Bitcoin — это такие торренты, которые вместо файлов позволяют обмениваться эдакими фантиками напрямую, бесплатно и без посредников. Которые можно продать за бабло. Этакие тру интернет-фантико-деньги, находящиеся полностью в Сети, никому не подконтрольные и доступные для всех. И всё это круто замешано на open source, стойкой криптографии и p2p-сетях.

Суть

Bitcoin — штука сложная и разносторонняя, разные люди видят в нём много всего интересного:

- нерды от криптографии — гениальное криптографическое решение, принципиально новую программную систему;
- инвесторы и стартаперы Кремниевой долины — новую подрывную технологию с невероятным потенциалом, не менее подрывную, чем сами интернеты были 20 лет назад;
- спекулянты и любители быстрых денег — новый высокорисковый финансовый инструмент, на котором можно поднять 10000% дохода, если поймать момент;
- гики и прочие погромисты — новый клёвый софт, который позволяет делать такие штуки, которые нельзя было сделать раньше;
- чиновники и банкиры — нечто непонятное, вроде как и имеющее отношение к деньгам, но вообще неясно ни что с этим делать, ни как оно работает, ни как его прижать к ногтю;
- криптоманьяки и анархисты — способ подорвать мировую диктатуру кредитного капитала;
- экономисты (особенно австрийцы) видят повод для развития новых теорий (Теорема регрессии Мизеса (http://www.rationalargumentator.com/index/blog/tag/regression-theorem/))
- наркоманы — возможность невозбранно, без рисков и изъёбов затариваться наркотой в интернетах
- нормальные люди — ничего не видят в биткоине, им похуй, до них ещё не дошло.

Не вдаваясь пока в технические детали, образно суть биткоина такова — представьте себе маленькие золотые монетки со встроенными телепортами и публичным логом транзакций. Метафора хреновенькая, но лучше пока нет, поэтому ещё раз:

- маленькие золотые монетки, потому что, как и количество золота, общее количество возможных биткоинов ограничено, создавать новые можно только через майнинг и с небольшой скоростью, а в обозримом будущем создание новых биткоинов прекратится навсегда;
- с телепортами, потому что биткоины можно передать через интернеты в любую точку мира, и никто не может этому помешать (разве только вырубив весь интернет целиком);
- и публичным логом транзакций, потому что любая смена владельца любого кусочка биткоинов записывается в общем списке транзакций, который хранится вечно всеми узлами сети и общедоступен для чтения.

И да, всё это основано на стойкой криптографии, то есть на тех же механизмах шифрования, которые используются в SSL, в SSH, в банковских сетях и т. д., которые проверены тысячи раз и на сегодня считаются надёжными. То есть взломать систему шифрования на сегодня шансов нет, а если кто и умудрится — вероятно, попутно взломает все стойкие системы шифрации мира, и тогда биткоин уже не будет никого парить. Более реальной угрозой видится так называемая атака 51%, когда большинство юзеров системы являются фейками и распространяют заведомо ложные данные о транзакциях, но проблема этой атаки в том, что на данный момент 51% от мощности сети Bitcoin — это в 9000 раз больше, чем у самого мощного суперкомпьютера в мире. Хотя прецедент имеет место быть (http://www.theguardian.com/technology/2014/jun/16/bitcoin-currency-destroyed-51-attack-ghash-io) .

Откуда взялся?

Происхождение биткоина — само по себе притча во языцех. Изначально спецификацию биткоина и первую версию кода создал некто, называющий себя Сатоши Накамото. В 2008 году он опубликовал Bitcoin Whitepaper (http://bitcoin.org/bitcoin.pdf) , в 2009 году выложил первую реализацию клиента, ещё немного пооколачивался вокруг и исчез.

Матчасть

Терминология

- **блокчейн (blockchain)** — база данных, в которой хранятся все транзакции, когда-либо происходившие, и все данные всех когда-либо существовавших кошельков. Она состоит из блоков публичных данных, связанных между собой. При этом применяемая шифрация никак не мешает читать содержимое блоков, а вместо этого математически связывает блоки между собой, и ни одну запись ни в одном блоке нельзя заменить — возникнут несоответствия в математике между блоками, и потребуется менять следующий блок, за ним следующий и так всю цепь. При этом блокчейн — распределённая база данных, то есть копии его хранятся независимо каждой программой биткоин-кошелька (кроме мобильных кошельков). То есть получается, что каждый клиент имеет у себя и независимо проверяет свою копию блокчейна, и любое несоответствие, которое попытается внести любой из узлов, будет мгновенно выявлено, и такой блок будет отвергнут другими узлами и не присоединён к цепи.
  Блокчейн открыт и публичен, и просмотреть его содержимое можно без проблем. Для этого есть или программы-парсеры, или онлайн-сервисы вроде blockchain.info (http://blockchain.info) .
- **кошелёк (wallet)** — программа, клиент сети Bitcoin, а также созданный ею специальный файл wallet.dat. Программа работает как узел сети (синхронизирует блокчейн, передаёт дальше новые блоки), а также даёт возможность юзеру посылать-принимать транзакции, смотреть историю своих транзакций и т. д. Wallet.dat — файл, в котором хранятся все данные кошелька. Проебал файл — проебал кошелёк и бабло, если не сделал бумажную копию кошелька, конечно. Программы-кошельки легко гуглятся. Программа Electrum — узкий клиент, не хранит локально всю историю блоков, а подгружает нужные части с серверов, при этом сам кошель хранится только локально.
- **адрес** — неудобочитабельная последовательность из 27-34 латинских букв и цифр. Пример: 1Jhbck6ziWRmQBp67GVDgLSJ9eFF5xNXgB. По сути — это всё, что нужно знать от получателя для перевода ему денег (намёк понятен?). В одном кошельке может быть сколько угодно адресов, но адреса между собой никак не связаны. Зная только адрес, можно выяснить, сколько денег было получено на него и с него отправлено, но нельзя выяснить, чей он, кто отправлял деньги и зачем.
- **подтверждение транзакции (confirmation)** — запись транзакции в блок и прикрепление блока к блокчейну, а также добавление новых блоков поверх блока с этой транзакцией. В сети Биткоин нормой считаются шесть подтверждений, то есть прикрепление шести блоков к блокчейну после отправки транзакции.
- **вознаграждение за транзакцию (transaction fee)** — необязательное добавление небольшой суммы к транзакции, которое отходит майнеру, успешно создавшему блок для этой транзакции. Ускоряет проведение транзакции. Без него транзакция иногда может идти до нескольких дней. Устанавливается и оплачивается всегда отправителем денег, дефолтное значение сейчас — ฿0.0001.
- **майнинг** — процесс создания новых блоков и записи в них транзакций, а также попутно — создания новых биткоинов. Майнинг нужен для существования сети Биткоин, именно майнеры создают новые блоки и записывают в них все транзакции, которые произошли с момента создания предыдущего блока. Процесс майнинга требует решения математически сложной задачи, а значит, требует нехилых вычислительных ресурсов. Чтобы люди не забили на процесс майнинга, к нему добавлена плюшка — каждый вновь найденный блок не только записывает свежие транзакции, но и даёт майнеру немного биткоинов (฿25 за блок в сентябре 2013).

- **сложность майнинга (mining difficulty)** — вычисляемый параметр, который определяет, насколько сложна математическая задача для нахождения блока. Сложность сделана для того, чтобы майнеры в погоне за профитом не добыли все блоки сразу. Сложность авторегулируется каждые две недели по всей сети, сразу исходя из количества блоков, добытых за прошлые две недели. Сложность регулируется так, чтобы при данной скорости майнинга находилось по одному блоку каждые 10 мин.
- **хэшрейт (hash rate)** — количество хэшей SHA256 в секунду, производимое всей общемировой сетью майнеров. Не определяет непосредственно скорость майнинга, так как при увеличении хэш рейта автоматически увеличивается и сложность.
- **сатоши** — мельчайшая часть биткоина, которая может быть отправлена, носит название в честь предполагаемого основателя Сатоши Накамото. 1 сатоши = 0.00000001 BTC (технических ограничений на мельчающую частицу нет, и в будущем она может быть равна $10^{-100500}$).

Как это работает

Для начала надо ещё раз сказать, что это децентрализованная система. Для того чтобы поменять или что-то изменить в алгоритмах, надо обновить все узлы сети или хотя бы большую их часть.

В отличие от, например, WebMoney, в котором при передаче средств идёт запрос серверу «вот мой счёт, переведи с него на другой счёт 100 рублей», а после владельцы сервера решают, надо переводить или нет. С биткоинами всё не так, так как серверов очень много, и они принадлежат разным людям. Транзакция выглядит так: пишем сообщение «перевожу 100 рублей со счёта А на счёт Б», подписываем его ключом, подходящим к счёту А, и отправляем это сообщение другим узлам, коих тысячи, и каждый из них независимо решает, стоит транзакция того, чтобы её включить в общий список, или нет.

То есть, чтобы повлиять на происходящее в системе WebMoney, нужно выкрутить руки людям, владеющим сервером WebMoney, что вполне реализуемо, а чтобы повлиять на сеть Bitcoin, надо выкрутить руки миллионам несвязанных майнеров, разбросанных по всему миру, что значительно сложнее. Есть теоретические способы добиться и этого, они изложены тут (https://en.bitcoin.it/wiki/Weaknesses#Attacker_has_a_lot_of_computing_power) , но всё это требует одновременно и многомиллионных вложений, и нетривиальных технических изъёбств, и всё равно остаётся легко обнаружимо и решаемо. Впрочем как получателю так и отправителю, если они известны, все-таки можно вывернуть руки или шею.

Биткоины — это такие же фантики, как и доллары, так как ни те, ни другие ничем не обеспечены. Но если копнуть глубже, становится ясно, что бакс имеет ненулевую стоимость, и на это есть причины. Вокруг этих причин и насколько они играют роль для битка разворачиваются нешуточные холивары. А разгадка проста, для экономики нужен «всеобщий эквивалент», расчетное средство. Есть вера и предпосылки, что биток станет таким универсальным расчетным средством на просторах этих ваших интернетов.

Впрочем есть определенное сходство с золотом и различие с баксом: общее количество возможных биткоинов заранее всем известно — и может быть строго не больше 21 миллиона, три четверти которых уже добыты (https://blockchain.info/charts/total-bitcoins?timespan=all) , а оставшиеся будут добывать приблизительно следующие 150 лет. Это значит, что, допустим, если есть 1000 BTC, то у обладателя в наличии примерно одна двадцатитысячная доля всех биткоинов, причём включая те, которые ещё будут добыты в обозримом будущем. А если есть миллион долларов, даже миллиард, то это не значит ровным счетом ничего, потому как сколько новых долларов завтра напечатает FED — не знает даже сам FED.

Если кто-то потеряет файл кошелька, 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 золотом ситуация другая: испортил — сам виноват. В этом контексте, количество биткоинов даже будет уменьшаться в долгосрочной перспективе. Впрочем, так как сейчас один сатоши — ₿0.00000001, а при необходимости можно легко увеличить количество знаков после запятой — постепенная потеря части биткоинов на функционирование системы не повлияет, только курс будет незначительно расти со временем.

Как этим пользоваться

Для начала — скачать программу-клиент или завести онлайн-кошелёк. Официальной программе-клиенту потребуется время и чуть более сотни гигабайт трафика для синхронизации всего блокчейна, онлайн-кошелёк готов сразу, но в онлайне безопасность обеспечивают владельцы сервиса, а десктопный клиент — твой собственный, и безопасность тоже твоя. Можно качать «лёгкие (https://electrum.org) » клиенты, хранящие у тебя не все гигазы, а только новейшую историю транзакций.

Следующим пунктом надо достать биткоинов. Если есть знакомые — попроси продать лично, если нет — см. ниже. Чтобы получить деньги от кого-то — скопируй и отправь им свой адрес. Адреса можно генерировать в кошельке, их может быть неопределённо много.

Достав биткоинов и переведя их в свой кошелёк — ты готов к участию в экономике дивного нового мира. В любом месте, где тебе встретится оплата биткоинами, тебе дадут адрес, на который платить, его скопипастишь/отсканируешь в свой клиент и отправишь деньги. Всё.

Биткоин — анонимен или нет?

Вопрос «анонимен биткоин или нет?» по-прежнему вызывает отдельные срачи, но суть тут проста — есть блокчейн, в нём видны абсолютно все транзакции, связывающие все когда-либо использованные кошельки друг с другом и позволяющие отследить каждое движение каждого сатоши. С другой стороны — отследить можно движение монеток между кошельками, а вот связать отдельные кошельки с реальными владельцами и движением товаров IRL куда сложнее, хотя и реально. Пользуешься дефолтным клиентом (http://bitcoin.org/en/download) с настройками по умолчанию — все узлы сети будут знать твой IP, и при совершении транзакции узлы, через которые транзакция вбрасывается в сеть, могут соотнести IP и адрес твоего кошелька. Если такой узел был запущен плохими дядьками, то они смогут сопоставить это с предоставляемой провайдерами инфой об IP пользователей и схватить за яйца владельца кошелька. Или не схватить, а записать в свою базу и дальше отслеживать все транзакции, идущие с этого адреса — вдруг попадётся что интересное? То есть хоть биткоин и не требует никаких регистраций, сам по себе от отслеживания концов не защищает, а также позволяет проследить цепочки перемещения денег и — возможно — связать воедино множество разрозненных транзакций.

Есть способы использовать биткоин достаточно анонимно, но они требуют дополнительных телодвижений и прямых рук. Задача анонимности расчётов состоит из:

1. получение в распоряжение кошелька с деньгами, который никак нельзя связать с личностью;
2. защита от прослушки, когда этим кошельком будешь пользоваться.

С последним всё ясно — Tor в помощь, или бесплатные публичные Wi-Fi, или ещё что-то в том же духе. А вот как получить анонимные монетки — вопрос новый.

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

Ещё есть специальные деньгоотмывалки — mixing services (https://en.bitcoin.it/wiki/Mixing_service) . Это специальные конторы, которые принимают биткоины с нескольких адресов и пересылают их на несколько других. Получается единая транзакция, у которой получатели — известны, отправители тоже, но кто именно из них кому и что именно передал — знает только сам миксер. По идее — несколько уровней смешивания дают достаточную анонимность, без идеи — за миксером тоже могут быть нехорошие дяди, а также он сам анонимен и может тупо кинуть, и все выходящие адреса транзакции будут вести в карман ему.

Ну и можно купить биткоины за нал, не раскрывая торговцу свою личность и переведя всё купленное на свежесозданный кошелёк без истории — получатся вполне анонимные монетки, никак не связанные с личностью реального владельца.

Важно потом не выводить сдачу, а лучше — использовать анонимный адрес один раз и никогда к нему не возвращаться. Ибо все транзакции в блокчейне сохранены навсегда (или пока вся система не навернётся), и через лет 10 кто-то может и внезапно найти чью-то неосторожную связь с кошельком, с которого ты оплатил убийство своей жены на Silk Road, например.

Преимущества и недостатки по сравнению с фиатными валютами (долларом, евро, рублём etc)

Pro

- Инфляция невозможна. Дядя Сэм, дядя Пу или враги не напечатают себе ещё стопицот денег и не смогут легально и незаметно отбирать у тебя заработанное честным трудом; Узкоглазый властелин правда успел намайнить себе чуть более чем 100500 биткоинов, чем уже обеспечил себе как минимум безбедную старость, а в пределе, если допустить что биткоин станет общемировой валютой он будет держать внушительную часть ее запаса, но в отличие от владельцев печатного станка потратить своё добро он сможет только один раз.
- Чтобы пользоваться всеми плюшками электронных денег, не нужно доверять деньги посреднику — банку, бирже, или «шлюзу в Интернете».
- Это распределённая система. Работоспособность обеспечивает огромное количество рядовых пользователей-узлов, каждый из которых сам принимает решение о (не-)валидности транзакций, а значит, цензура сети, ограничения на (не-)передачу денег по политическим мотивам — невозможны.
- Это распределённая система. То есть нет никакого единого центра, *организатора* системы, на которого можно надавить газом, ядовитым, или, наоборот, безвредным и полезным при сжигании, или авианосцами; куда можно выслать маски-шоу, чтобы ограничить хождение валюты или принудить отчитаться.
  - Печальным контр-примером служит централизованная псевдо-интернет-валюта Liberty Reserve, которую использовали для незаконных сделок[1]. LR умер, когда парни из ФБР пришли к его основателю и потрогали за вымя. BTW, за вымя нашего соотечественника [2].
- Высокая скорость. Обработка международных транзакций занимает минуты, а не дни и недели, и стоимость любой транзакции некогда составляла 0,0001฿ (по курсу на 20.04.14 — уже 0.05 USD) и в соседний дом, и на другой конец Земли.
- Логи всех транзакций публичны. Стало быть, все перемещения денег можно отследить: например, при (гипотетической) уплате налогов биткоинами можно проверить, куда именно пошёл каждый уплаченный сатоши[3].
- Без регистрации, без смс, без сканов паспортов и прочего. «Открытие счета» в клиенте производится нажатием одной кнопки. При должной сноровке биткоин позволяет организовать онлайн-расчёты настолько же анонимные, как покупка за кэш в подворотне. Если предпринять дополнительные телодвижения — то никто не узнает, что именно ты оплатил VIP-доступ к сайту с мультиками.
- Сверхмалая стоимость транзакций открывает принципиально новые возможности бизнеса. Например, донаты за хороший контент в размере считанных копеек с носа, или автоматическая уплата тех же копеек соседу за пользование его интернетом. Текущая рекомендованная стоимость транзакции — ฿0.0001, и даже это можно не платить в большинстве случаев.
- Счёт в биткоинах нельзя заблокировать, также нельзя отказать в обслуживании отдельным личностям по политическим мотивам.
- Биткоины нельзя отобрать через суды или давлением на банки, единственный вариант — терморектальное воздействие непосредственно на анус владельца, либо украсть секретный ключ кошелька.
- Неограниченные транзакции. Работает везде, где есть интернеты, игнорирует любые границы, загоны и подвыперды местных законов.
- Если не косячить с безопасностью — полностью теневая экономика. То есть налоговая в курсе, что бабло где-то есть и от кого-то к кому-то перетекает, но вот поймать тебя лично за руку и стрясти десятину — очень затруднительно.
- Поиск бенефициантов. Мошенники обманули твою бабушку и вытянули у неё кругленькую сумму? Не беда — ведь известно куда ведут концы (только если мошенники совсем дураки и не знают про пункт 8).

Contra

- Отсутствие обеспеченности биткоина. Государственные валюты обеспечены произведенными на ее территории товарами и услугами, кроме того, в нацвалютах уплачиваются налоги и сборы. Это делает нацвалюты востребованными. Биткоин же обеспечен исключительно спросом на него. Иными словами, пока есть на рынке желающие купить биткоины, он в цене, как это количество желающих начнет уменьшаться — стоимость биткоина начнет падать.
- Высокий риск ликвидности. Да, сейчас биткоин в цене, но сильная волатильность делает его ненадежным финансовым инструментом.
- Поиск бенефициантов. Мошенники обманули твою бабушку и вытянули у неё кругленькую сумму, а потом оплатили этими деньгами непотребщину? Беда-беда. Концы ведут к тебе. Пативен уже выехал.
- Достаточно трудно объяснить обывателю, зачем ему всё это и как оно работает. Из-за этого биткоин не станет объектом широкого пользования, так и оставшись инструментом для спекуляций на определенный промежуток времени.
- Потерял пароль к кошельку — потерял всё бабло (решаемо с помощью бумажного бэкапа).
- Ты — сам себе банк. Троян зохавал винду и грабанул кошелёк — ССЗБ. Впрочем есть онлайн-кошельки, которые делают доступ простым для технически неподготовленных пользователей, но и вся безопасность в таком случае на их стороне, если наебут или накосячат — ничего не сделаешь и не докажешь. Есть также и онлайн кошельки, которые не имеют доступ к секретным ключам, своего рода веб-программы (почти также безопасны, как и обычные программы). Также для частичной защиты от вирусни клиент лучше запускать не в своей винде, а на чистой виртуальной машине (VirtualBox и т. п.) с линуксом. Но разбираться что к чему все равно надо — это как выбирать сейф для бумажных денег.
- Софт всё ещё в бете. Найдут критический баг — всё навернётся, и пиздец баблу. Хотя искали уже очень много и старательно — пока не нашли.
- Нестабильный курс. Для трейдеров это конечно профит (даже при обвалах медведи фиксируют прибыль), но большое неудобство для торговли.
- Файл базы транзакций на май 2015 занимает 40 Гб, на январь 2017 года — уже более 100 Гб. А что будет, если весь мир захочет перейти на Bitcoin и транзакции посыпятся на порядки активнее? Всем ставить у себя в квартире серверную стойку, в ней собирать RAID-массивы из премиум-винчестеров максимального объёма и подключать гигабитный интернет? С другой стороны каждому узлу в сети не обязательно держать полную базу транзакций у себя на локальном жёстком диске, есть режим «лёгкого» клиента, который проверяет только несколько последних транзакций, а по поводу остальной истории — доверяет «полным» клиентам.
- Периодические предупреждения различных центробанков о сильной волатильности битка приводит к сильной волатильности битка.
- В нынешнем виде Bitcoin уже подходит (https://geektimes.ru/post/272154/) к своему пределу по пропускной способности транзакций в единицу времени, что мешает дальнейшему развитию. Решение — обновить все клиенты и ПО майнеров, однако тут возник срач между разработчиками и мы имеем как минимум две разных версии ПО для апгрейда, да и майнерам очень не хочется перенастраивать свои фермы. Так что либо будет форк и два разных биткоина (что плохо), либо сеть по мере роста популярности будет всё сильнее тормозить и глючить (что тоже плохо), либо разработчики всё же смогут договориться. Разумеется, данная ситуация не вызывает восторга у биткоин-гиков.

```
С лора, в обсуждении тяжести бд биткоина:
J: У тебя уже 7 гигабайт денег, че жалуешься?
```

b 422255 (http://bash.im/quote/422255)

Законность

По большому счёту во всех странах развитого мира и во многих — развивающегося работа с биткоином[4] вполне законна, ибо что не запрещено — разрешено. Но вот правовой статус биткоина пока что очень мутный. Сейчас (середина 2013) идёт активная работа всех серьёзных биткоиновых бизнесов с локальными правительствами, в первую очередь — американским, британским, немецким, чтобы совместно разобраться с тем, что биткоин вообще такое с точки зрения закона и как его регулировать. Матёрые криптоанархисты верещат, что регуляция не нужна, но крупные инвесторы, которые уже навострились вкладывать бабло в биткоин-стартапы, настаивают на регуляции, так как сейчас в мутной воде строить надёжный бизнес затруднительно.

В странах наиболее продвинутых некоторые госорганы выпустили разъяснения (http://bitcoinmagazine.com/3734/fincen-bitcoin-users-not-regulated-exchanges-are/) , которые на самом деле ничего не разъясняют, а только запутывают дело. А в стране родимых осин и бухих медведей биткоином (sic!) занялся ЦБ (http://www.cbr.ru/press/PR.aspx?file=27012014_1825052.htm) и Генпрогуратура (http://www.genproc.gov.ru/smi/news/genproc/news-86432/)

Впрочем, в той же Америке неофициальная пока, но вполне ясная позиция налоговой состоит в том, что все транзакции в биткоине облагаются так же, как и транзакции в наличных или безналом. То есть майнинг является доходом и облагается подоходным налогом, а продажа за биткоины облагается НСП.

Хотя механизмов собственно сбора налогов пока никаких нет, да и вообще как что-то отслеживать, пока не ясно, самые продвинутые биткоин-бизнесы честно рапортуют о расходах/доходах и платят налоги с биткоиновых транзакций превентивно. Если строить долгосрочный бизнес — это выгоднее, чем каждый день ожидать принудительного закрытия и потери всех инвестиций.

Интересны также отзывы людей из Bitcoin Foundation и примазавшихся, кто работает с госрегуляторами. Они утверждают (http://letstalkbitcoin.com/e37-meeting-mastercoin/#.UieNmq5hLSw) , что сейчас неприятие и пренебрежение сменилось интересом. То есть с одной стороны — все понимают, что джинн выпущен из бутылки, технология есть и распространилась, деньги вложены немалые и тупо запретить уже не выйдет, а с другой стороны — игнорировать тоже больше нельзя, и пора разбираться. То есть большие дяди из Конгресса, ФБР, АНБ, FED, ZOG etc силятся сейчас понять — что такое биткоин и что с ним делать. Так что возможно в обозримом будущем мы увидим что-то интересное в отношениях биткоина и закона. В магазине им можно платить на страх и риск свой и магазина, пока обе стороны это устраивает, но налоги магазин должен платить в долларах, рублях и т. д. Но кроме денег есть ещё товары, разнообразные финансовые инструменты, ценные бумаги и т. д. И какой-то статус такого рода биткоин имеет и в общем случае как ценный актив учитывается всеми заинтересованными сторонами.

Позиция американских финансовых регуляторов такова, что обмен биткоина на наличные должен регулироваться (http://www.fincen.gov/news_room/speech/pdf/20130416.pdf) так же, как и обмен «обычных» фиатных валют. Всем американским биржам и обменникам предписали зарегистрироваться в качестве Money Service Business и получить лицензии во всех штатах, где обитают их клиенты. Практически все после этого прекратили работу «на неопределённое время». В декабре 2013 состоялись слушания в Сенате, в ходе которых было решено не запрещать криптовалюты, а зарегулировать (http://www.hsgac.senate.gov/hearings/beyond-silk-road-potential-risks-threats-and-promises-of-virtual-currencies) . Курс биткоина после этого подскочил до $1000.

А в этой стране Центробанк сказал (http://www.cbr.ru/press/PR.aspx?file=27012014_1825052.htm) , что те, кто использует биткоин (а также меняет его на фиат) пособничают финансированию терроризма и нарушают законодательство страны. Метабанк и прочие сразу же повесили заглушку, что они прекращают работу «до выяснения обстоятельств». BTC-E, будучи зарегистрированной не в России и не на домен .ru, пока продолжает работу. Но скорее всего, учитывая откровенно ебанутые законы последнего времени, биткоин и РФ вряд ли найдут поддержку друг у друга. Sad but true — мы опять впереди планеты всей. Впрочем, нашлись недавно некие оптимисты, создавшие Национальный фонд развития криптовалют, позиционируемый как некая объединяющая биткоинюзеров площадка, лоббирующая их интересы как в Эрэфии, так и повсеместно.

Минфин готовит проект закона (http://regulation.gov.ru/project/17205.html?point=view_project&stage=2&stage_id=16241) о приравнивании криптовалют к денежным суррогатам. Первую версию проекта завернули в МинЭкономРазвития, покрутив пальцем у виска, ибо под запрет попадали любимые бонусные баллы, сертификаты, скидочные карты, авиамили и прочие плюшки. Минфин не расстроился, добавил абзац про то, что все суррогат, кроме рекламы, и дальше усердно пропихивает закон в Думу.

В сентябре 2014 Невьянский городской суд решил, что сайты bitcoin.org, indacoin.com, coinspot.ru, hasbitcoin.ru, bitcoinconf.ru, bitcoin.it, btcsec.com содержат информацию, распространение которой на территории РФ запрещено. Спустя 3 месяца Роскомнадзор их с радостью блокирует (http://bits.media/news/blokirovka-roskomnadzorom-bitcoin-saytov/) , но новость об этом получает эффект Стрейзанд и разносится всеми СМИ, после чего уже каждый школьник знает о существовании Bitcoin. Часть сайтов после этого сменили домены, bitcoinconf.ru и btcsec.com пошли судиться, а международным сайтам на законы банановых республик ожидаемо похуй.

Стоит отметить пока в России идут дискуссии по поводу полимеров, Америка и Великобритания успели молча прибрать 70% биткоин-компаний и теперь довольно улыбаются в сторонке.

Где взять

Есть варианты — пойти на биржу или в обменник и поменять фантики на циферки или списаться лично и купить у частного торговца, в онлайне или с рук.

Биржи

« *Jessika Lee > Alexander Kuzmich:* там ничего сложного, просто нужно сидеть за компом / с планшетом по 3-4 часа и мониторить пару бирж — одну, на которой торги более бойкие, к примеру — **bitstamp** а на второй, более тормозной, например, **btc-e** — торговать самому. тренд на биткоин сперва прорисовывается на более бойкой бирже и у тебя есть секунд 20-30 пока прочухается твоя »

—


Прогрессивные музыканты

Есть четыре основных биржи, которые держат большую часть рынка, и куча биржек поменьше. Каждая биржа функционирует и как обменка, то есть можно просто ввести свои кровные и купить на них биткоины по текущей цене, а можно попробовать поторговать, надеясь заработать на колебаниях курса. Большая часть бирж, особенно те, которые квартируются в культурных странах — требуют предварительного подтверждения личности для ввода/вывода фиатных валют, что выливается в геморройный процесс отправки емейлом скана паспорта и двухнедельное ожидание, пока кто-нибудь на том конце глянет на твою рожу.

- **Bitstamp (https://www.bitstamp.net)**

Тоже старая биржа, хоть и помоложе, чем mtgox. Драмы не генерирует, работает только с USD. По состоянию на начало декабря держит почти половину рынка BTC/USD.

- **BTC-E (http://btc-e.ru/)**

Раньше была русская биржа. Владельцы не стали заморачиваться с бешеным принтером и следуя правилам введения безопасного бизнеса в России (http://businessblogger.ru/10-pravil-vedeniya-bezopasnogo-it-biznesa-v-rossii.html) , свалили на тракторе, куда-то в сторону заморских островов. Какое горе! Как жаль, а ведь могла казну России-матушке пополнять!

Так же как и две предыдущие имеет треть объёма трейдинга в долларах, и тоже из тех, что были основаны в 2011 после первого пузыря. На февраль 2014 держит примерно 40% всего рынка торгов с биткоинами. Адаптирована к работе в рашкинских реалиях, имеет удобные вводы через мобильники, но геморрои с минимальной суммой вывода(при выводе кодами через людей с форума, такой проблемы нет). Зато не требует подтверждения личности (с декабря 2013 либо скан паспорта, либо money hold на месяц). Кроме джентльменского набора USD/EUR/RUB торгует ещё и несколькими говнофорками биткоина. К ней прикручен MT4, что позоляет хомячкам с форекса торговать биткоинами «не отходя от кассы» не меняя привычного интерфейса метатрейдера.

```
Из чата BTC-E:
xxx: Если школа мешает торговать на бирже, бросать надо такую школу
```

- **BTCchina (http://BTCchina.com/)**

Китайская биржа (http://vip.btcchina.com/) bitcoin с торгами в юанях. С октября 2013 года вдвое обгоняет MtGox по объёмам торговли, уделав бывшею большую тройку с торгами за бакс. Когда-то цена биткоина там была самой высокой, но после того как китайские власти всерьёз испугались битка и начали его душить стала самой низкой.

- **LocalBitcoins (https://localbitcoins.com)**

Биржа пропиаренная Росконадзором. Позволяет найти продавца в своем городе или выменять биткоин у папуасов на фрукты (https://ru.wikipedia.org/wiki/Киви_(фрукт)) . По-сути, обыкновенный пул с кучей продавцов крипты, принимающих несусветное множество способов оплаты.

- **Все остальные**

Кроме этих есть ещё пара десятков бирж поменьше (http://bitcoincharts.com/markets/list/) , в основном привязанных к конкретным странам и местным валютам. А ещё есть китайский рынок биткоина. Судя по данным тут (http://bitcoinaverage.com/#CNY) , это второй по объёму рынок после USD, и там есть свои очень крупные биржи, но что в реальности происходит в Поднебесной империи — тайна за Великой Китайской стеной.

Обменники

Кроме бирж, существуют и так называемые fixed rate exchangers (обменники электронных валют), которые выступают в роли посредников между биржами и своими клиентами, беря с них определённую комиссию за свои услуги. К преимуществам таких сервисов можно отнести более простую и быструю процедуру покупки/продажи, и больший выбор способов оплаты по сравнению с биржами, включая локальные банки. Существуют обменные пункты (например, 247exchange.com (http://247exchange.com/ru)) с возможностью купить биткоин используя кредитные карты, однако при таком способе оплаты первый заказ может превратиться в Ад и Израиль (то есть загружать дополнительные документы етц доказывая что ты не верблюд) из-за высокого риска приёма карт обменником. При этом пополнение баланса на биржах как правило также облагается значительной комиссией, в отличие от внутрибиржевых сделок при непосредственном участии в торгах.

Краны (Faucets)

Существует куча сайтов, раздающих биткоины на халяву. Конечно, речь идёт о смехотворно малых суммах — десятках и сотнях сатоши (независимо от курса), но зато ХАЛЯВА. Как правило, достаточно ввести свой Bitcoin-адрес и капчу, чтобы получить горсточку монеток. Но встречаются и более продвинутые варианты (http://myfreebitcoin.net/?lang=russian) . Основная польза таких сайтов — первое знакомство ньюфагов с криптовалютой, возможность разобраться с различными клиентами и получить первые реальные копеечки. С глобальной точки зрения польза от таких кранов тоже есть. Они помогают перемешивать потоки биткоинов, что затрудняет охотникам за любителями запрещённых ништяков отслеживание путей транзакций.

Покупка с рук

Можно найти и списаться с продавцом через localbitcoins.com (http://localbitcoins.com) , там тусуются продавцы биткоинов со всего мира, и можно запросто найти обитающих в Раше и окрестностях. Для того чтобы не кинули в онлайне — использовать внутренний escrow или сервис взаимного уничтожения кидал nashx.com (http://nashx.com) . Для того чтобы не кинули при покупке за нал IRL — изучить матчасть и проверить получение денег через независимый сервис, например, легко проверить состояние счёта, введя ID кошелька на blockchain.info (http://blockchain.info) .

Ещё можно спросить на bitcointalk.org (http://bitcointalk.org) , все известные и надёжные продавцы там есть, и их историю и репутацию несложно отследить поиском.

Что купить

Кроме наебизнеса «купи-продай на бирже» биткоины уже вполне можно применять для покупок ништяков, в онлайне и IRL.

- Многочисленные (https://allgamer.net/) хостинги (http://serverbros.co.uk/) , VPN-сервисы (http://www.bestvpnservice.com/blog/vpn-providers-with-bitcoins/) , доменные регистраторы (https://web.easydns.com/) и прочие продавцы воздуха подтянулись первыми, но кроме них есть и более полезные вещи.
- bitcoinstore.com (https://www.bitcoinstore.com/) давно торгует электроникой, и исключительно за биткоины. Продаёт вроде как дешевле чем Амазон, но доставка из Америки обойдётся в дополнительные сотни нефти, так что о цене можно спорить. Но торгует давно и успешно.
- На том же Амазоне и куче других зарубежных онлайн магазинов через гифт карточки (http://www.gyft.com/) , и даже получать небольшие скидочки.
- В Берлине местами есть небольшие скопления мелких магазинчиков, которые принимают биткоины параллельно с наличными, детали тут (https://bitcoinsberlin.com) .
- amagimetals.com (http://www.amagimetals.com/) и coinabul.com (http://coinabul.com/) давно торгуют ценными металлами за биткоины, доставляет по всему миру.
- В Лондоне (http://www.wired.co.uk/news/archive/2013-06/17/london-bitcoin-pub) и в Сиднее (http://www.theregister.co.uk/2013/09/16/australian_pub_to_serve_beers_for_bitcoin/) есть пабы, которые продают пиво за биткоины.
- Во множестве мест биткоины принимают в качестве пожертвований, ибо нет накладных расходов на транзакции и острой необходимости отчитываться.
-
- Baidu (гугл Китая) принимает биткоины (http://habrahabr.ru/post/197812/) в оплату услуг своего анти-DDoS сервиса.
- Конечно же, Silk Road — спрятанный в Торе онлайн-базар дури всех мастей и прочей нелегальщины. ФБР в октябре 2013 закрыл первый Silk Road, но свято место пусто не бывает, и Silk Road 2.0 ~~живее всех живых~~ быстро закрыли. Теперь закупаемся на **Agora marketplace** (http://agorahooawayyfoe.onion/register/wxXzdenMDM) .
- Женщин лёгкого поведения (http://www.birminghamescorts.co.uk/bitcoinescorts.html) , правда пока только в UK.
- Можно и в космос полететь (http://www.virgin.com/richard-branson/bitcoins-in-space) , особенно если ты бортпроводница с Гавайев.
- Ну и наконец, можно ничего не покупать, а просадить всё в многочисленных казино (https://en.bitcoin.it/wiki/Category:Gambling#Casinos) , букмейкерских конторах (https://en.bitcoin.it/wiki/Category:Gambling#Prediction_and_Sports_Betting) и различных сервисах по приёму ставок (http://bitbet.us/) (можно создать своё

«событие», хоть «сколько сможет выпить Петрович»). Интересно, что самым популярным сайтом азартной тематики является простой и незатейливый Satoshidice (http://legacy.satoshidice.com/)

- Можно получать биткоины за просмотр рекламы, PTC бтц заменяют старые PTC-системы, которые платили WMZ/WMR, и т. п. Примеры таких новичков: click2dad.net, coinad.com.
- Однако в Subway рядом со студгородком МФТИ до сих пор действует система оплаты биткоинами, дающая 15%-ую скидку, так-то.
- В начале июня 2014 о планах добавить поддержку биткоин заявил (http://www.cnbc.com/id/101734293) Paypal.
- Монжно купить билет на пепелац в латвийском лоукостере airBaltic (https://www.airbaltic.com/airbaltic-stala-pervoi-aviokompaniei-kotoraja-prinimaet-cifruju-valutu-bitcoin) .

В общем, биткоины ненавязчиво проникают в разные места по миру, особенно туда, где есть достаточно людей, готовых ими расплачиваться. Мест пока немного, и ещё ни одна действительно крупная ретейловая сеть или большой онлайновый магазин не взялись за это дело, но пару лет назад не было вообще ничего, нынче движение идёт по всему миру сразу, а через пять лет, возможно, биткоин будут принимать на каждом углу. Правда, судя по всему, Рашки и это касаться не будет.

Майнинг

1. Майнинг — это в первую очередь обеспечение инфраструктуры и безопасности биткоина, а добывание новых монет — сопутствующее поощрение.;
2. Майнинг биткоинов на процессорах и видеокартах устарел и неприбылен. Тут в биткоине уже давно нечего ловить. Возможно, что-то есть в форках, но статья не про них;
3. Майнинг на специализированном железе в принципе работает, но см. далее;
4. В майнинг вложены уже огромные деньги, и участвует куча людей;
5. Из-за самоподстройки сложности майнинга и фиксированного количества блоков в единицу времени и монеток в блоке общая скорость майнинга ограничена самой системой и составляет около 3600BTC в день на всех участвующих во всём мире. Поэтому количество гигахэшей само по себе значения не имеет, имеет значение только твоя личная скорость относительно скорости всей сети;

Монетка номиналом 25 BTC

В итоге для среднего анона в майнинге биткоинов ловить уже давно нечего — времена дикого майнинга прошли, и IT-ковбои остались не у дел.


Очень красивая монетка

Как работает майнинг?

Все когда-либо совершенные передачи биткоинов хранятся в виде «блоков» в блокчейне. Блок включает в себя транзакции, совершенные в течение примерно последних 10 минут. Каждый из майнеров независимо собирает транзакции в растущий блок, и каждый хочет этот блок создать и прикрепить к цепи. Узел, сумевший добавить блок в историю, получает вознаграждение в виде определенного количества монеток, и это вознаграждение оформляется как особая транзакция в этом же самом блоке.

Как узнать, какой узел станет создателем нового блока? Каждый узел, 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 общая скорость создания блоков увеличивается — через каждые 2016 блоков (две недели при дефолтной скорости) задача усложняется, и наоборот. Следовательно, у каждого отдельного участника понижается шанс её решить за 10 минут (среднее время решения). Сама задача заключается в подборе открытого текста, включающего блок, такого, чтобы применение к нему хеш-функции SHA256 давало число, с определённым количеством нулей в начале, то есть меньше заданного порога. Учитывая весьма хаотичный характер вывода SHA256(SHA256(текст+nonce)), задача не решается иначе чем прямым перебором параметра nonce. Чем ниже этот порог, тем больше времени займёт такой перебор. Сложность сети зависит от скорости вычисления (добычи) блоков и корректируется каждые 2 недели. То есть чем больше майнеров пытается подписать блок, тем больше сложность.

Вознаграждение за новый блок в общей истории уменьшается с течением времени. С 2009 года до декабря 2012 года сумма вознаграждения составляла 50 BTC. Затем это число снизилось до 25 BTC. Когда количество добытых биткоинов переваливает через половину, награда уменьшается в 2 раза. Когда их количество дойдет до 75%, награда упадет ещё в 2 раза, и так далее. Получаем функцию, асимптотически стремящуюся к 21 миллиону возможных биткоинов.

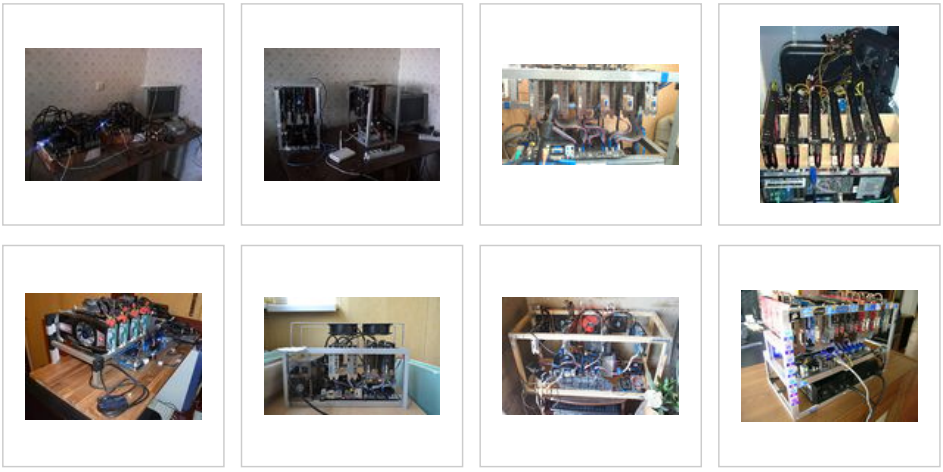
В кошельке монетки могут появиться только в результате транзакции (добыча — особый вид транзакции, в которой монетки переводятся из ниоткуда). Поэтому можно сказать, что монетки в бумажнике обывателя — это транзакции, переводящие деньги на кошельки обывателя, которые обыватель ещё не использовал на другие транзакции.

Единственным способом создания новых блоков и записи транзакций является майнинг, и майнеры являются фундаментом сети, который поддерживает её работоспособность, а они получают вознаграждение в виде добытых монеток. Но есть ещё один способ заработка майнеров: в каждой транзакции можно указать комиссию, которая отходит узлу, создавшему блок, в который попадёт транзакция. Комиссия в основном обязательна и обычно составляет ฿0.0001. Планируется, что комиссия станет основной мерой стимуляции поддержки сети, когда все монетки будут добыты, а также что комиссия будет определяться рынком, где майнеры продают, а все пользователи сети — покупают услугу обработки транзакций.

Майнинг на видеокартах

Решение такой задачи на GPU оказывается более эффективным, чем решение на CPU. Этот факт подтолкнул разработчиков софта для GPU, а возможно, и самих процев. В результате оказалось, что видеокарты ATI были гораздо лучше оптимизированы для выполнения данной операции. Редкий случай, когда холивар ATI против NVIDIA выявлял явного победителя. Однако компания nVidia с опозданием на годы, но поняла, что топовые видеокарты покупают не только для игры в Crysis, и серия GTX 900 по хэшрейту стала обгонять конкурентов от ATI/AMD.

Галерея ферм



Показать

Асики

Специализированные чипы, годные только для майнинга, а также локальный мем сообщества майнеров. Вещь, которая сбросила фермы из шести Radeon HD7970 с пьедестала прибыльности и в обозримом будущем грозит полностью уничтожить GPU-майнинг. Представляет собой микросхему, специально заточенную на вычисление SHA-256 хэшей и не умеющую ничего другого. Самые дешёвые и слабые асики равны по скорости самым дорогим фермам видеокарт, а энергии потребляют на три-четыре порядка меньше, sad but true. Владельцы тех самых ферм из трёх HD7970 обижаются и уходят на Litecoin.

В середине 2012-го ASIC-майнеры создали некоторое напряжение в комьюнити майнеров, так как ещё из идеи стало ясно, что это подорвёт экономику GPU-майнинга, поэтому самые умные бросились разрабатывать свои чипы, а все остальные — нести им своё бабло и сраться на bitcointalk.org о том, кто таки первый напилит. Сразу несколько контор взялись за дело — AVALON, BFL, ASICMiner. Все пообещали доставить в последнем квартале 2012-го и сразу подняли нехило бабла на предзаказах. Например, первая партия AVALON ASIC — всего 300 шт. по $1299, и все были раскуплены меньше, чем за сутки, а BFL денег на предзаказах подняла намного больше, так как не ограничивала количество обещанных аппаратов и смело продавала предзаказы всем желающим. В итоге у них скопилось заказов на $3-4 мегабакса, отдельные — по $100k+.

Но самая мякотка началась в конце года. 300 аппаратов AVALON прибыли к счастливым владельцам более-менее по графику, а вот BFL не доставила как в октябре, так и в ноябре и декабре, и в январе-феврале пламя батхёрта уже пылало термоядерным огнём, особенно на фоне новостей вроде этой (http://www.reddit.com/r/Bitcoin/comments/188ljj/jeff_garziks_avalon_asic_miner_paid_for_itself) . В итоге BFL начала доставлять по предзаказам только в мае 2013, и на сейчас отшипано где-то до начала весны 2013. При этом накал страстей не стихает, и свежеполученные асики быстро перепродаются вдвое дороже на Ебее, и даже предзаказы перепродаются за деньги намного большие, чем за них было уплочено. А самое смешное, что асики, заказанные ещё в 2012, уже не актуальны и, скорее всего, не окупят даже своей стоимости, потому что сложность с тех пор выросла на пять порядков и на подходе асики второго поколения, на чипах 28-22 нм вместо 65-45 нм первого поколения. Стоит также добавить, что производители асиков не дураки и сами вовсю на них майнят, прежде чем поставить их покупателю. В майнерах Авалона, например, находят дофига пыли, скопившейся там явно не за полчаса. В качестве бонуса хитрые китайцы отсоединяют некоторые шнуры внутри чудо-машины, чтобы покупатель пару дней помучился, втыкая их на место, и не участвовал в майнинге как можно дольше.

ASICMiner тут стоит отдельно, так как она аппаратов не продавала, а вместо этого продавала акции себя, с обещанием доставить генерирующие мощности в расчёте на акцию. Их история тоже сгенерировала драму 600+ страниц ветки форума (https://bitcointalk.org/index.php?topic=99497.12440) .

Такие разные асики

AVALON, первый выпущеный ASIC, 60Gh/s.

Приснопамятные асики от BFL в спецификации 2012 года, от 4,5Gh/s до 500Gh/s.

BFL Jalapeno, без корпуса, уже в актуальной спецификации 2013го, 5Gh/s.

KnCMiner Jupiter, второе поколение на 28нм техпроцессе, 400Gh/s, только предпродажа.

Показать

Піар

Биткоин начал набирать популярность в среде продвинутой молодёжи.

В конце 2010 — начале 2011 биткоин перерос стадию голого киберпанка и достиг паритета с долларом. Вполне взрослые дяди получили возможность делать деньги из воздуха, генерируя эмиссионные биткоины. Для этого всего-то надо купить хорошую видеокарту и запустить бесплатную программку. Восторженные дяди начали люто, бешено пеарить биткоин, получив первые доллары и окупив видеокарту за месяц.

Курс криптовалюты стремительно рос, с лёгкостью преодолев планку 10 долларов летом 2011-го. Обороты биткоина росли. В сети Tor начали появляться ресурсы типа «Silk Road», торгующие нехорошим за биткоины — начали с веществ и детей. Уже появляются объявления о продаже радиоактивного. Разумеется, потребители данных категорий контента внесли свою лепту в пеар инновации.

К пеару начали подключать тяжёлую артиллерию. Набрав в поисковой строке Ютуба «bitcoin», можно обнаружить массу репортажей вполне рукопожатных телеканалов — CBS, CNN, «Аль-Джазира». Пока это репортажи в передачах «с добрым утром» и «новости высоких технологий», но всё только началось.

Подключились уважаемые издания — Forbes, The Economist, Smart Money, PC World, Wired, New-York Times.

О биткоине заговорили сенаторы (http://themonetaryfuture.blogspot.com/2011/06/senator-schumer-vs-bitcoin.html) . Пока в негативном контексте, но какое это имеет значение, фокус внимания общественности привлечён.

Основатель шведской Пиратской партии Рик Фальквинге весной 2011 года объявил о том, что вложил все свои деньги в биткоины. Месяцем позже Wikileaks стали принимать в них пожертвования. Ведущий программы Keiser Report на Russia Today Макс Кайзер посвятил сабжу несколько эфиров, а потом еще и выступил на первой европейской Пражской биткоин-конференции, где пообещал привлечь в течение года миллион новых пользователей. Тем временем, с конца июня 2011 года курс упал с 30 долларов до 3-5, на радость всем недавно подключившимся спекулянтам. В сентябре Нобелевский лауреат по экономике и по совместительству ортодоксальный кейнсианец Пол Кругман в своей колонке в New-York Times подверг сабж довольно поверхностной критике, отметив, однако, что он имеет некоторое будущее как high-risk investment. К 2012 году про биткоин знали уже почти все, кто хотя бы немного интересовался новыми технологиями — бывший CEO Google Эрик Шмидт упомянул его на конференции в Барселоне, признавшись, что в Google планировали создать свою собственную децентрализованную валюту — «гугл-баксы», но свернули разработку из-за намечающихся проблем с законом; сам великий и ужасный Ричард Столлман положительно отозвался об идее peer-to-peer платежных систем, правда, как работает биткоин он пока, по его же словам, не разобрался.

Лулзы и драмы

> *Дело в том, что я собираю и продаю компы. Дешевые. С 5670 и 5770. Иногда с 6xxx. С левой виндой (на халяву) и майнером в трее. Интернета в нашем городе нет только у очень ленивых — провайдеры чуть ли не заставляют провести интернет, обещая блага неземные. И каждый день появляется 5-10 новых хомячков. Знаете, моя ферма очень красива ночью. Порой выйдешь на балкон вечерком, глянешь на светящийся огнями город и с гордостью говоришь — «Это — моя ферма!». P.S.: Люблю фильм «Матрица», особенно момент, где показана бескрайняя ферма с людьми-батарейками. :]*
>
> — Анонимус

Пицца за миллион

В мае 2010 года майнер lazslo на оф. форуме создал тему (https://bitcointalk.org/index.php?topic=137.0) , в которой предложил заказать ему пиццу, за что он готов заплатить 10 000 BTC. Хотя у него была возможность продать эти биткоины чуть дороже, чем стоимость пары пицц, ему было прельстиво от самого факта пиццы за биткоины. Чуть позже пользователь jercos заказал ему пиццу, за что получил 10 000 BTC. Примерно через год стоимость одного BTC подскочила до 32 $, то есть стоимость пиццы составила 320 000 $, а по курсу на конец января 2014 — уже более семи с половиной миллионов долларов. Узнав об этом, майнер lazslo выдрал из своей задницы не один клок волос. В честь памятного события, комьюнити принято отмечать Bitcoin Pizza Day (http://www.coindesk.com/how-the-crypto-community-is-celebrating-bitcoin-pizza-day/) каждое 22е мая, нажираясь пиццей и угощая ей бездомных, детишек и прочих пациентов (http://www.reddit.com/r/Bitcoin/comments/36w584/thanks_to_you_all_we_delivered_57_pizzas_to_the) .

QIWI

12 января 2011 года Киви внезапно заблокировала кошельки всех пользователей, замеченных в связях с российской биткоин-обменкой metabank.ru, и потребовала сканы паспортов от всех этих пользователей. Администрация хабра перенесла обсуждения этого (http://habrahabr.ru/blogs/i_am_angry/136130/) и этого (http://habrahabr.ru/blogs/i_am_angry/136063/) в закрытый блог, дабы не нагнетать панику и срач. Копия доступна тут (http://juick.com/1712406) . Через время работа с Qiwi была возобновлена без проблем, и драма сошла на нет.

Пожертвования WikiLeaks

В 2011-м из-за неофициального довления некоторых сенаторов Paypal и VISA заблокировали все пожертвования, собранные WikiLeaks на тот момент, и отказались пересылать им дальнейшие пожертвования, что обошлось (http://www.wired.co.uk/news/archive/2011-10/24/wikileaks-in-money-struggles) WikiLeaks в $15M. Биткоин спешит на помощь! С 2011 года WikiLeaks получил (https://blockchain.info/address/1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v) почти 4000 биткоинов в обход всех блокировок, что позволило ему выжить и не прекратить работу.

Скачки курса

Такие дела

В начале февраля 2013 года начался внезапный рост курса биткоинов к доллару. После долгого стабильного положения на уровне $10-15 курс начал расти. В итоге 8 апреля 2013 год был зафиксирован исторический максимум — $263. Казалось бы, сейчас спекулянты заработают денег, и он опять откатится назад на прежние позиции, но нет. После суперскачка и серии скачков с амплитудой в 20-30 баксов курс к июлю 2013 стабилизировался в коридоре 90-110 (MtGox).

После более чем месячного роста осенью 2013-го, биткоин начал бить свои исторические максимумы. 29 ноября он взял отметку 1242 доллара на MtGox. Кто-то запасается попкорном, кто-то сливает в обменниках зарплату.

MTGox

Самая старая и до 2014 года — самая крупная биржа. Именно на ней происходили все крупнейшие драмы с взлётом и падением курса. До 2013 года контролировала 80-95% всего трейдинга, в 2013, особенно после апрельского пузыря, начала сдавать позиции, так как на них начали сильно давить власти США. Работала с хуевой тучей реальных валют, больше чем любая другая биржа.

В США есть контора под названием Dwolla, которая реализует небанковскую систему мгновенных расчётов наподобие Paypal. У них была прямая интеграция с MTGox и возможность мгновенного ввода-вывода долларов. Однако в мае 2013 кровавая гэбня (http://www.dhs.gov/) Пендосии заставила Dwolla, во-первых, прекратить все расчёты с MTGox, а во-вторых — заморозить счёт MTGox и все деньги на нём. Официально MTGox обвинили в реализации услуг «money transmitter» без соответствующих лицензий. Точная отжатая сумма не называлась, но очевидно деньги были немалые, так как это был самый дешёвый, быстрый и удобный метод ввода-вывода долларов в Америке.

По итогу — MTGox потерял кучу денег и преимущество перед другими обменками, биткоин в целом поимел негативный пеар.

7 февраля 2014 гокс полностью заморозил вывод денег с биржи как биткоинов, так и долларов, объяснив это «техническими причинами». Владельцам биржи удалось ещё пару недель покормить трейдеров завтраками (за это время курс на бирже упал до 100$ по сравнению с ~600$ на других биржах). 24 февраля сайт ушёл в оффлайн, а вскоре его владельцам пришлось признаться, что «технические причины» — это проёбанные в неизвестном направлении 850000 битков (ни много ни мало 7% от всех биткоинов, находившихся на тот момент в обращении), и объявить о банкротстве.

Кстати, изначально mtgox.com должен был быть обменкой MtG, но биткоины оказались выгоднее, а название так и прижилось.

MTGox и вывод фиатных денег

После бума цены биткоина в апреле, вызванного тормозами MTGox'ом обвала цен, панического вывода денег, блокирования счетов Dwolla, взаимных исков с CoinLab и прочих неприятностей у MTGox начались серьёзные проблемы с выводом фиатных денег. 20-го июня 2013 MTGox объявил о заморозке всех выводов из обменки на две недели (кроме вывода биткоинов). Предлогом было переключение на работу с новыми банковскими партнёрами и на новые механизмы вывода. Через две недели (4-го июля) MTGox объявил, что а) выплаты возобновляются, б) за две недели было выплачено более $1M в ручном режиме. Для успокоения общественности тогда же в июле MTGox пригласил Роджера Вера (http://www.rogerver.com/) (которого неофициально называют Bitcoin Jesus за лютый, бешеный промоутинг биткоина) посмотреть на их бухгалтерию и подтвердить, что всё в порядке (http://www.thebitcoinchannel.com/archives/16852) .

Тем не менее, с тех пор и до текущего момента выплаты с MTGox чудовищно тормозят — на вывод фиатных денег требуется до трех месяцев, а быстрее — только за дополнительные 5% с выводимой суммы. Всё это не касается биткоинов, их можно выводить без проблем, но это создаёт искуственное давление на цену, так как всем приходится покупать биткоины, чтобы получить обратно свои деньги из MTGox. В результате на сентябрь 2013 цена биткоина на гоксе выше на $20, чем средняя по всем остальным обменкам (http://bitcoinaverage.com/#USD%7Cnogox) , а на реддите и в других местах активно обсуждается тот факт, что обменка без вывода не обменка и учитывать их курс нельзя.

«Арест» бабла терпилы-наркомана

12 апреля 2013 госнаркокартель США заявил, что арестовал ฿11.05 терпилы по имени Eric Daniel Hughes за покупку дури на Silk Road. Это несколько напрягло сообщество и всех, кто в теме, ибо один из фундаментальных плюсов биткоина в том, что отобрать деньги через суд и т. п. нельзя. Расследование (http://letstalkbitcoin.com/users-bitcoins-seized-by-dea/#.UjsJwD_AHGI) показало, что, скорее всего, это был не арест как таковой, а ловля на живца, то есть сами госнаркокартельщики зарегались как продавец на Silk Road и делали вид, что толкают дурь, а потом, получив транзакцию от подходящего терпилы, закричали «Попался!». То есть биткоин как система не скомпроментирован и вполне надёжен, и можно не париться, а вот покупая дурь на Silk Road — стоит озаботиться анонимностью.

Калифорния требует закрыть Bitcoin Foundation

30 мая 2013 местное калифорнийское правительство штата направило Bitcoin Foundation официальное требование «to cease and desist (http://www.coindesk.com/california-issues-cease-and-desist-letter-to-bitcoin-foundation/) » — прекратить предоставлять населению услуги по переводу платежей, иначе будет а-та-та. Лулз здесь в том, что Bitcoin Foundation — некомерческая организация, которая на общественных началах помогает решать вопросы легальности, выдаёт официальные комментарии от имени сообщества и делает прочие полезные вещи, и никакой коммерческой деятельности не ведёт. То есть это всё равно, что у клуба, где дальнобойщики собираются между рейсами выпить пива и попиздеть, потребовали бы лицензию на крупнотоннажные грузоперевозки. Короче, даже в сверхпродвинутой Силиконовой долине чиновники остаются чиновниками. Конечно, был выпущен официальный ответ-разъяснение (http://www.coindesk.com/bitcoin-foundation-issues-response-to-cease-and-desist-warning/) , и никого фактически не закрыли, но лулзов это письмо доставило. Сейчас использование любых виртуальных валют, в том числе биткоина, в Калифорнии абсолютно законно!

Драма Сноудена и NSA

Сама драма сливов Сноудена заслуживает отдельной статьи, а тут изложим только приложение тех сливов к Биткоину как системе. Срач и волну говна в биткоин-сообществе вызвала инфа о том, что NSA за закрытыми дверями давило на американские национальные организации, которые выдают сертификаты и выпускают отраслевые стандарты, в том числе и в области криптографии. И давили они с целью незаметно внести в стандартизируемые криптографические алгоритмы бэкдоры, или намеренные слабости, зная о которых, не сложно взломать вроде бы стойкую и рекомендованную к применению криптографию.

По итогам быстрого, навскидку, анализа алгоритмы, лежащие в основе биткоина — хэширование SHA256 и генерация публичных ключей с помощью эллиптических кривых — вроде бы не подвержены слабостям, внесённым NSA. Компрометация SHA256 в принципе не столь большая проблема, так как его потенциальный взлом, во-первых, легко решается переходом на другие варианты proof-of-work алгоритмов, а во-вторых, не открывает возможностей скрытной манипуляции.

А вот компрометация конкретных вариантов эллиптических кривых, положенных в основу механизма генерации публичных ключей, может привести к тому, что кто угодно с достаточными вычислительными мощностями сможет сгенерировать приватный ключ, имея в наличии публичный, а значит, незаметно и недоказуемо завладеть любыми чужими биткоинами. Это уже неприятнее, так как даёт новые возможности влияния, которых ранее у NSA не было. Но вроде бы в случае биткоина — пронесло, так как адрес кошелька хранит не публичный ключ, а его хеш, а публичный ключ адреса раскрывается при трате с этого кошелька. Помимо того, Сатоши, создавая систему, выбрал кривую, которая хоть и находится среди рекомендованных к применению (и потенциально скомпрометированных), но была придумана и широко известна задолго до выпуска скомпрометированных стандартов, а значит, вероятно, не подверглась воздействию NSA. А вот те, кто использовал другие кривые из рекомендованного набора (SSL, шифрование банковских систем etc) — вероятно, в жопе, потому как, зная, что уязвимости есть, и потратив сравнительно немного ресурсов на их поиск, не только NSA, а кто угодно сможет ими воспользоваться. Так что вся инфа в интернетах, включая «зашифрованные» соединения, должна считаться скомпрометированной по умолчанию. Как страшно жить!

Забыл о кошельке — стал миллионером

Удивительная история произошла с норвежским студентом Кристофером Кохом. В 2009 году он писал реферат на тему шифрования — и его внимание привлекла странная на тот момент криптовалюта Bitcoin. Для иллюстрации примера он купил 5000 биткоинов на 150 крон (примерно $26,60), чтобы реферат был подкреплен практическими действиями.

С тех пор Кристофер совершенно забыл о совершенной сделке. Он вспомнил о ней только в апреле 2013 года, когда ему на глаза случайно попалась заметка в СМИ о том, что курс биткоина достиг рекордного значения. И тут Кристофер вспомнил о старой покупке. Оказалось, что купленные тогда за бесценок монеты сейчас имеют рыночную ценность около 5 миллионов крон ($886 тыс.).

Кристофер в отчаянии провел целый день, вспоминая пароль от кошелька. Страшно подумать, что бы он с собой сделал, если бы так и не вспомнил его. К счастью, пароль все-таки подошел. Первым делом он потратил пятую часть денег на покупку роскошной квартиры в одном из самых богатых районов Осло — столицы Норвегии. По старом курсу 2009 года квартира обошлась ему примерно в пять долларов [1] (http://www.xakep.ru/post/61513/) .

Перековка транзакций

Драма с лулзами разыгралась где-то 7-го февраля 2014 г. ВНЕЗАПНО оказалось что не вся информация сохранённая в транзакции покрывается электронной подписью. Таким образом есть возможность изменить что-то в выпущенной транзакции. Конечно, такие кошерные вещи как адреса отправителя и адресата, а так же сумма перевода изменению не подлежат, но хэш всей транзакции всё же поменять можно. Проблема была известна давно, но мало кого волновала по тому что хэш транзакции использовался для удобства, в качестве номера перевода в некоторых обменниках.

Как это можно использовать. Коварный анон переводит BTC с кошелька обменника на свой личный, перехватывает транзакцию, меняет в ней что-нибудь не защищённое электронной подписью обменника и бешенно спамит этой транзакцией все пулы. Дальше есть шанс 50/50 что либо примут его транзакцию либо ту что вышла из обменника. При фейле можно повторить. BTC всё равно переведутся, а вот софту на обменнике попадает пыль в глаза и если этот софт следит за

каждым переводом по его хэшу, то он этого перевода не видит. Далее можно поднимать визг и требовать от админов обменника тут же, немедленно повторить перевод. Если они лохи — пошлют анону монетки хоть ещё 100 раз. Если нет — проверят счёт анона, увидят там подтверждённую транзакцию со своего счёта и пошлют его с банхаммером вдогонку. Если у него на кошельке в обменнике ещё что-то осталось, то заберут себе.

Как и во всех похожих драмах MtGox быстро занял лидирующую позицию. Софт на котором MtGox работает как раз следит за многим по хэшу транзакции. Так как на большинстве обменников все монетки лежат в общем кошельке, из него можно грести лопатой. На всякий случай MtGox заблокировал вывод монеток, подкрепив это дело объяснительной статьей (https://www.mtgox.com/press_release_20140210.html) . В результате поднялся шум и BTC навернулось с 930 енотов до 90. Нихрена не поняв в технических выкладках, хомячки обернулись леммингами и начали испуганно сбрасывать нахомяченные BTC. Решив, что негоже не воспользоваться ситуацией, владелец биржы распустил слухи, что в результате атаки украли всё, ~~две куртки кожаные, два магнитофона (импортных), два портсигара (серебряных)~~ все 750K биткоинов, а затем остановил работу биржи и обратился в суд по месту жительства с заявлением о начале процедуры защиты от банкротства, чтобы спокойно продать клиентскую базу новому владельцу, без юридических домогательств со стороны хомячков. Что примечательно, в суде он уже говорил о ~~трёх куртках кожаных~~ 850K украденных биткоинов.

Пикантность происходящему придал тот факт что за несколько часов до публичного заявления MtGox о баге и блокировке вывода Священная Яблочная Империя, следуя неисповедимым путям своим, убрала аппку кошелька blockchain.info. Это был единственный BTC-кошелёк поддерживаемый iБыдлодевайсами — и того не стало. Правда с учётом того что кошельки blockchain.info хранятся на сервере ими можно пользоваться и через браузер, а аппка была просто для удобства. Попкорн уже есть. Ждём статей из серии «ШОК! Хакеры взломали/убили/изнасиловали Bitcoin» и «СКАНДАЛ! Apple запретил Bitcoin!»

«Разоблачение» Сатоши Накамото

Кто такой Сатоши Накамото, один это человек или коллективный псевдоним — не знает никто. Эту тему неоднократно копали (http://old.computerra.ru/own/kiwi/640412/) разные журналисты, но более-менее однозначно указать человека, причастного к созданию биткоина, до недавнего времени не удавалось (http://habrahabr.ru/post/214903/) . В общем, Сатоши неплохо понимал, что и зачем он сделал, и судьба Прометея — быть прикованным к скале и кормить своей печенью прикреплённых орлов — его не прельщала, поэтому как только появилось жизнеспособное сообщество, которое могло развиваться без него — он исчез, правда, не с пустыми руками. Как самый первый майнер, он намайнил себе около полутора миллионов биткоинов (http://habrahabr.ru/post/177149/) , что по курсу на ноябрь 2013 составляло полтора **миллиарда** баксов.

Пиндостанский журнал Newsweek в лице журнализдки Лии Гудман поискал по реальным именам и нашёл нескольких людей, имевших или имеющих имя и фамилию Сатоши Накамото, не прибегая даже к стилометрии. Собрав о них информацию и пообщавшись с наиболее перспективным кандидатом по имени Дориан Накамото, они поняли, что это и есть настоящий Сатоши. Впрочем, ничто не мешает этой истории быть уткой, досадной ошибкой, подставой или приманкой для настоящего Сатоши, который сообщил, что Дориан — не он. Сам Дориан увлекается коллекционированием паровозиков, работает программистом и утверждает, что в первый раз услышал о Bitcoin у своего дома. Даже если Дориан и есть настоящий Накамото, прямых доказательств тому нет.

В дальнейшем объявился (http://www.bbc.com/news/technology-36168863) какой-то австралиец, заявивший, что Сатоши это он сам. Обещанных пруфов, правда, так в итоге и не предоставил.

Взлом MtGox и публикация улик

Некие хакеры, воспользовавшись уязвимостями в говнокоде гокса, взломали его. Был опубликован исходный код биржи, тут же обильно политый айтишниками говном. Чуть позднее были опубликованы данные, якобы свидетельствовавшие о том, что деньги с гокса никто не выводил, и они всё ещё на счетах биржи. Примечательно, что информация была опубликована в личном блоге директора биржи MagicTux (сначала в персональном, потом — на Reddit), от чего тот словил немало бугурта.

Пока не реализованные возможности

В протоколе биткоина есть ещё интересные вещи, которые возможны в принципе, но пока нигде не реализованы. Например:

- **multi-signature транзакции** — возможность создавать транзакции, в которых будет обязательна подпись более чем одним приватным ключом. То есть в простом случае — встроенная прямо в протокол двухфакторная авторизация, когда для отправки биткоинов надо, например, одновременно ввести пароль и авторизоваться на телефоне. Более сложный вариант — создание счетов с множественным владением, то есть когда деньги принадлежат сразу нескольким разным людям и только их общее согласие на перевод может этот перевод осуществить.
- **proof of existence (http://www.proofofexistence.com/)** — при отправке транзакции есть возможность встроить в блокчейн некоторое количество любых данных. Например, отправив транзакцию самому себе, можно встроить хэш определённого файла, и этот хэш будет надёжно сохранён в блокчейне, привязанный к определённому адресу и дате. Это фактически будет подтверждением факта существования этого файла в указанный момент времени, а также доступности файла владельцу кошелька с которого шла транзакция.
- **time limited deposit (https://en.bitcoin.it/wiki/Contracts#Example_1:_Providing_a_deposit)** — возможность создать транзакцию, которая будет видна всем заинтересованным, но при этом до определённого момента будет невозможно её потратить, то есть перевести деньги, переданные этой транзакцией, куда-то дальше. То есть деньги будут надёжно и безопасно заморожены внутри блокчейна, хорошо видны, но недоступны по желанию отдельным участникам процесса. Аварийный доступ к деньгам будет по прежнему возможен, но с согласия владельцев всех приватных ключей, которыми подписана транзакция.
- **умное имущество (https://en.bitcoin.it/wiki/Smart_Property)** — специфическое приложение блокчейна к RL. Если привязать к объекту RL (например, встроить внутрь машины) публичный ключ, а владельцу передать соответствующий приватный ключ, то будет возможно создать транзакцию, в которой с помощью некоторой криптографической магии публичный ключ машины будет передан новому владельцу, а в противоположную сторону будет переведена сумма биткоинов. То есть, проще говоря, акт купли-продажи, все стороны процесса, уникальный ID собственности и уплаченная сумма будут надёжно и независимо подтверждены блокчейном. И операция купли-продажи не будет требовать никаких доверенных посредников и оформления — обмануть или подделать блокчейн технически чрезвычайно сложно, а весь процесс купли-продажи можно автоматизировать, и всё, что будет нужно продавцу и покупателю, — встретиться со смартфонами у машины. От угонов и прочих способов присвоения чужого имущества, разумеется, не защищает.

И это ещё далеко не всё: возможностей и приложений технологий, лежащих в основе биткоина, к реальному миру — множество, и многие — подрывают существующие системы. Желающим просвещаться начинать тут (https://en.bitcoin.it/wiki/Contracts) (англ.).

Форки и что-то похожее

У биткоина развелось столько форков и говномодификаций, что даже Ubuntu нервно курит в сторонке. Каждая обезьяна с C++ считает своим долгом изобрести свой, намайнить в одиночку 100500 миллионов монет, затем вывести говнофорк на биржу и продать их все. Profit! На развитие монеты можно забивать. Хотя кроме наебалова подобного рода существуют и адекватные модификации:

- **Litecoin** — когда-то был наиболее успешным форком. По сравнению с биткоином, монет может быть до 84 миллионов, следовательно, эмиссия происходит в 4 раза быстрее. Лучше подходит для микроплатежей. Использует хеш-функцию Scrypt вместо SHA256. Scrypt задумывался как алгоритм, защищенный от майнинга на АСИКах, так как требует много быстрой памяти, но в конце 2014 года АСИКи под него таки появились.
- **Feathercoin** — один из форков лайткойна, известный тем, что он был таки взломан атакой 51%.

- **Novacoin** — в девичестве форк ppcoin, но активно развивается и уже давно ушел далеко, сочетает в себе scrypt алгоритм майнинга и новую технологию энергоэффективной добычи — Proof-Of-Stake, которая представляет из себя в прямом смысле утверждение — **деньги делают деньги**. PoS майнинг не требует траты вычислительных ресурсов, и каждая монета (входящая транзакция) в кошельке через месяц бездействия постоянно пытается сгенерировать блок. Вероятность этого события напрямую зависит от количества монет, того, как долго монета лежит и параметра PoS сложности (куда уж без нее). Благодаря PoS, форк получил защиту от атаки 51%, что породило очень много драмы для крупных держателей litecoin (и scrypt мощностей), привыкших кушать слабые форки на завтрак. Так же история с премайном (куча рисованных монет в первом блоке в награду разработчикам), который между прочим был публично уничтожен, добавляет масла в огонь и дает постоянный повод недовольным существованием novacoin снова и снова поднимать ор на форумах. Novacoin в результате негласно считается русской монетой, наверное из-за слабой поддержки англоязычных товарищей а так же активной деятельности ее ведущего русскоговорящего разработчика.
- **Namecoin** — распределённая доменная система, в которой нет единого центра, контролирующего делегирование доменных имён. В настоящее время уже никого не интересует, кроме трёх с половиной игроков на бирже, хотя сама идея когда-то многим казалась прорывной.
- **Zerocoin (ZCoin)** — анонимная криптовалюта, децентрализованный миксер транзакций в котором невозможно отследить историю транзакций.
- **DASH**. Пока разработчики Zerocoin слоупочили, несколько раз меняя направление разработки, не выпустив нормального релиза программы, другие ребята выпустили форк под названием Darkcoin, использующий встроенный в клиент миксер и наработки Zerocoin. В 2014 году они даже успели его переименовать в DASH (не путать с говнофорком Dashcoin). В отличие от Zerocoin, DASH работоспособен и вполне пригоден к использованию.
- **Monero** — этакий профиченный DASH. Использует более суровый миксер чем в DASH, но менее суровый чем в Zerocoin.
- **Ethereum** — криптовалюта, имеющая скриптовый движок, позволяющий делать разные вещи с деньгами без использования сторонних сайтов или программ. Создана канадоэмигрантом второго поколения по имени Виталик Бутерин, собравшим деньги на её создание с помощью краудфандинга. Форк получился юзабельным, но драмы и расколы в коллективе разработчиков повлияли на его популярность не лучшим образом.
- **BitMessage** — защищенная система обмена сообщениями, использующая некоторые идеи Bitcoin. Не является платежной системой, но как система шифрованной и неотслеживаемой почты/чатов очень даже ничего.

На начало 2016-го Litecoin уже не самый успешный форк. В хитпараде криптовалют его уже обошли несколько других. Биткоин пока что остается рулить на первом месте, но надолго ли? Многие аналитики склоняются, что сам биткоин, в существующем на данный момент виде, долго не протянет. Появляются криптовалюты 2-го поколения.