

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И МАТЕМАТИЧЕСКИЕ МЕТОДЫ

УДК 003.26

СОСТОЯНИЕ И ПЕРСПЕКТИВА ИСПОЛЬЗОВАНИЯ КРИПТОВАЛЮТ

А.А. Бондарчук, 2 курс

Научный руководитель – Л.П. Володько, к.э.н., доцент

Полесский государственный университет

В последние годы широкое распространение получил такой феномен как криптовалюта. Криптовалюту википедия описывает следующим образом: Криптовалюта – один из видов цифровой валюты. Ее эмиссия и учет основаны на разных криптографических методах. А функционирование происходит децентрализованно, в распределенной компьютерной сети.

Криптовалюта – это реальный программный продукт, рост курса которого зависит только от спроса и предложения, а не от вкладчиков.

Рассказывая о криптовалюте нельзя не упомянуть о биткойнах («Bitcoin»). Виртуальные деньги биткойн – это одна из многочисленных криптовалют, электронное средство, которое создал никому не известный программист (или группа программистов) под псевдонимом Сатоши Накамото. Произошло это в 2009 году. Термин "Биткойн" и специфику (алгоритм работы биткойна) придумал именно он.

Никто не знает, откуда этот человек и как его зовут в реальном мире. Он создал не только программу, но и специальное приложение – кошелек на вашем персональном компьютере, содержащий криптовалюту биткойн.

Криптовалюта биткойн имеет основные функции и свойства обычных денег разных стран: средство обмена, средство сбережения, расчетная единица.

Как и всякая валюта, биткойн имеет свой курс. Проверить текущий курс криптовалюты можно на сайте blockchain.info. Но тем не менее, биткойн остается криптовалютой.

Наряду с этим биткойн является пиринговой одноранговой сетью. Это означает что все участники сети являются равноправными, нет центрального сервера, который всем говорит, что делать. Также важно понимать, что все операции, происходящие в сети биткойну записываются в базу данных, и эта база данных хранится у всех участников сети одновременно и также одновременно обновляется. Эта база разбита на логические части, которые называются блоками. Каждый блок одновременно является:

- решением задачи;
- фактом эмиссии новых монет;
- подтверждением валидности транзакций, прошедших в период с момента – нахождения предыдущего блока и до времени нахождения этого блока;
- списком всех этих транзакций, с указанием кошельков отправителя и получателя, времени и суммы.

Математически биткойн представляет собой хэш-функцию с большим количеством вариантов ответа, но искомым считается так называемый «красивый» хэш, который характеризуется тем, что начинается с 15 нулей. Другими словами, сеть считает все возможные варианты хэша, и как только находит «красивый» она объявляет, что блок решен. В этот момент происходит эмиссия монет, которые начисляются тому майнеру (одна из профессий, кодифицированных в правовой системе «bitcoin») который нашел блок, в блок записываются все транзакции и сеть продолжает считать хэш, ища следующее значение. Это очень упрощенное изложение сути процесса.

Полезно знать, что всего биткойнов может быть 21 миллион. Для начала это может показаться неудобным, ведь 21 миллион — это слишком мало денег чтобы обеспечивать нормальное функционирование современной экономики. Но это также предусмотрено создателем и у биткойна есть такое качество как масштабируемость, т.е. 1 монету можно разделить не на 100 частей, как это обычно принято с традиционной валютой, а вплоть до 8 знака после запятой. Таким образом за единицу можно принять 0,00000001 BTC (используется для обозначения одного биткойна) что в итоге нам дает 10^{14} единиц валюты, или 100 триллионов. На данный момент суммарный ВВП Земли составляет порядка 70–80 триллионов, т.е. теоретически биткойн может заменить все деньги на Земле.

Возникает вопрос, ведь производительная мощность сети растет просто фантастическими темпами, нельзя ли найти решение быстрее 10 минут? Это также было предусмотрено создателем и в формулу задачи был введен дополнительный параметр, который называется сложность. Сложность отвечает за то, чтобы новые блоки находились по заранее утвержденному графику — раз в 10 минут. Если хэшрейт (единица измерения вычислительной мощности сети биткойн) сети растет и система начинает находить блоки быстрее, то каждые 2016 блоков включается механизм проверки, который оценивает скорость нахождения блоков и мощность сети и если они отклоняются от заданного значения то изменяет сложность, так чтобы вернуть все к желаемым показателям. Таким образом сеть сама регулирует себя.

Основная идея денег – обмен на товары, а в следствии и между людьми. Биткойн с этим справляется несколько лучше традиционных денег. Но и у криптовалют есть недостатки и достоинства. В результате проведенного анализа, можно выделить следующие достоинства:

- Анонимность. По сравнению с национальными валютами за переводами криптовалют никто не следит. Следовательно, применить какие-либо санкции к отправителю/получателю никто не может. Запретить осуществлять переводы определенному лицу тоже никто не может. Полная свобода транзакций.

- Малые комиссии. Минимальная комиссия, гарантирующая обработку транзакции, за перевод биткойн от одного кошелька к другому составляет 0.0001 btc, что по текущему курсу равняется примерно 2 рубля. Учитывая, что с такой комиссией можно переводить относительно крупные суммы (десятки, сотни тысяч рублей), она является совсем незначительной, можно сказать – её нет.

- Скорость перевода. Минимальное время осуществление перевода криптовалюты от одного человека к другому составляет пару минут. Бывают задержки и до нескольких часов, но, если добавлять к транзакции комиссию переводы будут осуществляться быстро. В то время как банков-

ский перевод между разными странами может продолжаться в течении нескольких недель, могут случиться какие-либо неполадки и тогда счёт могут заморозить на месяц.

– Отсутствие инфляции. Количество монет в этой системе растет с определенной скоростью, заложенной таким образом, чтобы она совпадала со скоростью добычи золота на планете. Так как нет ни политических сил, ни корпораций, способных изменить такой порядок, в системе нет возможности для возникновения инфляции.

– Невозможность отмены транзакции может расцениваться как достоинство, так и как недостаток, в зависимости от ситуации.

– Blockchain. Наличие обозревателя блоков в сети биткоин позволяет проследить с какого и на какой адрес производится перевод, какая комиссия взята, какие сделки попутно включены в вашу, просмотреть историю переводов каждого адреса. Банковская система традиционной экономики не предоставляет такой возможности вообще.

К недостаткам же биткойн можно отнести:

– Невозможность отмены транзакции. При переводе денег в криптовалюте никто не контролирует ваши средства и отменить перевод невозможно.

– Double spending или двойная трата одних и тех же биткоинов. Несмотря на постоянно растущую сложность, всё ещё существует возможность подобной атаки из-за сервисов подобных GHash.IO (Организация майнером). Существуют и другие типы уязвимостей, не встречающихся в мире традиционных денег, которые препятствуют глобализации криптовалют.

– Время транзакций в некоторых случаях уступает скорости перевода в пределах одного банка. Например, перевод с карты на карту одного банка занимает считанные минуты, в то время как биткоин перевод может длиться несколько часов (в зависимости от суммы и размера комиссии).

На завершение хочу сказать, что криптовалюта – это, возможно, валюта будущего. А вот близкого или далекого будущего? Это уже другой вопрос. Я думаю, в будущем произойдет слияние реальных и виртуальных денег с лучшими качествами тех и других. Но все-таки будет ли этой будущей мировой валютой именно криптовалюта Биткоин?

Список использованных источников

1. Ken Shirriff «Майним Bitcoin с помощью бумаги и ручки» //Информационный портал [Электрон. ресурс]. – 18 мая 2015. – Режим доступа: <https://habrahabr.ru/post/258181/>

2. Свободная энциклопедия [Электрон. Ресурс]. – Режим доступа: <https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82%D0%BA%D0%BE%D0%B9%D0%BD>

3. Сергей Лоншаков: Crypto 2.0 Projects Consulting [Электрон. ресурс]. –31 августа 2014. – Режим доступа: <http://bitfork-develop.com/ru/blockchain-technology-configure-e-currency-at-creation/>

4. Дмитрий Харитонов: «Алгоритм формирования блокчейна» //Информационный портал [Электрон. ресурс]. – 5 февраля 2015. – Режим доступа: <https://habrahabr.ru/company/dcoin/blog/249779/>