

# ДЕЦЕНТРАЛІЗОВАНА СИСТЕМА КЕРУВАННЯ ДОСТУПОМ НА ОСНОВІ ТЕХНОЛОГІЇ BLOCKCHAIN

А. К. Борецький<sup>1, а</sup>, А. М. Родіонов<sup>1</sup>

<sup>1</sup> Національний технічний університет України «Київський політехнічний інститут»

## Анотація

У даній доповіді запропоновано підхід до побудови децентралізованої системи керування доступом на основі технології Blockchain, яка, окрім основних функцій, забезпечує прозорість та історичність виконання дій, можливість перевірки коректності проведених операцій. Задля якісного забезпечення вищезазначених характеристик, було використано платформу Ethereum.

**Ключові слова:** децентралізована система, технологія Blockchain, керування доступом, транзакція, відкритість інформації, Ethereum

## Вступ

Збої у комп'ютерних системах та різноманітні порушення політики безпеки показують, що рівень забезпеченості правильної роботи застосунків у питаннях надання доступу знаходиться не в найкращому стані. У той час, як здійснюється велика кількість досліджень у цьому напрямку, лише їх незначна частка знаходить застосування на практиці через складність реалізації методу або ж наявність вагомих недоліків, що затьмарюють переваги. Основними з них є вразливість до різного роду атак, тіньова політика адміністрування центрального органу та неспроможність впевнитись у правильності винесеного рішення [1].

Метою даної роботи є створення децентралізованої системи керування доступом, використовуючи основні можливості Blockchain технології для усунення вищезазначених недоліків.

## 1. Шляхи адміністрування доступу

Існує два основних варіанти адміністрування управління доступом: централізований та децентралізований. При плануванні архітектури системи чи застосунку, необхідно розуміти обидва підходи, щоб обрати саме той, що забезпечить якісний рівень безпеки при мінімальних ресурсозатратах на впровадження.

### 1.1. Централізоване управління доступом

При централізованому адмініструванні, один суб'єкт (підрозділ або людина) слідкує за доступом користувачів до усіх системних ресурсів. Такий суб'єкт, що виконує функції адміністратора, налаштовує механізми, які реалізують управління доступом, виконує певні зміни у користувацьких профілях, назначає додаткові можливості їх поведінки чи повністю блокує [2]. Такий тип адміністрування надає

послідовні та уніфіковані методи управління, забезпечує строгий контроль даних, так як лише одна повністю централізована ланка має набір усіх необхідних прав для внесення будь-яких змін [3]. Вони не можуть бути відслідковані чи перевірені на правильність звичайними користувачами, такий механізм управління є тіньовим. Звичайно, що у випадку якісної атаки на центральний сервер чи сховище даних, безпека системи зазнає значного удару з боку порушників [4].

### 1.2. Децентралізоване управління доступом

Метод децентралізованого адміністрування надає управління доступом групі тих користувачів, які безпосередньо пов'язані з ресурсами та краще розуміють, хто повинен мати доступ до окремого функціоналу, а хто – ні. Таку групу часто називають функціональними керівниками, вони приймають рішення про розподіл можливостей між користувачами.

Звичайно, така модель управління, порівняно з попередньою, має ряд переваг. Наприклад, при децентралізованому управлінні, прийняття рішень відбуватиметься більш швидко, так як над його розглядом та аналізом працює не один центральний орган, а спрямована група співробітників, вони мають можливість приймати виважені рішення щодо кожного із запитів, не поспішаючи задовольнити потреби загальної системи [5]. Але не варто забувати, що в даному випадку може мати місце звичайний конфлікт інтересів, тому що при винесенні того чи іншого рішення, усі члени функціонального керівництва повинні дати згоду.

## 2. Технологія Blockchain

Ідея технології є досить простою – це своєрідна база даних загального користування, яка функціонує без централізованого керівництва, а її розподілений

<sup>а</sup>antony.london.uk@gmail.com

характер дозволяє контролювати достовірність транзакцій без нагляду будь-яких регуляторів. Таким чином, система, що створюється на її базі, позбавляється будь-яких посередників [6]. Ще однією перевагою, що вплинула на вибір саме даної технології для реалізації поставлених завдань є те, що досить тривалий термін вона знаходиться під впливом різноманітних загроз з боку шахраїв, але жодної успішної атаки ще не було здійснено, що говорить про високу стабільність та стійкість до стороннього впливу.

Структура даних «блокчейн» є впорядкованим зв'язним списком блоків, кожен з яких містить посилання на попередній (рис. 1). Вона може бути збережена у звичайному файлі або в простій базі даних [7]. Можемо візуалізувати задану структуру у вигляді стека з фрагментами, що базуються один поверх одного та першого блока, що слугує основою. Таке представлення дає змогу використовувати додаткові терміни, наприклад, «висота» – для позначення відстані від першого блока. Пройшовши всю відстань висоти, можна впевнитись у коректності проведення усіх здійснених транзакцій. Кожен фрагмент в межах «блокчейн» однозначно ідентифікується за допомогою хеш-алгоритму SHA-256, що приймає на вхід його заголовок [8].

Blockchain принципово відрізняється за своєю структурою та функціоналом від інших існуючих технологій із схожим призначенням, так як вона не відчуває впливу окремих користувачів чи сторонніх осіб та не належить жодній групі, а цифровим системам, не дивлячись на те, якого вони характеру, дозволяє працювати незалежно від стороннього втручання та водночас у доступному та відкритому для кожного режимі [9].

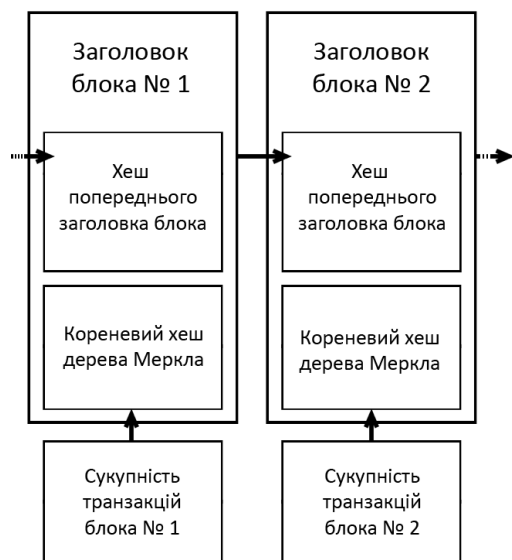


Рис. 1. Модель ланцюга блоків транзакцій

### 3. Реалізація

Коли ми говоримо про звичайний централізований сервіс, то у ролі гаранта здійснення коректних операцій виступають центральні сервери, на яких та-

кож зберігається й історія здійснених транзакцій. Усі дії центрального механізму управління автоматично вважаються правильними, він наділений властивістю беззаперечної довіри. Так як метою створеної системи є саме децентралізація, то вище згаданий метод підтвердження валідності, звичайно, не міг бути прийнятим. Задля вирішення цього питання було скомбіновано систему децентралізованого погодження та проведення транзакцій так, щоб у всіх учасників мережі зберігався єдиний список та порядок проведення операцій.

Використовувалась технологія Blockchain на базі платформи Ethereum (Java-реалізація EthereumJ), основним завданням якої є саме надання змоги створювати довільні децентралізовані застосунки, наділені одночасно властивостями стандартизації, масштабованості, Тюрінг-повноти, легкості розробки та сумісності [10]. Базову платформу ланцюга станів було реалізовано, описавши власні правила взаємодії, формат транзакцій, функції зміни стану.

#### 3.1. Модель поведінки користувачів

Кожен користувач системи має право створити транзакцію-запит на отримання доступу, ала вона не потрапить до «блокчейна» одразу, для цього потрібно отримати згоду від усіх функціональних керівників групи у вигляді накладання підпису на транзакцію. Якщо хоча б один учасник не погоджується із впровадженням запиту користувача, що її створив, він має право не підтверджувати операцію, тоді вона не буде проведена. Користувач отримує доступ лише у тому випадку, коли усі члени товариства дали згоду на це, транзакція буде надіслана до ланцюга блоків від імені усієї групи, а не конкретної особи.

Жоден користувач не має змоги порушити встановлений механізм, але кожен може перевірити правильність його функціонування, впевнитись у відкритості системи та прозорості винесення рішень усіма учасниками функціонального товариства, таку можливість нам надає саме використовувана технологія Blockchain.

#### 3.2. Принципи побудови

Кожен блок, що створюється системою, містить часову характеристику, значення «nonce» – випадковий код, хеш-значення попереднього блока, а також список усіх транзакцій, що потрапляють у нього – операції, здійснені після запису попереднього блока. Транзакції можуть бути створені як користувачами, так і контрактом у автоматичному режимі. Вони включають в себе адресу отримувача, успішне здійснення операції на яку, у даному випадку, виступає підставою модифікації доступу, електронний підпис відправника (функціональної групи), параметр доступу запиту, що оброблюється, додаткову інформацію.

«Майнінг» у створюваній системі служить для забезпечення безпеки від шахрайських операцій, шляхом перевірки нових транзакцій. Таким чином, вини-

кає ланцюжок блоків, у якому зміни не відбуваються, з плином часу він лише зростає та зберігає абсолютно всю інформацію про здійснені операції.

Кожному профілю відповідає його 20-байтова адреса. Функція зміни стану відповідає за переведення інформації. Профіль вміщує 4 поля: попсе – лічильник для одноразового проведення транзакції; поточне інформаційне значення, що використовується для регулювання доступу; код контракту, пов'язаного з профілем; сховище, що є порожнім за замовчуванням.

### 3.3. Здійснення операцій в системі

Транзакції є найбільш важливою частиною створюваної системи, тому їх опису та плануванню необхідно було приділити достатньо уваги при розробці. Усе інше лише забезпечує гарантовану можливість їх створення, поширення, підтвердження і, звичайно, додавання до загального архіву «блокчейн». Кожна транзакція у системі представляє собою структуру даних, яка описує визначення можливості доступу та є публічним записом, що дає змогу з легкістю перевірити усіма охочими правильність її виконання (рис. 2).

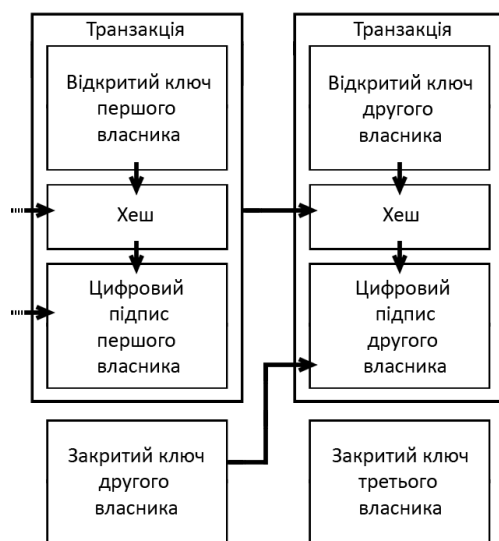


Рис. 2. Приклад структури послідовних транзакцій

Вона декларується у повній мірі відправником щодо того, як дані будуть зібрані та яким саме способом будуть розподілені. Звичайно, потім перевіряється валідність запланованої операції, на що відправник вже не може вплинути ніяким чином. Здійснюється це кожним вузлом мережі після підтвердження усіма членами функціональної групи, а наприкінці, після перевірки «майнером», транзакція додається в блок операцій та стає постійною частиною системи, новий стан якої приймається усіма її користувачами.

Закінчення виконання відбувається при появі помилки, доведення до кінця чи знаходженні спеціальних інструкцій. Система при здійсненні операцій звертається до таких місць розташування інформації: стек (контейнер для обробки декількох значень),

пам'ять (байт-масив довільного розміру), сховище контракту (інформація тут зберігається у вигляді структури ключ-значення). Стек та пам'ять після виконання коду одразу оновлюються, а у сховищі дані можуть знаходитися тривалий термін.

Використовуються також значення наявності доступу користувача до системи, відправника транзакції-запиту, інформації повідомлення та заголовка блока. Наприклад, у випадку перевірки встановлених системою умов перевірки, кожен раз, коли приходить вхідне повідомлення, активується певний код, який надає можливість повідомленню відкривати сховище та працювати з його інформацією, надсилати інші повідомлення.

### Висновки

У даній роботі було проведено розробку децентралізованої системи керування доступом на основі технології Blockchain, яка супроводжувалась детальним аналізом її архітектури, характеристик, поведінкової моделі, можливостей щодо задоволення усіх поставлених завдань. Було представлено та досліджено існуючі шляхи адміністрування доступу, доведено ефективність використовуваних технологій та кінцевої системи загалом.

Окрім того, створення системи супроводжувалось забезпеченням наявності відповідного користувацького інтерфейсу для можливості взаємодії із функціоналом у повній мірі, перевірки коректності описаних механізмів здійснення операцій та вдосконалення роботи системи в цілому.

### Перелік використаних джерел

1. Popper N. Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money. — Harper, 2015. — P. 156–197.
2. Reese G. Cloud Application Architectures: Building Applications and Infrastructure in the Cloud. — O'Reilly Media, 2009.
3. Faircloth J. Enterprise Applications Administration: The Definitive Guide to Implementation and Operations. — Newnes, 2013. — P. 1–27.
4. Fowler M. Patterns of Enterprise Application Architecture. — Addison-Wesley Professional, 2002.
5. Raval S. Decentralized Applications. — O'Reilly Media, Inc., 2015. — P. 22–40.
6. Swan M. Blockchain: Blueprint for a New Economy. — O'Reilly Media, Inc., 2015. — P. 16–28.
7. Antonopoulos A. M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. — O'Reilly Media, Inc., 2014. — Vol. 1. — P. 128–136.
8. Caetano R. Learning Bitcoin. — Packt Publishing, 2015.
9. Kelly B. The Bitcoin Big Bang: How Alternative Currencies Are About to Change the World. — Wiley, 2014. — Vol. 1. — P. 54–65.
10. Champagne P. The Book Of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto. — The Book Of Satoshi, 2014. — P. 195–206.