Вестник ЦЭМИ РАН. 2018-2023

ISSN 2658--3887

URL - <http://cemi.jes.su>

Все права защищены

Выпуск 1 Том 2. 2019

Технология блокчейн и уровни ее применимости.

Филькин Михаил Евгеньевич

*Центральный экономико-математический институт РАН
Москва, Нахимовский проспект, 47*

Аннотация

Статья посвящена обзору перспективных направлений развития технологии блокчейн. Приведены достоинства и недостатки, присущие данной концепции, обсуждены риски правового и технологического характера. Рассмотрены перспективы применения различных уровней блокчейн-технологии, аргументируется применимость специфики модели распределенного реестра к ряду экономических ситуаций. Обсуждаются возможности формализации коммерческих соглашений в терминах алгоритмов технологии блокчейн с целью создания эффективной системы мотивации экономических агентов.

Ключевые слова: виртуальная валюта, блокчейн, биткойн, смарт-контракты, распределенный реестр, криптовалюта, цифровая экономика.

Дата публикации: 02.07.2019

Ссылка для цитирования:

Филькин М. Е. Технология блокчейн и уровни ее применимости. // Вестник ЦЭМИ РАН. – 2019. – Т. 2. – Выпуск 1. URL: <https://cemi.jes.su/s265838870005646-3-1/>. DOI: 10.33276/S265838870005646-3

¹ Введение

² 31 октября 2008 году в сети Интернет появилась работа, автором (или группой авторов) которой значился Сатоши Накамото [1]. В работе описывалась концепция создания одноранговой сети, которая служила бы целям проведения электронных транзакций, аналогичным существующим платежным системам,

однако без привлечения посредников – финансовых организаций и институтов. Актив, который предлагался в качестве платежного средства, был назван биткойном. Биткойн представляет собой электронную запись на виртуальном «кошельке»; обмен активом происходит путем подтверждения методом доказательства выполнения работы (proof-of-work) на полностью децентрализованной системе распределенных вычислений. Транзакция между любыми кошельками-адресами системы является открытой и видимой всем участникам системы, платеж происходит без посредников и, будучи зафиксированным и подтвержденным в блокчейне, необратим. Электронный актив биткойн часто классифицируется как цифровая валюта, виртуальная валюта, электронная наличность, криптовалюта. Сатоши Накамото разработал протокол и опубликовал код системы в 2009 году, первая транзакция была проведена 12 января 2009 года. В мае 2010 был проведен первый известный обмен виртуальных биткойнов на реальный товар [2]. Начиная с этого времени, криптографические методы и технологии, использованные при создании биткойна, получили широкомасштабное развитие. Количество виртуальных валют (на апрель 2019 года их число составляет около 2 530 [3]) во много раз превысило количество «реальных» мировых валют, число которых составляет около 150. Однако использование технологии блокчейн в качестве децентрализованного распределенного массива данных (реестра), не ограничилось платежными функциями или имитациями таковых. В настоящее время ведутся исследования и практические разработки в области применения технологии для целей фиксации гарантийных обязательств, регистрации собственников материальных и нематериальных активов, ведения разнообразных реестров, учета исполнения контрактов и др. [4]. В настоящей статье сделан обзор ряда особенностей современной технологии блокчейн и обсуждаются перспективы использования данной системы в решении экономических задач.

3 Блокчейн или технология распределенного реестра.

4 Подробную информацию о том, как устроен и работает технология распределенного реестра (здесь и далее этот термин синонимичен термину «блокчейн»), можно найти в работе [5]. Здесь мы приведем основные особенности блокчейна, необходимые для понимания сферы его применимости. В настоящее время под блокчейном понимается последовательность (цепь, chain) блоков данных, которая последовательно растет по мере добавления новых записей в виде новых блоков, содержащих информацию о поступающих данных, часто универсально называемых транзакциями. Цепь блоков выстроена в хронологическом порядке, методы математической криптографии объединяют в неразрывную систему сами данные с моментом их записи в базу. Каждый участник сети в любой момент времени имеет актуальную базу данных и находится в контакте с другими участниками, называемыми узлами (nodes). Узлы с помощью специальной математико-криптографической процедуры могут добавлять новые блоки в базу, а также обязаны сообщать об изменениях списка блоков другим узлам. Опишем вкратце данную процедуру и механизмы, которые определяют надежность системы, что обусловило ее нынешнюю широкую популярность и перспективы применения. Изначально новая желаемая запись (традиционно будем использовать термин транзакция) попадает в пул необработанных транзакций,

который виден всем узлам сети. На данном этапе транзакция еще не является валидной, требуется ее подтверждение. Механизм подтверждения состоит в формировании блока узлами сети из пула имеющихся необработанных транзакций и подборе хэша, удовлетворяющего заданному разработчиками условию. Такой метод подтверждения называется доказательством выполнения работы (proof-of-work). Подбор хэша полностью случаен, функция его вычисления подбирается таким образом, чтобы исключить любые методы плавной сходимости или аналитического предсказания. Таким образом достигается вероятностная характеристика метода proof-of-work. Как только подбирается удовлетворительных хэш, новый блок рассылается всем участникам сети, которые верифицируют корректность подбора и автоматически подтверждают корректность транзакций, записанных в блоке. После того, как узлы сети «соглашаются» с соответствием блока всем условиям сети, узел, подобравший хэш, получает вознаграждение за проделанную работу. Цепь блоков удлиняется на найденный и хэшированный новый блок, а узлы сети начинают обработку новых транзакций из пула необработанных на основе уже обновленной базы. Каждый блок цепочки, начиная со второго, ссылается на предыдущий, что обеспечивает непрерывную верифицируемость всей цепи блоков.

⁵ Данная технология организации данных имеет следующие преимущества.

- Надежность: в случае наличия достаточно большого числа узлов сети вероятность проведения неправомерной транзакции, а также двойной траты, стремится к нулю.
- Децентрализация: распределение данных по большому числу ресурсов сети обеспечивает, с одной стороны, множественное дублирование данных и предотвращает их утрату, а с другой, не требует наличия единого финансового института-арбитра, подтверждающего валидность операций, что требовало бы необходимости доверия к этому институту.
- Открытость данных: все подтвержденные транзакции записаны в единую базу, доступную в любой момент всем узлам сети. Это позволяет проследить историю всех операций и исключает риски поддельных транзакций.
- Невозможность внесения в цепочку данных «задним числом». Как уже упоминалось, данные, записанные в блок, неразрывно связаны со временем создания блока. Через хэш-функцию все блоки (кроме первого) связаны со своими предшественниками. Внесение операции за любой прошедший период потребовало бы пересчета всех последующих хэшей блоков, что, в свою очередь, потребовало бы гигантских вычислительных мощностей и в конечном итоге (вероятнее всего) не было принято другими узлами сети [1].

⁶ Одновременно с достоинствами, необходимо отметить следующие недостатки системы.

- Псевдоанонимность: участниками транзакций являются виртуальные адреса-«кошельки», которые трудно, либо невозможно привязать к их владельцам, что создает риски нелегальных операций и усложняет для государств задачу контроля над финансовыми потоками.

- Необратимость операций: все подтвержденные транзакции остаются в системе навсегда и не могут быть исправлены или вычеркнуты из распределенного реестра.
- «Экологическое недружелюбие»: недостаток, обусловленный спецификой метода proof-of-work. Увеличение вероятности получения вознаграждения за поиск хэша подталкивает участников сети к использованию все большего количества вычислительных ресурсов и электрической энергии. По оценкам (см. [8]) в настоящее время минимальное годовое потребление энергии только майнерами биткойна составляет 38.5 тераватт-час. Это превышает годовое потребление электрической энергии многих стран мира.
- Отсутствие в настоящее время единой нормативной и юридической базы, обеспечивающей взаимодействия в сфере обращения цифровых валют.

⁷ «Экологическое недружелюбие», а также ряд других специфических недостатков системы proof-of-work обусловили поиски альтернативных методов подтверждения транзакций. Метод доказательства выполнения работы в настоящее время не единственный способ верификации блоков данных. Уже разработаны и применяются методы доказательства доли владения (proof-of-stake) [6], кроме того, обычно не переводящиеся на русский язык «доказательства деятельности» (proof-of-activity) [7], «доказательства емкости» proof-of-capacity и другие. В данной статье мы не будем останавливаться на их специфике, а обратимся подробнее перспективам применения блокчейн-систем для решения разнообразных экономических задач.

⁸ Уровни концепций применения блокчейн-технологий

⁹ Мелани Свон, основатель Института блокчейн-исследований (Institute for Blockchain Studies), разделяет технологические аспекты инструментария распределенного реестра на три категории [9]:

¹⁰ 1. Блокчейн 1.0: криптовалюта. Непосредственно концепция, разработанная Сатоши Накамото [1], заложившая основы технологии блокчейн. По данным [3] капитализация существующих 2 530 видов криптовалют на данный момент составляет более \$176 млрд., а ежедневный объем торгов ими превышает \$36 млрд. Данная категория блокчейн-систем, на наш взгляд, имеет специализированную, достаточно узкую сферу применимости, а именно анонимные платежи и спекуляции на биржевых курсах. Представляется, что на некотором этапе в массовом использовании останется ряд криптовалют, которые будут иметь скорость обработки транзакций, сопоставимый с существующими фиатными платежными системами (Visa, MasterCard и др.). Кроме того, волатильность этих цифровых валют по отношению к фиатным деньгам и другим массовым криптовалютам снизится до уровня, когда их можно будет использовать в виде удобного средства платежа. Однако на пути к этому есть ряд рисков как технологического характера (напомним, что, к примеру, наиболее популярная криптовалюта биткойн имеет предел на 7 транзакций в секунду), так и юридическо-правового. И тот, и другой риск может стать критическим для данной категории технологии блокчейн. На данный момент законодательства

большинства стран запрещают иметь средства платежа, альтернативные государственной валюте. Для центральных банков по мере роста популярности цифровых валют, все больше возникает проблема того, что они могут стать как раз такой альтернативной теневой системой.

11 2. Блокчейн 2.0 – это контракты. По-видимому, речь идет о так называемых смарт-контрактах. Свон утверждает, что на данной технологии будет работать «целый класс экономических, рыночных и финансовых приложений, в основе которых лежит блокчейн» [9]. На наш взгляд, это одно из наиболее перспективных направлений блокчейн-технологии. Смарт-контракт – это алгоритм, реализуемый в распределенном реестре, позволяющий заключать, контролировать исполнение, поддерживать и фиксировать в истории коммерческие соглашения. Центральным преимуществом, по нашему мнению, является возможность создания системы экономических стимулов, делающих невозможным или крайне невыгодным любое нарушение или уклонение от контрактных обязательств. Данная экономическая проблема в ряде случаев может быть сведена к задаче формулировки условий контракта в терминах алгоритмов блокчейна. Особенно привлекательным такой подход видится в свете начала широкого распространения Интернета вещей (Internet of Things, IoT). Интернет вещей – это концепция информационной сети некоторых объектов физического мира («вещей»), в которые встроены средства для взаимодействия друг с другом и с внешним окружением. В качестве примера такого смарт-контракта можно привести гипотетическую ситуацию сдачи квартиры в аренду. Если предположить, что обязательным условием пользования квартирой является своевременное внесение средств арендодателю каждое первое число месяца, то можно прописать смарт-контракт, в котором будет учтен контроль системой за наличием перевода средств на необходимый цифровой кошелек. В случае отсутствия платежа, система автоматически может давать сигнал на «умное» устройство (IoT) электронного замка квартиры, блокирующего вход вплоть до внесения средств (либо, к примеру, отключающего электричество в квартире). Все платежи и транзакции автоматически вносятся в распределенный реестр и верифицируются. Так, коммерческий контракт аренды квартиры может быть сформулирован в алгоритмах блокчейна, что позволяет создать систему стимулов для исполнения обязательств всеми сторонами и не требующего наличия контролера и арбитра.

12 3. Блокчейн 3.0 – это приложения. По классификации Свона это технологии, «область применения которых выходит за рамки денежных расчетов, финансов и рынков. Они распространяются на сферы государственного управления, здравоохранения, науки, образования, культуры и искусства» [9]. В данную категорию относятся как потенциально перспективные, так и уже применяемые способы организации данных, имеющих «реестровую природу». К примеру, таковыми могут быть реестры о праве собственности на земельные участки, свидетельства о регистрации транспортных средств, кадастры недвижимости, удостоверения личности, истории болезни и др. Этот уровень технологий уже начинает внедряться уже, в том числе, в некоторые российские компании [10].

¹³ Мы рассмотрели перспективные аспекты технологии распределенного реестра (блокчейн). На наш взгляд, наиболее многообещающими категориями будут те, которые обеспечат трансформацию стимулов экономических агентов в сторону мотивирования к выполнению контрактных обязательств. Одним из достоинств блокчейна является возможность алгоритмической формулировки условий коммерческих соглашений и автоматизированный контроль за их исполнением. В то же время существующие популярные на настоящее время криптовалютные воплощения, на наш взгляд, будут постепенно уходить в специализированную, возможно «маргинальную», нишу и играть менее значимую роль по сравнению с задачами организации хронологических баз данных для государственных и коммерческих нужд. Будучи относительно новой технологией, блокчейн с одной стороны, несет риски завышенных ожиданий, а с другой, сам по себе развивается в основном методом проб и ошибок. По данным исследования China Academy of Information and Communication Technology [11], исторически 92% блокчейн-проектов потерпели неудачу. Актуальной задачей является создание базовых протоколов технологии и нейтрализация ряда правовых и инструментальных проблем.

Библиография:

1. Nakamoto S. "A Peer-to-Peer Electronic Cash System" // Bitcoin. – URL: <https://bitcoin.org/bitcoin.pdf>
2. Mack E. "The Bitcoin Pizza Purchase That's Worth \$7 Million Today" // Forbes, December 23, 2013
3. Глобальный финансовый портал Investing.com // URL: <https://www.investing.com>. Апрель, 2019
4. A report by the UK Government Chief Scientific Adviser. "Ledger Technology: beyond block chain" // Government Office for Science, 2016
5. Генкин А., Михеев А. "Блокчейн. Как это работает и что ждет нас завтра" // М.: Альпина Паблишер. ISBN 978-5-9614-6558-7. 2017
6. Chohan, Usman W., "Proof-of-Stake Algorithmic Methods: A Comparative Summary" // Social Science Research Network (SSRN). February 28, 2018
7. Iddo Bentov I., Lee C. "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake", International Association for Cryptologic Research (IACR), 2014
8. Bitcoin Energy Consumption Index // Digiconomics. URL: <https://digiconomist.net/bitcoin-energy-consumption>, April, 2019
9. Свон М. "Блокчейн: Схема новой экономики" // М.: Олимп-бизнес, 2017

10. Газета «Коммерсантъ», архив электронного издания. «Газпром нефть» начала использование блокчейна при поставках оборудования // URL:

<https://www.kommersant.ru/doc/3535775>

11. China Academy of Information and Communication Technology. Trusted Blockchain Initiatives. "Blockchain White Paper" // URL:

http://www.caict.ac.cn/english/yjcg/bps/201901/t20190131_194150.htm, December, 2018

Blockchain technology and levels of its applicability.

Mikhail Filkin

CEMI RAS

Moscow, Nakhimovky prospect 47

Abstract

The possibilities of formalizing commercial agreements in terms of blockchain technology algorithms with the purpose of creating an effective system of motivation of economic agents are discussed.

Keywords: virtual currency, blockchain, bitcoin, smart contracts, distributed registry, cryptocurrency, digital economy.

Date of publication: 02.07.2019

Citation link:

Filkin M. Blockchain technology and levels of its applicability. // Herald of CEMI. – 2019. – V. 2. – Issue 1. URL: <https://cemi.jes.su/s265838870005646-3-1/>. DOI: 10.33276/S265838870005646-3