**FAQ по Биткоину**

**Короткая версия**

1. *Следует ли мне покупать Биткоины?*

Нет.

1. *Но я постоянно вижу все, что пишут про них в новостях и…*

Нет. Вся технологическая журналистика одинаково ужасна, всегда помните об этом.

1. *Как оно вообще работает? Я не понимаю!*

Оно и не работает, правда. Невозможно в точности объяснить, что такое Биткоин не скатываясь при этом в затуманивающие ум технические термины, так что вам, наверное, лучше не думать об этом. Займитесь лучше чем-нибудь полезным.

**Предисловие**

**В теории:** Полностью децентрализованная версия электронных денег позволит делать онлайн-переводы напрямую от одной стороны к другой, минуя финансовые учреждения.

- Сатоши Накамото, *Bitcoin: A Peer-to-Peer Electronic Cash System, 2008[1]*

Создана новая экспериментальная форма Интернет-денег, которые любой человек может создавать у себя дома. Люди собирают устрашающие компьютеры набитые видеокартами, заключая самих себя в тепловую ловушку, эти компьютеры нагреваются настолько, что один человек был госпитализирован с инфарктом и повреждением головного мозга.

Некто известный как «Pirateat40» создаёт «высокодоходную инвестиционную программу». Незадолго до того как она схлопнется по схеме Понци, в неё будет вложно 7% от всего Биткоина на тот момент. Пострадавшие инвесторы в итоге смогут убедить власти не только в том, что эти Интернет-жетоны чего-то стоят, но и в том что они дали их какому-то парню в Интернете потому что он обещал увеличить их состояние вдвое.

Молодой студент-физик создаёт революционную торговую площадку основанную на принципе неагрессии, неподверженную принуждению от государства. В конце концов, он начнёт заказывать убийства людей, потому что они могут угрожать его великому эксперименту, теперь он отбывает пожизненный срок без права на условно-досрочное освобождение.

Специалист по юридической криптографии предлагает полностью автоматизированную систему контрактов, которая работает с минимальным вмешательством человека, чтобы бизнес и закон работали лучше и пользовались большим доверием. Контракты которые создают люди устроены по принципу схемы Понци, позже они превратятся в нерегулируемые копеечные ценные бумаги под печатью которых сказано, что бумаги, которые вы покупаете – не имеют никакой ценности.

Самая большая краудфандинговая компания в истории привлекает 150 миллионов долларов инвестиций, создатели обещают, что у проекта будет *«железобетонно надёжный код*». На релизе его немедленно взламывают и крадут 50 миллионов долларов.

Доброе имя Биткоина было несколько запятнано наркотиками и криминалом, поэтому его сторонники пытаются продать технологию бизнесу как «Блокчейн». Полтора миллиарда венчурного капитала возвращают себе, пока что, ноль. Единственный видимый продукт это часы консультаций и пресс-релизы.

И как всё к этому пришло?

Цифровые деньги без посредника в лице центрального органа это, очевидно, полезная идея. На практике она превратилась в магнит для полных энтузиазма дилетантов с горящими глазами и мошенников, которые на них наживаются, последствия этого одинаково смешны и ужасны.

Биткоин и блокчейн это не история про технологию, а история про психологию: мышление экономическими пузырями и искусство воровства.

Несмотря на благие намерения создателей, сфера криптовалюты пресыщена мошенничеством и мошенниками. Технология используется как оправдание для того чтобы делать самые странные, почти что волшебные заявления. Когда начинают использоваться фразы вроде «абсолютно новая форма денег» или «старые правила больше не работают», люди становятся доверчивыми, а люди с недостатками этического характера включаются в творчество.

Вы можете зарабатывать деньги на Биткоине! Но *гораздо более вероятно,* что вы будете тем на ком *другие* заработают деньги.

Запомните, если что-то звучит слишком хорошо чтобы быть правдой, значит, наверняка так оно и есть.

В этой книге я рассказываю об истоках и истории Биткоина до сегодняшнего дня (*книга в вышла в 2017-ом году. Прим. переводчика*), рассказываю некоторые наиболее примечательные истории, рассказываю о других криптовалютах которые породил Биткоин – в особенности Etherium и смарт-контракты и попытки применить блокчейн в бизнесе. Будет так же изучение случая использования блокчейна в музыкальной индустрии.

Я вдаюсь в технические детали там, где это уместно, хотя более важным является общая суть явления. В цифровой версии книги есть много сносок со ссылками на источники для дальнейшего чтения и глоссарий.

**Глава 1: Что такое Биткоин?**

**Почему Биткоин?**

Бумажные знаки и металлические монеты неудобные и раздражающие, а ещё у нас теперь есть Интернет. Так что цифровые деньги – полезная идея.

Единственное решение, к которому, в основном, пришёл развитый мир это просто использовать банки – у вас есть счёт, и вы можете пересылать деньги на счета других людей при помощи дебетовой карты, PayPal или чего-то ещё. Наличие центрального органа означает, что процесс разумно отрегулирован, ошибки и воровство могут быть предотвращены и так далее. Кроме того это довольно мягкий переход от бумажных денег – то же самое, но теперь можно делать с деньгами новые вещи.

Но это не идеальное решение; кард-ридер в магазине может не работать, ваш платёжный шлюз может взимать комиссию, вы можете захотеть послать кому то деньги в банк отличный от вашего, вы цените вашу приватность, каждый раз делать всё через банк раздражает. Так что иметь цифровые деньги было бы неплохо.

Биткоин – это *криптовалюта*: вещь в Интернете, которая позволяет вам обмениться уникальными цифровыми объектами. Для того чтобы сымитировать эти объекты потребуется целая вечность, так что если мы назначим этим объектам ценность, мы можем обмениваться ими примерно так же как мы обмениваемся деньгами. Система децентрализована, так что вы можете отправлять деньги, минуя центральную расчётную палату.

В качестве бухгалтерской книги у Биткоина – *блокчейн*, который рекламируется как *невзламываемый*: никто не может изменить его содержимое, таком образом, чтобы этого никто не заметил. Идея в том, что нет управления из центра, кто угодно может создать счёт Биткоин и стать частью сети, никто не сможет заблокировать или отменить ваши транзакции, и никто не является хозяином сети.

**Что вы имеете, когда у вас есть «биткоин»**

Вы знаете, что для вас «деньги». Вы можете зарабатывать их, можете тратить на что угодно, можете копить их на будущее, можете инвестировать их. Они могут быть на банковском счету с карточкой, или в бумажных знаках и монетах в вашем кармане – всё это одинаково ощущается вами как фунт или доллар.

На практике, биткоины почти как деньги в банковском счету с дебетовой картой, только без какой-либо гарантии – всё это не регулируется, не страхуется, нет никакого способа отменить транзакцию, нет технической поддержки для клиентов.

Если у вас «есть» биткоины, у вас их нет как каких-то вещей хранящихся в вашем компьютере. То, что у вас есть это *адрес* Биткоина (как номер банковского счёта) и *ключ* к этому адресу (другой номер, который работает как PIN-код к первому номеру) [2]. Адрес Биткоина упоминается в транзакциях, хранящихся в блокчейне; ключ – уникален и делает ваши биткоины вашими.

Для того чтобы отправить биткоины с вашего адреса на другой (примерно как отправка денег через PayPal), вы генерируете транзакцию которая посылается в сеть и добавляется к следующему блоку транзакций. Как только она попадает в блок, эта транзакция становится навсегда публично видимой для всех в блокчейне.

*Кошелек* это то место, где вы храните свои ключи. Обычно это программа, которая генерирует и управляет адресами и показывает вам баланс. Вы можете сгенерировать новый адрес и соответствующий ему ключ в любое время.

Вы можете хранить свои биткоины на *горячем кошельке* (как на счету в банке), который работает на вашем компьютере с Интернетом, или на *холодном кошельке* (как хранить деньги в носке под кроватью), который может быть на компьютере без Интернета, или это могут быть ключи записанные на USB-флешку или напечатанные на бумаге.

Если вы потеряете ключ, ваши биткоины пропадут навсегда. Если кому-то достанется ваш ключ, он сможет забрать ваши биткоины. Если вы отправите биткоины на несуществующий адрес, они пропадут навсегда. Если вы отправите биткоины не на тот адрес, вы не сможете их вернуть. Безопасноть в Биткоине может быть очень технической, сложной и не прощающей ошибок; большинство людей держат свои биткоины на биржах. Но и у них есть свои проблемы, как мы увидим позже.

**Блокчейн**

Транзакции биткоина сгруппированы в блоки. У каждого блока есть криптографический *хэш,* это номер который быстро высчитывается и служит значением для проверки – примерно как последние цифры ISBN-номера у книги, или последние цифры у вашей кредитной карты, только длиннее – это нужно для того чтобы подтвердить что кусочек данных является самим собой.

Хэш будет совершенно другим даже если есть минимальные изменения в данных; поэтому две вещи с одинаковым хэшом принято считать идентичными.

Сторонники Биткоины любят говорить что он «защищён математикой». Всё это потому что криптография работает на арифметике которая быстро просчитывается «вперёд», и невозможно долго «назад» - для того чтобы создать кусочек данных с идентичным хэшем потребуется перебрать огромнейшее количество вариантов (майнинг Биткоина построен на этом, смотрите ниже).

В каждый блок кроме того захэширована цепочка предыдущих блоков, если кто-то попытается взломать цепь – это будет очевидно. Этот принцип называется *дерево Меркеля*, придуманное в 1979-ом году и широко используемое с тех пор. Биткоин делает возможным невзламываемую публичную бухгалтерскую книгу с транзакциями, без какого-либо центрального органа который бы сообщал чья книга официальная.

Блокчейн Биткоина хранит все подтверждённые транзакции начиная с Января 2009-ого года. В Июне 2017-ого его объем составляет 120 Гигабайт и увеличивается на 4 Гигабайта каждый месяц.

**Защита растратой: Proof of Work**

[1]

Satoshi Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System”. Bitcoin.org, 31 October 2008.

[2]

This is public key cryptography, where the address is the “public key” (that everyone knows) and the key is the “private key” (that only you know), which are a matched pair: a message encrypted with one key can be decrypted with the other.