Цифровая экономика и криптовалюты: вызов или угроза традиционному обществу

Получено: 10.10.2018; одобрено: 20.11.2018; опубликовано: 29.12.2018

УДК 338.2:004.9 JEL E42 DOI 10.26425/2658-3445-2018-2-80-92

Звягин Леонид Сергеевич

Канд. экон. наук, доцент, ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», г. Москва, Россия
e-mail: LSZvyagin@fa.ru

АННОТАЦИЯ

Информационные технологии не стоят на месте, находятся в постоянном изменении, отталкиваясь от предыдущих инноваций, подстраиваясь не только под тенденции на рынке, но и изменяющуюся экономическую обстановку, в которой они обитают. Ключевым фактором развития и роста как мировой, так и российской экономики в современных реалиях является цифровая экономика. От нее зависит национальная безопасность и независимость страны, конкурентоспособность игроков, место страны на мировой арене. Цель данной статьи разобраться в перспективах применения информационных технологий цифровой экономики и изучить способы их использования в среде программирования, связанного на прямую с экономической ситуацией. Важно определение роли и преимуществ использования технологий в цифровой экономике.

Технологии блокчейн берут исток в появлении криптовалюты «биткоин», служащей альтернативной платежной системой, которая в свою очередь, в отличии от традиционных платежных систем, не контролируется ни государством, ни банками. Отличительной особенностью этой системы является то, что добавление и хранение данных осуществляется в рамках сети узлов и принимает вид линейной цепочки, следовательно необходимости привлекать центральный контролирующий орган в таких условиях нет. Добавление новых транзакций осуществляется только пользователями сети. Таким образом, для цифровой экономики система блокчейн представляет собой распределенную базу данных, состоящую из отдельных блоков, принимающих вид непрерывной цепи, которая хранит в себе как все имевшие место транзакции, так и все данные кошельков, когда-то существовавших – это «вечный цифровой журнал», который можно запрограммировать для регистрации почти всего, что представляет собой некую ценность. Именно это объясняет то, что в блокчейн-системе не только криптовалюта находит свое применение. Каждая ячейка блокчейна включает в себя метку с указанием времени и ссылку на предшествующий блок. Из-за чего она может быть фактически бесконечной, однако в реальной жизни возможности техники ее ограничивают.

В качестве передовой технологии в статье рассмотрена модель блокчейн, различные виды криптовалют, в частности биткоин, а также вопросы математических основ процесса цифровизации, системных архетипов и формирования рамочной модели.

КЛЮЧЕВЫЕ СЛОВА

Цифровизация, блокчейн, биткоин, криптовалюта, цифровая экономика, системные архетипы, рамочная модель.

The digital economy and crypto-currencies: challenge or threat to traditional society

Received: 10.10.2018; approved: 20.11.2018; published: 29.12.2018

JEL classification E42 DOI 10.26425/2658-3445-2018-2-80-92

Zvyagin Leonid

Candidate of Economic Sciences, associate professor, Financial University under the Government of the Russian Federation, Moscow, Russia
e-mail: LSZvyagin@fa.ru

ABSTRACT

Currently, information technologies are not standing still, they are in constant change, starting from previous innovations, adjusting not only to market trends, but also the changing economic environment in which they live. A key factor in the development and growth of both the world and the economy of our state in modern realities is the digital economy. It determines the national security and independence of the country, the competitiveness of the players, the country's place on the world stage. The aim of this article is to make an attempt to understand the prospects of application of information technologies of the digital economy and to study the ways of their use in the programming environment related directly to the economic situation. It is important to identify the role and benefits of technology in the digital economy.

Blockchain technology takes its origin in the emergence of cryptocurrency-bitcoin, which serves as an alternative payment system, which in turn, unlike traditional payment systems is not controlled by any state or banks. A distinctive feature of this system is that the addition and storage of data is carried out within the network of nodes, and takes the form of a linear chain, there is no need to involve a Central Supervisory authority in such conditions. Only network users can add new transactions. Thus, for the digital economy, the blockchain system is a distributed database consisting of separate blocks taking the form of an unbroken chain that stores both all the transactions that took place and all the data of wallets that once existed.it is an "eternal digital magazine" that can be programmed to register almost anything that represents a certain value. This explains the fact that not only cryptocurrency finds its application in the blockchain system. Each cell of the blockchain includes a timestamp and a link to the previous block. Because of what it can be virtually infinite, but in real life the possibilities of technology limit it.

As an advanced technology, the blockchain model, various types of cryptocurrencies, in particular bitcoin, as well as the issues of mathematical foundations of the digitalization process, system archetypes and the formation of the framework model have been considered.

KEYWORDS

Digitalization, blockchain, bitcoin, cryptocurrency, digital economy, system archetypes, framework model.

CITATION

Zvyagin L.S. (2018). The digital economy and crypto-currencies: challenge or threat to traditional society. *E-Management,* vol. 1, № 2, pp. 80–92. DOI: 10.26425/2658-3445-2018-2-80-92

В 2008 г. впервые прозвучали такие понятия, как «биткоин» и «блокчейн». Однако до сих пор мало кто может доступно объяснить их идею, а уж тем более описать технические подробности. Технология блокчейн, представляющая собой полностью реплицированную распределенную базу данных, была впервые задействована именно в биткоин-системе. Немногие знают, что появлению биткоина предшествуют тщательные исследования в криптографической отрасли, занявшие более 40 лет, и разработка концепции виртуальной валюты, занявшая около 20 лет.

ПОСТАНОВКА ПРОБЛЕМЫ, ЦЕЛИ И ЗАДАЧИ ИССЛЕДОВАНИЯ

С. Брэндс и Д. Чаум стали первыми людьми, предложившими использовать электронные деньги, и описавшими эту концепцию еще в 1983 г. Как мы понимаем, идея была революционной для тех лет. В 1997 г. А. Баков сделал существенный вклад в формирование концепции цифровых денег, который заключается в предложении к использованию системы Hashcash, противодействующей отправке спама. Hashcash явилась основой для создания блоков системе блокчейн, и открыла возможности для работы с первой в мире криптовалютой. Далее описаны самые значимые, по мнению автора, этапы, предшествующие появлению криптовалют, хотя, конечно, история их появления значительно более насыщенная.

Технологию блокчейн называют прорывом, и утверждают, что за ней стоит будущее. Рассмотрим, что кроется за этим понятием и какую пользу приносит блокчейн обществу, бизнесу и человеку.

Чтобы представить мир блокчейна, можно попробовать представить мир, в котором происходят стремительные изменения, где все прозрачно, анонимно и что самое важное – защищено на все сто процентов. Большинство людей ассоциируют блокчейн с биткоином, а также с криптовалютами (что верно), но блокчейн представляет собой нечто большее, чем просто финансовый инструмент.

В финансово-экономическом словаре «криптовалюта» определяется как «единое название для денежных суррогатов, полученных с помощью компьютеров». На сегодня не существует единой интерпретации термина «криптовалюта». Существует несколько подходов к ее статусу, согласно которым она понимается как: денежное средство; товар; универсальный финансовый инструмент; денежный суррогат. Для того чтобы сформулировать свойства и функции криптовалюты, необходимо перейти к рассмотрению самой первой и крупнейшей криптовалюты – к биткоину (BTC).

История создания началась с биткоина. Создал ее японец С. Накомото в период сильного кризиса. Первой статьей, опубликованной по этой теме, принято считать фрагмент из e-mail рассылки The cryptography mailing list на сайте metzdowd.com от 31 октября 2008 г. Статья называлась «Bitcoin: A Peer-to-Peer Electronic Cash System», в ней была описана система электронной наличности — Биткоин. Первая версия биткоин-кошелька появилась 9 января 2009 г., тогда же был осуществлен запуск в сеть Биткоин. В течение года проводились определенные доработки. Была введена в поддержку операционной системы Linux (биткоин известен лишь небольшой группе его разработчиков и тестеров). Первый форум был открыт в ноябре 2009 г., этот шаг помог привлечь новых пользователей. Обмен биткоинов на реальный товар произошел в мае 2010 г. Начиная с 2012 г., проект bitcoin курирует американская компания Bitcoin Foundation. Разработчик этой компании – Г. Андресен, главная цель – создание безопасной, стабильной наличности в сети Интернет. С 2010 г. в погоне за выгодой многие люди начали заниматься майнингом (производством биткоинов). Постепенно интернет-магазины и сервисы стали принимать криптовалюту в качестве оплаты. С тех пор популярность биткоинов только растет.

Биткоины создаются как вознаграждение за выполнение математических вычислений – эта работа носит название майнинг. Суть майнинга заключается в том, что пользователи предоставляют свои компьютеры для верификации адресов и записи транзакций в реестр. В награду за это майнеры получают вновь создаваемые биткоины и комиссию за совершенные транзакции. Также эту криптовалюту можно получить в обмен на обычные фиатные деньги или с помощью электронного кошелька[1].

Биткоин, как и почти все криптовалюты, базируется на блокчейне. Блокчейн – многофункциональная и многоуровневая информационная технология, которая предназначена для надежного учета различных

[1] *Блокчейн* – новые возможности для производителей и потребителей электроэнергии / Исследование PwC (по заказу Центра по консультированию потребителей (Verbraucherzentral) земли Северный Рейн-Вестфалия, г. Дюссельдорф). Режим доступа: https://www.pwc.ru/ru/publications/blockchain.html (дата обращения: 23.09.2018).

активов [Равал, 2017]. Эту технологию возможно применять не только для совершения криптовалютных транзакций, но и во многих других сферах общественной жизни (медицина, образование, нотариат и т. д.). Блокчейн – цепочка блоков данных, которая постоянно растет по мере добавления майнерами новых блоков со сведениями о последних транзакциях. Это происходит примерно каждые 10 минут. У отправителя и получателя биткоинов есть кошельки, содержащие адрес и закрытый и открытый ключ (технология асимметричного шифрования); информация об определенной транзакции хешируется или, по-другому, кодируется, и майнеры пытаются обнаружить этот криптографический хеш, чтобы подтвердить совершенную транзакцию. Удобство данной технологии в том, что пользователям видно, какая, когда и на какую сумму была произведена транзакция, но в то же самое время вся персональная информация об отправителе и получателе недоступна.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ И ИХ АНАЛИЗ

Разберемся, могут ли криптовалюты выполнять те же функции, что и обычные деньги: мера стоимости, средство обращения товара, средство платежа, средство накопления, мировые деньги. С помощью биткоинов можно выразить стоимость товаров и услуг, также ими можно оплатить товар (существуют интернет-магазины и кафе, принимающие в качестве оплаты биткоины). Функция средства платежа биткоина отражается в технологии «умных контрактов», в них можно комбинировать любые условия оплаты, что напоминает обычные сделки, но здесь нет необходимости в доверии обеих сторон друг другу, так как умные контракты основаны на технологии блокчейн. Таким образом, возможно заключение договора с отложенной оплатой в биткоинах. Что касается функции средства накопления, то биткоины можно хранить в специальных электронных кошельках. Они будут сохранять свою стоимость, и даже увеличивать ее из-за усложнения процесса майнинга. Главной причиной того, почему биткоин не может использоваться в качестве мировых денег, является их ограниченность: они не могут полностью обеспечить обращение всех товаров и услуг.

Можно сделать вывод, что биткоин теоретически может стать мировой валютой, если он будет признан обществом, однако, учитывая повсеместное недоверие к криптовалюте, это крайне маловероятно. Если рассматривать криптовалюту с точки зрения марксистской теории, то биткоин – это товар, так как он может служить всеобщим эквивалентом всех других товаров. Существует также мнение, что криптовалюта – это денежный суррогат, так как она не выпущена государством и является заменителем законного платежного средства.

Ограниченность количества биткоинов наталкивает на мысль, что криптовалюта является финансовым инструментом, так как при добыче всех 21 млн биткоинов они будут применяться скорее в качестве инструмента для получения спекулятивного дохода, нежели как средство платежа.

Строение в системном виде

Для лучшего понимания работы и обращения криптовалют, составим и разберем схему по созданию стоимости биткоина и его обороту (рис. 1).

Составлено автором по материалам исследования

Рис. 1. Создание стоимости биткоина и его оборота

Цена на биткоин может формироваться двумя способами.

Первый:

1) происходит сам непосредственный майнинг биткоинов посредством создания сети или цепочки блоков;

2) цепочка блоков образует специальное приложение, в котором функционирует;

3) и уже в этом приложении формируется цена биткоинов.

Второй способ заключается в том, что биткоины, созданные майнерами, попадают в руки к спекулянтам, и цена формируется в ходе спекуляций с виртуальной валютой.

Математическая база построения биткоин-блокчейна

Популярность биткоина и вслед за этим возросший спрос на приложения для работы с криптовалютой во многом обеспечены строгой математической базой построения биткоина. Она обеспечивает гарантию надежности сделок между участниками сети, исключая воздействие человеческого фактора.

Разберем подробней математические основы биткоин-блокчейна, а именно эллиптические кривые, ECDSA (Elliptic Curve Digital Signature Algorithm) и ключи, используемые в системе. В основе биткоина лежат криптографические алгоритмы (совокупность операций, производимых над текстом при приведении его в уникальный, конфиденциальный вид (при криптографических преобразованиях)). Одним из таких алгоритмов является ECDSA, основе которого лежат эллиптические кривые и конечные поля для подписи данных (используется для защиты от подделки и подтверждения третьей стороной аутентичности подписи). Рассмотрим процессы, используемые в данном алгоритме для подписи и верификации данных.

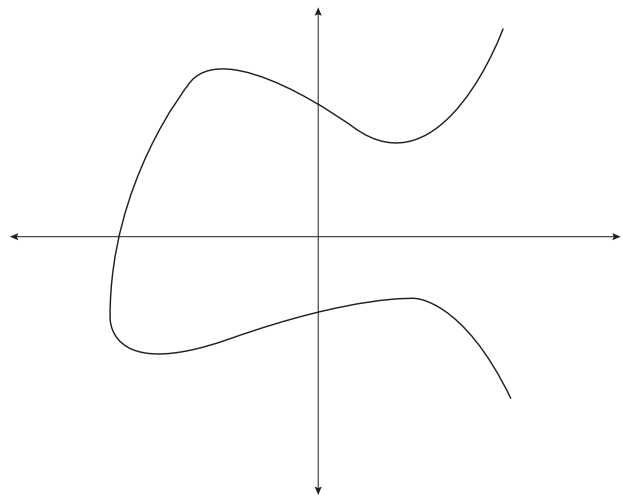
Эллиптические кривые

Эллиптическая кривая над полем – кубическая кривая над алгебраическим замыканием поля K, задаваемая уравнением третьей степени с коэффициентами из поля K и «точкой на бесконечности» [Коблиц, 2001, с. 254]. Одной из форм эллиптических кривых являются кривые Вейерштрасса.

$$y^2 = x^3 + ax + b. \quad (1)$$

В биткоине используются коэффициенты.

Построим график функции (рис. 2).



Составлено автором по материалам исследования

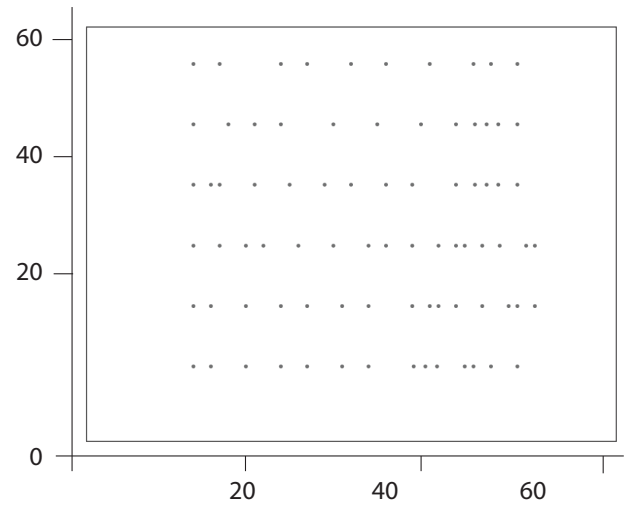
Рис. 2. График функции $y^2 = x^3+ax+b$, эллиптическая кривая

В эллиптической криптографии (ECC) используется рассмотренная кривая, на конечном поле, в котором отражаются результаты положительных вычислений.

$$y^2 = x^3 + ax + b \ (\text{mod } p). \quad (2)$$

Эллиптическая кривая биткоина определена на конечном поле.

Значение модуля 67, выглядит данное поле как множество точек (рис. 3), в которых все значения x и y представляют собой целые числа между 0 и 66.



Составлено автором по материалам исследования

Рис. 3. Эллиптическая кривая биткоина, определенная на конечном поле по модулю 67

ECDSA в биткоине

Протокол биткоина основывается на наборе параметров для эллиптической кривой и ее конечного поля, чтобы каждый пользователь использовал строго определенный набор уравнений. Среди зафиксированных параметров выделяют уравнение кривой, значение модуля поля, базовую точку на кривой и порядок базовой точки.

Рассмотрим значения для биткоина.

Уравнение эллиптической кривой: : $y^2 = x^3 + 7$.

Простой модуль: $2^{256}–2^{32}–2^9–2^8–2^7–2^6–2^4–1$= FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F[2].

Базовая точка:

*0*4 ***79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798*** 483*ADA*77 26*A3C*465 5*DA4FBFC 0E*1108*A*8 *FD*17*B*448 *A*6855419 9*C*47*D08F FB*10*D*4*B*8.

Жирным шрифтом выделена координата x в шестнадцатеричной записи. За ней сразу следует координата y.

Порядок:

*FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE*6 *AF*48*A03B BFD*25*E*8*C D0*364141.

В криптографии используется стандарт SEC (Standards for Efficient Cryptography).

В биткоине кривая используется совместно с алгоритмом цифровой подписи ECDSA.

В ECDSA секретный ключ – случайное число между единицей и значением порядка. Открытый ключ формируется на основании секретного: последний умножается на значение базовой точки.

Открытый ключ = секретный ключ · G.

Вычисление открытого ключа выполняется с помощью тех же операций удвоения и сложения точек. Когда пара секретный/публичный ключ получена, ее применяют для подписи данных.

[2] Математические основы биткоин-блокчейна / Блог компании Bitfury Group (все программные расчеты). Режим доступа: https://habr.com/ru/company/bitfury/blog/340378/ (дата обращения: 19.09.2018).

Порядок действий:

1) хеширование данных с целью получения уникального значения с числом битов, равным битности порядка кривой (256).

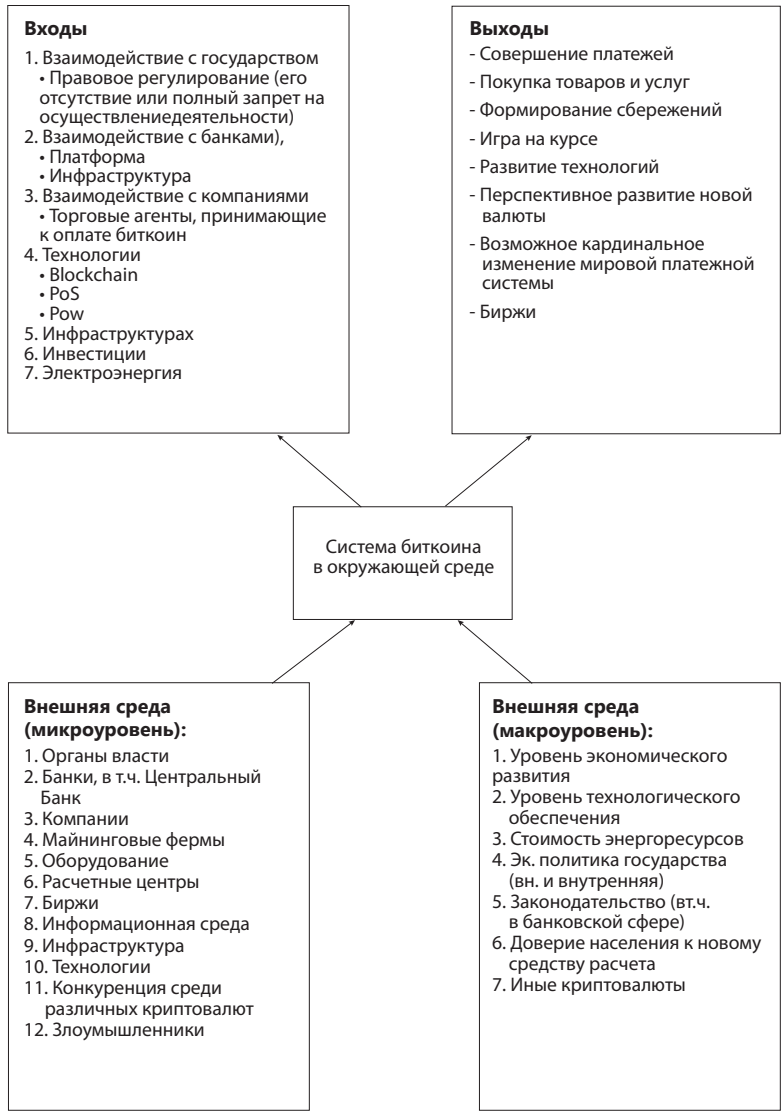
2) выбирается некоторое целое k в пределах от 1 до n–1. Рассчитывается точка с использованием скалярного умножения находится . Если $r = 0$, то возврат к шагу 1. Находится . Если $s = 0$, то возврат к шагу 1. Полученная пара (r, s) является нашей подписью.

После получения данных и подписи к ним, третья сторона, зная публичный ключ, может их верифицировать.

Безопасность ECDSA связана со сложностью задачи поиска секретного ключа. Помимо этого, безопасность исходной схемы зависит от «случайности» выбора показателя k при создании подписи. При использовании одинакового значения k более одного раза, нарушается безопасность, и из подписей можно извлечь секретный ключ. Поэтому современные реализации ECDSA, в том числе используемые в большинстве биткоин-кошельков, генерируют k на основе секретного ключа и подписываемого сообщения [Воронов, 2017].

Модель «черного ящика». Проблема обеспеченности биткоина

Данный тип статистической модели выделяется среди многообразия реальных систем и инструментальных средств моделирования (рис. 4). Он отображает реальную систему в базовом варианте. В этой модели отсутствует сведения о внутреннем содержании исследуемого объекта, границы не описываются, а лишь подразумеваются. Ее принято считать самой простой в системологии.



Составлено автором по материалам исследования

Рис. 4. Модель «черного ящика» системы биткоин

В основе этой модели лежат входные и выходные связи (никакая модель не может существовать в полной изоляции, данные связи отражают взаимодействие объекта с окружающей средой). При их выявлении необходимо воспользоваться декларативной (качественной, классификационной) моделью, где выходы и входы описываются по шкале наименований.

Обратимся к рассматриваемому нами объекту и попробуем составить модель «черного ящика» для системы биткоина. Изначально его создавали как абсолютно децентрализованный способ расчетов между экономическими агентами, в котором не участвуют ни государство, ни банки, что позволяет значительно снизить транзакционные издержки. Совершить транзакции между участниками напрямую, минуя финансовые институты возможно благодаря одноранговому устройству системы электронных денег.

Структура одноранговой сети, состоит из двух различных форм: пирингового приложения и одноранговой сети (англ. peer-to-peer, P2P – равный к равному). Самым простым примером данной сети, является домашняя сеть, с двумя подключенными к ней компьютерами, которые используют один принтер. Данные, сохраняемые в сети, могут располагается на любом из подключенных устройств. Для безопасного использования пользовательские аккаунты должны быть установлены индивидуально на каждом компьютере [Мащенко, 2017].

В силу необеспеченности биткоина банки с осторожностью относятся к этому новому способу расчетов. Ни один мировой Центральный банк, на данный момент не признал биткоин. Некоторые государства разрешают его хождение в качестве валюты, некоторые воспринимают его только как спекулятивное средство, а некоторые, как Китай, запрещают вовсе.

Биткоин, проблемы, связанные с его использованием

Биткоин – виртуальная валюта, не обеспеченная никакой реальной стоимостью, что считается главной проблемой его внедрения и повсеместного использования в качестве валюты. Пока же биткоин в основном принимается лишь в качестве финансового инструмента, на колебаниях курса которого и пытаются зарабатывать, но при его необеспеченности это больше напоминает финансовую пирамиду и мыльный пузырь. Для российских банков – это основная проблема для оборота биткоина. Из-за видимой пирамидальности всей системы биткоина банки не готовы отказываться от привычных электронных средств расчета [Нурмухаметов, 2017].

Угроза атак с захватом 51 % блоков фактически означает монополизирование всей системы и ее захват, чем могут воспользоваться мошенники. Если злоумышленник владеет мощностью более 51 %, он также сможет создать альтернативную цепочку, которая превратится в основную. Эта ситуация напоминает голосование на собрании акционеров, когда у одного из собственников имеется на руках контрольный пакет, блокирующий голоса других держателей.

Высокие расходы на производство и поддержание работы биткоина одновременно делает его и более безопасным. Безопасность сети поддерживается за счет стоимости физически дефицитных ресурсов, но это в то же время делает сети неэффективными с ресурсной точки зрения. В частности, специализированное оборудование необходимо для запуска вычисления. Также существенные расходы требуются на электричество для питания оборудования.

Биткоин описывают как полностью независимую, децентрализованную и максимально защищенную потенциальную валюту. Его идея состоит в том, что никто не может повлиять на ход платежей и они ни от кого независимы: ни от государства, ни от банков, ни от расчетных центров. Биткоин основывается на одноранговой системе распределенного хранения данных – блокчейн. Данная технология не позволяет проводить больше 7 операций в секунду, когда как централизованные системы позволяют проводить до 50 тыс. операций.

Необеспеченность биткоина, монополизирование системы расчета и получение контроля над многомиллионными оборотам, высокая стоимость оборудования для майнинга и его последующего оборота, и недостаточное техническое развитие – все это проблемы, которые возникают в криптомире и не дают данной технологии вступить во всеобщий обиход.

Блокчейн в информационно-технологической сфере

Блокчейн является порождением информационных технологий (ИТ), поэтому именно в этой области данная технология имеет множество вариантов использования. Облачная архитектура имеет централизованную

структуру, на которой базируется большинство современных технологий безопасности, что делает ее уязвимой. Необходима постоянная отправка отдельными серверами учетных данных, а также их получение, любой из серверов может оказаться слабым звеном, поставившим под удар всю систему.

Работа блокчейна, в свою очередь, осуществляется полностью автоматически. Взаимосвязанными устройствами управляют не люди или современные компьютеры, а системы и программы, посредством использования которых обеспечивается полная безопасность данных. Сложное шифрование и децентрализованная структура блокчейна (в качестве примера стоит привести алгоритм биткоина – SHA256 и 64-значные ключи), техническое отсутствие возможности его взлома, делают блокчейн панацеей в современном мире, который полон цифровых угроз.

Как известно, предотвращение угрозы всегда обходится дешевле и легче, нежели устранение ее последствий. Например, полгода назад известной всем «Лабораторией Касперского» была представлена разработанная ей на базе блокчейна система электронного голосования, обеспечивающего прозрачность и безопасность процесса. Сейчас электронная форма голосования на выборах применяется лишь в Эстонии, однако в скором будущем это, вероятно, в корне изменится.

Проект Adept представляет собой детище компаний IBM и Samsung. Он сделает возможным использование блокчейноподобных технологий для создания децентрализованной сети из огромного количества различных устройств семейства интернета вещей (IoT), которые смогут взаимодействовать друг с другом.

Блокчейн в розничной торговле

Блокчейн имеет огромное будущее в этой области. На Всемирном экономическом форуме (World Economic Forum) блокчейн не так давно был признан одним из шести масштабных трендов, которые окажут глобальное влияние на человечество в ближайшие 5–10 лет.

Например, совсем недавно известной американской сетью Walmart было объявлено о намерении внедрения технологии блокчейн в сферу закупок заграничных товаров посредством использования нового логистического инструмента, на основе блочных сетей которого был разработан консорциум Hyperledger, позволяющий контролировать весь путь продуктов от поставщика до супермаркета, содержащий данные как о сроке годности, так и о требованиях к условиям хранения, перевозки и т. д. В качестве еще одного примера можно привести японский ритлейлер Rakuten. Он выкупил компанию Bitnet с целью создания блокчейн-лаборатории. Полгода назад всем известный хайтек-гигант IBM представил проект с целью изучения возможности применения блокчейна для осуществления контроля поставок продовольствия и повышения безопасности пищи. Многие ритейлеры и пищевые компании уже приняли участие в данном проекте.

Блокчейн в сфере образования

Блокчейн можно внедрить в системы, осуществляющие хранение и контроль документов. Самым главным преимуществом в данном случае выступает невозможность манипуляций данными, которые записаны в систему, информация подлежит добавлению, но не перезаписи. Одновременно легко проследить подлинность документа, так как любой пользователь может посмотреть, кем он был записан и в какое время.

На практике такую систему почти никто не применяет. Одним из пионеров выступает Университет Никосии на Кипре, использующий ее для хранения дипломов и сертификатов. Этот университет также стал первым вузом, который начал принимать криптовалюту в качестве платы за обучение, диплом же данного университета имеет мировое признание. Открытый Университет в Великобритании, Массачусетский Технологический Институт (MTI) и другие вузы уже переняли подобную инициативу.

Блокчейн в юридической сфере

Не стоит забывать о том, что после сохранения данных в цепочку блоков, они не подлежат изменениям. Именно это делает возможным использование блокчейна как документальное свидетельство для подтверждения передачи цифровых активов и для хранения информации о владельце фактической собственности. Это позволяет, например, Национальной Земельной Службе Швеции разработать в ближайшем будущем экспериментальную систему на основе блокчейна, чтобы оцифровать процессы купли-продажи недвижимости, а также для соответствия процессов нормативным требованиям запись всех действий и результатов в блокчейне с успехом может выступать как аудиторский журнал для регулирующих органов. Последние также могут получить доступ к внутреннему блокчейну для просмотра информации финансовой организации. Все это может позволить последним обеспечить более эффективную регулятивную отчетность.

Блокчейн в медицинской сфере

Блокчейн в сфере медицины – «спасительная палочка», как минимум, потому что в области обработки данных медицинская отрасль давно трещит по швам. Впрочем, здесь не обойтись без проблем: блокчейн хорош для маленьких объемов информации, но, как всем известно, медицинские данные крайне обширны.

Тем не менее, это не стало препятствием для создания системы Healthureum: полная информация о каждом пользователе системы занимает все свободное место экосистемы, потому что пропускная способность и емкость невероятно велики. В общем, вместо того, чтобы быть носителем полной информации о пациентах, новейшая технология в здравоохранении, основанная на блокчейн-технологии, будет выступать в роли механизма контроля и учета данных в связи с изменениями в медицинских записях. Иными словами, выход заключался в том, что данные будут храниться вне блоков, а ссылки, которые будут вести к огромным файлам, расположены в блокчейне.

Что же касается шифрования данных, то здесь предлагается множество различных проектов для решения этой проблемы: например, разграничение типа доступа к информации о пациенте, либо внедрение закрытого массива данных на блокчейне с доступом только контролирующего органа или иной регулирующей организации.

И это не единственные проблемы использования блокчейна в медицинской сфере: к сожалению, блокчейн несовместим с Законом об охране и ответственности за информацию, полученную в результате медицинского страхования (HIPAA). Таким образом, необходимы дополнительные меры законодательного характера к остальным проблемам.

В отличие от других сфер, блокчейн в медицине пока что еще далек даже от начальной стадии широкого применения. И это, не говоря уже об отсутствии законодательной базы большинства стран в принципе.

Блокчейн в сфере развлечений

Здесь первое, что приходит в голову – блестящая возможность обхода запрета на азартные игры во многих странах за счет непризнания криптовалюты валютой или имуществом. Казино на криптовалюте вообще и биткоинах в частности в настоящее время множатся со скоростью света, что говорит о высоком спросе на них.

Но не только о гэмблинге речь: например, даже такая огромная индустрия, как музыкальная (производство аудиовизуальной продукции; проще говоря, артисты и группы) уже заинтересовалась блокчейном.

В блокчейне можно хранить данные обо всех транзакциях, зашифрованные данные о правах владения, финансировании, и что еще лучше – исполнять смарт-контракты (например, на уровне кода обмениваться ценностями без участия посредников). К примеру, компания Stem представляет из себя платформу для платежей и распространения аудиовизуальной продукции на основе блокчейна: можно публиковать контент, управлять контрактами и проводить платежи в одном месте.

Этот сервис и аналогичные можно назвать отличной площадкой для использования малоизвестными начинающими музыкантами. Микроплатежи с низкими комиссиями, более защищенные данные о продажах и потреблении создают интересную бизнес-модель.

Блокчейн в повседневной жизни

На сегодняшний день пока что никто не решился внедрить блокчейн в повседневную рутину, но такие возможности существуют, например, в сфере SP (англ. Smart Property, умное имущество).

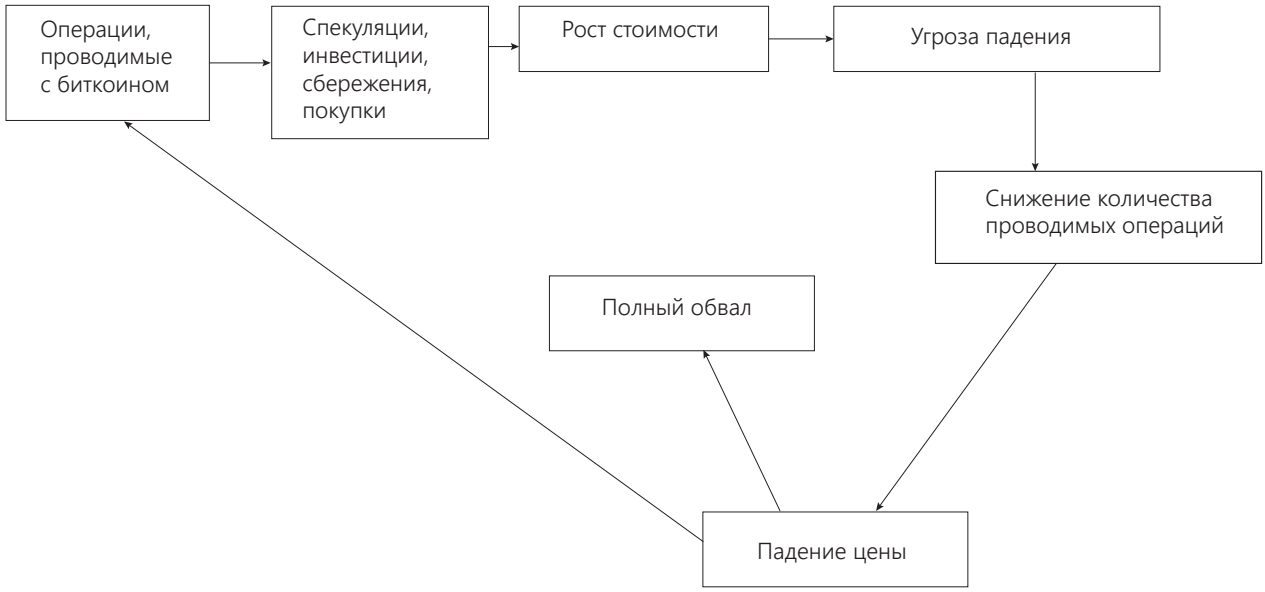
К примеру, если встроить в обычный автомобиль публичный ключ, а владельцу передать соответствующий приватный ключ, то можно будет использовать такую систему продажи автомобилей, при которой публичный ключ машины передается новому владельцу, а в противоположную сторону будет переведена сумма криптовалюты: в данном случае блокчейн подтверждает право собственности и уплаченную сумму.

Что хорошо в данной схеме – операция купли-продажи не будет требовать никаких посредников с доверенностью и оформления большого количества бумаг. Обмануть или подделать блокчейн технически чрезвычайно сложно, а весь процесс купли-продажи можно автоматизировать. Все, что будет нужно продавцу и покупателю, встретиться со смартфонами у машины.

Пока что ввиду запутанности и сложности законов, связанных с автовладением (а также нелегальности криптовалют в большинстве стран в качестве денежных средств), подобная схема – из разряда фантастики, но такой фантастики, которая вполне может быть реализована через несколько лет: рано или поздно появится соответствующий ICO-проект, и в таком случае, скорее всего, он будет одобрен на государственном уровне, поскольку потребует снятия части ответственности с государственных органов.

Системные архетипы, построение рамочной модели

Применительно к биткоину, трагедия систем коллективного использования заключается в том, что биткоин ничем не обеспечен, но необычайно популярен и пользуется повышенным спросом у спекулянтов, благодаря чему цена на биткоин продолжает расти сверхбыстрыми темпами [Коблиц, 2001]. Существует риск, что однажды подобная финансовая пирамида рухнет и тогда пострадают и инвесторы, которые вложились в биткоин, и спекулянты, и люди, использующие биткоин для оплаты покупок или как сбережения, общая схема рамочной модели представлена на рисунке 5.



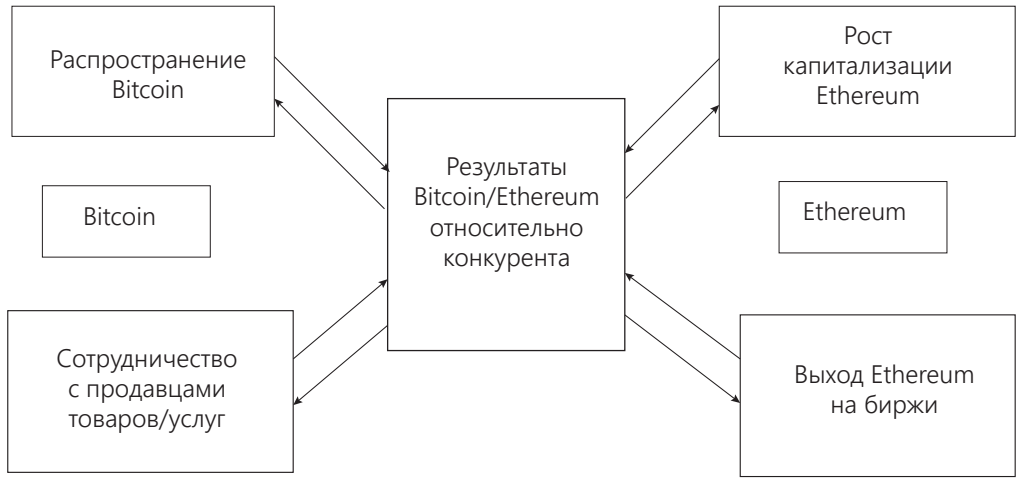
Составлено автором по материалам исследования

Рис. 5. Рамочная модель структуры операций с биткоином

Причиной беспокойства являются сверхбыстрые темпы роста, неподкрепленные реальными активами.

Принцип управления

Так как на некоторых биржах биткоин – свободно обращающийся финансовый инструмент, ценой которого невозможно управлять централизованно на уровне государства возможным принципом управления может являться полный запрет на обращение биткоина или ограничения.



Составлено автором по материалам исследования

Рис. 6. Система архетипа трагедии эскалации

НАПРАВЛЕНИЯ ДАЛЬНЕЙШИХ ИССЛЕДОВАНИЙ И ВЫВОДЫ

На сегодняшний день существует множество криптовалют, которые начинают конкурировать между собой, подрывая авторитет остальных, поэтому дальнейший интерес для автора представляет составление рамочной иодели «эскалация» для двух соревнующихся криптовалют: Bitcoin и Ethereum.

Ранние симптомы

Агрессивное поведение относительно своих конкурентов.

Принцип управления

Нужно найти путь, позволяющий обеим сторонам «победить» или достичь своих целей. Во многих случаях односторонние «мирные» действия могут разорвать порочный круг, поскольку при этом другая сторона избавляется от ощущения растущей угрозы. Система архетипа трагедии эскалации представлена на рисунке 6.

ЗАКЛЮЧЕНИЕ

Подводя итог, необходимо отметить, что несмотря на всю привлекательность биткоина как финансового инструмента для спекуляций, он имеет весьма существенные риски и недостатки. Так как криптовалюты ничем не обеспечены, никто не сможет угадать, когда инвесторы и спекулянты потеряют интерес к криптовалютам, перестанут вкладываться в них и весь «карточный домик» рухнет. Не может быть надежным тот финансовый инструмент, стоимость которого определяется исключительно доверием вкладчиков. Что касается криптовалют, возможно они и изменят финансовую систему в будущем, но имея другую форму и технологию выпуска и обеспечения.

На стоимость и популярность криптовалют и биткоина в частности оказывают большое влияние как факторы внешней среды, на макро- и микроуровне, заключающиеся в техническом оснащении, стоимости оборудования для майнинга и электроэнергии, уровне правовой системы и правового регулирования, так и внутренние факторы (скорость проведения операций, стабильность на биржах) [Свон, 2017].

С проблемой необеспеченности биткоина борются органы государственной власти отдельных стран. Так, в сентябре 2017 г. Центральный банк Китая признал незаконной финансовой деятельностью проведение операций ICO (Initial Coin Offering) – сбор средств инвесторов с использованием криптовалют, по аналогии с первичным размещением ценных бумаг на бирже (IPO). Чиновники объясняли свое решение тем, что такое размещение несет в себе финансовые риски, а иногда оказывается мошенничеством.

Запрет на проведение ICO связан с опасениями относительно того, что криптовалюты содержат признаки очередной финансовой пирамиды, а также с рядом крупных скандалов в этой сфере, таких как недавнее задержание в Греции россиянина А. Винника, подозреваемого в отмывании 4 млрд долл. США через одну из крупных биткоин-бирж. По данным китайского ЦБ, более чем 90 % проектов, проводящих ICO, могут нарушать нормативно-правовые акты о незаконной финансовой деятельности. Доля проектов, которые действительно привлекают криптовалюты для инвестиционных целей, составляет менее 1 %.

Это решение финансовых властей КНР мгновенно привело к падению курса биткоина. Действия китайских властей оказывают такое существенное влияние на курсы криптовалют из-за того, что две трети всех биткоинов добываются в этой стране (в основном из-за дешевого электричества). Почти четверть всех транзакций с криптовалютами приходятся на Китай.

Российские власти также активно обсуждают регулирование криптовалют. Центробанк не планирует приравнивать биткоин к денежным средствам или иностранной валюте, а глава регулятора Э. Набиуллина сравнивает майнинг с финансовыми пирамидами и ссылается на опыт Китая. Министерство финансов в августе 2017 г. выступило с инициативой запрета продажи биткоинов физическим лицам и в начале 2018 г. представило законопроект «О цифровых финансовых активах»[3].

При анализе были выявлены два существенных архетипа: трагедия систем коллективного использования, применимая к проблеме необеспеченности биткоина, предел роста и эскалация, связанная с конкуренцией между криптовалютами, где в качестве примера были приведены Bitcoin и Ethereum.

На данный момент очень сложно предугадать развитие оборота использования криптовалют, потому что это достаточно новый и уникальный финансовый инструмент, впервые появившийся на свет менее

[3] Проект Федерального закона «О цифровых финансовых активах» № 419059-7 (ред., внесенная в ГД ФС РФ, текст по состоянию на 20.03.2018). Режим доступа: Справочная правовая система «КонсультантПлюс» http://www.consultant.ru/cons/ (дата обращени: 23.09.2018).

10 лет назад. Но от грамотного его использования и регулирования может зависеть новое, альтернативное развитие мировой финансовой системы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Воронов М.П., Часовских В.П. (2017). Blockchain – основные понятия и роль в цифровой экономике // Фундаментальные исследования. № 9 (ч. 1). 30–35 с.

Коблиц Н. (2001). Курс теории чисел и криптографии. М.: Научное изд-во «ТВП». С. 188–200.

Мащенко П.Л., Пилипенко М.О. (2017). Технология Блокчейн и ее практическое применение // Наука, техника, образование. № 32. С. 61-64.

Нурмухаметов Р.К. (2017). Технология блокчейн: сущность, виды, использование в российской практике / Р.К. Нурмухаметов, П.Д. Степанов, Т.Р. Новикова // Деньги и кредит. № 12. С. 101–103.

Равал С. (2017). Децентрализованные приложения. Технология Blockchain в действии. СПб.: Питер.

Свон М. (2017). Блокчейн: Схема новой экономики / [перевод с английского]. Москва: изд-во «Олимп–Бизнес».

REFERENCES

Voronov M.P., Chasovskikh V.P. (2017), "*Blockchain – basic concepts and role in the digital economy*" ["Blockchain – osnovnyye ponyatiya i rol' v tsifrovoi ekonomike"], Fundamental'nyye issledovaniya, no. 9, p. 30–35

Koblitz N. (2001). "*Course in number theory and cryptography*" ["Kurs teorii chisel i kriptografii"], pp. 188–200, *Nauchnoe izd-vo* "TVP", Moscow.

Mashchenko P.L., Pilipenko M.O. (2017), "*Blockchain Technology and its practical application*" ["Tekhnologiya Blokchein i ee prakticheskoe primenenie"], *Nauka, tekhnika, obrazovaniye*, no 32, pp. 61–64.

Nurmukhametov R.K., Stepanov P.D., Novikova T.R. (2017), "*Blockchain Technology: essence, types, the use in the Russian practice*" ["Tekhnologiya blokchein: sushchnost', vidy, ispol'zovaniye v rossiiskoi praktike"], *Den'gi i kredit* [*Money and Credit*], no 12, pp. 101–103.

Raval S. (2017), "*Decentralized applications. Blockchain technology in action*" ["Detsentralizovannye prilozheniya. Tekhnologiya Blockchain v deistvii"], pp. 121–122, Piter, S-Peterburg.

Swan M. (2017), *The scheme of the new economy* [Blockchain: Skhema novoi ekonomiki, trans. from English], izd-vo "Olimp–Biznes", Moscow.