**ВІСНИК ПРИАЗОВСЬКОГО ДЕРЖАВНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ**
**2019р. Серія: Технічні науки Вип. 39**
**p-ISSN: 2225-6733; e-ISSN: 2519-271X**

# *ІНФОРМАТИКА*

**УДК 004** **doi: 10.31498/2225-6733.39.2019.201069**

**© Волошин В.С.[1], Федосова И.В.[2], Мироненко Д.С.[3]**

## К ВОПРОСУ О ТИПИЧНОСТИ БЛОКЧЕЙН-ТЕХНОЛОГИЙ В ИНЖИНИРИНГЕ

*В работе систематизированы основные термины, позволяющие пользователю познакомиться с особенностями блокчейн-технологий. Показано основное качество блокчейн-системы, дающее право ее участникам обеспечивать требуемый уровень доверительности к системе и к каждому инкогнитивному ее участнику. Представлены особенности формирования ключей доступа к системе со стороны участников, адреса программных продуктов для формирования публичного AEPuKey и приватного AEPrKey ключей. Предложен упрощенный алгоритм работы в блокчейне для типового пользователя, включающий порядок проведения транзакций и их вещественное содержание, правила записи информации о новой, необработанной транзакции, порядок и правила обработки протоколов в системе, проверки и подписи индивидуальным ключом всеми участниками на предмет ее возможности, наличия ресурса у автора транзакции. Даны представления о том, как осуществляется майнинг сформированных реестров и их хеш-кодирование, что собой представляет конвертатор со скрытым алгоритмом генерации случайных битовых рядов и как им пользоваться в первом приближении. Предложена наглядная и упрощенная модель майнинговой операции, дающая общее представление пользователю об этом виде работы в рамках блокчейн-технологии. Иллюстрированы примеры, когда происходит сбой системы на этапе легализации очередного протокола, действия системы и каждого из участников по приведению системы в новое доверительное состояние. Представлен механизм нарушения и распознавания целостности пиринговой сети и действия по их устранению. Подобная информация может быть полезна тем пользователям, которые только начали свой путь в освоении блокчейн-технологии в компании, в бизнесе. Методический материал не может быть полезным в существующих технологиях, например, Bitcoin, Ethereum и др., по причине их развернутости в сторону углубления и сложности профессионального майнинга, который уже не может быть обеспечен приватными компьютерными мощностями и требует более профессионального подхода и более профессиональной техники. Методика направлена на популяризацию блокчейн-технологий в среде микро-, малого и среднего бизнеса, в системах децентрализованного управления на самых различных его уровнях в виде простого и надежного от взломов программного продукта, позволяющего большому количеству потребителей эффективно создавать локальные технологии типа распределенного реестра для решения самых различных задач в области децентрализации.*

***Ключевые слова:*** *блокчейн-технология, транзакции, майнинг, децентрализация, доверительные протоколы, распределенные реестры, интернет вещей.*

[1] *д-р техн. наук, профессор, ГВУЗ «Приазовский государственный технический университет», г. Мариуполь*
[2] *д-р пед. наук, профессор, ГВУЗ «Приазовский государственный технический университет», г. Мариуполь, irivasilevna1964@gmail.com*
[3] *канд. техн. наук, доцент, ГВУЗ «Приазовский государственный технический университет», г. Мариуполь, mironenko_ds@ukr.net*

**p-ISSN: 2225-6733; e-ISSN: 2519-271X**

***Волошин В.С., Федосова І.В., Міроненко Д.С. До питання про типовість блокчейн-технологій у інжинірингу.*** *У роботі систематизовано основні терміни, що дозволяють користувачеві познайомитися з особливостями блокчейн-технологій. Показано основну якість блокчейн-системи, що дає право її учасникам забезпечувати необхідний рівень довіри до системи і до кожного інкогнітивного її учасника. Представлені особливості формування ключів доступу до системи з боку учасників, адреси програмних продуктів для формування громадської AEPuKey і приватного AEPrKey ключів. Запропоновано спрощений алгоритм роботи в блокчейне для типового користувача, що включає порядок проведення транзакцій і їх речовий зміст, правила запису інформації про нову, необроблену транзакцію, порядок і правила обробки протоколів у системі, перевірки і підпису індивідуальним ключем усіма учасниками на предмет її можливості, наявності ресурсу у автора транзакції. Дано уявлення про те, як здійснюється майнінг сформованих реєстрів і їх хешкодування, що собою являє конвертатор з прихованим алгоритмом генерації випадкових бітових рядів і як ним користуватися в першому наближенні. Запропоновано наочна і спрощена модель майнінгової операції, що дає загальне уявлення користувачеві про цей вид роботи в рамках блокчейн-технології. Ілюстровані приклади, коли відбувається збій системи на етапі легалізації чергового протоколу, дії системи і кожного з учасників по приведенню системи у новий довірчий стан. Представлений механізм порушення і розпізнавання цілісності пірингової мережі і дії щодо їх усунення. Подібна інформація може бути корисна тим користувачам, які тільки почали свій шлях в освоєнні блокчейн-технології в компанії, в бізнесі. Методичний матеріал не може бути корисним в існуючих технологіях, наприклад,* Bitcoin, Ethereum *та ін., через їх розгорнення в сторону поглиблення і складності професійного майнінгу, який вже не може бути забезпечений приватними комп'ютерними потужностями і вимагає більш професійного підходу і більш професійної техніки. Методика спрямована на популяризацію блокчейн-технологій в середовищі мікро-, малого та середнього бізнесу, в системах децентралізованого управління на самих різних його рівнях у вигляді простого і надійного від зломів програмного продукту, що дозволяє великій кількості споживачів ефективно створювати локальні технології типу розподіленого реєстру для вирішення найрізноманітніших задач в області децентралізації.*
***Ключові слова****: блокчейн-технологія, транзакції, майнінг, децентралізація, довірчі протоколи, розподілені реєстри, інтернет речей.*

***V.S. Voloshin, I.V. Fedosova, D.S. Mironenko. To the question of the typicality of blockchain technologies in engineering.*** *The work systematizes the basic terms that make it possible for the user to become acquainted with the distinguishing features of blockchain technology. The main quality of the blockchain system has been shown; the quality giving the right for its participants to provide the required level of the trust in the system and the trust in each of its incognitive participants. The features of generating access keys to the system by the participants, the addresses of the software products for generating public AEPuKey and private AEPrKey keys havebeen presented. A simplified algorithm for working in the blockchain for a typical user has been proposed, including the procedure for conducting transactions and their material content, the rules for recording information concerning a new, unprocessed transaction, the procedure and rules for processing protocols in the system, checking and signing with an individual key by all the participants for its possibilities, resource availability at the disposal of the author of the transaction. The procedures of carrying out mining of the formed registries and their hash coding have been shown as well as a converter with a hidden algorithm for generating random bit series and the way of using it in the first approximation. A clear and simplified model of the mining operation has been proposed, which gives a general idea to the user as to this type of work within the blockchain technology. The examples when the system crashes at the stage of legalizing the next protocol, the actions of the system and*

p-ISSN: 2225-6733; e-ISSN: 2519-271X

*each of the participants in bringing the system to a new trust state have been given. The violation and recognition of the integrity of the peer-to-peer network and the actions to eliminate them have been presented. Such information may be useful to those users who are just mastering the blockchain technology in a company, in business. The methodological material cannot be useful in the existing technologies, such as Bitcoin, Ethereum for example, etc. due to their deep and complex professional mining, which can not be provided with private computer capacities and require a more professional approach and more professional equipment. The methodology is aimed at popularizing blockchain technologies for micro, small and medium-sized businesses, in decentralized management systems at its most diverse levels, in the form of a simple, reliable, safe from hacking software product that makes it possible for a large number of consumers to efficiently create local technologies such as a distributed registry to solve a wide variety of decentralization tasks.*
***Keywords:*** *blockchain technology, transactions, mining, decentralization, trust protocols, distributed registries, Internet of things.*

**Постановка проблемы.** Недостаточное методическое обеспечение для пользователей из числа инженеров, представителей малого и среднего бизнеса, студентов, интересующихся проблемой блокчейн технологий, необходимость в представлении аналогового алгоритма для пользователей, описывающего понятия транзакций, майнинга, хеш-кодирования и другие особенности технологии.

**Анализ последних исследований и публикаций.** Технологии блокчейна или блокчейн-технологии сегодня на слуху у всей активной части человечества [1-7]. Без преувеличения, эти технологии, в основе которых доверительность и инкогнитивность, имеют распространение в мире существующих технологий, управления, сервиса и других областей деятельности. Мы наблюдаем проникновение блокчейн-технологий в самые различные области, в наиболее мощные компании, такие как IBM, BOSH, AliBaba, Amazon Uber, Samsung, General Electric и др.

В равной мере, как интернет стал независимым от посредников хранителем огромного пласта цифровой информации, так технологии блокчейн постепенно становятся независимыми от посредников хранителями и распорядителями интернета ценностей, интернета вещей. Этим он привлекателен для инжиниринга.

«Интернет вещей» становится связующим звеном между современным виртуальным цифровым миром и реальным физическим миром, в котором привык существовать человек. О блокчейне сегодня говорят как о: технологии децентрализованного распределенного реестра всего, что подлежит систематизации; возможности и потенциале новой технологической платформы в различных областях жизни; гигантской цепи уверенности во всем; доверительном продукте; хранителе правды [1].

Блокчейн описывается как технология распределенного реестра. Все блоки связаны между собой в непрерывную последовательную цепочку таким образом, что для легализации любого последующего блока необходима информация о предыдущих блоках. Это постоянно накапливаемая и дополняемая база данных обо всех транзакциях без права их удаления или корректировки. Главное достоинство блокчейна – это система цифровых «печатей», или меток, благодаря которым придается законность и незыблемость каждому последующему коллективному протоколу (блоку) транзакций в зависимости от предыдущего [1]. Вторым достоинством блокчейн-технологии является ее прозрачность для всех участников – о размерах сделки, ее пути, но не о личности адресата.

В целом, блокчейн-технология позволяет однозначно свести воедино в оцифрованном виде персональные данные любых собственников и их физическую собственность, без опасности ее дублирования в привязке к другому собственнику. Это кадастры различного назначения, право собственности, регистрация любых прав, предусмотренных законодательством, соглашений, контрактов и многое другое. Основными методами достижения результата являются цифровизация материальных ресурсов и их токенизация, то есть привязка принятой единицы учета и актива любого ресурса к объему некоторой деятельности (например, ценным бумагам, сертификатам, деньгам, энергии, лекциям, академическим часам). Токены, как право действия, мож-

p-ISSN: 2225-6733; e-ISSN: 2519-271X

но передавать, продавать, занимать в рамках пиринговой сети блокчейна.

Финансовый сегмент применения блокчейна является только одним из многих, на которые может претендовать эта уникальная технология. Чаще всего блокчейн-технологии связывают с биткоином, с такими терминами как майнинг, транзакции, доверительные протоколы, хэш-функции и др. Это отпугивает обычных пользователей. Любое применение технологии видится в цифровизации и доверительном обмене самой различной документацией: договорами, завещаниями, свидетельствами, патентами, гарантийными обязательствами, долговыми расписками, медицинскими историями болезней, анализов, учебно-методическими материалами, научными данными, бытовой документацией, и др. Но это не все. Применение технологии и особенно его перспективы впечатляют.

Создание и развитие системы удобных смарт-устройств и смарт-контрактов расширяет эту технологию на область, которую называют «интернет вещей», делая любой оцифрованный предмет уникальным и узнаваемым в системе распределенных реестров. Например, платформы онлайн-платежей типа PayPal, автономные логистические системы в транспорте типа Uber, в энергетике типа dron-service электрических сетей или системы учета распределенных мини-источников энергии, умные системы переработки отходов всех видов и классификаций, независимый мониторинг состояния окружающей среды, погодных условий, цифровизация коммунальных услуг, контроль за износом инженерных сооружений и машин, строительная индустрия и распределение недвижимости, заводы вещей с распределенными реестрами всех материальных потоков, начиная с многокомпонентного сырья, готовой продукции и отходов с обязательными смарт-чипами, позиционирующими каждый компонент или деталь. Это интернет-торговля и IT-маркетинг, умные и энергоэффективные дома и многое другое из «интернета вещей» [2-6].

**Целью работы** является создание упрощенного сегмента для понимания сути блокчейн-технологий для простого пользователя, инженера, бизнесмена, приблизить это понимание к тем ресурсам, для которых он может быть предназначен. И, прежде всего, к исследовательским и образовательным.

**Изложение основного материала.** Собирательный образ системы, которая предназначена для реализации блокчейн-технологии, включает: участников системы, соответствующую компьютерную базу и сети, общее согласование о предметах сделок в системе, знания о формах и способах записи информации в системе, соглашение о системном доверии для всех участниках системы (P2P – peer to peer, равноправность участников), соглашение об инкогнитивности персональных данных, программное обеспечение и доступ к майнингу путем создания индивидуального электронного кошелька.

Ключевые термины системы:

- ключ доступа – это специальным способом полученный набор автоматически сгенерированных символов в одном из форматов хранения (Hex, WIF, WIF-сжатый) в электронном кошельке. Ключи доступа бывают общие (открытые) и приватные (индивидуальные);

- транзакция – это процесс проведения некоторой логически завершенной сделки (соглашения) между двумя участниками системы, результаты которой записываются в протоколы всех участников системы. В более широком смысле под этим термином в блокчейн-технологиях следует понимать любое согласованное и легализованное участниками действие в отношении другого участника;

- доверительный криптографический протокол – это последовательность записей о действиях (сделках) участников по передаче оцифрованной информации или информационном обмене в определенном временном отрезке. Обеспечивается на основе конфиденциальности данных об участниках, аутентификации сторон сделки, невозможности отказа от сделки и целостности записанных ранее данных;

- распределенные реестры блокчейна – это децентрализованная база оцифрованных данных о предмете транзакций, которая хранится и обновляется каждым из участников сети;

- майнинг – это предоставление индивидуального вычислительного ресурса участника системы для обеспечения жизнедеятельности некоторого виртуального ресурса этой системы. Процедура майнинга – это решение математической задачи, в ходе которой вычисляется число, которое не является больше заданного целевого уровня сложности. Суть этого числа заключается в присвоении ему права «опечатывания» очередного протокола распределенного реестра;

p-ISSN: 2225-6733; e-ISSN: 2519-271X

- хеш-функция, в общем, как математическая операция свёртки, представляет собой функцию, которая обеспечивает преобразование массива входных данных любой заданности в битовую строку установленной длины, выполняемое скрытым алгоритмом. Такой алгоритм составляет основу блокчейн-технологии. Преобразование, производимое хеш-функцией, называется хешированием. Алгоритм хеширования в блокчейн-технологиях выдает случайное битовое число (между 1 и $2^{256} – 1$), состоящее из символов, расположенных в произвольном написании, неизменное на протяжении всего майнинга и после него;

- токен – единица учета. Аналог ценных бумаг и действий над ними в системе блокчейн-технологий.

Терминология этим не ограничивается, принимая во внимание достаточную сложность и необходимое упорство в освоении технологии.

Каждый участник, независимо от того, юридическое или физическое лицо, обладает двумя ключами доступа в систему, создаваемыми одним из известных методов, например, «Brain Wallet» или по адресу «bitaddress.org.»: один из них общепринятый, распознаваемый всей системой (Account Extended Public Key – **AEPuKey**), а второй – индивидуальный, принадлежащий только участнику (Account Extended Private Key – **AEPrKey**). Индивидуальный ключ доступа – это особая криптограмма, хешируемая (создаваемая) некоторым алгоритмом шифрования в одном из равнозначных форматов хранения (Hex, WIF, WIF-сжатый), которая дает участнику право персонального доступа к ресурсам (криптовалюта, доступ к счетам фирм, информационные ресурсы, know-how компаний), представляющим ценность в системе. Публичный или открытый ключ система генерирует сама на основе индивидуального ключа, который участник получает уникально. Владение приватным ключом позволяет всегда вспомнить открытый ключ, но не наоборот. Далее последовательность алгоритма блокчейна включает следующее.

1. Каждый участник системы обладает обезличенной информацией об оговоренных заранее ресурсах всех других партнеров пиринговой (P2P) сети.

2. Системная работа заключается в проведении последовательных *транзакций* (некоторый материальный обмен, платежи, перевод денег со счета на счет и др.), между любыми двумя участниками системы. Обезличенная цифровая информация об этом объявляется всем участникам для записи в следующей строке индивидуальных протоколов.

3. Запись информации о новой, необработанной транзакции осуществляется всеми участниками в свои протоколы под одинаковым номером сделки с указанием времени сделки и является обязательной для всех.

4. Периодически с равным интервалом конкретная транзакция обрабатывается путем проверки и подписи индивидуальным ключом всеми участниками на предмет ее возможности, наличия ресурса у автора транзакции (рис. 1). Заполняемый таким образом последовательностью транзакций доверительный протокол лежит в основе огромной цепи распределенных реестров блокчейна.

5. Протокол транзакций, заполненный полностью (например, N записей в одном доверительном протоколе), в дублированном виде присутствует у всех участников системы с указанием времени операции. Например, в системе биткоина каждые 10 минут проверяются все транзакции, они получают одобрение и сохраняются в блоке, *соединенном с предыдущим*, образуя таким образом непрерывную цепь блоков. Каждый последующий блок соотнесен с предыдущим, без него не существует и только тогда является действительным и доступным для просмотра всеми желающими.

6. Полностью заполненный протокол с транзакциями «опечатывается». Поиск единой для всех участников системы «печати» осуществляется самими участниками в процессе *майнинга*. Осуществляется майнинг при участии *конвертатора* (назовем его так для простоты понимания) со скрытым алгоритмом генерации случайных битовых рядов. Майнинговое оборудование участника, например, видеокарты, мощные процессоры или специальные asic-устройства, позволяет хешировать очередной этап «опечатывания» протокола и, после процедуры проверки, легализуется и помещается в распределенные реестры. Это сложный специфический алгоритм, позволяющий за счет использования электроэнергии генерации требуемого кода получать вознаграждение (например, в технологиях биткоина это определенная часть криптовалюты, обеспеченная затратами электроэнергии).

p-ISSN: 2225-6733; e-ISSN: 2519-271X

7. Конвертатор – машина одностороннего действия. Важной особенностью конвертатора является отсутствие обратного действия. Конвертатор, представляющий собой «черный ящик», в основе которого находится алгоритм, названный авторами как SHA-256, при помощи определенной *хэш-функции* генерирует *хеш-код* (НК), состоящий из случайным образом набранных букв и цифр. Входными данными для конвертатора являются данные об оцифрованном содержании протокола транзакций «А», цифровой код $\overline{x}_{i-1}$ предыдущего протокола, хешированный при его «опечатывании». Это данные, которые майнер загружает в компьютер (рис. 2).

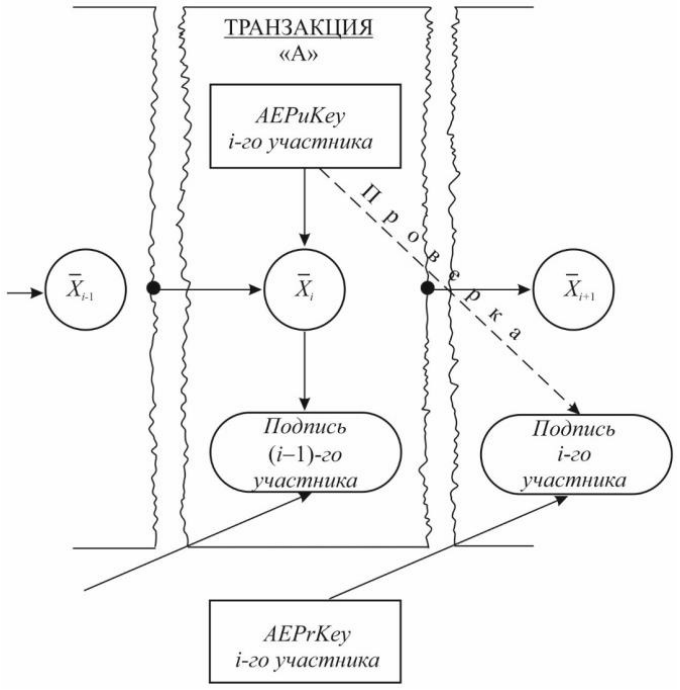


Рис. 1 – Схема учета и подтверждения транзакции «А» *i*-тым участником системы

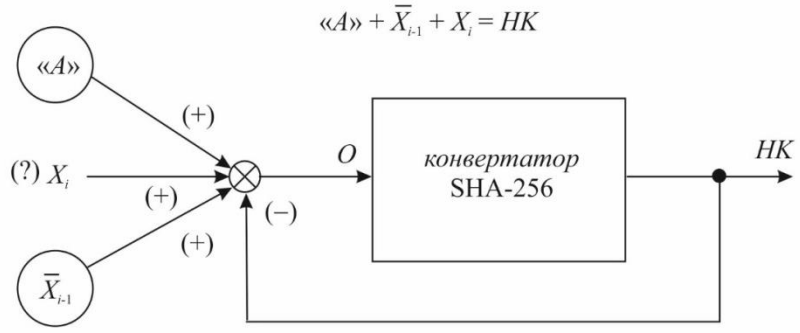


Рис. 2 – Упрощенная модель майнинговой операции

Решение задачи осуществляется многократно, до достижения результата. По данным Дино Марка Ангаритиса на 2015 год среднее число таких решений для каждой майнинговой задачи составляло $3 \cdot 10^{20}$ хешей, что не всякому компьютерному ресурсу под силу [2]. Появление таких инструментов как ASIC-майнинг резко снижает эффективность самых современных видеокарт в алгоритме SHA-256 (для биткоина), которыми владеет приватный майнер в домашних условиях. Уже запущен процесс «индустриализации» майнинга, когда крупные компании, занимающиеся этой процедурой, за счет крайне высоких мощностей имеют преимущества и получают большую часть вычислительных мощностей системы, максимально централизуя одну из главных операций блокчейна, «снимают» весь результат вне конкуренции.

p-ISSN: 2225-6733; e-ISSN: 2519-271X

8. На основании исходных данных майнер при помощи мощностей своей компьютерной системы подбирает необходимый код $x_i$ для нового протокола примерно в такой упрощенной интерпретации (см. рис. 2)

$$A + \overline{x}_{i-1} + x_i = HK .$$

Собственно *майнинг*, т. е. подбор числа $x_i = \overline{x}_i$, которое дало бы нам указанное равенство, осуществляется компьютерной системой методом подбора случайных чисел. Успех поиска зависит от мощности компьютерного оборудования, видеокарты, энергии и времени, затрачиваемого на майнинг. По данным И. Камински [7] усредненное количество энергии, расходуемое на операции майнинга в современном мире, соизмеримо с расходами энергии на острове Кипр.

9. Участник майнинга, первым нашедший число $\overline{x}_i$, сообщает его всем остальным участникам системы и после его проверки всеми участниками путем простой подстановки в программу SHA-256 опечатывает *i*-й протокол и кладет его в папку. Найденное число, обозначенное как $\overline{x}_i$, и является «печатью» для заполненного протокола с транзакциями всех участников системы за последнее время.

10. Таким образом, любой из «опечатанных» протоколов становится достоянием истории. Его уже невозможно переписать, изменить. Эта функция подтверждения (консенсуса) называется *«proof-of-work»* или *PoW*, – доказательство работы (реже можно использовать консенсус типа *«Proof of Stake»*, *PoS*, – доказательство владения). Любая последующая корректировка протокола участником системы легко выявляется другими участниками простым и условным подбором: если $A + \overline{x}_{i-1} + \overline{x}_i \neq HK$, это значит, что кто-то нарушил целостность протокола. Испорченный протокол будет ликвидирован, а нарушивший участник, в зависимости от целей такой корректировки, может заменить свой испорченный протокол либо выйти из числа участников системы.

11. Если один исключительный участник не подтвердил правильность майнинга числа $\overline{x}_i$, при том, что все остальные его подтвердили, идет дальнейшая проверка: либо этот участник неправильно записал найденное другим участником число $\overline{x}_i$, либо у него неправильные записи в протоколе транзакций, либо он нарушил правила работы. В этом случае исключительный участник уничтожает свой испорченный протокол и копирует правильный протокол у партнеров либо выбывает из системы.

12. Тот, кто предложит первым правильно найденное число $\overline{x}_i$, будет награжден за добавление блока поощрением, но не за счет других участников системы.

13. Возможен вариант, когда некто взломал цепочку и нарушил последовательность протоколов с «печатями». Теоретически он может начать свою собственную цепочку из искаженных транзакций (рис. 3). Но она легко вычисляется любым из участников, потому что один человек не в состоянии сравниться со скоростью транзакций всей остальной группы, с последовательным дублированием записей в протоколах партнеров по системе. Цепочки этого «некто» всегда будут короче, чем у остальных участников, что легко контролируется ими.

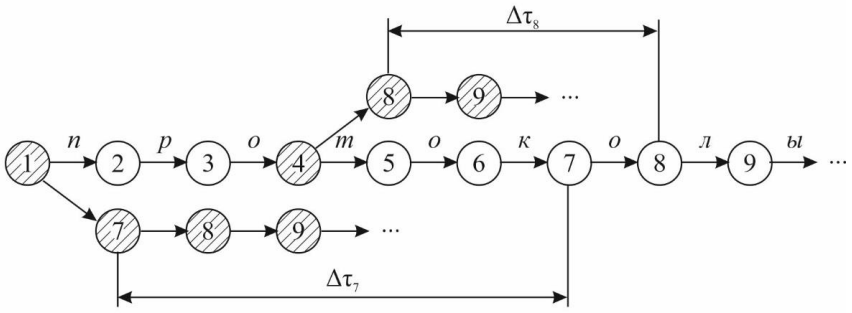


Рис. 3 – Механизм нарушения и распознавания целостности пиринговой сети

p-ISSN: 2225-6733; e-ISSN: 2519-271X

Блокчейн-технологии охватывают все большие области для применения, и результаты свидетельствуют о том, что за ними большое будущее. Сегодня мы вправе ожидать появления унифицированного и универсального механизма простого и надежного от взломов программного продукта, позволяющего большому количеству потребителей эффективно создавать локальные технологии типа распределенного реестра для решения самых различных задач децентрализации работы. Такого, какими в свое время стали оболочка Windows, пользовательский Office, интернет-сети и облачные технологии, универсальные инструментарии для повседневного применения.

**Выводы**

Читателю предложена упрощенная методика применения блокчейн технологии для решения различных стандартных задач в области управления, логистики, структуризации экономики предприятия и др. Показаны основные принципы создания таких систем для неподготовленного пользователя, некоторые их недостатки, с которыми можно встретиться при реализации. Все это дает возможности для более широкого применения блокчейн технологий в самых различных прикладных областях деятельности, позволит видеть в них инструмент для развития науки, бизнеса, образования.

**Список использованных источников:**

1. Винья П. Машина правды. Блокчейн и будущее человечества / П. Винья, М. Кейси; пер. с англ. М. Сухотиной. – М. : Манн, Иванов и Фербер, 2018. – 320 с.
2. Тапскотт Д. Технология блокчейн: то, что движет финансовой революцией сегодня / Д. Тапскотт, А. Тапскотт; пер. с англ. К. Шашковой, Е. Ряхиной. – М. : Эксмо, 2018. – 448 с.
3. Генкин А. Блокчейн: как это работает и что нас ждет завтра / А. Генкин, А. Михеев. – М. : Альпина Паблишер, 2018. – 592 с.
4. Thompson C. Apple Has a Smart Home Problem: People Don’t Know They Want It Yet [Электронный ресурс] : [Веб-сайт]. – Электронные данные. – Режим доступа: www.businessinsider.com/apple-homekit-adoption-2015-6.
5. An Executive’s Guide to the Internet of Things [Электронный ресурс] : [Веб-сайт]. – Электронные данные. – Режим доступа: www.mckinsey.com/business-functions/mckinsey-digital/our-insights/an-executives-guide-to-the-internet-of-things.
6. Пряников М.М. Блокчейн как коммуникационная основа формирования цифровой экономики. Преимущества и проблемы / М.М. Пряников, А.В. Чугунов // International Journal of Open Information Technologies. – 2017. – Vol. 5, no. 6. – Pp. 49-55.
7. Kaminska I. Bitcoin’s Wasted Power-and How It Could Be Used to Heat Homes [Электронный ресурс] : [Веб-сайт]. – Электронные данные. – Режим доступа: www.ft.com/content/384a349a-32a5-11e4-93c6-00144feabdc0.

**References:**

1. Vin’ia P., Keisi M. *Mashina pravdy. Blokchein i budushchee chelovechestva* [The machine of truth. Blockchain and the future of mankind]. Moscow, Mann, Ivanov i Ferber Publ., 2018. 320 p. (Rus.)
2. Tapskott D., Tapskott A. *Tekhnologiia blokchein: to, chto dvizhet finansovoi revoliutsiei segodnia* [Blockchain technology: what drives the financial revolution today]. Moscow, Eksmo Publ., 2018. 448 p. (Rus.)
3. Genkin A., Mikheev A. *Blokchein: kak eto rabotaet i chto nas zhdet zavtra* [Blockchain: how it works and what awaits us tomorrow]. Moscow, Al’pina Pablisher Publ., 2018. 592 p. (Rus.)
4. Thompson C. Apple Has a Smart Home Problem: People Don’t Know They Want It Yet Available at: www.businessinsider.com/apple-homekit-adoption-2015-6 (accessed 13 April 2019).
5. An Executive’s Guide to the Internet of Things Available at: www.mckinsey.com/business-functions/mckinsey-digital/our-insights/an-executives-guide-to-the-internet-of-things (accessed 05 March 2019).
6. Prianikov M.M., Chugunov A.V. Blokchein kak kommunikatsionnaia osnova formirovaniia tsifrovoi ekonomiki. Preimushchestva i problemy [Blockchain as the Communication Basis for the

**p-ISSN: 2225-6733; e-ISSN: 2519-271X**

Digital Economy Development: Advantages and Problems]. *International Journal of Open Information Technologies*, 2017, vol. 5, no. 6, pp. 49-55. (Rus.)
7. Kaminska I. Bitcoin's Wasted Power-and How It Could Be Used to Heat Homes Available at: www.ft.com/content/384a349a-32a5-11e4-93c6-00144feabdc0 (accessed 23 April 2019).

Рецензент: Е.Е. Пятикоп
канд. техн. наук, доц., ГВУЗ «ПГТУ»

Статья поступила 15.05.2019