УДК 338.242, 004.9

ТЕХНОЛОГИЯ БЛОКЧЕЙН И КРИПТОВАЛЮТА

Жданова С.Д. [1]

[1] Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», факультет технологического менеджмента и инноваций,
(197101, Россия, Санкт-Петербург, пр. Кронверкский, д.49), e-mail: ftmi@mail.ifmo.ru

Работа посвящена анализу новой технологии и новых денежных средств -биткоину. Криптовалюта существует уже больше 10 лет, но правовым статусом не обладает. Изначально к криптовалюте не отнеслись как к чему-то серьезному, но после того, как курс Биткоина по отношению к другим валютам поднялся, его активно начали изучать и модернизировать. За это время появилось огромное количество видов криптовалюты. С помощью нее уже научились зарабатывать деньги, и даже появилось что-то вроде новой профессии – майнер. В руках майнеров сосредоточено много задач. Они обеспечивают саму работу блокчейна, решая криптографические задачи. В статье автор касается истории технологии блокчейн, ее описания, участникам, достоинствам и недостаткам. Кроме этого производится анализ криптовалюты. На основе приведенных данных автор предполагает, что за технологией блокчейн и криптовалютой стоит будущее. Обращая внимание на тот факт, что наш все больше погружает в цифровую реальность, вполне вероятно, что через несколько лет мы уже будем расплачиваться биткоинами и голосовать на выборах с помощью технологии блокчейн.

Ключевые слова: технология блочейн, криптовалюта, биткоин, альткоин, достоинства и недостатки криптовалюты.

BLOCKCHAIN AND CRYPTO TECHNOLOGY

Zhdanova S.D.[1]

[1] Federal State Autonomous Educational Institution of Higher Education "St. Petersburg National Research University of Information Technologies, Mechanics and Optics," Faculty of Technological Management and Innovation,
(197101, Russia, St. Petersburg, Ave. Kronverksky, 49), e-mail: ftmi@mail.ifmo.ru

The work is devoted to the analysis of new technology and new funds -bitkoin. Crypto has existed for more than 10 years, but does not have legal status. Initially, crypto was not treated as something serious, but after the rate of Bitcoin against other currencies rose, it actively began to be studied and modernized. During this time there were a huge number of types of crypto. With the help of it already learned to earn money, and even appeared something like a new profession - a miner. Many tasks are concentrated in the hands of miners. They ensure the very operation of the blockchain by solving cryptographic problems. In the article the author deals with the history of blockchain technology, its description, participants, advantages and disadvantages. In addition, the analysis of crypto is carried out. Based on the data provided, the author suggests that the future is behind blockchain technology and crypto. Drawing attention to the fact that ours is increasingly immersive in digital reality, it is likely that in a few years we will already pay with Bitcoins and vote in elections using blockchain technology.

Keywords: technology of blochain, crypto, Bitcoin, altcoin, advantages and disadvantages of crypto.

ВВЕДЕНИЕ

Блокчейн вносят в список технологий Четвертой промышленной революции. Технология настолько уникальна, что может найти применение почти в любой сфере жизни общества. Но появление чего-то нового, как правило, ознаменовывает уход чего-то старого. К чему же может привести внедрение в нашу жизнь блокчейна? Неужели некоторые профессии просто перестанут быть нужными? Ответы на эти вопросы пока что до сих пор не найдены, потому что хоть технология имеет в себе много преимущественных моментов, но тем не менее во многих странах она не закреплена на законодательном уровне. Но несмотря на это она продолжает активно развиваться в сети, для нее продолжают создавать новые разработки и внедрять их.

"Блокчейна — такая технология, которую мы до конца еще не понимаем…. Мы понимаем только, что это основная прорывная технология, сравнимая значимостью с интернетом… По оценке наших исследователей, которые занимаются этой технологией, примерно через полтора года основные проблемы, технологические проблемы, которые на сегодняшний день мешают массовому внедрению этой технологии, будут решены. И взлет этой технологии через полтора года уже можно планировать", — сказал глава Сбербанка Герман Греф [1].

Криптовалюта существует уже больше 10 лет, но правовым статусом не обладает. За это время появилось огромное количество видов. Но тем не менее с помощью нее уже научились зарабатывать деньги, и даже появилось что-то вроде новой профессии – майнер. Изначально к криптовалюте не отнеслись как к чему-то серьезному, но после того, как курс Биткоина по отношению к другим валютам поднялся, его активно начали изучать и модернизировать.

1. ТЕХНОЛОГИЯ БЛОКЧЕЙН

1.1. История

Впервые технология, основа которой напоминает блокчейн была описана еще в 1991 году Стюартом Хабером и У. Скоттом Шторнеттом. Их идея заключалась в том, чтобы электронные документы не могли быть использованы мошенниками или быть подделанными. В системе использовалась цепочка блоков, в которой содержались данные о времени создания документа. Для шифровки использовалась криптография [2].

В 1992 году в разработку было добавлено дерево Меркла (дерево хешей). Дерево Меркла – двоичное дерево, которое состоит из соединенных блоков, которые по форме напоминают дерево. В каждом блоке к данным применяется хеширование, далее нижнее

блоки суммируются, и их сумма образует новый блок. И так происходит дальше. Эта же технология применяется в блокчейне [3].

Внедрение этой технологии сделала разработку ученых более эффективной и позволила в одном блоке собирать несколько документов. Но технология так и не получила применения.

В 2004 году Гарольд Томас Финни разработал систему RPoW (Reusable Proof of Work). Система позволяла бороться со спамерами с помощью Hashcash. Перед тем, как отправить токен (цифровая ценная бумага, единица учета, служащая мерой вознаграждения), он должен получить перед заголовком отметку hashcash, для вычисления которой требуется определенное количество времени. Чтобы ее подобрать, нужно перебрать достаточное количество вариантов для вычисления нужной. Правильным считается заголовок, содержащий в хеше первые 20 нулей. Для этого нужно перебрать около миллиона чисел. Получатель с помощью небольших вычислительных операций может подтвердить правильность отметки. Для спамеров невыгодно таким образом отправлять информацию [4].

В 2008 году был разослана документ, содержащий информацию о системе электронных денежных средств- Биткойн, содержащей также информацию о технологии блокчейн. Автором этой работы является человек или группа людей под псевдонимом Сатоши Накамото (предположительно их происхождение из Японии). В основе лежала децентрализованный одноранговый peer-to-peer протокол, для отслеживания и проверки транзакций.

3 января 2009 года появился Биткойн. Сатоши Накамото добыл биткойн-блок, за который в качестве награды было получено 50 биткойнов.

12 января 2009 года была совершена первая в мире транзакция биткойна, когда Сатоши Накамото «перевел» 10 биткойнов Хэллу Финну.

В 2010 году была совершена первая покупка за криптовалюту. Программист Ласло Ханьеш купил две пиццы за 10 тысяч биткоинов (на сегодняшний день это равняется 451 млрд рублей)

В 2013 году Виталик Бутерин заявил о необходимости создания децентрализованных приложений на основе технологии блокчейн. Свою идею он вложил в основу платформы Ethereum. В ней смарты-карты (программы или скрипты) используются для транзакций, есть возможность заключить смарт-контракт, создать приложения на основе технологии блокчейн и так далее [2].

1.2. Описание технологии блокчейн

Если переводить слово «Блокчейн» дословно, то получится, что это непрерывная цепочка блоков. По-другому блокчейн называют технологией распределенных реестров. Это объясняется тем, что любая информация хранится на нескольких компьютерах и соответственно, данные могут видеть несколько пользователей одновременно [5].

Одна из особенностей блокчейна в том, что технологи децентрализована, то есть нет единого центра, через который бы проходили вся информация. У нее нет единого сервера, а копии данных хранятся на всех компьютерах.

Пользователи могут обмениваться между собой различной информацией. Всего существует два типа сообщений: транзакции и блоки, причем блоки включают в себя несколько транзакций. Вся информация хранится в блоках в зашифрованном виде через криптографическую хеш-функцию SHA-256. Хешируется само название блока и его содержание. Каждая транзакция должна подтверждаться всеми пользователями.

Все блоки связаны между собой сложными математическими алгоритмами, которые закреплены между собой криптографической подписью. Чтобы создать следующий блок, нужно согласие всех участников. Новый блок создают майнеры и после децентрализованной проверки он присоединяется к цепочке и происходит обновление реестра. В новом блоке будет содержаться информация о всех предыдущих в зашифрованном виде (хеше) [6].

Данные не могут быть удалены или изменены. Каждая совершенная транзакция, появление нового пользователя или наоборот выход, да и вообще любые действия фиксируются в блокчейне. Данные невозможно подделать или изменить, так как копии могут храниться на бесчисленном количестве компьютеров. Для взлома будет необходимо получить доступ ко всем базам данных одновременно, что нереально, поскольку информация может храниться на нескольких тысячах компьютеров.

1.3. Участники блокчейна

1) Майнеры

В руках майнеров сосредоточено много задач. Во-первых, они обеспечивают саму работу блокчейна. Они собирают данные транзакций, проверяют их и организуют в блок. Новый блок они присоединяют к цепочки предыдущих. Чтобы создать новый блок, они решают криптографические задачи. Суть этих задач в том, что майнерам необходимо создать уникальный хеш, который начинается с определенного числа нулей (для каждой группы он задается автоматически). Конечно, все это делается не вручную, а через компьютеры. По сути, чтобы стать майнером нужно лишь специальное оборудование, которое по составу напоминает составляющие компьютера. Но проблема в том, чтобы

начать зарабатывать быстрее и больше, необходимо соответствующие оборудование, которое стоит больших денег. Именно поэтому майнерами могут стать далеко не все.

За каждый вновь созданный блок они получают вознаграждение, которое автоматически перечисляется на их электронный кошелек. Воспользоваться вознаграждением они могут только после 120 подтверждений (примерно через 20 часов после перечисления). Вознаграждение берется из комиссии транзакций остальных участников.

2) Аудиторы

Вся цепочка блоков сети Биткойн может занимать около 122 гигабайт. Именно у аудиторов хранится вся история транзакций. Также они контролируют работу майнеров и распределяют нагрузку в сети.

3) Остальные участники

Они совершают транзакции, за счет которых, грубо говоря, и формируется доход майнеров. Чем больший процент комиссии они заплатят, тем быстрее будет совершена их транзакция. У них нет истории операций. В их хранилище может содержаться только их личная информация [7].

1.4. Преимущества блокчейна

1) Децентрализация

В блокчейне нет единого центра управления и места хранения данных, а само существование поддерживают все участники. Совершение транзакций осуществляется напрямую, без посредников, что позволяет снизить затраты на комиссию, которая платиться лишь за подтверждение транзакции, и повысить скорость перевода по сравнению с другими финансовыми институтами, такими как банки.

2) Сохранность данных

Благодаря тому, что копии данных хранятся на всех компьютерах пользователей, это позволяет свести к минимуму возможность хищения или уничтожение информации. Даже если среди 100 участников, у 99 компьютеры будут испорчены, данные все равно сохранятся. Как уже было сказано выше, взломать такую систему крайне сложно и почти невозможно. Нужно обладать высокими мощностями, чтобы это сделать.

3) Прозрачность данных

Каждый участник может видеть всю историю транзакций. С помощью этого участники могут отследить, прошла транзакция между другими участниками, достаточно просто обратиться к истории.

4) Невозвратность транзакций

Плательщик не сможет отозвать свою транзакцию в корыстных целях, так как запись о ней уже есть в реестре и изменить или отменить ее нельзя. Это позволяет предотвратить мошенничество даже внутри группы участников [8].

1.5. Недостатки

1) Размер блокчейна

Чем больше транзакций совершается, тем больше блокчейн весит и растет. Но стоит помнить, что данные должны содержаться на каждом компьютере и из-за этого иногда требуется несколько часов или даже дней на скачивание.

2) Отсутствие конфиденциальности

В блокчейне не содержатся настоящие имя и фамилия пользователя, но есть адрес электронного кошелька и информация о всех транзакциях и их суммах. Если пользователь прикрепит ссылку на свой кошелек к какому-либо сайт, через который можно вычислить его настоящие личные данные, то он ставит под угрозу свои крипто счета. Особенная это плохо может сказаться на крупных компаниях, у которых крупные счета, которые могут раскрыть конфиденциальную информацию о клиентах, контрагентах, продажах и др.

3) Энергозатратность

Для создания новых блоков майнерам требуются огромные энергоресурсы, чтобы количество блоков, найденных ими, оставалось постоянным.

4) Неопределенный нормативный статус

На сегодняшний день блокчейн и криптовалюта находятся за пределами законодательно регулирования многих стран. Использование криптовалюты в сети в качестве денег осуществляется на свой страх и риск. В России использовать криптовалюту для оплаты товаров и услуг запрещено, и в качестве валюты она не признается [8].

1.6. Применение технологии блокчейн

Блокчейн нашел применение во многих областях жизни общества. Изначально он позиционировал себя только в финансовой сфере, как средство перевода цифровых денег. Но, как оказалась, эта технология весь универсальна.

В финансовой и бизнес сфере блокчейн может использоваться для перевода денег без посредников. С помощью платформы Ripple можно переводить деньги за короткий промежуток времени из одной точки мира в другую, при этом есть функция конвертации валют. Благодаря тому, что посредников нет, комиссия за транзакцию гораздо меньше, чем в банках [9].

Использование смарт-контрактов для заключения сделок или перевода крупных сумм сейчас активно используется и внедряется банками. Одной из крупных и самых первых таких сделок считается сделка-аккредитив между Альфа-Банком и S7 Airlines,

которая произошла еще в 2016 году. Заключение договоров таким способом осуществляется гораздо быстрее, дешевле, оно не требует обязательного присутствия юриста и необходимо лишь виртуальное присутствие в виде цифровой подписи, а не физическое [10].

Для правильного составления смарт-контрактов в блокчейне хранится вся база юридических книг, судебных прецедентов, договоров и т. д. и фактически пропадает надобность юристов. Это говорит еще об одной сфере применения блокчейна – юридической. Блокчейн нельзя подкупить или дать ему взятку, все происходит открыто и прозрачно. Участники будут просто обязаны выполнять условия договора. Конечно, есть возможность появления блокчейн-юристов, которые будут выступать в качестве посредников, но будут нужны лишь для большей убедительности надежности.

Широкое применение блокчейн нашел в логистике. Он способен решить почти все проблемы данной отрасли: устранить ненужных посредников, уменьшить объём рабочих потоков, обеспечить надёжную защиту, сократить количества возможных ошибок, предотвращение мошенничества и незаконного товарооборота, предоставление возможности огромной экономии средств для целой отрасли [9].

Блокчейн является огромной базой различных данных. Это свойство актуально для сферы медицины. В блокчейне можно хранить данные историй болезни всех пациентов и с помощью ключей различного доступа врачи могут увидеть данные в любой момент. Сейчас активно идет разработка блокчейн-системы для доступа врачей из других стран, ведь порой для решения проблемы требуется помощь заграничных специалистов. Особенно это будет необходимо, если болезнь продолжительная и длиться в течение нескольких лет, тогда наличие истории болезни будет как никогда нужно для правильно построения плана лечения [11].

2. КРИПТОВАЛЮТА

2.1. Определение криптовалюты

Криптовалюта – электронное денежное средство с распределенным хранением реестра на базе блокчейна. Принято считать, что такая валюта более безопасна, чем та, которую мы используем в обычной жизни.

У пользователя есть электронный кошелек, на котором хранятся все его биткоины или иная криптовалюта. К этому кошельку существует два ключа: открытый и закрытый. Открытый служит адресом аккаунта и предназначен для перевода денег. Приводя аналогию с жизнью, это номер нашей банковской карты. Закрытый ключ известен только владельцу кошелька. С помощью него можно получить доступ к деньгам кошелька. В

нашей жизни это CVV код нашей банковской карты. На данный момент насчитывается около 2504 видов криптовалют [12].

2.2. Биткоин

Биткоин – самая первая и самая дорогая криптовалюта. За десять лет его стоимость выросла более чем в 10 000 раз. Средняя длительность транзакции длиться 10 минут, а максимальное количество биткоинов, которое может быть на счету составляет 21 млн.

Биткоин подразделяется на мелкие составляющие для удобства для удобства осуществления платежей мелких сумм. Самый наименьший составляет 0,00000001 BTC и называется сатоши в честь создателя биткоина Сатоши Накамото.

Биткоин торгуется на открытом рынке, где его стоимость зависит от спроса и предложения. На него невозможно оказать прямое или целенаправленное влияние. Но это не значит, что криптовалюта не реагирует на происходящие в мире события. Так, в 2017 году курс Биткоина продемонстрировал свою реакцию в зависимости от нестабильности и кризиса в мире. В целом курс Биткоина отличается от традиционных активов более высокой волатильностью [6].

2.3. Альткоины

Термин альткоин применяют в отношении любой другой криптовалюты. Любой может использовать код Биткоина и на его основе создать свою криптовалюту. Проблема заключается лишь в том, примет ли её общество. На сегодняшний день насчитывается больше тысячи альткоинов. Мотивом их запуска служило желание улучшить биткоин и предоставить решения тех проблем, с которыми он не может справиться.

Второе место после биткоина занимает Эфириум. Эта криптовалюта придумана канадским программистом Виталиком Бутерином для своей платформы. С помощью этой криптовалюты оплачиваются смарт-контракты. Пользователь создает смарт-контракт с условиями “если — тогда” и вписывает туда любую информацию, а система автоматически выполнит вторую часть договора, как только первая будет соблюдена. Для запуска контракта платформе нужно будет заплатить и оплата производиться в ETH.

На третьем месте криптовалюта под названием Ripple. В отличии от других криптовалют в ней существует центральный орган, через который каждую секунду проходит несколько тысяч транзакций. Комиссия в нем минимальна, а скорость большая. Все деньги, которые отправляются через протокол Рипл автоматически конвертируются в XPR, а затем снова преобразовываются в нужную для получателя валюту. Ей уже заинтересовались некоторые банки и на основе нее модернизируют свои операции [13].

ВЫВОДЫ

На основе вышеизложенных данных можно сделать вывод, что за технологией блокчейн и криптовалютой стоит будущее. Обращая внимание на тот факт, что наш все больше погружает в цифровую реальность, вполне вероятно, что через несколько лет мы уже будем расплачиваться биткоинами и голосовать на выборах с помощью технологии блокчейн, будем иметь медицинские карточки и за несколько секунд переводить биткоины другу в Англию. Вопрос лишь в том, когда все это будет подтверждено на законодательном уровне. Конечно, и криптовалюта, и блокчейн еще нуждаются в разработке, но даже несмотря на все эти недостатки они уже активно входят в нашу жизнь. Возможно, сейчас мы это не замечаем, но уже спустя время все может измениться.

СПИСОК ИСТОЧНИКОВ

1. М. Блинов. Греф ожидает взлета технологии блокчейн через полтора года. // Новость.16.03.2017. [Электронный ресурс]. Режим доступа: https://ria.ru/20170316/1490214529.html (дата обращения 04.12.2019)
2. Разъяснение Bitcoin Protocol. Статья. // 23.12.2019. [Электронный ресурс] Режим доступа: https://www.binance.vision/ru/blockchain/what-is-bitcoin?_gl=1*swmhvm*_ga*aWFZUFVoYjFSVzdKajBNejNPNjZPb3VwNGpRVERWU1l3bGpPN3pacmx0bzJsVDloMGU2TTBvVzlqaWtjdm1NRg (дата обращения 04.12.2019)
3. Дерево хешей. Статья. // 04.12.2017. [Электронный ресурс] Режим доступа: https://ru.wikipedia.org/wiki/%D0%94%D0%B5%D1%80%D0%B5%D0%B2%D0%BE_%D1%85%D0%B5%D1%88%D0%B5%D0%B9 (дата обращения 04.12.2019)
4. Hashcash. Статья. // 23.12.2018. [Электронный ресурс] Режим доступа: https://ru.m.wikipedia.org/wiki/Hashcash (дата обращения 04.12.2019)
5. Что такое Блокчейн? Статья. // 2019. [Электронный ресурс] Режим доступа: https://kogio.ru/knowledge/chto-takoe/ (дата обращения 04.12.2019)
6. Технология блокчейн и криптовалюты. Пособие. // 2017. [Электронный ресурс] Режим доступа: https://blockchainwiki.ru/blockchain.pdf (дата обращения 04.12.2019)
7. Д. Бондарев. Что нужно знать о блокчейне. Статья. // 05.07.2017. [Электронный ресурс] Режим доступа: https://daily.afisha.ru/brain/6058-kak-ustroen-blokcheyn-i-zachem-on-nuzhen/ (дата обращения 05.12.2019)
8. Ю. Рейф. Преимущества и недостатки технологии блокчейн. Статья. // 18.06.2019. [Электронный ресурс] Режим доступа: https://magazine.decenter.org/ru/1-

blokchein-i-kriptovalyuty/2-preimushestva-i-nedostatki-tekhnologii-blokchein (дата обращения 11.12.2019)

9. П. Кравченко. Сферы применения технологий блокчейн. Статья. // 2017. [Электронный ресурс] Режим доступа: https://cryptomagic.ru/blockchain/primenenie.html (дата обращения 23.12.2019)

10. Технология блокчейн простыми словами. Статья. // [Электронный ресурс]. Режим доступа: http://kotnebankrot.com/texnologiya-blokchejn-sut-preimushhestva-i-nedostatki-investirovanie-primery-primeneniya/#_Toc501132423 (дата обращения 24.12.2019)

11. Е. Месропян. 20 областей применения Блокчейн вне финансовых сервисов. Статья. // 30.01.2017. [Электронный ресурс] Режим доступа: https://habr.com/ru/company/wirex/blog/397999/ (дата обращения 11.12.2019)

12. Криптовалюта. Статья. // 2019. [Электронный ресурс] Режим доступа: https://kogio.ru/knowledge/kriptovaljuta/ (дата обращения 12.12.2019)

13. Виды криптовалют и их назначение. Статья. // 2019. [Электронный ресурс] Режим доступа: https://prostocoin.com/blog/crypto-types (дата обращения 24.12.2019)