масштабованості. По-перше, це низька пропускна здатність (кількість транзакцій на секунду, TPS). Класичні блокчейни не

розраховані на обробку масивних потоків даних у реальному часі, які генерують IoT-системи. По-друге, це вимоги до зберігання даних: реєстр має тенденцію до постійного зростання, оскільки зберігає повну історію транзакцій. Це унеможливлює розміщення повних вузлів на пристроях з обмеженою пам'яттю, змушуючи їх покладатися на менш безпечні «легкі вузли». По-третє, це висока затримка при підтвердженні транзакцій, що виникає через час, необхідний для генерації та валідації блоків, і є неприйнятною для систем реального часу. Нарешті, високе енергоспоживання традиційних консенсус-алгоритмів, як-от Proof-of-Work, робить їх використання неможливим для пристроїв, що живляться від батарей. Це змушує дослідників звертати увагу на енергоефективні альтернативи, як-от Proof-of-Stake або безблокові структури DAG (Tangle). Крім того, існує проблема початкової довіри до даних: блокчейн гарантує незмінність даних, але не їхню початкову правдивість. Якщо скомпрометований сенсор, через апаратний збій або зловмисну дію, передасть некоректні дані, блокчейн лише надійно зафіксує цю дезінформацію [5]. **Метою доповіді** є проведення аналізу ключових переваг та фундаментальних технічних викликів при інтеграції блокчейн-технологій в розподілені системи Інтернету речей. **В доповіді** наводяться результати огляду сучасних методів, що пропонуються для вирішення конфлікту між вимогами безпеки блокчейну та апаратними обмеженнями IoT-пристроїв. Особлива увага приділяється розгляду гібридних багаторівневих архітектур та легковагих криптографічних протоколів. Наведені дані показують, що хоча технологія блокчейн пропонує потужні механізми для забезпечення цілісності даних та децентралізації, її практична реалізація вимагає вирішення складних проблем масштабованості, вибору енергоефективних механізмів консенсусу та розробки методів верифікації даних на етапі їх початкового збору.

Список літератури

1. Obaidat M. A., Rawashdeh M., Alja'afreh M., Abouali M., Thakur K., Karime A. Exploring IoT and Blockchain: A Comprehensive Survey on Security, Integration Strategies, Applications and Future Research Directions. *Big Data and Cognitive Computing*. 2024. Vol. 8, Art. 174. DOI: https://doi.org/10.3390/bdcc8120174

2. Yevheniev, A. M., Sydorenko, Z. M., & Sievierinov, O. V. (2025). Забезпечення цілісності даних у системах промислового інтернету речей на основі використання завадостійких кодів. Radiotekhnika, (221), 46-50.

3. Enaya A., Fernando X., Kashef R. Survey of Blockchain-Based Applications for IoT. *Applied Sciences*. 2025. Vol. 15, Art. 4562. DOI: https://doi.org/10.3390/app15084562

4. Чепель Л. В., Бойко Ю. В. Підхід до безпеки та організації мереж IoT з використанням блокчейн технології. *Вісник Вінницького політехнічного інституту*. 2024. № 4. С. 129–138. DOI: https://doi.org/10.31649/1997-9266-2024-175-4-129-138

5. Mezquita Y., Casado R., Gonzalez-Briones A., Prieto J., Corchado J. M. Blockchain Technology in IoT Systems: Review of the Challenges. *Annals of Emerging Technologies in Computing (AETIC)*. 2019. Vol. 3, No. 5. DOI: https://doi.org/10.33166/AETIC.2019.05.003