

# ВИМОГИ ДО ПРОТОКОЛІВ ГЕНЕРАЦІЇ ПАРАМЕТРІВ ДЛЯ ПІДПISУВАННЯ СМАРТ-КОНТРАКТІВ У БЛОКЧЕЙНІ

І. Г. Сліпак<sup>1</sup>

<sup>1</sup>Національний технічний університет України  
«Київський політехнічний інститут імені Ігоря Сікорського»,  
Фізико-технічний інститут

## Анотація

У даній роботі запропоновано ідею та сформульовано ряд вимог до протоколу генерації спільної пари відкритий та секретний ключ підпису, який може застосовуватися для підписання смарт-контрактів.

*Ключові слова:* блокчейн, смарт-контракти

## Вступ

На сьогоднішній день все більше набуває популярності така технологія, як блокчейн. Одна з головних сфер, куди зараз активно інтегрують блокчейн – це зберігання та контроль документів. Особливістю є те, що кожен бажаючий має право дізнатися хто додав певний запис в систему.

### 1. Блокчейн

Блокчейн (англ. Blockchain) – це розподілена база даних, яка підтримує перелік записів, так званих блоків, що постійно зростає [1]. Ця база захищена від підробки, а також має посилання на попередній блок геш-дерева.

Геш-деревом називають зображення даних у вигляді дерева з корнем, гілками і листям (рис. 1)

Ми маємо ланцюжок із блоків (рис. 2), кожен наступний блок містить геш-значення попереднього, будь-який спосіб змінити данні на певному рівні блоку потягне за собою зміну на всіх наступних рівнях, а також буде помічено іншими учасниками. Саме так забезпечується перевірка цілісності даних.

Геш-функція – це функція перетворення масиву вхідних даних довільної довжини у вихідний бітовий рядок фіксованої довжини, яке виконується за допомогою певного алгоритму.

Неможливість підробки блоків є одна з ключових властивостей. Її ще називають незмінність. Незмінність – це означає, що неможливо змінити чи підробити базу даних.

#### 1.1. Застосування технології блокчейн

Технологія блокчейн дозволяє спроектувати надійну систему, де людський фактор зводиться до мінімуму. Цю технологію застосовують в електронному голосуванні, децентралізованій торгівлі, публічних реєстрах.

Розглянемо детальніше децентралізовану технологію. Із застосуванням технології блокчейн і децентра-

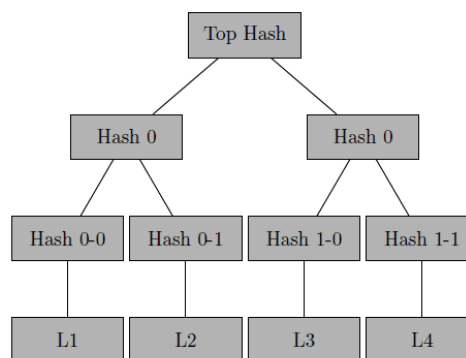


Рис. 1. Геш-дерево

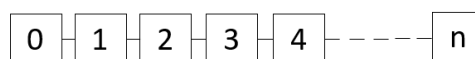


Рис. 2. Ланцюжок блоків

лізованими підходами можливо здійснити аукціони з безліччю дрібних торгових майданчиків. Товар, який виставляється на продаж на одному з майданчиків, буде доступний і на всіх інших. Таким чином, це дозволяє продавцеві показати товар максимально широкій аудиторії покупців. Оскільки виключається необхідність дублювати товар на кожному майданчику, продавець економить багато часу. Більш того, торги ведуться на них одночасно і дані про ставки синхронізуються в режимі реального часу. Тому кожний майданчик завжди знає всі ставки по кожному лоту, відповідно, переможець для всіх очевидний.

Людський фактор в такій системі зведений до мінімуму – провести аудит в такій системі не представляє складності і багато часу для цього не потрібно. Дані про всю історію операцій не можуть бути змінені непомітно.

## 2. Смарт-контракти

Смарт-контракт (англ. Smart Contract) – це комп'ютерний код, який запускається поверх блокчейн, що містить набір правил, згідно з якими сторони цього розумного контракту погоджуються взаємодіяти один з одним [2]. Якщо попередньо визначені правила виконуються, угода автоматично виконується.

Смарт-контракти досить складна річ, їхній потенціал виходить за рамки простої передачі активів – вони можуть виконувати операції в широкому спектрі галузей, від правових процесів до страхових угод, а також якихось фінансових активів. Смарт-контракти мають потенціал для послаблення правової та фінансової сфери завдяки автоматизації процесів, які людина неодноразово повторює, а також витрачає певні фінанси на відстоювання цих інтересів.

Безпосередньо адвокати, як людський фактор, можуть відійти в майбутньому на другий план, оскільки смарт-контракти дуже стрімко прогресують у сфері традиційних юридичних контрактів.

Технологія блокчейн, яка вбудовується в смарт-контракти, є гнучкою. Розробники мають можливість зберігати майже будь-які типи даних в рамках блокчейна, і вони мають широкий вибір варіантів транзакцій, які можна вибирати під час розгортання смарт-контракту.

Інтелектуальні контракти на основі блокчейн допомагають зробити бізнес та інші операції більш безпечними та економічно ефективними.

### 2.1. Переваги та недоліки смарт-контрактів

До безпосередніх переваг відносять:

- Незалежність. Людям, які беруть участь у продажі будь-якого майна, чи ще якихось покупок, більше не потрібно звертатися до послуг посередників.
- Безпека. Умови смарт контрактів змінити неможливо, адже вони знаходяться в розподіленому реєстрі.
- Ефективність витрат. Ці контракти усувають багато експлуатаційних витрат і заощаджують ресурси, включаючи персонал, необхідний для моніторингу їхнього прогресу.
- Відсутність витрат. Коли дві сторони досягають консенсусу то вони відразу обмінюються своїми активами.

Серед великої кількості переваг у даних контрактів є також мінуси:

- Правова сфера. Для того, щоб ці контракти працювали, використовують криптовалюту. Але офіційно криптовалюту не застосовують на рівні законодавства.
- Помилки. Щоб створити смарт-контракт, потрібно прописати все до деталей. Чим складніша

операція тим більше пунктів потрібно буде прописувати. Відповідно чим «важча» операція тим складніше створити інтелектуальний контракт

- Нерозуміння. Багато людей не усвідомлює, що це таке. Тому, попри свою необізнаність, бояться використовувати дану технологію.

### 2.2. Вимоги до протокола генерації параметрів цифрового підпису для підписання смарт-контрактів

Існують протоколи для побудови пари відкритого ключа та секретного ключа, які базуються на протоколі Шаміра, але вони є достатньо трудомісткими. Вирішити цю проблему можна створивши аналогічну пару відкритого ключа та секретного ключа підпису, побудовану за допомогою Китайської теореми про лишки.

Для підписання смарт-контрактів необхідно розробити такий протокол генерації параметрів цифрового підпису, який задовольняє наступним умовам:

- 1) В протоколі беруть участь всі (як мінімум «чесні») учасники;
- 2) Вся інформація, що наявна у блокчейн, є відомою всім учасникам;
- 3) Відкритий ключ учасники можуть встановити відразу;
- 4) Якщо в ході виконання протоколу не більше ніж половина учасників починають обманювати, то в результаті роботи цього протоколу все одно будуть побудовані коректні параметри підпису
- 5) Секретний ключ буде відомий лише тоді, коли не менше ніж половина учасників проголосують за його відновлення (тобто нададуть свої частини розподіленого секрету).

### Висновки

На даний час існує єдиний протокол, який частково задовольняє наведеним умовам. Протокол наведено на сайті <https://iohk.io>. Він базується на схемі Шаміра розподілу секрету. Тому запропоновані більш ефективні вимоги до протоколу генерації спільної пари відкритого ключа та секретного ключа, який може застосовуватися для підписання смарт-контрактів та базується на Китайській теоремі про лишки і задовольняє умовам (1 – 5).

### Перелік використаних джерел

1. Nakamoto Satoshi. Bitcoin: A peer-to-peer electronic cash system. – 2009. – Access mode: <http://www.bitcoin.org/bitcoin.pdf>.
2. Кравченко П. Скрябин Б. Дубинина О. Блокчейн и децентрализованные системы. – 2018. – С. 408 с.