УДК 004.72

БЕЗПЕКА IOT СИСТЕМ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Вергун А.І., Курдеча В.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: xhc044x@gmail.com

IOT SYSTEMS SECURITY USING BLOCKCHAIN TECHNOLOGY

Currently, the Internet of things is still a lot of problems related to safety and scalability. All these problems are solved with huge losses on the scale and the acquisition of certificates is also urgent security problem associated with centralization devices Internet of things. Solving these problems is possible through the application of technology for decentralized blokcheynu.

Інтернет речей (IoT) швидко увійшов в життя мільярдів людей по всьому світу. Однак зростання кількості підключених пристроїв веде до збільшення ризиків безпеки: від заподіяння фізичної шкоди людям до простоїв і пошкодження обладнання. Оскільки велика кількість об'єктів і систем IoT вже піддавалися нападу і було завдано значний збиток, забезпечення їх захисту виходить на перший план.

Безпека IoT систем можна розділити на чотири основні шари [1]: фізичний рівень захисту, мережевий рівень захисту, рівень захисту хмарного обчислення та программного коду IoT системи, рівень захисту додатку.

Рис. 1. Архітектура рівнів безпеки IoT системи

Основними невирішеними загрозами є:

- Атаки Сивіли (порушення конфіденційності, ненадійна передача данних);
- Аутентифікація та безпечне спілкування (Порушення конфіденційності);
- Проблеми розподілу ключів довіри та розподілення адрес для пристроїв;
- Проблема відстеження правопорушень.

Для вирішення деяких з обговорених загроз є відмінні бібліотеки з відкритим вихідним кодом, які виконують шифрування навіть в пристроях IoT з обмеженими обчислювальними ресурсами. Всі взаємодії вимагають надійної перевірки автентичності і взаємної довіри, отже економити на сертифікатах не можна. У більшості випадків сертифікатами можна легко керувати віддалено (OTA) за допомогою стандартних протоколів, таких як SCEP, EST і OCSP. Завдяки надійному центру сертифікації, який надає можливість обробляти сертифікати, ключі та облікові дані, фактичну перевірку справжності можна робити за допомогою потужних стандартів TLS і DTLS. За допомогою TLS/DTLS вирішується проблема підслуховування в мережі, дві кінцеві точки можуть обмінюватися ключами шифрування або отримувати їх для обміну даними, які неможливо розшифрувати іншим пристроям. Однак проблему досі залишається проблема вірогідності що треті

сторони та центри сертифікації можуть бути зламані або скомпрометовані.

Вирішення цих проблем можна забезпечити за допомогою технології децентралізованого блокчейну. Блокчейн є децентралізованим, розподіленим, спільним та незмінним базою даних, який зберігає реєстр активів та транзакцій через P2P мережу. Блокчейн використовує хешування SHA-256 для забезпечення сильного криптографічного підтвердження для автентифікації та цілісності даних. По суті, дані блоку містять список всіх транзакцій та хешу попереднього блоку. Блокчейн має повну історію всіх транзакцій і забезпечує транскордонну глобальну розподілену довіру.

В представленій нижче архітектурі мережі Інтернету речей з застосуванням технології Блокчейн [2] можна виділити декілька основних компонентів з яких вона складається:

- Блокчейн вузол (Node) - записує всі транзакційні блоки. Містить інформацію про керування пристрою користувачами, іншим пристроєм, керуванням, які виконує адміністратор та білінгом.

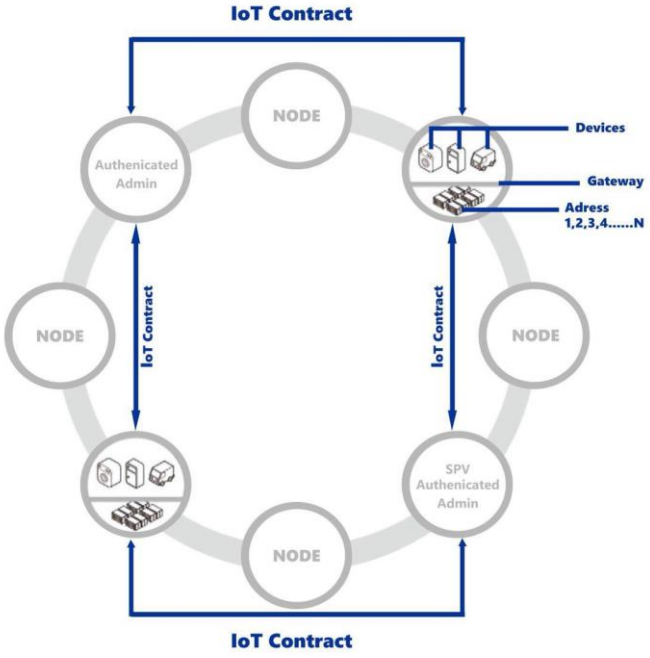

Рис. 2. Архітектура мережі Інтернету речей на базі технології Блокчейн

- Адміністратор (Admin) - особа, яка реєструє користувачів, шлюзи та пристрої в блокчейні та надає доступ для них. Ці налаштування безпечно зберігаються у вузлі блокчейна та передаються іншим користувачам, шлюзам та пристроям через мережу. Тому кожен користувач та пристрій підтримує останні пов'язані з ними налаштування.

- Шлюз (Gateway) - як такий, пристрій використовується для управління пристроями або датчиками. Він може аналізувати деталі контракту IoT, а потім передавати до пристроїв або датчиків. Надає кожному пристрою або датчику індивідуальну адресу.

- Пристрій (Device) - як такий, пристрій, підключений до шлюзу.

Блокчейн має 160-розрядний адресний простір, на відміну від адресного простору IPv6, який має 128-розрядний адресний простір. Адреса блоку становить 20 байт або 160-бітовий хеш відкритого ключа, створеного ECDSA (алгоритм цифрового підпису еліптичного кривизни). З 160-бітною адресою blockchain може створювати та розподіляти адреси в автономному режимі приблизно на 1,46 * 1048 IoT пристроїв. 21 Вірогідність зіткнення адрес становить приблизно 1048, що вважається достатньо захищеною, щоб забезпечити GUID (глобальний унікальний ідентифікатор), який не вимагає перевірки реєстрації або унікальності під час призначення та розподілу адреси на пристрої IoT.

Надійні треті сторони або централізовані органи та служби можуть бути порушені, скомпрометовані або зламані. Для того щоб забезпечити можливість єдиної та багатопартійної автентифікації на пристрої IoT за допомогою технології блокчейн можна надавати децентралізовані правила і логіку автентифікації. Крім того, smart-контракти [2][3] можуть забезпечити більш ефективні правила доступу до авторизації для підключених пристроїв IoT з меншою складністю порівняно з традиційними протоколами авторизації, такими як RBAC, OAuth 2.0, OpenID, OMA DM і LWM2M. Ці протоколи сьогодні широко використовуються для ідентифікації, авторизації та керування пристроєм IoT. Більш того, конфіденційність даних також може бути забезпечена шляхом використання smart-контрактів [2][3], які встановлюють правила доступу, умови та час для того, щоб певна особа або група користувачів або машин могли володіти, контролювати або мати доступ до даних.

Рис. 3. Як працюють смарт-контракти

За допомогою технології блокчейну, управління і розподіл ключів довіри повністю усуваються, оскільки кожен пристрій IoT матиме власну унікальний ідентифікатор GUID та асиметричну ключову клавішу після встановлення та підключення до мережі. Це також призведе до значного спрощення інших протоколів захисту, таких як DTLS та TLS.

Висновок. Отже саме за домогою технології блокчейн можна вирішити проблеми конфіденційності передачі данних, проблему автентифікації, розподілення ключів довіри серед IoT пристроїв, проблему сертифікації та зниження коштів на неї шляхом її виключення, проблему відстеження правопорушень шляхом відстеження транзакцій.

Література

1. M.A. Khan, K. Salah, IoT security: Review, blockchain solutions, and open challenges, Future Generation Computer Systems (2017).
2. Why blockchain and iot are best friends from IBM blog https://www.ibm.com/blogs/blockchain/2018/01/why-blockchain-and-iot-are-best-friends/
3. Internet of Things: Security challenges for next generation networks http://ieeexplore.ieee.org/document/7542301/