УДК 004.056.5

КРИПТОГРАФІЧНІ ПРОТОКОЛИ ЕЛЕКТРОННОЇ ГОТІВКИ НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН

О. М. Чорний[1], А. М. Кудін[1]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

У даній роботі розглядається система електронних платежів Чаума та способи її вдосконалення, що базуються на використанні технології блокчейн.

Ключові слова: електронні платежі, блокчейн, смарт-контракти

Вступ

Будь-яка економіка, у найбільш загальному вигляді, складається з процесу виробництва товарів (продуктів, послуг) і комерційної діяльності, основною метою якої є отримання прибутку за допомогою реалізації виробленого товару.

Електронна комерція – це різновид комерційної діяльності, в якій взаємодія між її учасниками на всіх або деяких її етапах здійснюється електронним способом. Ключовим питанням, пов'язаним з впровадженням і надійним функціонуванням системи електронної комерції, є забезпечення грошових розрахунків в електронному вигляді між постачальником і споживачем. Для досягнення цієї мети можуть бути використані різні електронні платіжні системи, принципова відмінність яких від традиційних полягає в тому, що весь процес від початку і до кінця відбувається в електронній (цифровій) формі.

1. Електронні платіжні системи

1.1. Система електронних платежів Чаума

Дана система анонімних електронних платежів була запропонована у 1982 році американським вченим Девідом Чаумом і базується на схемі сліпого цифрового підпису [1].

Сліпим підписом називається такий цифровий підпис, процедура генерації якого не розкриває змісту документу підписуючій стороні.

Опишемо тепер схему виконання електронного платежу на певну фіксовану суму на основі схеми сліпого підпису RSA. Нехай є абоненти A (платник), B (отримувач платежу) та Банк. Банк має криптосистему RSA із відкритим ключем (n, e) і приватним ключем (n, d). Також назвемо *монетою* $C = \langle SN \rangle$ кортеж, єдиною компонентою якого є число $0 \leq SN < n$, яке ми назвемо *серійним номером* монети. *Номіналом монети* назвемо суму платежу, який виконується з її допомогою.

Виконуються такі кроки:

1) A випадковим чином генерує серійний номер $0 \leq SN < n$.
2) A обирає випадкове число r, $1 < r < n$, $(r, n) = 1$ і обчислює $SN' = SN\ r^e\ mod\ n$.
3) A надсилає на підпис банку осліплений серійний номер SN'.
4) Банк генерує підпис $S' = SN'^d\ mod\ n$ і знімає із рахунку абонента A відповідну суму коштів.
5) A обчислює $S = S'r^{-1}\ mod\ n = SN^d\ mod\ n$, отримуючи таким чином дійсний цифровий підпис банку на серійному номері.
6) A формує монету $C = \langle SN \rangle$ та надсилає B пару (C, S).
7) B перевіряє підпис S за допомогою відкритого ключа банку, і, якщо він вірний, надає абоненту A домовлені послуги.
8) B надсилає пару (C, S) банку для перерахування коштів на свій рахунок.
9) Банк в свою чергу перевіряє підпис S серійного номера SN монети C і, у разі успішної перевірки, зараховує на рахунок абонента B відповідну суму коштів а також заносить SN у реєстр використаних монет.

Таким чином, банк виконує переказ коштів із рахунку абонента А на рахунок абонента B, не маючи при цьому ніякої змоги пов'язати їх між собою, тим самим забезпечуючи анонімність даного платежу.

1.2. Недоліки системи електронних платежів Чаума

Один із ключових недоліків схеми електронних платежів Чаума є неможливість передавати монету C від одного абонента системи до іншого без взаємодії із Банком. Це пов'язано із тим, що єдиним засобом захисту системи від подвійної трати монети є реєстр використаних монет зі сторони Банку. Якщо дозволити передачу монет між абонентами без взаємодії з банком, то запобігти використанню

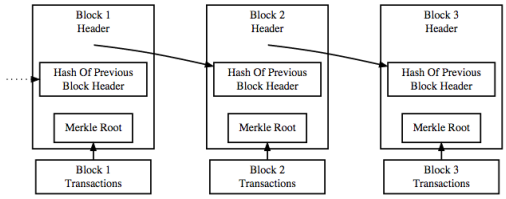

Рис. 1. Схематичне зображення блокчейна

однієї монети для проведення декількох платежів одночасно буде неможливо.

Таким чином банк зобов'язаний бути учасником кожного платежу, що створює додаткове навантаження на його програмне та апаратне забезпечення. Більш того, Банк повинен бути постійно доступним, що значно ускладнює підтримку його внутрішніх систем.

Метою даної роботи є модифікація системи електронних платежів Чаума таким чином, аби дозволити передачу монет між абонентами системи, забезпечуючи анонімність усіх операцій та неможливість подвійного використання монет.

2. Смарт-контракти та технологія блокчейн

2.1. Блокчейн

Блокчейн (англ. *blockchain*) є децентралізованою базою даних, що представляє собою набір блоків структурно об'єднаних в ланцюг. Кожен блок містить певний набір полів, основними із яких є геш заголовка попереднього блока у ланцюгу, перелік проведених транзакцій та корінь дерева Меркля, побудованому із гешів проведених транзакцій. Дана структура гарантує, що зміна інформації про будь-яку транзакцію приведе до зміни блоку в якому вона записана, а отже і до зміни всіх блоків, що були додані у ланцюг пізніше (рис. 1).

Повна копія усього блокчейну зберігається на комп'ютері кожного користувача мережі. Усі користувачі є рівноправними, а їх дії не контролюються жодним центральним органом. Окремою групою користувачів є так звані *майнери*. Вони відповідальні за підтримку роботи мережі, займаючись генерацією нових блоків. За виконання своєї роботи вони отримують певну грошову винагороду, зазвичай у валюті тієї системі, для якої вони генерують блоки. Для генерації блоку майнер повинен знайти таке значення поля nonce, що отримане геш-значення блоку буде задовольняти певним вимогам. Після цього згенерований блок розповсюджується по мережі, де користувачі перевіряють, що він дійсно був згенерований коректно і додають його до власної копії ланцюга.

У такому вигляді технологію блокчейн було вперше використано у якості основної складової криптовалюти BitCoin, що побачила світ у 2009 році [2].

2.2. Смарт-контракти Ethereum

У BitCoin блокчейн використовується для зберігання інформації про грошові транзакції, виконані користувачами системи. Проте згодом стало зрозуміло, що потенціал даної технології значено ширший і блокчейн може використовуватись як універсальна платформа зберігання та обробки інформації та слугувати основою для реалізації ідеї смарт-контрактів, запропонованої ще у 1996 році. У 2015 році відбувся перший реліз блокчейну Ethereum – першої практичної реалізації даного підходу [3].

Смарт-контракт – це електронний алгоритм, який полегшує або навіть автоматизує процес укладення договорів. Умови і результати смарт-контрактів описуються за допомогою спеціальних мов програмування. Програмний код не просто містить інформації про зобов'язання сторін – він підтверджує виконання умов контракту і автоматично визначає, що робити з зазначеним активом (передати учаснику угоди, повернутися відправнику або щось складніше).

Використання блокчейна як транспорту для смарт-контрактів виключає необхідність залучати третю сторону в якості гаранта дотримання умов. Таким чином, блокчейн дозволяє не покладатися на авторитет посередника. Децентралізований реєстр зберігає копію смарт-контракту, що забезпечує його захищеність і достовірність та не дозволяє жодній зі сторін змінити попередньо визначені умови контракту.

Описані властивості блокчейну та смарт-контрактів дають можливість використання цих технологій для вирішення задачі анонімної передачі монет Чаума між користувачами.

3. Вирішення задачі забезпечення можливості безпечної передачі монет між користувачами за допомогою технології блокчейн

3.1. Опис запропонованого рішення

Пропонований метод вирішення даної задачі базується на ідеї використання внутрішнього стану смарт-контракту для зберігання інформації про поточного власника монети. Для функціонування даного механізму передбачено три процедури: внесення монети в реєстр, передача іншому власнику та зарахування монети на рахунок її власника в Банку.

Внесення монети в реєстр. Процедура складається із двох основних кроків. Перший крок аналогічний класичній системі електронних платежів Чаума. Абонент Банку генерує монету C та отримує у Банку цифровий підпис її серійного номера за допомогою протоколу сліпого підпису. Після цього абонент використовує свій обліковий запис мережі Ethereum для внесення до смарт-контракту запису, який містить саму монету та адресу її власника. Внесення інформації про створену монету до смарт-контракту є кроком, обов'язковим для проведення будь-яких подальших операцій із даною монетою.

Передача монети іншому власнику. Для того, аби передати монету іншому власнику, поточний власник монети повинен викликати відповідну операцію смарт-контракту, передавши в якості параметрів серійний номер монети та адресу нового власника монети. Дана операція виконує перевірку того, що

дана монета дійсно існує, а користувач, який викликав операцію, дійсно є її власником. Якщо всі перевірки завершились успіхом, то до смарт-контракту записується новий власник даної монети.

Зарахування монети на рахунок в Банку. Дана процедура проводиться у випадку, якщо поточний власник монети вирішує зарахувати на свій рахунок у Банку кошти, що відповідають її номіналу. На відміну від класичної системи електронних платежів Чаума, у пропонованій нами реалізації ця процедура є більш складною та вимагає від Банку проведення таких перевірок.

- Перевірка того, що монета з таким серійним номером взагалі існує. Монети, які не були зареєстровані їх початковими власниками, Банк не обслуговує, оскільки для них неможливо відслідкувати спроби подвійного використання.
- Перевірка коректності цифрового підпису монети ключем Банку, який відповідає її номіналу. Ця перевірка є аналогічною перевірці у класичній системі.
- Перевірка того, що монета ще не була використана.
- Перевірка того, що користувач, який хоче зарахувати монету на свій рахунок, дійсно є її власником.

Аби зробити можливими проведення останніх двох перевірок, пропонується наступний підхід. Для зарахування монети на рахунок в Банку її власник робить відповідний запит до Банку. Банк генерує велике випадкове число r та повідомляє його абоненту A. Абонент A, аби довести Банку, що він дійсно є власником даної монети, додає до смарт-контракту запис, що містить отримане число r та серійний номер SN монети, яку він хоче зарахувати на свій рахунок. Після цього абонент повідомляє Банку значення SN. Банк перевіряє, чи дійсно смарт-контракт містить запис із серійним номером SN та числом r. У випадку успішної перевірки Банк виконує переказ коштів на рахунок абонента і викликає службову операцію смарт-контракту, яка помічає монету як використану для попередження спроб її подвійного використання.

3.2. Аналіз властивостей рішення

Анонімність. Оскільки система не передбачає наявності будь-якого зв'язку між обліковими записами користувачів банку та їх адресами у мережі Ethereum, встановити особу поточного або будь-якого попереднього власника монети неможливо. Більш того, проміжні власники монети можуть взагалі не мати облікових записів у Банку.

Завдяки використанню механізму сліпого підпису Банк також не має можливості встановити зв'язок між серійним номером монети та особою абонента, який вніс інформацію про дану монету до смарт-контракту. Єдиний абонент мережі Ethereum, чия особа встановлюється банком – це останній власник монети, який виконує зарахування коштів на власний рахунок Банку.

Підхід, який може бути використано для досягнення повної анонімності дій будь-якого абонента, полягає у створенні нового облікового запису (і, відповідно, нової адреси) у мережі Ethereum для отримання кожного нового платежу від інших абонентів. Зауважимо, що для багатьох абонентів такий підхід може бути надлишковим і використання однієї і тієї ж адреси для всіх операції може їх цілком задовольняти. Тому система дає змогу обирати той рівень анонімності, який абонент вважає доцільним для себе.

Можливість подвійної витрати монет. Завдяки використанню списку використаних монет та його відкритому зберіганню у мережі блокчейн подвійне використання монет стає неможливим. Також, за рахунок того, що всі операції, виконані над певним смарт-контрактом, мають строгий порядок, виключається можливість одночасного зарахування монети на власний рахунок в Банку та її передачі іншому користувачу.

Безпека. Структура описаного смарт-контракту та загальні властивості рішень на базі блокчейну Ethereum забезпечують такі властивості запропонованого рішення.

- В момент створення монети тільки її власник знає її серійний номер, тому тільки він може внести монету до смарт-контракту. Смарт-контрактом гарантується, що початковим власником монети може бути записаний тільки той користувач, який викликав операцію внесення.
- Смарт-контракт забезпечує можливість зміни власника монети тільки її поточним власником. Оскільки кожна транзакція в Ethereum підписується цифровим підписом користувача, який її додав, гарантується, що ніхто не може видати себе за власника деякої монети і використати її від імені власника.

Висновки

У даній роботі було запропоновано модифікацію системи електронних платежів Чаума, яка дозволяє передавати монети між абонентами системи, забезпечуючи при цьому повну анонімність усіх користувачів та безпеку всіх виконаних операцій. Система побудована на основі технології смарт-контрактів Ethereum, що відрізняє її від усіх існуючих рішень даної задачі.

Перелік використаних джерел

1. David Chaum. Blind signatures for untraceable payments // Advances in Cryptology Proceedings of Crypto. — 1983. — no. 82. — P. 199–203.
2. Satoshi Nakomoto. Bitcoin: A Peer-to-Peer Electronic Cash System // BITCOIN.ORG. — 2009. — no. 3. — P. 1–9.
3. A Next-Generation Smart Contract and Decentralized Application Platform. — 2015. — Access mode: `https://github.com/ethereum/wiki/wiki/White-Paper`.