КРИПТОВАЛЮТА НОВОГО ПОКОЛЕНИЯ BITBON

Гава Юрий Васильевич
кандидат экономических наук

Последние несколько лет широкой трансформации обрела сфера оборота денег. Деньги за последние несколько десятилетий изменились кардинально. От денег в форме золота, к электронным и интернет деньгам. И уже в 2009 году широкого распространения обретает криптовалюта.

Криптовалюта – это цифровой актив, учет которого децентрализован. Функционирование данных систем происходит при помощи распределенной компьютерной сети. При этом информация о транзакциях не должна шифроваться и быть доступна в открытом виде. Для гарантирования неизменности цепочки блоков базы транзакций используется криптография.

Криптогра́фия (от др.-греч. κρυπτός — скрытый и γράφω — пишу) — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), а также невозможности отказа от авторства.

Изначально криптография изучала методы шифрования информации — обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа. Помимо этого раздела современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хеш-функции, управления ключами, получения скрытой информации, квантовую криптографию.

Криптография не занимается защитой от обмана, подкупа или шантажа законных абонентов, кражи ключей и других угроз информации, возникающих в защищённых системах передачи данных.

Термин закрепился вследствие статьи о Bitcoin »Crypto currency» (Криптографическая валюта), опубликованной в 2011 году в журнале Forbes[3]. Сам же автор Bitcoin, как и многие другие, использовал термин «электронная наличность» (*Electronic cash*). Способ эмиссии криптовалют может представлять собой майнинг, форжинг или IPO.

Ключевой особенностью криптовалют является отсутствие какого-либо внутреннего или внешнего администратора. Поэтому банки, налоговые, судебные и иные государственные или частные органы не могут воздействовать на транзакции любых участников платёжной системы. Всё это обеспечивает необратимость сделок – никто не может отменить, заблокировать, оспорить или принудительно совершить транзакцию без доступа к приватному ключу владельца. Однако участники сделки могут добровольно временно взаимно блокировать свои средства в качестве залога или установить, что для завершения/отмены сделки требуется согласие всех (или произвольных дополнительных) сторон [1].

Для решения форс-мажорных задач, типа задачи византийских генералов о мошеннических сигналах внутри системы, даже когда большинство узлов являются злоумышленниками, используется технология блокчейн, впервые появившаяся в Bitcoin. Для хранения данных, транзакции объединяются в блоки, из которых формируется цепочка блоков. Непрерывность цепочки обеспечивается включением в текущий блок хеш-суммы предыдущего блока. Таким образом нет возможности изменить блок без изменения хешей во всех последующих блоках, а

действительной считается только самая длинная цепочка, все хеши в которой отвечают определённым требованиям. В разных криптовалютах для верификации блоков применяются методы *Proof-of-work*, *proof of stake* или их комбинация.

Как правило, в криптовалютах разработчики изначально вносят верхний предел общего объёма эмиссии. Однако у некоторых криптовалют, таких как PPCoin, Novacoin, Sifcoin и других, отсутствует фиксированный верхний предел общего объёма эмиссии и возможна как эмиссия, так и демиссия (путём обязательного уничтожения небольшой фиксированной суммы в каждой транзакции) [2].

Большинство криптовалют используются псевдонимно — все транзакции между всеми адресами (кошельками) общедоступны, но нет связки адреса с конкретным человеком. Однако личность владельца может быть установлена, если становится известна необходимая дополнительная информация.

Криптография для конфиденциальных платежей начала использоваться с 1990 года в системе DigiCash Дэвида Чома, компания которого обанкротилась в 1998 году. Однако, его платёжная система была централизованной.

Впервые термин «криптовалюта» начал использоваться после появления платёжной системы «Биткойн», которая была разработана в 2009 году человеком или группой людей под псевдонимом Сатоси Накамто. Позже другие криптоформулы и соответственно криптовалюты – Namecoin, Litecoin и другие. До июля 2013 года программное обеспечение всех криптовалют, кроме Rippe, базировалось на открытом исходном коде системы «Биткойн». С июля 2013 года стали выпускаться самостоятельно разработанные платформы, которые помимо криптовалюты поддерживают различную инфраструктуру — биржевую торговлю, магазины, мессенджеры и прочее. К таким криптоплатформам относятся: BitShares, Mastercoin, NXT [3].

Отличительной чертой криптовалюты в целом есть то, что она не есть титульными знаками существующих валют (как интернет деньги). Процессы майнинга или эмиссии с точки зрения процесса функционирования денег ставят эти валюты в прямое противоречие с существующими валютами национальных государств – долларом, евро, рублем, юанем или гривной.

Мы знаем, что одной из основных задач любой валюты есть выполнения функции масштаба цен в экономической системе. Только та валюта, которая исполняет это условие может претендовать на эту роль. В то же время, функция масштаба цен выполняется только при условии жесткого контроля и соответствия товарной и денежной массы и экономической системе. В классической системе эту роль выполняет государство во главе с центробанками.

С точки зрения теории и практики развития денег, криптовалюты есть валютными суррогатами чью эмиссию, а значит и объем в системе контролировать невозможно. Таким образом криптовалюты в той форме, в которой они существуют на данный момент не могут выполнят функцию масштаба цен, а значит и не могут выполнять роль денег.

Ситуативное распространение криптовалют сегодня, скорее есть следствием зарегулированной банковской системы транзакций и несоответствие быстро развивающемся рынку технологий и инновационного бизнеса, часть которого с каждым годом увеличивается вдвое [4].

Но в этом хаотическом процессе есть и первые конструктивные сигналы. Часть Центробанков мира, понимая важность работы «в тренде», заявили и активно разрабатывают собственную криптовалюту. Кроме того, IT и компании финансового сектора активно занимаются развитием данного вопроса.

Стоит обратить внимание на компании Simcord и UBK Markets. Завоевав, рынок современного брокериджда на постсовестком пространстве, в 2017 году компании готовятся к запуску криптовалюты нового поколения Bitbon.

По словам создателя, Александра Кудь, криптовалюта Bitbon будет иметь свойства цифровой наличности, основанной на базе технологии блокчейн итериум. Кроме того, новая криптовалюта будет наделена свойствами акции. Таким образом, Bitbon будет выполнять функции платежа, масштаба цен и в тоже время, будет подкреплен материально-технической базой компании и потенциалом ее развития.

По задумке основателей, Bitbon соединит в себе несколько важных, в современных условиях, свойств. Новая криптовалюта будет выполнять функции платежа, масштаба цен и акции. Руководство компании также считает, что Bitbon будет отличным инвестиционным инструментом.

Сфера товарного оборота, как и сфера денег стремительно развивается. Прогнозируя развитие технологий блокчейн и криптовалют в будущем можно сказать одно – мир уже никогда не будут таким, каким он был прежде. В этом мире совершенно иное место будет отведено банкам, инвестиционным компаниям, нотариусам и другим посредникам.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Фридрих фон Хайек, Denationalisation of Money: An Analysis of the Theory and Practice of Concurrent Currencies. — London: Institute of Economic Affairs, 1976.*
2. *Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. — 2008. — 9 с.*
3. *Кирилл Сарханянц, Ольга Шестопал, Роман Рожков Много денег из ничего // Газета «Коммерсантъ», № 102/П (5133), 17.06.2013*
4. *Криптовалюты // Mercatus Center, George Mason University (перевод на русский), 1 июля 2014 (англ).*