Вестник ВГУИТ/ Proceedings of VSUET ISSN 2226-910X E-ISSN 2310-1202
DOI: http://doi.org/10.20914/2310-1202-2022-3-337-344 Оригинальная статья/Research article
УДК 004.273 Open Access Available online at vestnik-vsuet.ru

Принцип работы децентрализованной информационной системы денежных переводов

Людмила А. Коробова [1] lyudmila_korobova@mail.ru 0000-0003-1349-732X
Сергей С. Бондаренко [1] ss.bond.98@gmail.com
Дмитрий П. Мухин [1] dmitrymukhin.official@gmail.com

1 Воронежский государственный университет инженерных технологий, пр-т Революции, 19, г. Воронеж, 394036, Россия

Аннотация. Статья посвящена обозрению понятия blockchain при реализации децентрализованной системы денежных переводов. Рассмотрено понятие отказоустойчивости технологии криптовалюты и приведены некоторые аспекты решения отказоустойчивости. Проведен анализ информационной безопасности предприятий. Затронуты вопросы анонимности банковских систем. Показана зависимость анонимности банковской системы от качества программного обеспечения и от политики безопасности. Даются рекомендации решения проблемы анонимности, в частности генерация приватного ключа или встраивание алгоритма соединения транзакций. Рассмотрены подходы к созданию транзакций. Приведены примеры алгоритмов, позволяющих проводить защиту транзакций пользователей. Проведено описание структуры blockchain и алгоритма консенсуса. Рассмотрены вопросы генерации цепочки блоков честного пользователя и цепочки блоков злоумышленника. Проведена формализация оценки вероятности безубыточности транзакции. Для оценки использовано биноминальное случайное блуждание. Так же обосновано окончание процесса транзакции, как ожидание добавления новых блоков в цепочку честного пользователя. Для идентификации принадлежности транзакции публичному ключу используют цифровую подпись. Рассмотрены процессы подписания транзакции и проверки подписи. Отдельно выделены подходы, используемые при проектировании криптовалют. В сети хранится вся история транзакций, есть возможность рассчитать баланс общей суммы поступающих средств и трат денег. Данные подходы представляют собой программные решения, основанные на теории игр и криптографии. Главное внимание обращается на бизнес-ценности криптовалют и способы их достижения. В результате сформулирован необходимый функционал программного клиента. В статье проведен тщательный анализ нового финансово-расчетного инструмента – электронных денег. Задаче разработки виртуальной платежной системы в последнее время уделяется большое внимание.

Ключевые слова: блокчейн, децентрализованные системы, программирование, криптовалюта, крипта, транзакция, майнер.

The principle of operation of a decentralized money transfer information system

Lyudmila A. Korobova [1] lyudmila_korobova@mail.ru 0000-0003-1349-732X
Sergei S. Bondarenko [1] ss.bond.98@gmail.com
Dmitry P. Mukhin [1] dmitrymukhin.official@gmail.com

1 Voronezh State University of Engineering Technologies, Revolution Av., 19 Voronezh, 394036, Russia

Abstract. The article is devoted to reviewing the concept of blockchain in the implementation of a decentralized money transfer system. The concept of fault tolerance of cryptocurrency technology is considered and some aspects of the fault tolerance solution are given. The analysis of information security of enterprises was carried out. The questions of anonymity of banking systems are touched upon. The dependence of the anonymity of the banking system on the quality of the software and on the security policy is shown. Recommendations are given for solving the problem of anonymity, in particular, generating a private key or embedding an algorithm for connecting transactions. Approaches to creating transactions are considered. Examples of algorithms that allow protecting user transactions are given. The description of the blockchain structure and the consensus algorithm has been carried out. The issues of generating a chain of blocks of an honest user and a chain of blocks of an attacker are considered. Formalization of the estimate of the probability of transaction break-even has been carried out. Binomial random walk was used for estimation. The end of the transaction process is just as justified as waiting for new blocks to be added to the chain of an honest user. A digital signature is used to identify whether a transaction belongs to a public key. The processes of signing a transaction and verifying a signature are considered. Separately, the approaches used in the design of cryptocurrencies are highlighted. The network stores the entire history of transactions, it is possible to calculate the balance of the total amount of incoming funds and spending money. These approaches are software solutions based on game theory and cryptography. The main attention is drawn to the business values of cryptocurrencies and ways to achieve them. As a result, the necessary functionality of the software client is formulated. The article provides a thorough analysis of a new financial and settlement instrument - electronic money. The task of developing a virtual payment system has recently received much attention.

Keywords: blockchain, decentralized systems, programming, cryptocurrency, crypt, transaction, miner.

Введение

Научно-технический прогресс входит во все сферы деятельности. Наиболее перспективным направлением является финтехе, в частности, платежные системы на блокчейн технологиях. Следствием совершенствования вычислительных и информационных технологий стало появление нового финансово-расчетного инструмента – электронных денег, особенность которого заключается в возможности существования как в централизованных, так и в децентрализованных системах. Задаче разработке децентрализованной платежной системы в последнее время уделяется большое внимание в специализированной литературе [1–3].

Для цитирования
Коробова Л.А., Бондаренко С.С., Мухин Д.П. Принцип работы децентрализованной информационной системы денежных переводов // Вестник ВГУИТ. 2022. Т. 84. № 3. С. 337–344. doi:10.20914/2310-1202-2022-3-337-344

For citation
Korobova L.A., Bondarenko S.S., Mukhin D.P. The principle of operation of a decentralized money transfer information system. Vestnik VGUIT [Proceedings of VSUET]. 2022. vol. 84. no. 3. pp. 337–344. (in Russian). doi:10.20914/2310-1202-2022-3-337-344

© 2022, Коробова Л.А. и др. / Korobova L.A. et al.
This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International License

В социальной сфере востребована услуга анонимной и отказоустойчивой системы оплаты. В случае с банковскими системами такой точкой отказа является само предприятие банка. Анонимность в банковских системах зависит от политик информационной безопасности самого предприятия и от качества программного обеспечения.

Технология криптовалют решает данные проблемы иначе.

Материалы и методы

Проблема отказоустойчивости решается созданием децентрализованной сети. Эти сети еще называют Peer to Peer или P2P. Теперь не конкретное предприятие совершает транзакцию пользователя, а участник сети. Таким образом, решается проблема отказоустойчивости. Решение этой проблемы проиллюстрировано на рисунке 1.

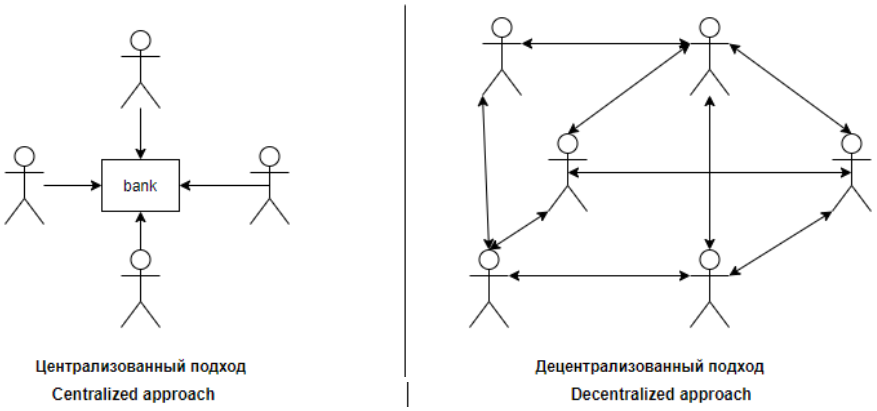

Рисунок 1. Отличие децентрализованных подходов и централизованных

Figure 1. The difference between decentralized approaches and centralized

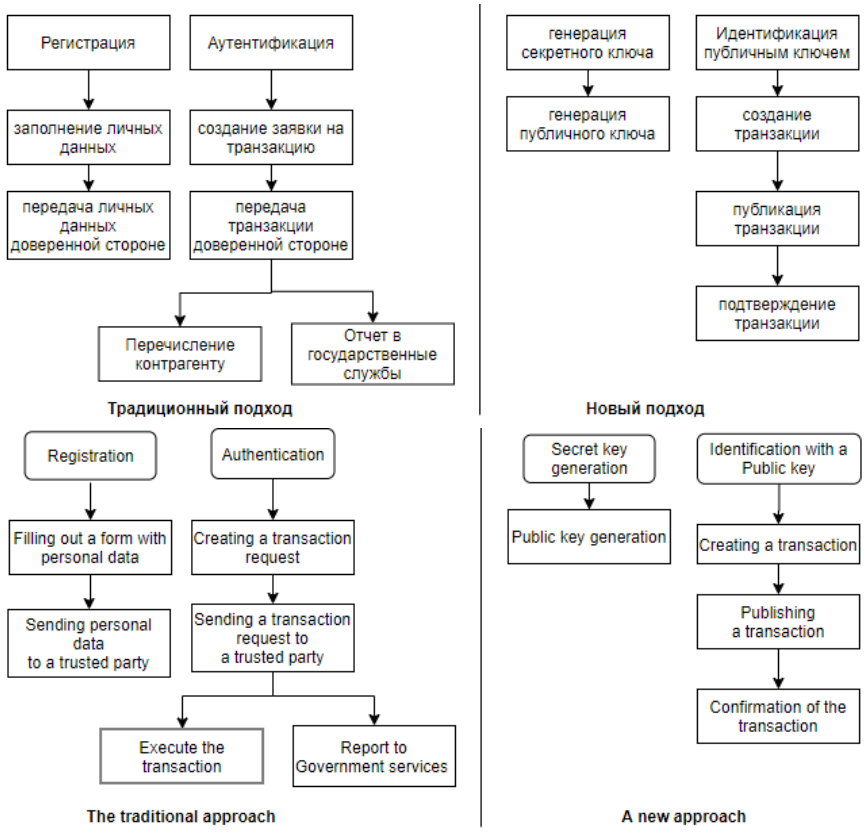

Рисунок 2. Подходы к созданию транзакций

Figure 2. The difference between business processes

Проблему анонимности в банковской среде трудно решить окончательно, так как у третьих лиц всегда имеется возможность узнать личные данные пользователя, или воспользоваться уязвимостями информационных систем. По этой причине и пользователю приходится доверять организации банка и надеяться, что его личные данные не будут использоваться в корыстных целях.

Проблема анонимности решается за счет того, что при регистрации пользователя в децентрализованной системе, не нужно указывать свои личные данные. Достаточно сгенерировать

приватный ключ, который будет являться секретом пользователя для подтверждения денежного перевода. И публичный ключ, который будет являться адресом, на который имеется возможность перевести деньги. Таких пар ключей у пользователя может быть несколько для разных целей. Данный подход проиллюстрирован на рисунке 2 [4, 5].

Также можно встроить алгоритм JoinCoin, который позволяет соединять транзакции. Теперь злоумышленник не может однозначно связать информацию о покупке с конкретным лицом.

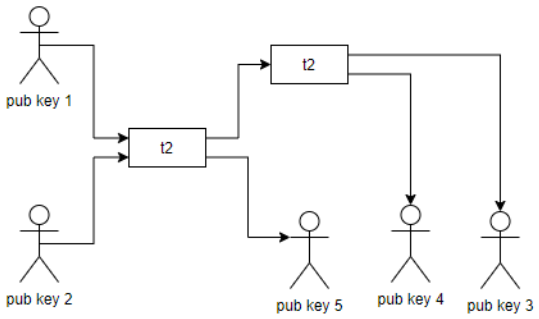

Рисунок 3. Пример применения JoinCoin

Figure 3. Example of using the JoinCoin algorithm

Чтобы объяснить это рассмотрим рисунок 3. Люди на рисунке обозначают публичные ключи (адресаты), причем несколько публичных ключей может принадлежать одному физическому лицу. Стрелками обозначены направления денежных переводов. Информация о транзакциях означена в прямоугольниках. На текущий момент уже не известно, происходит перевод другому физическому лицу или самому себе по разным счетам. Если произошел перевод между физическими лицами, также не известно с какой целью был произведен перевод, за оказание услуги, перевод зарплаты, или акт дарения денежных средств. Кроме этого, неизвестна точная конечная сумма, так как транзакции можно вложить друг в друга благодаря механизмам JoinCoin и UTXO. Данные механизмы опциональны, т. е. присутствует определенная нечеткость выбора одного из нескольких возможных способов действий. Любая неопределенность ведет к возникновению споров и конфликтов [8]. Для разрешения конфликтных ситуаций можно использовать более прозрачные способы оплаты [9, 10].

Чтобы создать децентрализованную сеть, требуется определить протокол транспортного уровня и протокол per to peer. Протоколом сетевого уровня может являться, например: TCP, UDP. Для протокола peer to peer сети может подойти Gossip. Цели протокола peer to peer:

1) обнаружение участников децентрализованной сети;

2) маршрутизация – поиск ближайших соседей для эффективной отправки сообщений;

3) идентификация участника по публичному ключу.

Очевидно, что теперь нет единой базы данных, в которой бы поддерживался актуальный баланс счетов. Для решения этой задачи можно использовать структуру blockchain и алгоритм консенсуса.

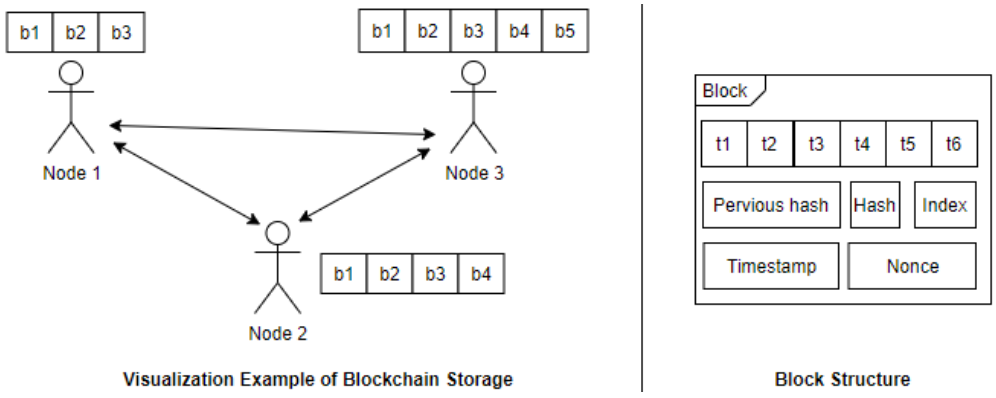

Рисунок 4. Пример хранения цепочки блоков

Figure 4. Visualization of an example of blockchain storage and block Structure

На рисунке 4 представлены механизм blockchain (хранение цепочки блоков) и структура одного блока. В блоке выделены следующие элементы: транзакции, производимые пользователями (*t*1, *t*2, *t*3, *t*4, *t*5, *t*6), ссылка на предыдущий блок, hash текущего блока, индекс, временная метка, индивидуальный (уникальный) номер – случайное число. Ссылкой на предыдущий блок является hash. Таким образом, выстраивается цепочка блоков. Данная цепочка распространяется ближайшим участникам сети. Самая длинная цепочка является актуальной, не актуальные цепочки не принимаются во внимание. Для проверки блоков можно применить алгоритм PoW (Prof of Work).

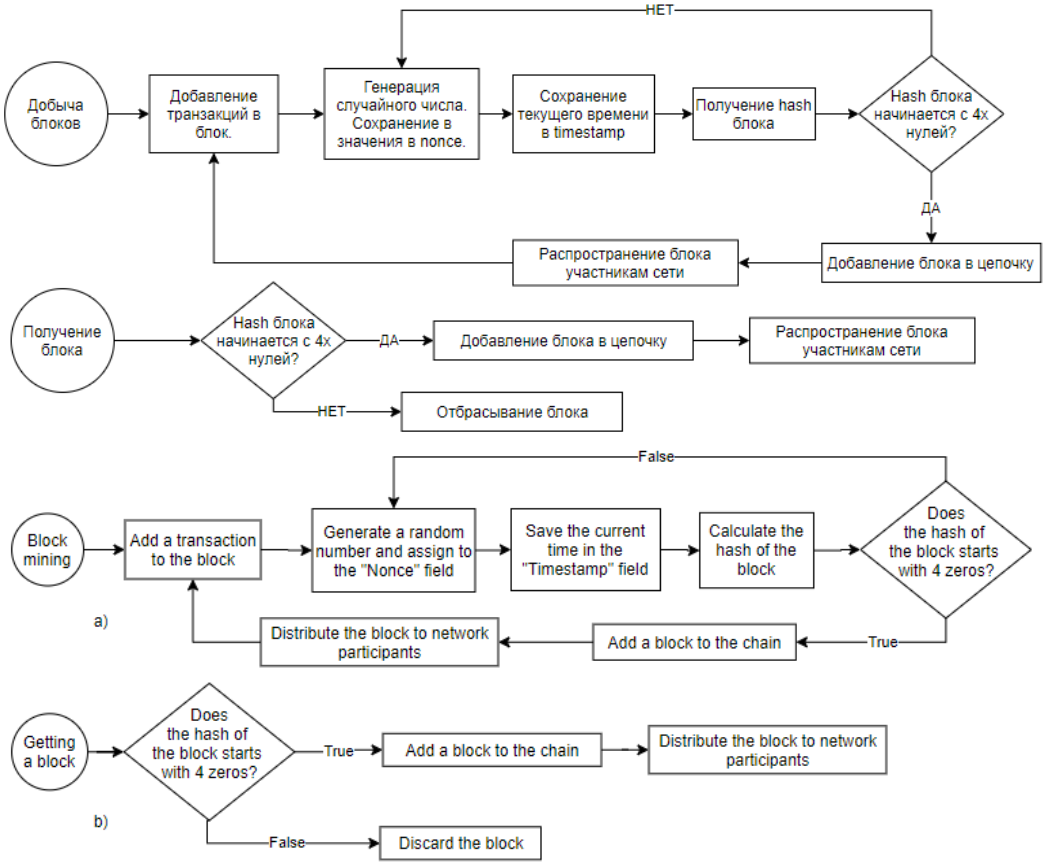

Рисунок 5. а) алгоритм *Prof of Work* и б) алгоритм консенсуса
Figure 5. a) PoW algorithm and b) Consensus algorithm

На рисунке 5 видно, что «Добыча блока» это цикличный и трудоемкий процесс, который и является доказательством работы алгоритма PoW. Инициализация работы алгоритма PoW является защитой от злоумышленников, которые захотят изменить цепочку блоков с целью выгоды. Так как добыча блоков это долгий процесс, то с увеличением числа блоков все менее целесообразно подменить транзакцию. Для того, чтобы был стимул поддерживать систему, майнерам (добытчикам блока) выплачивается комиссия за успешную генерацию блока.

Обсуждение

Генерацию блоков «честной» цепочки и цепочки блоков злоумышленника (атакующего) оценивают биномиальным случайным блужданием. Изменение расширения цепочки блоков на один со знаком «+» (+1), определяется как событие успеха или увеличение преимущества «честной» цепочки. По аналогии, изменение цепочки блоков на один блок со знаком «–» (-1), определяется как событие неудачи или расширение цепочки злоумышленника (атакующего) на один блок.

Вероятность безубыточности транзакции, или вероятность того, что атакующий когда-либо догонит «честную» транзакцию, начиная с z блоков (q_z), определим следующим выражением:

$$q_z = \begin{Bmatrix} 1, если\ p \le q \\ (q/p)^z, если\ p > q \end{Bmatrix},$$

где p – вероятность, что «честная» цепочка не изменена с целью выгоды, q – вероятность, что злоумышленник найдет следующий блок, z – количество блоков транзакции. Значение потенциального прогресса злоумышленника можно оценить по распределению Пуассона с ожидаемым значением $\lambda = z\,q/p$.

Вероятность того, что атакующий все еще может догнать, умножаем распределение Пуассона для каждой величины прогресса, который он мог бы достичь, на вероятность того, что он сможет догнать с определенной точки:

$$\sum_{k=0}^{\infty} \frac{\lambda^k \Delta e^{-\lambda}}{k!} \begin{Bmatrix} (q/p)^{(z-k)} \text{ если } k \le z \\ 1 \text{если } k > z \end{Bmatrix},$$

где k – счетчик блоков транзакции $k = \overline{1,}$.

Применим к предыдущей формуле перестановку, с целью не допустить суммирования бесконечного хвоста распределения. Таким образом, получаем следующую формулу для расчета вероятности того, что злоумышленник совершит успешную атаку на «честную» транзакцию,

$$1 - \sum_{k=0}^{z} \frac{\lambda^k \Delta e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right),$$

где k – счетчик блоков транзакций $k = \overline{1,z}$ [6–8].

Исходя из этого, процессом подтверждения транзакции является ожидание добавления нескольких новых блоков в цепочку. Это гарантирует то, что данная транзакция не будет изменена злоумышленником. Процесс подтверждения транзакции представлен на рисунке 6.

На рисунке 6 можно заметить новый элемент – цифровая подпись. Данный механизм, требуется для идентификации принадлежности транзакции публичному ключу (адресу пользователя), а также подтверждение того факта, что данные транзакции не были изменены в процессе добычи блоков другим участником сети.

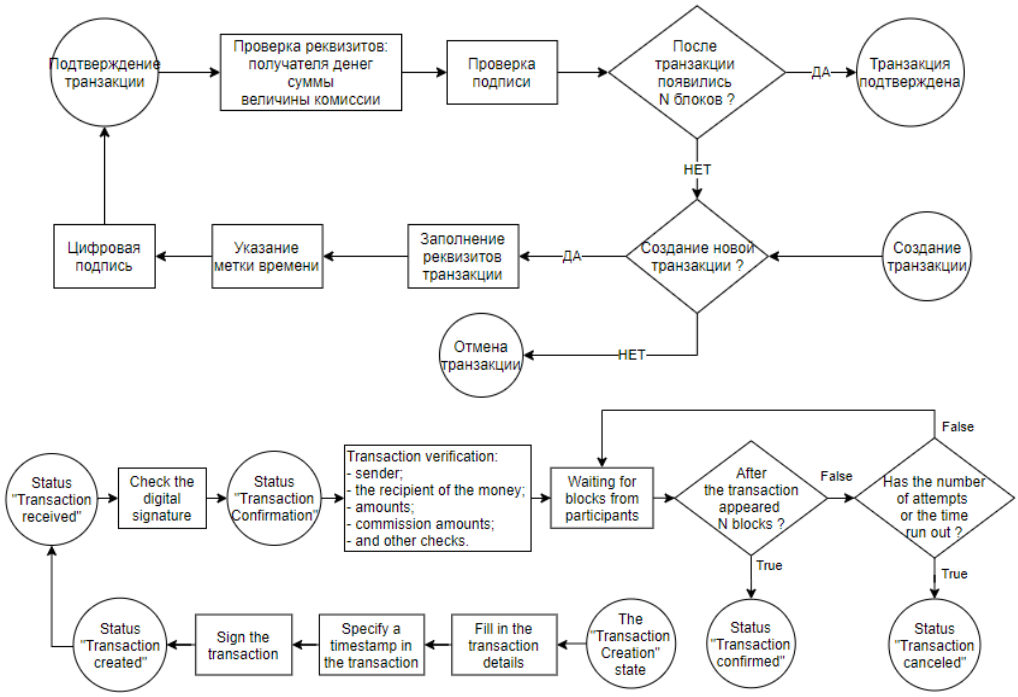

Рисунок 6. Процесс работы с транзакциями

Figure 6. Transaction lifecycle

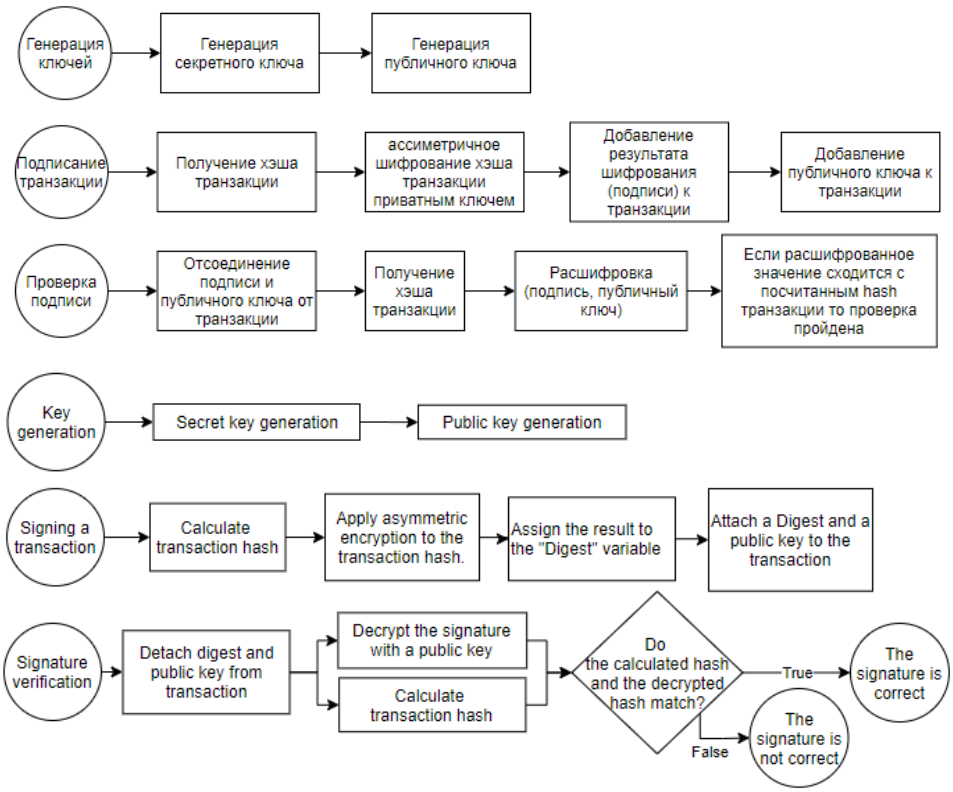

Рисунок 7. Алгоритм работы электронной подписи

Figure 7. Algorithm of digital signature operation

На рисунке 7 показаны процессы подписания транзакции и проверки подписи. Если проверка подписи пройдена, это означает, что только владелец секретного ключа мог создать данную транзакцию. Следовательно, злоумышленник не сможет перевести деньги с нашего счета в децентрализованной сети.

Узнать баланс можно посчитав разность между общей суммой поступающих средств и трат денег. Это можно реализовать, так как в сети хранится полная история транзакций.

Определим необходимый функционал программного клиента:

1) генерация пары ключей;
2) импорт пары ключей;
3) экспорт пары ключей;
4) получение списка пиров (клиентов участвующих в сети);
5) подключение к пирам;
6) публикация списка знакомых клиенту пиров;
7) опрос пиров;
8) получение транзакции и передача другим пирам;
9) создание транзакции и передача другим пирам;
10) подтверждение транзакции;
11) расчет текущего баланса;
12) добавление нового блока в цепочку;
13) публикация своего блокчейна;
14) добыча блока.

Замечание. В блоке указывается много транзакций, так как требуется провести большой объем работы, для этого и привлекаются майнеры. Если транзакций больше чем нужно, то они ранжируются в зависимости от предложенной клиентом комиссии. Список транзакций называют transaction pool [10–20].

Рассмотрим пример работы децентрализованной сети, представленной на рисунке 8. «Node 1» отправляет транзакцию майнерам. Майнеры распространяют транзакцию на другие пиры. «Mainer 1» успел найти блок первым, поэтому отправляет блок остальным пирам, в том числе «Mainer 2» и «Node 1». «Mainer 2» в свою очередь пересылает блок «Node 3». «Node 1» ожидает N новых блоков, пока не проверит легитимность транзакции.

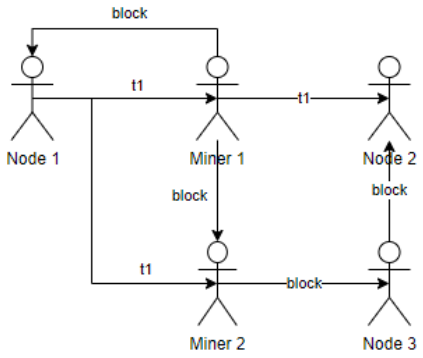

Рисунок 8. Пример работы децентрализованной сети

Figure 8. Example of a decentralized network messaging

Заключение

В статье проведен анализ работы децентрализованной платежной системы. Рассмотрены алгоритмы реализации бизнес-процессов, а также механизмы защиты распределенной информационной системы.

Литература

1 Чащин В.П., Гудков А.Б., Попова О.Н., Одланд И.О. и др. Характеристика основных факторов риска нарушений здоровья населения, проживающего на территориях активного природопользования в Арктике // Экология человека. 2014. № 1. С. 3–12.

2 Конторович А.Э., Коржубаев А.Г., Эдер Л.В. Прогноз глобального энергообеспечения: методология, количественные оценки, практические выводы // Минеральные ресурсы России. Экономика и управление: сетевой журн. 2006. № 5. URL: http://www.vipstd.ru/gim/content/view/90/278/

3 Раскина Т.А., Пирогова О.А., Зобнина О.В., Пинтова Г.А. Показатели системы остеокластогенеза у мужчин с различными клиническими вариантами анкилозирующего спондилита // Современная ревматология. 2015. Т. 9. № 2. С. 23–27. doi: 10.14412/1996-7012-2015-2-23-27

4 Терещенко Ю.В. Трактовка основных показателей вариабельности ритма сердца // Новые медицинские технологии на службе первичного звена здравоохранения: материалы межрегиональной конференции. Омск, 2010. С. 3–11.

5 Абдурахманов Г.М., Лопатин И.К. Основы зоологии и зоогеографии. Москва: Академия, 2001. 496 с.

6 Иванова А.Е. Проблемы смертности в регионах Центрального федерального округа // Социальные аспекты здоровья населения. 2008. № 2. URL: http://vestnik.mednet.ru/content/view54/30/

7 ГОСТ 8.586.5-2005. Государственная система обеспечения единства измерений. Измерение расхода и количества жидкостей и газов с помощью стандартных сужающих устройств. М.: Стандартинформ, 2007. 143 с.

8 Mbiti I., Weil D.N. Mobile banking: The impact of M-Pesa in Kenya // African successes, Volume III: Modernization and development. University of Chicago Press, 2015. P. 247-293.

9 Aker J.C. et al. Payment mechanisms and antipoverty programs: Evidence from a mobile money cash transfer experiment in Niger // Economic Development and Cultural Change. 2016. V. 65. №. 1. P. 1-37.

10 Tapscott A., Tapscott D. How blockchain is changing finance // Harvard Business Review. 2017. V. 1. №. 9. P. 2-5.

11 Carling J. Scripting remittances: Making sense of money transfers in transnational relationships // International migration review. 2014. V. 48. P. S218-S262. doi: 10.1111/imre.12143

12 Kirui O.K., Okello J.J., Nyikal R.A., Njiraini G.W. Impact of mobile phone-based money transfer services in agriculture: evidence from Kenya // Quarterly Journal of International Agriculture. 2013. V. 52. №. 892-2016-65177. P. 141-162. doi: 10.22004/ag.econ.173644

13 Bryans D. Bitcoin and money laundering: mining for an effective solution // Ind. LJ. 2014. V. 89. P. 441.

14 Kikulwe E.M., Fischer E., Qaim M. Mobile money, smallholder farmers, and household welfare in Kenya // PloS one. 2014. V. 9. №. 10. P. e109804. doi: 10.1371/journal.pone.0109804

15 Hashemi Joo M., Nishikawa Y., Dandapani K. Cryptocurrency, a successful application of blockchain technology // Managerial Finance. 2020. V. 46. №. 6. P. 715-733. doi: 10.1108/MF-09-2018-0451

16 Swan M. Anticipating the economic benefits of blockchain // Technology innovation management review. 2017. V. 7. №. 10. P. 6-13.

17 Suri T. Mobile money // Annual Review of Economics. 2017. V. 9. P. 497-520. doi: 10.1146/annurev-economics-063016-103638

18 Wakadha H., Chandir S., Were E.V., Rubin A. et al. The feasibility of using mobile-phone based SMS reminders and conditional cash transfers to improve timely immunization in rural Kenya // Vaccine. 2013. V. 31. №. 6. P. 987-993. doi: 10.1016/j.vaccine.2012.11.093

19 Larios-Hernández G.J. Blockchain entrepreneurship opportunity in the practices of the unbanked // Business Horizons. 2017. V. 60. №. 6. P. 865-874. doi: 10.1016/j.bushor.2017.07.012

20 Poongodi M., Sharma A., Vijayakumar V., Bhardwaj V. et al. Prediction of the price of Ethereum blockchain cryptocurrency in an industrial finance system // Computers & Electrical Engineering. 2020. V. 81. P. 106527. doi: 10.1016/j.compeleceng.2019.106527

References

1 Chashchin V.P., Gudkov A.B., Popova O.N., Odland J.O. et al. Description of Main Health Deterioration Risk Factors for Population Living on Territories of Active Natural Management in the Arctic. Human Ecology. 2014. no. 1. pp. 3–12. (in Russian).

2 Kontorovich A.E., Korzhubaev A.G., Eder L.V. Forecast of global energy supply: Techniques, quantitative assessments, and practical conclusions. Mineral resurses. 2006. no. 5. Available at: http://www.vipstd.ru/gim/content/view/90/278/ (in Russian).

3 Raskina T.A., Pirogova O.A., Zobnina O.V., Pintova G.A. Indicators of the osteoclastogenesis system in men with different clinical types of ankylosing spondylitis. Modern Rheumatology Journal. 2015. vol. 9. no. 2. pp. 23–27. doi: 10.14412/1996-7012-2015-2-23-27 (in Russian).

4 Tereshchenko Yu.V. Interpretation of main indices of heart rate variability. The New Medical Technology at Initial Stage of Public Care: Proceedings of Interregional Conference. Omsk, 2010. pp. 3–11. (in Russian).

5 Abdurakhmanov G.M., Lopatin I.K. Basics of Zoology and Zoogeography. Moscow, Akademiya, 2001. 496 p. (in Russian).

6 Kondrat'ev V.B. The global pharmaceutical industry. Available at: http://perspektivy.info/rus/ekob/globalnaja_farmacevticheskaja_promyshlennost_2011-07-18.html (in Russian).

7 State Standard 8.586.5–2005. Method of measurement. Measurement of flow rate and volume of liquids and gases by means of orifice devices. Moscow, Standartinform Publ., 2007. 10 p. (in Russian).

8 Mbiti I., Weil D.N. Mobile banking: The impact of M-Pesa in Kenya. African successes, Volume III: Modernization and development. University of Chicago Press, 2015. pp. 247-293.

9 Aker J.C. et al. Payment mechanisms and antipoverty programs: Evidence from a mobile money cash transfer experiment in Niger. Economic Development and Cultural Change. 2016. vol. 65. no. 1. pp. 1-37.

10 Tapscott A., Tapscott D. How blockchain is changing finance. Harvard Business Review. 2017. vol. 1. no. 9. P. 2-5.

11 Carling J. Scripting remittances: Making sense of money transfers in transnational relationships. International migration review. 2014. vol. 48. pp. S218-S262. doi: 10.1111/imre.12143

12 Kirui O.K., Okello J.J., Nyikal R.A., Njiraini G.W. Impact of mobile phone-based money transfer services in agriculture: evidence from Kenya. Quarterly Journal of International Agriculture. 2013. vol. 52. no. 892-2016-65177. pp. 141-162. doi: 10.22004/ag.econ.173644

13 Bryans D. Bitcoin and money laundering: mining for an effective solution. Ind. LJ. 2014. vol. 89. pp. 441.

14 Kikulwe E.M., Fischer E., Qaim M. Mobile money, smallholder farmers, and household welfare in Kenya. PloS one. 2014. vol. 9. no. 10. pp. e109804. doi: 10.1371/journal.pone.0109804

15 Hashemi Joo M., Nishikawa Y., Dandapani K. Cryptocurrency, a successful application of blockchain technology. Managerial Finance. 2020. vol. 46. no. 6. pp. 715-733. doi: 10.1108/MF-09-2018-0451

16 Swan M. Anticipating the economic benefits of blockchain. Technology innovation management review. 2017. vol. 7. no. 10. pp. 6-13.

17 Suri T. Mobile money. Annual Review of Economics. 2017. vol. 9. pp. 497-520. doi: 10.1146/annurev-economics-063016-103638

18 Wakadha H., Chandir S., Were E.V., Rubin A. et al. The feasibility of using mobile-phone based SMS reminders and conditional cash transfers to improve timely immunization in rural Kenya. Vaccine. 2013. vol. 31. no. 6. pp. 987-993. doi: 10.1016/j.vaccine.2012.11.093

19 Larios-Hernández G.J. Blockchain entrepreneurship opportunity in the practices of the unbanked. Business Horizons. 2017. vol. 60. no. 6. pp. 865-874. doi: 10.1016/j.bushor.2017.07.012

20 Poongodi M., Sharma A., Vijayakumar V., Bhardwaj V. et al. Prediction of the price of Ethereum blockchain cryptocurrency in an industrial finance system. Computers & Electrical Engineering. 2020. vol. 81. pp. 106527. doi: 10.1016/j.compeleceng.2019.106527

Сведения об авторах

Людмила А. Коробова к.т.н., доцент, кафедра информационных технологий, моделирования и управления, Воронежский государственный университет инженерных технологий, пр-т Революции, 19, г. Воронеж, 394036, Россия, lyudmila_korobova@mail.ru
https://orcid.org/0000-0003-1349-732X

Сергей С. Бондаренко студент, кафедра информационных технологий, моделирования и управления, Воронежский государственный университет инженерных технологий, пр-т Революции, 19, г. Воронеж, 394036, Россия, ss.bond.98@gmail.com

Дмитрий П. Мухин студент, кафедра информационных технологий, моделирования и управления, Воронежский государственный университет инженерных технологий, пр-т Революции, 19, г. Воронеж, 394036, Россия, dmitrymukhin.official@gmail.com

Information about authors

Lyudmila A. Korobova Cand. Sci. (Engin.), associate professor, information technology, modeling and management department, Voronezh State University of Engineering Technologies, Revolution Av., 19 Voronezh, 394036, Russia, lyudmila_korobova@mail.ru
https://orcid.org/0000-0003-1349-732X

Sergei S. Bondarenko student, information technology, modeling and management department, Voronezh State University of Engineering Technologies, Revolution Av., 19 Voronezh, 394036, Russia, ss.bond.98@gmail.com

Dmitry P. Mukhin student, information technology, modeling and management department, Voronezh State University of Engineering Technologies, Revolution Av., 19 Voronezh, 394036, Russia, dmitrymukhin.official@gmail.com

Вклад авторов

Все авторы в равной степени принимали участие в написании рукописи и несут ответственность за плагиат

Contribution

All authors are equally involved in the writing of the manuscript and are responsible for plagiarism

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Conflict of interest

The authors declare no conflict of interest.

Поступила 20/07/2022	После редакции 12/08/2022	Принята в печать 31/08/2022

Received 20/07/2022	**Accepted in revised** 12/08/2022	**Accepted** 31/08/2022