**Bitcoin**

Криптовалюта — вид цифровой валюты, эмиссия и учёт которой основаны на криптографических методах, а функционирование системы происходит децентрализовано в распределённой компьютерной сети. Из-за децентрализации криптовалют по умолчанию не предусмотрен принудительный возврат платежей.

Как правило, имеется верхний предел общего объёма эмиссии (у Bitcoin это 21 млн электронных монет, но об этом позже).

Однако у некоторых криптовалют отсутствует фиксированный верхний предел общего объёма эмиссии и возможна как эмиссия за счёт имеющихся накоплений, так и демиссия путем обязательного уничтожения небольшой фиксированной суммы в каждой транзакции.

Существующие на данный момент криптовалюты используются псевдонимно — все транзакции публичны, но привязки к конкретному человеку по умолчанию нет, однако личность пользователя может быть установлена, если известна необходимая дополнительная информация.

Криптовалюта не является долговым обязательством, как электронные кошельки, а сама является эквивалентом стоимости. Стоимость криптовалюты определяется спросом и предложением на рынке.

Сейчас в мире насчитывается более 274 криптовалют, но я хочу рассмотреть самую известную, с которой началось их тотальное распространение и которая вызвала такой массовый интерес к криптовалютам, тем более что большинство из них используются только для спекуляций на их курсах и больше нигде.

Биткоину уже более 5 лет, но широкое внимание общественности он привлек только в прошлом году, когда курс очень резко пошел вверх и увеличился более чем в 10 раз. За месяц валюта выросла в цене с $200 до $1050 за 1 биткоин. Это при том, что на начало 2013 года валюта стоила всего около $13. Итого за год получился прирост стоимости bitcoin почти в 100 раз!

Резкие падения курса были связаны со взломом крупнейшей биржи и запретом Китая.

Виртуальная валюта Bitсoin – по сути, это публично доступный регистр, который называется Blockchain. Blockchain хранит постоянно растущее количество транзакций и адреса кошельков пользователей, связанных с ними.

Это первая децентрализованная P2P платежная сеть, которая обслуживается ее же пользователями, без центральных органов управления или посредников. Одноранговая, децентрализованная или пиринговая (от англ. peer-to-peer, P2P — равный к равному) сеть — это оверлейная компьютерная сеть, основанная на равноправии участников. В такой сети отсутствуют выделенные серверы, а каждый узел (peer) является как клиентом, так и сервером. В отличие от архитектуры клиент-сервера, такая организация позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов. Участниками сети являются пиры. Таким образом, Bitcoin в равной степени контролируется всеми пользователями системы.

Личность изобретателя Bitcoin – это тайна. Ходят слухи, что это Сатоши Накамото, но сам он эту информацию опровергает.

Протокол Bitcoin и программное обеспечение имеют открытые исходники, опубликованные под лицензией MIT.

Почему они чего-то стоят? Биткоины имеют стоимость, потому что они полезны как форма денег. Имеют характеристики денег, основанные на математике (долговечность, портативность, взаимозаменяемость, дефицит, делимость и узнаваемость), а не полагаются на физическую собственность (таких как золото и т.д.) или на доверие центральному авторитету.

Bitcoin опирается на математику, но как и со всеми другими валютами, ценность биткоинов определяется только и напрямую от людей, желающих принять их как средство платежа.

* Децентрализованность (сами решаем как распоряжаться и где хранить)
* Ограниченность эмиссии (Последний блок, который создаст монеты, будет блок № 6 929 999. Он будет создан примерно в 2140 году. 20 999 999.9769 BTC)
* Анонимность (Что бы совершить платеж, нужен только адрес получателя. Среднее время синхронизации платежа не превышает 10 минут, а чаще не более 3-5 минут. Главное помнить, так как система Bitcoin децентрализована, отменить платеж не получиться и пожаловаться в случае чего будет некому)
* Отсутствие контролирующих органов

*Каждый кошелек — это случайно сгенерированная пара ключей. Адрес кошелька — это хэш от публичного ключа. Так его можно однозначно идентифицировать.*

*Транзакция - это запись о том, с какого кошелька на какой какая сумма переводятся. А так же, время и дата операции. Эта запись (её хэш) подписывается закрытым ключом отправителя и рассылается всем в округе в ожидании подтверждения.*

*Чтобы о транзакции узнали и все себе её записали, необходимо её подтверждение, которое получается в результате создания нового блока. Блок - это служебные данные + список транзакций + номер кошелька майнящего +* ***волшебное число****.*

*Цепочка блоков – это последовательность, в которой каждый следующий блок включает в себя Id предыдущего.*

*Новый блок создается в среднем каждые 10 минут. Через каждые 100 блоков, в зависимости от времени создания блоков, рассчитывается новая сложность для приближения к созданию блока за 10 минут.*

Сложность растёт так как всё больше усилий затрачивается на майнинг — всё больше и больше мощностей включаются в игру. Первоначально для майнинга хватало простого домашнего компьютера, затем «цифровые шахтеры» перешли к расчету на топовых игровых видеокартах, а потом и вовсе к специализированным устройствам для майнинга. Сначала это были просто перепрограммированные чипы, а затем в использование вошли ASIC, интегральные схемы специального назначения, отличающиеся высокой скорость расчёта хэшей и низким энергопотреблением.

Поскольку майнеров теперь очень много, чтобы не остаться ни с чем, люди объединяются в пулы. Пул — это множество клиентов, каждый из которых подбирает блоки. Но как только блок будет найден, «призовые» биткоины делятся на всех, кто участвовал в его подборе.

В Гонконге есть фабрика с жидкостным охлаждением, мощность которой составила 4% от всей мощности в сети — 35 терахэшей в секунду. Она производит около 26 биткоинов в сутки.

Также существуют трояны трояна, которые превращают компьютеры пользователей в биткоин-фермы без их ведома.

Интересное: В мае 2010 года один майнер предложил заказать ему пиццу, за что предложил заплатить 10 000 BTC. Примерно через год стоимость одного BTC подскочила до 32 $, то есть стоимость пиццы составила 320 000 $, а в пересчете по сегодняшнему курсу – он заплатил за пиццу почти четыре с половиной миллиона долларов.

Bitcoin других странах:

Министерство финансов Германии признало виртуальную валюту биткоин «расчетной единицей», то есть теперь она является законным платежным средством и ее можно использовать для уплаты налогов и торговли в этой стране.

В декабре 2013 года швейцарским парламентом был предложен постулат, согласно которому bitcoin следует рассматривать как иностранную валют.

Британии: биткоины приравнены к ваучерам.

Сингапур и Норвегия признали биткоин и определили налоговую политику его оборота.

В Америке активно используются, например, в Лас-Вегасе.

Лично меня в этой валюте особенно радует, хотя бы небольшая часть мировых финансов перешла в руки хакеров и инженеров-программистов, которые используют эти деньги так, как их никогда не потратит миллиардер с Уолл-Стрит.

Носит ли Предупреждения Банка России нормативный характер? – Нет  
Соответствуют ли факты в предупреждении действительности? – Да  
Запрещен ли биткоин или операции с ним на территории России? – Нет  
Изменилось ли правовое поле в области виртуальных валют в России? – Нет

Однако именно высокая волатильность bitcoin и привлекает многих инвесторов!

Пицца https://bitcointalk.org/index.php?topic=137.0

Часть денег перешла к хакерам и гикам. http://habrahabr.ru/post/209660/

Всем из MIT по 100$ (500 000) habrahabr.ru/post/221395/

Законодательство против <http://habrahabr.ru/post/220447/>

Первый абзац http://habrahabr.ru/post/214587/

<http://coinmarketcap.com>

http://btcsec.com/cbr\_about\_bitcoin/