

УДК 004.02

О.В. Палка

Тернопільський національний технічний університет імені Івана Пулюя, Україна

ИНТЕГРОВАНА АРХИТЕКТУРА РОЗУМНОГО МІСТА З БЛОКЧЕЙНОМ ТА ІОТ

O.V. Palka

INTEGRATED SMART CITY ARCHITECTURE WITH BLOCKCHAIN AND IOT

Для досягнення ефективності у мережі IoT, Kim та ін. [1] ввели концепцію довірчого управління, яка широко поширена у всьому світі. Вони вважали, що інфраструктура для підтвердження автентичності та авторизації IoT буде централізована та поширена по всьому світу. Пропонується гібридна архітектура мережі розумного міста зі стратегіями блокчейну та стратегіями програмно-визначеної мережі (SDN) для подолання обмежень поточної інфраструктури мережі розумного міста.

Як складне завдання для запам'ятовування хешування паролів та інших програм, Argon2 був обраний переможцем конкурсу хешування паролів у липні 2015 року [2]. Biryukov та інші запропонували схему пам'яті на основі доведення роботи з використанням хеш-дерева Меркла над серією хеш-систем Argon2, адже він містить параметри шифрування диска та посилення для криптовалютних програм. Для тих самих членів схема доведення роботи створює дерево Меркла, а псевдовипадковим чином вибирає набір листів на основі хеш-корінь дерева як доказ обчислення.

У запропонованій моделі мережа розумного міста розділена на дві окремі групи – основну мережу та мережеву мережу – за допомогою процесу блокчейн. Основна мережа складається з вузлів з високим підрахунком і наскрізними ресурсами, тоді як граничний вузол має обмежену ємність зберігання та обчислювальну потужність. Вузли майнера відповідатимуть за будівельні блоки та перевірку підтвердження продуктивності. Кожен вузол живиться від контролера SDN, щоб досягти максимальної швидкості та безпеки, зменшити витрати на управління обладнанням та відчутти простоту розгортання в інфраструктурі розумної міської мережі. Тут використовуються можливості безпеки моделі FS-Open Security SDN [3]. У запропонованій інфраструктурі кожен крайовий вузол діє як центральний сервер для певної загальнодоступної інфраструктури для надання основних послуг та локальної реалізації. Підтримує політику доступу та гарантує для своїх зареєстрованих організацій у сховищі та допомагає зменшити затримки та зменшити пропускну здатність мережі. Розподілений статус запропонованої моделі може зробити усю систему здатною витримати і обмежити вплив атаки в будь-який момент компромісу вузла. Іншими словами, якщо вузол на краю пошкоджений, отриманий ефект слід обмежити локальною зоною.

Література

1. Taxonomic Modeling of Security Threats in Software Defined Networking. [Electronic resource] – 2016. – Access mode: <https://www.blackhat.com/docs/us-15/materials/us-15-Hizver-Taxonomic-Modeling-Of-Security-Threats-In-Software-Defined-Networking.pdf>.
2. Egalitarian Computing. [Electronic resource] – 2016. – Access mode: https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_biryukov.pdf.
3. Blockchain based Hybrid Network Architecture for the Smart City. [Electronic resource] – 2018. – Access mode: <https://iranarze.ir/wp-content/uploads/2018/09/E9290-IranArze.pdf>.