

©БГЭУ

**ТЕХНИЧЕСКИЕ АСПЕКТЫ ФУНКЦИОНИРОВАНИЯ  
ТЕХНОЛОГИИ БЛОКЧЕЙН И КРИПТОВАЛЮТ**

**В.С. КНЯЗЕВА, Е.О. ЛАБУКО**

**НАУЧНЫЙ РУКОВОДИТЕЛЬ – Е.П. ТУРКИНА, КАНДИДАТ ЭКОН. НАУК, ДОЦЕНТ**

Одной из инноваций последнего времени стало появление криптовалют. Помимо самих криптовалют, существуют системы, которые являются местом обращения цифровой валюты. Они базируются на технологии Блокчейн, которая представляет собой универсальное, децентрализованное хранилище данных. Несмотря на разногласия, свя-

занные со статусом функционирования Блокчейн и криптовалют, можно утверждать, что они могут перевернуть наше представление об организации, хранении и обработке различных данных

Ключевые слова: криптовалюты, Блокчейн, майнинг, биткоин

На протяжении большей части мировой истории человечество использовало деньги в товарной форме. Около 1000 лет назад появились деньги, которые мы привыкли видеть в нашей повседневной жизни. Однако тенденции, происходящие в мировом сообществе, подсказывают, что это, возможно, не последний этап развития денежного обращения. Появление новых экспериментальных видов денег может полностью изменить нашу жизнь в будущем. Речь идет о криптовалютах, о способах и технологиях их применения в сложившихся экономиках как развитых, так и развивающихся стран.

Криптовалюты стали новым этапом развития денег. За 6,5 лет их полноценного использования, они распространились по всему миру, и теперь являются неотъемлемой частью денежного обращения, адаптируясь под потребности человека и обеспечивая осуществление транзакционных платежей в режиме удобства, комфорта, гибкости и надежности. Криптовалюты смогли воплотиться из идеи в реальность благодаря выдающимся IT-разработчикам, программистам и математикам, которые стояли у истоков создания денег с помощью криптографических методов шифрования, однако сегодня майнинг криптовалют имеет тенденции к анонимности, для того, чтобы обеспечить независимость работы системы.

*Криптовалюта* – название распределенной и децентрализованной системы безопасного обмена и передачи цифровых денежных знаков, основанной на средствах криптографии. Денежные знаки такой системы могут обмениваться на фиатные деньги по рыночному курсу [1]. Признаки криптовалют: являются одним из видов цифровых денег – так называемых электронных денег; используют криптографические методы защиты; функционирование происходит децентрализованно (в отличие от таких централизованных систем электронных денег – таких, как PayPal); менее зависимы от законов и правоохранительных органов; псевдоанонимна; сделки по криптовалютам являются необратимыми. Большинство криптовалют являются дубликатами существующих денег [2].

Одной из технологий, которая сопутствует распределению криптовалют между контрагентами, стала Блокчейн, которая способна решить задачу о византийских генералах, то есть устранить проблему двойной траты монет. Кроме того, технология не привязана к географии, что обеспечивает равный доступ к ней участников системы, а также устраняет возможность влияния политических, экономических и социальных факторов на функционирование Блокчейн.

Все чаще мы сталкиваемся с ситуацией, когда наша жизнь во многом зависит от третьих лиц. Такие необходимые нам операции как покупка жилья, получение страховки невозможны без участия банков, страховых фирм и т.д. А какова вероятность того, что нам дадут ложную информацию? С Блокчейн вместо того, чтобы доверять управление деньгами политикам и банкирам, мы отдаем его компьютерным и математическим вычислениям.

Технология будущего, способная повлиять на мир так же сильно, как Интернет – именно эти слова сегодня говорят преуспевающие банкиры и инвесторы о Блокчейн. Причем разговорами данная тема не ограничивается: в 2016 году капиталовложения в Блокчейн-проекты превысили 1 млрд долларов США. Постараемся разобраться, что такое Блокчейн, как он относится к криптовалюте, в каких сферах применяется сегодня и есть ли перспективы использования завтра.

Работа Блокчейн основана на технологии распределенных реестров (Distributed Ledger technology, DLT). Распределенный реестр является совокупностью реплицированных, совместно используемых и синхронизированных цифровых данных, географически распределенных по различным сайтам, странам и /или учреждениям. Вопреки распространенному мнению на базе DLT развивается множество других технологий (например, Ripple, MultiChain, HyperLedger Project), в том числе, такое направление как Блокчейн. DLT напоминает разновидность бухгалтерской книги, в которой создаются записи о совершаемых сделках в режиме реального времени. Пользователи получают выгоду, поскольку создается надежная среда в режиме реального времени для обмена информации.

Технология Блокчейн построена на трех очень важных принципах:

1) распределенность: все пользователи Блокчейн образуют собой сеть компьютеров, на каждом из которых хранится копия данных Блокчейн. Обычно это полная копия всех блоков, но допускается хранение лишь нужных на конкретном компьютере данных;

2) открытость: все данные Блокчейн – блоки и их содержимое – открыты всегда и для всех;

3) защищенность: для защиты данных и пользователей в Блокчейн широко используется шифрование. Благодаря этому можно одновременно достигнуть, как раньше считалось, несовместимое – открытость и достоверность при полном недоверии к остальным участникам и даже их злонамеренном умысле.

**Таблица. Структура блока в системе Блокчейн**

Поле	Описание	Размер, байт
BLOCK_ID	порядковый номер блока	4
TIME	время, когда был создан блок	4
USER_ID	ID пользователя, который создал блок	5
LEVEL	Уровень, на котором был майнер в момент создания блока	2
SIGN	Подпись, сделанная при помощи node-ключа	От 128 до 512
TRANSACTIONS	Информация о транзакции	До 3

Для иллюстрации принципов технологии приведем следующий пример. Допустим, что у кого-то есть миллион и любой участник системы может видеть этот миллион. Но вот у кого конкретно он есть – этот участник узнать не может, пока владелец миллиона не даст ему специальный криптографический ключ, тем самым подтверждая, что миллион есть именно у него. Структура блока в системе приведена в таблице [3].

Чтобы объяснить, как работает Блокчейн, приведем пример с молекулой ДНК, содержащей информацию обо всем живом организме. В Блокчейн имеется собственная цепочка блоков транзакций (сделок, платежей и т. д.). При этом после совершения и подтверждения любой транзакции (согласно установленным математическим правилам) в цепочку добавляется новый блок. И каждый такой блок, словно клетка ДНК, содержит информацию как о конкретной транзакции, так и обо всей сети в целом. Таким образом, технология блокчейн изначально предопределяет невозможность добавления фальшивого блока или изъятия существующего, поскольку это сразу же будет видно во всей системе. Нельзя в структуру добавить то, чего там быть не должно. При удалении блока система точно так же реагирует на изменение глобальной структуры. Мошенничество, попытки несанкционированного вмешательства и пиратство практически исключены, и кроме этого – бессмысленны, так как предполагаемый доход от взлома системы не сможет покрыть огромных расходов на глобальную атаку. Кроме того, при работе с ней задействованы всего две стороны, без привлечения посредников для проведения сделок любого типа.

Надежность данной системы держится на криптографических ключах. На самом деле ключ – это очень большое число, которое рассчитывается с помощью специального алгоритма, называемого хэш-функцией. Хитрость алгоритма в том, что для заданного набора данных хэш-функция дает строго один ключ, который обладает двумя очень важными свойствами:

- обладая ключом, нельзя узнать исходный набор данных;
- найти другой набор данных, дающий такой же ключ, практически нереально.

При этом два майнера могут одновременно обрабатывать две сделки. Но, чтобы избежать ветвления цепи, существует правило, согласно которому в цепочку будет включен только один блок: блок майнера, сгенерировавшего наименьшее значение хэша.

Все данные Блокчейн хранятся на компьютерах пользователей Блокчейн-сети. Все пользователи сети равноправны и могут делать все, что угодно, в том числе безуспешно пытаться обмануть других пользователей. Запретить им никто не может, потому что все находятся в равных условиях, обладают равными правами. Таким образом, пользователю Блокчейн-сети не нужны никакие посредники, например, банки, госорганы, аудиторы, контролеры, страховые компании или регистраторы. Важно отметить, что эта сеть никак не привязана к географии, то есть пользователь из Москвы может одновременно подключиться к пользователям из Пекина, Лондона, Нью-Йорка и Буэнос-Айреса. И это также защищает его от любых региональных особенностей.

Стоит отметить, что в мире наблюдается неоднозначное отношение к криптовалютам. Оно проявляется в том, что некоторые страны благоприятствуют развитию обращения криптовалют (например, Германия, Израиль, Канада, США, Сингапур) и, а некоторые не признают их (например, Бангладеш, Боливия, Китай, Кыргызстан, Румыния) [4]. Есть и такие страны, которые пока не определились с тем, как относиться к данному феномену (это Бразилия, Великобритания, Гонконг (автономная территория Китая), Индонезия, Польша, Швейцария и др.). Та или иная позиция по отношению к криптовалютам обусловлена различными факторами, определяющими уровень развития финансовых рынков, наличие необходимой правовой базы, а также внутренние интересы государства. Тем не менее, в условиях нестабильной экономической конъюнктуры курс наиболее распространенных криптовалют (Bitcoin, Ethereum и др.) растет, что говорит о том, что все крепче становится фундамент доверия к ним. Блокчейн же в контексте мирового сообщества находит применение от банковской от-

расли до логистики и прогнозирования. Крупнейшие банки мира основали консорциум R3, который инвестирует в развитие данной технологии в финансовой сфере. Происходит смена парадигмы по отношению к информации, размещенной в интернете, так как блокчейн делает возможным запись только достоверной информации, исключая возможность фальсификации данных. Исходя из тенденций того, в каких сферах может применяться Блокчейн, можно сказать, что сейчас формируется новый глобальный институциональный стандарт, в котором новой государственной системе необходимо будет решить творческую дилемму: активно внедрять независимые децентрализованные технологии или же самостоятельно определять и регулировать собственный путь развития.

В Беларуси идет активное развитие и освоение технологии Блокчейн. Основными направлениями внедрения является банковская сфера и сфера управления государством. Технология позволяет существенно снизить издержки и время осуществления сделки. Все это значительно способствует формированию единого национального информационного пространства как одного из этапов перехода к информационному обществу, обеспечивающего создание условий для повышения эффективности функционирования экономики, государственного и местного управления, право на свободный поиск, передачу, распространение информации о состоянии экономического и социального развития общества [5, с.333-334].

И если сейчас Блокчейн только начинает раскрывать весь свой потенциал, то, как сказал соучредитель Блокчейн.info Ник Кэри, «Поищи это на блокчейне» станет фразой 21-го века. Эта фраза станет такой же обыденной, как и фраза «Поугли это».

#### Литература

1. История криптовалют, часть I: от создания Биткоина до криптобума [Электронный ресурс]. – Режим доступа: <http://www.inliberty.ru/library/571-kriptoalyuty>. – Дата доступа: 01.05.2018.
2. топ-10 криптовалют мира. Инфографика [Электронный ресурс]. – 2015. – Режим доступа: <http://gordonua.com/infographics/virtualnye-dengi-i-kriptoalyuty-mira-infografika-65017.html>. – Дата доступа: 01.05.2018.
3. Как работает Блокчейн, преимущества, применение, перспективы [Электронный ресурс]. – 2016. – Режим доступа: <http://fb.ru/article/261672/blokcheyn---eto-kak-rabotaet-blokcheyn-preimuschestva-primeneniye-perspektivy>. – Дата доступа: 01.05.2018.
4. Дудина, О.И. Биткоин: денежный суррогат или валюта будущего? / О.И. Дудина, В.В. Кремлева // Фундаментальные исследования [Электронный ресурс]. – 2016. – № 9 (часть 3). – Режим доступа: <https://www.fundamental-research.ru/ru/article/view?id=40789>. – Дата доступа: 01.05.2018.
5. Князева В.С. Миф или реальность: Блокчейн – технология будущего / В.С. Князева, // Национальная экономика Республики Беларусь: проблемы и перспективы развития: материалы X Междунар. науч.-практ. конф. студентов Минск, 12–13 апр. 2017 года. – Минск: БГЭУ, 2017. – с.333-334.