

БЛОКЧЕЙН-ТЕХНОЛОГІЇ В СИСТЕМАХ УПРАВЛІННЯ ДОСТУПОМ У РОЗУМНИХ МІСТАХ

Сучасні розумні міста базуються на інтеграції цифрових технологій у всі сфери міської інфраструктури. Автоматизовані системи контролю доступу є важливою складовою безпеки та ефективності управління міськими ресурсами [1, 2]. Проте централізовані рішення часто стикаються з проблемами кібербезпеки, збоїв у системах, високих витрат на адміністрування та ризиків витоку персональних даних. У цьому контексті блокчейн-технології пропонують революційний підхід до управління доступом, що базується на децентралізованих механізмах аутентифікації та перевірки прав доступу [3].

З метою забезпечення безпечного та ефективного обміну інформацією запропоновано модель управління доступом на основі блокчейн-технологій, яка інтегрує децентралізовані ідентифікаційні системи. Ключовим елементом цієї моделі є смарт-контракти, що автоматизують процес перевірки прав доступу та знижують необхідність у посередниках. Правила доступу до різних міських сервісів фіксуються у блокчейні, що запобігає можливості несанкціонованого втручання та підробки даних.

Архітектура системи побудована таким чином, щоб забезпечити ефективну взаємодію користувачів з міською інфраструктурою. Аутентифікація користувачів відбувається за допомогою криптографічних методів, таких як біометричні дані, цифрові сертифікати або криптографічні ключі. Це дозволяє гарантувати точну ідентифікацію особи та запобігти шахрайству. Смарт-контракти визначають права доступу до міських сервісів, формують цифрові ключі для користувачів і контролюють виконання правил. Всі операції у системі реєструються у блокчейні, що робить їх прозорими, незмінними та доступними для аудиту.

Функціонування системи включає кілька ключових процесів. Перший етап – реєстрація користувача, що відбувається шляхом аутентифікації через криптографічні методи. Після підтвердження особи користувач отримує цифровий ідентифікатор, що буде використовуватись у подальших запитах на доступ. Запити на доступ проходять через смарт-контракти, які автоматично перевіряють відповідність даних користувача встановленим правилам. Якщо всі умови виконані, користувач отримує дозвіл на вхід у певну зону або доступ до ресурсу, а всі операції записуються в блокчейн.

Обмін інформацією між блокчейном і міськими інформаційними платформами забезпечується за допомогою міжданцюгових технологій, що дозволяють синхронізувати дані між різними блокчейн-мережами та централізованими базами даних. Це забезпечує можливість інтеграції блокчейн-системи з існуючими інформаційними структурами міста, що критично важливо для масштабованості та ефективного управління цифровими ресурсами. Використання децентралізованих ідентифікаційних платформ дозволяє організувати єдину систему обліку доступу, яка може застосовуватися у різних міських службах без необхідності дублювання даних.

Важливим аспектом впровадження системи є безпека транзакцій та захист конфіденційних даних. Застосування нульових доказів знання дозволяє підтвердити особу без розкриття персональних даних, що зменшує ризики витоку інформації. Гомоморфне шифрування забезпечує можливість проведення обчислень над зашифрованими даними без необхідності їх розшифровки, що підвищує рівень захисту в системі. Автоматизована система виявлення аномальних активностей дозволяє виявляти підозрілі запити на доступ і блокувати потенційні атаки.

Перевагою запропонованої системи є її автономність та відсутність єдиної точки відмови. Децентралізована природа блокчейну гарантує стійкість до атак і зовнішніх маніпуляцій. Смарт-контракти автоматизують процеси перевірки прав доступу, що дозволяє скоротити адміністративні витрати та виключити можливість людського фактору у прийнятті рішень. Використання блокчейну у системах управління доступом дозволяє знизити ризики шахрайства, покращити безпеку міської інфраструктури та підвищити рівень цифрової довіри між користувачами та міськими сервісами.

Запропонована архітектура створює передумови для ефективного управління цифровими ресурсами в умовах розумного міста. Система здатна адаптуватися до потреб різних міських сервісів, включаючи контроль доступу до будівель, управління транспортною інфраструктурою, автоматизований доступ до комунальних послуг та захист даних у цифрових реєстрах. Інтеграція з наявними системами міського управління дозволяє впровадити блокчейн без необхідності повної заміни існуючої інфраструктури, що робить її економічно доцільною та ефективною. Використання модульного підходу до реалізації системи дозволяє підключати нові компоненти без необхідності кардинальної перебудови всієї платформи, що сприяє її довготривалому використанню та масштабованості.

Застосування штучного інтелекту у поєднанні з блокчейном дозволяє покращити механізми прогнозування безпеки, оптимізувати процеси обробки запитів та адаптувати політики доступу до змінних міських умов. Наприклад, система може автоматично аналізувати поведінку користувачів і пропонувати зміни в політиках безпеки на основі даних про реальні сценарії використання. Це дозволяє зробити систему не лише безпечною, а й гнучкою, здатною самостійно вдосконалювати механізми контролю доступу.

Таким чином, впровадження блокчейн-технологій у систему управління доступом створює ефективну, захищену та масштабовану екосистему, що відповідає сучасним викликам цифровізації розумних міст. Вона дозволяє не тільки покращити безпеку та автоматизацію, а й створити єдину децентралізовану платформу, яка може адаптуватися до різноманітних завдань міської інфраструктури.

Висновок. Таким чином впровадження блокчейн-технологій у системи управління доступом у розумних містах дозволяє кардинально змінити підхід до безпеки та цифрової ідентифікації. Децентралізовані реєстри надають можливість ефективного управління правами доступу без необхідності централізованого контролю, що підвищує стійкість до атак та мінімізує ризики несанкціонованого втручання. Автоматизація перевірки прав доступу за

допомогою смарт-контрактів забезпечує швидке та прозоре виконання операцій без залучення третіх сторін, що знижує адміністративні витрати та виключає ризик людської помилки.

Список використаних джерел:

1. Treiblmaier H., Rejeb A., Strebinger A. Blockchain as a Driver for Smart City Development: Application Fields and a Comprehensive Research Agenda // Smart Cities. 2020. №3. С. 853–872. DOI: 10.3390/smartcities3030044.
2. Iansiti M., Lakhani K.R. The truth about blockchain // Harvard Business Review. 2017. №95. С. 118–127.
3. Khan M.A., Salah K. IoT security: Review, blockchain solutions, and open challenges // Future Generation Computer Systems. 2018. №82. С. 395–411.