https://doi.org/10.31649/1997-9266-2020-153-6-93-99

УДК 004.42

Є. С. Щербіна[1]
В. І. Месюра[1]

ПОШУК ОПТИМАЛЬНОГО МАРШРУТУ ПЛАТЕЖУ У LIGHTNING NETWORK

[1]Вінницький національний технічний університет

Розглянуто проблему масштабування біткойн блокчейну та основні методи її вирішення. Описано основні методи вирішення цієї проблеми, такі як: SPV-вузли (Simplified Payment Verification), SegWit, допоміжні блокчейни (sidechains) та Лайтнінг мережа (Lightning Network). Наведено переваги та недоліки вищезгаданих підходів.

У статті наведені деталі технічного влаштування мережі Lighting Network, механізм якої дозволяє уникати запису кожної транзакції на блокчейн. Описані такі ключові концепції як непідтверджені транзакції, механізм захисту від подвійної витрати (double spend), мультипідпис, тимчасові блокування, хеші і секрети. Розглянуто процес відкриття каналу та здійснення лайтнінг транзакції. Надано та проаналізовано вихідний код програм на стековій мові програмування Bitcoin Scrypt, що використовуються під час здійснення лайтнінг (lightning) транзакцій.

В рамках статті запропоновано моделі, зручні для опису мережі лайтнінг (lightning), а саме графова та мережева модель. Графова модель має на увазі проведення платежу вздовж одного шляху, в свою чергу мережева модель має на увазі розбиття платежу на декілька платежів меншого розміру (можливо з використанням алгоритму AMP (Atomic Multipath Payment).

У статті розглянуто задачі, з якими стикаються розробники гаманців для Lightning Network, а саме знаходження розміру максимального платежу, який може бути проведений за певних умов (з довільною або фіксованою кількістю посередників) та проведення платежу фіксованого розміру з мінімально можливою комісією. Здійснено їх формалізацію в термінах теорії графів за допомогою розроблених моделей. Запропоновано детальний алгоритм розв'язання формалізованих задач, з використанням алгоритмів бінарного пошуку, алгоритму пошуку у ширину та алгоритму пошуку потоку мінімальної вартості (min-cost-max-flow).

Ключові слова: криптовалюта, біткоїн, блокчейн, лайтнінг, теорія графів, алгоритми на графах, пошук найкоротшого шляху.

Вступ

Фундаментальною проблемою біткоїн блокчейну та блокчейнів узагалі є проблема масштабування. У класичному блокчейні кожна транзакція має бути записана на блокчейн, що має бути розповсюджений серед тисяч учасників мережею Internet. Це призводить до того, що розробники протоколів змушені закладати певні обмеження на кількість транзакцій, до прикладу, у біткоїн блокчейні — це приблизно 7 транзакцій у секунду. Існує велика кількість різноманітних підходів до масштабування біткоїн блокчейну. Частина з них направлена на те, щоб кінцевий користувач був не зобов'язаний слідкувати за усім блокчейном, а лише за невеликою його частиною як, наприклад, SPV-вузли, або Electrumx сервери тощо. Такі підходи вже не є повністю «не вимагаючими довіри» (trustless), проте пропонують досить високий рівень захисту.

Існують спроби оптимізувати розмір блокчейну, за допомогою зменшення розміру серіалізованої транзакції. Одним з таких прикладів є механізм SegWit. Такі рішення є повністю «не вимагаючими довіри», проте дозволяють збільшити пропускну здатність лише на приблизно 10…30 %.

Фундаментальними є рішення, побудовані на основі протоколів допоміжного блокчейну (sidechain) або за допомогою протоколу Лайтнінг (Lightning) Network, якому приділено основну увагу в статті.

Графова модель Lightning Network

В термінах теорії графів користувач мережі може бути представлений вершиною графу. При цьому відкритий канал між двома людьми зручно подати орієнтованим ребром графу. З кожним ребром у графі асоціюємо одне число, яке подаватиме кількість замкнених біткоїнів. Протокол Лайтнінг (Lightning) Network надає можливість провести платіж між двома вершинами A та B, якщо існує відповідний маршрут у графі.

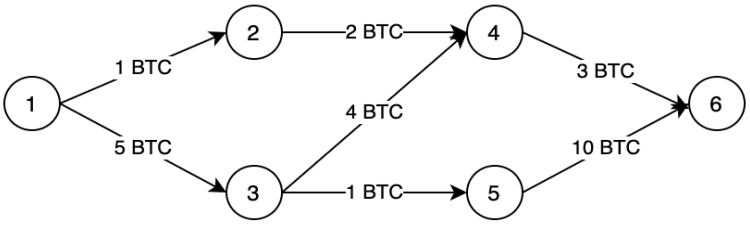

Рис. 1. Графова модель

Зауважимо, що розмір платежу не має перевищувати кількість замкнених біткоїнів на будь-якому ребрі графа.

Для зручності будемо позначати асоційоване з ребром число літерою K, а мінімальне значення K на певному шляху MIN_K.

Наприклад, на рис. 1, максимальний розмір платежу, що може бути проведений між вершинами 1 та 6 дорівнює 3 BTC. Оптимальний маршрут $1 \to 3 \to 4 \to 6$, згідно з нашими позначеннями K1 = 5 BTC, K2 = 4 BTC, K3 = 3BTC → MIN_K = 3 BTC.

Мережева модель Lightning Network

З іншої сторони при графовому поданні платіжної мережі Лайтнінг (Lightning) Network, кожне ребро має як пропускну здатність так і вартість. Вершина уособлює собою людину, а ребро — платіжний канал, в рамках якого здійснюється платіж, пропускна здатність вимірюється кількістю біткоїнів, замкнених у каналі, а вартість є комісією (fee).

Платіж у графовій моделі Лайтнінг (Lightning) Network подається шляхом у мережі. Якщо ми хочемо провести платіж розміром 1 BTC усі ребра на шляху повинні мати пропускну здатність більшу або рівну одному BTC, до того ж, під час проходження платежу на кожному ребрі сплачується комісія.

Постановка, обґрунтування та розв'язання задач з погляду кінцевого користувача

Розглянемо, стандартні задачі з погляду кінцевого користувача та те, як вони проєктується на запропоновані моделі.

Задача 1

Відображення в інтерфейсі користувача максимального розміру платежу, який він може провести у певний момент (довільна кількість посередників).

Обґрунтування задачі: ця функція була б дуже зручною для Лайтнінг (Lightning) Network wallet, оскільки гаманець (wallet) міг би для будь-якого з контактів користувача розрахувати і відобразити розмір платежу, що може бути проведений до цього контакту.

Постановка задачі в термінах теорії графів: дано графову модель мережі Лайтнінг (Lightning). Знайти максимальне, натуральне число N таке, за якого існує шлях з точки A в точку B, такий, що $N \le$ MIN_K.

Запропонований алгоритм розв'язання задачі: у цій задачі можна використати бінарний пошук по результату шляхом перебору результатів REZ у діапазоні $L = 0$, $R = 100$ BTC. В рамках цієї статті верхня межа вибрана довільно, проте 100 BTC здається обґрунтованим припущенням.

На першій ітерації виберемо REZ = 50BTC, на другій — 25BTC або 75BTC і так далі. Після фіксації REZ, викинемо з графу усі ребра для яких $K <$ REZ. Якщо у модифікованому графі існує шлях, збільшуємо ліву границю — L = REZ, якщо ні, то зменшуємо праву — R = REZ – 1.

Розглянемо це на прикладі. Нехай надано вихідний граф, зображений на рис. 1. На деякій ітерації зафіксовано, що REZ = 4 BTC, після відкидання ребер згідно з алгоритмом отримаємо граф, зображений на рис. 2. За допомогою пошуку в глибину перевіримо, що шляху між вершинами 1 та 6 не існує, це означає, що необхідно зменшити праву границю R = REZ – 1 = 3 BTC і перейти до наступної ітерації.

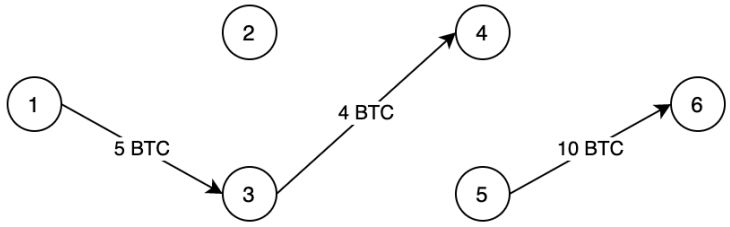

Рис. 2. Графова модель після відкидання ребер

Перевірити наявність шляху в орієнтованому, незваженому графі можна, наприклад, за допомогою алгоритму DFS. Нескладно зрозуміти, що в певний момент L буде дорівнювати R — це і є шуканий результат. Асимптотика алгоритму $O\left(\log R \cdot \left(N + M\right)\right)$, де N та M — кількість вершин та ребер, відповідно.

Задача 2

Відображення в інтерфейсі користувача максимального розміру платежу, який він може провести у певний момент (фіксована кількість посередників).

Обґрунтування задачі: мінімальна кількість посередників є досить зрозумілою вимогою, оскільки кожен наступний посередник зменшує вірогідність успішного проходження платежу. Наприклад, уявимо, що ми маємо мережу, в якій усі посередники мають надійність 90 % (вони коректно відповідають у 90 % випадках). Можемо помітити, що у випадку двох посередників, імовірність проведення платежу дорівнює 81 %, трьох — 72,9 % і т. д. Тобто вірогідність не тільки зменшується, а робить це експоненціально.

*Постановка задачі в термінах теорії графів***:** дано графову модель мережі Лайтнінг (Lightning). Знайти таке максимальне, натуральне число N, за якого існує шлях з точки A в точку B, такий, що $N \geq$ MIN_K і довжина шляху не перевищує деяку величину PATH_LEN.

Запропонований алгоритм розв'язання задачі: розв'язання аналогічне попередній задачі, проте необхідно перевіряти не тільки наявність шляху, а також і те, що його довжина не перевищує PATH_LEN. Знайти найкоротший шлях в орієнтованому, незваженому графі, можна за допомогою алгоритму BFS [1].

Задача 3

Провести платіж фіксованого розміру, з мінімальною комісією.

*Обґрунтування задачі***:** не потребує особливого обґрунтування, оскільки є базовою функціональністю будь-якого Lightning Wallet-а.

Постановка задачі в термінах теорії графів: дано мережеву модель мережі Лайтнінг (Lightning). Знайти максимальний потік мінімальної вартості.

Запропонований алгоритм розв'язання задачі: власне розв'язання задачі вже викладено у постановці задачі та у описі мережевої моделі. Таким чином, правильно застосовано модель та переформулювання задачі автоматично звело нашу проблему до досить відомого алгоритму min-cost-max-flow [2].

Технічний устрій мережі Lightning Network

Для глибокого розуміння мережі Лайтнінг (Lightning) Network передусім необхідно зрозуміти основні елементи на яких вона базується.

Елемент 1: непідтверджені транзакції. Взагалі транзакція складається з входів та виходів. Виходи мають два атрибути: Amount та LockingScript. Amount — кількість сатоші (дрібної частини біткойна), LockingScript — умови витрати цієї кількості сатоші.

Умови витрати — це довільний смарт-контракт, який зазвичай є досить простим. Наприклад він вимагає знання приватного ключа, що відповідає певному публічному ключу, або знання прообразу (preimage) для певного хешу, тощо.

Входи складаються з чотирьох атрибутів PreviousOutPoint, SignatureScript, Witness, Sequence.

PreviousOutPoint — це посилання на UTXO (Unspent Transaction Output), детальніше PreviousOutPoint складається з TxHash та OutputIndex. SignatureScript, Witness — містять так званий UnlockingScript або іншими словами — умови розблокування. Sequence використовується разом з OP_CSV опкодом [3].

Зазвичай транзакції після створення та підписання відразу поширюються мережею біткоїн та незабаром потрапляють у блокчейн, проте ідея непідтверджених транзакцій полягає у тому, що учасники обмінюються сформованими та підписаними транзакціями мережею Internet (наприклад

по протоколу TCP), у блокчейн транзакція посилається лише у крайньому випадку. В контексті непідтверджених транзакцій варто згадати SegWit [4]—[6].

SegWit — це розширення, що дозволяє будувати непідтверджені ланцюги транзакцій довжиною більше одиниці. Мається на увазі, що ми можемо сформувати непідтверджені транзакції, входи яких посилаються на непідтверджені транзакції і т.д.

Елемент 2: механізм захисту від подвійної витрати (Double Spend). Другий елемент Лайтнінг (Lightning) Network не потребує детальних пояснень, тому що це сенс існування самого біткоїна: захист від подвійної витрати.

Якщо дві транзакції (або, скоріше, два входи) надсилаються на той самий вихід, тільки одна з них може бути підтверджена майнерами. Важливо розуміти, що конфліктувати можуть навіть непідтверджені транзакції ще до підтвердження однієї з них.

Елемент 3: мультипідпис. Ідея мультипідпису є досить простою, існує можливість створювати такі виходи, розблокування яких вимагає знання певної підмножини приватних ключів. Мультипідпис — це один з прикладів застосування смарт-контрактів.

У протоколі Лайтнінг (Lightning) Network активно використовується так званий 2-of-2 multisig (мультипідпис), що означає необхідність двох підписів з двох.

Елемент 4: тимчасові блокування. Тимчасові блокування дають можливість створювати виходи, витратити які буде можливо в певний час в майбутньому. Існує два основні типи тимчасових блокувань CLTV та CSV. CLTV або OP_CHECKLOCKTIMEVERIFY — це блокування виходу до певного абсолютного часу або певного номера блоку. CSV або OP_CHECKSEQUENCEVERIFY — це відносне блокування, передбачається, що ви можете витратити вихід через *N* блоків після попадання і підтвердження транзакції з цим UTXO у блокчейні. Детальну специфікацію цих опкодів наведено у [3], [7].

Елемент 5: хеши і секрети. Хеши і секрети — це ще один спосіб використання смарт-контрактів біткоїна. А саме у Locking_Script виходу замикається певний хеш, а для розблокування цього UTXO необхідно знати секрет, який відповідає цьому хешу. Така ідея використовується у HTLC (Hashed Time-Locked Contract transactions) [8].

Перше завдання: двонаправлені платіжні канали. Ідея платіжних каналів обговорювалася ще до Лайтнінг (Lightning) Network. Безумовно, звичайні платіжні канали корисні, але обмежені: вони односпрямовані. Ключова особливість Лайтнінг (Lightning) Network — це двонаправлені платіжні канали «без довіри».

Відкриття каналу

Для початку необхідно сформувати відкриваючу транзакцію, яка є 2-of-2 multisig, зазвичай з декількома входами, що належать сторонам, які відкривають між собою канал, та двома виходами, один з яких — це 2-of-2 multisig а інший — решта.

2-of-2 multisig має такий вихідний код:

2 <pubkey1> <pubkey2> 2 OP_CHECKMULTISIG

Окрім відкриваючої транзакції для відкриття каналу необхідно також сформувати і так звані зобов'язуючі (commitment) транзакції (кожна сторона повинна мати свою commitment транзакцію, що має бути підписана іншою стороною). Зазвичай commitment транзакція має один вхід та два виходи. Вхід — це 2-of-2 multisig вихід відкриваючої транзакції, а виходи, відповідно, належать учасникам каналу.

Пояснимо сказане на прикладі. Нехай Alice та Bob хочуть відкрити між собою канал на 10 BTC, при цьому кожен зі своєї сторони вкладає по 5 BTC. Отже у найпростішому випадку формується відкриваюча транзакція з двома входами (по 5 BTC) і одним виходом 10BTC. Окрім того, формується пара зобов'язуючих (commitment) транзакцій.

Зобов'язуюча (commitment) транзакція для Alice має один вхід та два виходи, вхід — це 2-of-2 multisig виходу відкриваючої транзакції, вихід — це звичайний p2wkh для Bob з 5 BTC та з 5 BTC, замкнутому у спеціальному смарт-контракті. Біткоїни з цього смарт контракту можливо вивести двома способами, перший — це може зробити Alice, коли спливе CSV timelock, або Bob, знаючи секрет Alice.

Лайтнінг транзакція

Лайтнінг (Lightning) транзакція — це процес, який складається з двох основних етапів, першим — створення нових зобов'язуючих транзакцій, а другим — скасування попередніх зобов'язуючих транзакцій. Створення нових зобов'язуючих транзакцій на етапі лайтнінг (lightning) транзакцій не відрізняється від створення початкових зобов'язуючих транзакцій на етапі відкриття каналу.

Скасування зобов'язуючих транзакцій є розголошенням секретів з попереднього раунду. Технічно сторона все ще може підписати та поширити мережею застарілу зобов'язуючу транзакцію, проте, це не має сенсу, оскільки протилежна сторона знає секрет та може забрати усі замкнуті кошти.

Оскільки зобов'язуюча транзакція є одним з основних будівельних блоків на яких будується лайтнінг (Lightning) Network розглянемо її детальніше.

Вихідний код програми, що замикає UTXO, який належить Алісі:

```
OP_IF
   # Penalty transaction
   <revocationpubkey>
OP_ELSE
   `to_self_delay`
   OP_CSV
   OP_DROP
   <local_delayedpubkey>
OP_ENDIF
OP_CHECKSIG
```

Отже, ми бачимо що LockingScript має два основні розгалуження, в якості Unlocking Script ми можемо використовувати такі варіанти:

1) <revocation_sig> 1 — забрати гроші (іншою стороною), використавши попередньо отриманий (на стадії розголошення секретів) revocation_key.

2) <local_delayedsig> 0 — забрати гроші, використовуючи свій ключ після CSV затримки.

Multi-Hop транзакція — це дуже потужна особливість Lightning Network, що дозволяє здійснювати лайтнінг (Lightning) транзакції між сторонами, які не мають прямого каналу між собою. А саме уявімо, що ми маємо два канали Alice → Bob та Bob → Carol. Ідея полягає у тому, коли Alice хоче заплатити Carol, вона може зробити це через Bob, Alice дасть 1 біткоїн Bob (в рамках свого каналу), а Bob дасть 1 біткоїн Carol в рамках свого каналу. Таким чином баланс Alice зменшиться на 1 біткоїн, баланс Bob не змінюється, а баланс Carol збільшиться на 1 біткоїн, що й нам і було необхідно.

Висновки

Розглянуті задачі, які постають перед розробниками гаманців для Лайтнінг (Lightning) Network. Розроблено графову модель для Лайтнінг (Lightning) Network, яка дозволяє звести задачу пошуку маршруту проведення платежу до пошуку шляху в орієнтованому графі. Вперше запропоновано мережеву модель для Лайтнінг (Lightning) Network, яка дозволяє звести задачу пошуку маршруту проведення платежу до відомої і проаналізованої задачі пошуку максимального потоку або пошуку максимального потоку мінімальної вартості.

Вперше запропоновано алгоритм, що поєднує у собі використання графової моделі та бінарного пошуку за результатом для розв'язання задачі знаходження максимального розміру платежу, який може бути проведений за певних умов.

Розроблено алгоритм для розв'язання задачі знаходження максимального розміру платежу, за умови, що кількість посередників не перевищує заздалегідь заданої величини.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] «Пошук у ширину,» *Електронний журнал MAXimal*, 2008. [Електронний ресурс]. Режим доступу: https://e-maxx.ru/algo/bfs.

[2] «Потік мінімальної вартості,» Електронний журнал MAXimal, 2008. [Електронний ресурс]. Режим доступу: https://e-maxx.ru/algo/min_cost_flow .

[3] Btc Drak, Mark Friedenbach, and Eric Lombrozo, "CHECKSEQUENCEVERIFY," 2015. [Electronic resource]. Available: : https://github.com/bitcoin/bips/blob/master/bip-0112.mediawiki .

[4] Eric Lombrozo, Johnson Lau, and Pieter Wuille, “Segregated Witness (Consensus layer) ,” 2015. [Electronic resource]. Available: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki .

[5] Johnson Lau, and Pieter Wuille, “Transaction Signature Verification for Version 0 Witness Program,” 2016. [Electronic resource]. Available: https://github.com/bitcoin/bips/blob/master/bip-0143.mediawiki .

[6] Eric Lombrozo, and Pieter Wuille, “Segregated Witness (Peer Services),” 2016. [Electronic resource]. Available: https://github.com/bitcoin/bips/blob/master/bip-0144.mediawiki .

[7] Peter Todd, “OP_CHECKLOCKTIMEVERIFY,” 2014. [Electronic resource]. Available: https://github.com/bitcoin/bips/blob/master/bip-0065.mediawiki .

[8] Sean Bowe, and Daira Hopwood, “Hashed Time-Locked Contract transaction,” 2017. [Electronic resource]. Available: https://github.com/bitcoin/bips/blob/master/bip-0199.mediawiki .

Рекомендована кафедрою комп’ютерних наук ВНТУ

Стаття надійшла до редакції 21.12.2020

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]

Finding the Optimal Payment Route in the Lightning Network

[1]Vinnytsia National Technical University

The article is devoted to the problem of scaling the bitcoin blockchain and the main methods of its solution. The main methods of solving this problem are described, such as SPV (simplified payment verification) — nodes, SegWit, auxiliary blockchains (sidechains) and Lightning Network (Lightning Network). The advantages and disadvantages of the above approaches are presented.

The article provides details of the technical structure of the Lighting Network, the mechanism of which allows you to avoid writing each transaction on the blockchain. Key concepts such as unconfirmed transactions, double spend protection, multi-signature, temporary locks, hashes and secrets are described. The process of channel opening and lightning transaction are considered. The source code of Bitcoin Scrypt stack programming programs used during lightning transactions is provided and analyzed.

The article proposes models that are convenient for describing lightning network, namely graph and network model. The graph model involves making a payment along one path, in turn, the network model involves splitting the payment into several smaller payments (possibly using the algorithm AMP — atomic multipath payment).

The article describes the tasks faced by developers of wallets for Lightning Network, namely finding the size of the maximum payment that can be made under given conditions (with an arbitrary or fixed number of intermediaries) and making a fixed size payment with the minimum possible fee. Algorithms were formalized in terms of graph theory by the help of developed models. A detailed algorithm for solving formalized problems is proposed, using binary search, width search and min-cost-max-flow algorithms.

Keywords: cryptocurrency, bitcoin, blockchain, lightning, graph theory, graph algorithms, shortest path search.

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]

Поиск оптимального маршрута платежа в Lightning Network

[1]Винницкий национальный технический университет

Рассмотрена проблема масштабирования биткойн блокчейна и основные методы ее решения. Описаны основные методы решения этой проблемы такие как SPV-узлы (Simplified Payment Verification), SegWit, вспомогательные блокчейны (Sidechains) и Лайтнинг сеть (Lightning Network). Описаны преимущества и недостатки вышеупомянутых подходов.

В статье приведены детали технического устройства сети Lighting Network, механизм которой позволяет избегать записи каждой транзакции в блокчейн. Описаны такие ключевые концепции, как: неподтвержденные транзакции, механизм защиты от двойной траты (Double Spend), мультиподпись, временные блокировки, хэши и секреты. Рассмотрен процесс открытия канала и осуществления Лайтнинг транзакции. Представлен и проанализирован исходный код программ на стековом языке программирования Bitcoin Scrypt, используемый при осуществлении Лайтнинг (Lightning) транзакций.

В рамках статьи предложены модели, удобные для описания сети Лайтнинг (Lightning), а именно графовая и сетевая модель. Графовая модель подразумевает проведение платежа вдоль одного пути, в свою очередь сетевая модель подразумевает разбиение платежа на несколько платежей меньшего размера (возможно с использованием алгоритма AMP (Atomic Multipath Payment).

Рассмотрены задачи, с которыми сталкиваются разработчики кошельков для Lightning Network, а именно нахождения размера максимального платежа, который может быть проведен при данных условиях (с произвольным или фиксированным количеством посредников) и проведения платежа фиксированного размера с минимально возможной комиссией. Осуществлено их формализацию в терминах теории графов с помощью разработанных моделей. Предложен подробный алгоритм решения формализованных задач, с использованием алгоритмов бинарного поиска, алгоритма поиска в ширину и алгоритма поиска потока минимальной стоимости (min-cost-max-flow).

Ключевые слова: криптовалюта, биткоин, блокчейн, лайтнинг, теория графов, алгоритмы на графах, поиск кратчайшего пути.

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