Ежова Марина Алексеевна
преподаватель
ФГБОУ ВО «Пермский государственный национальный
исследовательский университет»
г. Пермь, Пермский край

КАК ШИФРУЕТСЯ БИТКОЙН?

Аннотация*: автором проанализировано понятие «биткойн». В статье рассматривается общий принцип существования биткойна и этапы, на которых происходит шифрование информации.*

Ключевые слова*: биткойн, хэш-функция.*

В далёком 2009 некто, назвавшийся Сатоси Накамото, опубликовал код-программы клиента. В январе того же года были сгенерированы первые 50 биткойнов, была проведена первая транзакция (перевод со счета на счет), а в сентябре того же года первый обмен биткойнов на реальные деньги.

Зачем нужен биткойн? Он не существует в реальном мире, ничего его не обеспечивает: ни золото, ни алмазы, ни даже древесина. Цена на биткойн напрямую связана со спросом на него. Нет спроса, нет – цены. Количество биткойнов ограничено, и со временем будет только уменьшаться: из-за ошибок в транзакциях биткойны уйдут в никуда; кто-то забудет пароль от своего кошелька, и биткойны будут утеряны.

Зато биткойны можно отдавать частями. Сейчас минимальная величина перевода 1 сатоши – 10^{-8} биткойна. По идее биткойн можно будет делить на любые мельчайшие части.

Рассмотрим действия простого человека. Чтобы начать работать с биткойнами нужно:

1. Создать электронный кошелек для биткойнов.

2. Начать получать биткойны:

– получить перевод от какого-либо другого адресата по доброте душевной или за какую-то работу в реальном мире;

– легкозарабатываемые бонусы за скачивание, просмотр реклам, заполнение анкет;

– стать частью биткойн-кранов, тоже, что и выше, но более регулярно;

– начать играть в биткойн-игры;

– стать частью блокчейна, но это требует мощные компьютеры для процесса вычислений.

Допустим, вы как-то заполучили несколько биткойнов на своем кошельке. Что с ними делать?

1. Можно обменять на другую валюту по текущему курсу (сейчас на июнь 2018 года это почти 6,5 тысяч долларов или более 400 000 рублей).

2. Купить что-нибудь (игры, фильмы, приложения – информационные, нематериальные товары).

3. Перевести другому человеку по доброте душевной ил за какую-то работу в реальном мире.

4. Копить и быть в восторге от самого факта, что у вас есть биткойны.

Так ситуация выглядит со стороны обывателя. Что же происходит с точки зрения информации?

Скачивая программу-кошелек, вы получаете генератор уникальных адресов для вашего кошелька. Теперь вы хотите отправить биткойны кому-то со своего кошелька (А). Вам высылают адрес другого кошелька (Б). Программа-кошелек на основе адресов кошельков А и Б, а также размера перевода генерируется длинная строчка до 34 символов из латинских букв и цифр – код транзакции. Там же указаны время начала транзакции и контрольные суммы для определения корректности переводов.

Дальше эта строчка путешествует по сети Интернет, пока не наткнется на машину, занимающуюся облачным майнингом (в переводе «добыча ископаемых»). Эти машины проверяют строчку на соответствие: может ли такая транзакция существовать, сходится ли контрольная сумма кода, и так далее. Если машина соглашается с верностью строчки, то записывает эту строку к себе в память, и отправляет строчку дальше с подтверждением. После 6 и более

подтверждений строчка добирается до адреса Б, и деньги появляются у получателя. Сделка свершилась.

Рис. 1. Общая схема «путешествия» транзакции

Откуда взялись машины, занимающиеся майнингом? Это те же компьютеры в биткойн сети, только они решили подзаработать и предоставляют свои вычислительные ресурсы для работы самой платежной сети. Зачем им это? За это тоже платят, биткойнами.

Такая машина записывает в непрерывную строку все транзакции, проходящие через нее. Как только нужная длина достигнута, формируется так называемый блок. На основе последнего сформированного блока дается ссылка на этот новый, и хозяин машины, сформировавший блок, получает биткойны.

Кажется, это слишком просто? Да, все сложнее. Параллельно с записью кодов транзакций должен идти сложный процесс вычисления хэш-функции имеющейся записи. Блок формируется только, если вычисленный хэш-суммы соответствует предъявленным требованиям.

Чем мощнее компьютер, тем быстрее можно вычислить нужный код. Вскоре после появления биткойна умные люди начали объединять свои компьютеры в пулы (pool – общий фонд), благодаря которым происходит распараллеливание вычислений, исключающее дублированные расчеты.

Первоначально награда за 1 блок составляла 50 биткойнов, к концу 2012 года – это было 25 биткойнов, в 2016 – уже 12,5 биткойнов. Уменьшение вполовину происходит при формировании каждых 210 000 блоков. К 2031 году

награда за блок составит 0, так как будет созданы все 21 млн биткойнов, на которые и рассчитана система.

Это общая схема существования биткойна. Каждый участник не только клиент, но вычислительный ресурс самой сети.

Теперь самая страшная часть: «крипто», ведь биткойны – это криптовалюта, то есть валюта, создание и контроль над которой основано на использовании криптографических методов.

Основная часть работы системы биткойнов – создание хэш-суммы. Что такое хэш? Это число (или набор символов), соответствующее первоначальному числу, но разительно короче. Например, сумма цифр.

Имеется номер: +7 (958) 258–09–12

Сложим все цифры: 7 + 9 + 5 + 8 + 2 + 5 + 8 + 0 + 9 + 1 + 2 = 56 => 5 + 6 = 11 => 1 + 1 = 2

Это самая простая хэш-функция. Представим нечто сложнее с переводом в бинарный код цифр и букв. Дальнейшая их перестановка, смешивание по определенному алгоритму, нахождение логических операций от разных фрагментов этой огромной цепочки 0 и 1, и, наконец, превращение обратно в набор символов: букв и цифр. Основные свойства хэш-функций:

1. По итоговому числу невозможно восстановить первоначальное сообщение.

2. Невозможно подобрать сообщение к уже имеющейся хэш-сумме (результат хэш-функции).

3. Незначительное изменение первоначального сообщения меняет итоговое значение.

Хэширование – значительный пласт в шифровании. Разработкой стойких хэш-функций заняты многие. Единственный проверенный способ размотать хэш-функцию в обратном порядке – это перебор всевозможных вариантов первоначального сообщения. А на это уходит астрономическое количество времени.

В системе биткойнов используется алгоритм SHA256. Этот способ шифрования достаточно надежен, чтобы вот уже 9,5 лет не было ни одной глобальной проблемы.

В биткойнах SHA256 используется на двух основных этапах: шифрование транзакции и создание блока.

Уточним состав кода транзакции. Она состоит из адресов отправителя, получателя, количество биткойнов, контрольной суммы и дополнительных данный (например, время отправки).

У каждого владельца кошелек генерирует множество уникальных пар ключей (длинная строчка символов): открытый и закрытый. Открытый ключ (512 бит) можно рассылать всем желающим. По нему одному перевести деньги нельзя, как и найти сам кошелек. Закрытый (256 бит) – нужен для правильного шифрования транзакций при отправлении и получения биткойнов на свой счет. Принимающая сторона присылает свой открытый ключ и хэш-сумму закрытого. Эта пара такая же уникальна, как и первоначальная пара открытый/закрытый ключ.

Фактически транзакция состоит из

1. Количество биткоинов (коды транзакций, благодаря которым эти биткоины осели в кошельке).

2. Открытый ключ получателя.

3. Хэш-сумма закрытого ключа получателя.

4. Закрытый ключ отправителя.

5. Контрольная сумма всей записи.

6. Дополнительные данные.

Как только транзакция добирается до получателя, он предъявляет свой закрытый ключ. Перевод считается выполненным, если в сети существуют не менее 6 блоков, подтвердивших и содержащих эту транзакцию.

Рассмотрим процесс создания блока. Блок считается созданным, если его заголовок соответствует требованиям. Он должен в себе нести

– хэш-функция от предыдущего блока;

– хэш-функция всех транзакций, которые уже записаны в этот блоке;

– некое подбираемое случайное число (nonce).

От всей этой цепочки берется хэш-функция. Итоговая хэш-сумма должна иметь большое число нулей вначале. Основная проблема заключается именно в подборе числа nonce. Здесь приходится просто перебирать всевозможные варианты, пока не наткнешься на нужный.

Список литературы

1. Что такое Биткоин: просто о сложном // BitcoinPaw – информация о заработке цифровой валюты Bitcoin: сайт [Электронный ресурс]. – Режим доступа: http://bitcoinpaw.com/chto-takoe-bitcoin/ (дата обращения: 01.06.2018)

2. Что такое биткоин? // Coinspot – ресурс о цифровых валютах: Сайт [Электронный ресурс]. – Режим доступа: https://coinspot.io/beginners/chto-takoe-bitcoin/ (дата обращения: 01.06.2018).

3. legkodymov. Биткойн изнутри для непонимающих // Хабр – ресурс для IT-специалистов, издаваемый компанией «ТМ»: Сайт [Электронный ресурс]. – Режим доступа: https://habr.com/post/125572/ (дата обращения: 01.06.2018).

4. Лекция 9: Хэш-функции и аутентификация сообщений. Ч. 2 / НОУ «ИНТУИТ». Курс «Криптографические основы безопасности» [Электронный ресурс]. – Режим доступа: www.intuit.ru/studies/courses/28/28/info (дата обращения 10.05.2018).

5. ARVICCO. Объясняем крипто-алгоритмы майнинга // BitNovosti – русскоязычный информационный ресурс, освещающий блокчейн-технологии, криптовалюты и смежные темы [Электронный ресурс]. – Режим доступа: https://bitnovosti.com/2014/03/19/krypto-algoritmy-mininga/ (дата обращения: 03.06.2018).