УДК 681.518

BLOCKCHAIN – ОСНОВНЫЕ ПОНЯТИЯ И РОЛЬ В ЦИФРОВОЙ ЭКОНОМИКЕ

Воронов М.П., Часовских В.П.

ФГБОУ ВО «Уральский государственный лесотехнический университет», Екатеринбург, e-mail: mstrk@yandex.ru

В настоящее время в России наблюдается оживленный интерес к технологии блокчейн (blockchain), как меняющей качество цифровой экономики. Поскольку в Российской Федерации данная технология является достаточно новой, в настоящий момент наблюдается малое количество русскоязычных научных публикаций, посвященных анализу функциональных возможностей технологии blockchain, проблематике ее применения в различных сферах деятельности, или раскрывающих понятия об основных компонентах технологии, обеспечивающих ее функционирование. Таким образом, на основе анализа зарубежных публикаций в данной статье представлены обобщенные характеристики основных компонентов технологии blockchain (криптовалюта, криптошифрование, трансакция, хеш-функция, хеш-значение, структура данных, целостность системы, распределенные системы, распределенные соглашения, пиринговые системы). В соответствии с выявленными характеристиками сформулировано наиболее полное определение технологии blockchain, представлено описание технологии и схема ее функционирования, определяется ее роль при использовании в рамках цифровой экономики. Также на примере одного из процессов цифровой экономики проиллюстрированы концептуальные отличия функционирования централизованных систем и распределенных систем (использующих технологию blockchain).

Ключевые слова: blockchain, технология блокчейн, цифровая экономика, распределенные системы, централизованные системы

BLOCKCHAIN – BASIC CONCEPTS AND ITS ROLE IN THE DIGITAL ECONOMY

Voronov M.P., Chasovskikh V.P.

Ural State Forest Engineering University, Yekaterinburg, email: mstrk@yandex.ru

Currently, in Russia, there is an interest in blockchain technology, which alters the quality of its digital economy. Since this technology is quite new in the Russian Federation, at the moment there is a small number of Russian-language scientific publications devoted to the analysis of the functionality of blockchain technology, the problems of its application in various fields of activity, or describing the main components of technology that ensure its functioning. Thus, based on the analysis of foreign publications, this article presents the generalized characteristics of the main components of blockchain technology (crypto currency, cryptographic encryption, transaction, hash function, hash value, data structure, system integrity, distributed systems, distributed agreements, peer systems). In accordance with the identified characteristics, the most complete definition of blockchain technology is formulated, a description of the technology and its operation scheme is presented, its role in the digital economy is determined. Also, as an example of one of the digital economy processes, conceptual differences between the functioning of centralized systems and distributed systems (using blockchain technology) are illustrated.

Keywords: blockchain, blockchain technology, digital economy, distributed systems, centralized systems

В настоящее время в России наблюдается оживленный интерес к цифровой экономике и технологии blockchain в частности [1, 2]. Blockchain (дословно «цепочка блоков») – это технология (структура данных и программный код) децентрализованного хранения данных, цепочка блоков транзакций, выстроенная по определенным правилам и обеспечивающая специфическую защиту от изменений.

Поскольку в настоящий момент наблюдается малое количество русскоязычных научных публикаций, посвященных проблематике технологии blockchain, целью данной работы стало определение технологии blockchain, ее основных компонентов и особенностей функционирования, а также определить роль и преимущества применения технологии blockchain в цифровой экономике.

Для того, чтобы составить себе детальное представление о технологии Blockchain, необходимо подробнее остановиться на базовых понятиях о таких ее компонентах, как [3]:

1. Криптовалюта (Bitcoins и прочие). Была разработана как средство для осуществления электронных платежей без посредничества финансовых институтов [4]. Часто рассматривается как одна из областей применения технологии blockchain. Для использования в рамках цифровой экономики средство платежей (криптовалюта) должно обладать следующими свойствами [3]:

– доступность и цифровая форма;

– признание во всем мире и в каждой стране в качестве средства платежа;

– свобода в движении от владельца к владельцу вне зависимости от их территориальной, национальной и иной принадлежности;

– стабильная ценность и покупательская способность;

– надежность и конвертируемость;

– отсутствие контроля со стороны какого-либо финансового института или государства.

В рамках технологии blockchain криптовалюта используется не только как электронное средство платежей, но и как средство для автоматизированного осуществления вознаграждений и штрафов участников за их вклад в развитие технологии [3]:

– за вклад в обеспечение целостности технологии;

– за вклад в обеспечение открытости технологии;

– за поддержку распределенной природы технологии;

– за вклад в развитие философии технологии.

2. Криптография (криптошифрование). Область знаний, которая при информационном взаимодействии дает возможность обеспечивать конфиденциальность (защита от просмотра третьими лицами), целостность (защита от стороннего изменения информации), аутентификацию (подтверждение подлинности сторон) информации, а также гарантирующая невозможность отказа сторон информационного взаимодействия от авторства [5]. Является крайне важной составляющей. В рамках технологии blockchain осуществляется с помощью криптографических хеш-функций.

3. Трансакция (transactions). В данном случае рассматривается как действие по передаче права собственности от одного участника технологии к другому. Каждая трансакция определяется следующими идентификаторами [4, 3]:

– идентификатор счета, владелец которого передает право собственности;

– идентификатор счета, владелец которого получает право собственности;

– количество товара (криптовалюты), на которое передается собственность;

– время, в которое должна быть осуществлена передача права собственности;

– комиссия, взимаемая за исполнение трансакции в рамках технологии;

– подтверждение согласия (подпись) передающего право собственности на осуществление трансакции.

4. Хеш-функция (hash function) и хеш-значение (hash value). Хеш-функция – это алгоритм, позволяющий представлять данные любого типа, независимо от размера в виде числа фиксированной длины (хеш-значения). Криптографические хеш-функции обладают следующими свойствами [6]:

– быстрое вычисление хеш-значения для любых типов данных;

– детерминизм – обеспечение соответствия хеш-значения исходным данным;

– псевдослучайность – непредсказуемость изменений хеш-значения при даже незначительном изменении исходных данных;

– необратимость – невозможность преобразования хеш-значения в исходные данные;

– противоречивоустойчивость – низкая вероятность подбора двух различных значений исходных данных, для которых вычисляемое хеш-значение окажется одинаковым.

Принимая во внимание перечисленные свойства, можно говорить о высокой надежности использования хеш-функций при идентификации исходных данных. Поэтому хеш-значения активно используются в рамках технологии blockchain для идентификации данных, в частности для подтверждения согласия на осуществление трансакции.

5. Структуры данных (data structures). В общем виде структура данных представляет собой набор переменных, объединенных определенным образом [7]. Также структура данных может быть определена как способ организации данных без учета их конкретного информационного содержания. В рамках технологии blockchain структура данных определяется как данные, структурированные в элементы, называемые блоками (blocks), связанные друг с другом по принципу цепочки (chain); из этого определения и происходит термин blockchain [3, с. 34]. В работе [3] в качестве аналогии блокам приводятся страницы, которые связаны между собой смысловым порядком и номером в рамках книги. Структуры данных тесно связаны с алгоритмами, при помощи которых эти данные будут обрабатываться [8]. Под алгоритмом в технологии blockchain понимается последовательность операций, при помощи которых информационное содержание множества структур данных в распределенных пиринговых системах согласуется между собой подобно системе демократического голосования [3].

6. Целостность системы (system integrity). Включает следующие составляющие:

– Целостность данных (data integrity) – обеспечение полноты, корректности и непротиворечивости создаваемых, корректируемых и хранимых в системе данных.

– Целостность поведения системы (behavioral integrity) – гарантирование отсутствия логических ошибок при работе системы, полного соответствия поведения системы запланированным сценариям ее развития и использования.

– Безопасность (security) – доступ к данным системы только для зарегистрированных пользователей, защита от несанкционированного использования данных системы.

7. Распределенные системы (distributed systems), включая программные средства распределенных вычислений [9]. В отличие от централизованной системы, в которой все данные хранятся на сервере, с которым связан каждый из пользователей системы, распределенные системы подразумевают порционное (распределенное) хранение данных на персональных компьютерах пользователей, связанных между собой и поэтому являющихся частью единой системы. Программные средства распределенных вычислений любой желающий может установить на свой персональный компьютер, тем самым вовлекая часть ресурсов своего компьютера в работу по проведению вычислений [9]. В сравнении с централизованными распределенные системы обладают следующими отличительными чертами:

– Повышение вычислительной мощности.

– Снижение денежных затрат на эксплуатацию, однако увеличение расхода вычислительных мощностей и затрачиваемых усилий с целью координации системы в целом и для обеспечения коммуникаций внутри системы.

– Высокая надежность системы в сравнении с централизованными системами, но при этом повышенная сложность программного обеспечения, координирующего работу системы.

– Способность развиваться естественным способом (путем включения новых пользователей в систему) и тем самым – почти бесплатно увеличивать вычислительную мощность системы, но при этом полная зависимость от работы сети и повышенные требования к безопасности в системе (чем проще осуществляется доступ к сети, тем выше требования к безопасности).

8. Распределенные соглашения (distributed consensus) – «соглашения» между персональными компьютерами в рамках чистых распределенных P2P систем о том, какой вариант истории трансакций считать верным (истиным), а какой – ошибочным (ложным). Основное предназначение распределенных соглашений – предотвращение так называемой «двойной траты» криптовалюты, т.е. осуществления трансакции по передаче собственности на сумму криптовалюты, которой нет на счете отправителя трансакции или собственность на которую уже была передана. Осуществление выбора между истинным и ложным вариантами истории трансакций осуществляется на основе подсчета агрегированной суммы вычислительных усилий, потраченных на создание истории трансакций. И основными критериями для оценки вычислительных усилий на создание истории трансакций являются:

– «Критерий длиннейшей цепочки» [4], т.е. цепочка blockchain, состоящая из наибольшего количества блоков, соответствует большей агрегированной сумме вычислительных усилий по ее созданию, чем по созданию более коротких цепочек.

– «Критерий тяжелейшей цепочки» [10]. Агрегированный уровень сложности цепочки часто называется весом цепочки, отсюда и название «тяжелой цепочки». Цепочка blockchain, для которой агрегированный уровень сложности по добавлению блоков к цепочке является наибольшим, соответствует наибольшей агрегированной сумме вычислительных усилий по ее созданию, чем по созданию цепочек с меньшим агрегированным уровнем сложности.

Соответствие по одному из этих критериев в отдельности не является достаточным условием для решения об истинности рассматриваемой цепочки, поскольку уровень сложности при создании каждого блока различается, т.е. «длиннейшая цепочка» не всегда требует наибольшей агрегированной суммы вычислительных усилий на ее создание. Аналогично, «тяжелейшая цепочка» (с наибольшим агрегированным уровнем сложности) не всегда является самой длинной. Однако соответствие цепочки blockchain обоим критериям в совокупности однозначно соответствует наибольшей агрегированной сумме вычислительных усилий и является достаточным условием для решения об истинности рассматриваемой цепочки.

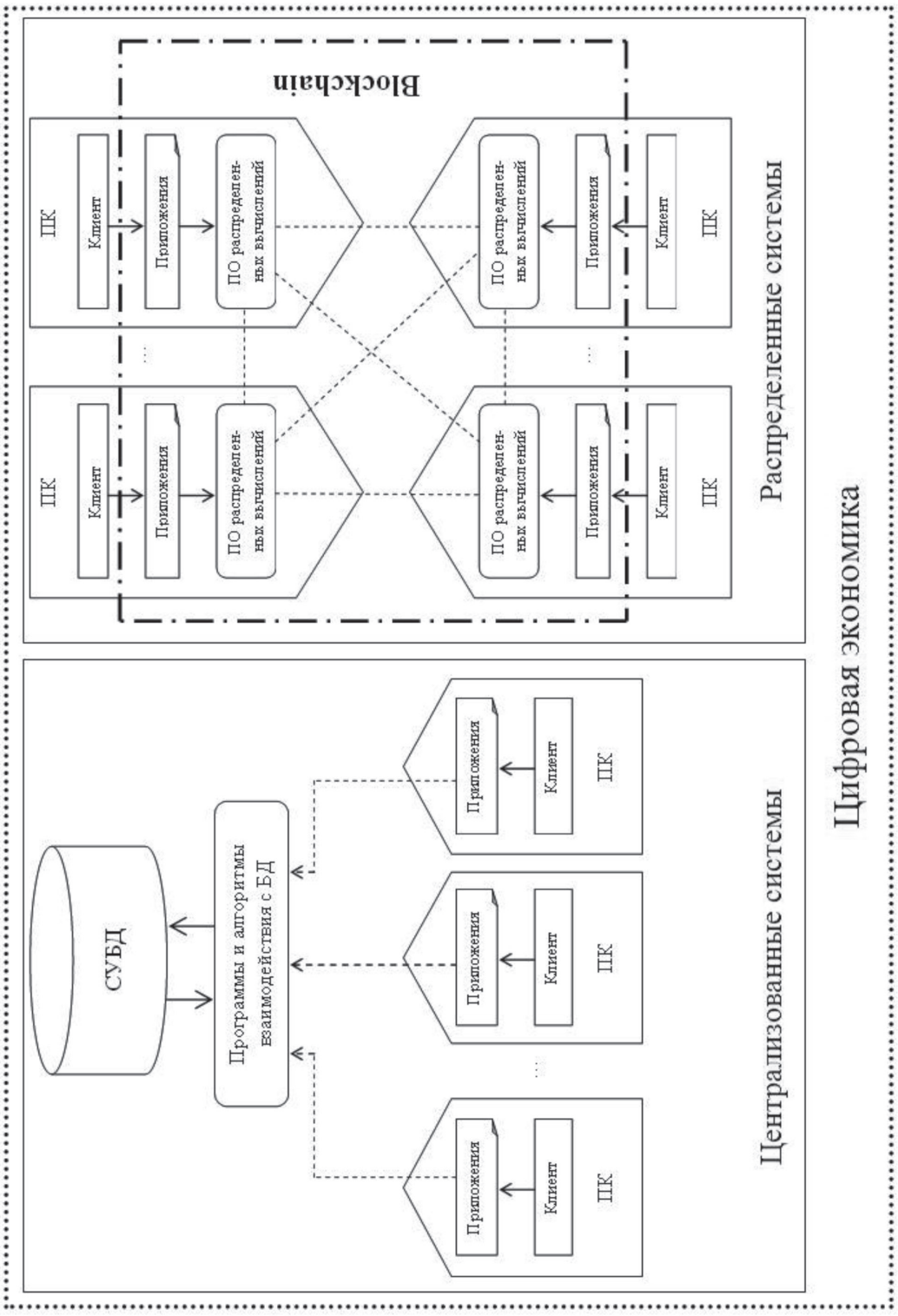
9. Пиринговые системы (peer-to-peer systems, P2P). Частный случай распределенных систем. Это распределенные системы, состоящие из узлов (персональных компьютеров), которые предоставляют доступ других узлов системы к своим вычислительным ресурсам (3, с. 23). P2P системы позволяют узлам системы взаимодействовать напрямую, без участия посредников. Также может рассматриваться как вид социальных коммуникаций, создаваемых на основе технологии web 2.0 [11]. При функционировании системы P2P используют такие ресурсы персональных компьютеров, как:

– вычислительные мощности;

– память жесткого диска для хранения информации;

– пропускная способность данных;

– пропускная способность сети.



Роль технологии Blockchain в цифровой экономике

За счет использования перечисленных видов ресурсов системы P2P обеспечивают пользователей системы таким функционалом, как:

– доступ к файлам;

– распределение контента (порционное хранение данных системы);

– защита данных.

Также существует отдельный подвид P2P систем – «централизованные пиринговые системы», имеющие центральный узел, который способствует взаимодействию между участниками системы (рядовых узлов – пиров), поддерживает директории с описанием сервисов, предоставляемых узлами системы, или выполняет поиск и идентификацию узлов системы [12]. Данный вид P2P систем позволяет комбинировать преимущества распределенной и централизованной системы.

Таким образом, опираясь на вышеизложенные понятия, можно рассматривать технологию Blockchain как средство обеспечения целостности в распределенных системах [3, с. 17]. В частности, чистые распределенные P2P системы используют технологию Blockchain с целью достижения и обеспечения целостности. Как правило, основными угрозами целостности P2P систем являются недобросовестные узлы (пиры) и технические сбои, в то время как для обеспечения целостности P2P системы в качестве основных факторов используются сведения о количестве узлов в системе и сведения о надежности каждого из узлов системы [3]. Если мы знаем количество и уровень надежности всех узлов в системе, мы достаточно легко способны обеспечить ее целостность. Однако, если эти факторы не определены, во много раз возрастает сложность задачи обеспечения целостности.

Роль технологии Blockchain в цифровой экономике может быть наглядно показана в виде схемы (рисунок). В рамках цифровой экономики могут существовать, функционировать и взаимодействовать и централизованные, и распределенные системы. Рассмотрим функционирование цифровой экономики на примере одного из ее процессов, а именно платежную систему, или «интернет-банкинг». Такая система должна обеспечивать конечного пользователя возможностями проверки баланса счета, перевода денег, оплаты услуг, размещения и снятия денежных средств со счета и т.д. Эти возможности могут обеспечиваться средствами как централизованных систем, так и распределенных систем (рисунок).

Функционирование централизованной системы в данном случае предполагает создание на сервере баз данных, хранящих данные о пользователях, счетах и произведенных операциях. Любая операция, производимая пользователем со своим счетом, отражается в этих базах данных. Для взаимодействия с базами данных пользователи устанавливают на ПК специализированное программное обеспечение (приложения – рисунок), либо использует web-сервис, являющийся частью платежной системы, с помощью которого осуществляет ввод и первичную проверку данных о желаемой платежной операции [9]. Следующим этапом является верификация отправляемых пользователем данных и обмен данными с БД с помощью программ и алгоритмов взаимодействия с БД (рисунок), установленных на том же сервере, что и СУБД. Любое взаимодействие между пользователями такой системы осуществляется через сервер-посредник.

В случае использования распределенной системы отсутствует сервер с централизованной БД и программами взаимодействия с ней. При этом ввод и первичная проверка данных о платежных операциях по-прежнему осуществляется посредством приложений, устанавливаемых на ПК пользователей системы. Функции же верификации и хранения данных в данном случае возлагаются на программное обеспечение распределенных вычислений (рисунок), которые осуществляют взаимодействие между пользователями системы (без сервера-посредника) и обеспечивают целостность и хранение данных в системе реестров, хранящихся на ПК тех же самых пользователей системы. То есть совокупность пользовательских приложений и программного обеспечения, осуществляющего хранение данных и взаимодействие участников системы, и получила название технологии blockchain (рисунок).

Результаты анализа, приведенного в данной статье, сводятся к следующим положениям:

1. Получено наиболее полное определение blockchain. Blockchain – это чистая распределенная пиринговая система реестров, использующих программное обеспечение, которое состоит из алгоритмов, согласующих и объединяющих информационное содержание упорядоченных и связанных блоков данных в единое целое, на основе технологий криптографии и безопасности, с целью обеспечения целостности системы.

2. Приведено описание и схема функционирования технологии blockchain (рисунок).

3. Определена роль blockchain в цифровой экономике. Она сводится к выполнению всех функций, связанных с хранением, изменением и доступом данных (т.е. функций,

традиционно выполнявшихся сервером-посредником в централизованных системах), а также функции взаимодействия между пользователями.

4. Определены отличия функционирования цифровой экономики на основе централизованных систем и распределенных систем (рисунок). Использование технологии blockchain позволит сокращать затраты на использование (за счет отказа от использования серверов-посредников) и одновременно повышать платежных и иных систем (за счет выше описанных преимуществ технологии blockchain).

5. Применение технологии blockchain возможно в разных сферах и секторах экономики, и, с нашей точки зрения, она весьма эффективна в вузовском образовании. Подобная технология наилучшим образом подходит для организации синхронного и асинхронного взаимодействия преподавателя и студента университета в рамках электронно-образовательной среды вуза.

Список литературы

1. Путин В.В. Пленарное заседание Петербургского международного экономического форума [Электронный ресурс]. – Режим доступа: http://kremlin.ru/misc/54667/videos/3509 (дата обращения 01.08.2017).

2. Институт экономических стратегий: конференция «На пороге цифрового будущего» [Электронный ресурс]. – Режим доступа: http://www.inesnet.ru/2017/05/konferenciya-na-poroge-cifrovogo-budushhego/ (дата обращения 01.08.2017).

3. Drescher D. Blockchain basis: a non-technical introduction in 25 steps. / D.Drescher – Frankfurt am Main: Apress, 2017. – 255 p.

4. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [Электронный ресурс]. – Режим доступа: https://bitcoin.org/bitcoin.pdf (дата обращения: 01.08.2017).

5. Основы криптографии: Учебное пособие / А.П. Алферов, А.К. Зубов, А.С. Кузьмин, А.В. Черемушкин. – 2-е изд., испр. и доп. – М.: Гелиос АРВ, 2002. – 480 с.

6. Rogaway P., Shrimpton T. Cryptographic hash-function basics: definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance // International Workshop on Fast Software Encryption. – Berlin Heidelberg: Springer. Lecture Notes in Computer Science, 2004. – vol. 3017. – P. 371–388.

7. Ахо А.В. Структуры данных и алгоритмы / А.В. Ахо, Д. Хопкрофт, Дж.Д. Ульман. – М.: Издательский дом «Вильямс», 2000. – 384 с.

8. Вирт Н. Алгоритмы и структуры данных / Н. Вирт. – М.: Мир, 1989. – 360 с.

9. Часовских В.П. Информационные системы в менеджменте лесопромышленного предприятия / В.П. Часовских, М.П. Воронов. – Екатеринбург: Уральский государственный лесотехнический университет, 2013. – 297 с.

10. Wood G. Ethereum: A secure decentralized generalized transaction ledger [Электронный ресурс]. – Режим доступа: http://gavwood.com/paper.pdf (дата обращения: 01.08.2017).

11. Воронов М.П. Становление концепции маркетинг 3.0 в контексте глобализации и развития социальных коммуникаций / М.П. Воронов, В.П. Часовских // Дискуссия. – 2013. – № 3 (38). – С. 103–114.

12. Tanenbaum A.S. Distributed systems: principles and paradigms / A.S. Tanenbaum, V.S. Maarten – Upper Saddle River, NJ: Pearson Prentice Hall, 2007. – 686 p.