УДК 004.738:004.056.5

ДОСЛІДЖЕННЯ ІНТЕГРАЦІЇ БЛОКЧЕЙНУ ДЛЯ БЕЗПЕЧНОГО ДЕЦЕНТРАЛІЗОВАНОГО УПРАВЛІННЯ ДАНИМИ IoT

В. Б. Юрченко[1,a], М. В. Коломицев[1]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

У роботі досліджено можливості застосування технології блокчейн для побудови безпечної децентралізованої моделі управління даними в системах Інтернету речей (IoT). Проаналізовано загрози в IoT, типи блокчейну, види протоколів консенсусу, а також особливості реалізації на основі смарт-контрактів. Запропоновано концептуальну модель інтеграції, яка дозволяє досягти високого рівня безпеки, контролю власності та цілісності даних.

Ключові слова: блокчейн, Інтернет речей, протокол консенсусу, смарт-контракт, децентралізація, безпека

Вступ

Інтернет речей (IoT) [1] – мережа фізичних об'єктів, які мають вбудовані технології, що дозволяють здійснювати взаємодію з зовнішнім середовищем, передавати відомості про свій стан і приймати дані ззовні. IoT-пристрої використовуються у різних сферах: від розумних будинків і виробництва до медицини та критичної інфраструктури. Зі зростанням масштабів IoT-мереж зростає і кількість векторів атак: централізовані підходи до зберігання та обробки даних створюють ризики витоку, підміни та втрати даних у разі компрометації одного з вузлів або серверів. Традиційні засоби забезпечення безпеки часто є недостатньо ефективними в умовах обмежених обчислювальних ресурсів IoT-пристроїв.

Одним з перспективних напрямів вирішення цих проблем є інтеграція технології блокчейн, яка завдяки своїй децентралізованій природі, криптографічному захисту даних та стійкості до маніпуляцій забезпечує високий рівень довіри між вузлами. Проте застосування блокчейну у сфері IoT вимагає врахування доступних обчислювальних і мережевих ресурсів, а також визначення відповідних типів блокчейн-систем і механізмів консенсусу. Ціллю цього дослідження є розробка моделі інтеграції блокчейну для безпечного децентралізованого управління даними пристроїв Інтернету речей.

1. Інтернет речей: загрози та вимоги до безпеки

Захист Інтернету речей вимагає врахування як унікальних особливостей самих пристроїв (їх обмежених ресурсів, розподіленості, відсутності уніфікованих стандартів), так і загроз, що випливають із централізованої архітектури, на якій зазвичай базуються IoT-системи. Централізоване управління, залежність від хмарних сервісів і відсутність прозорості призводять до низки вразливостей, які можуть бути послаблені за допомогою впровадження комплексної моделі безпеки.

1.1. Загрози безпеці в IoT

На відміну від традиційних IT-систем, пристрої IoT характеризуються обмеженими обчислювальними ресурсами, енергонезалежністю, широким розгортанням і значною різнорідністю. Це створює цілий спектр загроз [2]:

- **Несанкціонований доступ:** через слабку автентифікацію, використання стандартних паролів або невиправлені вразливості зловмисники можуть отримати доступ до системи, керувати її налаштуваннями. Скомпрометовані пристрої можуть стати частиною мережі ботнету і використовуватись для атак на інші сервіси. Наприклад, одна з відомих мереж ботнету Mirai складалася з пристроїв IoT, які мали облікові дані за замовчуванням [3].
- **Атаки типу «відмова в обслуговуванні» (DDoS):** обмеженість обчислювальних ресурсів IoT-пристроїв дозволяє легко вивести їх з ладу. До того ж, враховуючи централізовану природу Інтернету речей, можна атакувати лише точку контролю, щоб паралізувати всю систему.
- **Маніпуляція даними:** використання слабких протоколів передачі даних або недостатнє шифрування надає зловмисникам можливість перехоплювати, змінювати або фальсифікувати дані, що передаються між пристроями. Особливо критичною ця загроза стає при обробці інформації з обмеженим доступом.
- **Фізичні атаки:** з огляду на відкритий доступ до пристроїв порушники можуть маніпулювати компонентами системи. Видалення або мо-

[a]vikyur-ipt25@lll.kpi.ua

дифікація датчиків, змінення функціональності пристроїв можуть спричинити хибні тривоги чи перебої в критичних процесах.

1.2. Вимоги до безпеки IoT-систем

Для ефективного захисту IoT-інфраструктури необхідне впровадження багаторівневого підходу до безпеки. Відповідно до рекомендацій ENISA [4] та враховуючи виклики середовищ Інтернету речей, можна сформувати такі базові вимоги:

- **Автентифікація та авторизація пристроїв:** забезпечення достовірності джерел даних і взаємодіючих пристроїв. Важливо контролювати, що кожен пристрій може робити, щоб уникнути небажаних дій.
- **Шифрування даних:** всі дані, які передаються між пристроями та інфраструктурою, повинні бути зашифровані. Рекомендується використовувати AES (Advanced Encryption Standard) та інші перевірені алгоритми для захисту даних.
- **Захищене завантаження та оновлення ПЗ:** пристрої повинні завантажувати тільки перевірене програмне забезпечення. Оновлення мають проходити контроль на предмет цілісності та автентичності [2].
- **Безпечне управління життєвим циклом:** повинна забезпечуватись підтримка пристроїв протягом усього життєвого циклу, включаючи оновлення безпеки, моніторинг вразливостей та ізоляцію скомпрометованих компонент.
- **Дотримання принципів GDPR [5]:** персональні дані мають використовуватися чесно і прозоро. Важливо обмежити їх обробку та слідкувати за тим, щоб інформація не використовувалася не за призначенням.

2. Блокчейн і його переваги

Блокчейн – це децентралізований розподілений реєстр, який дозволяє здійснювати безпечні та прозорі транзакції без посередників [6]. Його архітектура унеможливлює змінення даних після запису і забезпечує довіру між сторонами без необхідності централізованого управління. Блокчейн вважається перспективною технологією для забезпечення цілісності, надійності та безпеки в різних сферах, зокрема фінансах, логістиці, управлінні цифровими правами тощо.

2.1. Типи блокчейну та протоколи консенсусу

Залежно від рівня доступу та участі у валідації транзакцій, блокчейни поділяються на [6]:

- **Публічні блокчейни** – відкриті для всіх користувачів мережі, забезпечуючи їх повну анонімність. Характеризуються високим рівнем децентралізації, але повільними транзакціями і високим енергоспоживанням.
- **Приватні блокчейни** – доступ обмежений лише певній групі користувачів, яку визначає контрольована організація. Забезпечують вищу швидкодію та контроль доступу, але менш прозорі.
- **Консорціумні блокчейни** – гібрид публічного та приватного блокчейнів, де група організацій об'єднуються для прозорого та ефективного обміну даними. Вони забезпечують баланс між децентралізацією та контролем, дозволяючи учасникам спільно ухвалювати рішення щодо перевірки транзакцій.

Протоколи консенсусу визначають, як учасники мережі погоджуються щодо запису нових блоків. Від їх дизайну залежить як безпека системи, так і її продуктивність:

- **Proof of Work (PoW):** базується на розв'язанні складних криптографічних задач. Має високий рівень безпеки, але потребує значних обчислювальних ресурсів.
- **Proof of Stake (PoS):** вибір вузла для додавання нового блоку залежить від кількості токенів, якими володіє учасник. Менш енерговитратний, але схильний до централізації.
- **Delegated Proof of Stake (DPoS):** PoS з використанням системи голосування, де учасники передають право генерації блоків делегатам. Забезпечує швидку обробку транзакцій та високу масштабованість.
- **Practical Byzantine Fault Tolerance (PBFT):** побудований на голосуванні між вузлами. Забезпечує узгодженість навіть за наявності недоброчесних учасників ($< 1/3$). Ефективний та швидкий, але тільки для невеликих систем через зростаючу навантаженість на мережу.
- **Proof of Authority (PoA):** консенсус, в якому транзакції підтверджують авторитетні вузли. Має високу пропускну здатність та придатний для корпоративних і регульованих середовищ.
- **Proof of Elapsed Time (PoET):** заснований на випадкових таймерах, де право на додавання нового блоку отримує вузол, чий таймер закінчиться швидше. Виконується в Trusted Execution Environment (TEE) та потребує високої довіри до учасників.

У таблиці 1 наведено порівняння описаних протоколів консенсусу [7].

2.2. Переваги блокчейну для забезпечення безпеки

Блокчейн пропонує низку механізмів, які роблять його надійним інструментом для забезпечення інформаційної безпеки [8]:

- **Незмінність даних:** після того як дані записано в блокчейн, їх не можна змінити без згоди мережі. Це забезпечує цілісність інформації і виключає можливість несанкціонованої модифікації.
- **Децентралізація:** усувається необхідність у центральному органі управління, що зменшує вразливість до атак на єдину точку відмови та

Таблиця 1. Порівняння протоколів консенсусу

Консенсус	**Доступність**	**Децентралізація**	**Масштабованість**	**Пропускна здатність**	**Затримка**	**Обчислювальне навантаження**	**Мережеве навантаження**	**Витрати на сховище**
PoW	Публічний	Висока	Висока	Низька	Висока	Високе	Низьке	Високі
PoS	Публічний	Висока	Висока	Низька	Середня	Низьке	Низьке	Високі
DPoS	Публічний	Середня	Висока	Висока	Середня	Середнє	Невідомо	Високі
PBFT	Приватний	Середня	Низька	Висока	Низька	Низьке	Високе	Високі
PoA	Публічний	Висока	Висока	Низька	Середня	Високе	Низьке	Високі
PoET	Приватний	Середня	Висока	Висока	Низька	Низьке	Низьке	Високі

знижує ризик зловживання повноваженнями. Кожен вузол мережі має копію блокчейну, що підвищує стійкість до атак.

- **Аудит і простежуваність:** кожна транзакція має мітку часу та ідентифікатор джерела, що спрощує аудит та виявлення аномальної активності. Це особливо важливо для критичних інфраструктур, де контроль над змінами є обов'язковим.
- **Криптографічний захист:** цифрові підписи, геш-функції та асиметричне шифрування гарантують автентичність джерел і цілісність даних.
- **Контроль доступу:** у приватних та консорціумних блокчейнах є можливість чітко визначати права доступу до інформації та обмежувати повноваження.
- **Інтеграція смарт-контрактів:** дозволяє автоматизувати взаємодії між вузлами без участі людини. Смарт-контракти виконуються лише за заздалегідь визначених умов, що зменшує ризик помилок та зловживань.

3. Використання блокчейну в IoT

Інтеграція блокчейн-технологій у системи Інтернету речей (IoT) відкриває нові можливості для безпечного, децентралізованого та прозорого управління даними. Завдяки блокчейну IoT-системи можуть функціонувати без центрального координатора. Кожен пристрій або вузол мережі може взаємодіяти з іншими через розподілений реєстр, уникаючи залежності від єдиної точки відмови. Це підвищує надійність системи, забезпечує безперервність роботи і зменшує ризик внутрішніх маніпуляцій із даними.

Смарт-контракти, які є самовиконуваними програмами, записаними у блокчейн, дозволяють автоматизувати взаємодію між IoT-пристроями. Наприклад, сенсор якості повітря фіксує перевищення рівня забруднення, після чого смарт-контракт у блокчейні автоматично надсилає команду пристроям у мережі, зокрема системам очищення чи вентиляції, активуватись. Усі дії фіксуються в блокчейні, що забезпечує прозорість, неможливість підробки та автономність без потреби у централізованому керуванні або зовнішньому сервері.

Серед прикладів інтеграції блокчейну в IoT можна виділити платформи `IoTeX, Helium, Grid+` та `VeChain`, які демонструють застосування децентралізованих підходів у сферах безпеки, енергетики та логістики [9].

Потенційні виклики та обмеження

Попри численні переваги, впровадження блокчейну в IoT стикається з низкою труднощів:

- **Обмежені ресурси пристроїв:** більшість IoT-платформ мають обмежені обчислювальні можливості, пам'ять та енергоспоживання, що ускладнює використання традиційних блокчейнів.
- **Масштабованість:** зі зростанням кількості пристроїв збільшується обсяг транзакцій, що вимагає адаптивних консенсус-алгоритмів та інфраструктури з високою пропускною здатністю.
- **Затримки:** системи Інтернету речей часто вимагають обробки інформації та прийняття рішень у режимі реального часу. Тому навіть короткі затримки в обробці транзакцій можуть бути неприйнятними.
- **Інтероперабельність:** IoT-пристрої можуть використовувати різні протоколи зв'язку. За-

безпечення їх взаємодії через блокчейн-мережі потребує деяких зусиль [8].

4. Концепція моделі

Основною метою цієї роботи є побудова безпечної децентралізованої моделі управління даними в середовищі Інтернету речей. З урахуванням наявних загроз, обмежень пристроїв та вимог до довіри між вузлами, було запропоновано архітектуру, що використовує блокчейн з децентралізованим контролем доступу та узгодженням дій між пристроями.

Для побудови моделі було обрано *консорціумний блокчейн*, у якому обмежене коло учасників (організацій або пристроїв) мають право брати участь у валідації транзакцій. Для досягнення консенсусу застосовується *PBFT*, який забезпечує узгодженість між вузлами навіть за наявності недовірених або скомпрометованих учасників (до 1/3).

Це рішення забезпечує:

1. Високу швидкість узгодження блоків;
2. Енергоефективність, критичну для IoT;
3. Надійність у розподіленому середовищі зі статично відомими вузлами.

4.1. Архітектура моделі

1. **IoT-пристрої** (сенсори, виконавчі механізми) – генерують дані і взаємодіють із блокчейном через шлюзи;
2. **Edge-шлюзи** [10] – агрегують дані, підписують і надсилають транзакції, беруть участь у PBFT;
3. **Смарт-контракти** – реалізують політику доступу, логіку взаємодії пристроїв і правила реагування на події.

Усі вузли мають заздалегідь визначені сертифікати або ключі автентифікації.

4.2. Фрагмент реалізації

Смарт-контракт нижче призначений для погодження команди між IoT-пристроями за принципом PBFT. Використано мову програмування Solidity для наочності.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract PBFTCommandApproval {
mapping(bytes32 => address[])
public commandVotes;
uint public totalMembers;
mapping(address => bool)
public consortiumMembers;
event CommandApproved
(bytes32 indexed commandId);
constructor(address[] memory members) {
  for (uint i=0; i<members.length; i++){
   consortiumMembers[members[i]]=true;}
   totalMembers = members.length;}

function voteCommand(bytes32 commandId)
  public {
   require(consortiumMembers[msg.sender],
   "Not a consortium member");
   address[] storage
   voters = commandVotes[commandId];
   for (uint i=0; i<voters.length; i++){
     require(voters[i] != msg.sender,
     "Already voted");}
   voters.push(msg.sender);
   if (voters.length>totalMembers*2/3){
     emit CommandApproved(commandId);}}}
```

4.3. Обґрунтування доцільності моделі

1. Консорціумна архітектура знижує потребу в анонімності, водночас підвищуючи контрольованість і надійність;
2. Протокол PBFT забезпечує високу узгодженість і стійкість до наявності певної кількості скомпрометованих пристроїв;
3. Смарт-контракти забезпечують гнучке управління доступом і реакцією на події;
4. Відсутність високих енергетичних витрат у процесі підтвердження транзакцій робить модель придатною для пристроїв із обмеженими ресурсами.

Висновки

У межах дослідження було проаналізовано проблеми безпеки, притаманні IoT-системам, та обґрунтовано доцільність використання блокчейну як основи для побудови децентралізованої моделі управління даними. Блокчейн забезпечує нову парадигму управління інформацією, уникаючи централізованого контролю. Його тип і механізм консенсусу слід обирати з урахуванням вимог до продуктивності, рівня довіри та ресурсних обмежень середовища застосування. Запропонована архітектура базується на консорціумному блокчейні з протоколом консенсусу PBFT, що забезпечує цілісність, контрольований доступ та автоматизовану взаємодію між пристроями. Включення смарт-контрактів дозволяє формалізувати політики

безпеки та погодження дій у розподіленому середовищі. Описана концепція придатна для створення безпечної системи управління даними IoT.

Перелік використаних джерел

1. *IT-Enterprise*. Internet of Things, IoT. — URL: https://www.it.ua/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iot.
2. *Aditya K. S.*, *Mohan S. G.* Internet of Things Security. — 2024. — DOI: 10.1201/9781003460367-4.
3. *Statt N.* How an army of vulnerable gadgets took down the web today. — 10/21/2016. — URL: https://www.theverge.com/2016/10/21/13362354/dyn-dns-ddos-attack-cause-outage-status-explained.
4. *ENISA*. Baseline Security Recommendations for IoT. — 2017. — DOI: 10.2824/03228. — URL: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.
5. *Парламент Є. С.* Загальний регламент про захист даних (GDPR). — URL: https://gdpr-text.com/uk/.
6. *Dave C.* Security Challenges with Blockchain. — 2024.
7. *Salimitari M.*, *Chatterjee M.*, *Fallah Y. P.* A survey on consensus methods in blockchain for resource-constrained IoT networks // Internet of Things. — 2020. — Т. 11. — С. 100212. — ISSN 2542-6605. — DOI: https://doi.org/10.1016/j.iot.2020.100212. — URL: https://www.sciencedirect.com/science/article/pii/S2542660520300482.
8. Exploring Integration of the Blockchain and Internet of Things (IoT) Computing for Secure and Decentralized Data Management / T. K. Vashishth, V. Sharma, K. K. Sharma, B. Kumar, S. Chaudhary, R. Panwar. — 2024. — DOI: 10.1201/9781003460367-10.
9. *Singh Y.* Blockchain in IoT Use Cases. — URL: https://ideausher.com/blog/blockchain-in-iot-use-cases/.
10. *Yin Z.* Edge gateways: Their role and importance in edge computing. — URL: https://stlpartners.com/articles/edge-computing/edge-gateways-their-role-and-importance/.