УДК 004.9

ПОЯВЛЕНИЕ КРИПТОВАЛЮТЫ. РЕШЕНИЕ ПРОБЛЕМЫ ДВОЙНОЙ ТРАТЫ И ВЛИЯНИЕ НА АТМОСФЕРУ

Воронина М.С., студент гр. ПИб-192, III курс
Научный руководитель: Киреева К.А., ассистент
Кузбасский государственный технический университет имени Т.Ф. Горбачева
г. Кемерово

В наше время каждый осведомлен понятием биткоина и криптовалюты в целом. Прогресс двигает человечество к тому, чтобы быстрее адаптироваться к новшествам и создавать их. Но мало просто услышать умные слова и повторить их. Необходимо понимать, как устроено явление криптовалюты и почему оно является одним из самых безопасных решений в наши дни. Слепое вложение в новые ресурсы не станет лучшим вариантом без понимания внутренней модели работы системы управления и перенаправления ресурсов. Итак, чем же криптовалюты лучше существующих платежных систем? Или все-таки хуже?

В основе концепции лежит безопасность хранения данных о переводах. Обычно представляется такая работа через журнал с последовательными записями о манипуляциях с деньгами. К каждой записи добавляется хэш, принцип распространения которого напоминает рекуррентные соотношения. Хэш представляет собой использование детерминированной схемы в процессе преобразования входной информации свободной длины в исходящую битную строчку с конкретным размером [1]. Но и этого мало. Тогда решили добавить обязательное условие на наличие нулей в определенных позициях получившегося хэша. Данное явление называется нонс, что в переводе с английского означает «число, которое может быть использовано лишь однажды». Уже из самой формулировки понятно, что придется приложить не малые усилия для выигрыша того самого биткоина.

Платежная система использует единицу биткоин для учета транзакций. Транзакция - денежная операция по записи данных. Каждая запись в отдельности представляет собой блок, а их последовательность - блокчейн. Участниками являются майнеры, совершающие плату за запись блока - комиссию.

Теперь, когда мы разобрались с общими понятиями, перейдем к преимуществам системы как единого целого.

Во-первых, децентрализация. Биткоин ничем не регулируется, хотя на него пытаются наложить запреты. Программный код открыт для любого участника, все зависит лишь от умений и навыков отдельно взятого человека. Как правило, истории транзакций и балансы хранятся на серверах финансовых организаций. Тут возникает вопрос о безопасности такого решения, ведь в сети часто мелькают новости о взломах подобного рода компаний. Однако

сама внутренняя архитектура биткоина предусматривает почти любые варианты тяжелых ситуаций.

Ограниченная эмиссия. Простыми словами, обычная валюта имеет ограниченную возможность в изготовлении и передаче кому-либо. В криптовалюте реализована функция обратной пропорциональности, которая автоматически уменьшает количество суммарно добываемых в единицу времени биткоинов. Решается проблема инфляции путем полного контроля производимых ресурсов системы.

Анонимность и стабильность решения на рынке. Каждый пользователь остается инкогнито в пределах сделок, никакой аутентификации или конфиденциальных данных. Более того, единственное, что необходимо для участия, это достаточное количество средств на счете. Что касается стабильности, все обусловлено невозможностью изменения какого-то блока в блокчейне. Нарушение правила привело бы к изменению записей по всему миру криптовалют.

Взломать можно любую систему, которую сделал человек. Зафиксированы те виды атак, которые довольно сложно спровоцировать, но не бывает ничего невозможного. Одной из таких ситуаций была «Атака 51%». Принцип заключается в том, что взломщик имеет больше совокупной мощности, чем имеет система. Тогда нет необходимости в безопасности с точки зрения подтверждения чужих блоков. Остается только подтверждать свои и блокировать чужие. Однако такая ситуация имела отношение только к старту системы, когда еще не имелось достаточного участников сделок внутри сети. Сейчас такая ситуация не предвидится, так как вероятность сбора всех суперкомпьютеров в руках одного человека близка к нулю. Атака-гонка возможна только в случае принятия факта оплаты без подтверждения в сети, что тоже не представляет возможности, так как давно был налажен механизм последовательного подтверждения. Эти виды атак и многие другие порождают проблему двойной траты.

Схема двойной траты предполагает собой использование одной и той же единицы денежного пространства в двух местах одновременно. Происходит путем копирования цифровых денег или осуществлением операций без своевременного подтверждения предыдущих. Такие уязвимости широко используются в сфере мошенничества, причем из сводок новостей можно заметить частоту такого явления. Тогда и придумали систему управления биткоином. Блокчейн предполагает механизм подтверждения транзакций и открытый леджер. С помощью упорядоченной регистрации транзакций их группы добавляются в леджер, ожидая подтверждения. Это дает время на проверку и фильтрацию двойных операций. Когда пользователь отправляет один и тот же биткоин дважды на разные счета, майнеры проверяют достоверность совершенной операции. Всегда выбирается та, которая получит больше всего подтверждений. Так исключается двойная трата.

Получение биткоина происходит посредствам траты электроэнергии. Тогда приобретение биткоина нельзя вернуть обратно. Архитектуры графического процессора и центрального процессора сильно различаются, исходя из

технических характеристик оптимальным вариантом для майнинга были выбраны видеокарты.

Как только количество компьютеров в сети криптопалюты стало стремительно увеличиваться, экологи подняли вопрос влияния биткоина на окружающую среду. «Биткоин использует больше электроэнергии на транзакцию, чем любой другой метод, известный человечеству, и поэтому это не очень хорошая вещь для климата», - сказал Билл Гейтс [2]. Самым страшным является даже не факт того, что энергия потребляется в огромных размерах. Проблема в том, что большинство предприятий для майнинга расположены в регионах, питаемых углем. Получается, что уголь питает биткоин. Происходят стабильные углеродные выбросы в атмосферу Земли. Так изменяется климат и порождается парниковый эффект.

В этом вопросе не все однозначно. Согласно статистике, майнеры используют и гидроэнергетику. Постоянно происходит поиск дешевой электроэнергии, к тому же возобновляемой. Следует понимать, что одна единица энергии, выработанная Солнцем, не равняется одной единице, выработанной угольной электростанцией. Их влияния на окружающую среду не совместимы.

На многих ресурсах приводят сравнение электрической энергии, ушедшей в биткоин, с энергией, затраченной на транзакции по карте Visa. Сообщается, что одна биткоин-транзакция равна 717,36 кВтч. Используя эту же энергию, можно совершить 482 649 транзакций по карте Visa. Конечно, в затраты на транзакции по Visa не включены затраты на прямые энергетические расходы, биоматериалы, платежные терминалы и обслуживание. Посчитав все банки, станции и иную аппаратуру, цифры тоже будут велики. Более того, энергозатратность биткоина не зависит от количества производимых транзакций в единицу временного интервала. Вся основная мощность используется в части защиты от атак реорганизации, то есть тратится на обеспечение пользовательской безопасности.

Подводя итог вышесказанному, нужно отметить следующее. Биткоин - постоянно развивающаяся инженерно-технологическая структура. Решаются проблемы утечки данных, сохраняется конфиденциальность, стабильность производимого ресурса, исключается возможность двойной траты. В то же время происходит повсеместное загрязнение окружающей среды, которое уже начали решать с помощью безопасных источников энергии. Важным моментом в практике криптовалют остается донесение информации до каждого участника сети с целью полного понимания действий им совершаемых. Внутри всего лежат алгоритмы и схемы, позволяющие повысить уровень безопасности и прикладное значение ресурса в общей мировой экономике. Законодательство неоднозначно в отношении такого продукта, но это лишь вопрос времени. Перед тем, как становиться майнером или заинтересованным участником сети, стоит ознакомиться с историей формирования криптовалюты и ее действием на внешние факторы существования.

Список литературы:

1. Что такое хэш в криптовалюте? [Электронный ресурс] // URL: https://tehnoobzor.com/cryptolife/o-kriptovaljutah/2678-chto-takoe-hesh-v-kriptovalyute.html (дата обращения 14.03.2022).

2. Проблема «влияния на климат» майнинга Биткоина [Электронный ресурс] // URL: https://habr.com/ru/post/546594/ (дата обращения17.03.2022).