

ВИКОРИСТАННЯ ЗАСОБІВ БЛОКЧЕЙН ТЕХНОЛОГІЙ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ ПЕРЕДАЧІ ДАНИХ МІЖ ПРИСТРОЯМИ ІНТЕРНЕТУ РЕЧЕЙ

Вступ. За останні роки спостерігається стрімке збільшення кількості пристроїв Інтернету речей (IoT), що призводить до значного обсягу конфіденційних даних, які генеруються та передаються через мережу. Незважаючи на поширення систем IoT у різних галузях, проблема безпеки IoT залишається актуальною і вимагає подальших досліджень. Забезпечення безпечного обміну даними між пристроями Інтернету залишається актуальною проблемою, адже на даному етапі розвитку технології немає засобів з гарантованим рівнем захисту.

Специфікація проблеми. Проблема безпечної передачі даних між пристроями Інтернету Речей (IoT) полягає у викликах, пов'язаних з захистом конфіденційності, цілісності та доступності даних, які пересилаються між цими пристроями. Оскільки мережа IoT може включати в себе велику кількість різноманітних пристроїв, таких як датчики, пристрої та інші девайси з вбудованими обчислювальними можливостями, інформація, що пересилається між ними, стає предметом загроз безпеки. Розв'язання цієї проблеми вимагає впровадження комплексних заходів забезпечення безпеки, які включають шифрування даних, аутентифікацію та авторизацію, моніторинг та виявлення вторгнень, а також ретельне проектування архітектури мережі IoT з урахуванням аспектів безпеки[1].

Основний матеріал. Технологія Blockchain має багато переваг для підвищення безпеки при передачі даних між пристроями Інтернету речей (IoT). За допомогою децентралізованого та захищеного від несанкціонованого втручання реєстру, Blockchain забезпечує цілісність та автентичність ідентифікаторів пристроїв IoT, що зменшує ризик підробки та несанкціонованого доступу, підвищуючи загальні заходи безпеки. Крім того, Blockchain забезпечує стійку систему ідентифікації пристроїв, де унікальні ідентифікаційні дані можна безпечно зберігати, усуваючи потребу в централізованих системах керування ідентифікаційними даними і зменшуючи ризик маніпулювання або дублювання особистих даних.

Блокчейн забезпечує незмінність даних шляхом створення ланцюжка блоків, де кожен блок містить унікальний хеш попереднього блоку. Це означає, що будь-яка спроба змінити дані у блокчейні буде автоматично виявлена, оскільки буде порушено цілісність ланцюжка. Такий механізм гарантує, що дані, що передаються між пристроями, залишаються незмінними та відповідають очікуваному формату.

Крім того, Blockchain сприяє точним механізмам контролю доступу через використання смарт-контрактів для зберігання прав доступу, що гарантує, що лише авторизовані пристрої можуть взаємодіяти з певними ресурсами або виконувати певні дії, запобігаючи несанкціонованим діям. Розподілена природа Blockchain гарантує реплікацію даних автентифікації на кількох вузлах, що робить систему надійною проти окремих точок збою або зловмисних атак.

Блокчейн може виступати як безпечний канал для передачі ключів шифрування між пристроями IoT. Використання публічних та приватних ключів дозволяє забезпечити безпеку та конфіденційність даних, які передаються між пристроями. Публічні ключі використовуються для шифрування даних перед їх відправленням, тоді як приватні ключі використовуються для їх розшифрування. Використання блокчейну забезпечує автентичність та незмінність публічних ключів, що зробить обмін ключами більш

безпечним та надійним. Такий підхід допомагає уникнути атак на дані та забезпечує конфіденційність інформації в мережі IoT[2].

Застосування технології Blockchain для безпечнішої передачі даних в IoT має безліч переваг, включаючи стійку ідентифікацію пристроїв, встановлення довіри, детальний контроль доступу, можливості аудиту, розширення прав і можливостей користувачів та підзвітність.

Висновки. Було окреслено методи та засоби для підвищення безпеки при передачі даних між пристроями Інтернету речей використовуючи блокчейн технологію.

Список використаних джерел

1. Fu, H., Wang, P., Li, H., Zhan, Y., Chen, J., Du, X., 2021. A Multiple-Blockchains based Service Monitoring Framework in Edge-Cloud Computing. In: 2021 IEEE 23rd Int. Conf. on High Performance Comp. & Comm.; 7th Int. Conf. on Data Science & Systems; 19th Int. Conf. on Smart City; 7th Int. Conf. on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys), IEEE, pp. 2111-2117
2. Cha, S.C., Tsai, T.Y., Peng, W.C., Huang, T.C., Hsu, T.Y., 2017. Privacy-aware and blockchain connected gateways for users to access legacy IoT devices. In: 2017 IEEE 6th global conf. on consumer electronics (GCCE), IEEE, pp. 1-3.

Науковий керівник: д.т.н., проф. Цмоць І.Г.

Попов Д. С.

студент

*Київський національний економічний
університет імені Вадима Гетьмана
dmitrii.p1711@gmail.com*

РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ КРИПТОІНВЕСТИЦІЙ

Для ефективного управління криптоінвестиціями необхідно ретельно дослідити сучасний стан криптовалютного ринку та потреб у розвитку інформаційної системи. Це включає вивчення основних криптовалют, їхніх обсягів торгів, волатильності та різноманітних стратегій інвестування. Потреба у розробці інформаційної системи виникає з ростом кількості криптоінвесторів, які шукають зручні та ефективні інструменти для управління своїми портфелями.

Проектування та розробка інформаційної системи для забезпечення безпечних та зручних криптоінвестиційних операцій включає в себе цілий ряд стадій та етапів, що мають бути підтримані відповідними методами та технологіями. Важливим етапом є забезпечення безпеки системи. Це включає захист від кібератак, шифрування даних та аутентифікацію користувачів. Розробники повинні врахувати всі можливі загрози безпеці та прийняти відповідні заходи для їхнього усунення.

Впровадження технологій блокчейну та смарт-контрактів в інформаційну систему дозволяє створити систему, що забезпечує прозорість та автоматизацію криптоінвестиційних операцій. Блокчейн зберігає дані безпечно та недоступно для змін, тоді як смарт-контракти автоматизують виконання угод.