



Логотип биткоина

Bitcoin

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 пришлось 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 США 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.

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).

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.