Владимир И. Будзко, Дмитрий А. Мельников
Федеральный исследовательский центр «Информатика и управление» РАН,
ул. Вавилова, 44, корп. 2, г. Москва, 119333, Россия
e-mail: vbudzko@ipiran.ru, https://orcid.org/ 0000-0002-8235-0404
e-mail: mda-17@yandex.ru, https://orcid.org/0000-0003-4515-9712

ИСТОРИЧЕСКИЙ РАКУРС ТЕХНОЛОГИИ «BLOCKCHAIN». «ВСЁ НОВОЕ – ХОРОШО ЗАБЫТОЕ СТАРОЕ»

DOI: http://dx.doi.org/10.26583/bit.2018.4.02

Аннотация. Блокчейн-технология (БЧ-технология) представляет неизменяемые распределённые системы цифровых реестров без центрального хранилища/репозитария, как правило, не имеющие единого центра управления. В настоящее время существует большой ажиотаж вокруг использования БЧ-технологии, хотя сама технология, с одной стороны, многим ещё не совсем понятна, а с другой (и это главное) – не нова. Поверхностное представление о БЧ-технологии как о феномене с «волшебными свойствами» приводит к многочисленным прогнозам о возможности революционных преобразований на основе её применения целых отраслей экономики и прежде всего в кредитно-финансовой сфере (КФС). В связи с этим в настоящей статье представлены систематизированный анализ, история возникновения БЧ-технологии, ведущая своё начало с международных стандартов ISO 7498-2 от 1989 года и ITU-T X.800 от 1991 года. Дано краткое неформальное определение БЧ-технологии, рассмотрены ее основные принципы и компоненты, среди которых криптографические однонаправленные функции (ОНФ), транзакции, адреса и их извлечение, реестры, блоки, операции с последовательностями блоков. Представление БЧ-технологии как последовательности блоков, связанных на основе известных способов обеспечения целостности данных с использованием ассиметричной криптографии, позволяет сделать вывод о возможности только эволюционного развития ее применений, хотя и быстрыми темпами в масштабе реального времени, что является характерной особенностью современного этапа становления и всех остальных разновидностей IT-технологий. В заключение обращено внимание на необходимость проведения дополнительных исследований оценки защищённости и надёжности БЧ-технологии в аспекте оценки перспектив её применения в конкретных бизнес-приложениях и системах критической информационной инфраструктуры.

Ключевые слова: *блокчейн, цифровой реестр, криптовалюта, электронный кошелёк, электронная подпись, транзакция, целостность виртуального соединения, открытый ключ, однонаправленная функция, компендиум, сертификат, аутентификация, неотказуемость.*
Для цитирования: *БУДЗКО, Владимир И.; МЕЛЬНИКОВ, Дмитрий А. ИСТОРИЧЕСКИЙ РАКУРС ТЕХНОЛОГИИ «BLOCKCHAIN». «ВСЁ НОВОЕ – ХОРОШО ЗАБЫТОЕ СТАРОЕ». Безопасность информационных технологий, [S.l.], v. 25, n. 4, p. 23-33, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1158>. Дата доступа: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.02.*

Vladimir I. Budzko, Dmitry A. Melnikov
Federal Research Center «Computer Science and Control» of Russian Academy of Sciences,
Vavilov str., 44/2, Moscow, 119333, Russia
e-mail: vbudzko@ipiran.ru, https://orcid.org/0000-0002-8235-0404
e-mail: mda-17@yandex.ru, https://orcid.org/0000-0003-4515-9712

The Historical View Of The Blockchain Technology. The More Things Change, the More They Stay the Same

DOI: http://dx.doi.org/10.26583/bit.2018.4.02

Abstract. Blockchain technologies (BC) are immutable distributed systems of digital ledgers (i.e., without central repository) and, as rule, without central authority. Currently, there is a lot of excitement around the use of BC technology, although the technology itself, on the one hand, is still not quite clear to many ones, and on the other (and this is the main thing) is not new. Superficial understanding of the BC as a phenomenon with «magical properties» leads to numerous predictions about the possibility of revolutionary transformations based on its application to entire sectors of the economy and, above all, in the credit and financial sphere. In this regard, this article presents a systematized analysis, the history of the BC

emergence, leading from the international standards ISO 7498-2 of 1989 and ITU-T X.800 of 1991, as well as a brief informal definition of BC and considered are the basic principles and components of this technology, including cryptographic one-way functions (hashes), transactions, addresses and their retrieval, «digital wallets», ledgers, blocks, blockchain in operations. Representation of the BC as a sequence of blocks bounded base on known mechanisms of the data integrity with using asymmetric cryptography allows us to conclude that only its evolutionary development is possible, although at a rapid pace in real time. This is a characteristic feature of establishing modern stage of and all other IT types. In conclusion, attention is drawn to the need for additional research to assess the security and reliability of the BC in terms of assessing the prospects for its use in specific business applications and critical information infrastructure systems.

Keywords: blockchain; ledger; repository; cryptocurrency; digital wallet; digital signature; transaction; connection integrity; public key; one way function; compendium; certificate; authentication; non-repudiation.

For citation: BUDZKO, Vladimir I.; MELNIKOV, Dmitry A. The historical view of the blockchain technology. The more things change, the more they stay the same. IT Security (Russia), [S.l.], v. 25, n. 4, p. 23-33, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1158>. Date accessed: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.02.

Введение

В настоящее время в связи с объявлением программы цифровизации экономики существует ажиотаж вокруг вопроса применения технологии «блокчейн» (БЧ, *blockchain*), хотя сама технология многим ещё не совсем понятна, а главное – не нова. Множество статей и видеоматериалов научно-популярного характера описывают «волшебные» свойства БЧ-технологии[1], хотя в ней нет ничего «магического», так как эта технология базируется на хорошо известных специалистам принципах и поэтому не способна решить все проблемы. Как и в случае со всеми «новыми» веяниями, существует тенденция, связанная со стремлением применить её в каждом секторе экономики (бизнес-проекте), причём самым невероятным образом. БЧ-технология – последовательность (цепочка) криптографически связанных блоков. Система БЧ (СБЧ) представляет собой совокупность неизменяемых цифровых реестров (хранилищ, *ledger*), объединённых в распределённую структуру (т.е. без центрального хранилища – репозитария, *central repository*) и, как правило, не имеющих единого центра управления. СБЧ позволяет сообществам пользователей регистрировать транзакции в хранилище, которое открыто для этого сообщества. После того как транзакция стала открытой, она не может быть изменена в дальнейшем. В 2008 году идея БЧ [1] была объединена инновационным образом с несколькими другими технологиями и вычислительными ресурсами, что обеспечило формирование современных криптовалют (*cryptocurrencies*), т.е. электронных денег, защищённых с помощью криптографических методов, без центрального репозитария. Первая криптовалюта, основанная на СБЧ, была «Биткоин» (*BTC*, «*Bitcoin*» [2]). Новизна таких валют на основе СБЧ заключается в том, что они якобы имеют стоимостное выражение (*value*), а не только информационный контент. Стоимость «привязывается» к «электронному кошельку» (*digital wallet*), представляющему собой комплекс программного обеспечения (КПО), который позволяет его владельцу осуществлять электронные торговые сделки (*transactions*). Кошельки используются для подписи торговых сделок, которые транслируются из одного кошелька в другой, и регистрируют доставленную стоимость открыто, что обеспечивает всем пользователям сети возможность проведения независимой проверки подлинности транзакций. Каждый пользователь (участник СБЧ) может хранить полную запись всех транзакций, что делает сеть устойчивой к попыткам модифицировать такую запись (или фальсифицировать транзакции) в дальнейшем. Как правило, каждая транзакция включает в себя один или

[1] Например, в Финансовом университете при Правительстве Российской Федерации проводятся платные курсы (16800 ₽) по изучению БЧ-технологии («Криптовалюты и технологии блокчейн. Смарт-контракты и коллективное инвестирование»), которые призваны показать слушателям её «безграничные» возможности (http://www.fa.ru/org/dpo/fintechschool/Pages/bc.aspx).

несколько адресов и запись того, что произошло, а также электронную подпись (ЭП). БЧ состоят из блоков, каждый блок представляет собой группу транзакций. Все транзакции в блоке группируются вместе и объединяются с результатом вычисления криптографической однонаправленной функции предыдущего блока (называемой *свёрткой (компендиумом) сообщения* (*message digest*) или просто *компендиумом*, *compendium*) [3]. Наконец вычисляется новый компендиум (C_m) для заголовка текущего блока с целью его размещения в самих данных блока, а также в следующем блоке. Далее каждый блок «привязывается» к предыдущему блоку в «цепочке» (последовательности) блоков путём добавления компендиума предыдущего блока в заголовок текущего блока (рис. 1).

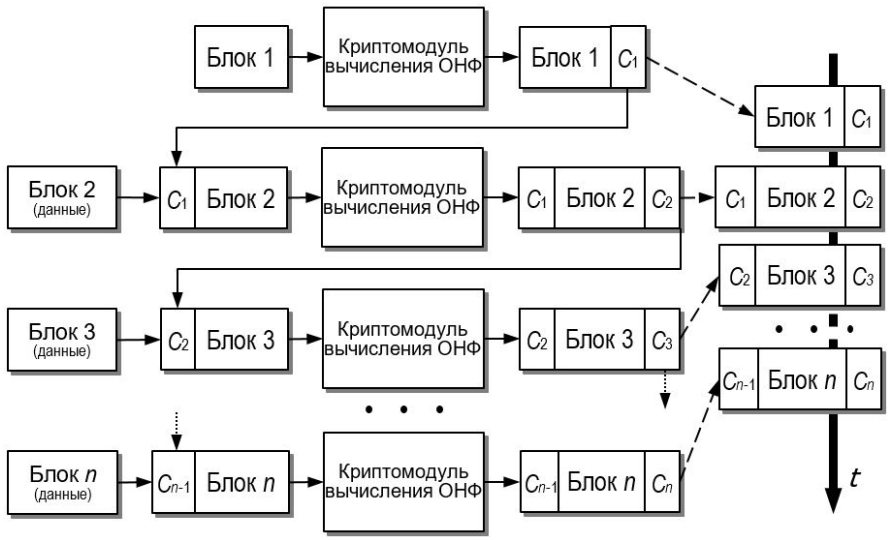

Рис. 1. Принцип формирования последовательности (цепочки) блоков данных
(Fig. 1. The sequence (chain) of data blocks creation principle)

В данной статье проанализирована ретроспектива появления и основные аспекты БЧ-технологии, а также сделан вывод о её дальнейшем применении.

1 Ретроспектива

Первое упоминание о «последовательности блоков», связанных с помощью криптографической функции (*binding*), появилось почти 30 лет назад в международном стандарте ISO 7498-2 от 1989 года [4], положившем начало развитию всей международной системы стандартизации в области информационной безопасности (ИБ). Полный аналог стандарта ISO 7498-2 – Рекомендация X.800 Международного союза электросвязи [5], вышедшая в 1991 году, в которой представлено понятие «*способ обеспечения целостности данных*» (*data integrity mechanism*) и, в частности, понятие «криптографическая связка».

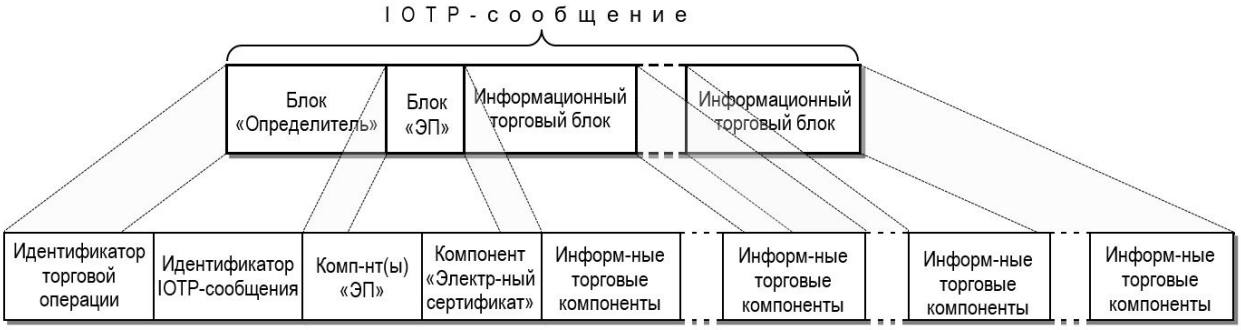

Рис. 2. Формат IOTP-сообщения
(Fig. 2. IOTP message structure)

Указанный способ обеспечения целостности широко применяется в электронной коммерции [6]. В интернет-сообществе принят стандарт RFC-2801 под названием «*Internet Open Trading Protocol*» (IOTPv1) [7]. Формат IOTP-сообщения представлен на рис. 2, а структура торговой транзакции IOTP-протокола – на рис. 3 [8].

Оба рисунка показывают, что каждая из взаимодействующих сторон (покупатель и продавец) подписывает каждое своё IOTP-сообщение, при этом каждая из них прибавляет к полученному IOTP-сообщению новый информационный торговый блок (ИТБ). В итоге завершающее IOTP-сообщение представляет собой последовательность ИТБ, в начале которой располагается определитель последовательности и субпоследовательность, состоящая из электронных подписей (ЭП) и сертификатов открытых ключей (СЕРТ|ОК) каждой из сторон. Наличие СЕРТ|ОК (это принципиальное отличие от СБЧ) позволяет проверить подлинность транзакции путём проверки владельца закрытого ключа ЭП и того, что на момент подписания электронного документа пара ключей не была просрочена и/или скомпрометирована. А в дальнейшем ЭП обеспечивает неотказуемость любой из сторон электронной торговой сделки, т.е. обеспечивает невозможность отказа любой из сторон от участия в транзакции.

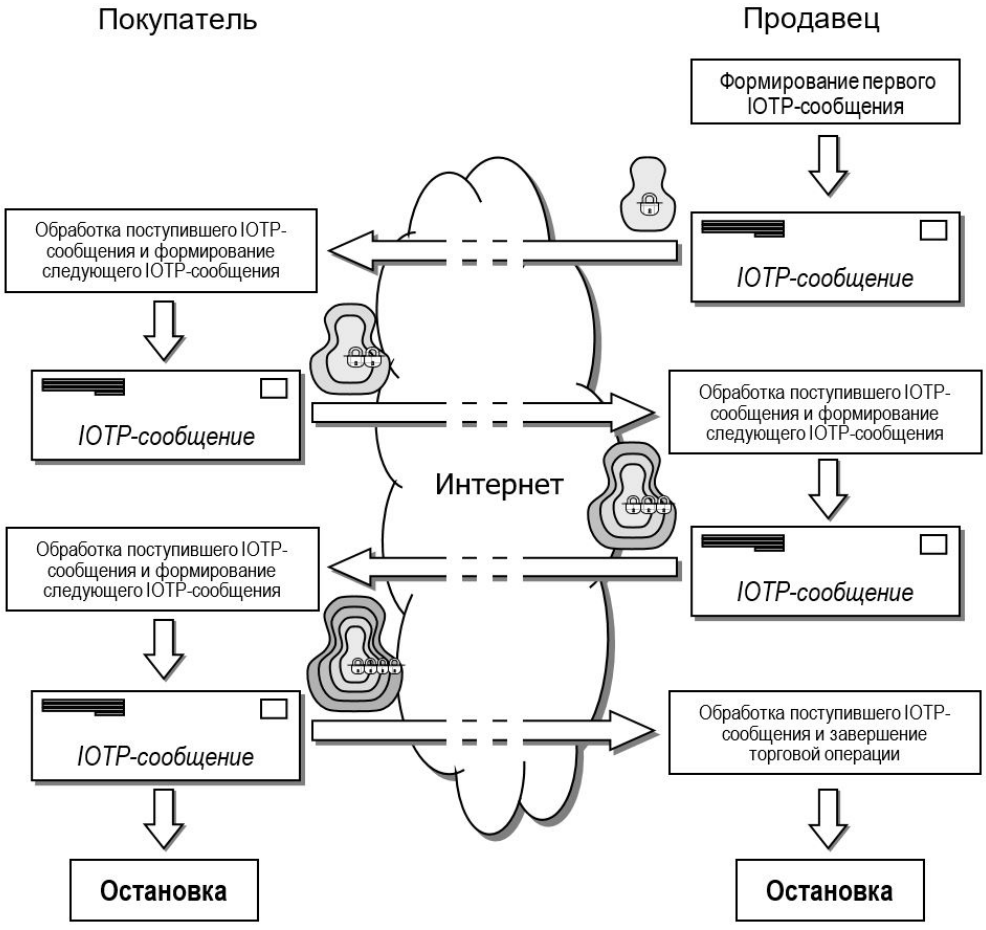

Рис. 3. Структура торговой операции (транзакции) IOTP-протокола
(Fig. 3. IOTP transaction)

В августе 2002 года был принят новый интернет-стандарт под названием «*Internet Open Trading Protocol Version 2 Requirements*» [9], в котором, в частности, содержатся два основных требования: отсутствие ограничений на число транзакций, включаемых в цепочку ИТБ (последовательность ИТБ может включать любое их число); наличие электронных кошельков в составе прикладных серверов (обязательное наличие КПО, реализующего функции электронного кошелька).

С прикладной точки зрения IOTP-протокол широко использует ассиметричные криптографические системы, а именно: ЭП, СЕРТ|ОК, инфраструктуру открытых ключей (*public key infrastructure*, PKI) [3] и соответствующие системы проверки ЭП и их авторов на основе подтверждения подлинности СЕРТ|ОК.

2 Основные принципы и компоненты СБЧ

СБЧ – это системы неизменяемых цифровых реестров, реализованные по распределенной структуре и, как правило, без центрального органа управления и контроля [10]. Они позволяют сообществу пользователей записывать транзакции в реестр, общедоступный для данного сообщества, и, как следствие, никакая транзакция после её опубликования не может быть изменена. Эта технология стала всемирно известной начиная с 2008 года (т.е. после IOTP-протокола), когда она была использована с целью создания условий появления и применения цифровых валют в распределённых финансовых системах, в которых осуществляется доставка электронных денег. Она способствовала развитию систем электронной коммерции, таких как «*Bitcoin*» (*BTC*) [2], «*Ethereum*» [11], «*Ripple*» [12] и «*Litecoin*» [13]. Из-за этого СБЧ очень часто рассматриваются как системы, связанные с *BTC* или, возможно, с электронными финансовыми системами в целом. Однако эта технология нашла более широкое применение и доступна для самых различных прикладных автоматизированных информационных систем (АИС).

С неформальной точки зрения, *БЧ-технологии* – это последовательности криптографически связанных блоков, которые представляют собой распределённые цифровые реестры, содержащие криптографически подписанные транзакции, сгруппированные в блоки. Каждый блок криптографически привязан к предыдущему блоку после подтверждения подлинности и принятия общего согласованного решения. Так как в последовательности криптографически связанных блоков постоянно добавляются новые блоки, модифицировать старые блоки становится всё значительно сложнее. Новые блоки дублируются во всех копиях реестров в сети, а любые конфликты разрешаются автоматически с использованием установленных правил.

2.1 Терминология

Для описания особенностей БЧ-компонентов используются термины «пользователь» (*user*) и «узел» (*node*). Термин «пользователь» может соотноситься с физическим лицом, организацией, объектом, бизнесом, ведомством и т.д., которые используют СБЧ. Термин «узел» означает систему внутри СБЧ и может означать «полнофункциональный узел» (*full node*, который хранит всю БЧ), «добывающий узел» (ДУ, *mining node*, полнофункциональный узел, который «публикует» новые блоки) или «усечённый узел» (УУ, *lightweight node*, узел, который не хранит всю БЧ).

2.2 Архитектура СБЧ

На самом верхнем уровне архитектура СБЧ использует стандартные компьютерные технологии («связанные» перечни (списки), распределённые вычислительные сети), а также криптографические алгоритмы и способы (ОНФ, ЭП, открытые/закрытые ключи), которые объединены с финансовыми концепциями (например, реестры).

2.2.1 ОНФ

Важный компонент БЧ-технологии – криптографическая ОНФ, которая применяется во многих процедурах, например, вычисление ОНФ по содержанию блока. Во многих БЧ-технологиях используется стандартный алгоритм вычисления ОНФ «*SHA*» (*Secure Hash Algorithm*) [14], который даёт выходную последовательность длиной 256 бит (SHA_{256}). Результат вычисления SHA_{256} – выходная последовательность, состоящая из 32 8-битовых субпоследовательностей. Из этого следует, что возможное число компендиумов составляет

$2^{256} \approx 10^{77}$, или

115792089237316195423570985008687907853269984665640564039457584007913129639936.

SHA_{256}-алгоритм считается устойчивым к коллизиям, так как для нахождения коллизии необходимо повторить SHA_{256}-алгоритм примерно 2^{128} раз.

2.2.2 Транзакции

В СБЧ под транзакцией понимается запись доставленных активов между взаимодействующими сторонами. Каждый блок в СБЧ включает несколько транзакций. Отдельная транзакция, как минимум, включает следующие информационные поля: *сумму* (*amount*) – общую сумму цифровых активов, предназначенных для доставки; *входные данные* (*inputs*) – перечень цифровых активов, которые подлежат доставке (их общая стоимость равна сумме); *выходные данные* (*outputs*) – учётные записи, определяющие получателей цифровых активов; *идентификатор/компендиум транзакции* (*transaction ID*/*Hash*) – уникальный идентификатор каждой транзакции.

2.2.3 Адреса и извлечение адресов

Адрес пользователя представляет собой короткую буквенно-цифровую последовательность ($\mathcal{C}_{\mathcal{K}_p}$), извлекаемую из открытого ключа ($\mathcal{K}_p$) пользователя с использованием ОНФ ($\mathcal{F}_H$), которая дополняется некоторыми данными (используемыми для обнаружения ошибок). Адреса короче открытых ключей, они несекретные. Как правило, процедура формирования адреса означает получение открытого ключа, его преобразование с помощью ОНФ и преобразование полученного компендиума в текстовый формат:

$$\text{открытый ключ } (\mathcal{K}_p) \rightarrow \text{ОНФ } (\mathcal{F}_H\ (\mathcal{K}_p)) \rightarrow \text{адрес } (\mathcal{C}_{\mathcal{K}_p})$$

Пользователи по своему желанию могут сформировать достаточно много пар ключей и, следовательно, много адресов, что позволяет им варьировать уровни псевдоанонимности. Адреса выступают в качестве открытых параметров подлинности пользователей в СБЧ, и часто адрес преобразуется в QR-код.

Когда СБЧ распределяет цифровые активы, она делает это путём присвоения им адресов. Чтобы потратить такой цифровой актив, пользователь должен доказать, что он (и только он) владелец закрытого ключа, соответствующего адресу.

2.2.4 Хранилище закрытых ключей

Большинство пользователей СБЧ не регистрируют свои закрытые ключи вручную, а, скорее всего, для их надёжного хранения будут использовать КПО, обычно именуемый как (электронный) «*кошелёк*». Электронный кошелёк (ЭК) может хранить закрытые ключи, открытые ключи и связанные с ними адреса. Кроме того, программная реализация ЭК может рассчитывать общее количество активов, которое может иметь пользователь.

Хранилище закрытых ключей – чрезвычайно важный компонент БЧ-технологии. В большинстве случаев БЧ-данные не могут быть изменены, поэтому после компрометации закрытого ключа и публичного перемещения связанных с этим ключом финансовых средств на другой счёт такую незаконную транзакцию отменить уже нельзя.

2.2.5 Реестры (электронные журналы бухгалтерского учёта)

Реестр представляет собой совокупность зарегистрированных транзакций [15, 16]. В настоящее время книги бухгалтерского учёта хранятся в цифровом виде (реестры), как правило, в больших БД, которые принадлежат и обслуживаются исключительно централизованными доверенными третьими сторонами (ДТС) от имени сообщества пользователей (т.е. ДТС – владелец реестра).

Несомненно, что любой централизованный реестр заинтересован в создании резервных копий данных, подтверждении подлинности транзакций, включении всех подлинных транзакций и неизменении истории. Встроенный реестр, использующий БЧ-

технологию, может снизить остроту указанных проблем за счёт использования способа распределённого согласования (консенсуса). БЧ-реестр будет дублироваться и распределяться между всеми узлами в системе.

Всякий раз, когда новые пользователи присоединяются к системе, они получают полную БЧ-копию, что затрудняет потерю или модификацию реестра. Все транзакции хранятся в блоках внутри СБЧ.

2.2.6 Блоки

Пользователи могут направлять в реестр транзакции-претенденты путём передачи таких транзакций в некоторые узлы, которые участвуют в СБЧ. Отправленные транзакции распространяются по другим узлам сети, но это само по себе не обеспечивает включения транзакции в СБЧ. Распределённые транзакции после этого ожидают в очереди, до тех пор пока не будут добавлены ДУ в СБЧ.

ДУ представляют собой подмножество узлов, которые обслуживают СБЧ путём опубликования новых блоков. Транзакции добавляются в СБЧ, когда ДУ публикуют блок. Блок включает совокупность подтверждённых транзакций. «Подлинность» гарантируется путём проверки того, что поставщикам финансовых средств в каждой транзакции принадлежит каждая криптографически подписанная транзакция.

Другие ДУ будут проверять подлинность всех транзакций в опубликованном блоке, и если блок будет содержать какие-либо недействительные транзакции, то его отвергнут.

После своего формирования каждый блок проходит обработку в соответствии с ОНФ-алгоритмом. В результате формируется компендиум, отображающий блок. Все узлы получат копию компендиума блока и затем смогут убедиться в том, что блок не был модифицирован.

На рис. 4 показан примерный состав «поля» данных, входящего в блок. «Уникальное слово» (*nonce value*) – это число, контролируемое (формируемое) ДУ с целью решения ОНФ-задачи, которое даёт ему право опубликования блока.

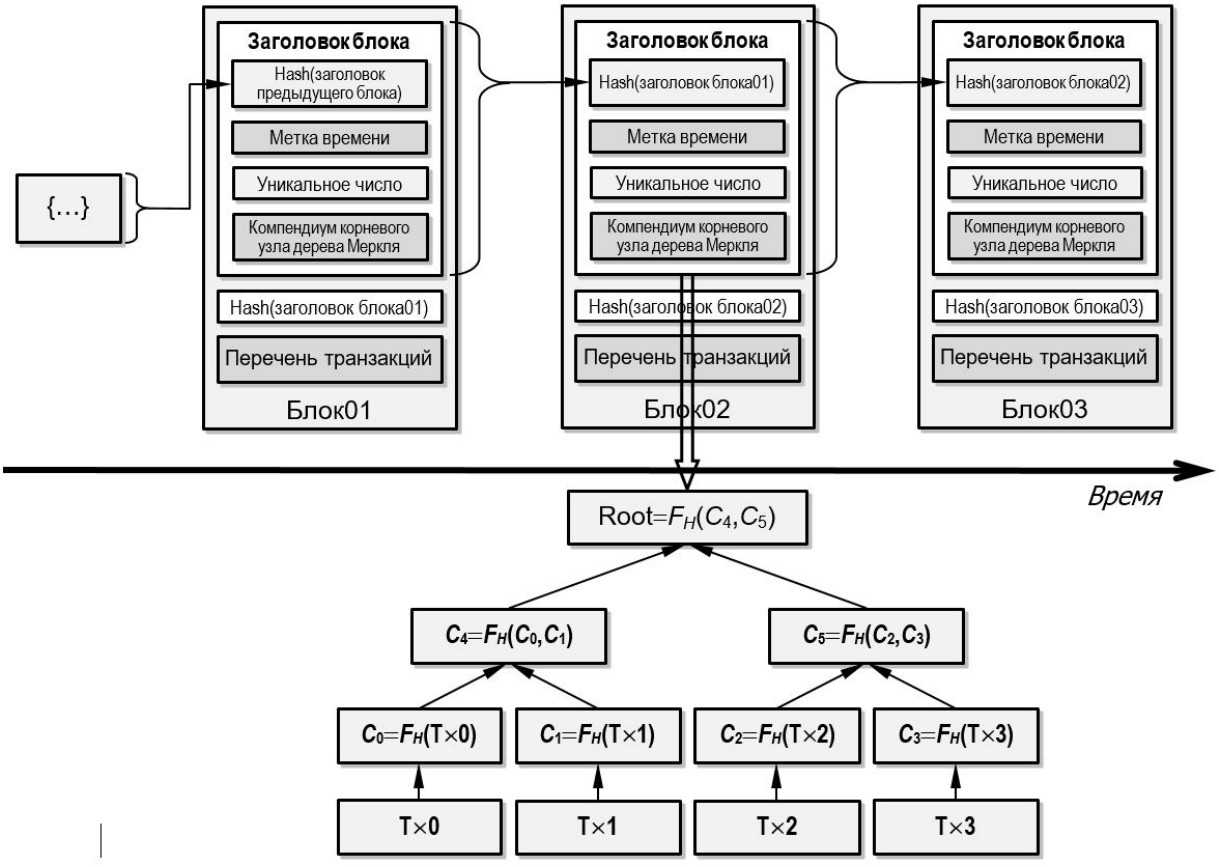

Рис. 4. БЧС на основе «дерева Меркли»
(Fig. 4. Blockchain with Merkle tree)

Вместо того чтобы хранить компендиум каждой транзакции в заголовке блока, используется структура данных, известная как «дерево Меркля» (ДМ, *Merkle tree* [1]). ДМ объединяет компендиумы данных до тех пор, пока существует единый корневой узел ДМ. Такой узел обеспечивает объединение транзакций в блоке и возможность проверки наличия транзакции в составе блока. Такая структура гарантирует, что данные, переданные по распределённой сети, достоверны, так как любое изменение исходных данных может быть обнаружено и такие данные могут быть отвергнуты. На рис. 5 представлен пример ДМ. Взаимосвязи между ДМ и блоком показаны на рис. 4.

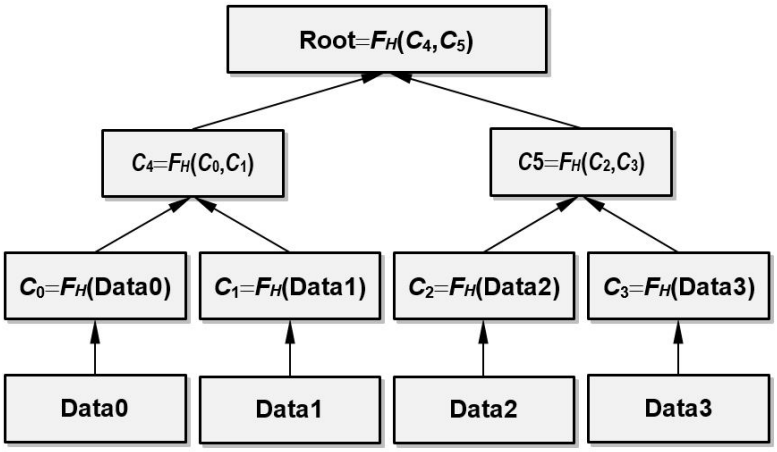

Рис. 5. Пример «дерева Меркля»
Fig. 5. Example Merkle Tree

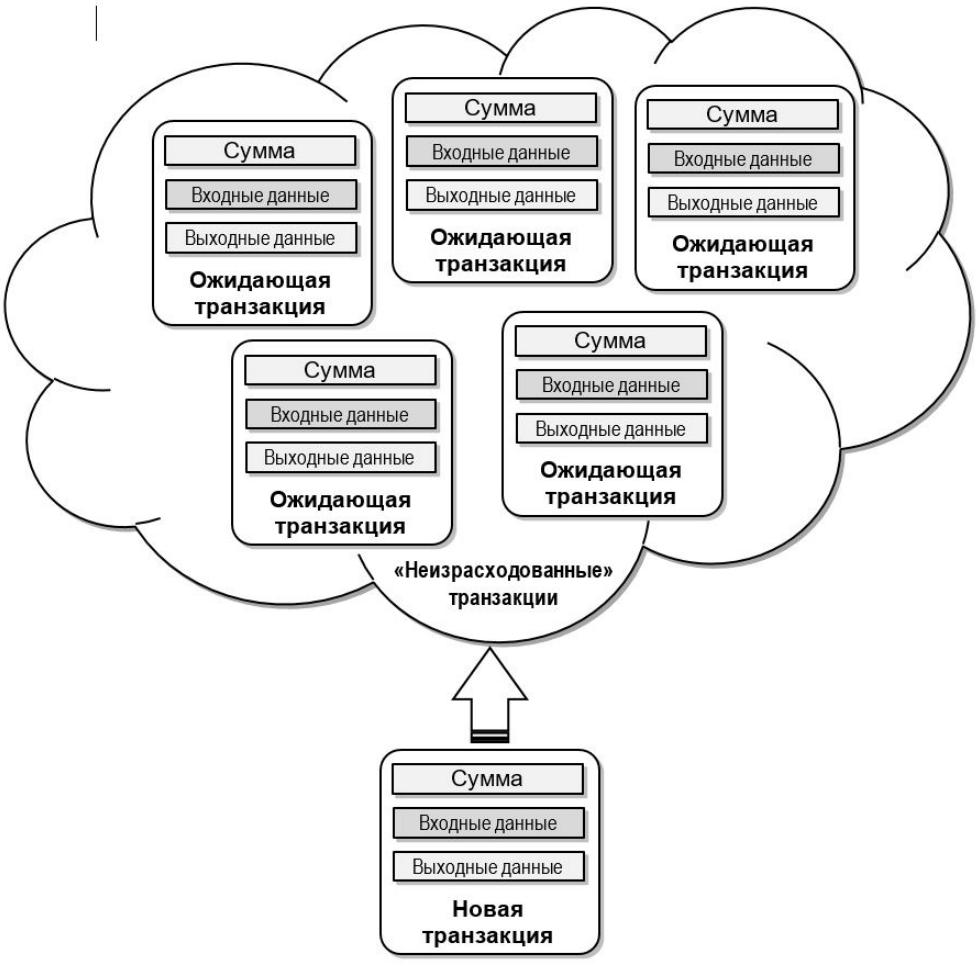

Рис. 6. Добавление транзакции в пул «неизрасходованных» транзакций
(Fig. 6. Transaction being added to unspent transaction pool)

3 Операции с последовательностями (цепочками) блоков

Рассмотрим процесс расширения СБЧ «без разрешения», который использует способ согласования (консенсуса) с доказательством «выполненной работы» (используется системой *BTC* и её аналогами). СБЧ функционируют на основании консенсуса (согласия) группы ДУ, использующих КПО БЧ. Каждый узел хранит копию БЧ и может предложить новый блок другим ДУ. Недействительные блоки будут выявляться и уничтожаться, так как весьма трудно вычислить действительный блок, но с вычислительной точки зрения его очень легко проверить. Добыча (*mining*, «майнинг») – это преднамеренно ресурсоёмкая задача, требующая больших объёмов вычислительной мощности, памяти или того и другого одновременно, что зависит от конкретной прикладной АИС с БЧ.

Функционирование ДУ заключается в хранении БЧ-данных, отправке данных другим узлам и обеспечении гарантий того, что вновь добавленные блоки действительные (подлинные). Подлинность обеспечивает гарантии того, что формат блока корректен, все компендиумы в новом блоке были вычислены правильно, новый блок содержит компендиум предыдущего блока, и каждая транзакция в блоке действительна и подписана соответствующими сторонами. ДУ могут формировать новые блоки. УУ не нужно хранить полные БЧ-копии, и очень часто они отправляют свои данные на обработку в полномасштабные узлы. УУ, как правило, встраиваются в смартфоны и устройства сети интернет-вещей. Такие устройства имеют ограниченные вычислительные ресурсы и/или объёмы памяти.

Предложенные транзакции в рамках СБЧ хранятся в ДУ в составе *пула «неизрасходованных» транзакций*, которые ожидают включения в блок (рис. 6).

Некоторые СБЧ требуют счёт об оплате за формирование нового блока, – например, за потраченное время и ресурсы или за предоставление привилегий. В системах, в которых требуются время и ресурсы, ДУ вычисляет несколько (достаточно много) значений случайных уникальных слов с целью попытки решить сложную с вычислительной точки зрения задачу («головоломку», *puzzle*).

ДУ-победитель получает право опубликовать следующий блок. Как правило, перед решением задачи ДУ опробуют много возможных значений уникальных слов. После того как задача будет решена, узел вычисляет компендиум данных блока и хранит его внутри самого блока. На рис. 7 представлена многоуровневая структура сформированного блока.

Рис. 7. Заключительный (обобщённый) блок
(Fig.7. Finalized (generalized) block)

Затем блок передаётся другим узлам для проверки. Если всё подтвердилось, то узлы принимают этот блок в качестве самого последнего (новейшего) и продолжают передавать его дальше по сети.

Заключение

Появление СБЧ было предопределено всеми предшествующими этапами развития информационных технологий, постоянно требующих их совершенствования с целью дальнейшего повышения уровня (качества) прежде всего государственного управления и/или бизнес-приложений. Поэтому, несмотря на применение в БЧ-технологии определенных инновационных решений, не стоит переоценивать ее «безграничные», революционные возможности применения во всех сферах цифровой экономики. Безусловно, СБЧ займут определенную нишу на рынке ИТ-технологий, в частности в сфере развития криптовалютных систем. Но, как и для всяких других прикладных АИС перспективы их практической реализации будут определяться возможностью выполнения основных принципов обеспечения информационной безопасности [17], среди которых: аутентификация (персонификация) и обеспечение неотказуемости для всех без исключения участников информационного взаимодействия, обеспечение надежности подсистемы обеспечения криптоключами. В настоящее время разработчики СБЧ просто игнорируют указанные принципы либо минимизируют их значимость. Другими словами, СБЧ пока что являются ненадёжными системами, которые не могут быть основой всеохватывающей инфраструктуры подтверждения подлинности (доверия), т.е. несут колоссальные риски. Отчасти это связано с принципиальной особенностью современных СБЧ, определенным преимуществом которых провозглашается принцип анонимности, обеспечивающий практически полное отсутствие централизованного (государственного) регулирования. С другой стороны, его реализация, очевидно, приведет к появлению новой сферы криминальной (и, возможно, террористической) деятельности. Таким образом, без решения указанной проблемы фундаментального характера давать какие-либо прогнозы о перспективах применения БЧ-технологий, особенно в сфере государственного управления, на объектах критической информационной инфраструктуры, пока что явно преждевременно.

СПИСОК ЛИТЕРАТУРЫ:

1. National Institute of Standards and Technology. «Blockchain Technology Overview». Draft NISTIR 8202, January 2018.
2. Nakamoto. S., «Bitcoin: A Peer-to-Peer Electronic Cash System», 2008. https://bitcoin.org/bitcoin.pdf
3. Фомичёв В.М., Мельников Д.А. Криптографические методы защиты информации: Учебник (в 2-х частях). — М.: Юрайт, 2016. ISBN 978-5-534-01741-0, ISBN 978-5-534-01740-3.
4. ISO, «Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture». ISO 7498 - 2: 1989.
5. ITU-T, X.800, «Security Architecture for Open Systems Interconnection for CCITT Applications», 03/1991.
6. D. Burdett, D.E. Eastlake III, and M. Goncalves, «Internet Open Trading Protocol», McGraw-Hill, 2000. ISBN 0-07-135501-4.
7. RFC 2801, «Internet Open Trading Protocol – IOTP Version 1.0», IETF, April 2000.
8. Мельников Д.А. «Организация и обеспечение безопасности информационно-технологических сетей и систем: Учебник». – М.: IDO Press. КДУ, 2015. ISBN 978-5-98227-960-6, 978-5-4243-0004-2.
9. RFC 3354, «Internet Open Trading Protocol Version 2 Requirements», IETF, August 2002.
10. Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfede, S., «Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction», Princeton University Press, 2016.
11. Wong, J. and Kar, I., «Everything you need to know about the Ethereum ‘hard fork’», *Quartz Media*, July 18, 2016. https://qz.com/730004/everything-you-needto-know-about-the-ethereum-hard-fork/.
12. «Introduction to Ripple for Bitcoiners», last modified December 10, 2013. https://wiki.ripple.com/Introduction_to_Ripple_for_Bitcoiners.
13. Hertig, A., «Litecoin’s SegWit Activation: Why it Matters and What’s Next», *CoinDesk*, April 26, 2017. https://www.coindesk.com/litecoins-segwit-activationwhy-it-matters-and-whats-next/.
14. National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 180-4, «Secure Hash Standard (SHS)», August 2015. https://doi.org/10.6028/NIST.FIPS.180-4.
15. Cachin, C., «Architecture of the Hyperledger blockchain fabric», in *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, July 2016.
16. «Hyperledger Business Blockchain Technologies», The Linux Foundation. https://www.hyperledger.org/projects.
17. Будзко В.И., Мельников Д.А. «Информационная безопасность и блокчейн» // Системы высокой доступности. 2018. Т. 14. № 3. С. 5 – 11.

REFERENCES:

[1] National Institute of Standards and Technology. «Blockchain Technology Overview». Draft NISTIR 8202, January 2018.
[2] Nakamoto. S., «Bitcoin: A Peer-to-Peer Electronic Cash System», 2008. https://bitcoin.org/bitcoin.pdf
[3] Fomichev V.M., Melnikov D.A. Cryptographic methods of information protection: Textbook (Two Paths). — M.: Urait, 2016. ISBN 978-5-534-01741-0, ISBN 978-5-534-01740-3. (in Russian).
[4] ISO, «Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture». ISO 7498-2: 1989.
[5] ITU-T, X.800, «Security Architecture for Open Systems Interconnection for CCITT Applications», 03/1991.
[6] D. Burdett, D.E. Eastlake III, and M. Goncalves, «Internet Open Trading Protocol», McGraw-Hill, 2000. ISBN 0-07-135501-4.
[7] RFC 2801, «Internet Open Trading Protocol – IOTP Version 1.0», IETF, April 2000.
[8] Melnikov D.A. «Organization and security management of IT networks and systems: Textbook». – M.: IDO Press. KDU, 2015. ISBN 978-5-98227-960-6, 978-5-4243-0004-2. (in Russian).
[9] RFC 3354, «Internet Open Trading Protocol Version 2 Requirements», IETF, August 2002.
[10] Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfede, S., «Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction», Princeton University Press, 2016.
[11] Wong, J. and Kar, I., «Everything you need to know about the Ethereum ‘hard fork’», *Quartz Media*, July 18, 2016. https://qz.com/730004/everything-you-needto-know-about-the-ethereum-hard-fork/.
[12] «Introduction to Ripple for Bitcoiners», last modified December 10, 2013. https://wiki.ripple.com/Introduction_to_Ripple_for_Bitcoiners.
[13] Hertig, A., «Litecoin’s SegWit Activation: Why it Matters and What’s Next», *CoinDesk*, April 26, 2017. https://www.coindesk.com/litecoins-segwit-activationwhy-it-matters-and-whats-next/.
[14] National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 180-4, «Secure Hash Standard (SHS)», August 2015. https://doi.org/10.6028/NIST.FIPS.180-4.
[15] Cachin, C., «Architecture of the Hyperledger blockchain fabric», in *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, July 2016.
[16] «Hyperledger Business Blockchain Technologies», The Linux Foundation. https://www.hyperledger.org/projects.
[17] Budzko V.I., Melnikov D.A. «Information security and blockchain» // Highly available systems. 2018. V.14. №3. p.p. 5 - 11. (in Russian).

Поступила в редакцию – 30 августа 2018 г. Окончательный вариант – 01 ноября 2018 г.
Received – August 30, 2018. The final version – November 01, 2018.