ТЕХНОЛОГИИ РАСПРЕДЕЛЕННОГО РЕЕСТРА В ЦИФРОВОЙ ЭКОНОМИКЕ

Я.А. Мова, *студент*
Финансовый университет при Правительстве РФ, Уфимский филиал
(Россия, г. Уфа)

DOI: 10.24411/2500-1000-2020-10491

Аннотация. *В данной статье проанализированы и раскрыты технологические основы функционирования технологии распределенного реестра и преимущества ее применения. Приведена классификация типов сетей блокчейн по доступности реестра данных и их сравнительная характеристика. Рассмотрены существующие и возможные направления использования технологии блокчейн в финансовом секторе. Приведен перечень недостатков блокчейна, которые мешают блокчейну стать по настоящему общепризнанной прорывной технологией.*

Ключевые слова: *цифровизация экономики, блокчейн, смарт-контракт, блок транзакций, блокчейн сети, механизм консенсуса.*

2017 год стал переломным моментом в осознании российским Правительством, экспертным сообществом и гражданским обществом значимости темы цифровых технологий для развития страны – «цифровизация экономики – это вопрос независимости России и национальной безопасности, конкурентности отечественных компаний, позиции страны на мировой арене на долгосрочную перспективу» [1].

Модернизация традиционных отраслей экономики в производстве путем цифровизации и проникновения информационных технологий в экономические процессы создает основу для новых условий функционирования рынка и новых подходов к аналитике, прогнозированию и принятию управленческих решений.

Под «цифровизацией» (англ. – digitization, или digitalization) понимаются социально-экономические преобразования, инициированные массовым внедрением и использованием цифровых технологий, т.е. технологий создания, обработки, обмена и передачи электронных данных [2].

1. Технологические основы функционирования блокчейн

Блокчейн – распределенный реестр, или распределенная база данных, содержащая информацию обо всех операциях, проведенных участниками некоей блокчейн-системы. Информация хранится в виде «цепочек блоков» (отсюда название blockchain). В каждом блоке записано определенное число операций. Блоки логически связаны друг с другом, потому их и называют «цепочкой».

В случае с криптовалютами транзакциями выступают денежные переводы между кошельками пользователей, в случае использования технологии блокчейн для перехода права собственности на объект, транзакция фиксирует смену собственника и т.д.

Таким образом, технология блокчейн основана на 4-х основных понятиях:

– транзакция или смарт-контракт;

– цепочка блоков транзакций;

– децентрализованная (одноранговая) сеть, объединяющая узлы цепочки блокчейн;

– механизм «консенсуса» – это набор правил (протокол), который согласовывается узлами в сети, чтобы признать очередной блок транзакций истинным или ложным.

Смарт-контракт (англ. Smart contract) – компьютерный алгоритм, применяющийся для заключения контрактов в информационных системах использующих технологии блокчейн. В качестве подписи в смарт-контракте используются криптографические электронные ключи подписантов (сторон) контракта. Это значит, что смарт-контракты смогут существовать только внутри среды блокчейн, которая в свою очередь должна иметь беспрепятственный доступ своего исполняемого программно-

го кода ко всем объектам и условиям исполнения умного контракта. Все условия контракта должны иметь своё математическое описание, а также логику исполнения. Например, объектом умного контракта на поставку товара является поставляемый товар, а условием его исполнения – поступление денежных средств от заказчика на электронный кошелек (счет) умного контракта. При поступлении средств на счет умного контракта товар отгружается продавцом, а при подтверждении получения товара заказчиком денежные средства автоматически переводятся на счет продавца. Таким образом, умные контракты (Smart Contracts) используются для тех видов деятельности, где возможно автоматизированное исполнение обязательств сторонами без участия и оценки человеком. Умный контракт самостоятельно отслеживает, были ли в полной мере исполнены те или иные условия контракта. Умные контракты способны обеспечивать лучшую защищенность сторон контракта, чем традиционные контракты, основанные на праве, а так же снизить транзакционные издержки, связанные с заключением договоров и возможных судебных расходов по ним.

Блок транзакций – специальная информационная структура для записи группы операций в системах блокчейн. Транзакция (единичная операция) считается завершённой и достоверной, когда проверены её формат и цифровые подписи, и транзакции объединены в группу и записаны в специальную структуру – блок. Содержимое блока может быть проверено любым узлом, так как блоки содержат информацию от одного к предыдущему. Все блоки построены в цепочку, где содержится информация обо всех когда-либо совершенных в базе операциях. Только начальный блок в цепочке (англ. genesis block) не имеет родительского блока. Каждый блок цепочки содержит заголовок и транзакционный список. Заголовки блоков включают в себя свой собственный хеш, хеш предшествующего блока, транзакционные хеши и идополнительную служебную информацию. В идеале обработка транзакции в рамках блокчейн-технологии должна соответствовать следующим характеристикам [3]:

– согласование транзакции с текущим состоянием системы, т. е. при финансовой транзакции если баланс некоторого лица А составляет 3000 руб., он не может заплатить лицу В 30000 руб.;

– авторизация транзакции, т. е. только у лица А должен быть ключ к осуществлению транзакций от имени лица А;

– неизменяемость транзакции, т. е. после внесения транзакции в реестр, ее невозможно изменить (например, транзакция, в которой А платит В 500 руб., злоумышленники не могут изменить сумму – нет платежа, отправителя либо получателя);

– конечность транзакции, т. е. после того как транзакция занесена в реестр, ее невозможно удалить, что, по сути, привело бы к возврату денежных средств отправителю;

– цензурная устойчивость, т. е. если транзакция соответствует всем правилам блокчейна, она должна быть в него добавлена.

Децентрализованная (одноранговая, или peer-to-peer) сеть приведена на рисунке 1.

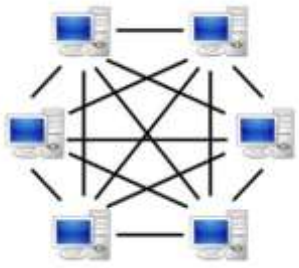

Рис. 1. Одноранговая (P2P) сеть [4]

Компьютеры в одноранговой сети называются «нодами» (nodes) или «узлами», и они работают совместно, чтобы гарантировать, что цепочка блокчейн является надежной и своевременной, т.е. узлы в одноранговой сети равноправны (нет центрального сервера) и связаны «каждый с каждым». Каждый узел хранит полную, обновленную версию блокчейн цепочки. Каждый раз, при добавлении нового блока, все узлы обновляют свою блокчейн цепочку. Использование одноранговой сети имеет следующие преимущества:

– всегда есть возможность проверить состояние цепочки блокчейн, используя программу-проводник (blockchain explorer).

– нет необходимости полагаться только на одну сторону, чтобы знать истинное состояние блокчейна.

– нет необходимости полагаться на безопасность одного сервера, для уверенности, что блокчейн защищен. Злоумышленникам придется одновременно взломать тысячи компьютеров, а не один сервер.

– уверенность в том, что блокчейн никогда не исчезнет, ибо для этого его надо уничтожить всем узлам.

Консенсусный механизм – это протокол, который позволяет узлам в одноранговой сети работать вместе, не зная и не доверяя друг другу. Консенсусный протокол устанавливает правила:

– каким образом блоки должны быть добавлены в цепочку блокчейн;

– когда и какие блоки считаются действительными;

– как разрешаются конфликты.

Существуют различные консенсусные протоколы используемые в технологии блокчейн [5]. В каждом конкретном случае проектируемой блокчейн-системы необходимо выбирать протокол консенсуса, который наилучшим образом удовлетворяет логике работы конкретной системы и ее предметной области (криптовалюта, регистрация права собственности, денежные переводы, электронное голосование и т.д.).

Обобщенная схема работы блокчейн системы приведена на рисунке 2.

По сути, блокчейн – система, записывающая проведение транзакции в хронологическом порядке со всеми сетевыми узлами, признающих действительность транзакций посредством выбранной консенсусной модели. Результатом являются транзакции, децентрализованно согласуемые всеми участниками сети , которые не подлежат отмене.

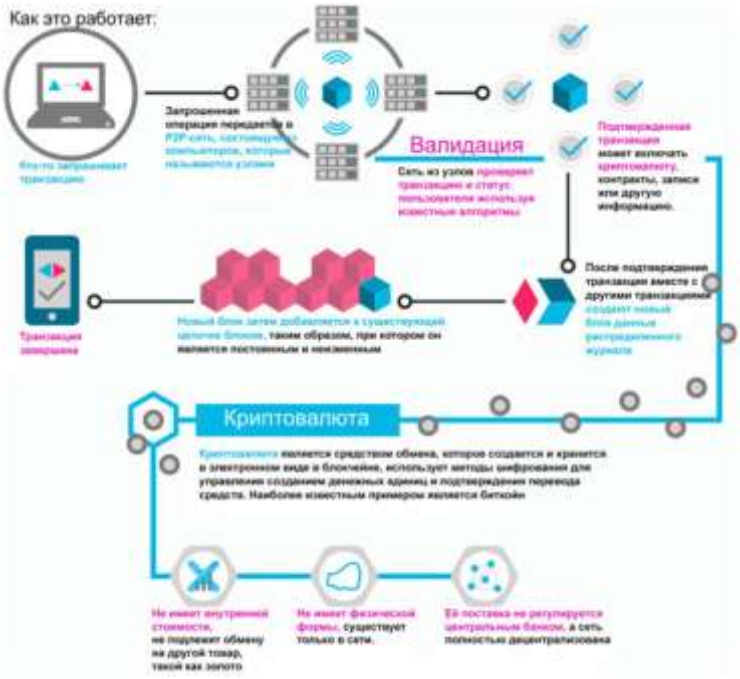

Рис. 2. Схема работы блокчейн системы [6]

2. Классификация типов сетей блокчейн

Цепочки блоков классифицируются по доступности реестра данных – именно по этому параметру делят блокчейн на типы (или классы). Выделяют три основные типа блокчейн цепей (распеределенных реестров):

– Публичная блокчейн цепочка/реестр (public blockchain). Она является полностью открытой для участников и каждый из них может как осуществлять операции в ней, так и участвовать в их администрировании.

– Блокчейн цепочка/реестр (consortium blockchains), принадлежащая консорциуму. В таких блочных цепях процедура согласования возлагается на заранее отобранные узлы. Часто, в таких цепях, выделяют роли пользователя и руководителя.

– Частная блокчейн цепочка/реестр (fully private blockchain). Администрирование и согласование процедур в такой сети осуществляется единым органом.

Сравнительная характеристика приведена в таблице 1.

Таблица 1. Сравнительная характеристика типов сетей блокчейн

	Тип блокчейна		
	Публичная блокчейн	Консорциум блокчейн	Частная блокчейн цепочка
Описание	Идентификация отсутствует	Идентификация участников сети	Идентификация в сети
	Ограниченииия для участия пользователей отсутствуют	Узкого круга допускающихся участников в сети (т. е. доступ к данным для клиентов является не прозрачным и ограниченным)	Опеделенные правила допуска для участия в сети (например, возможность просматривать только свои транзакции)
	Статус процесса не закрепляется за участниками	Статус валидаторов закрепляется за определенными контрагентами	Статус валидаторов закрепляется за определенными контрагентами
	Отсутствие надзора	Контролирующий орган	Контролирующий орган

В зависимости от типа блокчейн сети и предметной области в которой используется конкретная блокчейн система (криптовалюта, электронное голосование, регистрация перехода права собственности) по разному решаются две основные проблемы технологии блокчейн «стоимость верификации» блока (cost of verification – время потраченное на проверку блока) и «стоимость распространения блока по сети» (cost of networking-время на распространение блока по сети узлов блокчейн) [7].

3. Анализ возможных направлений использования технологии блокчейн в финансовом секторе

Многие исследователи вводят хронологию появления блокчейн [3]:

Блокчейн 1.0 – это криптовалюта. Криптовалюты применяются в различных приложениях, которые имеют отношение к электронным деньгам, например системы трансфера и электронных платежей.

Блокчейн 2.0 – это смарт-контракты. Классы приложений, в основе которых лежит технология блокчейн, работающие с различными типами финансовых инструментов – акциями, фьючерсами, облигациями, закладными и различными активами.

Блокчейн 3.0 – это приложения с областью применения выходящей за рамки денежных расчетов, финансов и рынков – это государственное управление, здравоохранение, наука, образование, культура и искусство.

На сегодня конечно самым известным и коммерчески успешным проектом использующим технологию распределенных реестров является криптовалюта биткоин. Но возможности предоставляемые технологией блокчейн выходят далеко за рамки эмиссии и обращения криптовалюты.

Блокчейн технология исследуется российскими банками. Так, Росевробанк в сотрудничестве с Microsoft предложил идентификацию клиента с помощью инфраструктуры Ethereum Consortium Blockchain через приложение другими банками, которые обмениваются данными с Росевробанком для идентификации клиента и определения его статуса. Открываются перспек-

тивы получения клиентом в одном месте (в одном приложении) услуг разных банков по принципу одного окна [8].

Центральный Банк России проводит тестирования на основе Microsoft Ethereum Consortium Blockchain новых программных комплексов «Мастерчейн» [9]. В основе – технология распределенных реестров для обмена и хранения информации о транзакциях. «Мастерчейн» станет интеграционной платформой на инфраструктуре ЦБ РФ, распределенными узлами которой будут российские банки. Система позволит интегрировать различные блокчейн и платежные системы. Система обеспечит среду цифрового доверия для баноков участвующих в обмене данными. Распределённые реестры хранят данные в зашифрованном (хешированном) виде, тем самым ни один банк участник не нарушает закона о доступе к персональным данным клиента, но при этом «Мастерчейн» позволяет управлять идентификацией, упрощать арбитража и ускорять взаимныые расчеты. Электронный документооборот с использованием электронно-цифровой подписи, на основе блокчейна, тестирует Сбербанк России.

Однако наряду с явными успехами у технологии блокчейн есть и проблемы. Аналитики Deloitte назвали пять препятствий, которые нужно преодолеть блокчейну, чтобы стать по настоящему общепризнанной прорывной технологией [10]:

– низкая скорость обработки транзакций. Зарекомендовавшие себя системы обработки транзакций могут обрабатывать десятки тысяч транзакций в секунду. Сейчас сервисы Ethereum обрабатывают всего 15 транзакций в секунду;

– отсутствие единых стандартов. Deloitte насчитала на GitHub 6500 блокчейн – проектов, которые отличаются разнообразием использованных языков программирования, протоколов и других решений. Для любого бизнеса отсутствие стандартов – это головная боль при внедрении;

– сложность и дороговизна. Разворачивание инфраструктуры для блокчейна – это серьезное препятствие для использования технологии. Amazon, Google и другие корпорации пытаются решить эту проблему, предлагая бизнесу использовать их облачные сервисы;

– отсутствие четких правил. 40% руководителей из сферы блокчейн называют законодательные пробелы препятствием для ее распространения, показал опрос Deloitte;

– избыток консорциумов. Разработчики технологии предпочитают объединяться в консорциумы, разрабатывая собственные стандарты и развивая свою инфраструктуру. Блокчейнов становится так много, что в них трудно разобраться.

Блокчейн – технологии представляют собой радикально новую тактику организации деловых и финансовых операций. Они знаменуют генерацию надежных и умных программных приложений для регистрации и обмена материальными и нематериальными, физическими и виртуальными активами. Благодаря ключевым понятиям криптографической безопасности, децентрализованному консенсусу и общему открытому реестру (должным образом контролируемому и ограниченному в видимости), технологии блокчейн могут коренным образом изменить организацию нашей экономической, социальной, политической и научной деятельности.

Необходимо чтобы Россия воспользовалась сложившейся научно-технологической ситуацией в мировой экономике, чтобы обеспечить глобально конкурентные позиции на бурно развивающемся рынке цифровой экономики.

Библиографический список

1. Выступление В.В. Путина 5 июля 2017 г. на заседании Совета по стратегическому развитию и приоритетным проектам. – [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/events/president/news/54983 (Дата обращения: 28.04.2020).

2. Цифровая экономика: глобальные тренды и практика российского бизнеса. – [Электронный ресурс]. – Режим доступа: https://imi.hse.ru (Дата обращения: 28.04.2020).

3. Бабкин А.В., Буркальцева Д.Д., Пшеничников В.В., Тюлин А.С. Технология блокчейн и криптовалюта в цифровой экономике: генезис развития. – [Электронный ресурс]. –

Режим доступа: https://economy.spbstu.ru/userfiles/files/articles/2017/5/01_babkin_burkaltseva_pshenichnikov_tyulin.pdf (Дата обращения: 25.04.2020).

4. Одноранговая (P2P) сеть. – [Электронный ресурс]. – Режим доступа: https://www.thinglink.com/scene/977515732151566338 (Дата обращения: 25.04.2020).

5. Proof of Stake versus Proof of Work. – [Электронный ресурс]. – Режим доступа: https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf (Дата обращения: 25.04.2020).

6. Схема работы блокчейн системы. – [Электронный ресурс]. – Режим доступа: https://blockgeeks.com/ (Дата обращения: 26.04.2020).

7. Университет Торонто. «Some simple economics of the blockchain». – [Электронный ресурс]. – Режим доступа: https://cdn.dal.ca/content/dam/dalhousie/pdf/faculty/management/cfb/Blockchain%20Article.pdf (Дата обращения: 25.04.2020).

8. TAdviser. «РосЕвроБанк» создал систему идентификации клиентов на базе блокчейна Microsoft. – [Электронный ресурс]. – Режим доступа: http://www.tadviser.ru/index.php/ (Дата обращения: 23.04.2020).

9. РБК. «Мастерчейн» – первый юридически чистый блокчейн в России. – [Электронный ресурс]. – Режим доступа: http://masterchain.rbc.ru (Дата обращения: 25.04.2020).

10. Обзор новостей по вопросам цифровой экономики. – [Электронный ресурс]. – Режим доступа: http://ac.gov.ru/files/attachment/18323.pdf (Дата обращения: 25.04.2020).

BLOCKCHAIN TECHNOLOGIES IN THE DIGITAL ECONOMY

Y.A. Mova, *Student*
Financial University under the Government of the Russian Federation, Ufa branch (Russia, Ufa)

Abstract. *This article analyzes and reveals the technological basis for the functioning of distributed registry technology and the advantages of its application. The author of the article gave a classification of types of blockchain networks based on the availability of the data registry and their comparative characteristics. The existing and possible directions of using blockchain technology in the financial sector are considered. The list of disadvantages of the blockchain, which prevent the blockchain from becoming a truly recognized breakthrough technology, is given.*

Keywords: *digitalization of the economy, blockchain, smart contract, transaction block, blockchain net, consensus mechanism.*