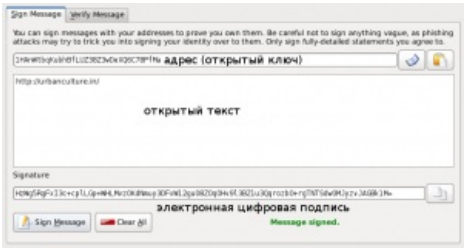
# Bitcoin — Urbanculture

Криптоконспирология

**Bitcoin** (BTC, *биткоин*, англ. *bit* — единица информации «бит», англ. *coin* — «монета») — криптографическая валюта и децентрализованная система, поддерживающая эту валюту. Разработана анонимусом для анонимуса и многим пришлась по вкусу. В отличие от банковских карт и традиционных систем электронных денег вроде WebMoney или Яндекс. Деньги, в биткоине нет вышестоящих чинов, способных заморозить ваш кошелек. Ни создатель сети bitcoin, ни правительство, ни даже правительство СШАшки не может отобрать «монетки» у их владельца, то есть того, кто распоряжается файлом бумажника. Это гарантируется алгоритмами, на которых построен биткоин. В биткоин можно оплатить большинство услуг, оказываемых через интернет.

## Для самых маленьких




Создание ЭЦП в клиенте биткоина

Программа-клиент bitcoin устроена предельно просто: есть кнопка, позволяющая узнать общее количество своих сбережений, передать деньги кому-то или узнать адрес своего кошелька, чтобы сообщить его тому, кто хочет заплатить вам. Основной ценностью является «бумажник», в котором можно создавать сколько угодно кошельков. Каждый кошелек имеет название и адрес, который является его открытым ключом. В файле бумажника для каждого созданного кошелька хранится пара ключей: открытый и закрытый. Размер закрытого ключа составляет 256 бит. Пример: 5Kb8kLf9zgWQnogidDA76MzPL6TsZZY36hWXMssSzNydYXYB9KF — закрытый ключ, 1CC3X2gu58d6wXUWMffpuzN9JAfTUWu4Kj — открытый ключ (адрес).

Проверка ЭЦП (удачная)

Проверка ЭЦП (неудачная)

В программе есть возможность поставить электронную цифровую подпись, доказывающую, что вы являетесь владельцем кошелька с данным адресом. В качестве открытого текста используется текст, о котором договорились заранее владелец кошелька и проверяющий. Важно при этом не допускать подписывания левых текстов, так как существует атака на ЭЦП, позволяющая получать ЭЦП одного текста, подписывая при этом другой текст, специально подготовленный атакующим. Чтобы этого не допустить, можно приписывать к открытому тексту что-нибудь, например, дату и время.

Когда биткоины передаются, транзакция подписывается закрытым ключом отправителя. Именно поэтому биткоины не может передавать никто, кроме владельца. Чтобы забрать биткоины против воли владельца, нужно насильственно отобрать у него файл бумажника. В случае, если владелец установил пароль на файл бумажника (это легко делается в самой программе), то атакующему придется каким-то образом узнавать ещё и этот пароль.

## Откуда берутся

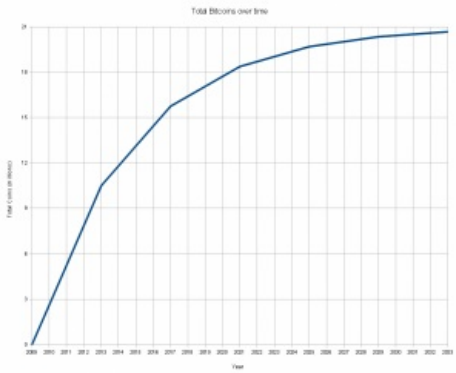
Если биткоины можно только передавать, то откуда они взялись изначально? Короткий ответ: их «добыли» (*намайнили* от *mine* — добывать).

Чтобы понять суть добычи биткоинов, нужно обратиться к способу организации сети. Все когда-либо совершенные передачи биткоинов хранятся в виде «блоков» на жестком диске каждого участника сети. Блок включает в себя транзакции, совершенные в течение примерно 10 минут. Транзакции, совершаемые пользователями, отправляются остальным участникам сети. Серверы собирают транзакции в растущий блок. Сервер, сумевший добавить блок в историю, получает вознаграждение в виде определенного количества монеток. Это вознаграждение оформляется как особая транзакция в этом же самом блоке.

Как определяется, какой сервер станет «родителем» нового блока? Можно было бы предположить, что тот, который раньше других поймал момент, когда пройдет 10 минут с предыдущего добавления. Но надежного способа организовать такое не найдено, поэтому пошли другим путем: каждый сервер, желающий создать блок, трудится над очень сложной вычислительной задачей, сложность которой подбирается самой сетью так, чтобы в среднем решение находилось 1 раз в 10 минут. Если число добывающих увеличивается, задача усложняется. Следовательно, у каждого участника понижается шанс её решить за 10 минут (среднее время решения).

Задача заключается в подборе открытого текста, включающего блок, такого, чтобы применение к нему хеш-функции давало число, меньшее заданного порога. Чем ниже этот порог, тем больше времени займет такой перебор. Решение такой задачи на GPU оказывается более эффективным, чем решение на CPU. Этот факт подтолкнул разработчиков программ для GPU, а возможно и самих GPU. В результате оказалось, что видеокарты ATI гораздо лучше оптимизированы для выполнения данной операции. Редкий случай, когда холивар ATI против NVIDIA выявил явного победителя.

Количество монет, которое получает сервер, добавивший блок в общую историю, уменьшается с течением времени. Так, с 2009 года до декабря 2012 года сумма вознаграждения составляла 50 BTC (по курсу на февраль 2013 года 1 BTC ≈ 1000 рублей). Затем это число снизилось до 25 BTC. Задумано, чтобы общее количество биткоинов стремилось к 21 миллиону. Когда количество добытых биткоинов переваливает через половину, награда уменьшается в 2 раза. Когда их количество дойдет до 75%, награда ещё в 2 раза упадет и так далее. Получаем функцию, асимптотически стремящуюся к 21 миллиону.



Количество биткоинов с течением времени

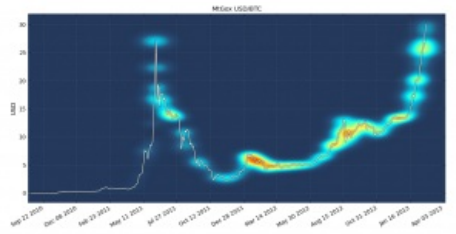
В кошельке монетки могут появиться только в результате транзакции (добыча — особый вид транзакции, в которой монетки переводятся из ниоткуда). Поэтому можно сказать, что монетки в моем бумажнике — это транзакции, переводящие деньги на мои кошельки, которые я сам ещё не использовал на другие транзакции[1]. В этом месте встает вопрос: как не дать использовать одну и ту же монетку дважды. Как раз для этого и придумана система группировки транзакций в блоки. Как только блок утверждается и принимается большинством серверов сети, все его транзакции становятся подтвержденными, любой пользователь может с ними ознакомиться, поэтому использовать второй раз монетки, если информация о первом использовании уже есть в блоке, принятом сетью, не выйдет — такую транзакцию не примет ни один сервер.

Жульничество с многократным использованием монеток остается зажатым в рамках 10 минут. В таком случае сеть примет только одну из конфликтующих транзакций. Это означает, что остальные, кому жулик успел за 10 минут втереть ту же монетку, останутся с носом. Поэтому при серьезных сделках всегда ждут, пока транзакция будет подтверждена многими серверами сети. Через 6 блоков (1 час) транзакция считается подтвержденной без разумных оснований для сомнения.

Единственным способом возникновения новых монеток является их добыча. Но есть ещё один способ заработка сервера: в каждой транзакции можно указать комиссию, которая отходит серверу, проводящему эту транзакцию. Комиссия не является обязательной, но она стимулирует сервер ускорить обработку транзакции и способствовать подтверждению её сетью.

## Ценность монеток

Биткоин представляет интерес, так как его инфляция жестко ограничена способом генерации новых монет. Общее количество тоже заранее всем известно. Скажем, если ты обладаешь 1000 BTC, то у тебя примерно одна двадцатитысячная доля всех биткоинов. А если у тебя есть миллион долларов, то это не значит ровным счетом ничего.



Курс биткоина по отношению к доллару. Скачет.

Есть нечто общее между биткоином и золотом: ресурс труднодобываемый, не представляющий интереса для промышленности (мы говорим про золото в средние века), ограниченный в количестве. Однако не стоит говорить, что биткоин — это золото 21 века. Ведь биткоин — это прежде всего валюта, а золото — материал, всегда имевший хоть какое-то применение (украшения, электроника, химические реакции). Как вложение, которое не отберет у вас очередная революция в этой стране, биткоин даже лучше золота — последнее революционеры конфискуют, если найдут.

Эти свойства пробудили интерес к валюте со стороны людей, занимающихся спорными вещами. Известно, что биткоин сейчас стал основной валютой в скрытосетях, где с его помощью приобретается оружие, наркотики и остальные товары и услуги, свободное приобретение которых затруднено.

Если кто-то потеряет файл бумажника, то бесследно пропадут все деньги, которые в нем лежали. Какая-то часть биткоинов выйдет из оборота. Если с обычными деньгами возможна замена рваных купюр на новые, то с биткоином и с золотом ситуация другая: испортил, сам виноват.

## Анонимность

Если пользоваться клиентом с настройками по умолчанию, то сервера биткоина будут знать ваш IP.

Невелика беда, если вы не посылаете никому биткоины, а только их получаете, тогда нельзя будет соотнести ваш кошелек с вашим IP-адресом. Однако при совершении транзакции серверы, через которые транзакция вбрасывается в сеть, могут соотнести IP и адрес кошелька. Если такой сервер был запущен федералами, то они смогут соотнести это с информацией об IP-адресах пользователей, предоставляемой провайдерами, и узнать, чей это кошелек. Чтобы этого избежать, в программе есть возможность выходить в сеть через прокси, причем, если это включить, то по умолчанию выставлен порт Tora. При совершении платежей биткоин через Tor нет риска, что выходной сервер сети Tor сможет подменить транзакцию, перенаправив деньги своему владельцу, так как транзакции подписываются, а необходимый закрытый ключ есть только у отправителя.

Важно, что история всех транзакций хранится неограниченно долго и доступна всем желающим. Значит, если ваш кошелек «запалили», то дальше все ваши переводы в сети биткоин сможет проследить каждый (а в случае с банковскими переводами иностранные банки могут и пободаться с федералами, прежде чем слить им инфу о клиентах). Чтобы сделать деньги на кошельке вновь анонимными, пользуются услугами биткоин-анонимайзера: это служба, в которую много людей передает свои деньги, потом анонимайзер смешивает деньги разных клиентов, переводя деньги через цепочку одноразовых кошельков, после чего возвращает их клиентам, удерживая у себя какую-то часть в качестве комиссии.

Существует немало служб обмена других электронных валют и AFK-денег на биткоины. Если есть счет в такой виртуальной валюте (например, Qiwi), который не выводит на вас, то, обменивая его через тор на биткоины, получаем анонимный счет в биткоинах.

## Критика системы

Скачки курса тоже не всех устраивают. Налоговики и ФБР озабочены возможностью отмывать деньги, а неудачники, у которых вирус стащил файл кошелька вместе со всеми биткоинами, недовольны невозможностью найти вора и набить ебальник. А теперь перейдем к адекватной критике.

Известно, что автора исходного клиента приглашали на беседу в ФБР в 2011 году, когда стало понятно, что идея p2p-денег работает. С учетом того, что исходный автор анонимен, нас терзают смутные сомнения, а уж не федерал ли он часом? А не заложено ли в биткоин уязвимостей, выгодных федералам? Но нет: код вычитывали, протокол изучали — закладок обнаружено не было.

Не всем удобно хранить у себя гигабайты истории транзакций всех людей, которых с годами будет становиться всё больше. Протокол не требует скачивания всех транзакций, однако стандартный клиент это делает — по-видимому, пережиток? времен, когда каждый клиент мог быть ещё и сервером и в меню была опция «Добывать монеты».

И из-за задержки между совершением платежа и его подтверждением (то есть, моментом, когда продавец может быть уверен, что деньги до него дошли) возникают трудности с биткоином при розничной торговле: не заставишь же покупателя в продуктовом магазине ждать, пока сеть примет транзакцию (это время может превышать 10 минут, даже сильно, так как транзакция может не «успеть» в очередной блок).

Прошел слух, что черный рынок Silk Road$_{(tor)}$, расположенный на скрытом сайте Tor и проводящий сделки в биткоинах, имеет оборот миллионы долларов в месяц[2]. Сенатор Джо Мэнчин даже призвал к «немедленному закрытию» «дерзкого» сайта по продаже запрещенных к свободному обороту веществ, что обернулось дополнительной рекламой проекта.

Кое-кто негодует, что несколько лет назад добыть биткоин не составляло труда (оставил комп на ночь — получил несколько решенных блоков и по 50 BTC за каждый). Сейчас такой возможности нет, в связи с чем подсуетившихся обладателей биткоинов ненавидят слоупоки, начавшие майнить, когда было уже поздно. Совместив этот пункт с первым (жадность с паранойей), можно дойти до совсем уж интересных мыслей, что федералы и есть основные держатели биткоинов и всё это их спецоперация.

## См. также

- Криптоанархизм
- Tor
- Даркнет

## Примечания

1. ↑ Если мне пришло 10 BTC, а я хочу кому-то передать 5 BTC, то совершается транзакция, поглощающая все 10 BTC и переводящая 5 BTC кому-то, а оставшиеся 5 BTC обратно мне.
2. ↑ Ежемесячный оборот SilkRoad достигает $2 миллионов