УДК 621.9.048.7

# ОБЩИЕ ПРИНЦИПЫ УСТРОЙСТВА СИСТЕМЫ ФУНКЦИОНИРОВАНИЯ КРИПТОВАЛЮТ

Блошкин Д. М.

БНТУ, МИДО, г. Минск, Беларусь, bloshkindzmitry@gmail.com

Первая в мире сделка, где криптовалюта была обменяна на реальный товар произошла 22 мая 2010 года. Ласло Ханеч, проживающий во Флориде, заказал 2 пиццы, он заплатил по 5000 биткойнов за каждую пиццу. В то время такой заказ обошелся ему примерно в 30 долларов США, а на сегодняшний день 10000 биткойнов равна сумме свыше 75 миллионов долларов.

В последние года у всех на слуху новости о быстрых ростах какой-нибудь криптовалюты. Например, биткойн за последний год подорожал больше чем в 5 раз, а такая криптовалюта как эфириум, придуманная российским программистом, в 33 раза. И у многих людей возникают вопросы:

- «по какому принципу работает криптовалюта?»;

- «откуда берут свою ценность?»;

- «откуда берется криптовалюта и как ее получить?»;

В последние года у всех на слуху новости о быстрых ростах какой-нибудь криптовалюты. Например, биткойн за последний год подорожал больше чем в 5 раз, а такая криптовалюта как эфириум, придуманная российским программистом, в 33 раза. И у многих людей возникают вопросы:

Основным принципом, на котором построены различные виды криптовалют является блокчейн (blockchain в переводе с английского означает цепочка блоков). Данный инструмент представляет собой цепь из блоков денежных переводов в распределенном реестре, база данных которая не хранится на каком-то обще сервере. База данных представлена в виде списка упорядоченных записей, называемый блоками. Каждый блок состоит описания времени транзакции и захешированого сообщения. Несколько транзакций группируются в блоки. Для создания одного блока, компьютерам необходимо выполнить определенный алгоритм, как только находится свободный код - все транзакции заносятся в цепочку. Полученный блок хеширут и получают новый и так далее. Хеш-запись это и есть один блок в цепочке, а блоки в свою очередь выступают ключом, подтверждающим выполнение действия. Самый старый блок невозможно изменить так как для этого потребуется одновременно поменять все блоки.

В интернете существует множество простых аналогий для показания работы блокчейна. На мой взгляд, объяснение на примере дневника наиболее понятное и удачное. Далее будет приведен алгоритм блокчейна на примере дневника.

Дневник состоит из списка дел

1. 8.00 - Проснулся
2. 8.15 - Приготовил завтрак
3. 8.45 - Съел завтрак

…

97. 17.00 - Одолжил Олегу 50 рублей
98. 18.30 - Поужинал
99. 24.00 - Лег спать

Если такой дневник находится у меня, то я всегда могу прийти к Олегу и показать, когда именно и сколько денег он у меня взял в долг. Но ничего не мешает Олегу взять мой дневник и поменять 97 запись на «забрал долг у Олега». После такого я уже ничего не смогу показать ему. Чтобы такого избежать нужно как-то зашифровать записи. Но чтобы нельзя было просто так поменять строчку мы будем добавлять к записи предыдущий хешкод и новую строчку и так до бесконечности. После чего дневник будет иметь следующий вид:

1. 5d908104fac3fb8a433260e47d12611f
2. 7ca7c4000689567594e32217e83d6f94
3. b88fb4ed86d6ce2ae19d8e9e91b02f97

…

97. b0cb8aba392a9e12c7eeb2932570e826
98. 75c538a8dc5412e4d443019320f68d9d
99. d26222d2fa7ce7ebdf4e107fd6bd0fe6

Получается, что у каждой новой записи есть информация о всех прошлых записях и о текущей. И в таком случае для того чтобы Олегу поменять одну строчку придется изменить весь дневник.

На этом примере можно увидеть, что подмена любой старой записи приводит к тому, что изменяется вся цепочка. И в случае подмены всех записей в дневнике можно было ы оставить незамеченным тот факт, что какая-нибудь запись была изменена, но в случае с криптовалютой такое сделать не получится. Сложность будет заключаться в том, что копии этих записей находятся у огромного количества пользователей, и подменить одновременно все записи не представляется возможным, так как просто ни у кого нет таких больших мощностей.

Криптовалюта хранится на компьютерах всех пользователей одновременно. Все транзакции доступны для просмотра каждому из пользователей, и любой из них может посмотреть сколько валюты было передано от одного пользователя к другому, но стоит отметить то, что личность пользователей идентифицировать не представляется возможным. Также нигде не хранятся записи о том, сколько именно валюты хранится на отдельно взятом кошельке. Из-за этих факторов система является надежной и анонимной. А еще из-за больших объемов и из-за сложности вычислений, которые специально сделали, получается идеальная денежная система, которую невозможно контролировать отдельным лицам.

Ценность криптовалюта, в частности биткойн, получила за счет анонимности транзакций. Что вызвала спрос у определенной категории людей, которые не хотят, чтобы их финансовую активность отслеживали. За последнее время курс биткойна очень сильно повысился, что свидетельствует об заинтересованности в данной валюте. На рисунке 1 представлен график колебания курса биткойна к доллару США за все время существования.


Рисунок 1 – Отношение курса доллара США к Биткойн валюте

Преимуществом биткойна является тот факт, что для операции не нужны посредники по типу банков или государства. Расчеты проводятся непосредственно между участниками.

Если подвести итоги о преимуществах криптовалюты, то можно выделить следующие:

1. В большинстве случаев комиссия за транзакцию намного ниже, чем в банках, так как ее назначают отправители денег.
2. Нет инфляции или каких-либо других факторов, которые влияют на стоимость валюты. А цена формируется лишь спросом на нее.
3. Нет контролирующего органа.

С каждым днем расширяется ассортимент товаров, которые можно приобрести за криптовалюту. Уже сейчас можно оплатить путевку или поход в ресторан.

Для того, чтобы начать пользоваться криптовалютой необходимо завести кошелек. Есть множество сервисов, которые помогут это сделать. Кошелки можно использовать как один для всех операций, так и для каждой операции с деньгами новый, что повысит анонимность.

Каждому адресу присваивается ключ, который выступает в роли пароля. При помощи данного пароля пользователь, можно сказать, подписывает совершенные транзакции.

Все свои адреса пользователь может хранить в различных видах. Например, самым простым видом хранения будет текстовый документ. Немного сложнее в виде QR кода, который можно хранить в электронном виде или распечатать на бумаге и хранить просто в кошельке среди привычных купюр. Также существуют различные сервисы в виде приложений или сайтов.

Но возникает вопрос «откуда взять биткойн?». Самым простым способом будет просто купить за обычные деньги. Но есть и другой способ. Интернет пестрит новостями о майнинге криптовалюты.

Как уже говорилось ранее у криптовалюты нет единого органа по типу банка, который берет управление транзакциями на себя. В роли банка выступают обычные пользователи, ко-

торые установили себе программу на компьютер. Эта программа решает крипто-задачи. Решением которой является подбор свободного бока для транзакции. С каждым днем таких блоков становится меньше, следовательно, вычисления становятся сложнее. Решение крипто-задач и называют майнингом. За то, что пользователь находит свободный блок, путем обычного перебора значений, он получает вознаграждение. Это вознаграждение и есть комиссия, но она по-прежнему невысока по отношению к комиссиям банков. Решая такие задачи майнеры и зарабатывают криптовалюту. Ранее говорилось про то, что размер комиссии обозначается продавцом и покупателем. Чем быстрее они хотят произвести перевод средств с одного счета на другой, тем выше они могут ставить вознаграждение майнеру.

Так как вознаграждение за решение задачи выставляют продавец и покупатель может возникнуть странная ситуация. Так, например, в 2016 году была проведена транзакция 0,0001 биткойна, комиссия которой составила 291 биткойн.

Сегодня люди скупают в магазинах видеокарты и ASIC-ы и собирают свои домашние фермы по добыче криптовалюты (рисунок 2).

Рисунок 2 – Домашняя ферма для майнинга криптовалюты

Но так как потребляемая электроэнергия при добыче криптовалюты высока, то добыча валюты таким способом становится все менее выгодным. Добывать криптовалюту на сегодняшний день выгодно в тех странах где цены на электричество относительно низкие. В таких странах строят огромные заводы по добыче различной криптовалюты, а счета за электроэнергии при относительно низких тарифах достигают десятков тысяч долларов (рисунок 3).

Рисунок 3 – Завод по добыче криптовалюты

При переводе криптовалюты на другой кошелек нужно быть внимательным, потому что при отправке на несуществующий адрес деньги будут уничтожены. Да и в принципе адреса можно потерять. И такое часто случается.

Наиболее популярная история о потере биткойнов была связана с 28-и летним британцем Джеймсом Хауэлзом. Майнить он начал в 2009 году и был один из первых майнеров в истории. Крипо-задачи он решал на обычном процессоре домашнего компьютера. Но его девушка начала жаловаться ему на шум, издаваемый компьютером, и Джеймс был вынужден прекратить майнить. На тот момент он уже насобирал 7500 биткойнов. Но из-за невысокой цены на тот период парень забыл о своем увлечении. Через время, когда компьютер вышел из строя, Джеймс поменял комплектующие, а старые оставил в ящиках. Там они пролежали до лета 2013 года после чего во время генеральной уборки все комплектующие и жесткий диск со всеми ключами были выкинуты на свалку. И только в конце ноября Джеймс увидел графики роста цен на биткойн. На тот период его 7500 биткойнов оценивались в 6,5 миллиона долларов США. По подсчетам Форбс 15% всех добытых биткойнов были утеряны.

Будущее криптовалюты предугадать сложно. Это связано с тем, что все государства не могут определиться с тем, что такое криптовалюта и к чему ее приравнять. Некоторые страны приравнивают ее к обыным деньгам и способствуют ее росту, пытаются открывать свою криптовалюту. Некоторое, наоборот, запрещают. А какие-то страны вообще приравнивают криптовалюту к товару.

Список использованных источников


1. bestcube.space [Электронный ресурс]: bestcube.space – Режим доступа: https://bestcube.space/chto-takoe-bitkoin-kriptovalyuta-i-majning-prostymi-slovami. – Дата доступа : 09.11.2017.
2. myfin.by [Электронный ресурс]: myfin.by– Режим доступа: https://myfin.by/crypto-rates/bitcoin. – Дата доступа : 09.11.2017.
3. bits.media [Электронный ресурс]: bits.media – Режим доступа https://bits.media/lost-coins/. – Дата доступа : 09.11.2017.