

Н. В. Лясников, Д. Д. Буркальцева¹

Проблемы поддержания работы информационной инфраструктуры в рамках экосистемы цифровой экономики в условиях сбоя при использовании технологии блокчейн

Аннотация

Цель. Актуальность темы исследования обусловлена следующим. Технология блокчейн может быть использована практически во всех отраслях промышленности, и со временем все больше и больше компаний внедряет ее в свою деятельность. Растущее число пользователей, глобальный масштаб использования технологий, высокая стоимость ошибок в коде — все это еще раз подчеркивает важность разработки эффективных процессов обеспечения качества и минимизации потенциальных сбоев на всех этапах разработки блокчейн-систем и их функционирования.

Цель статьи — рассмотрение проблем поддержания работы информационной инфраструктуры в рамках экосистемы цифровой экономики в условиях сбоя при использовании технологии блокчейн.

Материалы и методы. *В статье использовались методы анализа, синтеза, индукции, дедукции.*

Результаты. *В результате проведенного исследования были выделены основные проблемы, возникающие в ходе реализации информационной ин-*

¹ **Лясников Николай Васильевич**, доктор экономических наук, профессор, зав. лаборатории стратегического развития АПК Института проблем рынка РАН (117418, Москва, Нахимовский просп., 47); ведущий научный сотрудник (Институт менеджмента и маркетинга), Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (119571, Москва, проспект Вернадского, 82, стр. 1); acadra@yandex.ru

² **Буркальцева Диана Дмитриевна**, доктор экономических наук, доцент, профессор кафедры «Финансы предприятий и страхования», Крымский федеральный университет имени В.И. Вернадского (295007, Республика Крым, г. Симферополь, проспект академика Вернадского. Симферополь)

фраструктуры на базе технологии блокчейн в настоящее время, а именно – так называемая атака 51 %, проблема модификации данных, проблемы в использовании частных ключей, часто возникающая проблема неэффективности технологии во многих ситуациях, проблема хранения данных.

Выводы. Тем не менее, несмотря на недостатки, технология блокчейн имеет некоторые уникальные преимущества, которые позволяют обеспечить ей массовое внедрение во многих отраслях.

Ключевые слова: блок, блокчейн, криптовалюта, транзакция, майнинг, хэш.

Введение

Технология блокчейн была специально разработана, чтобы позволить людям, которые не доверяют друг другу, безопасно обмениваться ценными данными. Это связано с тем, что блокчейн хранит данные с помощью сложных математических и инновационных программных правил, преодолеть которые при хакерской атаке для последующего манипулирования очень сложно.

Но безопасность блокчейн может потерпеть неудачу в тех местах, где сложные математические правила и правила программного обеспечения вступают в контакт с людьми, которым свойственно ошибаться.

Цель статьи – исследование проблем поддержания работы информационной инфраструктуры в рамках экосистемы цифровой экономики в условиях сбоев при использовании технологии блокчейн.

Обзор литературы и исследований.

Исследованиями в области блокчейн технологий занимаются многие ученые и эксперты [1-11]. [Генкин А. С., Михеев А. А. [2] Пряников М. М., Чугунов А. В. [3], Тапскотт Д., Тапскотт А. [4], Цветкова Л. А. [5], D'Alfonso A., Langer P., Vandelis Z. [8], Kosten D. [6,9], Sabrina T. [10], Satoshi Nakamoto [11].

При этом остаются открытыми вопросы не в сущности, а в поддержании работы информационной инфраструктуры.

Результаты исследования

1. Сущность технологии блокчейн.

Технология блокчейн (англ. *blockchain* или *block chain*) представляет

собой выстроенную по определённым правилам непрерывную последовательную цепочку блоков (связный список), в которых содержится информация.

Для понимания природы возможных сбоев и проблем при использовании технологии блокчейн далее следует рассмотреть основные механизмы реализации технологии.

В блоке используется процесс хэширования, однако входные данные разделены на четыре секции:

- «block» – номер блока в цепи;
- «nonce» – случайное число, которое генерируется для получения такого хэша, который удовлетворял бы заложенным разработчиками условиям;
- «data» – набор данных;
- «prev» – хэш предыдущего блока в цепи.

Набор символов в поле «Hash» является уникальным для заданного набора входных данных поля «Data». Он также может быть получен для любого другого набора входных данных.

Однако процесс обратного извлечения входных данных с помощью имеющегося хэш-кода является задачей, требующей больших вычислительных мощностей [2].

Суть технологии блокчейн может быть представлена в виде следующей последовательности шагов:

1. Во все узлы сети отсылается некая транзакция.
2. Определенные узлы сети добавляют данные в блок.
3. Эти же узлы проверяют выполнение некоего заданного разработчиками условия.
4. В случае выполнения условия, блок данных отправляется всем участникам сети.
5. Блок данных проходит следующую проверку.
6. Если проверка пройдена, блок добавляется в цепочку (рисунок 1).

Поскольку в формировании хэша текущего блока, помимо других входных данных, участвует, в том числе, и хэш предыдущего блока, любое изменение любых входных данных предыдущего блока приведет к изменению как предыдущего хэша, так и хэша блока, следующего за ним, который из-за этого перестанет соответствовать заданному условию, а следом за ним некорректной станет и вся последующая цепь. Более того, чем старше блок в цепи, тем сложнее его изменить.

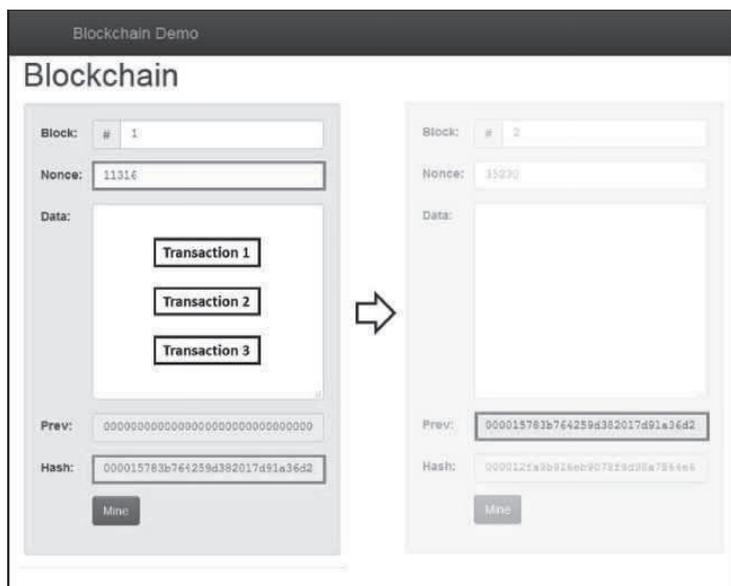


Рис. 1. Добавление блока в цепочку

Информация о транзакциях не передается в открытом виде, иначе каждый бы смог создать транзакцию, «представившись» в системе другим человеком, и таким образом отправить все средства самому себе. Данные об отправителях и получателях преобразуются в нечитаемый набор символов.

Каждый участник сети при регистрации в ней генерирует случайный набор чисел (приватный ключ), с помощью которого формируется другой, более сложный набор символов (публичный ключ) (рисунок 2). Получить приватный ключ из публичного невозможно, поскольку его длина очень велика и требует огромных вычислительных мощностей.

Приватный ключ принадлежит только тому пользователю, который сгенерировал его. Он не участвует в транзакциях, и его не следует разглашать никому. Он служит для осуществления подписи транзакции, однако в открытом виде не передается [1].

Для того, чтобы отправить транзакцию, каждый пользователь осуществляет подпись. В отправителях он вводит свой публичный ключ для обозначения своего участка, в получателях публичный ключ при-

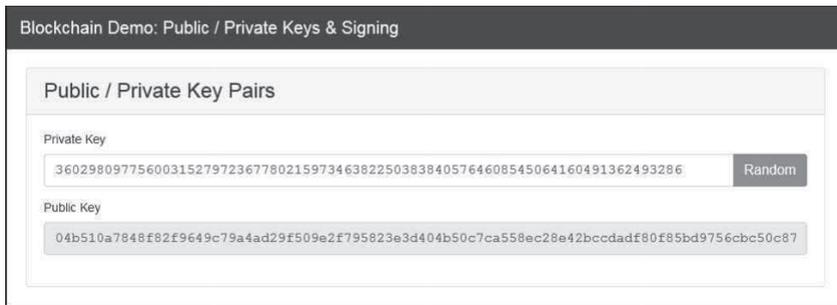


Рис. 2. Приватный и публичный ключи

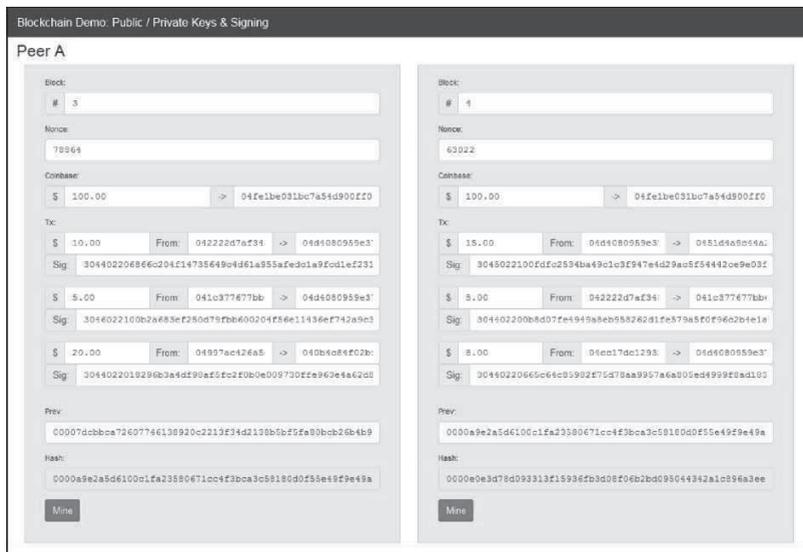


Рис. 3. Схема цепи блоков с публичными ключами и подписями в транзакциях

нимающего участка и информацию (например, сумму, которую пользователь желает перевести.

На основе этих входных данных и приватного ключа формируется подпись, а затем отправляется другим участникам для проверки и внесения транзакции в блок.

Имея подпись и все входные данные, каждый пользователь системы может проверить, что транзакция, которую пытаются внести

в блок, подписана пользователем, имеющим доступ к реальному приватному ключу.

Таким образом, блокчейн уже не имеет персональных данных о лицах, передающих информацию тому или иному лицу, а имеет лишь некие ключи, представляющие собой участки, за которыми находятся те или иные лица и подписи к каждой транзакции (рисунок 3).

Как уже было сказано выше, любое малейшее изменение входных данных, будь то номер участка отправителя или получателя, передаваемые средства или подпись, мгновенно приведет к изменению конечного хэша и некорректности всей цепи.

2. Основные проблемы поддержания работы в условиях сбоев при использовании технологии блокчейн.

Благодаря распределенной базе данных взлом хакерами практически невозможен, поскольку имеется множество копий базы данных на достаточно большом количестве компьютеров в сети, а получить к ним ко всем одновременный доступ практически нереально. DoS-атаки также неэффективны, благодаря отсутствию единого центра, работу которого можно было бы нарушить [1].

В блокчейн существует возможность доработки алгоритма его работы и включения изменений в блоки данных при условии, если все эти изменения будут одобрены большинством участников сети.

Тем не менее, существует ряд определенных проблем в реализации информационной инфраструктуры на базе технологии блокчейн, которые могут быть потенциальными источниками сбоев в работе системы. Рассмотрим их подробнее.

Атака 51 %

Алгоритм консенсуса, который защищает блокчейн, оказался очень эффективным на протяжении многих лет. Тем не менее, существует несколько потенциальных атак, которые могут быть осуществлены на блокчейн сеть, и **атака 51 %** является одной из наиболее обсуждаемых. Такая атака может произойти, если одному объекту удастся контролировать более 50 % мощности хэширования сети, что в конечном итоге позволит им нарушить ее работу, путем преднамеренного исключения или изменения порядка транзакций.

Несмотря на то, что теоретически это возможно, атака 51 % на блокчейн никогда не была успешной. По мере роста сети увеличивается ее безопасность, и маловероятно, что майнеры будут вкладывать боль-

шие суммы денег и ресурсов в атаку на сеть, поскольку они лучше будут вознаграждены за честные действия.

Помимо этого, успешная атака 51 % сможет изменить самые последние транзакции только в течение короткого периода времени, поскольку блоки связаны криптографическими доказательствами (замена старых блоков потребует непостижимых уровней вычислительной мощности). Кроме того, блокчейн очень устойчив и быстро адаптируется в ответ на атаку.

Модификация данных

Другим недостатком систем блокчейн является то, что после добавления данных в блокчейн их очень сложно модифицировать. Хотя его стабильность является одним из преимуществ, это не всегда хорошо. Изменение данных или кода в блокчейн, как правило, требует больших усилий и зачастую для этого необходимы сложные действия, когда одна цепочка оставляется, и начинается использоваться новая.

Приватные ключи

Блокчейн использует криптографию с публичным ключом (асимметричное шифрование), чтобы предоставить пользователям право собственности на свою часть криптовалюты (или любые другие данные в блокчейн). Каждый аккаунт в блокчейн (или адрес) имеет два соответствующих ключа: публичный ключ (которым можно поделиться) и приватный ключ (который должен храниться в секрете). Пользователям нужен приватный ключ для доступа к своим средствам, а это означает, что он действует как ваш собственный банк. Если пользователь теряет свой приватный ключ, деньги фактически теряются, и он ничего не сможет с этим поделать.

Неэффективность

Блокчейны во многих ситуациях могут быть крайне неэффективными. Поскольку майнинг высококонкурентен, и каждые десять минут выигрывает только один, работа каждого другого майнера теряется. Поскольку майнеры постоянно пытаются увеличить свою вычислительную мощность, у них появляется больше шансов найти действительный блок хеш, ресурсы, используемые сетью, значительно увеличились за последние несколько лет, и в настоящее время она потребляет больше энергии, чем целые страны, такие как Дания, Ирландия и Нигерия.

Хранилище

Блокчейн регистры со временем могут стать очень большими. Например, биткоин блокчейн в настоящее время требует около 200 ГБ

памяти. Текущий рост размера блокчейна, по-видимому, опережает рост количества жестких дисков, и сеть рискует потерять узлы, если регистр станет слишком большим для загрузки и хранения пользователями.

Выводы

Несмотря на недостатки, технология блокчейн имеет и уникальные преимущества. Ей еще предстоит долгий путь к массовому внедрению, но многие отрасли промышленности уже сегодня сталкиваются с преимуществами и недостатками систем блокчейн. В ближайшие несколько лет предприятия и правительства, вероятно, будут экспериментировать с новыми приложениями, чтобы выяснить, в каких случаях технология блокчейн приносит наибольшую пользу, а в каких ее использование неоправданно.

Дальнейшие исследования необходимо направить на изучение блокчейн, автоматизирующей доверие – как технологии управления, а не технологии оптимизации производственных циклов и взаимного использования данных, в условиях замещения платформ экосистемами моделей управления.

Список литературы

1. Блокчейн для корпораций [Электронный ресурс]. URL: <https://fldr.co/blockchain/153/1543/> (дата обращения: 18.05.2019).
2. Генкин А. С. Блокчейн: Как это работает и что ждет нас завтра [Текст] / А. С. Генкин, А. А. Михеев. Москва: Альпина Паблишер, 2018.
3. Пряников М. М. Блокчейн как коммуникационная основа формирования цифровой экономики: преимущества и проблемы [Текст] / М. М. Пряников, А. В. Чугунов // International Journal of Open Information Technologies. 2017. Т. 5. № 6. С. 49-55.
4. Тапскотт Д. Технология блокчейн: то, что движет финансовой революцией сегодня [Текст] / Д. Тапскотт, А. Тапскотт; пер. К. Шашковой, Е. Ряхиной. Москва: Эксмо, 2017. 448 с.
5. Цветкова Л. А. Перспективы развития технологии блокчейн в России: конкурентные преимущества и барьеры [Текст] / Л. А. Цветкова // Экономика науки. 2017. Т. 3. № 4. С. 275-296.
6. Цифровая трансформация начинается со смыслов [Элек-

- тронный ресурс]. URL: <https://ffc.media/ru/overviews/digital-essentials/>
7. Юридические аспекты применения блокчейна и использования криптоактивов [Электронный ресурс] / Голос – социальная сеть, построенная на публичном блокчейне, медиа-блокчейн. URL: <https://golos.io/ru--blokcheijn/@valet/yuridicheskie-aspektu-primeneniya-blokcheina-i-ispolzovaniya-kriptoaktivov> (дата обращения: 16.05.2019).
 8. D'Alfonso Alexander, Langer Peter, Vandelis Zintis. The Future of Cryptocurrency An Investor's Comparison of Bitcoin and Ethereum. Ryerson University. October 17th, 2016
 9. Kosten Dmitri. Bitcoin Mission Statement. Or What Does It Mean Sharing Economy and Distributed Trust? [Электронный ресурс] URL: <http://ssrn.com/abstract=2684256>
 10. Sabrina T. Howell, Marina Niessner, David Yermack. Initial Coin Offerings: Financing Growth With Cryptocurrency Token Sales, Working Paper 24774. National Bureau of Economic Research. 1050 Massachusetts Avenue Cambridge, MA 02138. June 2018, Revised April 2019. [Электронный ресурс] URL: <http://WWW.NBER.ORG/Papers/W24774>.
 11. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. satoshin@gmx.com [Электронный ресурс] URL: www.bitcoin.org

Для цитирования

Лясников Н. В., Буркальцева Д. Д. Проблемы поддержания работы информационной инфраструктуры в рамках экосистемы цифровой экономики в условиях сбоя при использовании технологии блокчейн // Экономика и социум: современные модели развития. 2019. № 2. С. 219-230.

doi: 10.18334/ecsoc.9.2.40866

N. V. Lyasnikov, D. D. Burkaltseva¹

The problem of maintaining the information infrastructure within the ecosystem of the digital economy in terms of failures when using the blockchain technology

Annotation

Purpose: *The relevance of the research topic is due to the following. Blockchain technology can be used in almost all industries, and over time, more and more companies are implementing it in their activities. The growing number of users, the global scale of the use of technologies, the high cost of errors in the code – all this once again emphasizes the importance of developing effective quality assurance processes and minimizing potential failures at all stages of the development of blockchain systems and their functioning.*

The purpose of the article is to consider the problems of maintaining the information infrastructure within the super system of the digital economy in the conditions of failures in the use of blockchain technology.

Materials and methods: *The article used the methods of analysis, synthesis, induction, deduction.*

Results: *As a result of the study, the main problems encountered in the implementation of information infrastructure based on blockchain technology at the present time were identified, namely – the so-called attack of 51 %, the problem of data modification, problems in the use of private keys, the often arising problem of technology inefficiency in many situations, the problem of data storage.*

¹ **Lyasnikov Nikolai V.**, Doctor of Economics Sciences, Professor, Ch. scientific employee of the Laboratory of Strategic Development of the APK, Market Economy Institute of Russian Academy of Sciences (MEI RAS) (47, Nakhimovsky Ave., Moscow, 117418); Leading Researcher of the Institute (Management and Marketing Institute), Russian Presidential Academy of National Economy and Public Administration (82, Vernadsky prosp., Moscow, 119571); acadra@yandex.ru

Burkaltseva Diana D., Doctor of Economics Sciences, Associate Professor, Professor of the Department “Finance of Enterprises and Insurance”, V.I. Vernadsky Crimean Federal University (4 Vernadskogo Avenue, Simferopol, Republic of Crimea, 295007, Russia), di_a@mail.ru

Conclusions: *Nevertheless, despite its drawbacks, blockchain technology has some unique advantages that allow it to be mass implemented in many industries.*

Keywords: *block, blockchain, cryptocurrency, transaction, mining, hash.*

References

1. Blockchain for corporations [Electronic resource] URL: <https://fldr.co/blockchain/153/1543/> (дата обращения: 18.05.2019).
2. Genkin A.S. Blockchain: How it works and what awaits us tomorrow [Text] / A.S. Genkin, A.A. Mikheev. Moscow: Alpina Publisher, 2018.
3. Gingerbread MM Blockchain as a communication basis for the formation of the digital economy: advantages and problems [Text] / MM Pryanikov, A.V. Chugunov // International Journal of Open Information Technologies. 2017. Т. 5. № 6. P. 49-55.
4. Tapscott D. Technology blockchain: what drives the financial revolution today [Text] / D. Tapscott, A. Tapscott; per. K. Shashkova, E. Ryakhina. Moscow: Eksmo, 2017. 448 p.
5. Tsvetkova L. A. Prospects for the development of blockchain technology in Russia: competitive advantages and barriers [Text] / L. A. Tsvetkova // Science Science. 2017. Vol. 3. No. 4. P. 275-296.
6. Digital transformation begins with meanings [Electronic resource]. URL: <https://ffc.media/ru/overviews/digital-essentials/>
7. Legal aspects of the use of the blockchain and the use of cryptoactive assets [Electronic resource] / Voice – a social network built on a public blockchain, media blockchain. URL: <https://golos.io/ru--blokcheijn/@valet/yuridicheskie-aspekty-primeneniya-blokcheina-i-ispolzovaniya-kriptoaktivov> (дата обращения: 16.05.2019).
8. D'Alfonso Alexander, Langer Peter, Vandelis Zintis. The Future of Cryptocurrency An Investor's Comparison of Bitcoin and Ethereum. Ryerson University. October 17th, 2016
9. Kosten Dmitri. Bitcoin Mission Statement. Or What Does It Mean Sharing Economy and Distributed Trust? [Electronic resource] URL: <http://ssrn.com/abstract=2684256>
10. Sabrina T. Howell, Marina Niessner, David Yermack. Initial Coin Offerings: Financing Growth With Cryptocurrency Token Sales, Working Paper 24774. National Bureau of Economic Research. 1050 Massachusetts Avenue Cambridge, MA 02138. June 2018, Revised

April 2019. [Electronic resource] URL: <http://WWW.NBER.ORG/Papers/W24774>.

11. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. satoshin@gmx.com [Electronic resource] URL: www.bitcoin.org

For citation

Лясников Н. В., Буркالتсева Д. Д. The problem of maintaining the information infrastructure within the ecosystem of the digital economy in terms of failures when using the blockchain technology. *Economics & Society: Contemporary Models of Development*. 2019; P. 219-230.

doi: 10.18334/ecsoc.9.2.40866