ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КОМП'ЮТЕРНА ТЕХНІКА

https://doi.org/10.31649/1997-9266-2021-155-2-85-91

УДК 004.42

Є. С. Щербіна[1]
В. І. Месюра[1]

МЕХАНІЗМИ ІНТЕГРАЦІЇ БЛОКЧЕЙНІВ МІЖ СОБОЮ

[1]Вінницький національний технічний університет

Розглянуто необхідність інтеграції блокчейнів між собою та проблеми, які виникають на цьому шляху. Розглянута ідея транспортування біткоїнів шляхом знищення їх на одному блокчейні та створення відповідної вартості на іншому блокчейні.

Наведено стислий опис таких понять як біткоїн транзакція та біткоїн блок. Детально описано структуру даних «дерево Меркла» (Merkle Tree), як її внутрішню організацію, так і її переваги. Наведено алгоритм побудови «дерева Меркла» (Merkle Tree) для блоку транзакцій та принцип побудови та верифікації «шляху Меркла» (Merkle Path) для заданої транзакції. Описано поняття «доказ роботи» (Proof Of Work) як з технічної, так і з економічної точки зору.

Вперше запропоновано детальний алгоритм транспортування біткоїнів з одного блокчейну на інший, що, здебільшого, базується на структурі даних «дерево Меркла» та ідеї «доказу роботи». Наведені та роз'яснені основні чотири етапи цього алгоритму. Наведена схема транзакції, що знищує один біткоїн, розглянуто її сценарій блокування (locking script). На реальному прикладі проілюстровано створення та перевірку доказу існування (proof of existence) транзакції на основі дерева Меркла. Наведено детальну схему транзакції на допоміжному блокчейн з її основними елементами, а саме: ланцюг заголовків блоків (над якими виконана певна кількість доказу роботи), доказ існування на основі дерева Меркла, закодована транзакція з біткоїн блокчейну. Також наведені зв'язки між цими елементами та розглянуто алгоритм формування вищезгаданої транзакції. Покроково розглянуто алгоритм валідації транзакції на допоміжному блокчейні з погляду смарт-контракту, що має бути розгорнутий на допоміжному блокчейні.

Описано недоліки ідеї інтеграції блокчейнів між собою як з технічної точки зору, так і з точки зору UI/UX для кінцевого користувача.

Ключові слова: криптовалюта, біткоїн, блокчейн, сайдчейн, інтеграція блокчейнів, дерево Меркла, смарт-контракт, доказ роботи.

Вступ

У 2009 році поява біткоїна була справжньою революцією, ця технологія та ідеї, що були закладені у неї, випереджали час. Проте на сьогодні у біткоїна виявлено чималу кількість проблем та його навіть можна назвати дещо застарілим.

Проблема полягає у складності внесення змін до біткоїн блокчейну. Оскільки біткоїн є децентралізованим, то копія програмного забезпечення знаходиться у сотнях тисяч користувачів, що робить неможливим миттєво оновити версію програмного забезпечення одночасно для всіх учасників. Це приводить до того, що всі оновлення мають бути зворотно сумісні. Це, у свою чергу, означає наявність двох основних проблем:

– навіть прості зміни до протоколу вимагають величезних зусиль, як от, наприклад, P2SH або SegWit.

– деякі зміни просто неможливі, до прикладу, зміна мови смарт-контрактів або хеш-функції, що використовується для майнінгу [1].

Існує два основні підходи для вирішення вищевказаних проблем:

– створення нових, незалежних, альтернативних криптовалют, так званих "altcoins";

– побудова певної ієрархії блокчейнів, де активи можуть бути транспортовані з одного блокчейну до іншого.

Перший спосіб піддається критиці, оскільки він фрагментує поточну інфраструктуру та єдиною сполучною ланкою між такими криптовалютами є централізовані біржі, що порушує фундаментальний принцип “trustless”, що закладений у технологію блокчейн.

Іншою проблемою є початковий розподіл та ціноутворення монет у новостворених криптовалютах. Досить часто такі монети розглядаються як механізм для спекулятивних торгів, а не з погляду нових технологій, які вони принесли у світ криптовалют.

Отже, враховуючи проблеми “altcoins”, сфокусуємо цю статтю на технології допоміжних блокчейнів (sidechains).

Механізм транспортування активів між блокчейнами

Постановка задачі. Необхідно транспортувати 1 BTC з блокчейну Bitcoin на інший blockchain (в подальшому sidechain), який підтримує мову смарт-контрактів. Під транспортуванням мається на увазі знищення 1 BTC на блокчейні bitcoin та створення аналогічної вартості на допоміжних блокчейнах sidechain. Новостворена вартість має бути під управлінням людини, що знищила 1 BTC на блокчейні bitcoin.

Важливим обмеженням є те, що смарт-контракти не мають доступу до мережі Інтернет, оскільки це б мало величезні ризики для безпеки програмного забезпечення.

Для вирішення цієї задачі необхідно скомбінувати декілька вже існуючих інструментів. Розглянемо їх детальніше.

Транзакція є набором входів та виходів. За відсутності комісій сума входів дорівнює сумі виходів. Транзакція знищує одні UTXO (входи) та створює нові UTXO (виходи) [2].

Блок складається з двох основних частин заголовку та тіла. Заголовок має фіксований розмір 80 байт та складається з посилання на попередній блок, merkle root, який обговоримо в подальшому, та іншої метаінформації. Тіло блоку — це упорядкований список транзакцій (рис. 1).

Merkle Tree (дерево хешів)

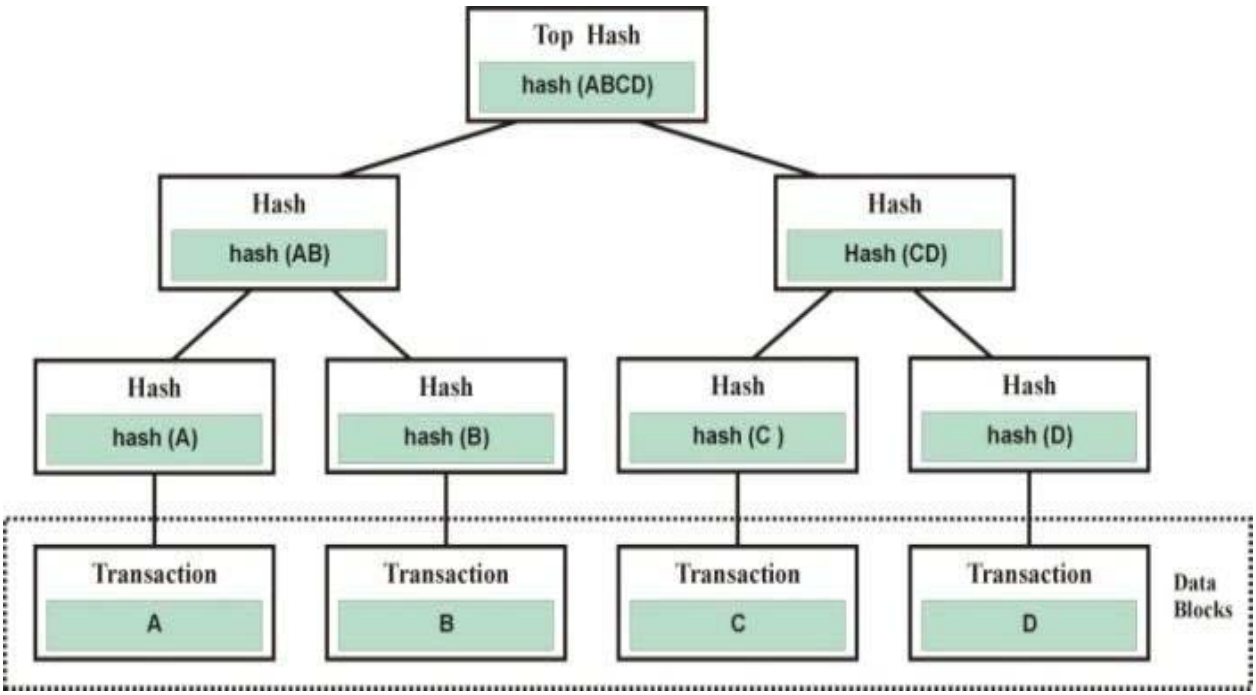

Рис. 1. Дерево Меркла для блоку, що складається з чотирьох транзакцій

Розглянемо випадок, коли блок складається з чотирьох транзакцій — A, B, C, D. Побудова дерева хешів складається з таких кроків:

1) розміщення транзакцій на нижньому рівні дерева;

2) формування наступного рівня дерева шляхом хешування кожної транзакції;

3) отримання однієї нової вершини рівня K-1 хешуванням двох сусідніх вершин рівня K.

Таким чином отримуємо дві цікаві властивості дерева хешів. Перша властивість полягає у тому, що зміна будь-якої транзакції в кінцевому випадку змінює і Merkle Root. Отже знання Merkle Root,

дозволяє миттєво виявити підроблені дані. Проте досягти цієї властивості можна і простішим способом, наприклад, застосувати операцію конкатенації до всіх транзакцій і потім застосувати хеш-функцію до результату [3].

Цікавішою є друга властивість, яку будемо називати proof of existence (доказ існування). Ідея полягає у такому. Нехай необхідно довести, що певна транзакція наявна у блокчейні, проте людина, яку необхідно в цьому переконати, немає копії блокчейну, а має лише Merkle Root. Звичайно, можна надати цій людині весь блок, щоб вона змогла розрахувати Merkle Root на основі цього блоку і переконатися, що транзакція дійсно існує. Проте, це буде не дуже ефективно. Кращим і ефективнішим є таке рішення: нехай потрібно довести, що транзакція C присутня у блоці. Для цього необхідно надати саму транзакцію, Merkle Path, в такому випадку це будуть вершини C, hash (D), hash (AB). Маючи ці вершини, користувач може самостійно зробити всі обчислення, аж до Merkle Root, таким чином:

1) обчислити хеш транзакції C, отримати hash (C);

2) застосувати конкатенацію до hash (C) і hash (D) — отримати hash (CD);

3) застосувати конкатенацію до hash (AB) і hash (CD) — отримати hash (ABCD);

4) перевірити, чи збігається отриманий hash (ABCD) з існуючим Merkle Root.

Таким чином, Merkle Tree дозволяє сформувати доказ існування транзакції в певному блоці, цей механізм має логарифмічну складність (як за пам'яттю, так і за часом) та вимагає від користувача знання лише Merkle Root конкретного блоку [4], [5].

Proof of work

Кожен блок у біткоїн блокчейні має цікаву властивість — його хеш є дуже малим числом, отже починається з великої кількості нулів. Це не випадково, майнери спеціально перебирають деякі параметри блоку таким чином, щоб його хеш мав таку властивість. Цей процес називається Proof of Work. Таким чином, отримання блоку з такою властивістю свідчить, що над ним була виконана велика кількість PoW, що в свою чергу гарантує (з високою долею ймовірності), що цей блок є справжнім (існує в блокчейні, не підроблений). Підробка такого блоку все ще можлива, проте це вимагає значних ресурсів і потенційному зловмиснику доцільніше/ефективніше направити ці ресурси на майнінг біткоїнів згідно з протоколом біткоїну [6].

Розв'язання поставленої задачі за допомогою описаних механізмів

Нагадаємо, що необхідно транспортувати 1 BTC з біткоїн блокчейну до іншого блокчейну, у спосіб, що не вимагає довіри від інших учасників. Транспортування біткоїну складається з таких кроків:

1) створення транзакції на біткоїн блокчейні, що знищує 1 BTC та має спеціальний формат;

2) формування Proof of Existence (доказу існування) на основі Merkle Path;

3) створення транзакції на допоміжному блокчейні, яка буде складатися з таких основних елементів:

– серіалізована транзакція з біткоїн блокчейну;

– доказ існування цієї транзакції;

– заголовок блоку, в якому присутня ця транзакція, та ще п'ять наступних заголовків блоків;

4) валідація транзакції на допоміжному блокчейні, що складається з таких кроків:

– перевірка за допомогою покажчиків у заголовку блоку того, що транзакції дійсно утворюють ланцюг блоків.

– валідація Proof of Work, що надає досить суттєві гарантії, що цей ланцюг блоків дійсно присутній у блокчейні.

– валідація Merkle Proof (доказ існування транзакції).

– десеріалізація транзакції, та перевірка того, що вона відповідає формату, зазначеному в протоколі.

Детальна ілюстрація задачі транспортування біткоїну

Розглянемо вищезапропонований спосіб транспортування біткоїну на прикладі. Для полегшення сприйняття зробимо декілька припущень, а саме, будемо представляти серіалізовану транзакцію як два байти, також у якості хеш-функції будемо використовувати SHA256, проте з результату будемо брати лише перші два байти. Протягом усього розділу будемо використовувати hex-encoding.

Створення транзакції на біткоїн блокчейні, що знищує один біткоїн

На рис. 2 показаний приклад транзакції, що знищує один біткоїн.

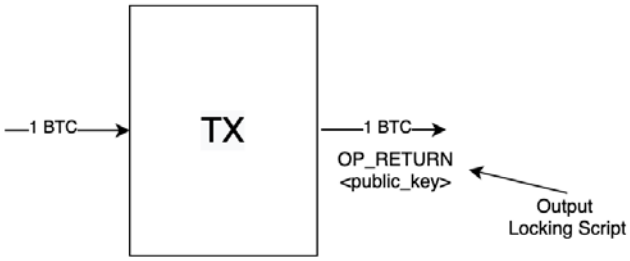

Рис. 2. Транзакція, що знищує один біткоїн

Щодо цієї транзакції необхідно звернути увагу такі дві основні речі:

1) Сценарій блокування (locking script) містить у собі спеціальний «опкод» OP_RETURN, призводячи до того, що цей біткоїн неможливо витратити у майбутньому, іншими словами він знищений. Це відбувається тому, що, який би сценарій розблокування не був поданий на вхід, транзакція завершиться за виключенням (помилкою) оскільки OP_RETURN завжди викликає виключення (“throw exception”). Цікавим, є те що всі подальші «опкоди», після OP_RETURN не мають жодного впливу на хід виконання транзакції, вони можуть лише слугувати як певна метаінформація.

2) Публічний ключ (public_key) слугує ідентифікатором людини, що знищила один біткоїн. Таким чином альтернативна одному біткоїну вартість може бути зарахована на новому блокчейні на певний публічний ключ [7].

Формування доказу існування (proof of existence) на основі шляху Меркла (Merkle path)

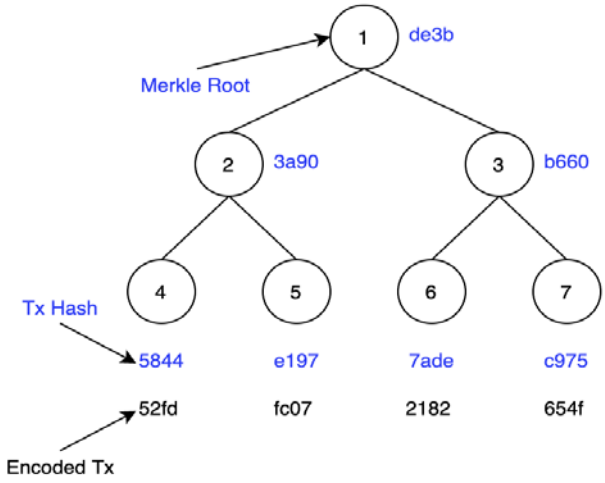

Рис. 3. Дерево Меркла, що містить транзакцію, яка знищує один біткоїн

На рис. 3 зображено приклад дерева Меркла, з яким працюватимемо.

Для наочності зробимо припущення, що блок з номером *N* складається з чотирьох транзакцій, які у закодованому вигляді мають такий вигляд: 52fd, fc07, 2182, 654f. Доказ існування (proof of existence) для транзакції 52fd буде складатися з чотирьох вершин, а саме: 52fd, e197, b660, de3b.

Перевірка доказу існування (proof of existence) на основі шляху Меркла (Merkle path)

Ілюстрацію прикладу перевірки доказу існування (proof of existence) для заданої транзакції, наведено на рис 4.

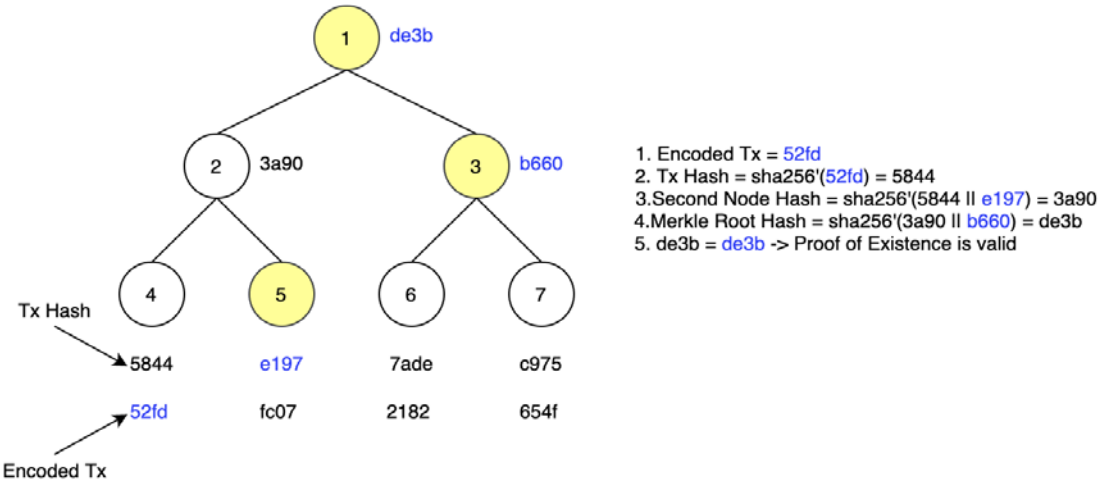

Рис. 4. Перевірка доказу існування (proof of existence) для заданої транзакції

Як зазначено вище, доказ існування (proof of existence) для транзакції 52fd складається з чотирьох вершин, а саме: 52fd, e197, b660, de3b. Для його перевірки (валідації) необхідно виконати такі дії:

1. Хешування транзакції за допомогою алгоритму SHA256', отримання значення хешу — 5844.
2. Конкатенація отриманого значення з e197 і нове хешування отримання значення хешу — 3a90.
3. Конкатенація отриманого значення з b660 і нове хешування отримання значення хешу — de3b.
4. Перевірка того, що отримане значення de3b збігається з останнім значенням у доказі існування [2], [8].

Створення транзакції на допоміжному блокчейні

Основні елементи транзакції на допоміжному блокчейні показані на рис. 5.

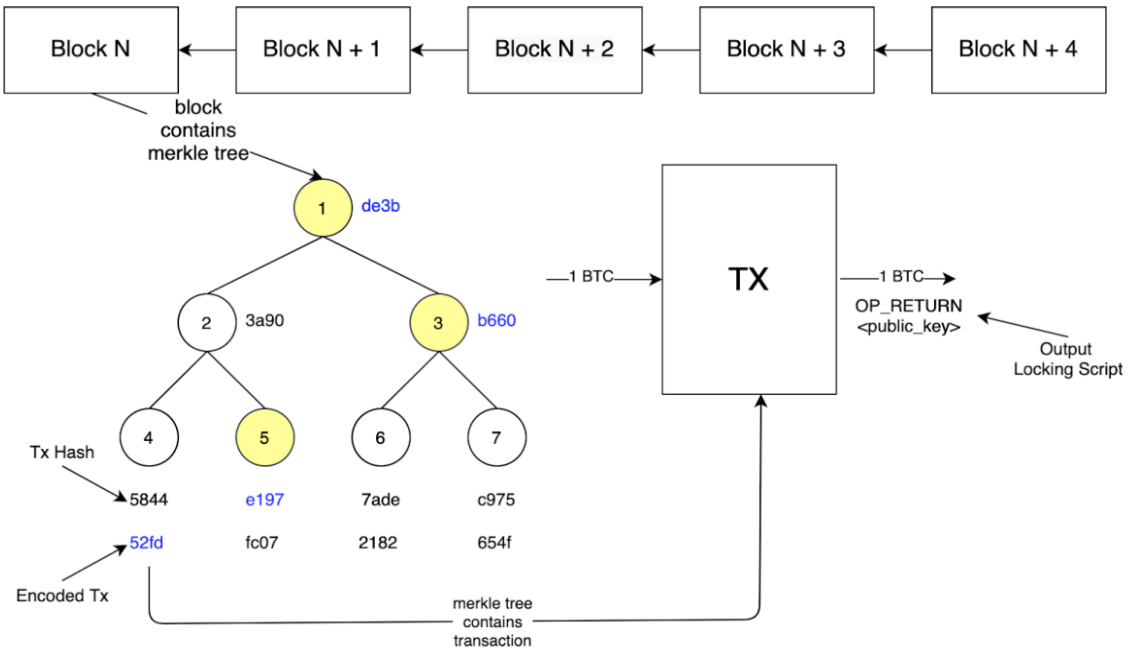

Рис. 5. Основні елементи транзакції на допоміжному блокчейні

Транзакція на допоміжному блокчейні складатиметься з таких основних елементів:

1. Ланцюг заголовків блоків, починаючи з блоку *N* (який містить у собі необхідну нам транзакцію) до блоку *N* + 4.
2. Доказ існування (на основі дерева Меркла для блоку з номером *N*) — e197, b660, de3b.
3. Закодована транзакція 52fd, доказ існування якої наведений у пункті 2.
4. У свою чергу транзакція містить кількість знищених біткоїнів (у цьому випадку один біткоїн) та публічний ключ, що слугує унікальним ідентифікатором людини.

Смарт-контракт на допоміжному блокчейні буде дотримуватися такого алгоритму:

1. Перевірити доказ роботи (proof of work) для усіх п’яти блоків.
2. Перевірити доказ існування (proof of existence) для транзакції 52fd.
3. Декодувати транзакцію 52fd, отримати з декодованої транзакції кількість знищених біткоїнів та публічний ключ.
4. У допоміжному блокчейні нарахувати на отриманий публічний ключ суму, еквівалентну сумі знищених біткоїнів.

Недоліки допоміжних блокчейнів (sidechain)

1. Не до кінця зрозумілий механізм транспортування біткоїну з допоміжних блокчейнів назад у блокчейн. Можна використовувати вищезгаданий механізм проте, це вимагає удосконалення мови смарт-контрактів bitcoin-a. Оскільки важко чи навіть не можливо імплементувати алгоритм валідації Merkle Proof та PoW на стековій мові програмування Bitcoin Script. Також можна розглянути більш високорівневі мови програмування, що компілюються у Bitcoin Script, проте на сьогодні не зрозуміло чи цього достатньо.

2. Ускладнюється та потребує суттєвих змін користувацький інтерфейс. Оскільки у такій конфігурації користувач може володіти кількома активами у декількох допоміжних блокчейнах. Вводяться поняття тимчасово заблокованих активів тощо.

3. Потребує додаткового аналізу явище реорганізації біткоїн блокчейну, оскільки це може мати побічні ефекти на допоміжні блокчейни.

Висновки

Розглянуто механізм допоміжних блокчейнів та сформульовано основну проблему яка стоїть перед розробниками — розробка trustless (що не вимагає довіри) механізму транспортування біткоїнів між блокчейнами.

Детально проаналізовано низку існуючих алгоритмів, таких як доказ роботи (proof of work), дерево Меркла, доказ існування (proof of existence) тощо.

Вперше запропоновано детальний алгоритм транспортування біткоїнів з одного блокчейну на інший, що здебільшого базується на структурі даних «дерево Меркла» та ідеї «доказу роботи». Наведені та роз'ясненні основні етапи цього алгоритму.

Покроково описано як формування транзакції на допоміжному блокчейні, так і її валідація з боку смарт-контракту. Наведено детальну схему транзакції на допоміжному блокчейні з її основними елементами, а саме: ланцюг заголовків блоків (над якими виконана певна кількість доказу роботи), доказ існування на основі дерева Меркла, закодована транзакція з біткоїн блокчейну.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2009. [Electronic resource]. Available: https://bitcoin.org/bitcoin.pdf .

[2] BitFury Group, "Smart Contracts on Bitcoin Blockchain," 2015. [Electronic resource]. Available: https://bitfury.com/content/downloads/contracts-1.1.1.pdf .

[3] Hellgirl34, Artillar, BeckyMH, "Merkle tree," 2017. [Electronic resource]. Available: https://en.bitcoinwiki.org/wiki/Merkle_tree .

[4] Hanniabu, Artillar, BeckyMH, "Simplified Payment Verification," 2017 [Electronic resource]. Available: https://en.bitcoinwiki.org/wiki/Simplified_Payment_Verification .

[5] Artillar, Becky. "Smart contract," 2017. [Electronic resource]. Available: https://en.bitcoinwiki.org/wiki/Smart_contract .

[6] Artillar, BeckyMH, "Bitcoin mining," 2017. [Electronic resource]. Available: https://en.bitcoinwiki.org/wiki/Bitcoin_mining .

[7] Mike Hearn, and Matt Corallo, "Connection Bloom filtering," 2012. [Electronic resource]. Available: https://github.com/bitcoin/bips/blob/master/bip-0037.mediawiki .

[8] Olaoluwa Osuntokun, Alex Akselrod, and Jim Posen, "Client Side Block Filtering," 2017. [Electronic resource]. Available: https://github.com/bitcoin/bips/blob/master/bip-0157.mediawiki .

Рекомендована кафедрою комп'ютерних наук ВНТУ

Стаття надійшла до редакції 16.03.2021

Щербіна Євгеній Сергійович — аспірант кафедри комп'ютерних наук, e-mail: evgeniy.shcherbina.es@gmail.com ;

Месюра Володимир Іванович — канд. техн. наук, доцент, професор кафедри комп'ютерних наук, e-mail: mesyura@vntu.edu.ua .

Вінницький національний технічний університет, Вінниця

E. S. Shcherbina[1]
V. I. Mesyura[1]

Mechanisms of Blockchains Integration with Each Other

[1]Vinnytsia National Technical University

This paper considers the need for blockchain integration and the problems that arise along the way. The idea of transporting bitcoins by destroying them on one blockchain and creating a corresponding value on another blockchain is considered.

A brief description of such concepts as bitcoin transaction and bitcoin block is given. The Merkle Tree data structure, its

internal organization, and its benefits are described in detail. The algorithm for constructing a “Merkle Tree” for a block of transactions and the principle of constructing and verifying a “Merkle Path” for a given transaction are presented. Describes what is behind the concept of "proof of work" (Proof of Work) from both a technical and economic point of view.

For the first time, a detailed algorithm for transporting bitcoins from one blockchain to another was proposed, which is mostly based on the data structure of the "Merkle tree" and the idea of "proof of work". The four main stages of this algorithm are given and explained. The scheme of the transaction destroying one bitcoin is resulted, its locking script is considered. A real example illustrates the creation and verification proof of existence of a transaction based on the Merkle tree. Given the detailed scheme of the transaction on the auxiliary blockchain, with its basic elements, namely: a chain of block headers, proof of existence based on the Merkle tree, encoded transaction from bitcoin blockchain. The connections between these elements are given and the algorithm of formation of the above-mentioned transaction is considered. The algorithm of transaction validation on the auxiliary blockchain from the point of view of the smart contract is considered step by step.

The disadvantages of the idea of integrating blockchains with each other are described.

Keywords: cryptocurrency, bitcoin, blockchain, sidechain, blockchain integration, Merkle tree, smart contract, proof of work.

Shcherbina Evgeniy S. — Post-Graduate Student of the Chair of Computer Science, e-mail: evgeniy.shcherbina.es@gmail.com ;

Mesyura Volodymyr I. — Cand. Sc. (Eng), Associate Professor, Professor of the Chair of Computer Science, e-mail: mesyura@vntu.edu.ua

Е. С. Щербина[1]
В. И. Месюра[1]

Механизм интеграции блокчейнов друг с другом

[1]Винницкий национальный технический университет

Рассмотрена необходимость интеграции блокчейнов и проблемы, которые возникают на этом пути. Рассматривается идея транспортировки биткойнов путем их уничтожения в одной цепочке блоков и создания соответствующего значения в другой цепочке блоков.

Дано краткое описание таких понятий, как биткойн-транзакция и биткойн-блок. Подробно описывается структура данных Merkle Tree, ее внутренняя организация и преимущества. Представлен алгоритм построения «Дерева Меркла» для блока транзакций и принцип построения и проверки «Пути Меркла» для этой транзакции. Описано, что стоит за концепцией «доказательство работы» (Proof of Work) как с технической, так и с экономической точки зрения.

Впервые был предложен подробный алгоритм транспортировки биткойнов из одного блокчейна в другой, который в большей степени основан на структуре данных «дерево Меркла» и идее «доказательства работы». Приводятся и объясняются четыре основных этапа этого алгоритма. Приведена схема транзакции, уничтожающая один биткойн, рассмотрен ее сценарий блокировки (locking script). Приведен реальный пример, который иллюстрирует создание и проверку доказательства существования (proof of existence) транзакции на основе дерева Меркла (Merkle tree). Приведена подробная схема транзакции на вспомогательном блокчейне, с ее основными элементами, а именно: цепочка заголовков блоков, доказательство существования (proof of existence) на основе дерева Меркла (Merkle tree), закодированная транзакция из биткойн блокчейна. Приведены связи между этими элементами и рассмотрен алгоритм формирования указанной транзакции. Поэтапно рассмотрен алгоритм проверки транзакции на вспомогательном блокчейне с точки зрения смарт-контракта.

Описаны недостатки идеи интеграции блокчейнов друг с другом.

Ключевые слова: криптовалюта, биткойн, блокчейн, сайдчейн, интеграция блокчейнов, дерево Меркла, смарт-контракт, доказательство работы.

Щербина Евгений Сергеевич — аспирант кафедры компьютерных наук, e-mail: evgeniy.shcherbina.es@gmail.com ;

Месюра Владимир Иванович — канд. техн. наук, доцент, профессор кафедры компьютерных наук, e-mail: mesyura@vntu.edu.ua