Феномен биткоина: новая валюта и новая система расчетов современном глобальном мире

С.Перцева, к.э.н., доц. кафедры международных финансов МГИМО (У)

Биткоин является уникальной и перспективной инновацией в области финансовой и платежной систем. Сегодня данная криптовалюта привлекает к себе все большее внимание. Стоит отметить, что уникальность биткоина состоит в том, что он является новой денежной единицей, основанной на криптографии, а также представляет собой новую децентрализованную блоковую систему платежей. Появление данной виртуальной валюты заставило переосмыслить традиционные платежные схемы и задуматься об эволюции мирового валютного порядка.

Говоря о предпосылках возникновения биткойна стоит отметить, что 2007-2008 гг. оказался периодом экономической турбулентности для мировой экономики. На данном временном отрезке произошли следующие события: ипотечный кризис в США, спровоцировавший мировой финансовый кризис и глобальную рецессию, ФРС впервые в своей истории прибегнул а к механизму количественного смягчения, ЕС столкнулся с долговым кризисом отдельных стран-членов. Подобные экономические сложности и снижение уровня доверия к денежно-кредитным властям стран подготовили благоприятную почву для появления новой валюты и новой системы расчетов биткоин.

Биткоин является не единственной криповалютой: таковых сегодня насчитывается более 150 и большинство из них называют альткоинами, то есть альтернативными денежными единицами, созданными по подобию биткоина и на основе его протокола, но обладающими своей уникальной комбинацией свойств. Биткоин, однако, является первой криптовалютой по хронологии, по масштабам использования и по рыночной капитализации. Несмотря на то, что сегодня капитализация биткоина составляет более 6,5 млрд. долларов США[1], а в среднем в день с криптовалютой совершается более 150 тысяч трансакций[2], история появления цифровой валюты не может быть установлена с абсолютной достоверностью, а официальной и документально подтвержденной версии нет. По наиболее распространенной в сети версии своим появлением биткоин обязан Сатоши Накамото, саму же концепцию криптовалюты в 1998 году впервые выдвинул Вей Даи (Wei Dai)[3]. Программист, принадлежащий к неформальной группе шифропанков (cyperpunks)[4], предложил идею новой формы денег, в которой будет использована криптография для осуществления контроля и трансакций, но будет отсутствовать централизованный регулирующий институт.

[1] http://coinmarketcap.com

[2] http://thenextweb.com/insider/2015/03/29/a-brief-history-of-bitcoin-and-where-its-going-next/#gref

[3] http://www.weidai.com/

[4] https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%BF%D0%B0%D0%BD%D0%BA

В октябре 2008 года в сети от имени Сатоши Накамото появился так называемый «белый лист»[5], в котором описываются суть, механизм функционирования и назначение криптовалюты. Первая трансакция с использованием биткоина была осуществлена в январе 2009, после того как чуть ранее был запущен первый блок, который получил название «генезис» и который положил начало процессу майнинга.

«Генезис» был создан 3 января 2009 года, и первый блок системы помимо хеш-алгоритма содержал следующую текстовую надпись «The Times 03/Jan/2009 Chancellor on brink of second bailout for banks», что в переводе означает: «Министр финансов Англии готовится провести второй раунд спасения банков при помощи механизма bailout». Данная фраза взята из заголовка от 3 января 2009 газеты Таймс[6]. Использование именно этой фразы в «генезисе» может еще раз указывать на идею, стоящую за созданием альтернативной валюты и альтернативной системы расчетов, - создание независимых денежных единицы и системы в силу утраты доверия к уже существующим.

Перейдем к непосредственной характеристике биткоина. Итак, криптовалюта обладает следующими чертами:

1. Биткоин является сетью, которая функционирует на основе базового принципа консенсуса, предполагающего, что между участниками сети всегда согласие по поводу происходящего в сети.
2. Биткоин можно назвать «электронными деньгами» Интернета, так как расчеты осуществляются напрямую между контрагентами без участия третьей стороны, то есть расчетного агента, как, например, при платежах с использованием банковской карты.
3. В силу того, что биткоин – децентрализованная система, никакое конкретное физическое лицо или конкретный институт ей не владеют и ее не контролируют; биткоин находится под управлением всего сетевого сообщества пользователей. Безусловно, группы программистов и разработчиков занимаются совершенствованием системы криптовалюты, однако любые нововведения не могут навязываться – пользователи сами решают, принимать или не принимать обновление и новую версию. Таким образом, выбор направления развития системы осуществляется путем достижения консенсуса в сети. Единственное условие, которое должно соблюдаться всеми участниками императивно, - наличие программного обеспечения, удовлетворяющего общим правилам сети.
4. Биткоин представляет собой довольно простой и понятный для потребителя механизм. С точки зрения пользователей, биткоин – это мобильное приложение или установленная на компьютере программа, которые дают доступ к персональному кошельку лица и позволяют этому лицу платить и получать платежи в криптовалюте. Платеж проводится следующим образом:

[5] White paper

[6] http://www.thetimes.co.uk/tto/business/industries/banking/article2160028.ece

1. На компьютере или телефоне устанавливается специальное приложение, которое выполняет функцию электронного кошелька;

2. В приложении вводится адрес получателя (возможно использование QR-кода) и сумма платежа.

Адрес пользователя напоминает обычный физический адрес или же адрес электронной почты. Однако важной особенностью адресов в системе биткоин является то, что определенный адрес может быть использован только для одной операции. Для каждой из последующих трансакций будет сгенерирован новый адрес.

3. Платеж отправляется.

4. Приходит подтверждения.

Получение уведомления о проведение платежа занимает секунды, однако существует задержка между трансакцией и началом процесса ее верификации для дальнейшего включения в блок. Под верификацией понимается достижение консенсуса в сети о том, что используемые при расчете биткоины не были отправлены чуть ранее пользователем в качестве оплаты за другой товар или другую услугу (для предотвращения «двойной траты»). После того как операция была проверена и получила одобрение сети, она включается в блок N, который в свою очередь становится частью блоковой цепи. Последующие блоки трансакции уже будут «ложиться» на данный блок N, что будет усиливать степень сетевого консенсуса и снижать риск «двойной траты». На проверку одного блока уходит от нескольких секунд до 90 минут, в среднем около 10 минут. Предполагается, что получение 6 подтверждений от сети достаточно, чтобы считать операцию абсолютно справедливой и честной.

Расчеты с биткоином осуществляются без взимания обязательной комиссии, однако трансакции, к которым пользователи системы не назначают дополнительного вознаграждения в пользу майнеров, могут находиться в очереди на подтверждение в течение долгого времени. Ряд сетевых платформ (к примеру, Bitcoin.org), на которых размещаются электронные кошельки, по умолчанию предлагают пользователю назначить дополнительное вознаграждение за проверку. Размер вознаграждение и сам факт вознаграждения в любом случае остаются на усмотрение пользователя. Комиссия за проверку выполняет две функции: во-первых, служит премией майнерам, во-вторых, позволяет отличать реальные операции от фиктивных, цель которых - перегрузка сети. Кроме того, стоит отметить, что размер комиссии никак не связан с количеством переводимых биткоинов.

Майнинг – это действия по использованию компьютерных мощностей для обработки трансакций, обеспечения безопасности и стабильности функционирования системы, а также для поддержания единства системы и взаимосвязанности ее частей. Майнинг является децентрализованным процессом: майнеры действуют в разных точках Земли независимо друг от друг и не имеют контроля над всей системой. Название процесса в переводе с английского означает «добыча» - майнеры участвуют в процессе эмиссии

биткоинов. Эмиссионный механизм построен следующим образом: за верификацию блоков расчетных операций, майнеры получают вознаграждение в виде биткоинов[7]. Майнером может стать любой, предварительно установив на компьютере специализированное программное обеспечение, которое «отлеживает» проходящие расчетные операции в сети и выполняет соответствующие действия по обработке и подтверждению этих операций. В первые годы работы системы для майнинга могли использоваться обычные компьютеры, сегодня в связи с ростом сети и увеличивающейся сложностью вычислений необходимо специализированное оборудование.

Сам процесс проверки представляет собой подбор хеш-кода при скорости вычислений несколько миллиардов комбинаций в секунду. С развитием сети биткоина все больше людей начинают принимать участие в процессе майнинга, что делает его более конкурентным и, как следствие, повышает сложность верификации блоков. Однако среднее время, затрачиваемое на проверку, остается равным 10 минутам.

Система проверки «по объему работы» (proof-of-work) разработана для поддержания хронологического порядка в блоковой цепи, то есть с той целью, что проверка текущего блока N зависела бы от проверки предыдущих блоков N_{n-t}. Фактически из блоков проверенных трансакций создается конструкция: на первые блоки проверенных операций надстраиваются последующие блоки – такой порядок делает практически невозможным изменение сути ранее осуществленной и верифицированной операции, так как эта операция, заключенная в блок, «лежит» в основе блоковой цепи. В силу того, что майнинг конкурентное занятие, возможна ситуация, при которой один блок успешно проверяется двумя или более майнерами и несколько версий одного блока рассылаются на узлы. В этом случае майнеры продолжают работу по проверке следующих блоков, а узлы сохраняют несколько версий крайнего проверенного блока, ориентируясь на ту, что получили первой. Когда же следующий блок найден, узлы переключаются на более длинную ветвь цепи. Вознаграждение же за проверку блока получит тот майнер, чья цепь окажется длиннее и станет признанным сетью продолжением общей блоковой цепи системы.

Выше упоминается термин «узел», со смыслом которого также необходимо разобраться. Каждый компьютер, подключенный к сети биткоина, является узлом. При этом узлы в зависимости от степени «вовлеченности» условно делят на две группы: полные (full) и неполные (lightweight)[8]. Полные узлы – это динамические базы данных, в которых размещается и постоянно обновляется информация о функционирование системы. Кроме того, полные узлы выступают в качестве противовеса сообществу майнеров. Полные узлы поддерживают сеть и ее протокол в исходном виде и выполняют в сети следующие функции:

[7] https://www.bitcoinmining.com/

[8] https://en.bitcoin.it/wiki/Full_node

- Хранят информацию обо всех когда-либо проведенных операциях;
- Следят за исполнением правил общего консенсуса;
- Сортируют трансакции и блоки операций для неполных узлов;
- Передают другим полным узлам информацию, накопившуюся за время отсутствия последних в сети;
- Передают майнерам информацию о совершенных операциях;
- Передают пользователям данные о проверенных блоках от майнеров[9].

Остановимся отдельно на одной из характерных и наиболее неоднозначных черт биткоина – на высокой степени анонимности платежей. Биткоин позволяет получать и отправлять платежи с существенным уровнем приватности. Однако стоит заметить, биткоин не является полностью анонимным платежным средством, как например, наличные деньги.

В традиционной платежной системе полной информацией о платеже, его сумме, валюте, направлении обладают плательщик, получатель платежа и расчетный агент, в роли которого обычно выступает банк. В децентрализованной новой системе иной подход: информация о самом факте совершения платежа доступна всей сети, однако благодаря механизму частных ключей личности плательщика и получателя платежа будут оставаться скрытыми. Кроме того, так как для каждой новой операции генерируется новый частный и общий ключи, практически невозможно связать несколько платежей с одним обезличенным адресом отправки или получения. Однако факт привязки платежа к обезличенному адресу все же может стать известен сети: транзакции с несколькими входами (multi-input) доказывают, что суммы принадлежат одному лицу, тогда как определенная информация о трансакции хранится в децентрализованном регистре.

Перейдем к преимуществам и недостаткам биткоина. К сильным сторонам криптовалюты относится следующее:

- Свобода платежей;
- Комиссия и ее размер на усмотрение пользователей;
- Невысокие риски для поставщиков товаров и услуг (безотзывность);
- Безопасность и контроль;
- Прозрачность (общедоступный регистр).

Среди недостатков биткоина следующее:

- Ограниченная распространенность криптовалюты;
- Волатильность;
- Активно продолжающийся процесс технической разработки и правового оформления биткоина;

[9] http://www.coindesk.com/bitcoin-nodes-need/

- Высокая степень анонимности (этот вопрос активно прорабатывается как разработчиками, так и органами финансового регулирования)
- Ряд рисков, а именно:

1. Операционный или технический риск;
2. Риск двойной траты;
3. Риск «атаки 51%» (если какой-либо группе майнеров удастся контролировать 51% всех компьютерных мощностей системы, то технически эта группа майнеров может менять историю совершенных трансакций и использовать одну денежную единицу несколько раз (риск двойной траты)).

Таким образом, в настоящее время создана альтернативная денежную единицу и платежную систему, где отсутствует расчетный агент. Биткоин функционирует на основе механизма цифровых подписей и криптографии, что обеспечивает сохранность прав владения цифровой валютой, однако при этом сохранялся риск «двойной траты». Для решения данной проблемы были разработаны децентрализованный регистр и механизм верификации трансакций «по объему работы». Децентрализованный регистр делает «историю» расчетов общедоступной, а схема «по объему работы» делает практически невозможным (с технической точки зрения) внесение изменений в «историю» расчетов, если в сети есть достаточно большое число полных узлов и большая часть вычислительных мощностей под контролем «честных» майнеров.

Литература:

1. Satoshi Nakamoto «Bitcoin: a peer-to-peer electronic cash system» 2009
2. Ali R, Barrdear J, Clews R and Southgate J «Innovations in payment technologies and the emergence of digital currencies» Bank of England Quarterly Bulletin, Vol. 54, No. 3 2014
3. Government Office for Science «Distributed Ledger Technology: beyond block chain» 2015
4. Bank For International Settlements «Digital currencies» 2015
5. ECB «Virtual currencies schemes - a further analysis» 2015
6. HM treasury «Digital currencies: response to the call for information» 2015
7. Federal Reserve Bank of Richmond «Digital currencies» 2013
8. ECB «Virtual currencies schemes» 2012
9. http://www.reuters.com
10. http://www.bbc.com
11. http://www.forbes.com
12. http://www.thetimes.co.uk
13. https://ru.wikipedia.org
14. https://bitcoin.org
15. https://en.bitcoin.it
16. http://bitcoinppi.com
17. http://usebitcoins.info
18. http://bitcoinconf.moscow/ru
19. http://bitnovosti.com
20. http://www.coindesk.com
21. https://blockchain.info
22. https://www.bitcoinmining.com
23. http://coinmarketcap.com
24. http://www.weidai.com
25. http://thenextweb.com