УДК 621.396

Д. В. Гаврілов
А. В. Левкін

ОГЛЯД ПРОТОКОЛІВ ПІДВИЩЕНОЇ КОНФІДЕНЦІЙНОСТІ ТА МАСШТАБУВАННЯ

Вінницький національний технічний університет

Анотація

Дана робота присвячена сучасним протоколам які допомагають в збільшенні масштабування та покращують конфіденційність користувачів блокчейну. Протоколи які будуть розглядатись в даній роботі, вирішують велику кількість проблем, а саме: вирішують недоліки які властиві майже всім поточним реалізаціям Блокчейна, пропонують радикальне скорочення об'єму даних протоколу Bitcoin*, що дозволить суттєво підвищити конфіденційність і вирішить питання пластичності транзакцій, надають значно більше можливостей для масштабування мережі, ніж поточна архітектура, пропонують можливість приховати кількість переданих коштів, зберігаючи при цьому здатність загальнодоступної перевірки в мережі* Bitcoin*. Більшість протоколів які розроблять для вирішення проблем конфіденційності і масштабування мають досить багато недоліків, але дані протоколи на думку багатьох розробників є одними з найкращих рішень для покращення роботи мережі* Bitcoin*.*

Ключові слова: Bitcoin, конфіденційність, масштабування, Блокчейн

Abstract

This work is devoted to modern protocols that help to increase scaling and enhance the privacy of Blockchain users. The protocols that will be considered in this paper solve a large number of problems, namely: solving the disadvantages inherent in almost all current implementations of Blockchain, offer a radical reduction in the amount of data Bitcoin protocol, which will significantly increase the privacy and solve the problem of plasticity of transactions, provide significantly more the possibilities for scaling the network, than the current architecture, offer the opportunity to hide the amount of funds transferred, while maintaining the ability of the public check on the network Bitcoin Most of the protocols that are designed to address the issues of privacy and scaling have many shortcomings, but these protocols are considered by many developers as one of the best solutions for improving the operation of the Bitcoin network.

Keywords: Bitcoin, privacy, scaling, Blockchain.

Вступ

Недостатня фінансова конфіденційність може призвести до великих проблем, пов'язаних з безпекою як особистих фінансових транзакцій, так і комерційних. Без належного ставлення до захисту, зловмисники можуть з легкістю заволодіти чужими коштами або цінною інформацією.

Кожен рік дає нам все більше нових протоколів які можуть поліпшити роботу мережі Bitcoin. Багато з них дуже подібні. Протоколи Confidential Transaction і MimbleWimble мають багато спільного, вони побудовані на подібній архітектурі яка використовує так званий Обов'язок Педерсена, що вирішує за допомогою криптографії проблему конфіденційності транзакцій, яка може призвести до поліпшення взаємозамінності. Коли деякі монети вважаються більш цінними за інші, через їхню історію транзакції, інколи за такі «чисті» монети користувачі готові заплатити більшу ціну а ніж за монети які мають невідому історію [1 - 3].

Огляд існуючих протоколів

Блокчейн Bitcoin частково вирішує проблему приватності транзакцій, використовуючи «псевдоніми». Під час кожної транзакції користувачі дізнаються адреса один одного і це порушує їхню конфіденційність. Маючи адресу іншого користувача, можна відслідкувати всі його здійснені транзакції. Наприклад, роботодавець виплачує робітнику заробітну плату в BTC. Коли робітник сплачує рахунки, всі ті кому він відкрив свою адресу, можуть дізнатись яка в нього заробітна плата і де він працює. Це може створити певні проблеми, які потрібно вирішити. Були запропоновані криптографічні методи для покращення конфіденційності, але більшість з них мають малу пропускну здатність, а також потребували великих витрат для впровадження в протокол Bitcoin [4, 5].

Таблиця 1 – Формат блока в мережі Bitcoin

Поле	Значення	Розмір
Константа	0xB1D8CFG7	4 байти
Розмір блоку	Кількість байтів в блоці, враховуючи транзакції	4 байти
Заголовок блоку	Завжди складається з 6 полів	80 байт
Лічильник транзакцій	Кількість транзакцій в блоці	1-9 байт
Транзакцій	Список транзакцій	не фіксоване

У табл. 1 представлено формат блока який використовується для передачі даних в мережі. Потрібно зазначити, що єдине поле яке не має константного значення, це розмір транзакцій в блоці, максимальне значення якого досягає 1 Мбайт. На даний момент, при підтримці софтфорка Segregated Witness, це значення збільшене, і може досягати 4 Мбайт, що дає можливість збільшити кількість транзакцій в блоці, не порушивши правил протоколу Bitcoin.

Таблиця 2 – Заголовок блоку

Поле	Значення	Розмір
Версія	Номер версії блоку	4 байти
Хеш-значення попереднього блоку	256-бітний хеш попереднього заголовка блоку	32 байти
Хеш-значення дерева Меркла	256-бітний хеш значення від усіх транзакцій в блоці	32 байти
Часова мітка	Поточна мітка часу	4 байти
Параметр складності	Поточна ціль у компактному форматі	4 байти
Вирішення задачі PoW	32-бітний номер (початок з 0)	4 байти

У табл. 2 показано заголовок блоку. Заголовок складається з шести полів, загальний розмір яких сягає 80 байт, це значення є константне [5].

Принцип роботи

Протоколи Confidential Transaction і MimbleWimble покращують ситуацію, роблячи суми транзакцій приватними, але водночас зберігають здатність загальнодоступної перевірки в мережі. Все це відбувається без додавання нових базових криптографічних змін в систему Bitcoin.

Confidential Transactions (CT) можливі завдяки криптографічній технології адитивних гомоморфних обов'язків. Як побічний ефект своєї архітектури, CT дозволяє обмін приватними даними (такими як номери рахунків), не збільшуючи розміру транзакцій, відновлюючи більшу частину витрат на криптографічні докази CT. Для приховання кількості BTC які передаються в транзакції Confidential Transaction використовують приховані фактори або стрічку випадкових цифр. Якщо в реалізації Blockstream, ці цифри задавались відправником і розшифровувались отримувачем за допомогою закладеної в транзакції інформації, то протокол MimbleWimble все робить навпаки, і дозволяє одержувачу самому генерувати рядок випадкових цифр, при цьому приватні ключі і адреса не використовуються.

Слід почати з прикладу криптографії, на основі Еліптичних кривих (або просто ЕК). ЕК – це нескінченна кількість точок, на кривій «Т», які можна складати, додавати, множити на цілі числа (скаляри). Припустимо, що «k» є цілим числом, тоді застосувавши скалярне множення, можемо обчислити k×H, що також є точкою на кривій Т. Якщо дано ще одне ціле число «j», тоді також можна обчислити (k+j)×H, що рівноцінно дорівнює k×H+j×H. Додавання і скалярне множення на ЕК

задовольняє властивості комутативності і асоціативності множення і додавання:

$$(k+j)\times H = k\times H+j\times H.$$

Взявши число k як приватний ключ (це повинно бути достатньо велике число), тоді рівність k×H буде відповідно публічним ключем. Це дає змогу бут впевненим, що якщо комусь відоме значення публічного ключа k×H, обчислення k прирівнюється до неможливості, незважаючи на тривіальність множення. Ділення точок на ЕК є вкрай складним завданням. Формула (k+j)×H = k×H+j×H, де «k» і «j» зберігаються в таємниці, показує, що публічний ключ може бути отриманий складанням двох приватних ключів.

Структура транзакцій вказує на ключові принципи протоколу: непорушну гарантію приватності і конфіденційності. Перевірка транзакцій MimbleWimble підтримується двома властивості:

- володіння приватними ключами: як і в інших криптовалютах, володіння виходами транзакції є доказом володінням приватного ключа. Однак докази володіння приватним ключем досягається інакше, ніж просто підписом транзакції;
- перевірка нульових сум: сума виходів мінус сума входів завжди повинна дорівнювати нулю, це доводить, що транзакція прийнятна і не створює монет з повітря, без розкриття сум переказів.

Транзакція MimbleWimble включає в себе наступне:

- набір входів, які посилаються на набір виходів попередніх транзакцій;
- набір нових виходів, які включають в себе:
  - кількість монет і фактор приховування помножень на ЕК;
  - доказ того, що «w» не є від'ємним (range proof).
- комісія транзакцій в відкритому вигляді;
- підпис, обчислений шляхом використання надлишкового значення (суми всіх виходів і комісії за вирахуванням суми входів) і використання цього значення в якості приватного ключа [1 - 3].

Обчислення балансу гаманця

Припустимо, що «w», це значення входу або виходу транзакції, H це точка на ЕК, тоді можна підставити значення w×H замість w в транзакцію. Це працює завдяки тому, що, використовуючи операції на ЕК, є можливість впевнитися, що сума виходів дорівнює сумі входів.

$$w1 + w2 = w3 => w1\times H + w2\times H = w3\times H \quad (1)$$

Перевірка цієї властивості для кожної транзакції дозволяє протоколу упевниться, що транзакція не створює нові монети, при цьому не розкриваючи кількості переданих монет. Звичайно є можливість вгадати передану кількість монет методом перебору, крім того можна дізнатися кількість w1 з попередньої транзакції, і звичайно w1×H, що розкриває значення виходів всіх транзакцій, які використовують w1. Через такий можливий варіант, потрібно ввести ще одну точку на ЕК, наприклад «G» (насправді, це ще один генератор групи, утворений кривою T, що і точка H), і приватний ключ «r» використаний як фактор приховування. Таким чином, значення входів і виходів транзакції можуть бути виражені як:

$$r \times G + w \times H. \quad (2)$$

Спираючись на основні властивості ЕК, ні w ні r не можуть бути обчислені. Вираз r×G+w×H називається Обов'язок Педерсена, який використовує як Confidential Transaction, так і MimbleWimble Як приклад, припустимо, що є транзакція з двома входами і одним виходом, тоді (без урахування комісії): wi1 + wi2 = wo3, де wi1 і wi2 входи, а wo3 – вихід.

На основі прихованих факторів створюються приватні ключі для кожних із значень, замінивши їх на відповідні Обов'язки Педерсена в попередньому рівнянні:

$$(ri1 \times G + wi1 \times H) + (ri2 \times G + wi2 \times H) = (ro3 \times G + wo3 \times H), \quad (3)$$

яке вимагає, щоб ri1 + ri2 = ro3.

Використовуючи властивості операції додавання над ЕК, є можливість створювати транзакції, які є абсолютно конфіденційними, але в той же час можуть бути перевірені на валідність. Маючи ті ж властивості для блоків, відпадає потреба в зберіганні всіх даних Блокчейна що сприяє відмінній масштабованості мережі і дає можливість швидкої синхронізації нових користувачів [4 ,7].

Висновки

В даній роботі було описано принцип роботи протоколів які можуть забезпечити підвищення рівня конфіденційності і масштабування. Зазначимо, що протокол MimbleWimble є більш кращим ніж протокол зі схожою структурою побудови Confidential Transaction. В своєму нинішньому стані протокол MimbleWimble не дуже сумісний з протоколом Bitcoin, оскільки його впровадження потребує видалення script із структури транзакцій. В результаті цього потрібно пожертвувати іншими функціями, наприклад, time-locked, що використовується в Lightning Network. MimbleWimble може бути ідеальним рішенням для Sidechain з підвищеним рівнем приватності [8 – 11].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Georg Fuchsbauer, Michele Orru, Yannick Seurin, "Aggregate Cash Systems: Cryptographic Investigation of Mimblewimble," (IACR) Cryptology ePrint Archive, vol. 2018, p. 1039, 2018.
2. Gregory Maxwell, Andrew Poelstra, Yannick Seurin, Pieter Wuille, Simple Schnorr, "Multi-Signatures with Applications to Bitcoin," (IACR) Cryptology ePrint Archive, vol. 2018, p. 68, 2018.
3. Harry Halpin, Marta Piekarska, “Introduction to Security and Privacy on the Blockchain,” 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2017, DOI: 10.1109/EuroSPW.2017.43.
4. Andreas M. Antonopoulos, Mastering Bitcoin: Programming the Open Blockchain, O'Reilly Media, 2nd ed., 416 p., 2017, ISBN: 978-1491954386.
5. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, 336 p., 2016, ISBN: 978-0691171692.
6. Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, Greg Maxwell, “Bulletproofs: Short Proofs for Confidential Transactions and More,” IEEE Symposium on Security and Privacy (SP), 2018, DOI: 10.1109/SP.2018.00020.
7. Mauro Conti, E. Sandeep Kumar, Chhagan Lal, Sushmita Ruj, “A Survey on Security and Privacy Issues of Bitcoin,” IEEE Communications Surveys & Tutorials, vol. 20, iss. 4, 2018, pp. 3416 - 3452, DOI: 10.1109/COMST.2018.2842460.
8. Christopher Ehmke, Florian Wessling and Christoph M. Friedrich, "Proof-of-Property - A Lightweight and Scalable Blockchain Protocol," 2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), Gothenburg, Sweden, 2018, pp. 48-51. doi: 10.1145/3194113.3194122
9. Bin Lian, Gongliang Chen, Jialin Cui and Maode Ma, "Compact E-Cash with Efficient Coin-Tracing," in IEEE Transactions on Dependable and Secure Computing. doi: 10.1109/TDSC.2018.2882507
10. Alvin Heng Jun Ren, Ling Feng, Siew Ann Cheong and Rick Siow Mong Goh, "Optimal Fee Structure for Efficient Lightning Networks," 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), Singapore, Singapore, 2018, pp. 980-985. doi: 10.1109/PADSW.2018.8644930
11. Zijiang Hao, Raymond Ji and Qun Li, "FastPay: A Secure Fast Payment Method for Edge-IoT Platforms using Blockchain," 2018 IEEE/ACM Symposium on Edge Computing (SEC), Seattle, WA, 2018, pp. 410-415. doi: 10.1109/SEC.2018.00055

Гаврілов Дмитро Володимирович — канд. техн. наук, доцент, доцент кафедри радіотехніки, Вінницький національний технічний університет, Вінниця, email: havrilov@vntu.edu.ua

Левкін Артем В’ячеславович — студент факультету ІРЕН ВНТУ, email: artm.levksn@ukr.net

Havrilov Dmytro — Cand. Sc. (Eng), Associate Professor of the Department of Radio-Frequency Engineering, Vinnytsia National Technical University, Vinnytsia, email: havrilov@vntu.edu.ua

Levkin Artem — student of the faculty of infocommunications, radioelectronics and nanosystems, Vinnytsia National Technical University, Vinnytsia, email: artm.levksn@ukr.net