**УДК 004.338**
**В.О. Дармограй А. М. Луцків канд. техн. наук, доц.**
Тернопільський національний технічний університет імені Івана Пулюя, Україна

# АНАЛІЗ БІБЛІОТЕК ДЛЯ РЕАЛІЗАЦІЇ BLOCKCHAIN-ІНФРАСТРУКТУРИ ДЛЯ СИСТЕМ IOT

**V. O. Darmohrai, A. M. Lutskiv Ph.D., Assoc. Prof.**

## APPLICATION OF BLOCKCHAIN TECHNOLOGY IN IOT SYSTEMS

Інтернет речей (IoT) — це сфера, яка доволі швидко розвивається й є у нашому повсякденному житті. Є ціла низка безкоштовних та відкритих програмних засобів для побудови інфраструктур IoT мереж, зокрема Eclipse IOT. Для забезпечення кросплатформової взаємодії, як правило, використовується технологія Java, яка використовується й у Eclipse IOT проектах. Доволі актуальною технологією для забезпечення конфіденційності, ідентифікації користувачів та пристроїв, є Blockchain. Blockchain знайшла використання у різних сферах діяльності людини. Найвідомішими її застосуваннями є інфраструктури криптовалют, водночас, є багато спроб застосувань у наступних сферах: платежі та перекази коштів, розумні контракти “smart contracts”, нотаріальні послуги, розподілені хмарні сховища, засоби цифрової ідентифікації, децентралізовані комп’ютерні мережі, а також системи підтримки та забезпечення інтернету речей. Розглянемо спеціалізовані бібліотеки Java для реалізації Blochain-інфраструктури.

Bitcoinj - це бібліотека для роботи з протоколом Bitcoin. Він може підтримувати гаманець, відправляти/отримувати транзакції без необхідності локальної копії Bitcoin Core та має багато інших розширених функцій. Він реалізований на Java, але може використовуватися з будь-якої мови, сумісної з JVM, зокрема Python та JavaScript. На ньому побудовано багато великих, добре відомих додатків і служб Bitcoin. Особливостями bitcoinj є:

- високооптимізований легкий режим спрощеної перевірки платежів (SPV). У цьому режимі завантажується лише невелика частина ланцюга блоків, що робить bitcoinj придатним для використання на обмежених пристроях, таких як смартфони або дешеві віртуальні приватні сервери;
- повний режим перевірки, який виконує ту ж перевірку, що і Bitcoin Core. У цьому режимі обчислюється невикористаний набір вихідних транзакцій (набір UTXO) і, завдяки базі даних PostgreSQL, може бути збережений у базу даних, що забезпечує швидкий пошук за адресою;
- підтримка каналів мікроплатежів, які дозволяють встановити контракт з багатьма підписами між клієнтом і сервером, а потім вести переговори по каналу, дозволяючи швидкі мікроплатежі, що дозволяють уникати оплати майнерам;
- забезпечує як асинхронну передачу даних, так і синхронний потік з'єднання для мережевого вводу-виводу, що дозволяє вибирати між масштабованими не блокуючими та блокуючими функціями, такими як наближення SOCKS.
- клас гаманця з шифруванням, розрахунком гонорару, багатопідписанням, детермінованим виведенням ключів, підключенням вибору монети/контролем монет, підтримкою розширень для повідомлення про події.
- інструменти командного рядка для роботи з файлами гаманця та ланцюжка, протоколом платежів, мережею тощо.

Web3j - друга найбільш розвинута бібліотека, криптовалюта, заснована на цій передовій технології. бібліотека дозволяє працювати з блокчейном Ethereum, без

додаткових накладних витрат, необхідності писати власний інтеграційний код для платформи. Особливостями web3j є:

- підтримка особистих API-програм Parity та персональних клієнтів Geth
- повна реалізація клієнтського API JSON-RPC Ethereum через HTTP та IPC
- автогенерування обгортки смарт-контрактів Java для створення, розгортання, взаємодії з смарт-контрактами та виклику смарт-контрактів із власного коду Java (підтримуються формати Solidity та Truffle)
- додаткове управління через API JSON-RPC за допомогою Geth і Parity

Fabric Hyperledger - це платформа з відкритим кодом та дозволеною корпоративною технологією розподіленої книги (DLT), розроблена для використання в корпоративних контекстах, яка забезпечує ключові можливості для розмежування порівняно з іншими популярними платформами для ведення журналів або блокчейнів. Hyperledger має високомодульну та настроювану архітектуру, універсальності та оптимізації для широкого кола галузевих випадків використання, включаючи банківські справи, фінанси, страхування, охорону здоров'я, людські ресурси, ланцюжок поставок і навіть доставку цифрової музики. Hyperledger є першою платформою розподіленої книги для підтримки розумних контрактів, створених на мовах програмування загального призначення, таких як Java, Go і Node.js.

Fabric Hyperledger може використовувати протоколи консенсусу, які не потребують конкретної криптовалюти для того, щоб заробити видобуток та використати розумне виконання контрактів. Уникнення криптовалюти зменшує деякі значні вектори ризику/атаки, а відсутність операцій з видобутку криптовалют означає, що платформа може бути розгорнута приблизно з тими ж операційними витратами, що і будь-яка інша розподілена система. Поєднання цих відмінних особливостей робить hyperledger однією з найефективніших платформ, доступних сьогодні як з точки зору проведення транзакцій, а також забезпечує конфіденційність транзакцій та розумних контрактів.

Платформа Fabric є відкритою, це означає, що, на відміну від загальнодоступної закритої мережі, учасники відомі один одному, а не анонімні. Хоча учасники можуть не повністю довіряти один одному, мережа може функціонувати за моделлю управління, яка будується на основі того, що існує довіра між учасниками, наприклад юридична угода або рамки для вирішення спорів. Fabric Hyperledger була спеціально розроблена, щоб мати модульну архітектуру. Незалежно від консенсусу підключення, протоколів управління підключеними ідентифікаторами, таких як LDAP або OpenID Connect, протоколів управління ключами або криптографічних бібліотек, платформа розроблена таким чином, щоб відповідати різноманітним вимогам використання підприємств.

**Література**

1. A Blockchain Platform for the Enterprise [Електронний ресурс] – Режим доступу до ресурсу: https://hyperledger-fabric.readthedocs.io.

2. bitcoinj [Електронний ресурс] – Режим доступу до ресурсу: https://bitcoinj.github.io.

3. web3j [Електронний ресурс] – Режим доступу до ресурсу: docs.web3j.io.