УДК 004.773
DOI: 10.31673/2409-7292.2020.012530

Гайдур Г.І., Гай Д.О., Алексенко С.О.

МЕТОДИКА ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ІНТЕРНЕТ РЕЧЕЙ НА БАЗІ ТЕХНОЛОГІЙ БЛОКЧЕЙНА

В статі розглянуто та запропоновано спосіб використання технології блокчейн в Інтернет-речах. Проведено дослідження що дозволяють виявити факти щодо використання технології блокчейн для захисту Інтернет-речей. Виявлено позитивні наслідки впровадження даної технології в бізнес-процесах. Досліджено, що технологія блокчейн має значний потенціал застосування у різних сферах діяльності, однак найбільш перспективою сферою застосування цієї технології є в Інтернет речах і кіберфізичних системах. Технологія блокчейн пропонує вирішення проблеми безпеки і конфіденційності у середовищі Інтернет речей, забезпечуючи новий обчислювальний рівень, де дані можуть бути безпечно оброблені та проаналізовані, залишаючись приватним. Розкрито потенційні переваги та виділено проблеми, які потрібно вирішити для ефективного використання цієї технології у середовищі Інтернет речей.

Ключові слова: технологія, блокчейн, Інтернет речі (IoT), безпека, конфіденційність, цілісність, аутентифікація.

Вступ

Останнім часом блокчейн широко відомий як децентралізована і захищена від несанкціонованого доступу технологія обліку, яка підтримується групою користувачів з певною метою. Він показує записи всіх транзакцій, наприклад фінансових угод, інформації про ланцюжок поставок і авторські права. Спільна робота пристроїв вважається «речами», за допомогою яких дані довкілля сприймаються і збираються для цілей управління центрами обробки даних або пропозиціями послуг [1, с.7]. Деякі з додатків IoT представлені бездротовими сенсорними мережами, автомобільними мережами, електронним охороною здоров'я і хмарними службами зберігання. В якості нового технічного предмета IoT з'єднує два світи, фізичний і інформаційний, пропонуючи широкий спектр веб-сервісів. Тому попит на IoT з кожним роком зростає та більш орієнтуйтеся на технології Smart (технології мобільного зв’язку), але вона є проблемною в безпеці та конфіденційності. Пристрої IoT пов'язані в децентралізованому підході, утворючі дуже складне для використання стандартного вже існуючого прийому в спілкуванні між вузлами IoT. Технологія блокчейн забезпечує децентралізацію та розповсюджування публічних записів та зберігання даних блоків, які обробляються і підтверджені в мережі IoT. Дані, що зберігаються в публічних записах керуються автоматично за допомогою "machine-to-machine". Блокчейн - це технологія, де транзакції, випущені у вигляді блоку створюються в середині вузлів IoT. Блоки пов'язані між собою і кожен пристрій має попередню адресу пристрою. Блокчейн та IoT спільно працюють в основі інтеграції IoT та Cloud (хмарному сервері). У майбутньому блокчейн зробить революцію з сумісництвом IoT.

Метою статті є визначення методів використання технологій блокчейн в сфері інтернет речей, а також наявності та змісту проблем захищеності при їх використанні.

Виклад основного матеріалу

Переваги використання блокчейну в IoT:

1. Децентралізована структура. Подібний підхід є в IoT і блокчейн. З нього вилучається централізована система і забезпечується створення децентралізованої системи. Це покращує ймовірність відмови та продуктивність загальної системи.

2. Безпека. У блокейн є створені транзакції між вузлам. Тому блокчейн дозволяє пристроям IoT спілкуватися між собою безпечним способом.

3. Ідентифікація. В IoT всі підключені пристрої однозначно ідентифікуються з унікальним ідентифікатором. Кожен блок в блокчейн також має унікальний ідентифікатор. Отже, блокчейн - це технологія, яка забезпечує однозначно визначені дані, що зберігаються в публічному записі.

4. Надійність. IoT-вузли та блокчейн мають можливість аутентифікувати інформацію передану в мережу. Дані є надійними, оскільки перевіряються до вступу в систему. Увійти можуть лише перевірені блоки блокчен.

5. Автономність. У блокчені до всіх IoT-вузлів можуть вільно спілкуватися з будь-яким вузлом в мережі без централізованої системи.

Роль блокчейну в IoT

IoT дозволяє працювати між собою для обміну своєї інформації [3, с.4]. Систему IoT на основі блокчейн можливо розділити на наступні розділи:

1. Фізичні речі. IoT надає унікальний ідентифікатор, яку при підключені можливо аутентифікувати у мережі. Маючи фізичне значення при якому він може обмінюватися даними з іншими вузлами IoT.

2. Шлюзи - це пристрої, які працюють серед фізичних речей та веб серверами, щоб переконатися, що встановлене з'єднання є безпечним для мережі.

3. Мережа використовується для управління потоком даних та знаходження найкоротший маршрут серед вузлів IoT.

4. Веб сервер використовується для зберігання та обчислення даних. Блокчейн - це ланцюжок перевірених та криптографічних блоків транзакцій, що проводяться пристроєм, підключеним до мережи. Дані блоків зберігаються в цифровому форматі, яка публічно передається та розповсюджується. Блокчейн забезпечує безпечне спілкування в мережі IoT (Рис. 1).

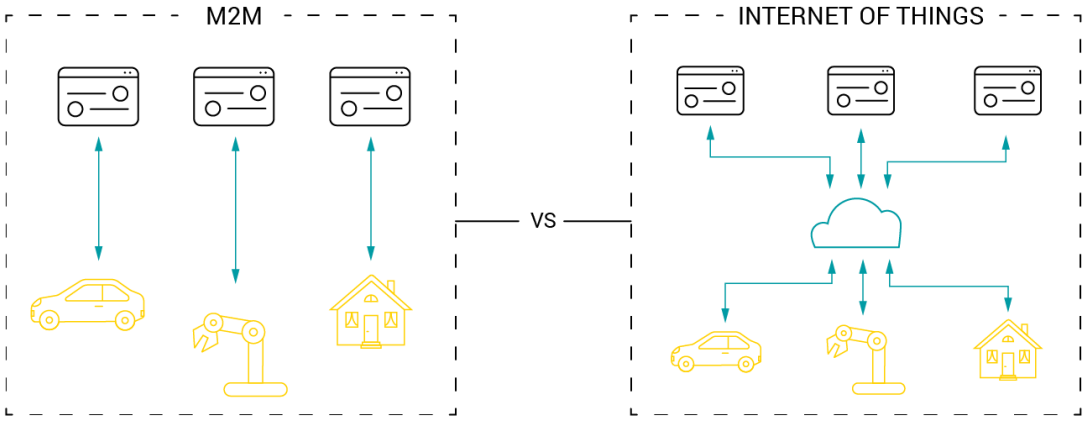

Рисунок 1 — Структура підключення пристроїв в IoT

Платформи з сумісним використанням блокчейну в IoT

Для розробки IoT використовуються наступні платформи, які пов’язані з технологію блокчейн:

а) IOTA - це нова платформа для блокчейн та IoT так зване наступне покоління блокчейна. Ця платформа надає високу цілісність даних та високу ефективність транзакцій. Висока дійсність блоків надає можливість використанням меншої кількості ресурсів. Це вирішує обмеження блокчейн [4] (Рис. 2).

б) IOTIFY. Система забезпечує інтернет-базування речей відправника та одержувача. Вона забезпечує пряме рішення для мінімізації обмежень блокчейн-зв'язку у якості технології користувацьких додатків [5] (Рис. 3).

в) XAGE. Xage використовує блокчейн у своєму продуктовому захисті, що дозволяє ефективно виявляти кібератаки, такі як компрометовані паролі чи політики. Ця технологія дозволяє захищати від несанкціонованого захисту, коли деталі, що зберігаються окремо в децентралізованій мережі, регулярно перевіряються. Якщо щось виглядає не так, це легко знаходяться. Xage стверджує, що її ієрархічна система дерев тепер дозволяє локальним оновленням блокчейн синхронізуватися з глобальними оновленнями без шкоди для безпеки.

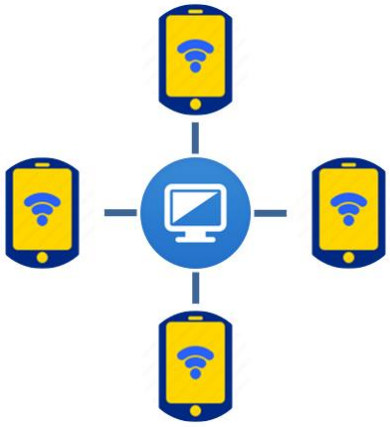

Рисунок 2 – Принципова схема IOTA

По суті, для локального оновлення слід спершу сформувати консенсус серед локальних вузлів. Потім він синхронізується з глобальним блокченчем, який відновлює локальні оновлення, змінюючи будь-які проблеми та приймаючи лише дійсні зміни. Це ієрархічне рішення гарантує, що робота може продовжуватися навіть тоді, коли локальний вузол відключений від глобальної мережі (Рис. 4).

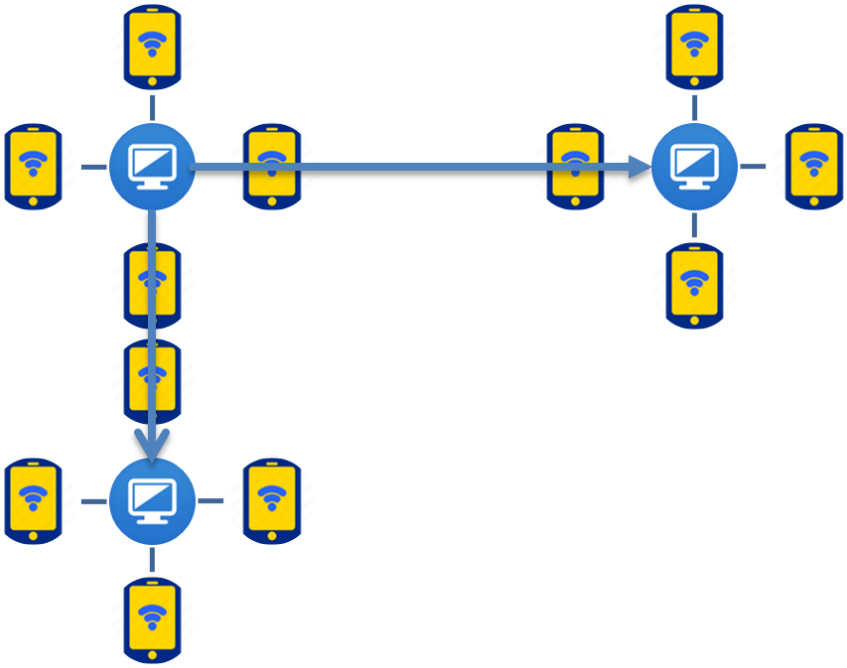

Рисунок 3 – Принципова схема IOTIFY

г) SONM. Це децентралізована платформа обчислення на основі блокчейна з використанням безпечних веб-серверів . IoT та блокчейн розширюють бізнес-можливості та відкривають нові ринки, де кожен або всі можуть спілкуватися в реальному часі з аутентифікацією та безпекою при децентралізованому підході. Інтеграція цих нових технологій змінить сучасний світ, де пристрої будуть спілкуватися без людей на різних етапах. Мета проекту - отримати захищені дані в потрібному місці, у правильному форматі, в режимі реального часу. Блокчейн може бути використаний для відстеження мільярдів

пов'язаних інтернет речей, координації цих речей, що дозволяє обробляти транзакції, вирішувати або усунути збої та створювати гнучку екосистему для запуску фізичних речей на ній. Методи хешування використовуються в блоках даних блокчейн для створення конфіденційності інформації для користувачів[6] (Рис. 5).

Рисунок 4 – Принципова схема XAGE

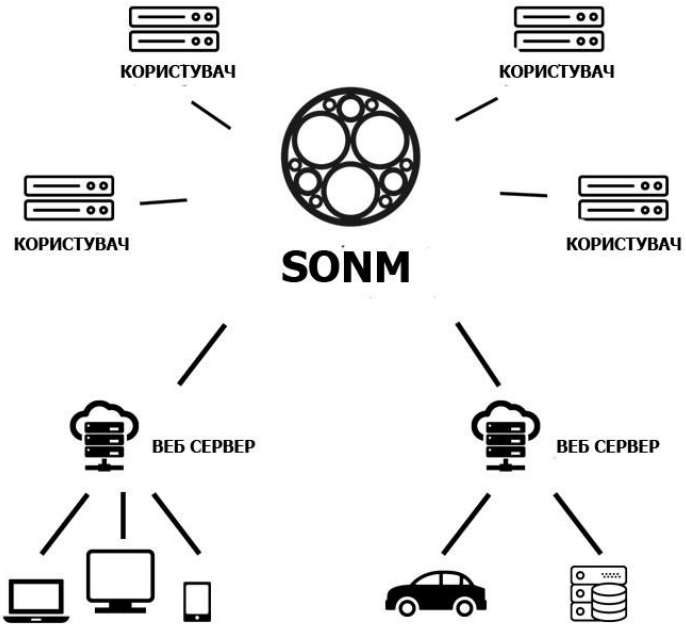

Рисунок 5 – Принципова схема SONM

Безпека та конфіденційність в IoT

Системи IoT з високим рівнем повсюдності і неоднорідності стикаються з різними загрозами безпеці та конфіденційності. Щоб гарантувати функціональність системи і досягти повної взаємодії користувачів, необхідно вказати питання безпеки і проблеми конфіденційності в IoT. Питання безпеки в основному включають в себе конфіденційність,

цілісність і аутентифікацію. Взагалі кажучи, конфіденційність гарантує, що вміст даних не буде розкрито. Цілісність гарантує, що пакети даних не будуть змінені під час передачі і запобігти доступу до системи неавторизованих користувачам. Проблеми конфіденційності виникають через те, що пакети даних, що передаються від користувачів в інфраструктури IoT, можуть містити конфіденційну інформацію (наприклад, особистість, місце розташування, траєкторію, звіт, запит). Оскільки інформація тісно пов'язана з конфіденційністю користувача, її витік може призвести до атак на користувача. Тому заходи забезпечення конфіденційності повинні забезпечуватися системами IoT. Багато механізмів захисту було запропоновані в різних сценаріях IoT. Ці запропоновані механізми спрямовані на вирішення означених проблем безпеки, оскільки системні вимоги і моделі безпеки розрізняються для різних додатків. Подання цих аспектів допоможе зрозуміти проблеми безпеки і конфіденційності в системах IoT і придумати більш підходящі механізми захисту. Тому в основному питання безпеки складаються з трьох аспектів: конфіденційність, цілісність та аутентифікація. Розглянемо проблеми безпеки та відповідні методи атаки в різних сценаріях IoT.

Конфіденційність даних означає що вміст даних під час передачі не просочується до будь-якого користувача. Вміст даних в системах IoT зазвичай відноситься до вмісту простого тексту, що генерується користувачем до того, як він виконує будь-які складні операції, такі як шифрування та збурення. Взагалі кажучи, конфіденційність захищена шифруванням для захисту від можливої атаки. Щоб захистити вміст даних від супротивника, ми спочатку змоделюємо напад та здатність яку отримує зловмисник. Припустимо, що супротивник А - це ймовірний злоякісний користувач який може запускати чотири типи атак:

• Атака лише для шифротексту. Найнижчий рівень атаки, який вважається найпоширенішим. У цьому випадку супротивник лише спостерігає за каналом зв'язку та шифротекстами в ньому та намагається отримати основні безперебійні тексти.

• Атака з відомим відкритим текстом. Стосується сценарію, коли зловмисник може отримати кілька пар простого тексту або шифротексту, створених під секретним ключем.

• Атака в прямому контексті. Атака є дещо руйнівнішою, ніж перші дві атаки, оскільки супротивник може отримати шифротексти для самостійного вибору просторових текстів.

• Атака вибраного шифротексту. Внутрішня атака, яка обумовлює прості тексти для самостійно вибраних шифротекстів.

Цілісність, тобто цілісність даних яка відноситься до властивості який вміст даних під час передачі не можливо змінити будь-яким користувачем. Взагалі кажучи, цілісність захищена цифровими підписами, яка гарантується неможливістю взаємодії перед зловмисником. Таким чином зловмисник може запускати три типи атак:

• Атака випадковими повідомленням. Зловмисник не може контролювати підписані повідомлення, але він може спостерігати лише за підписами, створеними підтвердженими особами на повідомленнях.

• Атака відомих повідомлень. Зловмисник має обмежений контроль над тим, які повідомлення підписуються, що означає, що противник повинен зазначати повідомлення заздалегідь незалежно від відкритого ключа підписувача та наступних підписів.

• Адаптивна атака вибраних даних. Зловмисник має повний контроль над тим, які повідомлення підписані, що означає, що противник може вибирати повідомлення після того, як він дотримується відкритого ключа підписувача та попередніх підписів.

Аутентифікація означає, що одержувач підтверджує, що отриманий пакет даних дійсно є від заявника, який споріднений заявнику. Типовою програмою є інтелектуальна домашня мережа, яка складається з центральної системи управління, зовнішнього користувача, декількох внутрішніх електричних приладів та хмарного сервера. Такий тип аутентифікації надає безліч зручних та цікавих послуг, оскільки пристрої в можуть спілкуватися, і це дозволяє користувачеві дистанційно керувати приладами, коли вони перебувають подалі ніж система. Наприклад, водонагрівач можна налаштувати перед тим, як користувач вийде з роботи. Завдяки повсюдному життю люди отримують можливість користуватися більш

сучасними домашніми послугами. У той же час, це стосується важливості аутентифікації. Уявіть, що приладами може керувати будь-яка шкідлива особа без автентифікації відправника інструкцій, усі прилади перетворяться в хаос.

Висновки

У цій статі розглянуті основні питання створення системи блокчейну в поєднанні з IoT. Встановленні головні аспекти безпеки та проблеми конфіденційності. Розглянуто основні методи атаки які можливі при використанні такої системи. Отже, використання технології блокчейна в Інтернет-речах має великий потенціал і потребує подальших досліджень. Створення такої інфраструктури є запорукою успішного впровадження інформаційних технологій в бізнес-процесах на всіх її рівнях, що дозволяє комп'ютеризувати управлінську та будь-яку іншу діяльність.

Перелік посилань

1. Blockchain Technology in Internet of Things./ [LiehuangZhu, KekeGai, MengLi,] // Springer Nature Switzerland AG – 2019.

2. Блокчейн-архітектура для Інтернету речей [Електронний ресурс] // - Режим доступу: https://www.ibm.com/blogs/research/2018/10/blockchain-internet-of-things/ (20.03.2020)

3. Blockchain та його роль в Інтернеті речей [Електронний ресурс] // - https://www.researchgate.net/publication/333294541_Blockchain_and_its_Role_in_the_Internet_of_Things_IoT (20.03.2020).

4. Documentation IOTA [Електронний ресурс] // - Режим доступу: https://docs.iota.org/ (20.03.2020).

5. Documentation IOTIFY [Електронний ресурс] // - Режим доступу: https://iotify.help/ (20.03.2020).

6. Documentation SONM [Електронний ресурс] // - Режим доступу: https://docs.sonm.com/ (20.03.2020).

Надійшла: 25.01.2020 Рецензент: д.т.н., доцент Кожухівський А.Д.