Компания Prypto
Биткойн для чайников

Об авторе

Компания Prypto была основана в 2013 году с целью внедрения в жизнь новых простых и эффективных решений, связанных с биткойном; при этом первым ее продуктом стала Crypto Scratch Card (скретч-карточка криптовалюты). Она позволяла своим владельцам получить первый опыт использования криптовалют, просто взяв ее в руки. Этот продукт компании получил широкое распространение по всему миру и позволил множеству людей легко и просто познакомиться с биткойном.

Подобно тому как цель этой книги – развеять мифы и заблуждения в отношении биткойна и технологии блокчейна, положенной в его основу, цель компании Prypto – упростить доступ к технологии блокчейна для бизнеса любого уровня, от крупною до самого мелкого, посредством предоставления программных решений, выполненных на заказ, в том числе индивидуальных. Компания намерена выпускать различные продукты, которые смогут наглядно продемонстрировать огромный потенциал блокчейна, причем именно таким образом, который будет понятен представителям бизнеса и позволит им сделать первые шаги в направлении интеграции этой новой технологии в их деятельность и открытии для себя невероятных горизонтов ее применения на практике.

Компания Prypto гордится тем, что является коллективным автором книги Биткойн для чайников, и абсолютно уверена в том, что чем больше будет использовано способов расширить в людях понимание того, чем являются биткойн и связанная с ним технология, тем лучше будет для всех. Мы твердо убеждены в потенциальном благе, которое принесет в мир дальнейшее развитие экосистемы биткойна и блокчейна, и надеемся, что вы сможете разделить наши убеждения, когда ближе познакомитесь с этой книгой.

Благодарности автора

Мы благодарим команду издательства Wiley за их предложение, а также постоянную помощь и поддержку на протяжении всего процесса подготовки этой книги, особенно Стейси Кеннеди (Stacy Kennedy) и Корбина Коллинза (Corbin Collins).

От издательства

Издательство “Диалектика” выражает признательность А. Ю. Барабашу, г. Москва, за выполнение перевода данной книги с английского языка на русский, а также Виталию Безродных – за редактирование и рекомендации по ее оформлению.

Введение

Мы рады приветствовать вас как нового читателя книги Биткойн для чайников! Полагаем, у вас немало к нам вопросов. Что же такое этот самый биткойн? Как вообще может существовать цифровая валюта? Возможно, это какие-то интернет-деньги? Это нечто, о приобретении чего следует побеспокоиться, или, наоборот, лучше держаться от него подальше? В различных массмедиа освещение темы биткойна, как правило, весьма отрывочно и довольно тенденциозно. Возможно, вы читали статьи о людях, потерявших свои деньги, или видели телепередачи о том, как биткойн используют для незаконных покупок на черном рынке? А может, вы слышали удивительные истории о невероятном успехе людей и предприятий, достигших процветания на основе

его использования?

Дорогие читатели, у вас нет повода для страхов. Эта книга сотрет с биткойна всю подоплеку загадочности и непонимания, предоставив вам необходимые факты и только факты. В ней терпеливо объясняется, что такое биткойн на самом деле, обсуждаются некоторые из невероятных возможностей той подрывной и в то же время вдохновляющей технологии, которая положена в его основу, а также поясняются те немалые потенциальные выгоды, которые он может дать всем нам. Биткойн может изменить нашу жизнь в той же степени, в какой это произошло с появлением и повсеместным распространением Интернета в последние десятилетия.

Короче говоря, в этой книге вы найдете все, что вам необходимо знать и понимать, чтобы начать использовать биткойн в собственных целях. Так чего же вы ждете? Итак, начнем!

Об этой книге

Назначение этой книги – дать вам начальную информацию об истории этой увлекательной технологии и обсудить биткойн как концепт и как продукт. Вы узнаете, как создать кошелек так, чтобы в дальнейшем в нем можно было безопасно хранить свои биткойны. Также мы расскажем вам, как и где можно получить эти цифровые монеты, и наглядно продемонстрируем, как в дальнейшем их можно будет использовать, в том числе для накопления капитала. Будут затронуты и нормативно-правовые рамки – в том виде, который они имели на момент написания этой книги. Мы подробно расскажем о процессе майнинга биткойнов и объясним, как вы сможете принять в нем участие, а заодно – почему это, возможно, не стоит делать.

Мы также приоткроем завесу таинственности над этой технологией и внимательно рассмотрим то, что предстанет вашему взгляду. Вы узнаете во всех деталях, как в сети биткойна выполняются транзакции и что именно скрывается под названием “блокчейн”. А еще мы бросим пристальный взгляд в хрустальный шар и поразмышляем над тем, как биткойн и лежащая в его основе технология блокчейна будут развиваться в будущем и как это может повлиять на различные аспекты нашей жизни. В завершение будут представлены полезные онлайн-ресурсы, которые позволят вам всегда быть в курсе событий, а также помогут принять активное участие в жизни онлайн-сообщества, активно поддерживающего биткойн. Присоединяйтесь к нам. Мы думаем, что для вас это станет захватывающим приключением!

Предположения авторов

При написании этой книги мы сделали одно важное предположение о вас, читатель. Мы полагаем, что вы заинтересованы в изучении важнейших основ этой новой формы валюты. Мы надеемся, что вам понравится то, что вы здесь прочитаете, и вы захотите создать собственный кошелек и начать использовать биткойн, а также расскажете об этом новом увлечении всем своим друзьям и коллегам. Но главное наше предположение состоит в том, что вы взяли эту книгу в руки, прежде всего, потому, что хотите больше узнать о биткойне, перед тем как решиться прыгнуть на борт этой технологии и отправиться с ней в дальнее плавание.

Мы также предполагаем, что у вас есть необходимый опыт работы с компьютерами и Интернетом. Мы полагаем, что вы уже знаете, как найти в Интернете то, что вам нужно, и какие элементарные шаги следует предпринять, чтобы защитить в Сети себя и свои деньги. Однако мы вовсе не ожидаем, что вы являетесь техническим экспертом, который знает все, что только можно знать о компьютерах, потому что вам не нужно быть подобным экспертом, чтобы начать работать с биткойном.

Условные обозначения, принятые в этой книге

Ниже поясняются условные обозначения, принятые в этой книге для повышения эффективности ее использования.

В книге используются определенные соглашения, направленные на облегчение восприятия материала.

• Адреса веб-сайтов или названия файлов представлены с помощью вот такого шрифта.

• Названия элементов управления, представленных на экране компьютера в текстовом виде, выделяются в книге специальным рубленым шрифтом.

Пиктограммы, используемые в этой книге

В тех случаях, когда необходимо было подчеркнуть что-нибудь очень важное или особенное, на страницах слева мы помещали приведенные ниже пиктограммы.

Эта пиктограмма сопутствует полезным советам в отношении того или иного обсуждаемою аспекта биткойна или технологии блокчейна. Отмеченные ею абзацы часто включают предоставленные компетентными лицами сведения, которые помогут вам достичь желаемого настолько быстро и эффективно, насколько это возможно.

Такой пиктограммой помечается информация, которую следует запомнить. Не пропустите подобные сведения или хотя бы загните уголок соответствующей страницы, чтобы быстро к ней вернуться позднее.

С помощью этой пиктограммы отмечаются предупреждения о типичных ошибках и разных опасностях, с которыми можно столкнуться на пути освоения биткойна. Мы не сомневаемся, что вы всегда будете руководствоваться здравым смыслом во всем, что касается ваших денег и особенно – интернет-транзакций. Но время от времени мы все же считаем полезным положить руку вам на плечо и предупредить: “Осторожно! Обратите внимание вот на это!”

В онлайн-финансах, в Интернете и в биткойне есть множество странных и весьма специфических способов описания или выполнения тех или иных вещей, углубленное освоение которых может показаться неискушенному читателю излишне затруднительным. Данной пиктограммой помечается более углубленная техническая информация, которую в принципе можно пропустить без особого вреда для понимая последующего материала. Однако интересующимся она поможет лучше понять те или иные особенности предлагаемых методов или инструментов.

Как пользоваться этой книгой

Как и в случае других книг серии …для чайников, вы можете начать чтение этой книги с любой главы и с любого интересующего вас места. Каждая ее глава строилась как нечто самодостаточное, насколько это было возможно. Как часто говорят, мы вовсе не хотели повторять самих себя слишком часто, поэтому в тексте книги вы найдете множество ссылок на другие главы, в которых обсуждаемая информация или понятие представлено более подробно.

Если вы не знаете, с чего начать, и при этом вам не очень хочется следовать стандартному правилу “начни сначала”, мы можем дать вам несколько следующих рекомендаций.

- Глава 9 – отличное место, с которого можно начать чтение этой книги. Здесь вы узнаете, разрешено ли законом использование биткойнов в вашей стране, прежде чем решить всерьез углубиться в изучение самого биткойна.
- Если вы намерены сразу начать работу с новой технологией и готовы создать собственный кошелек, который позволит вам приобретать и тратить биткойны, начните с главы 5.
- Глава 10 – также отличное место для читателей начального уровня. Здесь речь идет о защите сети биткойна, дается относительная оценка безопасности его использования и предлагаются необходимые меры предосторожности, которые обязательно следует принять во внимание.
- Из главы 12 вы почерпнете необходимое вдохновение – в ней рассказывается о том, что можно делать с биткойнами, когда они у вас появятся. В двух словах, все очень просто: тратить, тратить и тратить!

И все же следует сказать, что наилучшим местом для начала чтения этой книги будет… ее начало. Однако, с чего бы вы ни начали, мы надеемся, что эта книга вам понравится и вы сможете почерпнуть из нее что-то ценное.

От издательства “Диалектика”

Вы, читатель этой книги, и есть главный ее критик. Мы ценим ваше мнение и хотим знать, что было сделано нами правильно, что можно было сделать лучше и что еще вы хотели бы увидеть изданным нами. Нам интересны любые ваши замечания в наш адрес.

Мы ждем ваших комментариев и надеемся на них. Вы можете прислать нам бумажное или электронное письмо либо просто посетить наш веб-сервер и оставить свои замечания там. Одним словом, любым удобным для вас способом дайте нам знать, нравится ли вам эта книга, а также выскажите свое мнение о том, как сделать наши книги более интересными для вас.

Отправляя письмо или сообщение, не забудьте указать название книги и ее авторов, а также свой обратный адрес. Мы внимательно ознакомимся с вашим мнением и обязательно учтем его при отборе и подготовке к изданию новых книг.

Наши электронные адреса:
E-mail: info@dialektika.com
WWW: http://www.dialektika.com

Наши почтовые адреса:
в России: 195027, Санкт-Петербург, Магнитогорская ул., д. 30, ящик 116
в Украине: 03150, Киев, а/я 152

Часть I. Основы технологии Биткойн

В этой части…

- Знакомимся с основами технологии: что такое биткойн, как он стал тем, чем он является теперь, и как все это работает
- Выясняем, как заполучить собственные биткойны, где их после этого можно держать и где их лучше не держать
- Оцениваем преимущества и недостатки биткойна как валюты и как технологической системы
- Осваиваем функции майнинга, покупки, продажи и зарабатывания биткойнов

Глава 1. Знакомство с биткойном

В этой главе…

- Знакомимся с биткойном поближе
- Выясняем, чем биткойн мог бы быть нам полезен
- Усваиваем правила безопасности и хранения своих денег

Итак, биткойн… новая форма денег, цифровых денег (если быть точнее)… Но как же это работает?

Усаживайтесь поудобнее: мы начнем с основ, а именно – с трех главных аспектов, характеризующих биткойн.

- Происхождение: как появился биткойн.
- Технология: как это работает.
- Валюта: использование биткойнов в качестве денег.

Исследование каждого из этих аспектов поможет вам лучше понять биткойн (или BTC, как его иногда называют) и оценить, может ли он в принципе быть вам полезен и как именно. Не волнуйтесь, пока что мы не будем углубляться в детали. К деталям мы перейдем в следующих главах. Готовы? Поехали!

Происхождение биткойна

Пожалуй, главная составляющая Биткойна – это концепция, которая лежит в основе его технологии. Биткойн создал разработчик Сатоши Накамото. Сатоши не ставил перед собой цель изменить процесс совершения покупок в Интернете, он просто видел ряд принципиальных проблем с существующими средствами платежа и был намерен их решить.

Предпосылки создания биткойна довольно легко выявить: после финансового кризиса 2008 года люди по всему миру ощутили на себе его деструктивную силу. И на время написания этой книги (начало 2016) многие до сих пор ощущают его последствия в виде колеблющихся курсов национальных валют (так называемых фиатных валют, ценность которых поддерживается лишь решениями правительств). Когда мировая финансовая система оказалась на грани краха, многие центробанки прибегли к методу валютных вливаний иными словами, вовсю включили печатные станки. Центробанки залили кризис деньгами и в этом процессе обрушили процентные ставки почти до нуля, чтобы предотвратить повторение Великой Депрессии 1930 года. Эффект от этой меры был значительным – серьезные колебания валютных курсов и тот феномен, который впоследствии получил название валютные войны – гонка по обесцениванию собственных национальных денег с тем, чтобы экономика страны стала более конкурентоспособной (за счет снижения себестоимости экспортируемых товаров и услуг). Реакция центробанков по всему миру была в точности такой, какой она обычно бывает в подобных случаях: для спасения “утопающих” банков правительственные структуры печатают необеспеченную валюту, что еще больше обесценивает существующий денежный объем.

Спасение банков происходит за счет всего общества и трансформируется в дополнительные налоги и бремя госдолга. Этот шаг в определенном смысле лишь усиливает социальное неравенство. Кроме того, никто еще пока не знает, какие отсроченные последствия влечет за собой подобное валютное стимулирование. Возможно, со временем это повлечет за собой прогрессирующую инфляцию и последующее обесценивание фиатных валют в странах, правительства которых используют подобную схему? Получается, что некоторые центробанки, часто действуя независимо от правительства, завели не одну экономическую систему в тупик и были готовы обесценивать валюту, лишь бы только их внутренние механизмы продолжали работать исправно. В ходе операции “спасения”, те банкиры и финучреждения, безрассудные действия которых повлекли за собой наступление кризиса, получили поддержку и избежали последствий своей безответственности. Единственная реальная альтернатива в таких случаях – позволить всей финансовой системе рухнуть и самоочиститься, как это случилось, например, в Исландии. Эта страна просрочила выплаты по внешним долгам, после чего вошла в фазу экономического коллапса как следствия этого события.

Именно на фоне этих драматических событий возник биткойн – децентрализованная альтернативная финансовая система, которая неподконтрольна су-шествующим элитам.

Сатоши Накамото решил, что настало время для новой монетарной модели, не зависящей от существующей финансовой инфраструктуры (вполне справедливо было бы назвать это великим открытием). Независимо от того, рассчитывал ли он на то, что биткойн вытеснит все прочие финансовые структуры, нам известно, что сейчас многие банки уже всерьез заинтересовались технологией, которая лежит в основе биткойна, потому что они видят ее потенциал и хотят использовать ее преимущества для собственной выгоды. Они могут применять технологию по своему усмотрению, потому что основа биткойна – блокчейн (подробнее об этом – в главе 7) – источник с открытым кодом, и все могут ее свободно использовать. Открытый код Биткойна означает, что каждый может предложить свои улучшения или создать свою надстройку на его основе.

Если посмотреть на биткойн под таким углом, напрашивается вывод, что при создании биткойна автор руководствовался идеологическими причинами. Это нечто существенно большее, чем новый платежный метод с

виртуальными монетами. Речь идет о лежащей в основе технологии и постепенном раскрытии ее полного потенциала. Как вы решите использовать эту технологию – дело ваше. Ее можно адаптировать практически для любой финансовой операции, которая только может прийти вам в голову. Все, что для этого нужно, готовность к экспериментам. Даже если вы не сразу уловите суть, просто дайте шанс новому!

Давайте признаем: пересечение финансов и технологий не может быть бесшовным и гладким. Все мы пострадали от финансовых кризисов XXI века, и многие страны до сих пор борются с последствиями этих финансовых фиаско. Разработчику биткойна Сатоши Накамото не очень-то нравились топорные действия центробанков в кризисной ситуации, и он долго и напряженно обдумывал проблему перед тем, как предложить вариант ее решения. Большая часть традиционной финансовой инфраструктуры далеко не идеальна, и более устойчивая альтернатива крайне необходима. Станет ли биткойн такой альтернативой – это мы еще увидим.

Когда Сатоши Накамото придумал биткойн, ключевым его отличием стала особенность, которой суждено будет сыграть главную роль, – его полная децентрализованность. Децентрализация на практике означает то, что все мы являемся частью экосистемы биткойна и вносим свой вклад в ее развитие различными способами. Биткойн полагается не на правительство, банки или посредников, а принадлежит всем его пользователям в рамках пиринговой сети, в которой мы все вместе образуем сеть поддержки Биткойна. Без участия индивидуальных пользователей не будет и самого Биткойна. Чем больше людей включает в себя его сеть, тем лучше работает вся система. Постоянно растущее сообщество пользователей, активно использующих биткойн как платежный метод, расплачивающихся биткойнами за товары и услуги и предлагающих товары и услуги на продаж} за биткойны, является важнейшим фактором его успеха.

Следуя духу свободного рынка, парящему в мире криптовалют, любой пользователь в любой точке мира может создать свой бизнес, принимающий биткойн-платежи за считанные минуты. Кроме того, владельцы существующих бизнесов могут предложить своим работникам оплату в биткойнах в качестве альтернативы, тем самым расширив свои возможности по поиску рабочей силы до масштабов всей планеты Земля. Обрести первые биткойны и стать частью сети вовсе не трудно.

Поговорим о технологии

Раз уж речь зашла о пиринговой платежной системе, само собой, технология, лежащая в основе цифровой криптовалюты, стоит того, чтобы обратить на нее особое внимание. Много написано о том, как эта технология – блокчейн – может стать могущественным инструментом в финансовом секторе. Пока что все это в будущем, а сейчас основное внимание направлено на биткойн-криптовалюту.

Технология биткойна создает небывалые технические возможности и альтернативы, о которых несколько лет назад можно было лишь мечтать. При этом блокчейн еще не обнаружил большей части с во-его потенциала. Ярчайшие умы человечества сейчас придумывают новые сферы применения блокчейн-технологии, чтобы еще основательнее внедрить ее в нашу повседневную жизнь. Подробнее об этом читайте в главе 3.

Технология биткойна в прошлом была недооценена, и, честно говоря, в ранней истории формирования биткойна его чаще всего ветре-чало полное непонимание. Было создано несколько платформ, чтобы сделать биткойн более доступным и практичным, но не во всех случаях у этих начинаний было счастливое продолжение – особенно у тех площадок, у которых были проблемы с безопасностью. Все принципиально новые инструменты, такие как биткойн, подразумевают определенную кривую обучения. Биткойн только сейчас

начинает “взрослеть” в этом смысле.

Потенциал новой технологии стал привлекать к себе заинтересованных участников из разных сфер жизни. Первопроходцами стали выходцы из сектора финансовых услуг, заинтригованные концепцией открытого регистра Биткойна. Открытый регистр означает, что кто угодно из любой точки мира может удостовериться в проведении финансовой транзакции с того момента, как она появится в сети. Несмотря на то что с первою взгляда это может но-казаться немыслимым, открытый регистр в системе, которая позволяет отеле-живать многочисленные операции, имеет массу преимуществ. Разнообразные способы применения технологии вовсе необязательно должны иметь отношение к сфере финансов, но многие из них имеют большой потенциал именно в этом секторе.

Что касается биткойн-платежей, это целое пространство для исследований. Настроить свой сайт таким образом, чтобы можно было принимать платежи в биткойнах, можно в течение всего нескольких минут (в случае с интернет-магазинами это займет ненамного больше времени). Кроме того, многочисленные платежные операторы предлагают услуги по конвертации биткойнов в обычные (фиатные) валюты. При ближайшем рассмотрении эта модель в реальности еще удобнее: вы можете получать переводы на свой банковский счет на следующий рабочий день, вместо того чтобы ждать неделю до получения платежей по кредитным картам, пока они преодолеют всю банковскую волокиту. К тому же комиссионные за обработку платежей в биткойнах существенно ниже банковских.

Биткойн как валюта

Когда заходит разговор о биткойнах, первое, о чем, как правило, вспоминают, – это их цена. На момент публикации этой книги его цена колебалась вокруг отметки 1000 долларов.

До 2011 года биткойн практически ничего не стоил, затем его цена начала постепенно расти. В 2013 году биткойн достиг своей пиковой стоимости, поднявшись выше отметки в 1200 долларов, после чего последовал период затяжного падения, из которого он вышел только к 2016 году[1].

Цена биткойна формируется вследствие поведения участников сети, еле-дуя принципам свободного рынка и законам спроса и предложения. Несмотря на то что общий объем биткойнов будет равен всего 21 миллиону “монет”, эмиссия которых завершится к 2140 году, на сегодняшний день спрос на них не очень велик. Однако по мере “взросления” биткойна через несколько лет ситуация может измениться.

Почему именно 21 миллион? Никто не знает. Вероятнее всего, это просто результат, который получится к 2140 году, если начать с эмиссии 50 монет каждые 10 минут с уполовиниванием этой величины каждые 4 года.

Не следует забывать о том, что биткойн можно использовать в качестве платежного метода как в Интернете, так и в реальном мире. Однако все это еще не делает его полноценными деньгами, поскольку ему недостает нескольких пунктов из традиционного определения функций денежной единицы. Тем не менее, согласно мнению многих экспертов со всего мира, биткойн все же следует считать настоящей цифровой валютой в ее самом ярком воплощении. Пока что мы продолжаем разбираться в этой новой технологии, и так ли уж важно, каким именно термином она называется? Можно с уверенностью утверждать лишь то, что биткойн является реальным средством платежа за многие товары и услуги, и именно поэтому цифровая сущность этой валюты представляет особенный интерес для исследования.

Будучи децентрализованным методом совершения платежей (что означает, что никакие правительства или организации его не контролируют), биткойн позволяет каждому расплачиваться и принимать платежи, вне зависимости от их местонахождения. Кроме того, биткойн является цифровой валютой, независимой от государственных границ и национальных валют, но при этом сам биткойн можно обменять почти на любую из существующих валют. С очень низкими затратами вы получаете подтвержденный платеж в течение часа или

около того – чего еще желать? Кроме того, следует отметить, что мобильные платежи набирают популярность, а биткойн – отличная альтернатива мобильным платежам, поскольку позволяет качественно расширить клиентскую базу при несущественных затратах.

Биткойн как средство расчета

Для того чтобы люди стали повсеместно воспринимать биткойн как валюту, его необходимо чаще использовать. Как вы могли догадаться, поначалу не так-то просто убедить торговцев принимать платежи в этой новой валюте. Но еще труднее убедить покупателей включиться в этот процесс.

Преимущества для продавцов видны невооруженным глазом: биткойн позволяет сэкономить на комиссионных и сократить другие издержки. Однако, если мало кто из ваших покупателей использует биткойны, то нет никакого смысла принимать платежи в них. Таким образом, запустить весь этот механизм предстоит покупателям.

Для того чтобы превратить биткойн в удобный для себя инструмент совершения платежей, можно начать с привычной пластиковой карты. В настоящее время доступны:

• предоплаченные биткойн-карты;

• дебетовые биткойн карты.

К этим пластиковым картам можно подключить опцию биткойн-платежей или привязать их к биткойн-кошельку (подробнее об этом – в главе 5) – и в результате они позволят вам использовать цифровую валюту во всех местах, где принимают пластиковые карты. При этом продавец по-прежнему будет оплачивать комиссию за проведенные платежи, как и в случае со стандартными кредитками, и получать платежи в национальной валюте.

Биткойн на сегодняшний день еще далек от статуса самого популярного метода платежа; многих ритейлеров приходится убеждать принять оплату в биткойнах. Мы полагаем, что со временем придет момент, когда можно будет призвать всех вокруг оставить наличные и кредитки дома и использовать биткойн для повседневных трат с помощью мобильного приложения. Подобная перемена не произойдет в одночасье, этого момента биткойн-энтузиастам придется еще дожидаться некоторое время (не забывайте о том, что мы немного опережаем свое время).

Биткойн и продавцы

Всем дальновидным ритейлерам следует задуматься о том, как начать принимать биткойн-платежи в своих виртуальных и реальных магазинах. Для того чтобы начать принимать платежи в биткойнах, вам не потребуется дополнительное оборудование, этот способ будет мирно сосуществовать с традиционной для вас платежной инфраструктурой. Все, что вам потребуется, – подключение к Интернету, но у большинства продавцов оно уже давно есть.

Ниже перечислены основные преимущества получения платежей в биткойнах.

• Принимая платежи в биткойнах, вы платите минимальные комиссионные, существенно менее заметные по сравнению с 2–6 % от каждой транзакции с традиционной картой.

• Биткойны можно конвертировать в любую национальную валюту по вашему выбору, и средства будут переведены на ваш банковский счет на следующий банковский день. Если вы пользуетесь услугами хорошего платежного оператора, он возьмет с вас менее процента за конвертацию. Сравните с транзакциями с участием кредитных карт: зачисления средств там порой приходите я ждать по неделе, за вычетом 2–6 % комиссионных и дополнительных сборов за все конвертации, и вы поймете, что биткойн выигрывает по всем пунктам.

• Биткойн – международная валюта. Она работает одинаково во всех странах мира. Куда бы вы ни поехали, символ биткойна везде одинаков.

• Биткойн можно делить до восьмой цифры после запятой (до стомиллионной доли), в отличие от наличных, которые дробятся лишь до центов/копеек. Например, если вы продаете что-либо в США, цена в долларах может быть дробной лишь до такого предела: 11,99 доллара. Биткойн позволил бы вам оценить свой товар более точно, например 11,98765432 BTC. Быть может, этот пункт не покажется вам сверхзначительным, но с учетом экспоненциального роста стоимости биткойна в ближайшие годы эти дополнительные разряды будут полезны для ценообразования в будущем.

• Биткойн позволяет потенциально расширить международную клиентскую базу. Вовсе не обязательно предлагать целое изобилие способов платежей во всех национальных валютах, достаточно предложить оплату в биткойнах.

• Биткойн сохраняет свою стоимость в ходе транзакции и конвертации в выбранную вами валюту, поэтому ваши валютные риски легко контролировать.

Биткойн и потребители

Преимущества биткойна для потребителей также весьма очевидны. Во-первых, больше не нужны наличные, чтобы оплачивать товары и услуги в физических магазинах. Наличные неудобны в использовании, занимают место в кошельке и карманах, вам хочется их поскорее потратить, чтобы не мешали (или это только со мной так?). К тому же всегда есть шанс, пусть даже незначительный, что вам подсунут поддельные банкноты. Вам, наверное, знакома ситуация, когда, чтобы заплатить за что-либо, приходится тратить полдня? Примеров масса.

Биткойн, помимо прочего, является более эффективным средством совершения платежей за товары и услуги по сравнению с банковским счетом или банковской (кредитной или дебетовой) картой по следующим причинам.

• Вместо того чтобы полагаться на сервисы, созданные централизованной организацией, такой как банк, биткойн предоставляет возможность совершать платежи где угодно, когда угодно и кому угодно, невзирая на время суток, выходные и государственные праздники.

• Когда вы совершаете онлайн-платеж, он осуществляется незамедлительно.

• Биткойн не связан государственными границами, это цифровая валюта, которая одинаково хорошо работает в Европе, Америке, Африке, Азии и Австралии. С помощью биткойна кто угодно может расплатиться за что угодно в любой точке мира, в то время как добраться туда физически – порой непростая задача.

• Уже сейчас ежедневно предпринимается немало усилий, направленных на популяризацию биткойна среди ритейлеров, и появляются все более удобные способы совершения платежей в биткойнах, помимо использования упомянутых выше пластиковых карт.

Как работает Биткойн

Биткойн меняет само представление людей о деньгах и закладывает семена сомнения в человеческие умы – в позитивном и философском смысле. Если припомнить все финансовые кризисы последнего десятилетия, становится понятно, почему некоторые стремятся найти пути реорганизации экономики. Биткойн с его прозрачностью и децентрализованностью может оказаться весьма мощным инструментом достижения этой цели.

Одно из основных свойств биткойна заключается в том, что он не связан с существующей финансовой системой и поэтому может быть использован теми слоями населения, которые прежде были лишены финансового обслуживания. Да, в развитых странах личный банковский счет кажется нормой, а вот в других уголках планеты дела обстоят совсем по-другому. В некоторых странах Африки, например, процент населения, не имеющего банковских счетов, доходит до 50–90 %. Неужели эти люди менее достойны собственного счета и финансового обслуживания, чем американцы или европейцы? Естественно, это не так. Однако в некоторых странах требования, которые необходимо соблюсти, чтобы открыть свой личный счет, почти невыполнимы для большей части их граждан.

В последнее время общество эволюционирует в форму экосистемы без наличных: все больше и больше людей используют банковские и кредитные карты для оплаты товаров и услуг как в виртуальном, так и в реальном мире. Мобильные платежи – оплата покупок с помощью мобильного телефона – сегодня на подъеме, и скоро этот инструмент сможет составить конкуренцию транзакциям по картам. Биткойн доступен с мобильных устройств уже несколько лет.

Сейчас мы постепенно подходим к определению блокчейна и потенциальных возможностей его

использования. Блокчейн (см. главу 7) может практически все; нужно лишь верно найти и сложить фрагменты пазла.

Далее приведено несколько примеров того, на что эта технология способна (подробности – в главе 3).

• Свободные денежные переводы (перевод любых сумм без посредников) с массой прочих преимуществ.

• Время, которое занимает пересылка денег из одной части мира в другую. – не более нескольких секунд.

• Конвертация в любую национальную валюту на выбор.

• Функционирование в обход банковских структур – необычайно полезное свойство для регионов и слоев населения, лишенных банковского сервиса.

Представьте себе на мгновенье, что вы живете в регионе, где нет банковской системы и стабильного подключения к Интернету… Есть решение и на этот случай: некоторые сервисы позволяют отправлять текстовые сообщения на любые телефонные номера в мире в обмен на биткойны или другие криптовалюты. Снова биткойн доказывает, что является очень мощным инструментом помощи людям, лишенным доступа к финансовым сервисам.

Впрочем, самая впечатляющая способность биткойна – это сама по себе сеть. Все транзакции фиксируются в сети, и после этого их можно отслеживать в реальном времени. Эта особенность предоставляет пользователям беспрецедентный контроль над финансовыми данными из любой точки мира. К тому же блокчейн позволяет отслеживать путь платежа, даже если транзакция еще не проведена. Надеюсь, столь бескомпромиссный, открытый подход будет усвоен традиционной финансовой инфраструктурой несмотря на то, что некий переходный период здесь неизбежен.

Анонимность при использовании биткойна

Одно из первейших заблуждений насчет биткойна касается анонимности его пользователей в сети. Можно ли рассчитывать на полную анонимность при использовании биткойна? Простой ответ на этот вопрос – не совсем. Однако по умолчанию определенный уровень конфиденциальности биткойн и другие криптовалюты обеспечить способны. Сочтете ли вы его достаточным – решать вам.

Если вы решили переместить свои средства с помощью биткойна, можете с легкостью скрыть свои личные данные, используя только публичный номер кошелька (подробнее о кошельках – в главе 5). Адрес кошелька представляет собой длинный ряд чисел и букв (в обоих регистрах), которые не дают ни малейшего представления о том, кем является его владелец или где он находится. С этой точки зрения биткойн предоставляет определенный уровень защиты, который несвойствен всем прочим платежным методам.

Однако эта конфиденциальность распространяется только на личные данные пользователей, поскольку сами биткойн-адреса являются частью публичною регистра, блокчейна, который непрерывно фиксирует все переводы между кошельками. Например, если бы я прямо сейчас отправил вам 0,01 BTC, любой пользователь сети смог бы увидеть транзакцию из кошелька А в кошелек В. Никто не смог бы узнать, кому конкретно эти кошельки принадлежат, но сама по себе транзакция будет как на ладони.

Если кому-либо станет известен номер вашего биткойн-кошелька, этот некто сможет отслеживать все ваши транзакции на сайте https://www.blockchain.info в любое время суток. Притом этот некто увидит не только ваши текущие транзакции, но и список всех предыдущих переводов, связанных с вашим биткойн-адресом. В результате, если кому-либо известен номер вашего кошелька, ни о какой анонимности в биткойне и речи быть не может, поскольку все ваши транзакции будут видны.

Эта ситуация несколько меняется в случае, если в процесс реализации транзакций включаются биржи (в главе 2 читайте больше о биржах). Каждый может у видеть транзакцию из биткойн-кошелька на биткойн-адрес на бирже, для обретения которого, как правило, требуется официальная регистрация. Однако, если вы продадите свои биткойны, отследить, куда именно делись эти монеты, станет гораздо сложнее. В этом смысле некоторый уровень конфиденциальности присутствует и здесь, но, опять же, насколько он достаточен, решать вам.

Анонимность и посредники

Существует несколько способов сохранить анонимность, используя биткойн, однако ни один из них на сегодняшний день не является простым и легкодоступным. По большому счету тем, кто стремится к анонимности, как правило, есть что скрывать. Возможно, кто-то желает избежать налогов или скрыть покупку нелегальных в переделах своей юрисдикции товаров и услуг. Если вы пользуетесь услугами какого-либо провайдера онлайн-кошельков, вы можете воспользоваться функцией “смешивания монет” и извлекать их из разных биткойн-адресов, не имеющих между собой никакой связи. Эта технология постоянно совершенствуется – даже в тот момент, когда вы читаете эти строки. Однако использование подобных сервисов сопряжено с определенными рисками, и если в процессе смешивания ваши монеты “потеряются”, то вернуть их обратно не будет никакой возможности. Впрочем, по этому поводу не стоит беспокоиться – мы подробно объясним, как управлять своим кошельком, в главе 5.

Перед тем как начать пользоваться любым внешним сервисом, всегда следует провести собственное расследование его надежности и обязательно задать себе вопрос “Действительно ли мне сейчас необходима полная анонимность для пересылки монет?”

Одна из самых серьезных проблем с внешними сервисами заключается в том, что, по сути, вы доверяете свои монеты посредникам. Биткойн и другие криптовалюты были созданы для того, чтобы исключить посредников и предоставить пользователям постоянный, прямой и полный контроль над своими активами. Передача контроля над своими деньгами доверенным посредникам противоречит базовым принципам Биткойна. К тому же использование анонимных сервисов вызывает подозрения в отмывании нелегальных доходов. Учитывая тот факт, что вы и без того действуете инкогнито, используя публичный биткойн-адрес без личных данных, дополнительные шаги, направленные на достижение анонимности, могут навлечь на вас подозрения касательно чистоты ваших намерений. В главе 5 подробно описаны наиболее доступные способы управления активами.

Защита личных данных

С защитой личных данных ситуация примерно такая же, как и с анонимностью.

Существуют способы защиты личных данных при использовании биткойнов в процессе передачи средств, но эти меры потребуют от вас дополнительных усилий и четкою планирования.

- Лучше всего генерировать новый адрес для каждой новой транзакции.
- Следует избегать раскрытия своего биткойн-адреса в открытых источниках.

Генерация нового адреса

Ожидая транзакцию от какого-либо пользователя, вы можете сообщить ему свой новый, только что сгенерированный адрес биткойн-кошелька, который не имеет никакой связи с другими биткойн-адресами, которыми вы пользовались ранее. Подобные одноразовые адреса позволяют пользователям изолировать свои транзакции, что является первейшей мерой безопасности для защиты личных данных.

В зависимости от выбранного способа хранения активов (версии биткойн-клиента и операционной системы, которыми вы пользуетесь) вы даже можете настроить для себя функцию автоматической генерации адресов. Например, если на свой компьютер или ноутбук вы установите клиент Bitcoin Core, то сможете менять адреса каждый раз, когда пересылаете деньги кому-либо.

Смена адреса происходит каждый раз, когда на вашем счету есть определенное количество биткойнов и вы пересылаете часть из них другому пользователю. Предположим, у вас есть 3 биткойна и вам нужно потратить 0,25 из них. В таком случае вам необходимо получить “сдачу” в размере 2,75 BTC на свой кошелек. Клиент Bitcoin Core (как и некоторые другие клиенты) позволяет подключить функцию, которая пересылает эту “сдачу” на новый только что сгенерированный адрес. В результате между исходным адресом и новым не возникает

связи, несмотря на то что все операции с биткойнами можно отследить непосредственно в блокчейне.

Держите свой биткойн-адрес в секрете

Еще один способ защиты данных – в определенных пределах – неразглашение вашего публичного биткойн-адреса. Публикация своего биткойн-адреса на веб-сайтах, в блогах, аккаунтах социальных сетей и на форумах – не слишком хорошая идея, если вы заботитесь о безопасности. Если кто-то наткнется на ваш биткойн-адрес и найдет способ связать ею с вашими личными данными, то восстановить конфиденциальность можно будет только вышеописанным способом.

Взаимозаменяемость

Одна из проблем биткойна – взаимозаменяемость, вернее, отсутствие оной. Взаимозаменяемость – это термин, означающий то, что все единицы данного финансового инструмента являются идентичными с точки зрения пользователя. Так, можно сказать, что все стодолларовые купюры являются полностью взаимозаменяемыми. С биткойном это не совсем так, поскольку с каждой единицей цифровой валюты неразрывно связана история операций. Однако в некоторых ситуациях отсутствие у биткойна упомянутой черты является его преимуществом.

Большинство правительств во всем мире привыкли полагаться на собственную, полностью контролируемую систему эмиссии фиатных валют. Местные валюты подчиняются принципу централизации и выпускаются только центробанками. Если правительству нужно больше денег, центробанк может просто “довыпустить” еще валюты, включив печатный станок и прибегнув к “валютным вливаниям”, как у них это называется. Таким образом, либо по указу правительства, либо по собственной инициативе центробанк повышает денежною ликвидность посредством вбросов новых денег в экономику. С биткойном такой номер не пройдет, потому что выпуск биткойнов возможен лишь в определенном фиксированном объеме: 21 миллион монет. Каждая из 21 миллиона монет имеет свою историю транзакций, а это означает, что биткойн не относится к числу полностью взаимозаменяемых активов, как, скажем, наличные деньги.

Концепция Биткойна

Когда новая технология стучится в дверь, то, чтобы впустить ее в свою жизнь, нам необходимо преодолеть существенную преграду, а именно: решиться в нее поверить. В случае с биткойном доверие должно быть обоюдным. Даже невзирая на то, что вы как пользователь полностью контролируете свои активы, вам все равно необходимо будет поверить в то, что вся остальная сеть не исчезнет с лица Земли завтра утром.

Конечно, шансы на то, что Биткойн вдруг просто исчезнет, не слишком-то высоки, так что не стоит об этом сильно переживать. Однако жизнь учит всех нас одной универсальной истине: в ней нет ничего постоянного. Вся сеть Биткойна полностью децентрализована, она состоит из множества индивидуальных участников, а также большого количества независимых узлов, которые нужны для того, чтобы непрерывно поддерживать систему. Мы расскажем подробнее об узлах и их роли в главе 6.

Эта тема подводит нас к тому свойству Биткойна, которое по-прежнему у многих вызывает сомнения: децентрализация. Как отмечалось выше, Биткойн – децентрализованная цифровая валюта, а это означает, что в рамках этой системы не существует централизованного органа, от которого критически зависела бы работоспособность системы Биткойна. Каждый независимый пользователь является интегрированной частью экосистемы Биткойна, поэтому потребуются невообразимые усилия для того, чтобы добраться до каждого из них, чтобы “заглушить” всю систему одновременно.

Децентрализованную модель Биткойна можно сравнить с тем, как работает поисковый движок Google. Миллионы людей одновременно пользуются этим поисковиком, однако он никогда не тормозит. Это потому, что поисковый движок Google работает на многочисленных серверах – децентрализованным образом. Поэтому для того, чтобы замедлить или прервать его работу, потребуются гигантские усилия.

У децентрализации есть еще одна особенность, которая заставляет людей задуматься дважды, прежде чем присоединиться к биткойну. Сеть состоит из миллионов независимых пользователей и не имеет никакого

централизованного органа управления, который контролировал бы ее работу. Это означает, что, если у вас есть биткойны и что-то по какой-то непредвиденной причине пошло не так, никто вам ничего не возместит. Если ваши биткойны утрачены, не важно, потратили вы их или потеряли, они утрачены навсегда, и нет ни единого шанса их вернуть.

Доверие к технологии Биткойн

Человеческая натура подсказывает нам продолжать делать дела так же, как мы делали их раньше, и опасаться перемен. Когда в начале 90-х годов появился Интернет, лишь очень немногие (в основном гики) верили в то, что он станет распространенным явлением, которое будет присутствовать практически в каждом доме. И вот посмотрите, что мы имеем теперь: дедушки и бабушки и даже домашние животные имеют свои аккаунты в Сети. Без Интернета просто не обойтись. Следует признать, что переход от мира без Интернета к Всемирной паутине – это большая перемена.

Биткойн часто сравнивают с Интернетом на ранних стадиях развития: новая, революционная технология, которая, как кажется, опережает само время. Отчасти это так и есть, поскольку биткойн решает те проблемы, о которых немногие задумывались. Проблема не в том, что нет доказательств стабильной работы сети, а в том, что человеческая природа не благоволит к переменам, поскольку “вроде все и так работает нормально”.

И так же, как это было с Интернетом, пройдет немало времени, по крайней мере несколько лет, прежде чем биткойн станет мейнстримом. Даже невзирая на то, что несколько глобальных биткойн-проектов и платформ уже сейчас находятся в разработке, пройдет не один день, прежде чем обычные люди массово будут готовы их использовать. Исходя из этого можно утверждать, что сейчас необходимо больше образовательных инициатив, рассказывающих о биткойне с точки зрения его идеи и технологии, положенной в его основу, а не только как об “альтернативной валюте”.

С другой стороны, очень многие уже поверили в эту технологию. Большинство развивающихся технологий на сегодняшний день подчинены потребностям финансового сектора, например рынка денежных переводов. Технология биткойна позволяет пересылать деньги кому угодно в мире с очень низкой комиссией. На поприще денежных переводов такие игроки, как Western Union, Moneygram и даже традиционные банки, вскоре столкнутся с серьезным конкурентом в виде Биткойна, системы “выдуманных интернет-денег”, как некоторые его часто называют.

“Стоит ли доверять этой технологии?” – столь серьезный вопрос, что ответить на него можете только вы сами. Биткойн был, есть и будет существовать для того, чтобы вы могли обрести максимальный контроль над вашими деньгами. Если вы готовы к такой свободе, вы найдете много полезного в этой книге. Надеемся, что затраченное время оправдает себя.

Доверие к биткойну как к валюте

Как отмечено выше, биткойн является не валютой в традиционном понимании, а скорее альтернативным, цифровым средством платежей. Естественно, вы можете покупать и продавать товары и услуги за биткойны, но некоторых характеристик, свойственных классическим валютам в традиционном понимании, биткойну, очевидно, недостает.

Тем не менее многие продавцы принимают платежи в биткойнах наряду с другими, традиционными средствами платежа, а значит, доверяют этой технологии. Причины, по которым это происходит, предельно просты.

• Нет никаких дополнительных сборов за прием платежа.

• Нет необходимости в дополнительной инфраструктуре.

Будучи продавцом, вы можете, затратив минимальные усилия, начать принимать биткойн-платежи как в реальных, так и в интернет-магазинах. Вы можете моментально конвертировать поступления в биткойнах в любую выбранную вами фиатную валюту и получить средства на счет в банке уже на следующий рабочий день.

С точки зрения покупателя, возможность использовать биткойны в качестве средства платежа означает, что наличные вам больше не нужны, так же как и кредитные карты и банко ею кие счета. Однако для того, чтобы обрести биткойны вначале, как правило, приходится их покупать, а значит, тратить фиатные деньги. Нет денег на подобные эксперименты? Не стоит отчаиваться: есть масса способов заработать биткойны без особых вложений, и они будут подробно рассмотрены в главе 4.

Смысл биткойна заключается в том, чтобы предоставить пользователю возможность полностью контролировать свои средства в любой момент времени. И именно эта мысль многих пугает, потому что на протяжении последних 50 лет или даже дольше банки и правительства неустанно стремились прибрать контроль над всеми денежными потоками к своим рукам. Ответственность за свои действия и решения может быть обузой, и многие боятся такой ответственности. И если вы готовы честно признаться себе в том, что не готовы тратить время на у правление собственными активами (во время отдыха, при необходимости, в момент, когда они вам понадобятся, в любой требующей вашего участия ситуации), тогда биткойн не для вас.

Но если вы сыты по горло неэффективностью современной финансовой системы, подконтрольной правительствам и банкам, то, вполне возможно, что время и усилия, затраченные на исследование биткойна, себя оправдают. Никто не говорит о том, что биткойн должен полностью заменить местные валюты, которыми вы пользовались до сегодняшнего дня. Обе системы вполне могут мирно сосуществовать. Если вы все же решитесь оценить преимущества и потенциал биткойна для различного рода онлайн-транзакций, то вскоре ощутите будоражащий, живительный дух полной финансовой свободы.

Глава 2. Покупка и хранение биткойнов

В этой главе…
- Как купить биткойны
- Как выбрать биржу
- Как зарегистрироваться
- Как хранить биткойны

В этой главе мы рассмотрим некоторые практические аспекты использования биткойна и постараемся ответить на основополагающие вопросы начинающих: “С чего начать?”, “Как сохранить полученное?”, “Как потратить первый биткойн?” и, конечно, “Как соблюсти правила безопасности, отправляясь на свой первый биткойн-шоппинг?”

К концу главы вы научитесь покупать биткойны и узнаете, как ими управлять. Перед тем как приступить к практическому уроку, вам потребуется выполнить один из нижеперечисленных пунктов (или оба).

- Установить программу биткойн-кошелька на свой компьютер или ноутбук (загрузить ее можно с сайта https://bitcoin.org/ru/[2])·
- Установить мобильную версию биткойн-кошелька на свое мобильное устройство (загрузить ее можно также с сайта https://bitcoin.org/ru/).

Начинаем: где взять биткойны?

Первое препятствие на пути в мир криптовалют – “Где взять биткойны?” Несмотря на то что есть несколько способов сделать это, которые мы подробно рассмотрим в этой главе, самый очевидный из них – это просто купить биткойны.

Но куда же идти, если вы задались целью обрести цифровые токены в обмен на реальные деньги? Такие площадки называются биржами (exchanges), и так же, как в пункте обмена валют, где вы меняете одну местную валюту на другую, на биткойн-бирже вы можете поменять фиатную валюту на биткойны.

Биткойн-биржи реализуют сервис, который в традиционной финансовой системе выполняют банки и другие регулируемые структуры, которые осуществляют конвертацию валют; или конверсионные операции, как их еще

называют. Вы можете зарегистрировать свой аккаунт на биткойн-бирже, завести на него деньги в национальной валюте и купить на них биткойны. С этого аккаунта вы можете отправить биткойны на выбранный вами кошелек и использовать биткойны по собственному усмотрению – так же, как вы использовали бы фиатные деньги, лежащие на банковском счету.

Как вы помните, биткойн был спроектирован как децентрализованный, трансграничный метод осуществления платежей, который не требует конвертации одной валюты в другую. Несмотря на то что за биткойны можно приобрести многие товары и услуги, нам в повседневной жизни все равно нужны фиатные деньги – ну, хотя бы для того, чтобы платить налоги и тому подобное. Для этого и нужны биржи: чтобы упростить операции обмена.

Регистрация на бирже

Биткойн-биржа обычно имеет вид веб-сайта, однако есть и несколько физических бирж (о них подробнее читайте ниже). Когда вы решите выбрать биржу, вариантов у вас будет предостаточно. В зависимости от вашего местонахождения и типа фиатной валюты, которую вы хотите использовать, одни биржи могут показаться вам более предпочтительными, чем другие. В настоящий момент не существует такой биткойн-биржи, которая обслуживала бы все страны в мире, ввиду тех или иных правовых ограничений. На момент издания книги крупнейшими биткойн-биржами мира являются:

https://www.bitfinex.com
https://www.bitstamp.net
https://coinbase.com
https://kraken.com
https://btc-e.com

Мы также советуем ознакомиться со списком бирж, представленным на сайте Bitcoin.org или в одном из обзоров существующих бирж на каком-либо тематическом новостном сайте, например на BitNovosti.com. Возможно, вы найдете для себя что-то полезное, перейдя по следующим ссылкам[3]:

http://bitnovosti.com/2014/11/25/kupit-bitcoin-missiya-vypolnima
https://www.buybitcoinworldwide.com/ru

Основная цель биткойн-биржи – упростить процесс конвертации фиатной валюты в цифровую, например в биткойны, и обратно. Кто у годно может создать аккаунт на биткойн-бирже, не имея при этом биткойнов или предварительного опыта распоряжения ими.

Вот как работает онлайн-биткойн-биржа (детали будут варьироваться в зависимости от конкретной биржи).

1. Вы создаете аккаунт пользователя, предоставляя базовую информацию.
2. Вы получаете письмо на свой почтовый ящик со ссылкой для активации аккаунта.
3. После подтверждения активации происходит регистрация.

Как и любой рынок, биткойн-биржа является осциллографом колебаний рыночных цен. В случае с биткойн-биржами цены могут колебаться довольно значительно, поскольку каждый бизнес строится по собственной бизнес-модели. Одни биржи устанавливают курс на биткойны ниже или выше средней рыночной цены, но при этом не берут комиссию. Другие биржи предложат вам актуальные рыночные цены, но возьмут 0,05–0,5 % комиссионных за каждую транзакцию.

Даже несмотря на то, что цена биткойна зависит только от законов спроса и предложения в условиях свободного рынка, все равно нужны площадки, на которых покупатели и продавцы могли бы найти друг друга. Большинство биткойн-бирж используют торговые движки, которые автоматически соотносят совпадающие ордера на покупку и продажу. Однако встречаются и другие варианты, например локальный пиринговый обмен, о котором мы поговорим подробнее далее в этой главе.

Очень важная особенность биткойн-бирж заключается в том, что они позволяют обменивать BTC на другие традиционные валюты, и далеко необязательно это будет ваша местная валюта. Например, если вы живете в Китае, ваша национальная валюта – китайский юань. Однако, если вы хотите получить доллары (USD), евро

(EUR) или британские фунты (GBP), можете использовать для конвертации биткойн-биржи, которые предлагают такие валютные пары.

Чтобы вывести свои валютные средства с биржи и положить на собственный банковский счет, в некоторых случаях их все же придется конвертировать в свою национальную валюту, если ваш банк не принимает переводы в других валютах. Всегда обращайте внимание на условия реализации транзакции, прежде чем вступать в эту игру.

Биткойн-биржи обязаны подчиняться местным законам и соответствующим контролирующим инстанциям финансового сектора стран, в которых они расположены. Зачастую эти законы предписывают им запрашивать ваши личные данные, в том числе это могут быть ваше полное имя, телефонный номер (мобильный или домашний), а также адрес проживания. Помимо этого, большинство биткойн-бирж попросят вас указать дату рождения, адрес и другую информацию, необходимую для верификации пользователя (см. следующий раздел). Некоторые особо придирчивые биржи даже требуют от клиентов копию идентифицирующих документов (например, загранпаспорта).

Знай своего клиента

Для того чтобы воспользоваться услугами большинства биткойн-бирж, вам придется пройти процедуру авторизации в соответствии с международным банковским принципом “знай своего клиента”. Этот процесс со стороны кажется гораздо страшнее, чем в действительности, несмотря на то что подразумевает передачу приватной информации.

Этап 1. Подтверждение номера мобильного телефона

Первый этап – это подтверждение номера мобильного телефона. Большинство бирж отправят на ваш номер сообщение с кодом. Этот код необходимо ввести на определенной странице сайта в процессе идентификации, чтобы подтвердить, что именно вы имеете доступ к этому телефонному номеру, на случай экстренной ситуации или для восстановления пароля.

Этап 2. Подтверждение личных данных

На следующем этапе вас могут попросить подтвердить свою личность, предоставив копию документа, удостоверяющего ее. На одних биржах это обязательно с самого начала, другие могут запрашивать это только после того, как ваша торговля достигнет определенных оборотов. В зависимости от того, с какой именно биржей вы имеете дело, таким документом может являться скан-копия пас порта или водительских прав, недавний счет за коммунальные услуги на ваше имя (для подтверждения адреса проживания) или копия свидетельства о рождении. Для некоторых бирж эти документы придется также переводить (с нотариальным заверением перевода), поскольку у них нет русскоязычной поддержки.

Количество идентифицирующих документов, которые могут у вас запросить, зависит от объема валюты, с которым вы планируете вести операции на этой площадке. Ввод и вывод крупных сумм обычно требуют предоставления более полной личной информации.

И это одна из основных сложностей, с которыми сталкиваются новички, впервые пытающиеся приобрести биткойны на бирже. После того как вся необходимая информация предоставлена, но до того, как документы будут верифицированы, часто следует период ожидания, который тоже надо принимать во внимание. Основные биткойн-биржи рассматривают документы от нескольких часов до нескольких дней, но бывали случаи, Когда этот процесс длился более недели.

Отправляя документы, убедитесь, что все копии разборчивы, и тогда регистрация пройдет быстрее.

Выяснение обменных курсов

Когда вы будете сверять текущий курс биткойна к национальной валюте, имейте в виду, что курсы на покупку и на продажу могут сильно различаться. Курсы зависят, конечно же, не только от времени суток (существуют знач и-тельные различия между разными торговыми площадками).

Биткойн-биржи – очень конкурентный бизнес по своей природе, и каждая площадка стремится завоевать так

много пользователей, как только возможно. Чтобы достичь этой цели, каждой биткойн-бирже необходимо придумать собственную бизнес-модель, отвечающую запросам как можно большего числа пользователей. В большинстве случаев новообращенные пользователи – это самый лакомый кусок рынка, поэтому новые площадки прилагают немало усилий, чтобы сделать биткойн более доступным для них.

Для того чтобы выяснить наиболее выгодные для себя обменные курсы, следуйте таким рекомендациям.

• Когда бы вы ни решили поменять биткойны на национальною валюту или обратно, сначала уточните их актуальную стоимость. Для выяснения необходимых деталей внимательно прочитайте врезку (см. ниже) “Зачем следить за курсом”. Последние несколько лет отдельные биткойн-биржи начали предлагать пользователям биткойны по фиксированной цене (конечно, если вы проведете транзакцию в течение условленного времени). Например, конвертируя биткойны в национальную валюту, пользователь должен успеть произвести трансферт в течение 15 минут после конвертации, чтобы курс не утратил актуальность. Если не сделать этого, то в итоге транзакция будет пересчитана по другому, более актуальному курсу, который может оказаться либо выше, либо ниже.

• Регулярно следите за биржевым курсом биткойна к вашей местной валюте, чтобы умножить свою прибыль и сократить потери. Несомненно, одним из самых полезных источников релевантной информации по курсам является сайт Bitcoinwisdom.com. Существуют и другие схожие ресурсы, такие как Cryptrader.com или Bfxdata.com. Какие бы ресурсы вы ни выбрали, везде, как правило, можно найти графики изменения стоимости, схожие с теми, которые составляют для обычных, традиционных валют, или просто актуальный курс BTC к местным валютам в цифрах. Вот список сайтов, на которых можно найти свежие данные:

https://bitcoinwisdom.com
https://cryptrader.com
http://bfxdata.com
http://coinmarketcap.com/currencies

• Будьте готовы к тому, что в какой-то момент вас попросят оплатить биржевой комиссионный сбор, поэтому изначально выясните все существующие условия. Большинство бирж берут маленькую комиссию за каждый выполненный ордер на покупку или продажу, но некоторые берут больший процент или зачисляют на счет меньшую сумму. К тому же возможны дополнительные сборы, например за вывод активов на банковский счет или за другую операцию.

Обменные курсы биткойна на подобных биржах колеблются постоянно, отчасти в связи с колебаниями кривых спроса и предложения в условиях свободною рынка. В последние годы общий торговый объем биткойнов растет экспоненциально, и при этом большая часть торгов происходит в Китае, Японии и США. Но несмотря на это местные биржевые курсы обмена в других странах мира могут расти, тогда как на основных биткойн-биржах он будет падать, и наоборот.

Зачем следить за курсом

В зависимости от того, какой платформой вы пользуетесь, возможны несколько удобных способов отслеживать актуальный курс биткойна. Для тех, кому удобнее проверять изменения курса на компьютере подойдет сайт bitcoinwisdom.com. На этой платформе вы найдете актуальную статистику по курсам большинства мировых валют относительно биткойна (доллар, евро, рубль и юань), а самые популярные биржи совершают операции и с более специфичными валютами.

Для пользователей мобильных устройств совет будет другим. Большинство мобильных кошельков отображают стоимость биткойна относительно вашей местной валюты (см. главу 5 для получения более подробной информации). Это отличный способ определить, сколько стоят ваши биткойны в определенный момент времени. Учтите, что вашему мобильному устройству потребуется стабильное интернет-соединение – мобильный Интернет или Wi-Fi – для того, чтобы данные регулярно обновлялись.

Сравнение пиринговых транзакций и бирж

Существует два способа конвертации биткойна: пиринговые транзакции (прямые сделки между пользователями) и, как мы привыкли их называть, обычные биржевые сделки.

Стандартные биткойн-биржи сводят заявки продавца и покупателя в централизованной торговой системе. При этом ни у продавца, ни у покупателя нет ни малейшего представления о том, кем является другая сторона сделки, и эта деталь позволяет сохранить определенный уровень анонимности и безопасности частных данных. Это самый распространенный способ обмена местной валюты на биткойны и обратно.

Однако биткойн изначально был создан для пиринговых транзакций. В отличие от других знакомых вам пиринговых технологий, например торрентов, в биткойне пиры представлены не множествами, а отдельными пользователями. Пиринговая транзакция предполагает, что вы обладаете какой-то информацией о лице, с которым вступаете во взаимодействие. Информация о пользователе, с которым вы заключаете сделку, может варьироваться от публичного номера биткойн-адреса, до имени пользователя, его местонахождения, IP-адреса и т. п. Возможно, вам придется даже встретиться лично, чтобы обменять биткойны на наличные.

Вместо того чтобы использовать систему ордеров для соотнесения покупателей и продавцов, тем самым передавая контроль над средствами в руки посредников, в пиринговых операциях продавцы и покупатели действуют напрямую, никуда не передавая средства на хранение.

Например, вы решили купить биткойны у кого-либо, кто живет в вашем городе. Вместо того чтобы надеяться, что натолкнешься на подобного пользователя на обычной бирже (шансы невелики), вы можете использовать специальную платформу, помогающую осуществлять пиринговые транзакции между индивидуальным пользователем. Существует несколько таких биткойн-платформ, которые позволяют зарегистрировать аккаунт для поиска других биткойн-энтузиастов, живущих с вами в одном городе или даже в одном районе. Наиболее распространенным сервисом прямых сделок по покупке-продаже биткойнов между пользователями является https://locaibitcoins.net/[4].

К слову сказать, далеко не каждый готов к сделкам в стиле “из рук в руки”. Многие привыкли к традиционным способам оплаты и предпочтут, например, PayPal или прямой перевод на карту.

В зависимости от того, какой способ обмена вы предпочитаете, пиринговые транзакции могут оказаться более (или менее) подходящим для вас способом конвертации в повседневной жизни. В целом для пиринговых транзакций не нужны документы, удостоверяющие личность, вместо этого существуют репутационные системы для отслеживания вашей и чужой истории торгов (например, https://www.bitrated.com). С их помощью вероятность удачного завершения сделки гораздо выше.

Один из наиболее интересных аспектов пиринговых платформ – встроенная репутационная система. Из-за того, что участники торгов действуют напрямую, не передоверяя свои фонды владельцам платформы, принцип доверия становится важен, как никогда ранее. Важно знать историю предыдущих сделок вашего потенциального контрагента, прежде чем решить, стоит ли с ним связываться.

Правила безопасности при биржевой торговле

Один из важных моментов, о которых нельзя забывать, если вы решите доверить свои активы на хранение бирже, – это далеко небезопасно. Использование услуг посредников и зависимость от централизованных сервисов и платформ идут вразрез с основной идеологией биткойна.

Несмотря на то что платформы-посредники имеют дело с децентрализованной цифровой валютой, сами они

представляют собой централизованные структуры, что делает их уязвимыми для атаки. Впрочем, их разработчики тоже не сидят сложа руки. Больше информации о том, какие усилия предпринимают разработчики для защиты ваших активов, можно найти во врезке “На страже форта «Биткойн»” ниже в этой главе.

Ко всеобщему сожалению биткойн-пользователей мира, биткойн-биржи не могут похвастаться незапятнанной репутацией в плане сохранности цифровых сокровищ. Если биржу взломали или если ее владельцы решили сбежать со всеми деньгами, к несчастью, мало что можно будет предпринять. Разве что попытаться подать иск в суд и надеяться, что рано или поздно обстоятельства дела прояснятся. Когда вы кладете деньги в банк, их безопасность гарантирует государственная система страхования, например в США все ваши депозиты до 100 тысяч долларов застрахованы. В случае с биткойн-биржами это не так.

Если вы решили хранить биткойны на бирже, вам придется не только полагаться на то, что сервис будет доступен круглосуточно (обычно так все и есть, но как знать наперед!), но и довериться этой площадке в плане безопасности. Если творить конкретно, вы доверяете свое финансовое имущество площадке, которая заявляет, что способна обеспечить достаточный уровень безопасности для сохранности ваших данных и денег.

К счастью для биткойна, биржи существенно эволюционировали с точки зрения безопасности, хотя бронебойной защиты пока еще никто не придумал. Как это всегда бывает с новыми революционными технологиями, требуется время, чтобы люди, во-первых, оценили ее потенциал и, во-вторых, поняли, каким способом лучше всего ее защищать. В прошлом биржи уже выяснили, как защищать не надо (весьма жестоким и дорогостоящим способом).

Несмотря на то что биткойн-биржи стали гораздо безопаснее, чем в 2010 году, это не значит, что к ним стоит относиться так, как будто это провайдер кошельков для хранения (подробнее о криптокошельках читайте в главе 5). У биткойн-пользователей есть масса разных способов хранения BTC, более де централизованных и надежных. Тем не менее централизованные сервисы-провайдеры кошельков, например Blockchain.info и Coinbase.com, все еще популярны среди пользователей.

На страже форта “Биткойн”

В оригинале технической документации биткойна (https://bitcoin.org/files/bitcoin-paper/bitcoin_ru.pdf) авторства Сатоши Накамото подробно описано, как технология биткойн может способствовать повышению безопасности, которая в современной банковской инфраструктуре оставляет желать лучшего. Развитие этой сферы не терпит спешки. Например, такой инструмент, как мультиподпись, появился только в 2013 году.

Мультиподпись в мире биткойна – это примерно то же самое, что требование нескольких подписей для перевода в корпоративном банкинге. Вместо того чтобы доверять одному-единственному человеку право доступа к определенному кошельку, с помощью этой технологии можно распределить множество ключей среди нескольких пользователей.

Например, Марк и Эллис хотят завести совместный биткойн-кошелек, в случае, если между ними возникнут разногласия, в роли беспристрастного арбитра выступит Дейв, ему тоже дают ключ, В процессе создания кошелька генерируются три приватных ключа. Один ключ принадлежит Марку, другой – Эллис, а третий – Дейву-гаранту. Если Марк или Эллис хотят совершить биткойн-транзакцию, они сначала должны убедить друг друга или Дейва в том, что это хорошая идея.

На практике функция мультиподписи в биткойн-кошельке означает, что множественные стороны должны прийти к соглашению и подписать транзакцию своим ключом, чтобы она была проведена. В нашем случае либо Марк и Эллис, либо Эллис и Дейв, либо Марк и Дейв должны прийти к соглашению перед тем, как какие-либо средства будут списаны с биткойн-кошелька. Если только одна сторона хочет потратить биткойны, а две не хотят, транзакцию провести не удастся, Узнать об этом подробнее можно здесь: https://en.bitcoin.it/wiki/Multisignature.

Тем не менее защитить финансовую платформу (а биткойн-биржи именно таковыми и являются) не так-то просто, Оплата услуг экспертов по безопасности, тестирование новых программных функций, приостановка торгов в случае возникновения проблем и т. д… Так или иначе, поддержка безопасности – это работа 24x7.

Еще одна разработка для повышения безопасности на биржах – двухфакторная идентификация. Несмотря на то что эта функция опциональна, всем пользователям бирж рекомендуется установить режим двухфакторной

идентификации для своего аккаунта (подробнее о двухфакторной идентификации читайте в следующем разделе этой главы).

Биткойн-биржи тоже стали внедрять кошелки с мультиподписью. Если хакер взломает биткойн-биржу, вывести средства с нее будет не так-то просто, поскольку необходимо, чтобы другие подписанты одобрили каждую транзакцию Однако не все биржевые активы хранятся в “холодных” кошельках с мультиподписью (подробнее об этом читайте ниже в этой главе).

Если вкратце, то хранение биткойнов на бирже в течение длительного времени – небезопасное решение. Однако, если вы планируете потратить или вывести эти средства в течение нескольких дней или часов, нет ничего страшного в том, чтобы оставить их в биржевом кошельке на это время. Оставляя же средства на бирже более чем на несколько дней, вы подвергаете себя ненужному риску.

Самый лучший способ хранить биткойны – в кошельке под вашим контролем, неважно, находится он на компьютере или на мобильном. В главе 5 вы узнаете об этом подробнее.

Биткойн спроектирован так, чтобы предоставить контроль над средствами конечному пользователю, а необходимость в услугах посредников, в том числе для безопасного хранения этих средств, полностью отпала. Переводите свои средства с биткойн-биржи на цифровой кошелек на своем компьютере или мобильном устройстве как можно скорее.

Использование двухфакторной аутентификации

Даже если вы не планируете хранить биткойны на бирже долгое время, вам все равно будет полезно познакомиться с существующими методами защиты своего аккаунта. Большинство обычных (не биткойн) онлайн-сервисов требуют от пользователя ввести логин и пароль для авторизации, что не является наилучшим решением для защиты частных данных.

В последние годы стало очевидно, что для обеспечения безопасности необходимо несколько слоев защиты, помимо стандартного протокола аутентификации. Одним из наиболее популярных решений этой проблемы является двухфакторная аутентификация (2FA), предполагающая, что для получения доступа к вашему аккаунту потребуется еще один токен. Если в соответствующее поле вводится неверная комбинация цифр, интерфейс выдает сообщение об ошибке.

Как известно, бывали случаи, когда неавторизованная третья сторона получала доступ к логинам и паролям пользователей. Это не всегда происходит из-за небрежности пользователя, порой сами онлайн-сервисы используют небезопасные способы хранения данных. Двухфакторная идентификация (2FA) позволяет добавить новый уровень защиты для большей сохранности ваших средств и данных.

Двухфакторная идентификация бывает различных видов, но выбранная вами площадка может не поддерживать все виды. Одна из наиболее распространенных форм двухфакторной идентификации называется Google Authenticator – приложение, которое можно установить на любое мобильное устройство. Использовать Google Authenticator довольно легко. Скачав приложение на свое мобильное устройство, нужно сделать следующее.

1. Войдите в свой аккаунт сервиса или платформы, который вы хотите защитить с помощью технологии 2FA.
2. Отсканируйте QR-код, проассоциированный с функцией 2FA, с помощью камеры мобильного устройства.
3. Используйте этот QR-код, чтобы привязать мобильное устройство к данным вашего аккаунта.

Каждый раз, когда вы открываете Google Authenticator, он генерирует новый 2FA-код для вашего аккаунта. Эти коды действительны только в течение очень короткого промежутка времени, после чего автоматически генерируется новый код. Запрос кода происходит автоматически при входе в аккаунт. Ввод кода, исчерпавшего срок давности, вернет вас на страницу авторизации.

Несмотря на то что двухфакторная авторизация с помощью мобильного устройства выглядит довольно удобной, у этой системы есть ряд недостатков, которые стоит держать в уме.

• Вам придется всегда носить с собой это мобильное устройство и его нужно всегда держать заряженным, чтобы своевременно сгенерировать 2FA-код. Для многих это вполне посильная задача, но в ряде случаев такая система может вызвать неудобства.

• Если вы потеряете свой смартфон или его украдут, вы утратите свой идентификатор. В этом случае можно аннулировать двухфакторную идентификацию и переключить ее на другое устройство, но этот процесс не из приятных, и проходить его без насущной необходимости вы вряд ли захотите.

Другие способы подключить двухфакторную аутентификацию предлагают такие сервисы, как Clef и Authy, которые можно найти в соответствующем каталоге приложений для вашего мобильного устройства; к тому же есть старая добрая (но и менее безопасная) система смс-подтверждений. Впрочем, все эти способы предполагают, что вам придется носить дополнительное оборудование, чтобы подтвердить свою личность, что не слишком-то удобно.

Система смс-подтверждений также неидеальна. Например, если вы находитесь в зоне с плохим сигналом сотовой сети или вовсе без покрытия, смс-подтверждение для двухфакторной авторизации не сработает. К тому же, если вы находитесь в чужой стране, с вас могут списать дополнительные сборы за международную связь.

Не столь важно, какую именно форму двухфакторной авторизации вы выберете, важно, чтобы у вашего аккаунта на биткойн-бирже была какая-либо форма двухфакторной авторизации. Эта мера защитит вашу учетную запись, и, несмотря на то что эта предосторожность потребует дополнительных телодвижений, безопасность ваших средств стоит того.

Распределение ответственности

Вопрос о распределении ответственности в рамках биткойн-биржи – тема крайне неопределенная. Тем не менее в этом разделе мы постараемся как можно точнее установить границы вашей ответственности.

Биткойн – это нерегулируемая и неподконтрольная правительству цифровая валюта; это означает, что сервисы, осуществляющие операции с биткойнами, как правило, никем не регулируются. Однако, в зависимости от географического расположения биржи, у нее могут быть некоторые правовые ограничения, которые вам придется учитывать.

На момент написания книги по-прежнему оставалось неясно, кто будет нести ответственность, если биржу взломали хакеры или если сервис вдруг ни с того ни с сего закрывается. Большинство крупных, заработавших репутацию биткойн-бирж внедряют системы страхования, которые способны защитить вас от финансовых рисков до определенной степени. Смысл подобной системы в том, что если биржу взламывают или ваши средства исчезают с этой платформы иным образом, биржа возмещает вам потери из собственного кармана. Тем не менее советуем вам подойти к выбору ответственно, хранить на биржах лишь столько, сколько вам понадобится в ближайшее время, и не относиться к аккаунтам на бирже как к надежному месту хранения биткойнов.

Некоторые экономисты считают, что биткойн-биржа – это саморегулирующаяся платформа, так же как NASDAQ. Несмотря на то что NASDAQ – это огромная биржа и ее представители заявляют, что платформа обладает иммунитетом к компьютерным сбоям, на практике это означает, что в случае сбоя, если он все же произойдет, площадка не будет возмещать средства, утраченные ввиду “сбоя”. Биткойн-биржи устроены

по-другому, у них нет регулирующей инстанции, и никто не может вам гарантировать, что вы получите назад свои деньги.

Уровень защиты, который биржи готовы предложить своим клиентам, может зависеть от страны их регистрации и требований лицензии к биржам (или их отсутствия) в этой юрисдикции. Еще раз повторимся: в любом случае хранить биткойны на бирже дольше нескольких дней – это плохая идея. Если по какой-то причине биржа перестала работать, в дальнейших своих действиях вы должны руководствоваться нормами той юрисдикции, к которой принадлежит эта биржа. В общих чертах, чем более строгим лицензионным правилам соответствует биржа, тем более высоким будет уровень защиты, который вам здесь смогут предложить. Однако всегда следует уточнять детали соглашения с биржей и выяснять, какой уровень защиты они могут или не могут предложить. Само собой, вы можете инициировать судебный процесс, если случится самое худшее, но следует знать, что этот процесс весьма дорогостоящий и трудоемкий.

Все больше бирж объявляют свои площадки открытыми для независимых аудиторских проверок. Аудитор может подтвердить, что биржа заслуживает доверия и может продолжать функционировать, а в случае необходимости готова подвергнуть свою систему безопасности стресс-тесту, чтобы доказать, что данные будут храниться в надежных условиях.

Каждая биржа имеет свою процедуру публикации аудиторских отчетов. Если хотите узнать подробности аудиторского отчета о деятельности выбранной вами биржи, свяжитесь с ее представителями через чат или почту. Представитель как минимум обязан сообщить вам, проводятся ли на бирже аудиторские проверки и где публикуются отчеты по ним.

Хотите ли вы того или нет, в конечном итоге вся ответственность за распоряжение вашими цифровыми деньгами целиком ложится на вас. Биткойн возвращает финансовый контроль в руки пользователей. И принимая решение хранить свои средства на бирже, вы делаете это под свою ответственность.

Как зашифровать свой кошелек

Безопасность – очень важный вопрос в мире биткойна: без надлежащей защиты ваше цифровое золото может вмиг испариться. Разработчики Bitcoin Core долго думали над решением этой проблемы и придумали функцию в биткойн-клиенте, которая позволяет “зашифровать” кошелек, защитив его ключевой фразой (подробнее о биткойн-кошельках читайте в главе 5).

Bitcoin Core – это стандартный биткойн-клиент для пользователей компьютеров. Многие другие программные биткойн-кошельки основаны на приложении Bitcoin Core, но предлагают для него разные интерфейсы и некоторые дополнительные функции.

Выбор ключевой фразы

Выбрав ключевую фразу, вы “запираете” свои биткойны в кошельке, после чего их нельзя потратить, не зная этой фразы. Даже если злоумышленник получит доступ к вашему устройству, на котором установлен биткойн-клиент, он все равно ничего не сможет сделать с вашими активами, если только вы не сообщите ему ключевую фразу.

Ваша приватная биткойн-информация хранится в файле wallet.dat, который подтверждает ваше право собственности на биткойны – и этот файл изначально не зашифрован. Это означает, что, если вы только что установили биткойн-клиент на свой компьютер или ноутбук, ваши данные еще не защищены по умолчанию. В

такой ситуации злоумышленник, получив доступ к вашему компьютеру или ноутбуку, сможет запросто тратить ваши биткойны.

Поэтому следует предусмотрительно зашифровать свой биткойн-кошелек. Последняя версия клиента Bitcoin Core содержит опцию, которая позволяет зашифровать кошелек с помощью не просто пароля, а более длинной ключевой фразы. Или, если желаете, вы можете воспользоваться внешним инструментом, чтобы зашифровать файл wallet.dat – большинством подобных инструментов можно воспользоваться бесплатно. Не забывайте, что ключевую фразу теперь нужно будет вводить каждый раз, когда вы захотите получить доступ к своим активам. Шифрование биткойн-кошелька делает его доступным только в режиме наблюдения, в котором вы можете увидеть текущий баланс и входящие транзакции, но другие детали недоступны.

Всем пользователям биткойна следует зашифровывать свои биткойн-кошельки, и лучший способ сделать это – использовать надежный и сложный для взлома пароль, предпочтительно содержащий цифры, заглавные и строчные буквы и даже специальные символы, такие как @ или #. Этот пароль должен казаться случайным набором знаков любому, кроме вас, но при этом не забывайте, что вам придется вводить его вручную всякий раз, когда вы решите воспользоваться биткойн-кошельком с полным набором его функциональных возможностей.

Если вы захотите зашифровать мобильный биткойн-кошелек, процесс будет несколько иным. Большинство мобильных приложений сохраняют файл wallet.dat (или его мобильный аналог) на самом устройстве, а защитить его, как правило, предлагают с помощью PIN-кода. Несмотря на го что PIN-коды в основном менее надежны, чем коды шифрования, для большинства пользователей такой уровень защиты кажется достаточным. Однако существуют и другие способы шифрования мобильных кошельков. Попробуйте ввести в свой любимый поисковик ключевые слова 7Zip, Axcrypt, TrueCrypt или Irzip, а затем подыскать программное решение себе по вкусу.

Опасайтесь вирусов!

Всем пользователям биткойна следует помнить о том, что вне зависимости от того, зашифрован ли ваш кошелек, абсолютно надежной и безопасной виртуальной среды не существует.

У большинства биткойн-пользователей уже установлены антивирусы, но когда они начинают сохранять на свой компьютер финансовые данные, в том числе касающиеся биткойнов, требуется больше слоев защиты.

Пользователям компьютеров необходимо защититься от всех вредоносных программ и средств. Предустановленного антивируса отныне недостаточно, особенно если вы пользуетесь биткойн-кошельком. Вам понадобятся профессиональные защитники от вредоносных кодов и шпионов, которые легко найти в Интернете: Bitdefender, Kaspersky и Norton Antivirus. Имейте в виду, что все приведенные примеры называются “антивирусными продуктами”, но обычно содержат расширенный арсенал средств защиты от темных сил в Интернете.

Основную опасность для биткойн-кошельков всего мира представляют вирусы. Вирусы – особенно неприятная разновидность программных кодов, потому что пользователь обычно никак не замечает их присутствия, пока не станет слишком поздно. Существуют разные виды вирусов, каждый из которых потенциально может привести к утрате биткойнов, если не защитить себя специальными программными средствами. Вирус можно подхватить в Интернете, во время посещения сайтов, содержащих вредоносный контент (как правило, это сайты для взрослых), перейдя по неизвестной ссылке, открыв подозрительное письмо или загрузив нелицензионный контент. Каждое из этих действий может быть сопряжено с большой у грозой для компьютера и биткойн-кошелька, поэтому их следует избегать любой ценой.

Не каждое письмо из тех, которые вы получаете, содержит вредоносные файлы или изображения, и не стоит впадать в паранойю из-за каждого неизвестного сообщения. Однако, если вы не знаете, кто отправитель, не открывайте прикрепленные файлы. Небезопасные ссылки сложнее вычислить, так как иногда они распространяются через социальные сети, особенно через Facebook и Twitter, которые весьма склонны к такого рода инфекциям (и вот вы уже на расстоянии одного щелчка мышью от катастрофы…).

Программы-шпионы часто сравнивают с компьютерными вирусами, несмотря на то что между ними есть несколько принципиальных различий. Программа-шпион крадет информацию, например какие сайты, с помощью каких паролей и логинов вы посещали, какие программы установлены на вашем компьютере и какие письма вы пишете и получаете. Это критично важно для людей, использующих биткойн-сервисы в Интернете, поскольку шпион может завладеть личными паролями и извлечь выгоду из этой информации.

Достойный уровень антивирусной и антишпионской защиты, как правило, предлагают программы, которые не распространяются бесплатно, однако большинство из них можно испытать в течение пробного периода. Впрочем, если вы готовы к решающему шагу, хотите взять на себя финансовый контроль и управлять своими деньгами самостоятельно с помощью биткойна, безопасность для вас должна стать приоритетом номер один.

Биткойны в реальном мире

Вместо того чтобы хранить биткойны на компьютере или в телефоне, есть третий вариант, который довольно распространен среди энтузиастов цифровых денег: материальные биткойны. Да, они существуют, и это не просто объекты коллекционирования; они помогают сохранить стоимость цифровых биткойнов. Если точнее, большинство из них выполняет эту функцию.

Существует несколько видов материальных биткойнов, также как и у валют есть монеты различного достоинства. Об одном популярном примере рассказывается во врезке “Биткойн-монеты Casascius” ниже в этой главе.

У каждой материальной монеты есть своя цена, поскольку они сделаны из различных сплавов. Самые распространенные на сегодняшний день биткойн-монеты чеканят из серебра, однако существуют также серии бронзовых, никелевых, титановых и золотых монет – на выбор. Приобретение таких монет предполагает определенные инвестиционные вложения, поскольку их стоимость складывается из цены самого биткойна и цены монеты как объекта коллекционирования.

Материальные биткойн-монеты содержат биткойн-адрес и секретный ключ – под голограммой на оборотной стороне монеты. Получить доступ к секретному ключу невозможно, не повредив голограмму. Поэтому сохранность голограммы является свидетельством того, что средства пока не израсходованы (соответственно, если голограмма повреждена, значит, на эти средства кто-то уже покусился). Проверить биткойн-содержание монеты можно с помощью блокчейн-эксплорера, посмотрев, сколько биткойнов имеется на данном адресе. Все монеты снабжены специальными инструкциями, поэтому, чтобы узнать подробнее об их обеспечении, ознакомьтесь с этой документацией!

Не забывайте, что, владея монетой, именно вы будете ответственны за сохранность ее биткойн-адреса и связанного с ним секретного ключа. Поэтому обязательно позаботьтесь о том, что вы всегда будете единственным человеком, который сможет получить доступ к этой информации на монете.

Биткойн-монеты Casascius

Наверное, самая популярная линейка материальных биткойнов – это монеты под торговой маркой Casascius, придуманные Майком Колдвеллом За несколько лет было создано несколько поколений таких монет – стоимость каждой из них подкреплена цифровым биткойном. Например, материальная монета номиналом 0,5 BTC эквивалентна минимум 0,5 биткойна. За несколько лет, прошедших с момента выпуска этих момент, их коллекционная составляющая сильно выросла в цене. Если вы решите приобрести подобную монету, постарайтесь сильно не переплатить.

Основная причина, по которой монеты Касаскус стали так популярны, состоит в том, что они выпускались

малыми партиями; к тому же наиболее ценные из них были отчеканены из золота или серебра. Кроме того, несколько монет Касаскус были выпущены “с ошибками”, что делает их еще более ценными, с точки зрения коллекционера.

Узнать больше о монетах Касаскус можно, скопировав в адресную строку поисковика ссылку https://bitnovosti.com/2013/12/19/bitcoin-monety-ne-nravyatsa-regulyatoram/.

Многие люди хранят материальные монеты в надежде на то, что их цена в будущем существенно вырастет. К тому же эти монеты нельзя потратить, не повредив голограммы и не вызволив из-под нее секретный ключ.

Инвестиция в материальные биткойны – это хороший способ удержаться от соблазна слишком рано потратить свои биткойны на что-то не очень нужное, о чем впоследствии придется пожалеть.

Покупка биткойнов при личной встрече

Покупка биткойнов при личной встрече – это отличный экскурс в мир цифровых валют. Такая сделка не только введет вас в курс пиринговых взаимосвязей, но и предоставит отличный шанс встретиться с новыми людьми со схожими интересами в области биткойна.

К сожалению, такого рода частные сделки могут привлечь нежелательное внимание в том случае, если в них участвуют наличные. Злоумышленники уже осведомлены о том, что биткойны продаются за большие деньги, и один из участников (тот, который с чемоданом денег) вполне может стать объектом для нападения. Так что важно знать, с кем имеешь дело.

Прежде чем приступить к пиринговым сделкам, вам стоит к ним подготовиться. Пожалуй, самый важный аспект совершения биткойн-сделки – это генерация собственного кошелька. В конце концов, без биткойн-кошелька вам негде будет хранить ваши BTC.

Адрес вашего кошелька

Адрес вашего биткойн-кошелька – это длинная строчка случайных цифр, заглавных и строчных букв. Запомнить эту последовательность практически невозможно. И сделано это преднамеренно. Причина проста: дополнительная безопасность. Если бы кто-то мог запомнить ваш биткойн-адрес, он смог бы найти его в блокчейне и отслеживать там все ваши операции в реальном времени, например через сайт https://www.blockchain.info.

Вы можете создать биткойн-адрес несколькими способами, но если уж речь зашла о пиринговых сделках, то мобильные решения будут в самый раз. Если вы установите любое из многочисленных приложений мобильных биткойн-кошельков на свой телефон, то, скорее всего, генерация вашего адреса будет предусмотрена самой программой. Однако имейте ввиду, что вам, возможно, придется пройти регистрацию, прежде чем начать пользоваться мобильным приложением, и эту часть работы стоит проделать заранее.

Биткойн-адрес генерируется автоматически после установки программы, обеспечивающей работу с этой валютой, на ваш компьютер или мобильный.

Когда вы все уже установили и готовы к действиям, осталась одна маленькая деталь. В процессе пиринговой биткойн-транзакции необходимо будет предоставить партнеру свой биткойн-адрес в какой-то удобной для него форме. Вместо выписывания своего биткойн-адреса (длинной строки случайных символов) на бумаге можно использовать QR-коды. Вы, наверное, видели эти странные черно-белые квадратные коды на фирменных

упаковках, рекламных плакатах или по телевизору. Возможно, ваш банк пользуется ими для аутентификации мобильных платежей. QR-коды – отличное средство для передачи друг другу деталей, необходимых для совершения платежа.

Создав QR-код, вы сможете с легкостью делиться своим адресом с другими пользователями. Все, что нужно сделать другой стороне, – это навести камеру своего мобильного, чтобы отсканировать QR-код в установленный на мобильном устройстве биткойн-кошелек. Все прочие необходимые для завершения транзакции условия выполняются автоматически.

Применение QR-кодов для биткойн-сделок – это очевидное проявление вежливости но отношению к партнерам: так весь процесс занимает гораздо меньше времени, что в целом благоприятно для пользователей. В конце концов, кто захочет носить с собой ноутбук?

Еще одно преимущество использования QR-кодов состоит в том, что продавец биткойнов может показать вам на своем устройстве, что транзакция ушла, и к тому моменту, когда вы проверите свой кошелек, монеты уже поступят на него. Учтите, что каждая биткойн-транзакция требует подтверждения перед тем, как эти деньги можно будет потратить. Любая биткойн-транзакция должна быть подтверждена сетью, прежде чем получатель сможет воспользоваться посту – пившими на его адрес средствами.

Каждый раз, когда в сети обнаруживают блок, примерно раз в десять минут, выполненная перед этим транзакция получает подтверждение. Обычно одного подтверждения вполне достаточно, но если сделка очень крупная, можно подождать и несколько (до шести) подтверждений. В некоторых случаях проходит целый час до того, как биткойны станут доступными.

Различные биткойн-кошельки по-разному отражают прохождение транзакции, несмотря на то что норма – не менее шести подтверждений для транзакции до того, как средства можно будет начать перемещать дальше. В главе 6 читайте об этом подробнее.

Встречи в людных местах

Если речь идет о сделке “из рук в руки”, встречаться для осуществления таких транзакций лучше всего на публике. Это мера предосторожности, актуальная для обеих сторон: дополнительная осторожность никогда не повредит. К тому же найти известное место проще, даже если вы там никогда раньше не были.

Выберите место для встречи, в котором вы будете чувствовать себя безопасно, желательно такое, к которому вы не имеете прямого отношения. Не стоит приглашать продавца к себе домой или на работу, или в те места, где вы часто бываете. В большинстве случаев у участников сделки нет дурных намерений, но никогда нельзя быть уверенным на 100 %.

Другая причина, по которой людные места лучше подходят для биткойн-сделок, заключается в том, что обеим сторонам необходим Интернет. Огромное количество публичных мест наподобие кофеен, предлагают посетителям бесплатный Wi-Fi. Кое-где Wi-Fi-сеть охватывает даже весь город.

И конечно, большинство мобильных провайдеров в США, Европе и Азии готовы предложить вам мобильный Интернет в тех местах, где доступен сигнал сотовой сети. И этот пункт также говорит в пользу встречи в публичном месте, а не в удаленных районах, где сиг нал сотовой сети может быть слабым и ненадежным.

Пиринговая биткойн-сделка – это всегда некоторый риск. Бывали даже случаи, когда биткойн-трейдеров

встречал вооруженный грабитель, требуя отдать биткойны. К счастью, такое случается крайне редко. Следуйте здравому смыслу и проявляйте интерес к деталям, особенно если ваш продавец выглядит или ведет себя как-то подозрительно. Помните: “Береженого Бог бережет”.

Биткойны с наценкой

Покупка биткойнов при личной встрече может обернуться одним большим недостатком: цена, скорее всего, окажется не в вашу пользу. Это означает, что цена, которую заявляет продавец биткойнов, скорее всего, окажется выше актуального биржевого курса.

Не все пользователи; желающие продать биткойны, имеют правильное представление об актуальной рыночной стоимости этих монет на ключевых торговых площадках. Проверка биржевого курса перед заключением пиринговой сделки – полезная привычка. Она не только поможет вам составить более грамотное представление о том, по каким законам существует рынок биткойнов: с ее помощью вы будете получать максимум биткойнов за свои деньги.

Обменные курсы биткойна колеблются в обе стороны, и нет закона, запрещающего вам устанавливать собственную цену, если вы решите продавать биткойны. В этом одна из самых привлекательных черт свободного рынка биткойнов – каждый волен сам выставлять цены. Покупатели всегда будут стремиться купить настолько дешево, насколько это только возможно, но если цена, выставленная продавцом (пусть и с наценкой), окажется оптимальной на какой-то момент времени, покупатели с удовольствием пойдут на сделку.

Какова будет цена, зависит только от продавца. Схожим образом работают биткойн-банкоматы (см. врезку “Биткойн-банкоматы” ниже в этой главе): 5 % комиссионных сверх текущего курса – далеко не исключение из правил. Одна ко вы можете столкнуться с совершенно разными курсами. Это свободный рынок, в конце концов. Будьте готовы к тому, что цена при пиринговой сделке будет несколько выше – это небольшая жертва, которую придется заплатить, если вы желаете ку пить биткойны с удобством, избежав волокиты с регистрацией на бирже и ожиданием поступления на торговую площадку вашего денежного перевода.

Выбор платежного метода

При совершении пиринговой покупки биткойнов у вас есть выбор платежных методов. Однако, если уж люди условились встретиться лично, они, должно быть, сообщат друг другу, какой платежный метод предпочитают. В большинстве случаев самым удобным средством расчета являются наличные.

И этот пункт подводит нас к черте, которая делает пиринговые биткойн-торги несколько рискованным предприятием. Если вы планируете купить какое-то количество биткойнов стоимостью менее четырехзначной суммы в вашей национальной валюте, все должно быть в порядке. Но не стоит планировать пиринговую сделку, если на кону стоят тысячи долларов, евро или фунтов и биткойны эквивалентной стоимости, – наличный расчет при такой сделке может навлечь на вас неприятности.

Некоторые продавцы принимают банковские переводы, тогда они передадут вам детали своего счета при встрече для оплаты онлайн или через банкомат. Однако этот расчетный метод редко используется по понятным причинам. Если продавца устраивает банковский перевод, то какой смысл затевать личную встречу?

Такие платежные способы, как PayPal или кредитная карта, – неподходящие инструменты для пиринговых биткойн-сделок. Причина проста: платежи через PayPal и платежи с кредитки являются обратимыми, в отличие от биткойн-транзакций. В результате теоретически вы могли бы купить биткойны, используя PayPal или кредитку, а получив монеты, просто отозвать свой платеж. В большинстве случаев платежная система такой запрос удовлетворит. Именно поэтому большинство продавцов биткойнов стараются избежать подобного риска.

Биткойн-банкоматы

Биткойн-банкомат работает, как обыкновенный банкомат, но есть и отличия. С помощью биткойн-банкомата вы можете купить биткойны за свою национальную валюту. Некоторые биткойн-банкоматы позволяют не только покупать, но и продавать биткойны за национальную валюту. Каждый биткойн-банкомат берет фиксированный процент комиссионных, которые могут варьироваться от 0 до 12 %.

Больше информации о биткойн-банкоматах вы найдете здесь: https://en.wikipedia.org/wiki/Bitcoin_ATM.

Горячие кошельки и холодное хранение

Раз уж речь зашла о тортовых площадках для операций с биткойнами, вам следует познакомиться с двумя терминами: горячие кошельки и холодное храпение.

И горячие кошельки, и холодное хранение – это меры безопасности, которые придумали биржи, чтобы избежать потери цифровых монет.

• Холодное хранение означает, что биткойны хранятся офлайн. Этот способ можно сравнить с тем, как банки помещают основную массу вкладов клиентов в надежное хранилище вместо того, чтобы хранить их прямо у кассовой стойки. В случае с биткойнами холодное хранение предполагает больше слоев защиты. Например, биткойны можно хранить на съемном диске или в специальном аппаратном кошельке.

Как вы уже, наверное, догадались, большинство биткойн-кошельков хранят средства на серверах, подключенных к Интернету. Кошельки для холодного хранения отключены от сети практически всегда, что является способом защиты от хакерской атаки на платформу.

Большинство биткойн-бирж стремится защитить своих пользователей от опасностей. Однако на бирже должен поддерживаться определенный уровень ликвидности биткойна (это значит, что часть средств должна быть легкодоступна постоянно), потому что всегда есть пользователи, которые хотят немедленно вывести биткойны. Достойная биржа должна осуществить такой вывод незамедлительно, а не заставлять пользователя ждать несколько часов.

• Горячие кошельки – это способ, с помощью которою биржи держат определенный объем биткойнов наготове на случай, если вдруг последует большая волна выводов. Можно сравнить эти фонды с банковским наличным резервом, который банк должен иметь наготове, чтобы клиенты могли получить доступ к деньгам в любой момент. В отличие от холодного хранения горячий кошелек подключен к Интернету 24 часа в сутки 7 дней в неделю.

Хороший пример для любой биткойн-биржи: никогда не хранить слишком много в горячем кошельке. Даже если в нем хранится всего 1 % всех биткойнов, циркулирующих на бирже, эта сумма вполне может оказаться равной нескольким тысячам BTC. И если вдруг плат форму взломают, потери будут довольно катастрофичными.

По этой причине большинство бирж не станет делать крупные выводы биткойнов из горячего кошелка, а скорее, вы ведет часть средств из холодного хранения, когда получит подобный запрос от пользователя. У каждой платформы есть внутренние лимиты для подобных случаев, что делает затруднительным точное определение понятия крупные суммы (однако, как мы уже говорили, пользователям крупные суммы хранить на бирже вообще не следует).

Защита средств пользователей

Защита пользовательских активов – приоритет номер один для любой биткойн-биржи. Если хотя бы один пользователь пожалуется на то, что он утратил свои средства из-за несовершенной системы безопасности, репутация биржи будет сильно подпорчена. К тому же, как известно, плохие вести всегда распространяются быстрее, чем хорошие.

Для защиты средств пользователей биткойн-биржи используют и другие меры, помимо горячих кошельков и холодного хранения (см. предыдущий раздел), хотя эти два метода – самые распространенные.
Биткойн-площадкам еще есть куда расти в плане безопасности, но несколько ярких умов уже вовсю трудятся над “Стандартом безопасности для биткойн-бирж”.

Этот стандарт призван усилить безопасность разных биткойн-бирж и провайдеров кошельков и утвердить перечень основных требований, которым каждая платформа должна соответствовать. Изначально не все биткойн-площадки уделяли должное внимание безопасности, что привело к многочисленным взломам, кражам и потере многих биткойнов.

На сегодняшний день существует десять стандартизированных процессов, например генерация закрытых ключей, управление холодным хранением и горячими кошельками. Должное внимание в новом стандарте будет уделяться контролю за безопасностью, доказательству резерва и другим вопросам, которые пока не разглашаются.

Вместо того чтобы каждой бирже самостоятельно изобретать стандарт безопасности и защиты пользователей, унифицированный эталон мог бы придать более официальный статус всем площадкам. Подобный структурный подход привел многих к невообразимым историям успеха, которые также являются частью эволюции экосистемы биткойн.

К тому же унифицированный стандарт мог бы сильно помочь регуляторам. За биткойном пристально наблюдают руководящие лица многих стран мира, и мне кажется, что все биткойн-сообщество должно быть заинтересовано в том, чтобы помочь им разобраться в теме. Цель госаппарата – разработать правовую базу для финансовых видов активности в экосистеме биткойна. Если у биткойн-бирж будет единый стандарт безопасности, это сильно упростит задачу обеим сторонам.

Предотвращение хакерских атак

Биткойн-биржи часто становились целью хакеров, прельстившихся блеском цифрового золота. За всю историю биткойна крупные суммы не раз попадали не в те руки, и в большинстве случаев причина этого заключалась в несовершенствах систем безопасности биткойн-площадок.

История крупных биржевых взломов началась с первой атаки на Mt.Gox, токийскую биржу, услугами которой пользовались клиенты со всего мира. Злоумышленники взломали один из администраторских аккаунтов, что немедленно вызвало обрушение цены на биткойн с 32 долларов до нескольких пенни. Однако в тот момент хакеры столкнулись с ограничением на вывод: не более 1000 долларов в день, что и свело все их усилия на нет.

Bitcoinica была популярной биткойн-биржей в 2012 году, но ее репутация сильно пострадала, когда биржа “потеряла” тысячи биткойнов, принадлежавших пользователям. Владельцы биржи дали обещание, что возместят из собственных карманов утраченные средства пользователей. Однако наступил новый день, и еще больше средств исчезло со счетов пользователей. В итоге в истории биржи Bitcoinica не наступила ясность и по сей день. Тот факт, что биржа Bitcoinica была связана с биржей Mt.Gox, никак не повлиял на развитие событий.

В сентябре 2012 года пришел конец еще одной площадке, BitFloor, когда 24 тысячи BTC были похищены с ее счетов неизвестными хакерами. На примере этого взлома вы можете составить представление о том, насколько хлипкими были системы защиты биткойн-бирж в те дни: хакер смог получить доступ к резервному хранилищу ключей от кошельков биржи BitFloor, где они хранились незашифрованными. В конце концов большинство пропавших средств пользователям вернули – правда, в долларах США. а не в биткойнах.

Февраль 2013 стал самой черной полосой для всего биткойн-сообщества – 24 февраля 2013 года биржу Mt.Gox взломали во второй раз и она закрылась уже навсегда. Несмотря на то, что общая сумма пропавших собственных средств компании была небольшой, всего 2000 BTC, из средств клиентов было украдено 750 000 BTC. Расследование о пропаже этих биткойнов ведется до сих пор.

Список взломанных и нечистых на руку бирж можно продолжать и продолжать. В 2015 и 2016 годах от рук хакеров также пострадало несколько бирж. Создание надежной безопасной платформы, на которой пользователи смогут спокойно хранить свои деньги, – непростая задача, а пока процесс усовершенствования безопасности еще не завершен, советуем вам не хранить деньги на бирже на протяжении длительных отрезков времени.

Глава 3. Преимущества и недостатки биткойна

В этой главе…

• Возможности, предоставляемые биткойном

• Поддержание безопасности
• Рост доверия к системам и технологии

У всего есть свои преимущества и недостатки, не так ли? В конце концов, если бы вещи вокруг нас не имели недостатков, мы бы слишком привязывались к ним. Небольшая ложечка дегтя может выступать в качестве баланса и не помешает вам, если вы ее четко осознаете. В этой главе мы рассмотрим обе стороны монеты биткойна.

Преимущества биткойна

Давайте посмотрим на светлую сторону и начнем с перечисления положительных сторон биткойна. Все описанное ниже – мои личные взгляды о преимуществах биткойна. Для себя вы сможете найти другие плюсы в использовании этой цифровой валюты. Так что, повторюсь, в этой главе отражено главным образом субъективное мнение.

Финансовая свобода

Биткойн предоставляет своим владельцам множество преимуществ, но самое главное из них – беспрецедентный уровень свободы. Эта свобода имеет большое количество граней: финансовая свобода, вытекающая из отсутствия необходимости полагаться на существующую инфраструктуру, а также возможность самому контролировать свои средства и используемую технологию.

Использование биткойна для оплаты товаров и услуг – если бы он стал мировой валютой – было бы как минимум не менее удобным, чем использование наличных денег или кредитных карточек. Но при этом вы могли бы полностью контролировать свои деньги. Никто не мог бы указывать вам, где хранить ваши биткойны и что вы можете или не можете с ними делать. Единственным ограничением финансовой свободы в системе биткойна являются стены непонимания, которые мы сами же и строим. Принятие биткойна во всем мире заставит эти стены окончательно разрушиться.

Движение к финансовой свободе

На протяжении всей истории банки и финансовые институты медленно, но верно сплетали кокон вокруг нас, навязывая свои услуги без каких-либо альтернатив. И большинство потребителей не имеют ничего против этого, поскольку они рады придерживаться того, что знают. Ведь если система функционирует, то и чинить ее незачем, не так ли? Биткойну удалось стать жизнеспособной альтернативой, но прежде чем получить настоящую финансовую независимость, нам нужно, в первую очередь, достичь критической массы принятия биткойна.

Под критической массой мы понимаем момент, когда биткойн становится глобальной и широко распространенной формой технологии и финансов. Большинство потребителей все еще не понимают биткойн и не знают, как он может стать частью их жизни. Достаточно сказать, что сегодня биткойн имеет очень “нишевой” рынок, и хотя сообщество растет с каждым месяцем, сторонники этой цифровой валюты составляют лишь очень небольшую долю населения Земли.

Купи биткойн – помоги цивилизации развиться

Существует множество путей, которыми биткойн и лежащая в его основе технология блокчейна помогают нам создавать наилучшую финансовую экосистему. Если бы жители не охваченных банковскими услугами частей мира могли получать зарплату в биткойнах и использовать их для оплаты своих ежедневных покупок, они смогли бы освободиться и получить в свои руки глобальный финансовый инструмент, которого они в данный момент лишены.

Инструменты, которые позволят людям получить контроль над собственными жизнями, все еще необходимо разработать. К примеру, технологию блокчейна можно будет использовать для управления контрактами и хранения всех деталей на виду. Ее можно использовать в выборах, сделав избирательный процесс более

прозрачным и менее подверженным коррупции. Потенциальная польза от применения технологии блокчейна в реальном мире ограничена лишь воображением.

Очевидно, что на основе этой технологии будут разработаны и различные коммерческие решения. С учетом всего этого тот факт, что наименее привилегированные члены общества получат выгоду от личных свобод, что, в свою очередь, улучшит практически все аспекты их жизни, звучит очень заманчиво!

Финансовая свобода не придет сама, если продавцы начнут принимать биткойны в качестве оплаты: в первую очередь, покупатели сами должны захотеть использовать биткойн. Многие магазины – как обычные, так и онлайн – позволяют оплачивать товары и услуги биткойнами, но для достижения финансовой свободы необходимо, чтобы как можно больше покупателей и продавцов предпочли цифровую валюту традиционным платежным средствам.

Главным препятствием здесь является сила привычки: современная финансовая инфраструктура слишком привязала потребителей к себе. В течение последних 50 лет люди привыкли использовать кредитные карточки вместо наличных денег. Следующим эволюционным шагом будут мобильные платежи, которые все еще привязаны к банковским счетам; однако в будущем вам уже не придется носить с собой наличку или карточки.

Осознание нехватки свободы

Еще одна проблема, с которой сталкивается биткойн при попытке дать людям финансовую свободу, заключается в том, что большинство потребителей не видят и не понимают недостатки существующей финансовой инфраструктуры. Между тем во всем мире сейчас нарастает практически неразрешимая проблема неуклонного роста денежной массы, что многие считают признаком приближающегося краха глобальной фиатно-кредитной денежной системы.

Если ФРС США – или, к примеру, ЕЦБ – внезапно решит напечатать больше денег “для разгона экономики”, никто не помешает им это сделать. В результате существующая проблема неуклонною падения ценности фиатных валют не решится; вместо этого увеличится сумма долга. И угадайте, кто будет расплачиваться за этот долг? Правильно, обычные потребители.

Когда денег становится больше, их ценность девальвируется. Это, в свою очередь, требует печати еще большего количества денег, и круг замыкается. Биткойн же защищен от подобной проблемы.

Загоняем себя в беду

Представьте такой сценарий. Допустим, во всем мире находится в обращении миллион долларов и Федеральная резервная система принимает решении напечатать дополнительный миллион долларов, чтобы “стабилизировать экономику”. Вы можете подумать, что из-за увеличенного вдвое количества денег их общая покупательная способность возрастет, но на самом деле это не так.

Теперь в обращении находится два миллиона долларов, но в сумме покупательной способности они дают все тот же “старый” один миллион, ведь от того, что денег напечатано вдвое больше, товаров-то больше не стало. Просто цены на них скорректировали, и каждый доллар теперь стоит в два раза меньше

Удвоение денежной массы для достижения изначальной финансовой ценности только усугубляет проблему, вместо того чтобы решать ее. Изначально находившийся в обращении миллион лишь потерял свою ценность. В конце концов возникает эффект домино, и за одним долгом следует другой и так далее, пока не остаются лишь пустые обещания.

Если такой цикл продолжается, страна может войти в период гиперинфляции, что и произошло в Веймарской республике в 1920-х годах или, например, в Зимбабве на рубеже XX–XXI веков. Таким образом, хотя центральные банки и действуют (мы надеемся) в интересах всеобщего блага, нельзя закрывать глаза на потенциальные проблемы.

Разница между биткойном и фиатными валютами

Описанная во врезке “Загоняем себя в беду” ситуация (можно назвать ее также “Как напечатать себе проблемы”) приводит нас к пониманию основных различий между биткойном и фиатными деньгами, особенно в том, что касается финансовой безопасности. Фиатная валюта, которую вы храните в кошельке или на банковском счете, имеет определенную ценность. К примеру, двадцатиевровая банкнота “стоит” 20 евро. По крайней мере, такую цену называет центральный банк, поскольку у потребителя нет возможности проверить, сколько на самом деле стоит их клочок бумаги.

В случае же с биткойном цену валюты устанавливает свободный рынок. Если этот свободный рынок, состоящий из пользователей биткойна по всему миру, решает, что цена биткойна должна вырасти с 250 долларов до 10 тысяч долларов США, ни одно правительство не может помешать этому случиться. Биткойн – одна из немногих “валют без границ”, которая может как потерять свою стоимость, как фиатные валюты, так и вырасти в цене, как драгоценные металлы.

Цена биткойна сегодня рассчитывается в различных местных валютах, что также является позитивным сигналом. Хотя биткойн и является свободным от границ средством обмена денег, его все еще приходится в большинстве случаев перед использованием конвертировать в местные валюты. Этот уровень финансовой свободы позволяет каждому отправить деньги человеку в любую точку планеты, а получатель, в свою очередь, сможет оставить биткойны у себя или обменять на фиатную валюту по своему желанию.

Биткойн устраняет необходимость в сервисах денежных переводов, таких как Money Gram и Western Union, которые не только устанавливают высокие комиссии, но и требуют предоставления личной информации при каждой отправке или получении платежа. С биткойном же можно оставаться анонимным, что дает пользователям беспрецедентно высокий уровень конфиденциальности по сравнению с банковскими услугами или наличными деньгами.

Освобождаем свой ум

На психологическом уровне ощущение себя свободным от всех препятствий, установленных традиционной финансовой инфраструктурой, дает вам возможность насладиться чистой свободой. Вы и представить себе не сможете, насколько это здорово, пока сами не попробуете! Существует множество способов это сделать, начиная от оплаты каждодневных счетов биткойнами и заканчивая получением зарплаты в биткойнах. В вашем распоряжении есть все инструменты, необходимые для избавления от посредников – банков и подобных им учреждений, и эти инструменты постоянно развиваются и улучшаются.

То же самое можно сказать и в отношении свободы от идеологий, которую дарит биткойн. Даже просто используя его для совершения покупок, вы активно помогаете сети биткойна развиваться и укрепляться. А чем больше людей начнут использовать биткойн, тем больше интереса к нему будут проявлять продавцы, учреждения, правительства и компании, что еще сильнее ускорит развитие сети.

И в будущем это развитие сможет создать для нас лучший мир. Можете называть это эффектом бабочки, но наилучший способ оказать поддержку биткойну – быть активным участником сети и постоянно растущего сообщества.

Безопасность

Когда речь заходит о безопасности, биткойн вызывает горячие споры. Это происходит из-за того, что те же самые аспекты, дающие биткойну его уровень свободы, вызывают у людей озабоченность по поводу безопасности. И это справедливо, поскольку риски безопасности присущи любому финансовому механизму, включая биткойн.

Биткойн не подчиняется желаниям и капризам центральных банков, согласных девальвировать свою валюту с целью “повысить конкурентоспособность экономики”. Таким образом, потенциально биткойн может предложить более безопасную и крепкую схему по сравнению с традиционными финансовыми институтами. С учетом вышесказанного со временем, когда экосистема биткойна достигнет достаточного уровня ликвидности и высокого объема торгов, рынок окончательно определит стоимость биткойна, и никакое государственное

учреждение или группа трейдеров не сможет влиять на цены. Ассоциирующиеся с биткойном услуги всегда дорабатываются с точки зрения безопасности, а будущая работа над технологией блокчейна только повысит общую безопасность сети.

Большинство людей хотят сами контролировать свои финансы, и то же самое относится к владельцам биткойнов. Но если устройства, которые вы используете для осуществления транзакций, недостаточно защищены, никто не поможет вам, когда вы потеряете свои деньги. В случае с биткойном безопасность начинается с самих пользователей доверенные посредники, которые “позаботятся о ваших деньгах”, здесь совсем не обязательны. Конечно, подобные сервисы существуют и в мире биткойна, но при желании можно обойтись и без них. Помните, что биткойн является децентрализованной системой, и то же самое касается безопасности; вы должны осознавать это и брать контроль над ситуацией в свои руки с самого начала.

С технологической точки зрения технология блокчейна (о которой мы расскажем в главе 7), на основе которой работает сеть биткойна, применима во многих сферах. Использование этой технологии предоставит нам гораздо более высокий уровень безопасности – а ведь мы только начинаем открывать ее скрытый потенциал! Простой пример того, как технология блокчейна может повысить безопасность в нашей повседневной жизни – логин без пароля. Для доступа к большинству сервисов или платформ (к примеру, электронной почте) вам обычно нужно вводить имя пользователя и пароль. Технология блокчейна помогает избавиться от системы “логин-пароль”, связав свои аккаунты с биткойн-кошельком. Больше никаких забытых паролей!

Есть и другой пример безопасности, которую сулит нам биткойн. Так, контрафактные товары не дают спокойно спать правительствам всего мира. Эта преступная деятельность приводит к тому, что люди теряют свои деньги и иногда даже здоровье. Благодаря технологии блокчейна мы сможем отслеживать процесс производства любого товара и проверять его подлинность. Захотят ли правительства всех стран вводить подобную систему – другой вопрос, на который нам еще только предстоит узнать ответ.

Технология, лежащая в основе сети биткойна, позволяет находить и добавлять множество дополнительных средств безопасности, о которых десять лет назад приходилось только мечтать. Но для развития этой технологии нужно время, и особенно важно, чтобы как можно больше разработчиков стали изучать эти возможности. Сила сети биткойна заключается в силе людей – как обычных пользователей, так и разработчиков, – которые ее поддерживают. Здесь требуется лишь терпение.

Борьба с мошенничеством

Одним из крупнейших недостатков современной финансовой инфраструктуры является риск мошенничества и возвратных платежей.

Мошенничество имеет множество форм – от постельных банкнот до украденных кредитных карт, взломанных аккаунтов PayPal и банковских счетов. Однако существует мошенничество и на принимающей стороне, так как некоторые платежные средства не позволяют вам вернуть свои деньги в случае какой-либо проблемы.

Нельзя никому доверять

Если вы захотите купить что-либо в Интернете на таком сайте, как eBay, или в обычном интернет-магазине, единственными средствами оплаты почти наверняка окажутся кредитные карточки, PayPal и банковский перевод. В этом случае последний вариант окажется наихудшим выбором, поскольку банковские переводы нельзя вернуть.

Чтобы отправить деньги на банковский счет компании, которой принадлежит интернет-магазин, вы должны им доверять. Но вы никогда не можете быть полностью уверены, что по получении ваших денег магазин вышлет вам товар. И если они не сделают этого, вы никогда не сможете вернуть свои деньги, хотя на словах вы и “защищены” своим банком. Звучит странно, не так ли?

Система PayPal – также не самый безопасный вариант. В большинстве случаев он защищает продавцов, хотя его сервис и пропагандирует лозунг “Защита покупателя”. Мошенничество возможно с обеих сторон, поскольку как продавец может получить деньги и не отправить товар, так и покупатель может получить товар и все равно потребовать возврата денег, утверждая, что товар не дошел. Если вы заплатили за товар и не получили его, можете открыть спор; но если продавец предоставит номер отслеживания посылки – даже если он отправил эту посылку пустой – вы ничего не сможете сделать.

Теперь мы плавно подходим к наименее безопасному способу оплаты, который используется как в интернет-магазинах, так и в реальной жизни, – к кредиткам. Кредитная карточка – это кусочек пластика с магнитной полоской, содержащий много конфиденциальной информации, такой как ваши имя, номер карты, срок ее действия, защитный код CVV, пин-код карты. Иногда вся эта информация хранится в специальном чипе, который также находится на карточке.

Главная проблема кредитных карточек заключается в том, что вам необходимо отдать свою карту (или конфиденциальную информацию о ней) для совершения платежа. В некоторых случаях при оплате карточкой у вас могут попросить расписаться на чеке или показать удостоверение личности. Однако все эти способы не слишком безопасны и могут легко обходиться злоумышленниками.

А вот биткойну доверять можно

Транзакцию в сети биткойна нельзя отменить. Как только средства были отправлены на другой адрес – даже если транзакция еще не была подтверждена узлами сети, – вы не можете их вернуть. Это оборотная сторона полного контроля за своими финансами – если что-то пойдет не так, никто не поможет вам вернуть свои деньги.

Всегда проверяйте детали платежа, прежде чем отправить свои биткойны.

Однако эта особенность биткойна особенно привлекает продавцов, которые в противном случае должны полагаться на милость традиционных финансовых институтов. Как только биткойны были перечислены, продавец может приступить к выполнению заказа, не волнуясь о потенциальном мошенническом возврате средств. В то же время биткойн позволяет продавцам возвращать деньги покупателю, к примеру, если товар оказался бракованным, поскольку они знают адрес, с которого была осуществлена транзакция.

Вместо того чтобы полагаться на эмитентов кредитных карточек или банки для осуществления денежного возврата, продавцы могут сами осуществить эту операцию напрямую. Помимо этого, транзакции в сети биткойна проходят значительно быстрее, чем в традиционных платежных системах, что также выгодно и для покупателя, и для продавца.

Биткойн делает многое для предотвращения мошенничества как со стороны покупателя, так и со стороны продавца. Но если вдруг ваш кошелек взломают, ничто не сможет помешать вору потратить ваши деньги. Учитывайте это – в системе биткойна нет центрального регулятора, и поэтому, еще раз повторюсь, конечные пользователи несут полную ответственность за свою безопасность.

Прозрачность

Главное преимущество биткойна – или, если быть точнее, лежащей в его основе технологии блокчейна (см. главу 7) – заключается в полной прозрачности работы системы.

Конечно, для людей и компаний, желающих по какой-либо причине (к примеру, для уклонения от уплаты налогов) избежать прозрачности, это скорее недостаток. Однако открытый характер блокчейна, позволяющий ему выступать в качестве публичной книги записи финансовых транзакций, также открывает возможности по его использованию для хранения файлов, записи прав собственности и даже проверки производственных процессов. Возможности блокчейна ограничены лишь человеческой изобретательностью.

Технология блокчейна и биткойн всегда сосредоточивались на финансовой стороне. И хотя биткойн позволяет практически бесплатно отправить деньги в любую часть мира – и предоставляет возможность отслеживать эту транзакцию вплоть до ее получения, – всем угодить все равно невозможно. Поэтому так важно помнить, что технология Биткойн – это нечто большее, чем просто платежная система. К примеру, на блокчейне вы можете обозначить свои права на автомобиль. Если вы когда-нибудь решите продать его, будет достаточно передать права на владение в цифровом виде, просто отправив их на адрес покупателя. Как только эта транзакция будет завершена и подтверждена узлами сети, покупатель официально вступит во владение автомобилем. Не нужно подписывать никаких бумаг – нужно лишь обменяться ключами и передать цифровой актив, представляющий автомобиль.

Не каждый потребитель хочет, чтобы информация о его финансах была доступна для просмотра любым человеком. Это можно понять, но нужно иметь в виду, что в сети биткойна все псевдонимны – т. е. никто не сможет узнать, кто вы, если вы сами не раскроетесь. К транзакции привязан адрес вашего кошелька, но там нет никакого имени или адреса.

Учтите, что современная финансовая инфраструктура не обеспечивает контроль за использованием ваших средств. Деньги, которые вы храните на банковском счете, выражены лишь набором цифр, которые банк должен вам. Но все знают, что банки используют наши деньги, чтобы создать еще больше денег (хотя мало кто представляет, как это работает). Достаточно знать, что банки играют с нашими деньгами, и, если они потеряют их слишком много, правительству придется вступать в игру и выручать их. Точнее, обычным людям придется выручать банки, если они потеряют деньги, которые мы же им и доверили.

Открытость биткойна и блокчейна приносит много пользы огромному числу людей. Все больше компаний и разработчиков работают над способами использования технологии блокчейна за пределами финансов, и никто не знает, что еще будет изобретено в будущем. Так почему бы не присоединиться к сообществу и не начать использовать биткойн, чтобы посмотреть, к чему все это приведет?

Низкие комиссии

Если что-то в биткойне и улучшает финансовое положение людей по всему миру, так это тот факт, что транзакции в сети можно проводить за очень низкую плату. Обычно это всего несколько центов за перевод любой суммы. Это серьезный вызов традиционной финансовой инфраструктуре, которая берег с нас до 50 долларов за международные денежные переводы (а если речь идет о таких системах, как Western Union, комиссии могут быть еще выше – в зависимости от размера перевода и местонахождения получателя).

Вы можете возразить, что перевозить ценности через границу можно и в виде драгоценных металлов. Однако провоз золота или серебра через границу сопряжен со многими трудностями и расходами и в итоге обойдется еще дороже вышеописанных способов. И, к слову, сколько золотых слитков вы храните у себя дома за шкафом?

И именно в этой сфере биткойн способен поменять расстановку сил. В странах, где открыть банковский счет или получить кредитную карту сложно или вообще невозможно, биткойн сможет оказать особенно большое влияние, предоставив гражданам альтернативный способ осуществления транзакций.

Некоторые компании уже работают в этой сфере, среди их целевых рынков – Африка и Филиппины. В малых масштабах эти сервисы показали себя успешными, поэтому их почти наверняка ждет экспоненциальное развитие на глобальном рынке. А поскольку мы все еще только изучаем потенциал технологии блокчейна, в будущем эта система будет еще неоднократно улучшена.

Поскольку комиссии за транзакции в сети биткойна оплачивает отправитель, получатели платежа также извлекают из этого пользу. Это открывает много путей по снижению издержек на оплату труда компаниями, особенно когда сотрудники работают удаленно в разных странах. Также все транзакции осуществляются практически мгновенно, в то время как при использовании традиционной финансовой инфраструктуры процесс может занять до нескольких недель.

Недостатки биткойна

Биткойн великолепен! Да, мы все это знаем и надеемся, что вы уже готовы начать использовать его прямо сейчас. Но погодите немного: было бы справедливо рассказать и о нескольких потенциальных недостатках этой цифровой валюты.

Осознание и понимание

Заговорите о биткойне с обычным человеком на улице, и, вероятнее всего, вы получите от него следующую

реакцию.

• Он ничего не слышал о биткойне либо знает о нем несколько фактов и неспособен составить полную картину. Недостаток внимания со стороны крупных СМИ является одной из проблем, преследующих биткойн и до настоящего момента. Фактически им интересуются лишь технически продвинутые люди.

• Он думает, что биткойн – это такая кибервалюта для преступников. Он что-то слышал о связи биткойна с онлайн-наркоторговлей, сайтом Silk Road, биржей Mt.Gox или любым другим схожим мошенничеством. Подобные истории были подхвачены СМИ всего мира, в то время как положительные истории, связанные с развитием биткойна, остаются вне поля их внимания.

Продвижение биткойна

Справедливости ради следует заметить, что тематика биткойна прямо-таки нашпигована техническими терминами, особенно что касается особенностей работы технологии блокчейна. Но дело в том, вам вовсе не нужно знать и понимать всю эту технологию, чтобы с успехом ее использовать. Для создания биткойн-кошелька достаточно скачать и установить приложение на компьютер или мобильное устройство. Больше ничего не нужно. (Не верите? Тогда вам следует вернуться к главе 2, в которой рассказывается, как создать свой кошелек.)

И все равно в мире полно людей, которые никогда не слышали о биткойне. А даже если и слышали что-то – неважно, что. – то он не вызвал у них никакого интереса. В результате для биткойна характерна проблема образования, что заставляет аналитиков в один голос твердить: “Он опередил свое время”. Чем больше людей биткойн-энтузиасты смогут убедить использовать эту цифровую валюту, тем известнее она станет и тем больше вырастет.

Пока сторонники биткойна не начнут продвигать его на потребительском уровне, он не получит массового признания. Технологическая сторона уже достаточно хорошо развита стараниями сотен компаний, работающих над различными способами применения биткойна. Теперь пришло время рассказывать случайным прохожим на улице о преимуществах биткойна для всего мира и для них лично.

Встречи с последователями биткойна

Если вы сможете убедить кого-либо попробовать использовать биткойны, за этим, скорее всего, последует эффект домино. Люди быстро убеждаются на практике в его преимуществах, когда сталкиваются с этим лично. Распространение информации о биткойне, которую люди могут понять, осознать и передать другим, – ключ к массовому принятию в будущем. Слава биткойну!

К сожалению, не так просто передать полную и адекватную информацию о биткойне в разговоре или во время презентации. Каждый год в мире проходит несколько достаточно крупных биткойн-конференций, но цена билета на них слишком высока для обычного человека. Большинство выступлений позже появляются в записи в Интернете – в частности, на YouTube, – что, несомненно, является хорошей новостью. Следите за интернет-сообществом, и вы не пропустите ни одной важной новости.

К счастью, по всему миру существуют и локальные группы сторонников биткойна. Они проводят встречи, являющиеся отличным способом познакомиться с единомышленниками, живущими недалеко от вас. Узнать больше об этих встречах вы сможете, заглянув на сайт https://www.meetup.com и набрав слово bitcoin в строке поиска. И даже если в вашем городе не проходят подобные биткойн-встречи, ничто не мешает вам организовать свою. Организация не будет стоить вам ни копейки: встреча может проходить в любом общественном месте, таком как бар или ресторан, где каждый участник будет платить за себя сам. Даже если в выбранном вами пабе не принимают биткойны, люди будут рады встретиться и обсудить общие темы.

Одна из вещей, за которые так мною людей любят биткойн-встречи, – это то, что посещать их можно даже с нулевыми знаниями о биткой не. А рассказывать новичкам обо всех благах, которые принесут нам цифровая валюта и блокчейн, – вообще одно из самых любимых занятий участников этих встреч. При этом старайтесь не перегружать объяснения техническими терминами, чтобы понять их мог любой.

Биткойн может объединять людей из совершенно разных групп, и как только вы найдете общую тему,

разговор пойдет сам собой. Почувствовав, что способны легко объяснить людям суть биткойна и цифровой валюты, вы всегда сможете начать выступать с презентациями. Существует множество возможностей стать спикером. Конечно, этот вариант доступен не каждому: вы должны комфортно чувствовать себя перед большой аудиторией. На биткойн-встречах собираются как правило от 5 до 150 человек, в то время как на конференциях присутствует в среднем от 300 до 500.

Еще важнее не просто сделать презентацию, а найти способ заинтересовать своих слушателей. Здесь общение с аудиторией ничем не отличается от разговора один на один. Убедитесь, что они могут взаимодействовать с вами, а не просто сидеть и слушать.

Как только люди заинтересуются концептом биткойна, они сами захотят узнать больше об этой теме. О биткойне можно рассказать очень много, даже не используя слова “блокчейн” и “технология”! Просто опишите, за что он выступает, вместо того, чего и как он пытается достичь сейчас.

Доверие

Одним из ключевых элементов каждой платежной технологии является доверие. Если вы не доверяете банку, вы никогда не откроете в нем счет и не возьмете кредитную карточку. Вы будете хранить свои деньги наличными где-нибудь в тумбочке. То же самое можно сказать и о биткойне: если вы не доверяете ему, вы не начнете его использовать. “Кто его знает, что из этого выйдет…” Так, скорее всего, вы отреагируете в этом случае на подобное предложение. Чтобы луч-те оценить ситуацию и, возможно, изменить свою точку зрения, обратитесь ко врезке “Доверие современной технологии” ниже в этой главе.

Учитывая количество заголовков в новостях, связывающих биткойн с разного рода мошенничеством, взломами и прочим, можно сказать, что ему еще предстоит преодолеть значительное недоверие со стороны общества. Вместо того чтобы доверять экономической ценности биткойна, важнее оценить то, насколько можно доверять всей его экосистеме. Это включает в себя все связанные с биткойном сервисы, компании, майнинговые пулы, тех, кто сегодня пользуется цифровой валютой, и тех, кто начнет это делать в будущем.

Биткойн все еще находится на заре своего развития. Он существует всего лишь немногим больше шести лет. Как и в случае с любым другим платежным средством, его принятие идет медленными темпами и сталкивается с сильным недоверием. Люди часто забывают, что биткойн не обязательно должен полностью заменить современные платежные средства, но может показать другое, более открытое будущее этих систем.

Задайте себе вопрос “Доверяю ли я современной финансовой (банковской) инфраструктуре, служит ли она моим интересам, надежно ли она хранит мои личные данные и мои деньги?” Если вы не можете утвердительно ответить на этот вопрос, вам стоит обратить внимание на биткойн.

Хотя сегодня финансы большинства людей контролируются институтами, которые уже много раз не справлялись со своими обязанностями, мы все равно доверяем им наши деньги. Причина этого проста: банковские счета и кредитные карты удобны для хранения и передачи денег. Именно так нас учили их использовать. Банки всегда имели монополию на предоставление финансовых услуг, и альтернатив им в истории практически не было.

Но сегодня происходит сдвиг в потребительском поведении, поскольку традиционные финансовые институты все больше и больше стремятся диктовать нам, как мы можем тратить свои деньги и, что самое главное, сколько мы их можем тратить. В большинстве стран банки ограничивают максимальную сумму, которую можно снять через банкомат, величиной 500 или 750 евро. “Но ведь платить за товары и услуги можно не только наличными”, – скажете вы. Это так, существует много других способов оплаты: банковские и кредитные карточки и даже банковские трансферы позволяют ку пить буквально все, и наличные деньги постепенно теряют популярность. Но что если банк решит также ограничить сумму, которую вы можете потратить с помощью этих платежных средств? Или вовсе “заморозить” выдачу денег, как это происходило не так давно на Кипре, в Греции или в Индии?

Традиционные финансовые институты желают как можно дольше хранить ваши деньги, перезанимая их другим людям и зарабатывая на этом. Это одна из причин, по которым банковские переводы идут по нескольку дней: каждый банк хочет в процессе немного их “прокрутить” и заработать на ваших деньгах. Конечно, есть и другие причины, включая врожденную медлительность банковских клиринговых платформ, таких как SWIFT. Хотя панъевропейская платформа SEPA значительно ускорила переводы между европейскими банками, ее эффективность может зависеть от того, как система реализована в конкретных банках-исполнителях.

Нельзя сказать, что это плохо; это обычная бизнес-модель, ничем не отличающаяся от других. Однако жертвой этих задержек становится клиент. Су-шествуют способы ускорить этот процесс, но финансовые институты не хотят ничего менять.

Если быть точным, существует один способ изменить эту систему: объединиться и потребовать изменений. Разве вы не хотели бы, чтобы ваши деньги хранились в открытом гроссбухе, где вы могли бы в любое время их проверить и отправить в любую часть света без задержек и транзакционных издержек? Если вы положительно ответили на этот вопрос, обязательно обратите внимание на биткойн.

Никто не говорит, что вы должны полностью довериться биткойну с первых минут: изучайте его постепенно. Но если вы поймете биткойн и его цели, то сможете принять взвешенное решение, доверять цифровым валютам или нет.

Доверие современной технологии

В наше время нет ничего проще, чем получить доверие со стороны потребителей. Мы слепо доверяем большинству сервисов, которые используем. Социальные сети, такие как Facebook, Twitter и Instagram, хранят много ценной информации о нас, и мы с радостью делимся ею с ними. Почему? Мы достаточно доверяем им и используем их, чтобы с удобством делиться информацией с нашими друзьями и близкими.

Но мало кто отдает себе отчет, что эти компании могут делать с нашими данными. Создавая аккаунт в соцсетях, мы соглашаемся с правилами их использования. А в них обычно указано, что сервис может делиться информаций о вас с третьими лицами в рекламных и иных целях.

И все равно многие из тех, кто слепо доверяет Google, Apple и Facebook, настороженно относятся к биткойну. Этим и отличаются интернет-сервисы, которые не затрагивают напрямую наши деньг и, от интернет-сервисов финансовых услуг. Человеческая натура заставляет нас остерегаться всего нового и сулящего изменения, поскольку мы не слишком любим менять устоявшийся порядок.

Если бы банки имели основанную на блокчейне систему транзакций, денежные переводы по всему миру осуществлялись бы практически мгновенно. С такой системой, к примеру, мигрант из Нигерии, работающий в Лондоне, мог бы отправить зарплату своей семье буквально за несколько минут. Разве это не замечательно?

Риск и волатильность

Биткойн – финансовый инструмент, и ему присущи те же риски, что и другим валютам и платежным средствам. Однако в случае с биткойном эти риски немного отличаются от традиционных валют и платежей. Частично это вызвано высокой волатильностью курса, хотя от этого не застрахована ни одна валюта.

Биткойн и лежащая в его основе технология блокчейна уменьшают риски, характерные для традиционных платежных систем. Здесь нет возврата средств, открытость системы играет злую шутку с мошенниками, а транзакционные издержки очень низки по сравнению с кредитными карточками, банковскими и денежными переводами.

Однако нельзя сказать, что биткойн защищен от всех рисков. Это новая технология, являющаяся одновременно идеологией и платежным средством. Пока вы читаете эту книгу, технология все еще находится в разработке. Мы открываем все новые и новые способы использования блокчейна. Так что, если вы планируете инвестировать в биткойн с точки зрения технологического развития, готовьтесь к определенной доле риска.

Даже лучшие решения и способы его применения не всегда могут оказаться жизнеспособными на практике: их могут просто не принять.

Однако, к счастью, есть и оборотная сторона медали. Развитие технологии блокчейна показывает, что существует еще множество возможностей для развития, которые в перспективе создадут новые рабочие места. Каждое новое технологическое открытие требует людей, которые смогут воплотить его в жизнь и развить, желательно в удобной для пользователей форме.

С технологической точки зрения вы не несете практически никаких рисков, инвестируя в сам биткойн. Другое дело, если вы собираетесь инвестировать в компанию, работающую с этой новой технологией, но этот же принцип касается любой компании, в которую вы готовы вложиться. Инвестиции в биткойн-компании не более рискованные, чем инвестиции в любые другие стартапы.

Совсем другое дело, когда речь заходит о спекуляциях на курсе биткойна. Если вы рассматриваете биткойн с точки зрения инвестиционного инструмента, ценность которого должна вырасти в будущем, то здесь существуют некоторые риски. Спекуляции на волатильности – это плохая идея, а цена биткойна достаточно сильно колеблется изо дня в день.

С момента возникновения биткойна экономисты и инвесторы внимательно следили за его ценой. Начавшись как ничего не стоящий цифровой токен, он постепенно превратился в нечто ценное, как только была достигнута планка в 1 доллар. И хотя цена биткойна продолжила расти и смогла в какой-то момент превысить 1100 долларов в 2013 году, много людей все равно считают его “ненастоящими интернет-деньгами”. Их отношение до сих пор не сильно поменялось.

В то же время в финансовом мире появление биткойна наделало много шума. Инвесторы всего мира скупают биткойны, поскольку считают их более безопасным средством хранения и передачи ценности по сравнению с драгоценными металлами и традиционными платежными средствами.

Ограниченные (пока) возможности использования

Биткойн пока еще не может быть использован в каждом аспекте нашей повседневной жизни, хотя вы уже можете оплатить этой цифровой валютой практически любую покупку. Более того, вы даже можете оплачивать им свои счета, используя сторонние сервисы. Но все это отличается от предполагаемого создателями способа использования биткойна и технологии блокчейна: их главной целью было устранение посредников.

Понадобится еще как минимум несколько лет, чтобы продавцы начали продавать свои товары и услуги за биткойны, не переводя их в обычные валюты. Но прежде чем это случится, биткойн должен быть принят массовым покупателем, а не только узким кругом энтузиастов. Произойдет это только тогда, когда мы начнем обучать людей во всех частях света. К сожалению, сегодня эти образовательные усилия направлены главным образом на развитые рынки наподобие США, где биткойн не сможет радикально повлиять на ближайшее будущее.

Ключевые рынки – Африка, Азия и даже Австралия – были, по нашему мнению, упущены из виду. Хотя Австралия и выглядит странно в этом списке, она является подходящим местом для развития цифровых валют. Азия и Африка же – очевидный выбор из-за их большого потенциала, недостаточного охвата банковскими услугами и технологического героизма.

Несмотря на все это, биткойн можно использовать для оплаты чего угодно, хотя в некоторых случаях придется столкнуться с определенными препятствиями. Хороший пример – дебетовые биткойн-карты, поскольку они позволяют тратить биткойны, используя существующую финансовую инфраструктуру. В то же время, с точки зрения продавцов. – это обычная банковская карточка, так что ее использование не заставит их пересмотреть свое отношение к биткойну.

Аналогично можно оплачивать биткойнами различные счета, хотя большинство предлагающих эти услуги сервисов сегодня ограничены единой зоной платежей в евро (SEPA). Повторимся, это не заставит компании начать принимать биткойны, поскольку для них операция будет выглядеть как обычный банковский перевод. Однако оба эти примера служат другой цели.

Единая зона платежей в евро. SEPA, – это европейские страны, в банках и финансовых институтах которых используется протокол SEPA. Он позволяет гражданам отправлять быстрые банковские переводы в евро (обычно это занимает один-два рабочих дня).

SEPA – это своеобразный предвестник биткойна; он тоже способен изменить современную финансовую систему. В то время как технология блокчейна все еще дорабатывается – и на это уйдут еще многие годы, – биткойн можно легко конвертировать в фиатные деньги и затем оплачивать ими товары и услуги.

В то время как мобильные платежи становятся все более и более распространенными, платежи в биткойнах со временем займут серьезную долю на этом бурно растущем рынке. К слову, мобильные биткойн-кошельки появились даже раньше, чем большинство финансовых институтов разработали свои мобильные приложения. И большинство этих кошельков были значительно доработаны за последние годы, так что сегодня для передачи биткойнов достаточно просто отсканировать QR-код камерой своего телефона.

Что бы ни ожидало нас в будущем, можно быть уверенным, что биткойн (или по крайней мере лежащая в его основе технология блокчейна) сыграет в нем главную роль. Если все пойдет по плану, блокчейн и биткойн станут самыми популярными средствами передачи денег между странами. Более того: биткойн может стать наилучшей формой денег из когда-либо изобретенных человечеством.

Глава 4. Как заработать с помощью биткойна

В этой главе…
- Знакомимся с биткойн-майнингом
- Как привлечь средства с помощью биткойна
- Что такое биткойн-торги
- Как заработать биткойны

В этой главе описаны многочисленные способы получения прибыли с помощью биткойна. Инвестирование в биткойн представляется наиболее очевидным способом, но существуют и другие, менее явные. Не все эти способы требуют серьезных вложений, так что читайте далее и узнайте, какой способ подходит именно вам.

Майнинг биткойнов

Майнинг биткойнов (от англ. mining – добыча руды, горное дело) – это несколько обманчивое название. Никто не стучит киркой по горной породе, чтобы добыть из нее немного биткойнов. Биткойн-майнинг – это на самом деле процесс постепенной эмиссии новых биткойнов в существующую экосистему.

Всего к 2140 году в обращении будет 21 миллион монет, а на момент написания этой книги их уже выпущено приблизительно 16 миллионов.

Как добывают биткойны

Как биткойны вообще появляются на свет? Новые биткойны генерируются в результате вычислительного процесса, известного как биткойн-майнинг. Вы тоже можете майнить биткойны, поручив своему компьютеру просчитывать сложные математические уравнения, – эти задачи можно выполнять в любое время дня и ночи. Начав майнить биткойны, вы становитесь значимой частью биткойн-сети, не только поддерживая ее работоспособность с помощью своего оборудования, но и добывая новые монеты, которые отныне будут

циркулировать в сети.

Этот процесс имеет некоторые сходства с добычей других ресурсов, например золота. Доступный резерв постепенно увеличивается по мере того, как все больше средств вкладывается в процесс добычи. Иными словами, добыча биткойнов – это решение сложных математических задач, и со временем майнинг начинает требовать все больших и больших вложений.

Для того чтобы обеспечить изначально предусмотренную равномерность эмиссии (сегодня выпускается биткойнов не больше, чем вчера и позавчера), процесс майнинга соотнесен с коэффициентом сложности. Этот коэффициент растет по мере того, как все больше вычислительных мощностей присоединяется к сети биткойн, а когда число майнеров падает, коэффициент уменьшается.

Краткая история майнинга

За последние годы майнинг биткойнов пережил колоссальные перемены, хотя бы с точки зрения количества оборудования, необходимого для осуществления этого процесса. Изначально, когда биткойн только появился, в 2009 году, специального оборудования для майнинга вообще не требовалось, поскольку тогда майнинг был еще мало кому интересен. Но по мере того, как все больше людей узнавало о биткойне и присоединялось к сети, вычислительная мощность, необходимая для добычи монет, росла по экспоненте. Коэффициент сложности майнинга (который определяет, сколько необходимо вычислительных мощностей, чтобы решить математические уравнения, позволяющие генерировать биткойны) регулярно меняется для того, чтобы новые блоки биткойнов формировались не чаще, чем раз в десять минут. Новые блоки должны появляться с такой частотой, чтобы можно было собрать все транслируемые за 10 минут транзакции в один блок и подтвердить их все, вместе.

В 2009 году первые версии обычного биткойн-клиента имели встроенную функцию майнинга, которая позволяла каждому пользователю майнить биткойны с помощью центрального процессора на персональном компьютере (главный процессор на компьютере). Поскольку у каждого компьютера есть центральный процессор и всего несколько человек занималось майнингом биткойнов, на тот момент конкуренция среди них была совсем невелика. Можно было просто запустить свой компьютер, установить на него биткойн-клиент, подключиться к сети и сразу начать генерировать новые биткойны. На самом деле первые монеты, сгенерированные в первые месяцы существования биткойна, добыл сам Сатоши Накамото, который также раздал какое-то количество монет всем желающим, чтобы протестировать систему.

Прошло какое-то время, прежде чем один из майнеров сообразил, что для реализации алгоритмов майнинга больше подходит графический процессор, чем центральный. Графические процессоры, которые устанавливают на видеокартах, специально спроектированы для того, чтобы решать сложные математические задачи, поэтому они могут майнить биткойны значительно эффективнее, чем центральный процессор. Однако сдвиг в плане производительности повлек за собой значительный рост энергозатрат, так как графический процессор потребляет существенно больше энергии, чем центральный процессор. Эта замена знаменовала собой окончание первого этапа в долгой и многоэтапной истории гонки биткойн-вооружений.

После этого разработчики и инженеры решили, наконец, приступить к проектированию устройства, способного майнить биткойны значительно эффективнее и быстрее, чем графические и центральные процессоры. Спустя пару лет на свет появился первый чип – Программируемая пользователем вентиль-пая матрица (ППВМ, FPGA), – который по производительности майнинга явно превосходил обычные центральные процессоры. Важно отметить, что эти микросхемы позволяли майнить биткойны так же быстро, как и графические процессоры того времени, но потребляли при этом гораздо меньше электричества.

Читая об истории майнинга тех дней, часто можно встретить термин, который у многих вызывает вопросы: ASIC, или специализированная прикладная микросхема. Это микрочип, разработанный специально для майнинга биткойнов. Первые биткойн-ASIC посту пили в продажу в начале 2013 года и настолько превосходили центральные и графические процессоры по скорости и производительности, что многие майнеры, распихивая конкурентов локтями, ринулись покупать эти сверкающие чипы. Однако и у ASIC обнаружились свои недостатки: они потребляют много электричества, сильно шумят и греются. С другой стороны, майнеры на основе ASIC по-прежнему гораздо эффективнее других майнинговых устройств, существующих на сегодняшний день, хотя цена у них отнюдь не низкая.

С появлением подобных устройств потребность в электроэнергии сильно возросла, в результате чего майнинг

биткойнов перестал быть прибыльным занятием в ряде стран мира при отсутствии доступа к дешевой или бесплатной электроэнергии. В большинстве случаев необходимые вложения в майнинговое оборудование и затраты на энергопотребление превращают домашний майнинг в довольно бессмысленное времяпровождение. Впрочем, решение этой проблемы уже найдено: облачный майнинг позволяет майнить биткойны, покупая вычислительные мощности на устройствах, расположенных в другой части света.

Облачный майнинг стал довольно популярен в последние годы. Этот способ позволяет майнить без необходимости покупать и обеспечивать работу собственного оборудования. Большинство сервисов облачного майнинга берут ежедневную или ежемесячную плату за энергопотребление. Облачный майнинг позволяет пользователям начать майнить незамедлительно, не дожидаясь доставки дорогого специализированного чипа. В главе 11 мы расскажем об облачном майнинге подробнее.

В будущем, по мере развития компьютерных технологий, производители микрочипов научатся делать их еще миниатюрнее и без ущерба для вычислительной мощности, а чем меньше чипы, тем больше их может уместиться на плате, тем самым увеличивая майнинговую мощность всего устройства. Инженеры уже вовсю работают над энергоэффективностью чипов, чтобы вновь сделать майнинг прибыльным по крайней мере для каких-то регионов. Узнать о современном состоянии биткойн-майнинга можно из следующего материала: https://bitnovosti.com/2017/02/17/vygodno-li-majnit-bitcoin-v-2017/

Биткойн – торги

Торги на бирже – это один из самых простых и соблазнительных способов получения прибыли с помощью цифровой валюты. Стоимость биткойна волатильна, это означает, что она регулярно колеблется то вверх, то вниз.

Опытные трейдеры успешно зарабатывают, прогнозируя его взлеты и падения. Удачные сделки с биткойнами могут принести немалые деньги, однако, не стоит упускать из внимания, что возможна и обратная ситуация. Играйте на свой страх и риск и ставьте лишь то, с чем готовы расстаться.

Дей-трейдинг за фиатные валюты

Дей-трейдинг (или внутридневная торговля) – это покупка и продажа финансовых инструментов (например, биткойнов) в течение одного и того же биржевою дня. Под фиатными валютами подразумеваются национальные, уза-коне иные правительством средства платежа.

Биткойн позволяет торговать несколькими доступными способами. Наиболее очевидный способ – продажа биткойнов за фиатные валюты и наоборот в тех валютных парах, в рамках которых обмен возможен. Преимущественно люди стремятся держаться рынков основных фиатных валют (USD, EUR), поскольку они генерируют гораздо больший торговый оборот в сравнении с менее известными валютами. На сегодняшний день, кроме долларового и евровалютною, основными биткойн-рынками считаются также Китай и Япония, где BTC торгуется против китайского юаня (CNY) и японской иены (JPY). Обычно это доступно только жителям данных стран. Однако при желании звонок или визит в офис вашего банка может снабдить вас достаточной информацией касательно возможных способов приобретения юаня или иены (если вы хотите поучаствовать в азиатских биткойн-торгах).

Все прочие основные валюты можно с легкостью конвертировать в биткойн и обратно благодаря услугам многочисленных бирж, которые осуществляют конвертацию биткойна (на момент написания книги) в такие валюты, как

- британский фунт,
- канадский доллар,
- российский рубль,
- австралийский доллар.

Если у вас уже есть биткойны, то нет необходимости приобретать какие-либо фиатные валюты, чтобы

приступить к биржевым торгам. Переведите то количество биткойнов, которым вы готовы рискнуть, и приступайте к торгам против выбранной фиатной валюты. Биткойн известен волатильностью своего курса, поэтому победы и промахи будут поджидать вас здесь на каждом шагу. Иногда эти выигрыши и проигрыши будут значительными, иногда наоборот. Такова уж суть дей-трейдинга.

Впрочем, есть и другие варианты, которые предоставляют возможность, помимо прямой продажи или покупки биткойнов, дополнительно спекулировать на валютных рынках. Несколько торговых площадок позволяют играть на повышение и на понижение стоимости биткойна против определенной валюты – они даже принимают транзакции в биткойнах. К ним можно отнести следующие.

- Vaultoro (https://www.vaultoro.com), где биткойны торгуются против золота
- Bitfinex (https://www.bitfinex.com) – биткойны против USD
- Plus500 (https://www.plus500.com)
- Avatrade (https://www.avatrade.com)
- Etoro (https://www.etoro.com)

Несмотря на то что пока не так уж много продавцов принимают к оплате биткойны, те, которые принимают, незамедлительно конвертируют биткойны в фиаты. Это делается с целью обезопасить самого продавца от скачков курса биткойна, которые происходят спонтанно. Благодаря такой возможности многие владельцы бизнеса готовы рискнуть и примкнуть к криптовалютному тренду.

С другой стороны, эти операции с непосредственной конвертацией биткойнов в фиатные валюты имеют и побочный эффект, поскольку предложение порой может перевешивать спрос. Платежным системам, проводящим биткойн-транзакции, необходимо реализовать эти платежи так быстро, как это только возможно, чтобы передать нужную сумму продавцу. В результате на бирже может образоваться несколько увесистых ордеров на продажу, что создает прекрасную возможность заполучить немного недорогих биткойнов.

Следует отметить, однако, что биржевые игры на курсе биткойна – занятие не для слабонервных, и затевать игру стоит с большой осторожностью. Традиционные факторы, влияющие на курсы фиатных валют, также оказывают определенное воздействие и на стоимость биткойна; к тому же очередная афера мошенников или просто некоторое изменение вотума доверия к биткойну способны несколько пошатнуть курс. Тем не менее иногда со стоимостью биткойна происходят такие колебания, которым нет четкого объяснения (в мире биткойна такое случается).

Дей-трейдинг против альткоинов

Итак, после прочтения предыдущего раздела у вас уже есть общее представление о том, что такое внутридневные торги (если вы пропустили его, пролистайте туда, где дается определение этого понятия). Теперь позвольте представить вам альткойны, также известные как альтернативные криптовалюты. Это всевозможные клоны биткойна, его соперники, которых существует великое множество. К тому моменту, когда вы прочтете эти строки, в мире будет существовать более четырех тысяч различных альткойнов.

Если вам не нравится идея торговать или играть против фиатных валют, можете попробовать торговать против альткойнов. Альткойны призваны усовершенствовать те идеи, которые впервые были сформулированы в концепции биткойна. Кому-то, например, нужно больше конфиденциальности, тогда как в иных случаях разработчики этих валют просто стремятся исследовать возможности технологии, лежащей в основе биткойна– блокчейна. При этом вместо того, чтобы предлагать свои усовершенствования разработчикам биткойна, они используют программный код системы Биткойн, меняют ею название, внедряют какие-то мизерные улучшения и выпускают в свет под видом новоиспеченной криптовалюты. Узнать больше об альткойнах можно из следующих материалов: https://bitnovosti.com/2013/11/30/problema-s-altcoinami/, https://bitnovosti.com/2014/04/27/gibel-altcoinov/.

За прошедшие годы лишь дюжине альткойнов удалось удержаться на плаву (пока), в основном благодаря сплоченному сообществу и уникальной комбинации черт, которых еще не было в первоначальной версии биткойна. Однако ни одно из этих сообществ не является таким же большим и сплоченным, как сообщество биткойна. По сути, большинство альткойнов представляют собой самую банальную попытку их разработчиков заработать денег, продавая мечту о “более лучшем биткойне” доверчивым инвесторам. Огромное количество альткойнов просто-напросто исчезло, едва успев появиться. Тем не менее это вовсе не означает, что на рынке альткойнов нет места успешной биржевой игре. Более того, именно по причине их неустойчивости множество биржевых игроков предпочитает работать именно на рынках альткойнов, где всегда есть достаточно возможностей как для быстрого обогащения, так и для стремительного разорения.

Большинство альткойнов разрабатывается, следуя алгоритму pump-and-dump (раскрути и распродай). Это означает, что разработчики создают много шумихи вокруг нового альткойна и обещают новые и уникальные функции. Когда люди слышат столь щедрые обещания, они стремятся купить монеты по низкой цене, что, в свою очередь, подталкивает цену вверх. Лишь очень немногие группы разработчиков алькойнов действительно серьезно работают над своим детищем, имея серьезные цели и не следуя принципам быстрой наживы: это, прежде всего. Litecoin, CasinoCoin и Guldencoin (подробнее о них – в главе 13).

Вместо того чтобы подталкивать цены вверх, скупая монеты самим, некоторые альткойн-разработчики стремятся убедить членов сообщества вложить немалые средства в “бесценный” альткойн, а когда цена вырастает, они сливают свои монеты и тут же приступают к разработке следующего койна.

В мире существует немалое количество альткойнов, и большинство из них никогда не выполнит свое предназначение. Тем не менее, если вам удалось дешево купить несколько монет, пока их цена не взлетела, вы можете неплохо заработать на этом. Но не жадничайте чересчур, потому что цены способны обрушиться быстрее, чем взлетели. Пожалуй, гораздо больше людей “со стороны” потеряли свои деньги на подобных “инвестициях”, чем выиграли. Зато инсайдеры точно в накладе не остались.

Краудфандинг с помощью биткойна

Вместо того чтобы полагаться на одного инвестора или источник финансирования для своего проекта, можно запустить краудфандинговую кампанию, которая позволит децентрализовать процесс финансирования, обрести сторонников и поклонников, которые смогут снабдить вас деньгами наперед. Добавив функцию биткойн-платежей в качестве средства финансирования вашей кампании, вы можете сделать процесс сбора средств еще более распределенным и выйти на мировую аудиторию.

Биткойн предоставляет компаниям и индивидуальным предпринимателям эффективный инструмент сбора средств для будущих проектов. Учитывая тот факт, что в большинстве стран биткойн-активы не облагаются налогами, многие пользователи рассматривают биткойны как безопасное средство безналогового финансирования.

Когда вы конвертируете полученные средства в фиатную валюту, налоги с вас могут стребовать все равно, это зависит от суммы транзакции и других факторов.

Если вы хотите собрать деньги посредством краудфандинга, никогда не заявляйте фальшивых проектов или целей, которых не собираетесь осуществлять. Несмотря на то что биткойн – необратимое средство платежа, вас

все равно вычислят, если вы попытаетесь скрыться с деньгами.

К счастью для биткойн-энтузиастов, большинство краудфандинговых кампаний до сегодняшнего дня оказывались вполне реальными и привели в исполнение большую часть поставленных задач. В некоторых случаях вам может потребоваться больше времени для достижения цели (это зависит от типа проекта, который вы собираетесь реализовать), в особенности если проект предполагает использование блокчейн-технологии.

Однако не все пользователи используют краудфандинговые платформы в благородных целях. Некоторые деятели рассматривают краудфандинг как способ быстрого сбора средств без каких-либо обязательств по возврату. Несмотря на то что большинство площадок предусматривают свои меры безопасности для предотвращения нецелевого использования, всегда остается небольшой шанс, что авторы проекта не смогут выполнить обещанного. Однако это не имеет никакого отношения к биткойну как таковому – такое может случиться с любым краудфандинговым проектом. Взгляните, сколько людей поддержали разные кампании на Kickstarter и так никогда и не получили заранее оплаченных товаров и услуг: www.kickstarter.com/help/stats.

Всякий раз, решив поддержать финансово биткойн-проект, предварительно выясните, какое вознаграждение вам причитается, если оно вообще предусмотрено. Краудфандинг – это не то же самое, что покупка доли компании или продукта по сниженной цене. Ваш взнос в пользу проекта с “народным” финансированием означает лишь то, что вы помогаете кому-то осуществить мечту и за это вам, возможно, будет некое поощрение (а возможно, что и не будет). Впрочем, не стоит принимать участие в краудфандинговом проекте только из-за поощрения. В конце концов, эта система сбора средств была придумана для других целей.

Что такое ICO и IPO: разбор понятий

Первое публичное размещение монет (или ICO – initial coin offering) и первое публичное размещение акции (или IPO – initial public offerings) – это не дроиды из “Звездных войн”, а финансовые термины.

- ICO. Потенциальным инвесторам предоставляется возможность купить часть будущего общего резерва альткойнов еще до начала майнинга. Большинство инвесторов идут на этот шаг в надежде на то, что в ближайшем будущем цена альткойнов сильно возрастет.
- IPO. Публичное размещение акций имеет место, когда биткойн или альткойн-проект рассчитывает привлечь дополнительные средства для своей деятельности. Инвесторы получают долю акций компании, проценты с которой периодически выплачиваются им в виде дивидендов.

Оба термина имеют несколько негативные коннотации в мире биткойн-финансов в связи с недобросовестными действиями мошенников, не раз прибегавших к таким инструментам, как ICO и IPO, а также с обманутыми ожиданиями инвесторов. Однако оба типа финансовых операций вполне могут использоваться и в законных целях.

Например, вы придумали новую область применения блокчейн-технологии и хотите на новой площадке использовать собственный токен (монеты), т. е. вы фактически объявили ICO. За определенную сумму, инвестированную в проект, пользователь получит X токенов, которые он сможет использовать на новой платформе, как только она начнет функционировать. Таким образом, вы предлагаете своим поручителям вполне реальное вознаграждение. Пусть и не овеществленное. Какой стоимостью впоследствии будут обладать эти виртуальные токены, целиком и полностью зависит от успешности вашего проекта. К тому же, поступая таким образом, вы мотивируете своих инвесторов распространять информацию о вашем фандрайзинговом проекте, которому еще предстоит пройти неблизкий путь до того, как он станет успешной платформой.

Вы вовсе не обязаны раздавать цифровые токены тем, кто хочет поддержать ваш проект. Однако инвесторы, как мелкие, так и крупные, больше всего на свете любят получат прибыль от инвестиций, и чем раньше, тем лучше.

Такие финансовые инструменты, как ICO/IPO, могут помочь вам на этом этапе, но в какой степени, зависит от масштабов вашего проекта и последующих событий.

Несомненно то, что, выступая организатором или участником ICO или IPO. вы обрекаете себя на дополнительный стресс. Если вы выступаете в качестве инвестора, вам придется следить за развитием проекта и за тем, чтобы вам вовремя выплатили причитающиеся монеты. Если вы выступаете в качестве разработчика или основателя проекта, вы берете на себя определенные обязательства, в том числе распределение цифровых активов между поддержавшими вас инвесторами.

Любая IPO или ICO связана с большими волнениями и ожиданиями. Даже несмотря на огромный потенциал вашего проекта в будущем, многие инвесторы будут ждать только роста стоимости цифровых токенов, притом желательно сразу после запуска платформы. А у людей, доверивших кому-либо свои деньги, есть одна общая черта: терпение – не их конек.

Доли, акции и дивиденды

Вместо того чтобы предлагать потенциальным инвесторам цифровые токены, вы можете переуступить им долю в своей компании или проекте в качестве компенсации за их инвестиции. Руководствуясь таким подходом, вы вольны назначить за свои акции такую цену, какую пожелаете, но придется предоставить гарантии того, что они представляют собой какую-то ценность.

Дивиденды по акциям могут выплачиваться на еженедельной, ежемесячной или даже ежеквартальной основе. Действуя таким образом, вы мотивируете потенциальных инвесторов распространять информацию о вашей компании, что является бесценной рекламой вашею проекта, какие бы цели вы перед собой ни ставили.

Чтобы сделать свое предложение еще более заманчивым для потенциальных инвесторов, вы можете предложить им выплату дивидендов в биткойнах. Несмотря на го что эти суммы поначалу будут невелики, все равно инвесторы смогут увидеть прибыль от своих первоначальных вложений. Кроме того, такой шаг даст повод для публичною обсуждения компании и ее ближайших планов.

Выплату дивидендов в биткойнах можно опробовать даже с теми инвесторами, которые больше тяготеют к традиционным средствам платежа и не рискуют покупать биткойны самостоятельно. После того как они перечислили вам условленную сумму, вы можете начать выплачивать им дивиденды в биткойнах, чтобы постепенно ввести их в курс дела, – в том случае, разумеется, если они предварительно согласились на такие условия.

10 000 биткойнов за две пиццы?

Вопрос о реальной стоимости биткойна впервые привлек к себе внимание медиа, когда пользователь по имени Ласло на форуме BitcoinTalk (https://www.bitcointalk.org – онлайн форум, где единомышленники обсуждают биткойн) предложил заплатить 10 000 биткойнов за две пиццы. Другой пользователь форума согласился заказать две пиццы из Dominos с доставкой на дом к Ласло в обмен на цифровое вознаграждение.

В тот день в блокчейне была зарегистрирована первая “настоящая” биткойн-транзакция в качестве оплаты за товар и услугу. Это произошло 22 мая 2010 года, и с тех пор этот день, 22 мая, в разных странах мира празднуют как День Пиццы. Многие биткойн-энтузиасты поддерживают традицию и 22 мая обязательно заказывают пиццу и обсуждают последние новости из мира биткойна и блокчейна.

С этого дня люди стали придавать все больше значения потенциальной ценности биткойна и инвесторы стали скупать монеты горстями. Кое-кто из обеспеченных адептов технологии, а именно – братья Уинклвосс (прославившиеся благодаря истории с Facebook), даже задались цепью завладеть 1 % всех биткойнов, находящихся в обращении, и удерживать этот показатель в будущем. Весьма амбициозная цель. Особенно если

принять во внимание, что к 2140 году в обращении будет 21 миллион биткойнов.

Биткойны как инвестиция, в будущее

Биткойн притягивает к себе множество спекулянтов со всего мира. Учитывая то, что стоимость биткойна постоянно колеблется, можно неплохо заработать, если купить их по сравнительно низкой цене в расчете на то, что в будущем их стоимость вырастет.

Не забывайте, что к 2140 году их будет всего 21 миллион, ввиду чего кажется логичным, что их цена со временем возрастет. Верно это предположение или нет – покажет время.

Направляйте свои инвестиции в будущее

Вкладывая деньги в биткойны, вы используете инвестиционный инструмент, хотя этим термином и бросаются часто не по делу. Когда биткойн только появился, некоторые пользователи скупали дешевые монеты в расчете не только на то, что сеть разрастется, но и на то, что цена биткойнов со временем вырастет. Это описание в точности соответствует определению инвестиционного механизма.

Следует сказать, что цена биткойна проделала немалый путь с момента возникновения этой цифровой валюты в 2009 году. Поначалу первые добытые биткойны не стоили практически ничего, и так оно и было на протяжении всего первого года до тех пор, пока сеть не начала расширяться, привлекая в свои ряды все больше заинтересованных пользователей.

Когда интерес к биткойну начал расти, рыночная цена стала медленно, но верно подниматься и пребывала в этом тренде с 2010 по 2013 год. Год 2013 стал особенно важным для биткойна: тогда его стоимость резко рванула вверх и достигла своего предельного максимума на тот период – отметки в 1163 долларов. Как и следовало ожидать, биткойн не смог надолго удержать эту высоту, и вскоре после стремительного восхождения цена его стала падать.

Весь 2014 и начало 2015 года биткойн продолжал падать и падать в цене, невзирая на рост числа продавцов, принимающих к оплате биткойны, а также числа создаваемых кошельков (рис. 4.1). Одни финансовые эксперты посчитали это падение концом биткойна, в то время как другие усмотрели в нем начало нового жизненного цикла революционной цифровой технологии, в процессе которого большинство биржевых спекулянтов смоет за борт. Если придерживаться финансовой терминологии, это был пузырь, который впоследствии лопнул, а цена биткойна вернулась к тем показателям, на которых и была до раздувания пузыря. На момент написания книги по-прежнему непонятно, кто был прав[5]. Ясно лишь одно: слухи о кончине биткойна сильно преувеличены.

Рис 4.1. Падения и взлеты курса биткойна на протяжении первых лет его существования

“Моя прелесть”

Столь многие пользователи вложили разные суммы денег в биткойны в качестве долгосрочной инвестиции, что криптовалютное сообщество столкнулось с новой проблемой: инвесторы, купившие биткойны по очень низкой (или очень высокой) цене держатся за свои сбережения в надежде оправдать свои вложения или получить максимальную прибыль.

При таком количестве монет, изъятых из активного обращения на неопределенный срок, будущее биткойна вызывает опасения. Пока что цена движется по горизонтали, а не по вертикали, и самый насущный спрос, кажется, удовлетворен. С другой стороны, притом, что многие пользователи хранят большое количество монет и держат руку на пульсе, не приведет ли еще одно потрясение к тому, что цена биткойна рухнет до показателей 2012 года?

Как и с любыми другими видами инвестиций, всегда есть шанс, что у кого-то сдадут нервы и это выразится в

сливе активов. Биткойн в этом смысле ничем не отличается от других видов инвестиций. Накопительство, как ни странно, имеет и один благоприятный побочный эффект.

Биткойн – одна из тех цифровых валют, резервный запас монет которой строго ограничен. К тому моменту, когда вы будете читать эти строки, система сгенерирует около 75 % от общего объема биткойнов. Несмотря на это монеты все равно будут в дефиците, поскольку далеко не все из них находятся в обращении.

Таким образом, желающим приобрести биткойны останется не так уж и много монет, что вновь подтолкнет цену вверх. В зависимости от того, по какой цене запасливые пользователи покупали свои биткойны, может пройти немало времени, прежде чем они сочтут разумным продать часть своих накоплений.

Вне зависимости от того, как вы относитесь к этой ситуации, накопительство – это проблема в мире биткойна. Однако не упускайте из внимания, что этой цифровой валюте всего шесть лет отроду и впереди еще много времени для ее развития и признания на мировом уровне. Каким образом в будущем будет решаться проблема накопительства и как эволюция биткойна отразится на его функции инвестиционного инструмента, покажет время.

Актуальную стоимость биткойна можно отслеживать по графику на указанном ниже веб-сайте, чтобы всегда быть в курсе текущей стоимости ваших BTC. Мы рекомендуем вам установить настройку 1W (одна неделя), чтобы получать наиболее релевантную и подробную картинку: https://bitcoinwisdom.com/markets/bitstamp/btcusd.

Как заработать биткойны

Вместо того чтобы покупать биткойны на бирже (см. главу 2), вы можете заполучить их другими способами. Существует несколько способов “заработать” биткойны: с их помощью вы сможете принимать более активное участие в жизни сообщества и узнаете о новых аспектах криптовалюты, которые могут оказаться полезными вам в будущем.

В качестве первого шага следует зарегистрироваться на биткойн-форуме и начать его читать. Ниже приведены два примера наиболее актуальных онлайн-площадок:

- BitcoinTalk (http://bitcointalk.org)
- Bitcoin subReddit (http://www.reddit.con/r/Bitcoin/)

Как зарабатывать на форумах

Большинство онлайн-диспутов, посвященных биткойну, происходят на форуме BitcoinTalk (https://www.bitcointalk.org). Поскольку эта площадка обрела немалую популярность за последние годы, шансы заработать здесь существенно выше. В особенности для новых (и не очень) биткойн-компаний форум BitcoinTalk – это перспективная площадка для продвижения собственного бизнеса.

Если вы смогли приобрести определенный авторитет в сообществе и ваши посты на форумах собирают приличную аудиторию, у вас появляется возможность зарабатывать на продаже рекламного места в своей “подписи”. Блок “подписи” (он размещен в нижней части страницы профиля и отображается вместе с каждым постом, сделанным пользователем) позволяет авторам постов на BitcoinTalk зарабатывать небольшое количество биткойнов всякий раз, когда они пишут осмысленный текст или поднимают важную тему. Человек, организовавший подписную кампанию, отслеживает число постов, сделанных пользователем за неделю, и выплачивает оговоренную сумму в условленное время. Участие в дискуссиях – ваш аргументированный комментарий или ответ – также засчитывается. Если у вас есть вопрос, на который вы хотите получить ответ,

такая публикация также идет в зачет. К тому же вам может быть начислено поощрение за каждый конструктивный ответ к, вашему посту.

Размер вознаграждения за упоминание в блоке “подписи” зависит от многих факторов. Во-первых, компания, кагора я ищет авторов для рекламирования своих услуг, может обладать как большим, так и маленьким рекламным бюджетом, и размер выплат за упоминание в посте зависит от его размера. В одних случаях плата за упоминание близка к нулю, в других – вполне ощутима. Многое зависит от того, какой продукт или услугу компания собирается продвигать и какой отклик от пользователей она получает в связи со своей рекламной кампанией.

Во-вторых, некоторые компании ограничивают количество постов с упоминанием о них, которые вы можете сделать в оплачиваемый период. Оплачиваемый период – это условленный промежуток времени, в ходе которого пользователь может публиковать оплачиваемые посты с упоминанием компании в блоке “подписи”. В большинстве случаев с авторами расплачиваются еженедельно, но компания, рекламирующаяся подобным образом, может указать максимально допустимое число постов с упоминанием в неделю. Любой пост, превышающий максимальное значение, не будет засчитан.

Один из наиболее важных факторов, определяющих, сможете ли вы заработать на подписных кампаниях, – это ваш пользовательский рейтинг на BitcoinTalk. Рейтинг активных пользователей, часто принимающих участие в дискуссиях, вскоре начнет расти. Чем выше ваш рейтинг, тем выше будут выплаты за упоминание в постах.

Легендарные пользователи (с рейтингом активности выше 850) и Героические пользователи (уровень активности – выше 500). как правило, зарабатывают больше всех и вряд ли количество упоминаний в их публикациях ограничивают какими-либо максимумами.

За спам на форуме (слишком короткие сообщения или сообщения не по теме) могут заблокировать профиль пользователя и лишить его права участвовать в рекламных кампаниях.

Больше информации о рекламных кампаниях на BitcoinTalk вы найдете здесь: https://bitcointalk.org/index.php?board=52.0

Как зарабатывать на микротаскинге

Существует несколько платформ, на которых можно получать и выполнять задания с оплатой в биткойнах. Хотите ли вы сделать карьеру в этой среде и получать прибыль в биткойнах – это другой вопрос, однако выполнение небольших задач за биткойны – отличный способ зарекомендовать себя и получить неплохой дополнительный заработок.

К сожалению, большинство подобных задач не принесет существенного дохода, однако некоторые из них способны открыть новые возможности в будущем. А эти возможности, в свою очередь, способны помочь выстроить карьеру, впрочем, подобные случаи – скорее исключения из правил, чем закономерность.

Выполняя задания за биткойны, не следует забывать, что предпочтительно иметь дело только с легитимными компаниями или предпринимателями. Если вы выполняете какое-либо задание для официально зарегистрированной компании, ваши шансы получить свою оплату существенно выше, чем если вы будете иметь дело со случайными пользователями.

Кроме того, имейте в виду, что в мире биткойна не существует понятия предоплаты. Так же, как и со стандартной работой, сначала придется предоставить заказчику товар или услугу, чтобы впоследствии получить оплату. Как правило, стороны не заключают между собой никаких контрактов, поэтому гарантий оплаты также

нет, а значит, будьте внимательны при выборе заказа.

Помимо мелких заданий, существуют вакансии от крупных биткойн-компаний или компаний, исследующих сферу криптовалют – с оплатой в биткойнах. Если у вас есть навыки программирования – предпочтительно на таких языках, как PHP, SQL, JavaScript или C#, – для вас найдется целый ряд вакансий на выбор. Биткойн – это по-прежнему новая индустрия, и многие компании считают, что способны претворить в жизнь эту великую идею. В результате люди, которые смогут сейчас найти себе работу в мире биткойна, будут получать не только зарплату в криптовалюте, но и доли в компаниях (акции). Возможно, вам удастся найти работу на дому, однако большинство позиций требуют личного присутствия, где бы компания ни находилась.

В зависимости от вашего гражданства любой вид доходов в биткойнах может подлежать налогообложению. В каждой отдельно взятой стране этот вопрос будет решаться по-своему. Мы советуем вам проконсультироваться с органами местной администрации или налога-вой инспекцией, чтобы прояснить ситуацию с налогообложением доходов в биткойнах в вашей стране.

Биткойны на халяву: краны

Один из простейших способов заработать частички биткойнов – это так называемые краны. Кран – это веб-сайт, который начисляет пользователям небольшие количества биткойнов за определенный период времени, который может варьироваться от нескольких минут до нескольких дней.

Не рассчитывайте, что разбогатеете за один день, посещая различные биткойн-краны, потому что большинство из них платят совсем ничтожные суммы. Однако, чтобы их получить, делать ничего не нужно.

Биткойн-краны работают по простейшему принципу: раздают небольшие порции биткойнов до тех пор, пока есть рекламодатели, желающие разместить свои баннеры на веб-сайтах кранов (щелчок на рекламном баннере приносит небольшой доход веб-сайту). Микродоли биткойнов быстро разлетаются, и деньги должны откуда-то поступать. В большинстве случаев первые недели или месяцы операторы биткойн-кранов платят посетителям из собственного кармана до тех пор, пока не создадут достаточный трафик, чтобы привлечь рекламодателей на веб-сайт.

Для новичков биткойн-краны – отличное средство получить дробные доли биткойнов. Впрочем, даже если вы потратите целый день на посещение сайтов-кранов, максимум, что вы сможете заработать, – это два-три доллара, так что вам решать, стоит ли вообще тратить на это свое время. В большинстве случаев время оказывается дороже, потому что существуют более продуктивные способы заработать биткойны, такие как рекламные посты или подработка за биткойны (подробнее об этом – в предыдущих разделах).

Больше информации о других способах заработка биткойнов можно найти в этом материале: https://bitnovosti.com/2017/03/01/4-ways-to-get-btc-for-free/

Часть II. Манипулирование биткойном как валютой

В этой части…

• Учимся держать биткойны в кошельках разных типов, которых насчитывается всего четыре.
– Программные кошельки: программные приложения, работающие на компьютерах и отслеживающие движение биткойнов.
– Аппаратные кошельки: физические переносимые устройства, в которые можно “сложить” свои биткойны.
– Бумажные кошельки: в действительности не совсем бумажные и позволяющие хранить биткойны чрезвычайно защищенным образом без подключения к блокчейну (иногда их называют холодными хранилищами).
– Веб-кошельки: сторонние компании, действующие как посредники, обеспечивающие хранение биткойнов клиентов и обслуживание их счетов.
• Выясняем все подробности о транзакциях биткойна, сетевых подтверждениях и сборах
• Углубляемся в технические детали технологии блокчейна и выясняем, чем это может быть нам полезно.

Глава 5. Ваш биткойн-кошелек

В этой главе…
• Как работает биткойн-кошелек
• Типы кошельков
• Правила безопасности при использовании биткойн-кошелька

Если вы прочитали хотя бы одну из предыдущих глав этой книги, то, без сомнения, уже не раз столкнулись с понятием “биткойн-кошелек”. И всякий раз вы, наверное, спрашивали себя “Что это вообще такое – биткойн-кошелек?” Эта глава все прояснит!

Как можно понять непосредственно из названия, биткойн-кошелек – это место, где хранится вся релевантная информация о ваших биткойнах. В биткойн-кошельке можно не только хранить средства, с его помощью можно также получать и пересылать активы, и в этом состоит его сходство с банковским счетом.

Всем, кто входит в мир биткойна и криптовалют, можно без преувеличения сказать, что биткойн-кошелек – это самый важный в мире цифровых финансов объект, оберегать который следует особо тщательно.

Когда вы установите биткойн-кошелек на свой компьютер или мобильное устройство (см. главу 2), программа сгенерирует для вас биткойн-адрес. Биткойн-адрес – это идентификационный номер, под которым вы будете фигурировать в сети Биткойн. Он будет использоваться как номер вашего счета для пересылки и хранения средств.

Что открывают открытыми и закрытыми ключами

За понятием биткойн-кошелька кроется нечто большее, чем просто адрес. Оно подразумевает также открытый и закрытый (или секретный) ключи для каждого из ваших биткойн-адресов. Ваш секретный биткойн-ключ – это случайным образом сгенерированный ряд символов (числа и буквы), знание которого позволяет распоряжаться биткойнами и тратить их. Закрытый (секретный) ключ математически соотнесен с биткойн-адресом, однако воссоздать его исходя из этой связи невозможно благодаря надежному методу шифрования.

Если вы не сделаете копию закрытого ключа и потеряете оригинал, у вас больше не будет доступа к своему биткойн-кошельку и лежащим в нем средствам.

Больше информации о закрытых ключах и используемой в биткойне криптографии можно почерпнуть здесь: https://bitnovosti.com/2014/07/17/tak-chto-zhe-takoe-bitcoin/

Как уже упоминалось, существует еще и открытый ключ, и этот факт иногда приводит к недоразумениям, так как некоторые пользователи поначалу полагают, что биткойн-адрес и открытый ключ – это одно и то же. Однако это не так, хотя математически они связаны между собой. Адрес биткойн-кошелька – это хешированная версия открытого ключа.

Каждый открытый ключ содержит 256 бит информации (простите за математическое отступление), а финальный кеш (ваш биткойн-адрес) – только 160 бит. Открытый ключ используется для подтверждения владения адресом, на который можно пересылать средства. Открытый ключ также является математической производной от закрытого (секретного) ключа, однако вычисление закрытого ключа посредством обратной функции на самом мощном суперкомпьютере займет несколько триллионов лет.

Помимо этих парных ключей и адреса, биткойн-кошелек хранит отдельный регистр ваших входящих и исходящих транзакций. Информация о каждой транзакции, связанной с вашим биткойн-адресом, будет храниться в биткойн-кошельке, чтобы владелец мог проанализировать свои траты и поступления.

И наконец, биткойн-кошелек хранит информацию о предпочтениях пользователя, что также немаловажно. Впрочем, объем информации о ваших предпочтениях зависит от того, каким типом кошелька вы пользуетесь и на какой платформе. Клиент Bitcoin Core, например, не обременен дополнительными настройками, так что новичку будет нетрудно в нем разобраться.

Ваш биткойн-кошелек генерирует мастер-файл, в котором сохраняются все данные. Для пользователей компьютерной версии файл будет называться wallet.dat. На компьютерах с системой Windows он будет автоматически сохранен здесь: C: \User\yourname\Documents\AppData\Roaming\Bitcoin\folder. Обязательно сделайте одну или несколько резервных копий этого файла на других устройствах, например на флешке или карте памяти. Программный кошелек позволит вам снова импортировать этот файл в случае повреждения или утраты оригинала без изменения текущих настроек и финансовой информации.

Больше информации об импорте открытых ключей можно найти здесь: https://en.bitcoin.it/wiki/How_to_import_private_keys. Также, возможно, вам будет интересно ознакомиться с информацией во врезке “О секретных ключах”, ниже в этой главе.

О секретных ключах

Секретный ключ от вашего биткойн-кошелька – это самая важная информация, которую нужно хранить в безопасности и тайне во веки веков. Этот “секретный номер” позволяет тратить биткойны из вашего кошелька, поскольку он подтверждает, что тот, кто знает его, является полноправным владельцем баланса электронной валюты на вашем биткойн-адресе.

Биткойн-кошельку, будь то компьютерная версия или мобильная, может принадлежать несколько секретных ключей, и все они будут храниться 8 файле wallet.dat.

Секретные ключи к биткойн-кошельку обычно представляют собой 256-битовое двоичное число, которое можно представить на бумаге различными способами. Ниже приведен пример закрытого ключа при его записи в шестнадцатеричном представлении. 256-битовый ключ в шестнадцатеричной системе исчисления – это 32 байта или 54 символа, в пределах от 0 до 9 и от A до F. E9 87 3D 79 C6 D8 7D C0 FB 6A 57 78 63 33 89 F4 45 32 13 30 3D A6 1F 20 BO 67 FC 23 3A A3 32 62

Без знания соответствующего закрытого ключа средства, хранящиеся на биткойн-кошельке, потратить невозможно. Восстановить закрытый ключ, зная только открытый ключ и биткойн-адрес, практически нереально, что превращает биткойн в один из самых трудных для взлома алгоритмов.

С другой стороны, чтобы узнать открытый ключ (он же биткойн-адрес), вовсе необязательно знать и

соответствующий секретный ключ. Однако с помощью открытого ключа можно лишь принимать транзакции и проверять текущий баланс. А вот потратить биткойны, хранящиеся в данном биткойн-кошельке, без секретного ключа невозможно.

Если ваш секретном ключ стал известен кому-либо еще, единственный способ защитить содержимое вашего кошелька – это вывести средства на другой, безопасный счет (например, переместить в другой кошелек). Биткойны можно потратить лишь однажды, и транзакции в этой сети необратимы. Это значит, что, когда кошелек опустеет, секретный ключ к нему станет бесполезным

Как пользоваться биткойн-кошельком

Когда вы снимаете бумажные деньги с карты, вам нужно куда-то их положить, как правило, в кошелек или в сумочку. Внимание, сюрприз: биткойны тоже нужно где-то хранить. Где-то, откуда вы сможете легко их достать, когда они понадобятся. Существует несколько разновидностей биткойн-кошельков: программные кошельки, аппаратные кошельки, бумажные кошельки и веб-кошельки (онлайн-кошельки). Биткойн-кошелек можно сравнить с обычным кошельком или сумочкой, вот только в нем нельзя хранить фото детей.

Все биткойны хранятся в огромной базе данных или публичном регистре под названием блокчейн. Биткойн использует программу, которая взаимодействует с блокчейном и позволяет вам проверить свой баланс в любой момент времени. Узнать больше о блокчейне можно, ознакомившись с главой 7, но, рассказывая о кошельках, упомянуть о нем необходимо, так как блокчейн – это хребет биткойна, без него система Биткойн не смогла бы существовать. Каждый биткойн-кошелек сверяется с блокчейном, чтобы подтвердить ваш баланс.

К биткойн-кошельку может быть привязано несколько биткойн-адресов, тогда он будет объединять их для вас в единый интерфейс.

Программные кошельки

Программный кошелек – это приложение биткойна, которое устанавливается на жесткий диск и обеспечивает вам полный контроль и безопасность, поскольку все ваши биткойны будут доступы только через ваш компьютер. Клиент Bitcoin Core был разработан и обслуживается организацией Bitcoin Foundation.

Когда программный кошелек установлен, он создает файл wallet.dat, который содержит данные, относящиеся к вашему биткойн-кошельку.

О том, где взять программный кошелек, читайте здесь: https://bitcoin.org/ru/choose-your-wallet.

Программный биткойн-кошелек – это открытый исходный код (имеется в виду, что его программный код полностью открыт и доступен всякому, кто хочет с ним ознакомиться). Открытый исходный код гарантирует прозрачность и позволяет пытливым пользователям проверять исходники, чтобы убедиться в том, что в них нет вирусов или иных подозрительных кодов, которые могли бы повредить компьютер или нарушить безопасность. Открытый код означает так- же, что если в вас есть сколько-нибудь от технического гения, то вы можете сочинять приложения, подобные кошельку Bitcoin Core, собственными силами (впрочем, большинство из нас – не спецы-разработчики, так что никто от нас этого не потребует).

Синхронизация кошелька

Чтобы убедиться в том, что ваш программный кошелек отображает наиболее актуальную информацию о счете, следует чаще его синхронизировать (технический термин, означающий “обновлять”, “приводить в соответствие”). Различные компьютеры и планшеты реализуют этот процесс по-разному, так что изучите, как синхронизировать эту программу именно на вашем устройстве.

Когда вы впервые загружаете и устанавливаете клиент Bitcoin Core (который придется скачать, чтобы можно

было начать пользоваться программным кошельком), его синхронизация после установки может занять пару дней. Дело в том, что программе необходимо будет загрузить всю историю всех транзакций, начиная с 2009 года до самой последней зафиксированной в блокчейне.

Каждый раз после того, как вы закрыли программный кошелек, выключив компьютер или просто свернув приложение, не забывайте синхронизироваться, когда откроете программу в следующий раз.

Защита кошелька

Клиент Bitcoin Core позволяет зашифровать пароль к кошельку, и мы настоятельно рекомендуем это сделать, потому что даже если кто-либо получит доступ к вашему жесткому диску, без пароля злоумышленникам не добраться до биткойнов. Но если вы установили сложный пароль, то можете спокойно вздохнуть, зная, что ваши биткойны спрятаны так надежно, как это только возможно.

Всякий раз, когда вы захотите потратить биткойны из своего кошелька, программа спросит у вас пароль, который вы использовали для защиты, так что убедитесь в том, что вы способны его запомнить.

Резервная копия кошелька

Создавая новый биткойн-кошелек, не забудьте сделать резервную копию (в самой программе). Затем можно поместить файл с копией на флешку или внешний диск и, если его предварительно зашифровать, спать спокойно, зная, что доступ к биткойнам можно будет восстановить, даже если с вашим компьютером случится что-то неладное.

Несколько биткойн-адресов

При установке биткойн-кошелька программа позволяет генерировать несколько биткойн-адресов, что на практике означает, что у вас могут быть разные адреса для разных типов транзакций.

Аппаратные кошельки

Ряд компаний разрабатывает различные версии аппаратных кошельков, которые позволяют хранить биткойны на отдельном материальном переносном устройстве. Если у вас есть при себе это устройство, все что необходимо сделать, чтобы потратить немного биткойнов, – это подключиться к Интернету, и можно наслаждаться шопингом (или как-то еще использовать их с более благородными целями). Узнать больше об аппаратных кошельках можно здесь: https://bitnovosti.cот/2014/10/20/trezor-bitcoin-safe/.

Бумажные кошельки

Бумажный кошелек в биткойн-реальности означает, что адрес, на котором лежат биткойны, не подключен к блокчейну, а следовательно, он “неактивен”. До того момента как кошелек подключится к блокчейну, биткойны находятся на холодном хранении (биткойн-жаргонизм для обозначения аккаунтов, отключенных от сети).

Вы всегда можете проверить баланс любого биткойн-адреса, заглянув в блокчейн-эксплорер. Но для того, чтобы их потратить, необходимо воссоединить номер на бумажном носителе и адрес кошелька.

Бумажные кошельки считаются наиболее безопасным средством хранения биткойнов, если вы не собираетесь тратить их в ближайшее время.

Биткойны, поступившие на адрес кошелька, будут храниться в блокчейне, но для того, чтобы их потратить, потребуется секретный ключ. Как уже отмечалось, ключ – это просто цифробуквенный ряд символов, который открывает доступ к монетам, хранящимся в вашем биткойн-кошельке и позволяет их тратить. Таким образом, бумажный кошек – это очень надежное средство хранения биткойнов, но на владельца ложится дополнительная ответственность за его сохранность, что актуально для любых финансовых документов.

Прежде чем создать новый бумажный кошелек, убедитесь в том, чтобы ваш компьютер отключен от Интернета: если вы подключены к сети, есть шанс, что программа-вирус сможет перехватить ваши данные,

записать секретный ключ и впоследствии получить доступ к вашим биткойн-монетам.

Ознакомьтесь с приведенной ниже пошаговой инструкцией по созданию бумажного кошелька.

Вот краткое руководство по созданию бумажных кошельков. Сервис, которым мы воспользуемся для этих целей, называется BitAddress.org; это самое простое решение при создании новых бумажных кошельков для хранения биткойнов. В приведенном здесь списке вы найдете пошаговые инструкции, которым необходимо следовать, чтобы за несколько минут создать собственный бумажный кошелек.

1. В окне своего браузера откройте веб-страницу https://bitaddress.org.

Вы увидите экран, похожий на представленный на рис. 5.1 и предназначенный для автоматической генерации новых биткойн-адресов и секретных ключей.

Рис. 5.1. Генерация нового биткойн-адреса

2. Осмотритесь здесь, подвигайте указателем мыши, а затем введите случайный текст в поле ввода. Перемещение указателя мыши и ввод произвольного текстового фрагмента используются, чтобы повысить степень случайности при генерации секретных ключей и адресов.

3. Не сохраняя секретных ключей или QR-кодов, которые предложит программа, сразу же перейдите в этом окне на вкладку Paper wallet. Вид этой вкладки показан на рис. 5.2.

Рис 5.2. Генерация нового биткойн-адреса

4. Выберите на этой вкладке русский язык, а затем в поле Address to generate укажите количество адресов, которые вы хотите сгенерировать. Здесь же, установив флажок Без дизайна, вы при желании можете отказаться от художественного оформления, хотя стандартный шаблон выглядит довольно неплохо.

5. Щелкните на кнопке Сгенерировать. Это запустит процесс генерации указанного количества бумажных кошельков.

6. Чтобы сохранить новые бумажные кошельки, достаточно просто распечатать их изображение на экране. Для этого щелкните на кнопке Распечать. Вы также можете не только распечатать свои вновь приобретенные бумажные кошельки, но и сохранить их на жестком диске в виде PDF-файла. Впрочем, хранить сведения о бумажных кошельках в виде файлов не рекомендуется, лучше и безопаснее всего распечатать эти файлы немедленно после генерации.

7. Чтобы начать пользоваться новым кошельком, отсканируйте QR-код с левой стороны изображения на бумаге с помощью вашего мобильного биткойн-клиента либо введите значение публичного адреса в биткойн-клиент на вашем компьютере. Сделав это, вы сможете начать перемещать биткойны на свои новые бумажные кошельки. Личный ключ, который нужен для подтверждения права на владение аккаунтом и распоряжение хранящимися на нем средствами, зашит в QR-коде с правой стороны.

Crypto-кошелек с картами

Компания Prypto выпустила продукт под названием “Crypto wallet” – кошелек с двумя картами: одна из них – ваш биткойн-адрес, другая – ваш секретный ключ, и обе они покрыты защитной пленкой (если пленка на месте, ключ никто не вскрывал). Это еще одна мера для повышения безопасности хранения ваших биткойнов. Более подробно об этом можно почитать здесь: https://cryptowalletcards.com.

Веб-кошельки

Ряд компаний предоставляют услуги провайдеров для осуществления биткойн-платежей. Они эффективно справляются с функционалом посредников, принимают биткойны на хранение и позволяют с удобством распоряжаться ими, принимая на себя ответственность за управление и безопасность средств пользователей. Кроме того, посредники попросят предоставить личные данные, превращая всю затею в заведомо

неконфиденциальную модель.

Если вы планируете все же воспользоваться услугами посреднической фирмы – провайдера кошельков, убедитесь в том, что эта компания заслуживает доверия. Бывали случаи, когда компании-посредники принимали на хранение биткойны пользователей, а затем внезапно испарялись или подвергались взлому либо разорялись. Например, в феврале 2014 года, основная на тот момент биткойн-биржа Mt.Gox внезапно прекратила все операции и закрылась, а клиенты биржи потеряли все биткойны, хранившиеся на этой площадке. Так что будьте внимательны при выборе. В целом к посредническим структурам, готовым принять ваши биткойны на хранение, еле-дует относиться с осмотрительностью. У правительств стран, где зарегистрированы биткойн-компании, зачастую бывают различные представления о том, как следует регулировать их деятельность и какие требования к ним выдвигать. Поскольку правовая основа регулирования биткойна как финансового сервиса во многих странах все еще находится на стадии разработки, следует выбирать компанию, зарегистрированную в стране с сильной правовой системой регулирования финансовых сервисов, например в США, Великобритании или на острове Мэн. Пока правовое поле вокруг криптовалют окончательно не сформировалось, мы настоятельно рекомендуем отнестись с особым вниманием к вопросу хранения своих средств у посредников – и никогда не хранить больше, чем вы собираетесь потратить в ближайшее время или что вы готовы потерять при наступлений худшего из сценариев.

В сети можно встретить самые различные типы посреднических структур, которые функционируют в качестве провайдеров веб-кошельков. Ниже приведено несколько примеров.

• Биткойн-биржи. Некоторые пользователи предпочитают хранить свои монеты (или их часть) на бирже, что дает преимущество быстрого доступа и возможность быстрой конвертации монет в любую из фиатных валют, например в доллары, фунты или евро, а также в другие альтернативные криптовалюты. Несмотря на кажущееся удобство, мы не рекомендуем вам поступать подобным образом в силу перечисленных выше причин.

• Специализированные провайдеры кошельков. Существуют веб-сайты, предлагающие пользователям выделенные биткойн-кошельки без привязки к биржам.

• Мобильные кошельки. Несмотря на существующее на рынке разнообразие программ-кошельков для мобильных устройств, некоторые компании предлагают еще и веб-кошельки для мобильных устройств.

Управление биткойн – адресами

Биткойн-адрес имеет сходство с адресом электронной почты: его тоже можно использовать для получения и пересылки данных (в данном случае биткойнов). Однако существует и принципиальное различие между ними. Пользователи биткойна, как правило, используют множество биткойн-адресов для получения и отправления транзакций. По сути, желательно использовать новый адрес для каждой новой транзакции, но такая задача не всем покажется осуществимой: многое зависит от частоты использования кошелька. Вопреки расхожему мнению генерация биткойн-адреса даже не требует подключения к Интернету.

Биткойн-адрес – это идентификатор, представляющий собой пункт назначения или отправления биткойн-транзакции. Каждый биткойн-адрес содержит в себе от 26 до 35 цифробуквенных символов и может начинаться с цифр от 1 до 3. Генерировать дополнительный или новый биткойн-адрес можно совершенно бесплатно с помощью предустановленной биткойн-программы, либо можно создать новый биткойн-адрес на бирже или с помощью веб-кошелька.

При наборе биткойн-адреса следует соблюдать регистры и достоверность данных. Биткойн-адрес, как, например, нижеследующий, содержит как строчные, так и прописные буквы в цифробуквенном ряду: lL5wSMgerhHg8GZGcsNmAx5EXMRXSKR3He. Если при вводе в этом (или любом другом) биткойн-адресе заменить строчную букву прописной (или наоборот), то введенный адрес будет недействителен, а значит, и перевод средств станет невозможным.

Существует небольшая вероятность того, что неверный адрес будет принят системой, но это возможно только раз на 4,29 миллиарда транзакций.

Мы советуем использовать новый биткойн-адрес для каждой новой транзакции. Технически нет ничего неправильного в том, чтобы использовать один и тот же адрес снова и снова. Однако применение различных адресов повышает уровень конфиденциальности.

Каждый биткойн-адрес – это выставленный счет для платежа. Как только платеж получен, отправителю нет никакого смысла хранить эту информацию. Однако, если данные кошелька будут утрачены или дискредитированы, все будущие платежи на этот адрес отправятся прямиком в “черную дыру” и будут навеки утрачены для первоначального держателя счета. Используя новый адрес для каждой новой транзакции, вы сокращаете риск возможных потерь.

Как защитить свой кошелек

Так же, как не стоит разгуливать по улицам с торчащим из кармана бумажником или хранить PIN-код от карты на листочке бумаги, вложенном в кошелек, при пользовании биткойн-кошельком следует соблюдать определенные меры безопасности. В этом разделе перечислены советы и рекомендации по защитите своею цифрового имущества.

Защита мобильных кошельков

Мобильный биткойн-коше лек удобен в использовании, потому что его можно установить на планшет или смартфон. Мобильный метод платежа в целом ближе и понятнее среднестатистическому пользователю и не требует дополнительных устройств.

Подключение к Интернету (мобильному или стационарному – не важно) будет большим плюсом при отправлении или получении транзакции на мобильный кошелек. Однако это необязательное условие, поскольку мобильные кошельки позволяют пользователям отправлять и получать средства также через NFC и Bluetooth. В свою очередь, эта особенность делает мобильные кошельки более универсальными по сравнению с компьютерными версиями, за что они и полюбились пользователям.

С точки зрения безопасности мобильные кошельки мало чем отличаются от компьютерных версий. Секретный ключ, позволяющий тратить деньги из вашего кошелька, хранится на самом мобильном устройстве. С одной стороны, эта мера уменьшает шансы на то, что ключ попадет не в те руки.

С другой стороны, эта же мера увеличивает потенциальные риски. Ввиду современного темпа развития технологий и потребительских запросов смартфоны и планшеты очень быстро будут сменять друг друга. Зная о том, что секретный ключ будет храниться в самом мобильном устройстве, при установке мобильного приложения не забудьте сделать резервную копию. Вне зависимости от того, какую версию мобильного кошелька вы предпочтете, функция резервного копирования, как правило, доступна в любой программе.

Копию ключа затем можно экспортировать в облачное хранилище, например в Dropbox или Google Drive, или даже отправить себе по почте. Теперь, после резервного копирования, приложение, которое вы установили,

можно будет начать использовать.

Аутентификация – это важная мера безопасности для предотвращения кражи или нецелевого использования средств со стороны всякого, кто “позаимствует” ваш телефон. Большинство мобильных кошельков оснащены системой PIN-кодов, которая потребует от пользователя ввести 4- или 6-значный код, прежде чем предоставить доступ к кошельку. При многократном вводе неверного кода кошелек будет заблокирован. Владельцу кошелька будет выслано смс или письменное уведомление с инструкциями по разблокировке кошелька.

Говоря по существу, мобильные кошельки предоставляют пользователям оптимальное соотношение удобства и безопасности, но в конечном счете все зависит от самого пользователя. Если пользователь будет обращаться с устройством беспечно, забудет или потеряет секретный ключ, доступ к мобильному кошельку будет утрачен. Биткойн способен предоставить пользователям полный контроль – под личную ответственность, притом во всех ее проявлениях, и своевременное резервное копирование ценных данных – это одно из них.

Стоит ли защищать веб-кошелек

Полагаю, вы теперь с легкостью обнаружите определенные параллели между тем, как работают провайдеры веб-кошельков и такие финансовые структуры, как, например, банки. Оба типа структур временно принимают на хранение ваши личные средства. То есть, если вы передаете деньги на хранение в банк, это означает, что вы ему доверяете, но в биткойне такой принцип не работает. В рамках концепции биткойна понятие “доверие” играло немаловажную роль на всех этапах развития этой парадигмы. Мы убеждены в том, что Сатоши Накамото предвидел, что развитие биткойна в дальнейшем приведет к отказу общества от услуг “доверенных лиц”, и все операции будут осуществляться между пользователями напрямую, в обход посредников.

Сервисы веб-кошельков довольно удобны, но они предполагают огромные риски. Возможность хранить биткойны онлайн и иметь доступ к ним в любую секунду прямо из браузера довольно заманчива, но чтобы воспользоваться ею, пользователю придется поверить на слово в кристальную честность провайдера услуг.

Провайдеры веб-кошельков – это посредники, и они готовы контролировать ваши средства вместо вас. Огромный риск, сопряженный с использованием подобных кошельков, заключается в том, что вы не знаете свой секретный ключ, только адрес. Если этот онлайн-сервис закроется или подвергнется взлому, вы будете лишены возможности сделать что-либо со средствами, хранящимися в таком кошельке.

Помимо того, на вас ложится вся ответственность за безопасность данных собственного аккаунта. Большинство провайдеров веб-кошельков предлагают такую защитную меру, как двухфакторная аутентификация (см. главу 2). И несмотря на то, что эта дополнительная мера в большинстве случаев способна обеспечить защиту аккаунта пользователя, она никак не защитит его средства, если сам сервис будет взломан, поскольку его собственная система была неидеальна.

Если вы уже решили для себя, что впредь хотите самостоятельно управлять собственными средствами, у вас нет причин пользоваться услугами провайдеров веб-кошельков. Как бы ни были удобны эти сервисы, хранить на них деньги – рискованная затея, поскольку, поступая таким образом, вы утрачиваете контроль над своими активами. Вряд ли Сатоши Накамото, проектируя сеть Биткойн, предполагал участие в ней посредников вроде провайдеров веб-кошельков.

Защита бумажных кошельков

Бумажный биткойн-кошелек можно описать как документ, содержащий в себе необходимые данные для генерации секретных ключей, а потому он представляет собой “кошелек для секретных ключей”. Однако это не единственный способ его применения – на бумажном носителе с тем же успехом можно хранить сами биткойны. В этом случае бумажный биткойн-кошелек будет содержать в себе также публичный адрес и

непогашенные коды.

Смысл такого кода заключается в том, чтобы сперва обеспечить его средствами, а затем “погасить”, тем самым использовав средства, проассоциированные с данным конкретным биткойн-адресом. Однако следует помнить, что бумажный кошелек не стоит использовать повторно, потому что он отнюдь не предназначен для повседневного использования.

Бумажные кошельки могут служить для разных целей. Например, это отличный подарок для родственников, друзей и близких, которых вы хотите познакомить с миром биткойна. Их также можно использовать в качестве чаевых или поощрения за хорошо проделанную работу. Для того чтобы использовать подаренный кошелек, человеку, получившему подарок, потребуется установить компьютерную или мобильную версию кошелька на одно из своих устройств, чтобы импортировать в него ключ, ассоциированный с адресом.

К бумажным кошелькам можно относиться по-разному, но это, безусловно, надежный способ хранения биткойнов. Бумажный кошелек не подключен к Интернету, его невозможно взломать, и посредники ему не нужны. Впрочем, это бумажный кошелек, а потому его могут украсть, вода или огонь могут нанести ему повреждения, ею можно потерять или им может воспользоваться кто-то еще. Если вы решите сохранить бумажный кошелек в сейфе или депозитном боксе, это будет надежным решением для защиты средств, но многим такой способ не покажется практичным.

Глава 6. Биткойн-транзакции

В этой главе…

- Узнаем все о биткойн-транзакциях
- Важность подтверждений сети
- Разбираемся с комиссией за транзакции

Идею биткойн-транзакции достаточно легко объяснить. Не правда ли, хорошие новости для начала главы?

Прежде всего, и это самое главное, биткойн-транзакция представляет собой передачу цифровых прав владения определенным количеством BTC в сети Биткойна. Например, если изначально вы владеете пятью биткойнами, а затем отправляете два из них на биткойн-адрес пользователя “Джо”, то в действительности вы передаете цифровое право владения этими двумя BTC кошельку Джо. Оставшиеся три BTC остаются в вашем кошельке, и поэтому вы остаетесь полноправным владельцем этой суммы.

В этой главе описываются основные принципы биткойн-транзакций и даются ответы на некоторые из вопросов, часто задаваемых относительно обмена BTC.

Выясняем, как работают биткойн-транзакций

В самом простом смысле транзакция работает так, что в результате ее выполнения вы передаете другому человеку определенное количество биткойнов из числа тех, которыми владеете.

Чтобы биткойн-транзакция считалась “подлинной”, должен быть по крайней мере один вход (input), хотя вариант с несколькими входами также возможен. Вход является ссылкой на “выход” (output), оставленный предыдущей транзакцией. Запомните, что каждый вход, ассоциированный с биткойн-транзакцией, должен быть непотраченным выходом предыдущей транзакции. Помимо этого, каждый вход в биткойн-транзакции должен быть подписан, что происходит посредством использования приватного ключа, ассоциированного с

инициирующим транзакцию BTC-адресом.

В случае, когда с одной биткойн-транзакцией ассоциированы несколько входов, это будет означать, что присылаемый получателю объем валюты приходит из нескольких биткойн-адресов, генерируемых одним кошельком. Как было указано в главе 5. любой пользователь криптовалюты может генерировать неограниченное количество биткойн-адресов, каждый из которых может хранить неограниченные суммы в BTC.

Вот пример: если вы снова отправите счастливчику “Джо” 2 BTC, 1 BTC будет отправлен с адреса #2 в вашем кошельке, 0,33 BTC отправится с адреса #7, а остаток – будет взят с адреса #8. В данном примере адреса #1, #3, #4, #5 и #6 не имеют биткойнов на балансе, а следовательно, не могут использоваться в качестве “входов”, так как нет неизрасходованных выходов, ассоциированных с этими адресами.

Однако биткойн-транзакция может иметь не только несколько входов, но и несколько выходов. Как вы могли ожидать, несколько выходов указывают на то, что транзакция осуществлялась с целью разделить сумму между несколькими разными адресами. Например, ваш баланс в 5 BTC вы хотите разделить между богачом Джо (2 BTC) и Мэри (1 BTC), а оставшиеся 2 BTC отправить на один из других кошельков, находящихся под вашим контролем. На блокчейне одна эта транзакция будет иметь 3 разных выхода: один пойдет Джо, другой пойдет Мэри, а третий – на биткойн-адрес вашего другого кошелька.

Сумма отправки в биткойн-платеже может быть выражена совокупностью сатоши, самых мелких частиц биткойн-транзакций (8 цифр после запятой). Так как биткойн столь хорошо делится по сравнению с традиционными фиатными валютами, цена 1 сатоши очень изменчива. Сегодня 1 сатоши практически ничего не стоит, однако он может стоить несколько центов – или даже долларов – в будущем, по мере того, как использование биткойна станет популярным трендом. (О динамике курса биткойна рассказано в главе 4.)

Проведение платежей биткойнами и наличными деньгами происходит схожим образом. Общее количество биткойнов, ассоциированное со всеми входами транзакции, может превышать количество биткойнов, необходимое для заключения сделки, что образует “сдачу”. В случае с обычными фиатными валютами сдача выдается покупателю посредством купюр либо монет. В случае биткойн-валюты сдача выдается в форме цифрового права владения на биткойны, ассоциированные с вашим адресом. Если объем биткойнов, хранящихся на адресах-входах, превышает объем, необходимый для отправки на все адреса-выходы, то будет создан дополнительный выход на адрес отправителя, куда и попадет “сдача”.

Могу ли я получать биткойны, когда мой компьютер выключен?

На биткойн часто ссылаются как на вариант интернет-денег не только потому, что он больше всего используется в Интернете, но и потому, что вам необходимо иметь активное соединение с Интернетом, чтобы осуществить биткойн-транзакцию. Однако нет никакой необходимости поддерживать соединение с Интернетом постоянно, даже с целью получения транзакций.

Как только ваши биткойн-адреса в кошельке были сгенерированы, они остаются активными на протяжении вечности – или по крайней мере пока существует блокчейн биткойна. Есть ли у вас синхронизированный биткойн-клиент – на компьютере или на устройстве, – не имеет значения, потому что это не влияет на механизм, с помощью которого вы можете получать биткойн-транзакции на свой адрес.

А вот когда дело касается траты биткойнов, активное интернет-соединение необходимо и для пользователей компьютеров и для пользователей мобильных устройств, поскольку выполняемая транзакция должна быть распространена по сети. Чтобы это выполнить, необходимо иметь соединение с Интернетом, подойдут как Wi-Fi, так и мобильный Интернет. Соединение даже не должно быть быстрым – вам просто необходимо быть в режиме онлайн достаточно долгое время, чтобы отправить транзакцию другим узлам в сети. Обычно весь процесс занимает менее секунды.

Представьте, что вы – получатель в биткойн-транзакции, но не подключены в этот момент к Интернету. Средства все равно будут переведены с адреса отправителя на ваш адрес, так как ваш биткойн-адрес “живет” (и будет жить) на блокчейне во все времена. Просто вы не сможете узнать, что средства были перемещены на ваш

адрес, пока ваше устройство с ПО биткойна снова не будет подключено к Интернету. Когда это случится транзакция появится в вашем кошельке вместе с указанием количества ее подтверждений на текущий момент.

Каждая биткойн-транзакция отслеживается самой сетью и распространяется через разные узлы, чтобы удостоверить свою подлинности. Даже если ваш компьютер или смартфон не подсоединен к Сети на момент осуществления транзакции, трансфер все равно регистрируется блокчейном. Средства от каждого имевшего место перевода отобразятся в вашем кошельке при последующем подключении к Интернету.

Принцип получения биткойн-транзакций офлайн можно сравнить с принципом получения электронных писем, когда вы не за компьютером. Вы не узнаете, что кто-то прислал вам письмо, пока не проверите почту в Интернете с помощью того или иного устройства. Однако, как только вы откроете почтовый клиент – или биткойн-клиент в данном случае, – его информация синхронизируется с сервером (или блокчейном) и любая новая информация, направленная вам, будет получена в считанные минуты.

Существует несколько способов отправить биткойн-транзакцию другому биткойн-пользователю. Прежде всего, вы можете попросить у получателя его биткойн-адрес и отправить деньги через специальное ПО на вашем компьютере или мобильном устройстве. Для пользователей смартфонов есть более простая альтернатива в форме сканирования QR-кода, генерируемого получателем. Любой тип программного обеспечения биткойна позволяет пользователю создавать QR-коды, которые могут включать адреса для отправки средств на них, а также итоговую сумму сделки.

Например, на ваш адрес в кошельке поступило 5 биткойнов на протяжении определенного периода времени, и теперь вы отправляете 2 биткойна Джо. Транзакция будет иметь один вход (нерастраченные выходы той транзакции, через которую вы получили 5 BTC) и создаст два разных выхода во время отправки средств Джо. Первым выходом станет транзакция Джо, ему будет отправлено 2 BTC. Вторым выходом станет транзакция со “сдачей”, которая возвращает неизрасходованные 3 BTC на ваш адрес в кошельке.

Больше информации относительно биткойн-транзакций можно найти здесь: https://bitnovosti.com/2014/07/17/tak-chto-zhe-takoe-bitcoin/.

Получаем подтверждения

Биткойн-транзакциям необходимы подтверждения – они появляются в сети, как только транзакции включаются в новый блок майнерами. (Читайте главу 4 для получения детальной информации о майнерах; это слово является производным от англ, miner – шахтер. Подсказка: кирка и фонарик вам не понадобятся.) Каждый блок, найденный в сети, включает некоторое количество биткойн-транзакций, произошедших чуть раньше. Эти транзакции затем распространяются по сети среди всех биткойн-узлов с целью определения подлинности.

Каждый блок, найденный в биткойн-сети после того, как транзакция была распространена, сможет – при условии, что транзакция подлинная, – предоставить одно сетевое подтверждение. Как уже упоминалось, минимум шесть подтверждений сети необходимо, чтобы “официально” считать биткойн-транзакцию расходуемой (см. следующий раздел).

Подтверждение в мире биткойна означает, что транзакция была признана действительной узлами сети. Без подтверждений транзакция все еще “происходит между” пользователями, и пока на блокчейне не появится некая форма подтверждения, транзакция представляет собой риск для отправителя и получателя. Определенно, транзакциям на подтверждение понадобится время, но это требование в большей степени – мера безопасности, чем просто досадный раздражитель.

Большинство биткойн-кошельков покажут биткойн-транзакцию как “потраченную” (spent), вне зависимости от количества подтверждений сети. Пользователи ПК могут увидеть статус вида “n/unconfirmed”, где n показывает количество подтверждений, полученных транзакцией. Получение шести подтверждений в

большинстве случаев может потребовать до часа времени, хотя бывают и исключения (в сторону увеличения).

Биткойн-клиент не может “заставить” сеть генерировать подтверждения, это действие всецело зависит от майнеров биткойна. Учитывая, что время между появлением биткойн-блоков равняется примерно 10 минутам, не существует способа повлиять на скорость получения подтверждения в период между блоками. Учитывая сказанное, становится понятным, что существует только один решающий фактор, т. е. момент, когда ваша транзакция будет включена в сетевой блок.

Если предположить, что информация о вашей биткойн-транзакция была распространена в сети как раз перед тем, как был найден новый блок, то первое подтверждение может быть получено довольно быстро. Однако, если ваша транзакция будет включена только в следующий блок – а данный процесс является совершенно случайным, – придется ждать чуть больше времени, чтобы получить первое подтверждение.

Главное правило в отношении транзакций следующее: биткойн-транзакция, у которой нет подтверждений, всегда является относительно высоким риском в смысле атаки двойной траты. Говоря упрощенно, двойная трата означает, что биткойн-пользователь может потратить свои средства в биткойн-кошельке дважды (подробнее о двойной трате читайте в главе 10). По факту любая транзакция, у которой еще нет шести подтверждений, несет в себе аналогичный риск. Тем не менее торговцы или платежные процессоры могут устанавливать собственное число необходимых подтверждений. Это правило не касается пользователей, которые пользуются кошельками на ПК, так как средства будут оставаться “неподтвержденными” до тех пор, пока не наберется именно шесть подтверждений сети. Пользователи мобильных устройств, в зависимости от того, какой кошелек они выбрали, обычно могут тратить поступившие им средства значительно раньше.

Обычные шесть подтверждений

Учитывая, что каждое подтверждение транзакции происходит в момент, когда в биткойн-сети найден новый блок – что происходит примерно раз в 10 минут, – шесть подтверждений могут появиться только спустя час. Как только транзакция обрела эти шесть подтверждений, монеты становятся доступными к трате для получателя.

Тот час, за который транзакция будет подтверждена, в общем случае может выступать в роли как благословения, так и проклятья. К тому же ожидание появления шести (или более) подтверждений дает дополнительную уверенность, что транзакция настоящая и что вы не стали жертвой атаки двойной траты на сеть биткойна. В конце концов, транзакции биткойна – не возмещаемые, и согласие на транзакцию, не получившую шести подтверждений, может оказаться финансовой катастрофой для получателя.

Имеются сведения о случаях, когда транзакция набрала шесть подтверждений в течение нескольких часов. Тем не менее подтверждения задерживаются все реже и реже, а время зависит от общей используемой для нахождения блоков вычислительной мощности.

Даже несмотря на то, что транзакция считается “подтвержденной” биткойн кошельком по получении шести и более подтверждений, это совсем не делает ее “подлинной” для протокола биткойна. Когда биткойн был создан, в его протокол была вписана некоторая часть кода, отвечающая за признание новых намайненных монет (найденных блоков) подлинными только после того, как они наберут 100 подтверждений. По факту большинство майнинговых пулов биткойна (как было упомянуто в главе 4) не будут высылать майнерам вознаграждения за блоки, пока не получат 120 подтверждений от сети.

Двойная трата

Сеть биткойна очень безопасна сама по себе, однако всегда присутствует риск двойной траты. С помощью двойной траты, как уже упоминалось, пользователь может потратить одну и ту же сумму дважды. Чтобы уменьшить шансы проведения подобной атаки, сеть биткойна закрепляет каждую отдельную транзакцию с помощью подтверждений.

В общих чертах самый большой потенциал для атак двойной траты появляется, когда торговцы или поставщики выдают товар или деньги сразу, как только транзакция появилась в сети. Эти неподтвержденные транзакции – также известные как транзакции нулевого подтверждения (zero confirmation transactions) – являются основным риском в смысле двойной траты. В результате всем биткойн-пользователям рекомендуется ждать как минимум 6 подтверждений перед тем, как пытаться пересылать полученные средства. Чем больше

подтверждений имеет конкретная транзакция, тем выше шансы, что она подлинная и не является двойной тратой.

Шансы на успешное выполнение двойной граты биткойнов практически равны нулю. Нет системы, которая полностью устойчива к взломам, но протокол биткойна – это другая разновидность технологии, которая потребовала бы достаточно больших усилий для обеспечения успешности атаки двойной траты. Ввиду вышесказанного существует пять потенциальных форм атак, связанных с двойной тратой. О них говорится в следующих подразделах.

“Гонка” (Race attack)

Торговцы и поставщики, принимающие платеж незамедлительно после тою, как заметят “0/unconfirmed”-транзакцию в своем кошельке, открыты к атаке двойной траты, если имела место мошенническая попытка успешно переслать торговцу одну транзакцию, одновременно отправив другую транзакцию, которая тратит ту же монету, запись о передаче которой естественным образом должна была первой попасть в блокчейн.

“Атака Финни” (Finney attack)

Атака Финни – это ложная двойная трата, которая требует участия майнера, как только блок был найден. Риск атаки Финни нельзя ликвидировать, вне зависимости от предосторожностей, предпринятых торговцем, однако необходимы участие майнера и особая последовательность обстоятельств. Таким образом, эта атака не тривиальна, не дешева в исполнении и имеет смысл для атакующего только в том случае, если его ждет существенная добыча.

Атака Вектор76 (Vector76 attack)

Вариант Вектор76 также иногда называют атакой одного подтверждения. Это комбинация атак Гонка и атаки Финни, при которой транзакция, имеющая одно подтверждение, все еще может быть потрачена дважды. Те же защитные действия, которые используются против атаки Гонка, заметно уменьшают риск успешности этой операции.

Брутфорс-атака (Brute force attack)

Атака грубой силы заключается в следующем. Атакующий присылает торговцу/сети транзакцию, которая платит торговцу, и в то же время тайно майнит форк (разветвление, создание ложного дубликата) блокчейна, в котором транзакция двойной траты включается вместо настоящей. После ожидания n подтверждений торговец отправляет товар. Если атакующий сможет найти больше чем n блоков к этому моменту, он останавливает свой форк и получает свои монеты обратно: в другом случае он может продолжить расширять свой форк с надеждой, что сможет поспевать за сетью.

Атака >50 (>50 percent attack)

Также известна как атака 51 процента. Если атакующий заполучил контроль более чем над 50 % мощности сети биткойна, вышеописанная брутфорс-атака имеет гарантированный шанс на успех. Так как атакующий может генерировать блоки быстрее, чем остальные участники сети, он может упорно развивать свой личный форк до тех пор, пока его ветка не станет длиннее, чем та, которая ведется честной сетью, преодолев любые препятствия. Больше деталей по этому вопросу можно найти по адресу: https://en.bitcoin.it/wiki/Double-spending.

Нулевые подтверждения

В мире биткойна назрел тренд: продавцы зачастую даже не беспокоятся о шести подтверждениях, сразу помечая транзакцию как завершенную. Такой отказ от ожидания шести подтверждений повышает шанс стать жертвой атаки двойной траты. Пока сама сеть биткойна не покажет подтверждения для транзакции, считать ее “выполненной” рискованно.

Тем не менее торговцы и платежные процессоры имеют право определять количество подтверждений, необходимое для подтверждения подлинности биткойн-транзакции. Тогда как большинство сервисов видят это

число в пределах трех-шести подтверждений, остальные сервисы действуют, как только транзакция начинает распространяться по сети в своем неподтвержденном состоянии. Это не только позволяет быстрее завершить покупку на вебстраничке, но и вообще ускоряет завершение заказов.

Большинство торговцев, завершающих сделку при нуле подтверждений, продают недорогие или цифровые активы. Например, большинство баров и ресторанов будут считать транзакцию “завершенной” после нуля подтверждений, так как они защищены платежным процессором на случай двойной траты. Платежные процессоры вроде BitPay, BitKassa или Coinbase предоставляют торговцам некоторый вид защиты от двойной траты, даже если установлено нулевое число подтверждений для завершения транзакции.

Биткойн-транзакции нулевою подтверждения являются хорошим средством для бизнесменов и частных лиц получать биткойны быстро и безопасно, несмотря на риски, ассоциированные с таким подходом. Тем не менее раз получатель может подать в суд на платежный процессор с целью защититься от потери средств из-за атаки двойной траты, у него нет никаких причин не установить для своего сервиса нулевое число необходимых подтверждений.

Считаем биткойн – комиссии

На биткойн иногда ссылаются как на глобальную сеть платежей, в которой практически нет комиссий за транзакции. До определенного момента это утверждение верно, однако оно не раскрывает данную тему полностью. Да, получателю любой биткойн-транзакции никогда не придется платить комиссию. Но вот отправителю все же необходимо заплатить комиссию за перевод, чтобы майнеры включили его транзакцию в блок, хотя, как правило, речь идет о небольшой сумме (несколько центов).

От размера комиссии (которую пользователь устанавливает самостоятельно) зависит то, насколько быстро майнеры добавят ее в новый блок, а соответственно, и скорость подтверждения данной транзакции. По факту большинство биткойн-кошельков позволяют пользователю регулировать размер комиссии за транзакцию с целью ее ускорения. Под ускорением мы подразумеваем, что транзакция с прикрепленной небольшой комиссией будет приоритетно включена в следующий сетевой блок, тогда как транзакция с низкой или нулевой комиссией получает самый низкий приоритет и может “застрять” в сети, потому что у майнеров не будет никакого интереса включать ее в блоки.

Существуют некоторые исключения, связанные с включением платы за транзакцию, которые не влияют на скорость выполнения транзакции. В клиенте Bitcoin Core, если ваша транзакция имеет размер меньше 1000 байт, все суммы выходов в ней – от 0,01 BTC и выше и ей присвоен достаточно высокий приоритет, сбор за транзакцию не взимается. Чтобы это правило исключения было применимо, должны соблюдаться все указанные условия. В противном случае в операцию будет добавлена стандартная комиссия за транзакцию в размере 0,0001 BTC за каждую тысячу байтов. Пользователи клиента Bitcoin Core получат соответствующее извещение о том, что с проводимой транзакции будет взята комиссия. В подобной ситуации им предоставляется право согласиться с этим или отказаться от уплаты комиссии. Однако отклонение этой платы снижает приоритетность транзакции и в конечном счете влияет на скорость, с которой для нее будут поступать сетевые подтверждения.

Большинство биткойн-транзакций имеют размер 500–600 байт и в зависимости от выходов могут или не могут облагаться комиссией в 0,0001 BTC. Включение транзакции в сетевой блок происходит случайным образом, однако на нега влияет комиссия (если она необходима). Каждый блок оставляет 50 000 байт места для транзакций с высоким приоритетом (вне зависимости от комиссии за транзакцию (TX)), чтобы они были включены в него (примерно по 100 транзакций на блок). После этого в блок добавляются транзакции, у которых проставлена комиссия в размере 0,00001 BTC/Кб, при этом первыми транзакциями становятся те, у которых

сумма комиссии будет сравнительно выше. Этот процесс повторяется до тех пор, пока размер блока не достигает 1 Мбайт.

Больше информации о размере комиссии за транзакции можно найти здесь:
https://bitnovosti.com/2017/03/29/bitcoin-fee-market/.

Поговорим о скорости транзакции

Приоритет транзакции определяется достаточно сложной математической формулой. Приоритет считается так: это взвешенная по стоимости сумма возраста входов (насколько транзакция стара), разделенная на размер транзакции в байтах. Для достижения лучшего значения взвешенная сумма должна быть более 57 600 000.

Как вы уже могли догадаться, иногда в очереди на распространение находится больше транзакций, чем можно включить в текущий блок. Любые оставшиеся транзакции будут оставаться в пуле транзакций майнера (это коллекция транзакций, которые еще не были подтверждены сетью Биткойна) и будут включены в следующие блоки с приоритетом, вычисленным согласно их комиссиям (если она взимается).

Распространение биткойн-транзакций также зависит от того, была ли назначена для нее комиссия. Процесс распространения транзакций не учитывает, является ли сумма всех выходов транзакции равной 0,01 BTC или более, а лишь проверяет, была ли транзакция помечена как “бесплатная”. “Бесплатной” транзакция помечается в зависимости от того, была ли добавлена комиссия в 0,00001 BTC. Если нет, транзакция помечается как “бесплатная” и получает низкий приоритет.

Больше информации о ретрансляции транзакций можно найти здесь:
https://en.bitcoin.it./wiki/Transaction_fees.

Чем комиссия является для майнеров

Биткойн-транзакции включаются в блоки благодаря майнерам (подробно о майнерах – в главе 4). Отсюда следует, что прикрепление комиссии к каждой транзакции служит стимулом для майнеров включить вашу транзакцию в следующий блок.

Каждая комиссия за транзакцию может рассматриваться как небольшая награда всем майнерам, способствовавшим решению блока, включающего вашу транзакцию (или несколько).

Процесс майнинга биткой на подойдет к концу, когда все монеты будут добыты, что запрограммировано на 2140 год. Предполагается, что далее майнеры будут продолжать заниматься добычей блоков сети (они содержат сведения о транзакциях) в обмен на комиссии, прикрепленные к каждой отдельной транзакции. Разгорелось множество споров относительно этих комиссий и того, стоит ли их увеличивать ради стимуляции майнеров. Так или иначе, пройдет еще много лет, прежде чем консенсус по данному вопросу будет достигнут, так что вам сейчас не стоит об этом волноваться.

Кроме комиссий майнерам, для них нет никаких стимулов подтверждать ваши транзакции. Несмотря на то что никто не обязан добавлять комиссию к транзакции – разве что вашим кошельком предусматривается иное, –

хорошей практикой было бы всегда включать маленькую комиссию ради поддержки сети биткойна и индивидуальных майнеров.

Разбираемся в транзакциях с мультиподписью

Возможно, вы думаете, что конечный пользователь всегда единолично контролирует свои запасы биткойнов в любое время. Тем не менее, поскольку конечный пользователь является единственным лицом, владеющим приватными ключами от адресов, содержащихся в его кошельке, в общем случае должен был быть разработан и более безопасный вариант. Дело в том, что оставлять одному человеку контроль над одним кошельком – вполне нормально, но все становится немного по-другому, когда речь идет о компаниях, семьях или даже друзьях, вместе работающих над проектом. Доверие может рассеяться очень быстро.

Вот как работает типичный биткойн-кошелек. Один пользователь имеет приватный ключ и полный контроль над биткойн-адресом. В этой ситуации, если два или более людей создают проект вместе, у них будет только одна возможность: доверить одному из пользователей приватный ключ от общего адреса в кошельке. И если этот ответственный пользователь захочет вывести все средства в свою пользу, другие ничего не смогут с этим поделать, поскольку у них нет никакого контроля над кошельком.

Ясное дело, этот вариант – далеко не идеальное решение, необходим иной вариант действий, предоставляющий сразу нескольким пользователям контроль над одним кошельком. Следуя этому принципу, со временем была разработана система мультиподписи, при которой несколько пользователей контролируют один кошелек и никто не имеет полного контроля над его содержимым без согласия хотя бы одного другого человека в группе. Эта система известна как аккаунт с мулътиподписями или Multisig-аккаунт.

В противовес обычному биткойн-кошельку биткойн-адреса с мультиподписями требуют наличия нескольких приватных ключей для того, чтобы можно было потратить хранящиеся в них средства. Получение транзакций в такой кошелек с мультиподписью работает точно так же, как в обычном кошельке, просто потому что приватный ключ не используется в процедуре получения средств. А вот в случае отправки средств из кошелька каждая транзакция снабжается цифровой подписью посредством программного обеспечения биткойна на вашем компьютере.

Биткойн-адрес с мультиподписью требует указания “m–из–n” приватных ключей, чтобы разрешить трату средств, ассоциированных с данным отдельным биткойн-адресом. Например, адрес с тройной мультиподписью потребует по крайней мере двух из трех приватных ключей, относящихся к этому адресу: если трое людей создают кошелек с мультиподписью (m = 3), нужны будут по крайней мере две подписи для отправки транзакции (n = 2).

Неспособность предоставить два приватных ключа для подписи транзакции приведет к отказу в отправке транзакции. Биткойн-адреса с мультиподписью предоставляют более высокий уровень безопасности для бизнеса и групп людей, разделяющих общий адрес в кошельке, при этом для одиночных пользователей нет почти никакой разницы между обычным кошельком и его версией с мультиподписями. Так или иначе, для тех из нас, кто всерьез воспринимает проблему безопасности биткойна, было бы неплохой идеей генерировать себе кошелек с мультиподписями, даже для личного использования.

Armory, один из многих доступных пакетов ПО биткойн-клиента, был первым кошельком, внедрившим в систему мультиподписи. Более года назад компания Armory представила свою новую “фишку” Lock Boxes, которая является практической иллюстрацией того, как генерируется биткойн-адрес с мультиподписью.

Детальное видео руководство представлено здесь: https://bitcoinarmory.com/tutoriais/armory*advanced-features/lockbox/create-lockbox/.

Пример использования мультиподписи

В группе из трех человек – Джона, Дилана и Марии – есть три возможные комбинации для достижения согласия двух из трех приватных ключей.

- Джон и Дилан подписывают транзакцию с помощью своих приватных ключей.
- Джон и Мария подписывают транзакцию с помощью своих приватных ключей.
- Дилан и Мария подписывают транзакцию с помощью своих приватных ключей.

Без любой из этих процедур, проведенных правильно, транзакцию вывода биткойнов провести невозможно.

Глава 7. Блокчейн

В этой главе…

- Что такое блокчейн и блоки
- Какой у блокчейна потенциал
- Какое у этой технологии будущее

Блокчейн биткойна представляет собой первое воплощение этой инновационной технологии. В данной главе будут рассмотрены различные составляющие блокчейна биткойна. Прочитав главу до конца, вы будете знать по большей части все, что следует знать о блокчейне и о том, как он взаимодействует с биткойном.

Как всегда, начнем с основ. Что такое блокчейн? Если коротко, блокчейн – это открытый распределенный реестр, предполагающий небывалую прозрачность финансовых операций в рамках экосистемы биткойна. Говоря по-простому, это полный список всех биткойн-транзакций начиная с первой, совершенной в 2009 году. Любая последующая за ней транзакция также зафиксирована в блокчейне. Однако эта технология не ограничивается простой записью транзакций, она способна на нечто гораздо большее.

Блокчейн – это уникальное достижение технической мысли: в его децентрализованной структуре отсутствует центральное управление, которое могло бы поставить всю систему под удар.

Чтобы узнать больше о принципах работы блокчейна, посмотрите это видео, где данный вопрос рассматривается подробно: https://www.youtube.com/watch?v=mcuwRUDOFRg.

Запись транзакций

Один из самых часто задаваемых вопросов по теме – “Почему эта технология называется блокчейном?” Чтобы понять, почему это так, сперва следует разобраться, что такое блок. Если бы блокчейн действительно был обычной бухгалтерской книгой, то первый блок транзакций разместился бы на первой странице. Каждый новый блок в сети биткойна содержит хеш предыдущего блока (краткую последовательность цифр и букв). В результате с тех пор, как в 2009 году появился первый блок (его еще называют генезисным), в биткойн-сети формировалась непрерывная цепь транзакций в составе блоков. С помощью этих блоков путь любой транзакции можно отследить вплоть до генезисного блока

Если вернуться к аналогии с реестровым журналом, то каждая новая страница начиналась бы с краткого описания предыдущих страниц, поэтому размер страниц со временем пришлось бы увеличивать. Эта метафора сейчас стала весьма актуальной для блокчейна, который неимоверно разросся из-за объема хранимых в нем данных.

Блокчейн биткойна получил широкую известность именно как открытый реестр: это означает, что он фиксирует все биткойн-транзакции в прошлом, настоящем и будет фиксировать в будущем. Блокчейн – это не только журнал бухучета, это невероятно прозрачная финансовая экосистема. И именно эта степень прозрачности системы расчетов внушает опасения традиционным финансовым институтам. Им не нравится раскрывать свои данные и информацию о денежных операциях, в то время как биткойн не дал бы им возможности скрыть эту информацию. Впрочем, в системе все же существует определенная прослойка конфиденциальности, так как и индивидуальные пользователи, и компании представлены только номером своего биткойн-адреса, а вовсе не именем и физическим адресом.

Блокчейн биткойна с финансовой точки зрения представляет собой распределенную базу данных, содержащую информацию обо всех транзакциях. Каждый биткойн-узел (компьютер, непрерывно подключенный к сети и работающий как программный биткойн-коше-лек, фиксируя и подтверждая транзакции) в сети Биткойн хранит полную копию всей истории биткойн-транзакций с самого начала (2009) до настоящего момента. В будущем все больше и больше транзакций будет добавляться к существующему блокчейну, формируя тайм-лайн эволюции биткойна в мире финансов.

К тому же каждый новый биткойн-блок хронологически упорядочен, поскольку содержит в себе хеш предыдущего блока. Если хеш отсутствует, сеть не примет такой блок. Более того, предыдущие блоки биткойна невозможно изменить, потому что это означало бы, что придется изменить и все последующие блоки. Функция редактирования в блокчейне недоступна и никогда не будет доступна.

В результате того, что в открытом регистре фиксировались все биткойн-транзакции начиная с 2009 года и до того самого момента, когда вы читаете эту книгу, блокчейн существенно вырос в размерах. К тому моменту, когда вы прочтете эти строки, размер блокчейна уже превысит 100 (байт. Учитывая то, что все больше и больше транзакций транслируется в сеть Биткойн, размер блока со временем придется увеличивать, а файл с блокчейном станет еще объемнее.

Анализ в блокчейне

В 2014 году в мире биткойна и блокчейна стал выкристаллизовываться новый тренд. Блокчейн-анализ – это совершенно новый рынок, формирующийся в рамках экосистемы биткойна: его появление стало возможным исключительно благодаря прозрачным свойствам блокчейна. Чем станет блокчейн-анализ, проклятием или спасением для биткойна, еще предстоит разобраться, потому что на данный момент мнения разделились.

Наблюдая за тем, на что люди тратят свои биткойны (не только за тем, какие товары и услуги чаще покупают, но и как долго в среднем они хранят биткойны, посту пившие к ним на кошелек), можно способствовать эволюции биткойна в основное средство расчетов. Биткойн задумывался как подобное наличным платежное средство, которым можно будет воспользоваться где у годно в любой момент времени. Проанализировав, как долго пользователи обычно хранят свои средства на счетах, сообщество способно помочь распространению биткойна в разных частях мира. Для этого может пригодиться и блокчейн-анализ.

Позитивные стороны блокчейн-анализа распознать несложно. Биткойн – по-прежнему юная и незрелая финансовая система, и детальный анализ даст экспертам ценную информацию о том, что следует сделать, чтобы система перешла на следующий уровень.

- На что тратят биткойны?
- Где создают много новых кошельков?
- Проблема накопительства отступает или становится актуальнее?

Все эти вопросы заслуживают достойных ответов, и здесь на помощь приходит блокчейн-анализ.

Ни для кого уже не секрет, что “старейшие” биткойны, зарегистрированные в системе, никуда не перемещались годами. Одни полагают, что они принадлежат Сатоши Накамото, создателю биткойна, другие – что это монеты первых пользователей, которые потом просто забыли о биткойне и никогда больше не вспоминали, или просто секретные ключи от них утрачены в результате поломки жесткого диска, что делает эти монеты недоступными.

Сделать биткойн более дружелюбным к пользователям – эго еще одна задача, с которой блокчейн-анализ может помочь справиться. Например, большинство пользователей считает, что было бы уместным получать текстовое сообщение но факту отправления или получения средств. Некоторые крупные провайдеры кошельков уже предлагают такую опцию, прочие пока отстают. Текстовые сообщения могут помочь новичкам сориентироваться в своих расходах и изменениях баланса.

Что кроется за реестром транзакций

Блокчейн можно использовать практически для всего, что только можно придумать: отслеживание почтовых посылок по всему миру в режиме реального времени, фиксация авторских прав на интеллектуальную собственность, борьба с интернет-пиратами, тотальная расправа над рынком подделок. Здесь перечислено лишь несколько идей, которые можно реализовать с помощью технологии блокчейна. Разумеется, блокчейн получил основную известность благодаря его возможностям именно в финансовом секторе, которые стали осуществимыми ввиду уникального способа фиксации транзакций. Однако важно понимать, что технология блокчейна представляет собой нечто существенно большее, чем валюта биткойн.

Помимо финансовою аспекта, технология блокчейна сама по себе позволяет создать кое-что поинтереснее, чем глобальная книга бухучета. Сейчас находятся в разработке немало проектов, которые призваны сделать доступными такие инструменты, как смарт-контракты и цифровая регистрация передачи прав собственности, и даже авторскими правами можно будет управлять прямо на блокчейне. Приведем лишь несколько примеров интересных блокчейн-платформ.

• Stampery (https://stampery.com/). Нотаризация цифровых документов и подтверждение их подлинности и неизменности.

• Factom (https://www.factom.com/). Надстройка блокчейна биткойна, предназначенная для учета и хранения данных (например, медицинскою характера).

• Soundchain (http://soundchain.org/). Управление авторскими правами и лицензиями на использование музыкальных произведений на блокчейне.

• Storj (https://storj.io/). Децентрализованное облачное хранилище – проект вознаграждает пользователей токенами Storj за хранение данных на персональных компьютерах.

Благодаря прозрачной структуре блокчейна возможности его тех ни-ческою применения почти безграничны. В настоящее время разработчики исследуют лишь верхушку айсберга, который являет собой потенциал блокчейна. К тому же число возможных способов применения технологии растет день ото дня.

Как использовать блокчейн

Что касается развития приложений блокчейна, то основные разработки сейчас ведутся в финансовом секторе. Это абсолютно нормально, так как одна из особенностей биткойна в том, что он способен предоставить доступ к финансовым сервисам тем людям, которые ранее были лишены финансового обслуживания. К тому же блокчейн более всею известен как открытый регистр транзакций.

Тем не менее потенциал блокчейна пока еще мало исследован в плане возможностей ею применения, так что остается только гадать, какое приложение появится следующим. Что нам известно наверняка – это то, что

сейчас разнообразные блокчейн-проекты уже находятся в стадии разработки и те из них, которые не ориентированы на финансовый сектор, призваны изменить в лучшую сторону нашу повседневную жизнь. Однако до тех пор, пока эти идеи не будут облечены в достойный код, они остаются просто умозрительными построениями.

Идеи, лежащие в основе блокчейн-приложений, как правило, имеют сходство с концепцией биткойна: восстановление прав индивидуального пользователя без необходимости согласовывать свои действия с централизованными структурами и посредниками. Благодаря децентрализованной и прозрачной структуре блокчейна блокчейн-приложения обладают небывалыми преимуществами. (Подробнее о централизации и децентрализации говорится во врезке ниже в этой главе.)

Технические преимущества блокчейна станут более очевидными со временем, по мере более тесного знакомства с этой технологией всего сообщества создателей ПО. Однако разработка блокчейн-приложений – это вам не фунт изюму. Даже маститые разработчики сначала осваивают новые параметры и API-вызовы (инструмент, применяемый разработчиками для вызова определенной функции в рамках платформы или приложения), применимые в рамках блокчейн-платформ.

Основная цель разработки новых блокчейн-приложений заключается в том, чтобы сделать нашу повседневную жизнь лучше, привнося больше прозрачности и надежности в существующую инфраструктуру. Этих свойств сейчас часто катастрофически не хватает, в особенности в сфере финансов. Впрочем, и в других сферах многое можно откорректировать посредством внедрения блокчейна, и будущее подскажет, в какую сторону нам следует двигаться.

Разработка достойного блокчейн-приложения – это длительный процесс, потому что требуется написать много кода и учесть все возможные результаты его использования. Кроме того, разработка блокчейн-приложения “с нуля” потребует вложений, хотя бы потому что программистам нужно платить за их старания. В мире биткойна, впрочем, это не станет непреодолимой преградой – венчурные инвестиции в блокчейн-проекты идут непрерывным потоком, невзирая на колебания курса биткойна.

Блокчейн служит благодатной средой для формирования сообществ и возникновения таких возможностей для индивидуальных пользователей, о которых ранее не могло быть и речи. Часто схожим образом мыслящие пользователи, которые одинаково представляют себе, как можно воплотить в жизнь ту или иную идею, притягиваются друг к другу. Яркий пример – сообщества соавторов альтернативных криптовалют, иначе именуемых альткойнами. Как результат разработка блокчейн-приложений не привязана жестко к одному языку программирования: диверсификация – это большое благо для разработчиков блокчейна. Перерастет ли командный дух в нечто большее, трансформировавшись в рабочее приложение блокчейна, имеющее финансовый смысл, станет ясно со временем. Помимо прочего, существуют явные параллели между развитием Интернета в первые годы его существования и сценарием развития блокчейна в наши дни.

Централизация против децентрализации

Существует одно колоссальное различие между централизованным и децентрализованным типами устройства системы. Централизованные системы предлагают очень узкий набор вариантов реализации повседневных операций для индивидуальных пользователей и компаний, а также моделей взаимоотношений с покупателями. Децентрализованные системы больше сосредоточены на сообществах и их потребностях, в результате участие каждого пользователя становится частью совместных усилий.

• Централизованные компании и сервисы предполагают, что лишь несколько специалистов способны предоставить товар или сервис пользователю

• Децентрализованные компании или сервисы предоставляют возможность всем участникам как получить, так и предоставить товар или услугу практически вне зависимости от местонахождения участников в любое время суток и в любом месте,

Система для пользователей, сделанная пользователями и совместно с пользователями, – это те ценности, которые подразумевает децентрализованная система.

Любое блокчейн-приложение можно написать на разных языках программирования, включая JavaScript, Ruby, Perl и PHP. А еще существуют операционные системы для мобильных устройств, такие как Android, iOS, Windows Phone, Blackberry и другие, о которых тоже не стоит забывать, поскольку их пользователи весьма заинтересованы в соответствующих блокчейн-приложениях. Чтобы узнать больше о платформах разработки блокчейн-приложений, откройте ссылку https://ethclassic.ru/.

Движемся дальше к Биткойну 2.0

Биткойн изначально задумывался как универсальная валюта для разнообразных целей начиная от освобождения от контроля властей и заканчивая получением инвестиционной прибыли и т. д. Однако многие пользователи еще только начинают осознавать, что биткойн является чем-то большим, чем просто методом осуществления платежей. Биткойн 2.0 – понятие, подразумевающее новое поколение биткойн-приложений и платформ, большинство которых не будут сосредоточены на финансовых потребностях. Платформы и приложения платформы Биткойн 2.0 будут использовать блокчейн-технологию, чтобы изменить нашу повседневную жизнь, в самых различных ее проявлениях.

Сам биткойн и все прочие приложения блокчейн-технологии способны на гораздо большее, чем обслуживание финансовых потребностей пользователей, несмотря на то что в этом сама соль инновационного протокола. Впрочем, весьма вероятно, что в будущем акцент на развитии блокчейн-приложений для финансовой экосистемы сохранится. В этой сфере еще многое нуждается в усовершенствовании, поскольку сектор финансов не видел серьезных инновационных изменений на протяжении последних 50 лет.

Однако существует множество других способов применения биткойна и блокчейна в пределах нашей досягаемости. Как раз о них мы и поговорим далее. Использование блокчейнов для аутентификации вместо традиционных и ненадежных механизмов аутентификации от Facebook и Twitter – это лишь один из примеров того, на что способен Биткойн 2.0.

Потенциал приложений платформы Биткойн 2.0 и блокчейна не останется незамеченным. Разнообразные финансовые институции уже ищут способы внедрения блокчейна в существующую финансовую инфраструктуру. Даже если эти финансовые институции не воспринимают биткойн как жизнеспособную валюту, блокчейн и его возможности все равно могут стать перспективной средой для их развития в самом ближайшем будущем.

Привлекательность экосистемы Биткойн 2.0 заключается в том, что блоки и данные транслируются и формируются прямо в сети. Помимо данных о самой транзакции, с помощью блоков биткойна пользователи могут передавать друг другу любую информацию иного характера в прозрачной информационной среде. Цифровые средства массовой информации, цифровые сертификаты собственности, цифровые договора страхования – вот лишь несколько идей, над которыми уже сейчас трудятся различные блокчейн-разработчики.

Приложения Биткойн 2.0 позволят радикально изменить традиционную модель биткойн-торгов, которой мы пользуемся сейчас. Современные биткойн-биржи позволяют пользователям хранить, пересылать и получать цифровую валюту без каких-либо дополнительных опций. Технологии Биткойн 2.0 позволят добавить такие возможности, как пиринговое кредитование, процентные цифровые вклады и даже покупка ценных бумаг в кредит без участия посредников, таких как брокеры или банки.

Приложения и платформы формата Биткойн 2.0 способны устранить необходимость в услугах посредников, по крайней мере в сфере продажи и покупки товаров и услуг. Права собственности на различные товары теоретически также могут быть привязаны к цифровым токенам, которые можно будет передать другим пользователям блокчейна, одновременно с проведением транзакции в рамках оплаты за этот товар. По большому счету блокчейн обладает почти неисчерпаемым потенциалом возможностей для мировой интернет-торговли.

А что вы скажете насчет применения блокчейн-технологии для выпуска виртуальных удостоверений личности, которые можно будет использовать для верификации в сети биткойна и за ее пределами? Вместо того

чтобы передавать ценные документы в руки посредников, которые чаще всего хранят их на центральных серверах, подлинность виртуального удостоверения личности можно будет подтвердить прямо в блокчейне. Владельцу цифрового удостоверения не нужно будет никому передавать свои личные данные, а продавцу не нужно будет хранить копии этих данных.

Использование технологии Bitcoin 2.0 для создания нового типа децентрализованного рынка – еще одно направление технологического развития, которое в настоящее время находится в стадии разработки. Одним из примеров является торговля через блокчейн драгоценными металлами в обмен на фиатную или цифровую валюту. Но и в других аспектах нашей жизни, таких, например, как торговля цифровыми медианосителями, также можно извлечь выгоду из организации соответствующих децентрализованных рынков. Причина проста: поскольку нет посредников, накладные расходы для авторов произведений будут существенно меньше.

И последнее, но не менее важное: технология блокчейна – это, прежде всего, сообщество, поддерживающее эту новую волну инноваций. И члены этого сообщества заслуживают права голоса как в биткойн-проектах, так и в различных ситуациях реальной жизни. Предположим, что местные власти решили открыть информацию о планируемых расходах своим налогоплательщикам. Эту задачу можно решить с помощью приложения на основе технологии Bitcoin 2.0. благодаря которому планы, бюджеты, возможные варианты и наиболее благоприятные решения могут быть представлены всему сообществу, могут обсуждаться и даже быть проголосованными напрямую. У такого приложения как ни у какого другого имеется необходимый потенциал, чтобы сделать процессы и принимаемые решения открытыми, демократичными и легитимными. И это действительно так: конечный результат голосования будет абсолютно прозрачным, в то время как личная информация избирателей будет полностью скрыта.

Создание новых децентрализованных приложений и сервисов станет основной целью технологии Bitcoin 2.0. Эта волна инноваций позволит любому человеку стать его собственным боссом и создать собственный стиль и методы работы. Пусть даже пока трудно понять, что это в конечном счете – курьерское обслуживание компании или оказание транспортных услуг людям, которые не любят ждать, – компания Uber является хорошим реальным примером внедрения децентрализованного обслуживания. Мы считаем, что, как только технология Bitcoin 2.U выйдет из младенчества и обретет необходимое признание, в мире останется совсем немного того, чего нельзя было бы достигнуть.

Часть III. Использование биткойна в бизнесе

В этой части…

• Выясняем, как торговать с оплатой биткойнами, как работать с процессорами биткойн-платежей и как организовать прием биткойнов в своем магазине

• Знакомимся с вопросами налогообложения, административного регулирования и лицензирования в отношении использования биткойнов

• Учимся защищать свои инвестиции в биткойны и выясняем все об опасности атаки двойной траты и других видов атак

• Обсуждаем майнинг биткойнов: как это работает и будет ли вам интересно этим заниматься. В частности, здесь рассмотрены четыре основных недостатка облачною майнинга:

– недостаточный контроль; по существу, компьютерное и серверное оборудование арендуется у кого-то другого, т. е. вы не контролируете эти активы;

– опора на честность кого-то другого; если выплаты покажутся вам недостаточными, нет реального способа выяснить, почему вам не платят столько, сколько вы предполагали получать;

– расходы на обслуживание и электроэнергию возлагаются на вас; компания, осуществляющая облачный майнинг, должна будет оплачивать расходы, связанные с эксплуатацией оборудования, и выплата всех этих сумм будет возложена на вас;

– нелегальные или уязвимые компании; некоторые компании, занимающиеся майнингом биткойнов, могут выглядеть вполне законными, но на самом деле это не так (кроме того, любая компания может оказаться уязвимой и подвергнуться атаке хакеров; в этом случае вы вряд ли сможете что-либо сделать)

Глава 8. Использование биткойна в онлайн-коммерции

В этой главе…

- Продаем за биткойны
- Обзор систем оплаты биткойнами
- Принимаем биткойны в магазине

Понимать, что такое биткойн и как он работает, и купить немного монет из любопытства или развлечения ради – это все неплохо. Однако мы уверены, что вы хотели бы также узнать, как использовать его в качестве твердой валюты (пусть и виртуальной).

В этой главе описаны лучшие способы использования биткойна в качестве инструмента продаж, заменяющего фиатные валюты и позволяющего принимать платежи в Интернете.

Продавайте свои товары за биткойны

Есть несколько способов начать продавать товары за биткойны. Прежде всего, вы можете убедить друзей и близких приобрести биткойны, а затем продавать им свои товары в обмен на BTC.

Однако мы не будем рассматривать здесь этот вариант, так как мы обсуждаем бизнес, а не получение денег от друзей и близких. В этом разделе мы расскажем о различных платформах, облегчающих продажу товаров за биткойны: онлайн-аукционах, использовании собственного интернет-магазина и форумах в Интернете.

Продажи на аукционах

Биткойн используется для продажи товаров практически с самого момента своего появления. Однако понадобилось какое-то время, чтобы в мире биткойна появились специальные платформы, предназначенные для этой цели. Самое очевидное место, где можно продать любой продукт за биткойны, – онлайн-аукцион, подобный eBay.

На момент написания этой книги существовало совсем немного интернет-аукционов, принимающих биткойны. В то же время все больше разработчиков рассматривают возможность создания децентрализованных аукционов и торговых площадок, так что в ближайшие годы количество подобных мест значительно увеличится. Полный перечень биткойн-аукционов можно найти по адресу https://en.bitcoin.it/wiki/Trade#Auction_sites.

За годы существования биткойна мир видел различные торговые площадки, предлагавшие оплату биткойнами в качестве одной из своих услуг, но опыт не всех из них можно назвать успешным. Такие популярные сайты, как Silk Road и Silk Road 2 – оба печально известны в связи с торговлей наркотиками и другими запрещенными товарами, – показали сообществу, сколько всего нужно изменить для принятия

биткойна широкими массами.

Около двух лет назад первый интернет-аукцион начал осуществлять эксперименты с платежами в биткойнах. В отличие от eBay этот аукцион не просто соединяет продавцов и покупателей со всего мира. Для пресечения нелегальной деятельности аукционы используют систему репутации и обратной связи – в то время мир биткойна сильно нуждался в чем-то подобном.

Вместо централизованных платежных систем, таких как PayPal, биткойн-аукционы используют BTC в качестве платежного средства. Но вот в чем загвоздка: биткойн-платежи нельзя отменить, что заставляет биткойн-аукционы искать другие способы защиты продавцов и покупателей.

Применение эскроу, или условного депонирования (когда третья сторона получает средства и хранит их, пока покупатель не подтверждает успешный факт покупки товара), – замечательный способ защиты как покупателя, так и продавца. При покупке клиент отправляет биткойны на эскроу-адрес. Это дает продавцу гарантию получения денег без необходимости доверяться покупателю. Сам покупатель также защищен, поскольку средства хранятся на эскроу-адресе до тех пор, пока приобретенный товар не будет доставлен по назначению. Покупатель получает товар и в случае отсутствия каких-либо претензий уведомляет эскроу-сервис, после чего тот отправляет средства продавцу. После завершения транзакции обе стороны могут оставить отзыв друг другу.

Создание собственного интернет-магазина

Другой способ использовать биткойн в торговле – создать собственный магазин (онлайн или офлайн) для продажи своих продуктов и/или услуг за биткойны. Сделать это достаточно просто, поскольку большинство популярных платформ имеют специальные, готовые к использованию плагины, обеспечивающие прием платежей в биткойнах.

Один из вариантов начать – создать веб-сайт на базе WordPress (http://www.wordpress.com). Этот движок хорошо подходит для самых разных целей – от блогов до онлайн-магазинов. Такие плагины, как WooCommerce, WP E-Commerce и GoUrl MarketPress, позволяют начать принимать биткойны буквально за пару минут. Полный список плагинов для WordPress, поддерживающих биткойн, можно найти здесь: https://wordpress.org/plugins/tags/accept-bitcoin.

систем, включая BitPay и Coinbase (обе они подробно обсуждаются ниже в этой главе), имеют готовые решения для интеграции в интернет-магазины, созданные на базе множества платформ, включая XCart и ZenCart.

Если вы не хотите поддерживать собственный веб-сайт с онлайн-магазином, воспользуйтесь решением, которое позволяет открыть биткойн-магазин любой тематики “под ключ”: https://openbazaar.org/. Открыть полноценный магазин на этой платформе можно буквально за полчаса, все покупки по умолчанию оплачиваются именно биткойнами.

Вам нужно определиться, хранить ли все полученные деньги в биткойнах. Хранение в биткойнах связано с определенными рисками, поскольку курс BTC до сих пор достаточно волатилен, даже на протяжении суток. Храня свои средства в биткойнах, вы можете как выиграть, так и потерять. И в зависимости от типа товаров, которыми вы торгуете, и необходимости платить поставщикам, вам стоит рассмотреть возможность немедленного обмена BTC на местную валюту.

Продажа на форумах BitcoinTalk

Это, вероятно, самый легкий способ: продавать товары за биткойны, просто размещая объявления на форумах BitcoinTalk. Чтобы больше узнать об этом, посетите сайт https://www.bitcointalk.org. Он имеет специальный раздел для покупки и продажи различных вещей – как цифровых, так и физических. Тем не менее в использовании форума вместо аукциона или собственного магазина имеются свои недостатки.

Продажи на форумах BitcoinTalk основаны на рейтингах, заработанных за выполнение заказов предыдущих покупателей. Поскольку поначалу ваш рейтинг будет нулевым, вам будет трудно найти клиентов, готовых купить ваш продукт за такое “неотменяемое” средство оплаты, как биткойн. Решить эту проблему, однако, не так сложно, как может показаться. Есть много людей, готовых депонировать сумму через эскроу (мы рассказывали об условном депонировании ранее в этой главе). В таком случае вся схема будет выглядеть точно так же, как на биткойн-аукционах: покупатель отправляет деньги на эскроу-адрес, продавец отправляет товар и, как только покупатель подтверждает доставку, деньги переводятся продавцу.

В теории все это выглядит так, как будто обе стороны защищены от возможного мошенничества, но здесь есть одна загвоздка. В случае возникновения спора человек, предоставляющий эскроу-услуги, должен принять решение на основе предоставленной ему информации. Представьте, что вы отправили товар, а покупатель утверждает, что ему дошла лишь пустая коробка. Покупатель высылает фотографии закрытой посылки, а затем пустой вскрытой коробки без товара внутри.

Если вы не делали фотографии в процессе упаковки и отправки товара, вам будет сложно доказать свою невиновность. Наличие номера почтового отправления может помочь, но финальное решение остается за эскроу, а людям, как мы знаем, свойственно ошибаться.

Таким образом, наилучшим способом продажи вещей за биткойны является онлайн-аукцион или собственный интернет-магазин. И все-таки использование форумов BitcoinTalk придает транзакциям пиринговый аспект, поскольку в сделку (обычно) не вовлечены никакие третьи стороны, за исключением эскроу. В конце концов, главной целью является удовлетворение клиента и получение своих денег в виде биткойнов. Выбирайте тот способ, который считаете нужным, и доводите начатое до конца.

Раздел форума BitcoinTalk, посвященный продаже товаров, находится по адресу https://bitcointalk.org/index.php?board=51.0.

Обзор системы оплаты биткойнами

Как мы уже говорили, в отличие от операций с кредитными картами, которые характеризуются достаточно высокими комиссиями, биткойн является невозвратным способом платежа. Это означает, что, как только отправитель передает деньги на кошелек получателя, нельзя отменить транзакцию и вернуть деньги назад.
Конечно, в случае необходимости получатель может отправить деньги назад отправителю. Однако нельзя напрямую отменить платёж в биткойнах или сделать возврат средств. Причина этот отличия биткойна от кредитных карт проста: последние выпускаются центральным финансовым органом, к кого-рому можно обращаться для запроса возврата. В случае же с биткойном не существует какого-либо центрального органа, и пользователи несут полную ответственность за хранение и расходование своих средств.

В то же время нет никаких причин отменять транзакции в сети биткойна. Они записываются в блокчейне – публичной книге, содержащей информацию обо всех транзакциях в прошлом, настоящем и будущем (подробнее о блокчейне мы рассказали в главе 7). Запись в блокчейне демонстрирует всем в мире, куда были отправлены средства с “адреса А” и в каком количестве.

Это подводит нас к следующему важному аспекту в отношении биткойна и возвратных платежей. Когда один человек продает биткойны другому, очень важно никогда не использовать обратимый способ платежа. К

примеру, если вы продаете биткойны Джонсу и он хочет заплатить за них через PayPal, ни в коем случае не соглашайтесь. Причина этого проста: традиционные платежные методы, такие как PayPal (https://www.paypal.com), Skrill (https://www.skrill.com) и кредитные карточки, позволяют вернуть средства после осуществления сделки.

Система PayPal меньше всего подходит для продажи биткойнов, и этому есть несколько причин. Во-первых и прежде всего, система PayPal не предоставляет защиту продавцу при работе с “цифровыми товарами”. Во-вторых, на момент написания этой книги биткойн все еще рассматривался правилами компании как “цифровой товар”. Если покупатель запросит возврат средств, даже получив свои биткойны, PayPal без лишних вопросов заберет у продавца деньги. Такой же принцип действует и в системе Skrill, хотя было заявлено, что все платежи в этой системы являются “необратимыми”. Если покупатель откроет спор, ему, скорее всего, деньги будут возвращены.

В обоих сценариях продавец потерял свои биткойны, поскольку они являются невозвратным средством платежа, и вернуть их нельзя.

Вся ответственность за биткойны лежит на конечных пользователях, поэтому к ним нужно относиться с должной серьезностью. Обладание полным контролем за своими личными финансами дает ощущение собственной силы, но и налагает большую ответственность.

С другой стороны, принимающие биткойны продавцы видят преимущество в невозвратности платежей. Мошенничество посредством платежей в Интернете является одной из самых больших угроз интернет-магазинам по всему миру. Биткойн позволяет решить эту проблему раз и навсегда. Кроме того, прием платежей в биткойнах откроет для вас новую и весьма обширную базу потенциальных покупателей, находящихся в любых уголках мира.

Сегодня проще, чем когда-либо начать принимать биткойны как в Интернете, так и в обычных магазинах. Десятки различных сервисов позволят вам интегрировать биткойн-платежи на сайге или сгенерировать QR-коды для вашего магазина. В этом разделе мы рассмотрим несколько из них.

BitPay

Возможно, самой известной биткойн-процессинговой компанией сейчас является BitPay (https://www.bitpay.com). Она одной из первых начала проводить платежи в биткойнах и до сих пор является одной из лидирующих платежных систем в мире биткойна.

BitPay предлагает множество преимуществ как для покупателей, так и для продавцов, желающих начать принимать биткойн-платежи. Так, покупателю предоставляется несколько вариантов отправки биткойнов: он может либо сосканировать сгенерированный QR-код, либо скопировать адрес продавца вручную, либо щелкнуть на предложенной сервисом ссылке, чтобы провести платеж с помощью установленного на компьютере программною обеспечения для оплаты биткойнами.

Продавцам, с другой стороны, не стоит слишком волноваться об интеграции BitPay в свой бизнес-процесс. Все, что для этого требуется, – добавить несколько строк кода в настройки корзины заказа. Всем остальным, включая конвертацию цен в биткойны, занимается собственно BitPay, что обеспечивает легкость установки и настройки соответствующею ПО.

Еще одно преимущество BitPay (впрочем, как и других платежных систем, описанных в этом разделе) – возможность мгновенной конвертации каждой биткойн-транзакции в фиатную валюту. Это очень важный момент для продавцов, поскольку большинство из них платят поставщикам в фиатной валюте. С учетом сильной волатильности курса биткойна конвертацию стоит делать максимально быстро.

В отличие от транзакций с кредитной картой, которым требуется до недели, чтобы дойти до банковского счета продавца, платежи посредством BitPay доходят до адресата на следующий рабочий день. Это хороший способ снизить издержки и избавиться от любых возможных проблем с поставщиками из-за задержанных платежей.

BitPay предлагает сервис по конвертации платежей в рамках начального пакета услуг, и все описанное выше абсолютно бесплатно для продавца. Повторимся: биткойн – гораздо более дешевое платежное средство в сравнении со всеми существующими сегодня. Помимо этого, с учетом отсутствия необходимости настраивать дополнительную инфраструктуру, для интеграции BitPay в магазин не нужны никакие вложения.

Но и это еще не все. BitPay позволяет продавцам принимать биткойны и через мобильные устройства. Специальное мобильное приложение позволяет генерировать QR-коды, состоящие из адреса продавца и требуемой суммы. Чтобы оплатить товар, покупателю нужно лишь отсканировать QR-код с помощью своего приложения и подтвердить транзакцию. Это действительно очень удобно как для продавцов, так и для покупателей!

Если же возникнет необходимость перейти в BitPay на другой тарифный план – к примеру, для интеграции QuickBooks POS или доступа по VPN, – в системе BitPay предлагаются два платных пакета услуг. Оба пакета предоставляют дополнительные возможности для клиентов компании. Однако заметим, что бесплатного пакета более чем достаточно для большинства ритейлеров. Чтобы получить больше информации о ценах и услугах в системе BitPay, посетите веб-страницу https://bitpay.com/pricing.

Coinbase

Coinbase – еще одна популярная платежная система в мире биткойна. Как и BitPay (см. предыдущий раздел), система Coinbase предлагает своим клиентам все необходимое, чтобы начать принимать биткойны. Услуги компании доступны компаниям всего мира.

Что касается ценовой политики, то в этом система Coinbase немного отличается от своих конкурентов. Первые биткойн-транзакции на общую сумму до миллиона долларов (в эквиваленте) будут для вас бесплатны, но после достижения этой цифры к вашим платежам начнет применяться комиссия в размере 1 %. Учитывая, что большинству продавцов понадобится немало времени, чтобы достичь этой отметки, пока это условие не может повлиять на выбор Coinbase в качестве платежной системы.

Конвертация биткойнов в фиатную валюту занимает от одного до трех дней в зависимости от местоположения продавца. В то же время платежи осуществляются ежедневно, что делает сервис быстрее традиционных платежных систем, таких как кредитные карты и банковские переводы.

Еще одной интересной особенностью Coinbase является возможность осуществлять возврат биткойнов покупателю. Как мы уже писали, оригинальные биткойн-транзакции отменить нельзя, хотя получатель может самостоятельно отправить деньги назад. В Coinbase используется тот же принцип, но оформлен он более профессионально. В случае необходимости продавец может вернуть деньги покупателю всего за пару щелчков мышью.

Больше информации о предлагаемых системой Coinbase услугах можно найти по адресу https://www.coinbase.com/merchants?locale=en.

Принимаем биткойны в магазине

Чтобы начать принимать биткойны в магазине, вам не потребуется много времени и денег для реорганизации существующей инфраструктуры.

В отличие от традиционных платежных способов, биткойн является гораздо более удобным средством платежа как для продавца, так и для покупателя, и может похвастаться значительно более низкими комиссиями за транзакции. Кроме того, свою роль в удобстве пользования биткойном играет и тот факт, что он нематериален.

Интернет-магазины

Владельцы интернет-магазинов могут с легкостью интегрировать биткойн-платежи в свои сайты. Все, что для этого требуется. – добавить несколько строчек кода, которые предоставит вам компания, обрабатывающая биткойн-платежи. Выполнив этот пункт, вы сразу же можете начать принимать биткойны и расширить свою базу покупателей практически по всему миру.

Большинство процессинговых биткойн-компаний предлагают готовые решения для интернет-магазинов и даже готовы помочь настроить ваш сайт в случае необходимости. Кроме того, большинство популярных платформ для электронной коммерции уже поддерживают интеграцию биткойн-платежей. Причина этого проста: отсутствие дополнительных издержек при работе с биткойном и в то же время возможность привлекать покупателей со всего мира. Какой продавец откажется от такого предложения?

Если у продавца уже есть свой веб-сайт и домен, для подключения биткойн-платежей не нужно вкладывать деньги в какую-либо дополнительную инфраструктуру. Существует множество решений, предлагающих легкую и быструю интеграцию биткойна (см. предыдущий раздел).

Если говорить о работе с сервисами по обработке биткойн-платежей, большинство из них не берут комиссию даже за конвертацию средств в фиатную валюту. Каждая подобная компания предлагает своим клиентам возможность мгновенно конвертировать все или часть биткойнов в любую выбранную валюту, чтобы избежать рисков, связанных с волатильностью курса. Конвертированные средства затем зачисляются на банковский счет клиента в течение 48 часов (двух рабочих дней).

Как только вы интегрируете биткойн-платежи в свой магазин, останется один важный шаг. Разместив на страницах своего магазина известный логотип “Bitcoin Accepted Here” (Мы принимаем биткойн). представленный на рис. 8.1, вы проинформируете всех потенциальных покупателей о возможности расплатиться биткойнами. Это не только поможет повысить осведомленность о биткойне во всем мире, но также сможет вдохновить других продавцов последовать вашему примеру.

Рис. 8.1. Логотип “Мы принимаем биткойн”

Процесс оплаты биткойнами в интернет-магазинах очень прост. Все цены – указанные в фиатных валютах – пересчитываются в биткойны процессинговой компанией по курсу на момент оплаты. На странице оплаты покупатель увидит QR-код, который можно сканировать с помощью мобильного устройства, и биткойн-адрес, по которому можно отправить деньги вручную. Как только транзакция будет передана в блокчейн, процесс покупки будет завершен.

Обычные магазины

Как и в случае с интернет-магазинами, обычным продавцам не нужно инвестировать в дополнительное оборудование, чтобы начать принимать биткойны. Все, что вам нужно, – это компьютер, смартфон или планшет, а также интернет-соединение. Большинство физических магазинов имеют целый ряд подобных устройств и выход в Интернет, а это означает, что они могут начать принимать биткойны буквально в течение пары минут.

Просто выберите процессинговую биткойн-компанию, которая предлагает клиентам мобильное приложение или веб-интерфейс для приема платежей в биткойнах. Установка такого приложения либо настройка веб-интерфейса займет несколько минут, после чего вы будете готовы принимать платежи.

Как и в интернет-магазинах, для оплаты биткойнами в физических магазинах используются QR-коды. Процессинговые компании позволяют продавцам легко генерировать такие коды с необходимой суммой и адресом.

Когда покупатель просканирует QR-код с помощью своего биткойн-кошелька – обычно установленного на смартфон, – платеж будет совершен в течение нескольких секунд.

Как вы могли догадаться, начать принимать биткойны как в Интернете, так и в обычном магазине очень просто. Конечно, вам понадобится потратить некоторое время на изучение технологии и генерацию QR-кодов, однако впоследствии все преимущества биткойна во много раз превзойдут эти неудобства, которые, к слову сказать, характерны для любой новой технологии.

Глава 9. На стороне закона

В этой главе…

- Как разобраться в налогах
- Как разобраться в законах
- Нужна лицензия или не нужна

Вещи, которые мы не понимаем, нас страшат, поэтому мы хотим их контролировать: инопланетяне, лохнесское чудовище, юристы и система налогообложения. Вместе с тем контролировать биткойн можно лишь до определенной степени. Запретить биткойн вовсе невозможно, потому что не существует универсального способа ею регулирования. Невзирая на прозрачность блокчейна, адреса кошельков по-прежнему позволяют сохранить анонимность, не раскрывая ни имен, ни местонахождения их владельцев.

Однако кому вообще может понадобиться запрещать биткойн? (Ознакомьтесь с врезкой в конце этой главы, посвященной существующим в мире запретам; в ней приведены некоторые из возможных причин.)

Определенные аспекты биткойна требуют более подробного изучения, чтобы сформировать адекватную систему регулирования. Использование биткойна в качестве валюты в легальных целях, например для покупки или продажи товаров и услуг, не противоречит закону. С другой стороны, многие центробанки предупреждают граждан и финансовые организации о потенциальных рисках, связанных с использованием биткойна, но не запрещают использование цифровых валют вовсе. Вот такое предупреждение, выпущенное Банком России: http://www.cbr.ru/press/pr.aspx?file=27012014_1825052.htm

Правовые и государственные структуры по большей части обеспокоены тем, что биткойн неподконтролен какому-либо центральному органу управления. Каждый пользователь биткойна отчасти определяет его будущее без какой-либо необходимости подчиняться воле кучки людей, находящихся у власти. Децентрализация – это новый социально-технологический концепт, суть которого большинству людей сложно уловить сразу, и это непонимание, мягко говоря, тормозит развитие биткойна.

В этой главе рассматриваются правовые условия существования биткойна в различных странах и рассказывается, что можно сделать, чтобы и защитить себя, и не разозлить своего налогового инспектора.

Биткойн и налоги

Как писал Даниэль Дэфо, “В этом мире неизбежны только смерть и налоги…” Это высказывание часто

перефразируют так: “Нет ничего более неотвратимого, чем смерть и налоги”. Я могу помочь вам разобраться в налогах применительно к биткойну, но, боюсь, в остальном вам придется разбираться самостоятельно.

Несмотря на предостережения властей и центробанков касательно биткойна и его революционной натуры (см. главу 1), большинство стран будут рады распространению цифровых валют по одной простой причине: налоговые сборы.

Поскольку цифровые валюты можно расценивать как статью доходов или заработок, их можно обложить налогами. К тому же применение биткойна для оплаты товаров и услуг также облагается налогами в ряде стран. Постольку поскольку правительства могут извлечь выгоду из этой новой “разновидности электронных платежей”, большинство правительств не особенно препятствует их распространению.

Следует, однако, помнить о том, что налоговый ландшафт законодательства может измениться в любой момент, поэтому не помешает время от времени уточнять у представителей власти, каким образом можно легально применять биткойны и взимаются ли с них налоги в текущий период. Такие страны, как Бразилия, Канада. Финляндия, Болгария и Дания, уже издали постановления о правилах сбора налогов с оборота биткойнов, однако далеко не все эти нормы применяются на практике на момент публикации книги. В то же время иные страны, такие как Бельгия. Греция. Гонконг, Япония и Новая Зеландия, не планируют (на данный момент) собирать налоги с цифровых активов.

Впрочем, нет никаких сомнений в том, что каждая отдельно взятая страна изучает феномен биткойна и его возможное влияние на экономику страны. Учитывая децентрализованную и трансграничную природу этого феномена, вполне возможно, что сначала целесообразно будет договориться о неких международных нормах права, прежде чем каждая конкретная страна будет решать, каким образом регулировать оборот этой цифровой валюты и признавать ли ее валютой вообще. На практике многие страны руководствуются собственными специфическими правовыми нормами, направленными против отмывания денежных средств и финансирования террористических организаций (ПОД/ФТ), несмотря на то что эти сферы являются зоной контроля Международной организации по противодействию отмывания преступных доходов (FATF). Вполне возможно, что некоторые страны займут выжидательную позицию, дожидаясь появления каких-либо международных стандартов или лучших практик, прежде чем они начнут издавать собственные нормы регулирования или на-лотовые рекомендации в отношении оборота биткойна и других криптовалют на их территории. Так или иначе, этот дополнительный движущий фактор (необходимость пополнения госказны за счет налоговых сборов) может способствовать правовому признанию и налоговому регулированию биткойна и его приложений.

Страны, в которых биткойны облагаются налогами

Правила налогообложения в разных странах меняются весьма регулярно, и практически невозможно представить здесь всю актуальную информацию по этому вопросу.

В Европе этот процесс “на верхнем уровне” регламентируется решениями Евросоюза. Однако некоторые страны принимают собственные налоговые нормы касательно биткойна, которые впоследствии неоднократно пересматриваются. Евросоюз вряд ли в ближайшее время придет к единой правовой концепции; впрочем, ландшафт законодательств постоянно меняется. В то же время в Азии ситуация с налогообложением биткойна достаточно спокойная – только Сингапур активно собирает налоги с оборота биткойнов, как с продажи товаров, так и с оборота активов. При покупке или продаже товаров за биткойны с местных организаций взимается НДС или торговый налог.

В списке, приведенном в данной главе, рассматриваются основные правила налогообложения для биткойна в различных странах, принявших собственные налоговые нормы. Обязательно примите к сведению, что на момент написания книги эта информация являлась актуальной, однако к тому моменту, когда вы будете читать эти строки, ряд положений может подвергнуться изменениям.

Австралия

Налог на товары и услуги применительно к биткойну действителен для транзакций свыше 10 тысяч австралийских долларов. Однако недавно на обсуждение был вынесен проект новою закона, предлагающий расценивать биткойны и другие цифровые активы как “настоящие деньги”, что в дальнейшем может привести к появлению новых налоговых сборов.

Бразилия

Налоговое управление Бразилии Receita Federal издало свои распоряжения о налогообложении биткойна: цифровые валюты рассматриваются как финансовые активы, с которых взимается налог на прирост стоимости капитала в момент их продажи в размере 15 %. Однако, если суммарная стоимость проданных биткойнов не превышает 35 тысяч реалов, налог взиматься не будет. Любой пользователь, владеющий цифровой валютой, эквивалентной сумме, превышающей тысячу реалов, должен задекларировать свои активы до конца года.

Болгария

Болгария – одна из немногих европейских стран, облагающих налогами активы в биткойнах. Национальное резервное агентство приравняло продажу цифровых валют к статье доходов от продажи финансовых активов. В результате с граждан Болгарии, продающих криптовалюту, взимается налог в размере 10 % на прирост капитала. Сделки с участием биткойна или других цифровых валют облагаются налогом, как любой регулярный или корпоративный доход.

Канада

Канада взимает налоги со всех биткойн-активов, но здесь существует несколько видов налоговых сборов с цифровых валют. Биткойн-транзакции с целью покупки или продажи товаров попадают в категорию бартерных сделок, однако вся прибыль с товарных операций классифицируется как статья дохода или капитал.

Каждая биткойн-транзакция рассматривается индивидуально, и все виды деятельности, которые связаны с извлечением прибыли, облагаются налогами в конце года в соответствии с классификационным списком. Стоимость товаров и услуг, приобретенных посредством бартера, должна быть включена в общий список доходов налогоплательщика, если они представляют коммерческую ценность.

Финляндия

Финляндия – этакая белая ворона среди прочих стран, поскольку представители властей не только ввели налог на прирост капитала для биткойна, но и обложили налогами биткойны, добываемые посредством майнинга, как регулярный доход. Однако в 2014 году биткойн был признан товаром, поскольку он не соответствует определению валюты. В результате налоги на биткойн-активы в Финляндии остаются загадкой, поэтому лучше всего уточнять актуальную информацию у местных представителей властей.

Германия

Германия – пожалуй, самая прогрессивная страна Европы в плане налогового права, применяемого к биткойнам. Любое количество биткойнов, находящихся в собственности дольше одного года, освобождается от налоговых сборов на прирост капитала в размере 25 %. Биткойны на территории Германии признаны “частными деньгами”.

Остров Мэн

Остров Мэн – самоуправляющееся владение Британской короны, одно из немногих государственных образований, внедривших рациональную нормативно-правовую базу для регулирования цифровых валют. Биржи, зарегистрированные на этой территории, должны соблюдать правило “знай своего клиента” и законы против отмывания денежных средств и финансирования террористических организаций. Соблюдение этих норм обеспечивается финансовым ведомством под названием “Государственная комиссия по регулированию рынков финансовых услуг острова Мэн”.

Не в пример многим другим местам на карте, остров Мэн предпринимает активные действия по созданию нормативно-правовой базы для регулирования цифровых валют. Биткойн и прочие цифровые валюты не входят

в спектр активов, действия с которыми подлежат обязательному лицензированию, но компании, связанные с криптовалютами, обязаны соблюдать законы ПОД/ФТ (Противодействие отмыванию денег и Финансирование терроризма) в соответствии с поправками 2015 года к Закону о противодействии легализации доходов, полученных преступным путем, принятому в 2008 году. В итоге этот практичный подход позволяет регистрировать стартапы без необходимости проходить суровую процедуру лицензирования, которую непременно обеспечивает предпринимателям большинство уважающих себя финансовых регуляторов. Эта особенность способствует развитию предпринимательской среды и процветанию криптовалютной активности на острове наряду с формированием правового поля. Подобные меры со временем приведут к полной легитимации биткойна, так как цифровые валюты обладают многочисленными преимуществами (как вы уже, безо всяких сомнений, поняли из предыдущих глав).

Нидерланды

В Нидерландах налоговое законодательство в отношении биткойна прописано очень четко. Биткойн официально признан одной из многих валют, обращающихся на территории страны, и применимо к цифровым валютам действуют те же налоговые законы, которые актуальны для других традиционных валют.

Словения

Словения решила не взимать налоги с продажи биткойнов на биржах и пиринговых сделок. Однако с биткойн-вкладов взимается налог на доходы, как и с других валютных вкладов, а размер налога исчисляется исходя из обменного курса биткойна к евро на момент осуществления транзакции.

Соединенное Королевство

Великобритания рассматривает проект закона, исключающего биткойн из списка валют, облагаемых налогом на добавленную стоимость, что является позитивной мерой по отношению к бизнес-проектам, работающим в этом секторе. На момент написания книги известно, что остров Джерси, другое владение Британской короны, собирается предпринять “стимулирующие меры” для регулирования биткойна в ближайшем будущем. Следите за развитием событий в этой области.

Соединенные Штаты Америки

Федеральные органы Соединенных Штатов Америки выпустили ряд нормативных документов в отношении биткойна и криптовалют, которые, к сожалению, во многом противоречат друг другу. Налоговое ведомство США классифицирует биткойны не как валюту; а как вид инвестиций. С одной стороны, это обеспечивает льготную ставку налогообложения для биткойн-инвесторов, особенно если биткойны находятся в их собственности более года. С другой стороны, это усложняет повседневные операции с биткойнами, так как любая биткойн-транзакция потенциально может рассматриваться как налогооблагаемое событие. Ввиду того, что по-прежнему остается неясным, каким будет влияние биткойна на экономику страны, определить процент налоговых сборов довольно сложно, равно как и то, стоит ли взимать налоги с индивидуальных пользователей или только с организаций.

В общем случае граждане, которые получают любой доход, в той или иной форме, например в биткойнах, обязаны платить налоги. Однако этот доход подразделяется на четыре категории: зарплаты, доход от хобби, доход от бартерных сделок и доход от азартных игр. Все эти категории доходов облагаются разными налогами. Избежать налогов за счет тог о, что вы имеете дело с биткойнами или другими цифровыми валютами, не получится. Уклонение от налогов – это то явление, которого многие биткойн-энтузиасты стремятся избежать посредством сотрудничества с государственными структурами с целью сформировать адекватную нормативно-правовую среду.

Налоговая практика по криптовалютам пока еще только складывается, например многие штаты все еще не определились, стоит ли облагать биткойны налогами на местном уровне. Есть также разногласия между штатами в отношении регулирования биткойна. Каждый штат может издавать собственные законы и предписания для индивидуальных пользователей биткойна и компаний. Некоторые штаты даже склоняются к тому, чтобы не регулировать биткойн вовсе в зависимости от того, признают ли они его валютой, цифровым активом или объектом обмена.

Таким образом, потребуется немало времени, прежде чем законодатели и представители власти придут к единому решению в плане того, как следует регулировать использование биткойна. Несколько стран уже издали собственные директивы касательно налогообложения биткойн-активов, однако правительство США стремится прояснить, каково будет потенциальное воздействие биткойна на местную экономику, прежде чем предпринимать какие-либо шаги.

Помощь в расчете налоговых выплат

Биткойн сам по себе – новое явление, поэтому давать какие-либо рекомендации в плане соблюдения налоговых положений в этой сфере – задача не простая. К счастью, существует несколько сервисов и компаний, которые предлагают биткойн-пользователям свою помощь для вычисления предполагаемых налоговых выплат.

Следует отметить, что не все эти сервисы доступны во всех странах мира. Со временем их будет все больше, однако официально признанных консультантов этой сфере пока не существует.

Ниже перечислены несколько сервисов и компаний, позволяющих пользователям вычислять предполагаемый размер налоговых выплат.

• Бесплатная программа LibraTax (http://www.libratax.com) теперь поддерживает расчеты для биткойна. С помощью программы LibraTax вычислить предполагаемый налог на прирост капитала, равно как и получить расчет по другим налоговым отчисленням с биткойн-вкладов, можно всего за несколько минут. За небольшую плату программа сгенерирует подробный отчет, который поможет вам сэкономить деньги и время и защитит от бумажной волокиты.

• Другая платформа под названием “Coyno” (https://coyno.com) позиционирует себя как бухгалтерское решение для биткойн-пользователей. Вы можете импортировать сюда кошельки основных провайдеров, после чего программа сгенерирует детальный отчет о входящих и исходящих транзакциях. На момент написания книги функция точного подсчета налоговых выплат еще недоступна, но должна появиться в течение ближайших 12 месяцев.

• BitcoinTaxes (https://bitcoin.tax) – это платформа для вычисления налогов на прирост капитала в биткойнах с учетом последних изменений законодательства. Пакет BitcoinTaxes поддерживает расчеты не только для биткойна, но и для других цифровых валют, таких как лайткойн и доджкойн. Данные о транзакциях можно импортировать с основных бирж и онлайн-площадок, кроме того, программа поддерживает вычисления еще для дюжины фиатных валют. Существует бесплатный тариф, который позволяет делать расчеты для любого числа транзакций в пределах 100, а также платный тариф (19 долларов в год), который работает без ограничений и позволяет импортировать данные о транзакциях непосредственно из блокчейна.

Правовое регулирование биткойна в мире

Правовые нормы регулирования биткойна в разных станах заметно различаются, так же как и налоговые положения (см. предыдущий раздел). В некоторых странах они могут разниться даже от штата к штату, от провинции к провинции. Международных правовых положений на этот счет нет, поэтому некоторые страны могут не издавать своих норм о биткойне вовсе.

Лишь у очень небольшого количества стран законодательство включает в себя обязательные правовые нормы, касающиеся биткойна. Большинство государств ограничиваются предупреждениями, разъясняющими гражданам риски применения биткойна, связанные с тем, что его обращение не регулируется государством и сами биткойны не привязаны к реальным активам.

Готов ли мир к появлению этой революционной технологии, которую представляет собой биткойн, еще предстоит увидеть. Перераспределение финансовых сил, обретение частными лицами полного контроля над собственными деньгами и отказ от централизованных сервисов и институций – это большая перемена для мира

финансов.

Нечего и говорить о том, что многие правительства и финансовые учреждения опасаются этой смены парадигмы, поскольку совершенно точно не останутся в выигрыше в случае массового признания биткойна. Несмотря на то что многие страны взимают налоги с биткойн-капиталов, распространение цифровых валю! может иметь неожиданные последствия для различных экономических систем, которые, в свою очередь, могут позитивно или негативно отразиться на судьбе финансовых организаций.

Управление с помощью Битлицензии

Применение традиционных финансовых приемов к биткойну вряд ли будет иметь успех, потому что, скорее всего, произведет обратный эффект. Яркий пример неэффективности подобных мер – Битлицензирование в Нью-Йорке. Вопреки усилиям экспертов биткойн-индустрии местные власти все же ввели свои правила для биткойн-компаний в штате Нью-Йорк, которые большинству из них показались неоправданно строгими и нерациональными.

Основная проблема, с которой сталкиваются большинство биткойн-компаний в результате введения Битлицензии, – это пространные инструкции, с учетом которых владелец такой лицензии должен предоставлять информацию о своих клиентах штату Нью-Йорк. Многие лидеры индустрии биткойна рассматривают это как вторжение в неприкосновенность частной жизни клиентов, в результате чего несколько компаний приостановили обслуживание клиентов на территории штата Нью-Йорк.

Для того чтобы подать заявление на Битлицензию, нужно внести невозвратный взнос в размере 5 тысяч долларов, а в совокупности с расходами на юристов для подготовки необходимых документов общая стоимость оформления Битлицензии вполне может составить 20 тысяч долларов. К тому же нет никаких гарантий, что заявление на получение Битлицензии будет удовлетворено, а власти штата имеют право запросить у биткойн-компаний дополнительные данные касательно того, как устроена их бизнес-модель, а также особенностей их взаимоотношений с клиентами.

Помимо всего прочего, правила Битлицензии включают в себя дополнительные положения против отмывания денег, которые противоречат федеральным нормам. К довершению всех бед, к биткойн-компаниям власти относятся с большим пристрастием, чем к традиционным финансовым организациям, невзирая на связанные с ними многочисленные случаи мошенничества, коррупционные схемы и управленческие ошибки, не раз приводившие к потере клиентских средств.

Сумма в 25 тысяч долларов может показаться не столь уж существенной для крупных финансовых компаний, зарегистрированных в штате Нью-Йорк, однако многие биткойн-стартапы такими суммами разбрасываться не могут. А если представить, что примеру Нью-Йорка последуют другие штаты, то за лицензирование биткойн-компании во всех 50 штатах придется заплатить больше миллиона долларов.

Правовое регулирование биткойна может поспособствовать легитимации цифровых валют, однако, на наш взгляд, Битлицензия – это пример того, чего делать не следует. Подобные нормативные требования способны лишь воспрепятствовать развитию биткойна в штате Нью-Йорк, а чрезмерные расходы, связанные с оформлением лицензии, пока что не по карману многим компаниям, начинающим работать в этой сфере.

Своим отказом подчиняться требованиям Битлицензии и прекращением деятельности в Нью-Йорке биткойн-компании транслируют четкое послание: правовое регулирование биткойна – это полезное начинание, но не стоит пытаться копировать нормативно-правовую базу для традиционных финансовых организаций и применять ее к биткойн-бизнесу, да еще и прикрепив к лицензии завышенный ценник.

Правовое регулирование в других странах

Другие страны мира на сегодняшний день не предпринимают серьезных шагов, направленных на создание нормативно-правовой базы для биткойна. Такие страны, как Нидерланды и Финляндия, объявили биткойн-активы подлежащими обложению налогом на прирост капитала, но дальше этого дело пока не пошло. Обе страны придерживаются принципа невмешательства до тех пор, пока Евросоюз не определится на верхнем уровне, хочет ли он пускать биткойн в зону действия правового регулирования.

Некоторые азиатские страны, с другой стороны, стремятся полностью запретить банкам и платежным

операторам использовать биткойны. Никакие официальные законы, ограничивающие обращение биткойнов на территории Азии, пока что не принимались, за исключением Вьетнама, однако центральные банки многих азиатских стран делают все возможное, чтобы предотвратить использование биткойнов платежными операторами.

В ближайшие несколько лет должна решиться судьба правового статуса биткойна и массового признания этого цифрового актива. Здоровая дискуссия между регуляторами и представителями биткойн-индустрии может стать хорошим началом, но сейчас невозможно с точностью предсказать, какая страна в будущем признает или запретит биткойн.

Нужна ли лицензия для реализации денежных переводов

Многих биткойн-пользователей волнует этот актуальный вопрос: “Могут ли местные органы власти отнести их к числу посредников, осуществляющих денежные переводы?” Лицо, осуществляющее денежные переводы, – это субъект предпринимательской деятельности, который реализует услуги по переводу денег или платежных инструментов.

Действительно, биткойны можно тратить, продавать и покупать посредством трансграничных переводов. Ответить на этот вопрос довольно сложно, однако некие общие рекомендации в той или иной степени актуальны для всех.

В зависимости от места проживания индивидуального пользователя местные власти могут признать его субъектом, реализующим денежные переводы, или не признать таковым на основании факта купли, продажи или обмена биткойнов на товары или услуги. Если индивидуальный пользователь желает обменивать биткойны на фиатную валюту у других или для других пользователей с целью извлечения собственной выгоды, ему может потребоваться лицензия на реализацию денежных переводов в зависимости от его местонахождения.

Биткойн-энтузиасты, вовлеченные в процесс майнинга с целью генерации дополнительных биткойнов и подтверждения транзакций, относятся к иной категории. Генерация биткойнов и их последующая продажа другим пользователям за фиатные валюты или товары, эквивалентные по стоимости, – это, по сути, осуществление денежных переводов. Однако правовые положения о майнинге еще не приняты ни в одной из стран. Этого следует ожидать в ближайшем будущем.

Страны, где биткойны под запретом

Правительство Вьетнама официально запретило использование биткойнов в качестве платежного средства на территории с! раны. Будет ли принят соответствующий закон о привлечении к ответственности граждан Вьетнама, использующих биткойны, пока что неясно, Однако наказание последовать может.

Схожая ситуация сложилась в Боливии. Центробанк Боливии, El Banco Central de Bolivia, официально запретил обращение любых валют или монет, за исключением тех, которые были выпущены и контролируются государством. Этот запрет относится и к биткойну, равно как и к другим цифровым валютам, таким как патесот, feathercoin. доджкойн, quark и peercoin. Нормативный акт, изданный в 2014 году, гласит следующее: “Использование любых валют, кроме выпущенных и контролируемых государством или авторизованной инстанцией, приравнивается к нарушению закона”. Ни одна из существующих цифровых валют не была выпущена или одобрена государством или авторизованным органом, а это означает, что в ближайшее время криптовалюты в Боливии будут вне закона.

Колумбия – другая страна Южной Америки, которая планировала запретить биткойны, но пока что эти планы не реализованы. Биткойн способен оказать существенное влияние на экономические системы стран, в первую очередь, на те, для которых инфляция и гиперинфляция являются самыми насущными проблемами. Относительно Колумбии пока что неясно, распространится ли запрет на биткойн-транзакции, осуществляемые в коммерческих целях, на продажу и покупку биткойнов на бирже либо же под запретом окажутся и те, и другие.

Власти Эквадора приняли решение о запрете биткойна и прочих цифровых валют в 2014 году. Вместе с тем Национальная ассамблея Эквадора согласовала руководящие положения для создания собственной централизованной, контролируемой государством валюты. Чиновникам будет разрешено осуществлять платежи в “электронных деньгах”, так что вскоре мы сможем оценить, как проект будет реализован на практике.

Исландия занимает несколько иную позицию по поводу запрета биткойна. Использование биткойна для осуществления транзакций в Исландии не запрещено, однако покупать и продавать биткойны на иностранных

биржах противозаконно Подобные действия приводят к утечке капитала из страны, что противоречит исландским принципам контроля за капиталом.

В Киргизии тоже не слишком-то жалуют биткойны! Национальный банк Республики Киргизия провозгласил использование биткойна и других цифровых валют в качестве средства платежа незаконным в соответствии с действующим законодательством Единственная легальная валюта на территории страны – это сом.

Другие страны мира пристально наблюдают за биткойном, чтобы понять, каким образом он влияет на экономику. В будущем, возможно, большее число стран запретят биткойн или, напротив, признают его в зависимости от того, как будут развиваться законодательные системы на разных континентах.

И последнее, но не менее важное: операторы биткойн-бирж – индивидуальные пользователи или компании, конвертирующие биткойны в фиатные валюты и обратно – обязаны получить лицензии на осуществление посреднических услуг по денежным переводам в большинстве действующих юрисдикций.

Вне зависимости от того, торгуют ли они биткойнами с определенной периодичностью или регулярно против фиатных валют, лицензия требуется практически в любой стране. Единственное примечательное исключение – это остров Мэн. Криптовалютные компании, действующие в этой юрисдикции, обязаны соблюдать лишь актуальные нормы ПОД/ФТ, признанные Управлением по финансовым услугам острова Мэн, однако их целевая деятельность на текущий момент не лицензируется согласно распоряжению УФУ.

Глава 10. Безопасность биткойна

В этой главе…

- Анализ защищенности, присущей децентрализации
- Как предотвратить атаку 51%
- Двойное расходование средств и как его избежать

Защищен ли биткойн? Один из наиболее частых вопросов о биткойне – “Достаточно ли хорошо защищена вся экосистема биткойна, чтобы противостоять атакам хакеров (людей, стремящихся нарушить работу сети в попытке многократно потратить свои монеты)?”

Ответ на этот вопрос выходит за рамки простого “да” и порой включает технический жаргон. В этой главе будут описаны основы и дано объяснение, почему биткойн защищен и что делается для усиления уровня безопасности по мере роста его экосистемы.

Сеть биткойна: как это работает

Если верить СМИ, то за последние несколько лет сеть и протокол биткойна неоднократно взламывались. Однако это далеко не так. Сама по себе сеть биткойна ни разу не была успешно взломана и, вероятно, никогда не будет – в традиционном понимании того, что такое взлом.

Конечно, некоторые биткойн-пользователи за эти годы потеряли свои монеты, но ни один из этих случаев нельзя отнести к дырам в системе безопасности самой сети. Такие сервисы, как биржи и провайдеры облачных кошельков, выстроенные поверх сети биткойна, стали жертвами их собственных недостатков в системах безопасности. Как только эти сервисы оказывались взломанными, пользователи теряли хранящиеся там монеты. Повторим еще раз: это не имеет ничего общего с дырами в безопасности самой сети Биткойн, так как децентрализованные сети по типу биткойна не могут быть “взломаны”.

Что делает сеть биткойна безопасной

Что делает сеть биткойна настолько безопасной, что нечего даже беспокоиться об угрозах со стороны хакеров? Давайте посмотрим.

- Сеть биткойна децентрализована. Участие в системе множества пользователей, ни один из которых не

обладает “особыми полномочиями”, гарантирует отсутствие единой точки отказа, через которую можно было бы взломать протокол биткойна. Каждый отдельно взятый пользователь может стать жертвой хакерской атаки, но эго не окажет никакого влияния на сеть биткойна в целом. Даже если все пользователи в одной стране одномоментно подвергнутся хакерской атаке, сеть биткойна продолжит работать как ни в чем не бывало.

• Для гарантии целостности и сохранения хронологической последовательности блокчейна и всех сохраненных в нем связанных транзакций в сети биткойна используется мощнейшая криптография. Теоретически криптография такою уровня могла бы быть взломана, но это потребовало бы объединенной вычислительной мощности всех существующих на данный момент суперкомпьютеров на протяжении неопределенного периода времени (число с 15-ю нулями; мы вместе с редакцией не знаем правильного слова для его обозначения; пожалуй, можно описать его как квантовый скачок компьютерных мощностей), чтобы получить призрачный шанс взлома сети биткойна как таковой.

• Каждый отдельно взятый биткойн-адрес защищен закрытым ключом, который необходимо предъявить при отправке в сеть транзакции со средствами с этого адреса. Пользователи биткойн-кошельков, устанавливаемых на компьютер или мобильное устройство, являются единственными владельцами закрытого ключа. И до тех пор, пока устройство не скомпрометировано, никто другой в мире не может заполучить этот ключ.

• Процесс генерации новых биткойнов, называемый майнингом (за дополнительной информацией о майнинге обратитесь к главе II), работает на основе распределенной консенсусной системы, которая подтверждает (или отклоняет) транзакции, распространяющиеся в сети Биткойн посредством сложного вычислительного алгоритма. Для успешного майнинга биткойнов требуется специализированное компьютерное оборудование, и общее количество такого оборудования, используемого по всему миру, до сих пор от месяца к месяцу растет. Плюс к тому ключевую роль в этом процессе играет децентрализация, поскольку биткойн-майнеры рассеяны по всему миру. У правительства нет возможности раз и навсегда остановить создание новых биткойнов, поскольку в системе отсутствует централизованное управление (оно же – точка отказа).

Для более детального ознакомления с устройством сети Биткойн читайте описание биткойна от его создателя Сатоши Накамото https://bitnovosti.com/2012/12/22/bitcoin-genesis/ (оригинал на английском: https://bitcoin.org/bitcoin.pdf).

Роль полных узлов биткойна

Отдельные пользователи биткойна – не единственная движущая сила в отношении усиления безопасности сети. В течение последних нескольких лет специально выделенные биткойн-узлы присоединялись к сети с единственной целью – прием и распространение новых биткойн-транзакций среди других пользователей и узлов сети. Это действие выводит аспект децентрализации биткойна на принципиально новый уровень.

Каждый узел сети Биткойн это устройство (такое, как, например, компьютер, мобильное устройство или даже микрокомпьютер по типу Raspberry Pi 2), на котором размещается весь блокчейн, начиная с генезис-блока, созданного в 2009 году. Генезис-блок был первым блоком данных в сети биткойна; за его майнинг Сатоши Накамото получил награду в 50 биткойнов. Начиная с этого момента пользователи биткойна получили возможность генерировать биткойны и распространять биткойн-транзакции по всему миру.

Биткойн-узел совмещен с биткойн-клиентом, но этот софт не принимает и не рассылает монеты сам по себе, если это противоречит воле его оператора. Такие узлы просто выполняют функцию хранения копии блокчейна с целью возможности проверки целостности, нейтральности и хронологической последовательности транзакций начиная с генезис-блока и до текущего момента (больше о блокчейне – в главе 7).

Запуск и поддержание работы биткойн-узла не приносит его владельцу вознаграждения в виде новых биткойнов. Единственным смыслом существования биткойн-узла является усиление сети. На момент написания этой книги в сети было уже более 6 тысяч полных узлов, и все время добавляются новые. Распределение полных биткойн-узлов по странам мира можно увидеть на сайте https://getaddr.bitnodes.io/.

Защита биткойна от хакеров

Как уже упоминалось, сеть биткойна основывается на защищенной технологии, которую не могут взломать даже самые “продвинутые” хакеры с помощью мощнейших компьютеров. Криптография – технология безопасных коммуникаций в присутствии посторонних с использованием длинных последовательностей секретных кодов, которые невозможно разгадать – играет немаловажную роль в безопасности биткойна. При правильном использовании криптография может сделать систему экстремально защищенной.

В последние годы в СМИ была большая путаница относительно того, как именно работает биткойн. Вопреки распространенному мнению биткойн не управляется каким-то одним лицом или организацией, т. е. нет какого-то “биткойн-босса” или “биткойн-директора”. Все пользователи равноправны и ни один из них не играет какой-то особенной роли и не обладает специальными полномочиями. Это делает биткойн непривлекательной мишенью для хакеров.

Попытка взлома сети биткойна была бы подобна взлому Интернета. Это просто невозможно. И биткойн, и Интернет по природе своей децентрализованы и не имеют единой точки отказа. Если какая-то часть сети отключится, маршрутизация пакетов перестроится таким образом, чтобы обходить проблемный участок, и сеть продолжит работу. Те же самые принципы применимы к сети биткойна.

Отсутствие центральной точки отказа означает, что у сети биткойна нет “выключателя”. Сеть биткойна охватывает весь мир, работает на всех континентах, и невозможно одновременно выключить каждый компьютер и все прочие устройства, подключенные к сети. Даже правительства не смогут это сделать. Официальные лица могут запретить использование биткойна в каких-то странах, но это не будет означать, что сеть прекратит работать даже там.

Кроме того, стимулы для взлома сети биткойна отсутствуют, так как это не дает хакерам никакой финансовой выгоды. Все предыдущие блоки включают биткойны, которые уже были высланы одними и получены другими пользователями биткойна, и это! факт невозможно изменить. И свежесозданные монеты – даже если сеть была бы взломана (что практически невозможно) – также не попадут напрямую к хакеру.

Сеть биткойна по праву можно назвать технологическим чудом, так как она дает невиданный ранее уровень финансовой защищенности. Но несмотря на все эти перспективы в сети биткойна – и в блокчейне, лежащем в ее основе – есть многое, что пока непонятно и что может послужить поводом для беспокойства. Полное постижение сети биткойна и ее технологической мощи придет через много лет, именно поэтому так важно продолжать расширять сообщество биткойна. У каждого участника свой взгляд на вещи и на то, как что-то можно было бы улучшить или использовать для взлома. Предотвращение атаки всегда лучше, чем исправление ее последствий.

Взлом сервисов на основе биткойна

Конечно, всегда существует возможность того, что в какой-то точке платформа биткойна может быть взломана. Причина этого проста: несмотря на общую концепцию полной децентрализации сети большинство биткойн-сервисов и платформ (в отличие от биткойн-сети самой по себе) развернуто и работает на одном или нескольких централизованных серверах.

Когда у хакеров есть цель в виде централизованной точки отказа, выключение единичного сервиса значительно проще, чем атака на саму сеть биткойна. Даже если хакеры взломают биткойн-сервис, это не скажется на работе самой биткойн-сети, поскольку эти два элемента не связаны между собой.

Биткойн-сервисы используют блокчейн для проверки и обработки транзакций, но блокчейн не зависит от них. Некоторые полагают, что если биткойн-биржа оказывается взломанной, то ее связь с блокчейном сделает сеть биткойна также уязвимой. Но это не так, поскольку биткойн-биржи представляют собой сервисы, построенные поверх блокчейна, и они действительно централизованы.

Фактически в настоящий момент нет прямой связи между сетью биткойна и каким-либо существующим биткойн-сервисом. Единственное, что связывает пользователей и блокчейн, – это биткойн-кошельки, которые, в свою очередь, образуют отдельный слой поверх блокчейна. Единичные пользователи не могут напрямую изменять блокчейн, поэтому взлом единичного пользователя никоим образом не влияет на работу биткойн-сети в целом. Тот же самый принцип применим и к взлому биткойн-сервисов. Они представляют собой слой поверх биткойн-сети, т. е. не оказывают влияния на работу всей сети как таковой. Все, что делают биткойн-сервисы, – эго распространяют определенные типы транзакций в сети биткойна, но если эти транзакции никогда не будут оттранслированы в сеть, то она продолжит работать так же, как и прежде.

По сути, биткойн-сеть не может быть затронута ничем находящимся за ее непосредственными пределами. Проблема возникла бы только в случае, если бы сеть биткойна подверглась взлому и была изменена 51 % или большим количеством хеш-мощности сети (подробнее – в следующем разделе). Принимая во внимание вычислительную мощность, обеспечивающую безопасность сети на текущий момент, набрать 51 % от ее общей вычислительной мощности – почти нереализуемая задача ни для частника, ни для правительства.

Вдобавок взлом биткойн-сервисов – гораздо более прибыльное дело, чем взлом сети как таковой. Например, биткойн-биржи хранят большое количество клиентских средств в биткойнах, что создает соблазн для хакеров попытаться украсть часть этих денег. Биржи, на которых безопасность была не на высоте, за время существования биткойна не раз становились жертвами таких атак благодаря именно плохой организации их индивидуальной защиты.

Независимо от того, сколько биткойн-бирж и сервисов было взломано, эти случаи не оказывают никакого влияния на сам блокчейн. До тех пор, пока хотя бы у одного пользователя запущен биткойн-клиент на любом поддерживаемом устройстве, блокчейн будет продолжать делать свое дело. И с каждым днем все увеличивающееся количество клиентских приложений помогает все лучше защищать сеть биткойна.

Поговорим об атака 51-го процента

Одна из очень немногих вещей, которые могли бы нанести существенный вред сети Биткойн, – это так называемая “атака 51 %”. Проще говоря (а мне нравятся простые формулировки, как и многим из вас), атака 51 % означает, что какой-то майнер или картель майнеров завладевает 51 % от общего количества вычислительных ресурсов сети. Это может привести к форку (разделению единого журнала транзакций, блокчейна, на два с определенного момента противоречащих друг другу варианта) сети биткойна. В результате будет создан новый “искусственный” вариант блокчейна, с точки зрения которого любые транзакции “старого” блокчейна будут недействительны.

Теория атаки 51%

Вероятность атаки 51 % в мире биткойна очень мала, хотя и не нулевая. Как только злоумышленник получит в свое распоряжение 51 % (или более) хеширующей мощности всей сети, он сможет по своему усмотрению блокировать новые транзакции или изменять их порядок, что позволит ему контролировать запись информации в блокчейн биткойна.

Атака 51 % может иметь неприятные последствия для сети биткойна в целом. Например, человек, группа лиц или компания, несущие ответственность за атаку 51 % в сети биткойна, получили бы возможность обращать транзакции на протяжении всего времени атаки. Транзакции с двойной тратой – возможностью потратить одни и те же биткойны дважды – в это время стали бы настоящей проблемой, ведь было бы невозможно понять, какая транзакция настоящая, а какая нет (мы поговорим об этом еще чуть позже в этой же главе).

Кроме того, лица, ответственные за атаку, могут помешать любой транзакции по выбору – или сразу всем – набирать подтверждения. К тому же стоит атакующим пожелать, и майнеры не смогут майнить правильные блоки в сети, при том что весь доход будет уходить к атакующим. Это основная из причин, по которым эксперты индустрии биткойна хотят быть уверены, что атака 51 % никогда не произойдет ни при каких обстоятельствах, хотя стопроцентной гарантии никто, конечно же, дать не может.

Но говоря об этой сугубо теоретической возможности, стоит упомянуть еще кое о чем. Чего злоумышленник (или злоумышленники) не сможет сделать, так это изменять транзакции, инициированные другими пользователями. Не смогут они также украсть биткойны других пользователей, ведь у них все равно не будет секретного ключа. Только собственные транзакции атакующих смогу! быть обращены, но даже одно только это может нанести сети биткойна значительный ущерб, ведь проведение транзакций другими пользователями также может стать невозможным, если атакующие решат помешать этим транзакциям получить подтверждения в сети. Подтверждения происходят в результате подписания новых блоков в биткойн-сети, и атака смогла бы полностью остановить этот механизм. Но создание монет из ничего или даже изменение награды за блок – это два базовых параметра сети, которые все равно никак нельзя изменить. В итоге получается, что, даже завладев 51 % вычислительной мощности сети биткойна, найдется не так уж и много вещей, на которые злоумышленники смогли бы повлиять.

Только теория

Надо понимать, что не все стратегии, существующие в теории, имеют шанс реализоваться в действительности. Именно к такой группе относится стратегия “Атаки 51 %”, по мнению подавляющего большинства блокчейн-экспертов.

Зачем же тогда вообще обсуждать эту проблему? В мире биткойна считается, что необходимо тщательно изучать любые потенциальные дыры в сетевом протоколе до того, как злоумышленники получат возможность их использования. Всегда гораздо лучше заранее “перебдеть”, чем потом сожалеть и пытаться исправить ситуацию, так что биткойн-девелоперы непрестанно работают, чтобы застраховать сеть от нанесения ей любого вреда.

По мере развития технологии девелоперам придется оставаться на переднем крае и принимать все технологические новинки близко к сердцу. Безопасность – постоянно меняющаяся сущность, и, если ей не уделять должного внимания, она может привести к многочисленным плохим последствиям. К счастью, биткойн-разработчики стоят на страже наших интересов.

Большинство экспертов в области безопасности ожидают, что в обозримом будущем атаки 51 % не произойдет. Нет каких-либо стимулов к атаке, кроме того что появится возможность двойной траты монет, которыми владеет сам злоумышленник. Если у злоумышленника мало монет, то проведение успешной (и, заметим, крайне дорогостоящей) атаки не принесло бы атакующему никакого монетарного вознаграждения. Если же у него большое количество монет, го проведение такой атаки способно их существенно обесценить, что вряд ли компенсируют попытки двойной траты, успешность которых тоже далеко не гарантирована.

Насколько вероятна атака 51%

Проведение атаки 51 % частным биткойн-майнером или хакером практически невозможно. Однако в последние годы некоторые из крупнейших майнинг-пулов подходили близко к тому, чтобы завладеть более чем пятьюдесятью процентами вычислительной мощности сети. Однако благодаря своевременно принятым мерам в отношении затронутых пулов потенциал доминирования единственного из участников сети был каждый раз успешно блокирован.

Узел Ghash.io, в прошлом один из крупнейших майнинг-пулов биткойна, неоднократно подходил к границе

51 % мощности сети. Последний раз Ghash.io пересек черту 51 % в июле 2014 года, вынудив биткойн-сообщество сесть за стол переговоров с владельцами пула и всем сообществом майнеров биткойна, чтобы найти решение.

Были разработаны меры, включавшие обязательство со стороны Ghash.io с этого момента никогда более не преступать порог в 29,99 % общего хешрейта (общая вычислительная мощность, определяемая как сумма мощностей всех майнеров) сети Биткойн. И несмотря на то что 29,99 % – это все равно слишком много для контроля со стороны одного майнинг-пула, это также может рассматриваться как буфер, чтобы помешать кому-то другому, кто захочет начать злонамеренную “атаку 51 %” на сеть.

Это был уже второй случай менее чем за год, когда Ghash.io был близок – или превзошел – уровень 51 % всей вычислительной мощности сети. В январе 2014 года Ghash.io также был близок к тому, чтобы завладеть 51 % хеш-мощности сети – результатом этого стало приостановление возможности регистрации в пуле новых пользователей на достаточно длительный период.

Впрочем, в мире майнинг-пулов ничего не остается постоянным, новые пулы появляются, набирают популярность, потом идут к закату и исчезают. То же самое произошло с Ghash.io. После 2014 года пул постепенно исчез с горизонта. Компания CEX.io – владелец узла Ghash.io – в конце 2014 года решила приостановить сервис облачного майнинга из-за того, что низкая цена биткойна делала бесприбыльной работу всего оборудования, используемого для майнинга в пуле Ghash.io. Если оборудование подразделения облачного майнинга CEX.io в будущем когда-либо будет включено вновь, будет интересно посмотреть, сможет ли Ghash.io стяжать былую славу.

На момент выхода книги вычислительная мощность сети биткойна делится между множеством майнинг-пулов. Самый крупный на текущий момент пул – китайский AntPool (в нем 17,8 % мощности сети); за ним следуют пул BTC.Top (11,7 %), Bixin (9,7 %) и BitFury (8 %). Актуальную информацию о распределении хеш-мощности можно получить на странице https://blockchain.info/pools.

Все вышеупомянутые пулы управляются китайскими операторами, что делает Китай страной, которой в настоящий момент принадлежит около половины вычислительной мощности сети биткойна.

Двойная трата

Одним из главных опасений в отношении биткойна является вопрос “Сможет ли хакер потратить свои монеты дважды?” Теоретически двойная трата могла бы произойти, и на практике она происходила. Тем не менее фактор риска, ассоциированный с таким событием, близок к нулю, поскольку шансы здесь в пользу биткойн-пользователя или торговца. Но что же такое атака двойной траты и как ее можно провести?

Атака двойной траты

Название говорит само за себя. Технически атака двойной траты позволяет одному пользователю дважды потратить все монеты, находящиеся у него на балансе. Например, если у кого-то в кошельке находится 5 биткойнов, то теоретически при реализации сценария двойной траты он мог бы потратить 10 биткойнов. Тем не менее в сети биткойна есть различные правила для предотвращения двойной траты, что делает ее крайне редким явлением.

Каждая биткойн-транзакция при ее распространении в блокчейне проверяется каждым отдельным узлом сети. Каждая биткойн-транзакция содержит ввод, эквивалентный последнему непотраченному выводу, на аккаунте, о котором здесь идет речь. Каждый непотраченный вывод может быть потрачен только однократно, что должно сделать двойную трату биткойнов невозможной.

Атака в спешке

И хотя атака двойной траты в настоящее время очень редка, все равно есть шансы, что кто-то может стать ее жертвой. Из соображений удобства интернет-торговцы и трейдеры склонны считать, что биткойн-платеж уже

прошел даже при нуле подтверждений – это дает возможность атакующему потратить те же самые деньги еще раз. По мере того как транзакция набирает все больше подтверждений, шансы проведения двойной траты сокращаются экспоненциально.

Торговцы могут принять определенные меры предосторожности, чтобы обезопасить себя от атаки двойной траты. Во-первых, и в самых главных, это работа с биткойн-процессором платежей, который согласует риски на стороне торговца. – это шаг в правильном направлении. Большинство платежных процессоров защитят торговца от убытков даже в случае атаки двойной траты.

Во-вторых, торговцы и рядовые пользователи сети могут запретить входящие соединения в клиенте, чтобы он мог только сам соединяться с доверенными узлами. Эти действия сводят к нулю риск атаки двойной траты. Но даже если так, все равно лучше дожидаться как минимум шести подтверждений транзакции.

Против биткойн-сети могут быть применены различные типы атаки двойной траты. Мы только что обсудили атаку “в гонке”, которую можно провести, только пока транзакция не получила ни одного подтверждения.

Ожидание нескольких подтверждений – лучшее средство убедиться в том, что транзакция легитимна, даже если это и самый удобный вариант для торговцев.

Атака Финни

Еще одним популярным видом атаки двойной траты является атака Финни, которая требует участия биткойн-майнера сразу после того, как в сети был найден очередной блок. Меры предосторожности, предпринятые торговцем, не могут помешать успешному осуществлению атаки Финни, хотя для того, чтобы атака считалась успешной, злоумышленнику потребуется совершить вполне определенную последовательность действий. В целом этот метод достаточно дорогостоящ, что снижает риск проведения атак такого типа для торговцев и провайдеров сервисов.

Комбинация атаки “в спешке” и атаки Финни позволяет провести атаку Вектор76. Теоретически эта атака позволяет двойную трату биткойнов даже после первого сетевого подтверждения транзакции. Успешная атака будет стоить атакующему один блок – атакующий должен утаить этот блок и вместо того, чтобы распространить информацию о нем в сети, оттранслировать его атакуемому узлу в надежде, что успеет скрыться с товаром или воспользоваться сервисом до того, как сеть распознает атаку.

Брутфорс-атака

И последние, но не менее значимые – брутфорс-атака и атака >50 %. Для проведения обеих требуется неимоверное количество вычислительной мощности сети биткойна. Вероятность проведения любой из этих атак в настоящее время крайне мала, так как атакующему понадобилось бы получить контроль над существенным количеством всей майнинговой мощности сети биткойна.

Брутфорс-атака происходит так.

1. Атакующий отправляет в сеть транзакцию с оплатой товара и в то же время в частном порядке майнит форк блокчейна (разветвление цепи блоков), где вместо этого включена транзакция двойной траты.
2. После ожидания n подтверждений торговец отправляет товар.
3. Если у атакующего к этому моменту получается посчитать более n блоков, он публикует свой форк и получает монеты обратно; в противном случае он может попытаться продолжить считать свой форк в надежде когда-нибудь обогнать сеть. Если этого никогда не произойдет, то атака считается захлебнувшейся, платеж остается совершенным, а средства остаются у торговца.

Вероятность успеха атаки – функция от хешрейта атакующего (как доли общего хешрейта сети) и числа подтверждений, которые будет дожидаться торговец перед тем, как выдать товар. Например, в случае, если атакующий контролирует 10 % хешрейта сети, но торговец ждет прохождения шести подтверждений, вероятность успеха атаки будет порядка 0,1 %.

Как описывалось в предыдущем разделе, атака >50 % преуспеет только в случае, если злоумышленник получит контроль над более чем 50 % хеш-мощности всей сети. Поскольку в этом случае злоумышленник может генерировать блоки быстрее, чем оставшаяся часть сети, он может попросту упорно наращивать блоки в

своем форке до тех пор, пока его цепь не станет длиннее цепи, построенной “честной” сетью. Тогда никакое количество подтверждений не спасет от атаки.

Самую большую угрозу торговцам и провайдерам биткойн-сервисов несет атака >50 %. поскольку она также косвенным образом обеспечивает успех брутфорс-атаке. Но учитывая, до каких размеров выросла вычислительная мощность сети биткойна к настоящему времени, возникают большие сомнения в том, что такая атака когда-либо сможет быть успешно проведена.

Наибольшей проблемой биткойн-сети является то, что поверх нее понастроили слишком много централизованных сервисов. Почти каждая биткойн-биржа и каждый майнинг-пул представляют собой централизованные сервисы. Когда биткойн-биржа оказывается взломанной, это не оказывает влияния на блокчейн сам по себе, равно как и не открывает возможность к проведению атаки двойной траты. Но когда взламывают большой майнинг-пул, это может быть совсем другой коленкор. К счастью для всех участников, сейчас в сети нет майнинг-пула биткойнов, который контролировал бы половину сети. Самые большие майнинг-пулы контролируют до 25 % общей вычислительной мощности сети. Гем не менее, если злоумышленник решит провести брутфорс-атаку для двойной траты биткойнов, то такой доли мощности сети ему будет достаточно.

Глава 11. Майнинг биткойнов

В этой главе…
- Разбираемся в основах майнинга
- Осмысливаем облачный майнинг
- Решаем, имеет ли смысл связываться с майнингом

Концепция майнинга биткойнов основывается на процессе создания новых биткойнов. Этот процесс будет идти вплоть до момента достижения предела в 21 миллион монет. Биткойны не появляются из воздуха, не выпускаются банками или правительствами. Они генерируются в ходе решения компьютерами сложных математических уравнений.

Без биткойн-майнеров новые монеты не попали бы в обращение. И хотя для большинства людей это и не стало бы проблемой, требующей немедленною решения, это также означало бы, что в сети перестали подтверждаться транзакции, что вызвало бы гораздо большее беспокойство. В условиях, когда в сети перестали бы считаться блоки, транзакции остались бы неподтвержденными, и получатели не смогли бы потратить свои монеты.

Но майнинг биткойнов нужен не только для создания новых монет. Он добавляет записи транзакций в открытый распределенный журнал транзакций, называемый блокчейном (более подробно о блокчейне – в главе 7). Каждая биткойн-транзакция должна быть записана в блок данных, и этот блок данных должен быть “вычислен” майнерами. Как только транзакция оказывается включенной в какой-то биткойн-блок, она получает первое подтверждение.

За последние несколько лет процесс майнинга биткойнов стал очень сложным и ресурсоемким. По мере того

как все больше и больше людей соревнуются в попытках посчитать следующий биткойн-блок, неуклонно растет сложность, ассоциированная с этими математическими расчетами. По мере роста сложности частота нахождения новых блоков остается стабильно на уровне одного блока раз в десять минут – это делает возможным ожидание года окончания майнинга, когда последний блок будет найден.

В наши дни затраты на электричество и вложения в оборудование при организации правильной биткойн-фермы весьма высоки. Домашний майнинг стал почти невозможным, разве что есть доступ к дешевому или бесплатному электричеству. Это главная причина, по которой оборудование подавляющего большинства биткойн-майнеров находится в Китае, где оптовые цены на электроэнергию значительно ниже, чем в большинстве стран мира. Увидеть своими глазами, на что похожа современная промышленная биткойн-ферма, можно здесь: https://www.youtube.com/watch?v=GNZ6Bg-Onj0.

Спускаемся в шахту

Для майнинга биткойнов не нужна кирка, канарейка или газовая лампа.

Основной целью майнинга является создание консенсусной экосистемы, чтобы биткойн-узлы могли определить, является ли транзакция действительной. Общеизвестно, что шесть подтверждений – это минимум, необходимый для того, чтобы средства, пришедшие в транзакции, можно было “официально” потратить.

Основная причина, по которой майнинг биткойна со временем все более и более усложняется и становится более ресурсоемким, заключается в том, что реализация алгоритма SHA-256 делает расчет хеша блока очень сложным. Каждый блок должен начинаться с определенною количества нулей, а это значит, что нужно предпринять довольно много попыток перед тем, как удастся найти правильное решение.

Кроме того, сложность майнинга пересчитывается сетью каждые 2016 биткойн-блоков, и едва ли удастся припомнить, чтобы она когда-либо снижалась. Коэффициент сложности зависит от общею количества вычислительной мощности, использовавшейся для решения предыдущих 2016 блоков в сети за прошедшие две недели, и компенсирует прирост или уменьшение количества майнинговой мощности.

В начале времен биткойна каждый добытый блок приносил награду 50 BTC. По мере того как все больше майнеров вступали в бой, награда за блок стала распределяться среди участников майнинг-пула, находившего очередной блок. На момент публикации книги награда за блок составляет 12,5 BTC и должна уменьшиться вдвое, до 6,25 BTC, примерно в марте 2020 года.

За биткойн-транзакции нужно платить комиссионные сборы. Эти сборы получают майнеры за включение транзакции при майнинге очередного блока. И хотя основную часть дохода майнеров пока составляет вознаграждение за решение блока, в будущем доля этих комиссионных сборов в структуре вознаграждения майнеров будет расти.

По мере своего развития экосистема майнинга биткойна претерпела радикальные изменения. Для того чтобы получить хоть какую-то прибыль, теперь требуется специализированное майнинговое оборудование. Как уже упоминалось, майнинг биткойна очень затратен с точки зрения расходов на электричество; также постоянно требуется обслуживание и обновление майнингового оборудования.

Необходимость сокращения дисперсии доходов майнеров рано или поздно должна была привести к созданию майнинг-пулов. В начале индивидуальным майнерам принадлежали все возможности, но индивидуалы постепенно исчезали из биткойн-мира по мере того, как майнинг в пуле становился все более и более предпочтительным. Объединение вычислительной мощности многих майнеров увеличивает шансы нахождения следующего биткойн-блока, при том что награда за найденный блок делится между участниками в соответствии с объемом вычислительной мощности каждого из них.

Майнинг биткойна: как это работает

Напомним: в отличие от традиционных фиатных валют, когда правительства всех стран мира могут по необходимости допечатать столько банкнот и дочеканить столько монет, сколько им нужно, в биткойне объем эмиссии строго ограничен. Это ограничение установлено на уровне 21 миллион монет и не будет достигнуто до 2140 года. А до этого времени майнеры будут использовать специализированное компьютерное оборудование с целью майнинга новых биткойнов в сети.

Как только биткойн-транзакции распространяются 8 сети, они подхватываются майнерами и включаются в биткойн-блок. Этот биткойн-блок должен быть проверен майнерами, и как только блок “решен”, все включенные в него транзакции записываются в блокчейн. Каждый последующий блок, образовавшийся в сети, добавляет к транзакции одно дополнительное подтверждение.

Биткойн-майнеры играют ключевую роль, обеспечивая точность блокчейна, поскольку берут информацию о биткойн-блоке и проверяют ее целостность. После этого к блоку данных биткойна применяется сложная математическая формула, которая превращает блок в нечто иное.

Этот “иной” вариант блока состоит из более короткой последовательности цифр и букв, которая кажется случайной. В биткойн-мире эта последовательность известна как хеш. Биткойн-майнерам гораздо легче считать хеши, чем полный блок данных, поскольку новые блоки должны генерироваться и майниться примерно раз в десять минут, и, как мы уже сказали, эти хеши чрезвычайно сложно находить, а потому этот процесс требует специализированною компьютерного оборудования.

После того как хеш решен, он хранится на блокчейне биткойна вместе с блоком, на основе которого он был получен. Этот процесс подтверждает все транзакции, записанные в данный блок, и помечает их как имеющие одно сетевое подтверждение. И хотя майнерам легче решать хеши, чем полные блоки, растущая сложность майнинга биткойна уравновешивает это и обеспечивает создание новых блоков не чаще, чем раз в десять минут.

Использование хешей само по себе достаточно интересно. Это криптографическое решение полностью защищено от подделок и работает как “печать подтверждения” для предыдущего сетевого блока. Каждый хеш основывается на хеше предыдущего блока и удостоверяет действительность предыдущего блока так же, как и любого предшествующего по цепочке.

С учетом того, сколько специализированного майнингового оборудования сейчас активно используется индивидуальными майнерами, компаниями и даже производителями оборудования, становится почти невозможно сказать, сколько же людей в данный момент активно майнят биткойны. Конкуренция очень жесткая, поскольку награда за блок в размере 12,5 BTC является щедрым вознаграждением, способным привлечь майнеров со всего мира.

Несмотря на увеличение майнинговой сложности, все большая вычислительная мощность регулярно вливается в сеть биткойна. Усиление сети не только увеличивает шанс майнеров найти очередной блок – и получить вознаграждение в зависимости от доли участия в этой напряженной работе; также это делает сеть биткойна еще безопаснее, чем раньше.

Облачный майнинг

К сожалению, когда речь заходит о майнинге биткойнов, как уже было сказано, обычным людям почти невозможно заниматься майнингом в домашних условиях (с учетом затрат на электричество, обслуживание и обновление компьютерного железа, а также уровня шума и объема тепла, выделяемых при работе оборудования, функционирующего в датацентрах). Самостоятельное решение подобных проблем подходит не

всем, поэтому появились компании, предоставляющие сервис по сдаче в аренду специализированного майнингового оборудования. Такой сервис называется облачный майнинг биткойнов.

Этот термин может заинтриговать потенциального инвестора, и тем не менее в облачном майнинге биткойнов есть свои преимущества и свои недостатки. Прежде всего, надо отметить, что, к сожалению, далеко не все компании, предоставляющие услуги облачного майнинга, являются легитимными. Появилось множество скаммеров, заявлявших, что они предоставляют услуги облачного майнинга, но впоследствии оказывалось, что это финансовые пирамиды. Подробнее о различных видах мошенничества, окружающих облачный майнинг, можно узнать из следующего материала: https://bitnovosti.com/2015/07/08/s-bitcoin-mining-a-ponzi-scheme/. Тем не менее, если предположить, что вы смогли найти одну из немногих легитимных компаний, предоставляющих этот сервис (такую, как, например, Genesis Mining, о которой мы скоро поговорим), облачный майнинг биткойнов имеет немало преимуществ.

Надо помнить, что прибыльность облачного майнинга биткойнов в большой степени зависит от текущей цены биткойна, и для большинства сервисов облачного майнинга цена биткойна выше тысячи долларов (при текущих затратах на майнинг) позволяет получить приличный возврат на инвестиции.

Преимущества облачного майнинга биткойнов

Говорят, что деньги делают деньги, и это справедливо для биткойна. Вступить в игру по майнингу биткойнов просто невозможно, не сделав первоначальных инвестиций в том или ином виде. Тем не менее облачный майнинг позволяет избавиться от необходимости инвестирования в оборудование для майнинга, оплаты за его доставку до дверей вашего дома, уплаты НДС в стране производителя и т. д., и т. п.

Как и со многими иными облачными сервисами, когда вы заказываете облачный сервис майнинга биткойнов, на самом деле вы арендуете оборудование у кого-то, кто купил его ранее и установил на нем соответствующее программное обеспечение. У вас не возникает необходимости оплаты доставки оборудования, поскольку оно уже установлено в компании, предоставляющей услугу. Это значительно сокращает расходы на изначально необходимые инвестиции, но, конечно, в немалой степени зависит от вашего местоположения.

Тем не менее при покупке облачного майнинга биткойнов остается необходимость в определенном инвестировании. Большинство компаний предлагают своим клиентам контракт на год или пожизненный, при этом данная компания обязуется в течение оговоренного срока майнить биткойны от вашего лица. Цена таких контрактов варьируется от провайдера к провайдеру.

Взамен вы как клиент сможете воспользоваться услугой облачного майнинга биткойнов уже через несколько минут после оплаты заказа. И вам не потребуется накручивать какие-то сложные настройки, поскольку каждый провайдер облачного майнинга биткойнов автоматически направит арендованное вами оборудование в какой-нибудь майнинг-пул. После этого какой-то доход начнет капать в ваш карман, и в зависимости от того, с каким провайдером вы решили связаться, ожидание возврата ваших вложений может занять больше или меньше времени.

Принимая во внимание отсутствие платы за доставку, а также налога с продаж, начисляемого страной производителя майнинг-комбайна, облачный майнинг биткойнов может показаться неплохой начальной ставкой, когда речь идет о входе в майнинг-бизнес. Важнейшим фактором, который в этом случае надо у честь, является время ожидания возврата инвестиций, не говоря уже о прибыли. А оно зависит от нескольких факторов – от цены биткойна и сложности майнинга, ко-горам изменяется каждые найденные 2016 блоков, равно как и от общей вычислительной мощности всей сети в целом.

Недостатки облачного майнинга биткойнов

Если в предложении просматриваются какие-то преимущества, то можете быть уверены, что в нем найдутся и некоторые недостатки… И в облачном биткойн-майнинге их немало.

Клиент облачного майнинга не может полностью контролировать арендуемое оборудование, поскольку не может получить доступ к майнеру физически или удаленно. Вам приходится полагаться на централизованную третью сторону, верить в то, что провайдер ведет себя честно по отношению к вам и не кладет в свой карман часть вашего дохода. И если оплата не соответствует ожиданиям клиентов, именно тут и начинается большинство проблем, касающихся облачного майнинга биткойнов. Есть несколько причин, по которым выплаты от провайдера могут казаться недостаточными, и некоторые из них даже могут быть легитимными. Непредвиденные расходы на обслуживание оборудования, изменение цены за электричество и вечно меняющаяся цена биткойна – только некоторые из возможных причин.

И опять же, нет никакого способа убедиться в том, что причина уменьшения биткойн-дохода в какой-то период времени является выдуманной. Клиенты вынуждены доверять третьей стороне – провайдеру майнинговых услуг, – а это как раз то, что призван изменить биткойн, давая каждому пользователю полный контроль над своими средствами в любой момент времени.

Другим недостатком облачного майнинга биткойнов являются платежи за обслуживание и электричество. Даже при том, что у вас нет никакого майнингового оборудования, за которое вам пришлось бы нести эти расходы, их несет провайдер облачного майнинга, и он перекладывает их на вас. Серверы, выделенные под майнинг, конечно же, не плавают в облаках. Они физически где-то находятся и для своей работы должны постоянно тратить электроэнергию. В некоторых странах мира, где электричество сравнительно дешево (например, таких, как Китай), эти затраты менее существенны.

Самым большим заблуждением людей в отношении облачного майнинга является то, что они считают, что покупают определенную вычислительную мощность и будут получать всю награду, которую намайнит эта мощность. Так не бывает, потому что провайдер будет высчитывать стоимость электричества и обслуживания пропорционально “арендованной” вами хеширующей мощности.

Тем не менее облачный майнинг может быть выгоден разумным инвесторам, которые всесторонне исследовали вопрос и все рассчитали заранее. Никогда не следует полагаться на расчет доходов, предоставленный оператором сервиса облачного майнинга, поскольку там присутствует слишком большое количество переменных, влияющих на конечный результат. К тому же в сети немало калькуляторов прибыльности майнинга, которые выдадут совсем иной – значительно худший – результат, но зато этот результат будет гораздо ближе к реальности.

Риски, связанные с облачным майнингом биткойнов

Вероятно, наибольший риск, связанный с облачным майнингом биткойнов. – это когда провайдер сервиса выглядит легитимным, но на самом деле это не так. Большинство компаний облачного майнинга биткойнов предложат вам посмотреть на фотографии их майнинг-ферм, которые, конечно, могут быть вполне реальными, но могут и не быть.

Вдобавок к этому всякий раз, когда компанию облачного майнинга взламывают – а это сейчас стало происходить сплошь и рядом, – подобный инцидент не проходит без отрицательных последствий для доходов клиентов. В подобных случаях средства пользователей, как правило, пропадают, и провайдеры майнинговых услуг вынуждены снизить выдачу монет клиентам для покрытия собственных потерь.

Как положительный пример можно привести компанию Genesis Mining (www.genesis-mining.com) – компанию облачного майнинга из Гонконга, легитимность которой уже достаточно подтверждена. Компания присутствует на рынке облачного биткойн-майнинга с 2013 года и предлагает пожизненные контракты по приемлемым ценам. В отличие от прочих компаний такого рода, при покупке контракта у Genesis Mining можно не бояться скрытых комиссий.

Если вы в какой-то момент решите купить контракт на услуги облачного майнинга, имейте в виду, что очень скоро может появиться гораздо лучшее предложение. Рынок облачною майнинга постоянно развивается, изменяется и становится все более конкурентным. Всегда проводите собственные исследования, рассматривайте несколько предложений от разных провайдеров и принимайте хорошо обоснованное решение. Не поддавайтесь на предложения, которые выглядят слишком хорошо, чтобы быть правдой. Обычно так оно и оказывается.

Влияние майнинга на безопасность биткойна

Сеть биткойна настолько сильна и безопасна, насколько люди поддерживают ее посредством запуска биткойн-узлов или выделением компьютерных мощностей на майнинг.

Как уже обсуждалось в главе 10, одной из вещей, создающих у грозу биткойн-сети, является так называемая атака 51 %. Чем больше вычислительных мощностей участвует в процессе майнинга, тем меньше шансы потенциального злоумышленника завладеть 51 % хеш-мощности сети и принести вред биткойну.

С точки зрения майнера, конечно, монетарный выигрыш является наиболее очевидным стимулом выделения мощного майнингового оборудования. Тем не менее есть и такие майнеры, которые выполняют эту “работу” с целью усилить защищенность сети биткойна. Денежное же вознаграждение рассматривается ими как дополнительный бонус. Но вне зависимости от того, на какой стороне силы они находятся, майнинг усиливает защищенность сети биткойна посредством подтверждения транзакций и наращивания блокчейна.

Но есть и еще кое-что. Майнинг также защищает нейтральность сети, препятствуя одиночному майнеру или пулу заблокировать другие транзакции. Как объясняется в главе 10, любой, кто набирает достаточно вычислительной мощности, может подтверждать только свои блоки и на неопределенное время оставлять без подтверждений все остальные транзакции.

Биткойн-майнинг делает обращение свершившейся транзакции все более сложным с течением времени для одиночного майнера или майнинг-пула, так как придется переписать все блоки, следующие за этой транзакцией. Каждый блок в сети с течением времени получает все больше подтверждений. Поэтому критически важно, чтобы блокчейн продолжал расти и новые блоки генерировались примерно раз в десять минут.

Биткойн-майнинг задумывался очень ресурсоемким и с течением времени должен становиться даже еще более ресурсоемким. Каждый блок, найденный в сети, требует предоставления определенного доказательства выполненной работы перед тем, как он будет засчитан. Затем он проверяется всеми биткойн-узлами сети. Как только эти узлы приходят к непротиворечивому консенсусу об отсутствии подделки, новые монеты децентрализованно распространяются по сети, поощряя майнеров продолжать поддерживать сеть компьютерными мощностями. Большее количество ресурсов означает более высокий уровень безопасности, и весь этот цикл продолжает самовоспроизводиться.

Как начать собственный майнинг

Принять участие в майнинговой игре сейчас еще сложнее, чем раньше. В последние годы эволюция майнингового оборудования развивалась со все возрастающей скоростью, – как следствие увеличения сложности майнинга. В свою очередь, это требовало все более мощных аппаратных средств для решения блоков. Тем не менее все еще сохраняются широкие возможности для желающих поучаствовать в майнинге,

конечно, при условии, что вы согласны вложить в это дело значительные ресурсы и все тщательно просчитали заранее.

Обзаводимся правильным оборудованием

Когда в 2009 году биткойн только появился, процесс майнинга был достаточно прост. Все, что нужно было сделать пользователю, – так это поставить программу – биткойн-клиент, синхронизоваться с сетью Биткойн и удостовериться, что флажок на вкладке Майнинг установлен. Любые типы компьютерных процессоров – даже те, которые были установлены в ноутбуках – подходили для майнинга, потому что в сети почти отсутствовала конкуренция. Фактически первые несколько недель существовала всего горстка майнеров.

У биткойн-энтузиастов не ушло много времени на то, чтобы придумать код для запуска вычислительного процесса на видеокартах, ведь видеокарты как раз и были задуманы для вычислительных операций. Даже во время воспроизведения картинки в видеоиграх видеокарта занимается ничем иным, как обработкой данных и вычислениями – снова и снова, с огромной скоростью.

Разница в скорости майнинга на CPU и GPU была просто поразительной. Когда первые майнеры на GPU вступили в игру, мощность сети возросла десятикратно. Но несмотря на всю эту дополнительную майнинговую мощность, новые блоки по-прежнему добывались раз в десять минут из-за изменения уровня сложности вычислений.

Несколько лет назад, когда наступила эра FPGA, майнинг на CPU и GPU полностью устарел. Аббревиатура FPGA расшифровывается как “Программируемая пользователем вентильная матрица”. Эта матрица предоставляет вычислительную мощность, сравнимую с хеш-мощностью видеокарт, распространенных в 2013 году, но при этом матрица FPGA гораздо более энергоэффективна, чем видеокарта. Разумеется, многие майнеры за несколько лет переключились с CPU на GPU, а затем на FPGA.

Но бизнес аппаратного обеспечения для майнинга продолжает эволюционировать и сейчас, так что и FPGA очень быстро стали бесполезными. В 2013 году на арену вышли биткойн-АСИКи (ASICs); энергопотребление этих “интегральных схем специального назначения” было еще меньше, чем у FPGA, и при этом их производительность была значительно выше, чем у GPU и FPGA.

Надо сказать, что и АСИКи не идеальны. Хотя их энергопотребление значительно ниже, чем у графических адаптеров, производимый ими шум вырос экспоненциально, эти машины никак нельзя назвать бесшумными. Вдобавок АСИК-майнеры вырабатывают огромное количество тепла и имеют радиаторы воздушного охлаждения, температура которых превышает 150 градусов по фаренгейту (49 С).

Покупка АСИК-майнера также требует существенных затрат на перевозку – эти машины весьма тяжелы. Вдобавок вам гарантированно вменят к оплате пошлину за импорт ввиду их немалого размера и веса. В общем, в настоящий момент АСИК-майнеры являются очень дорогостоящей инвестицией, не предоставляющей абсолютно никаких гарантий в отношении выхода в безубыточность, не говоря уже о какой-либо прибыли.

И последнее, но очень важное замечание: вычислительная производительность АСИКов так велика только до тех пор, пока они не упрутся в невидимый предел. Эти устройства по большей части не способны выдавать больше чем 1,5 TH/c (терахеш в секунду), что вынуждает клиентов покупать их оптом, если они намерены начать хоть сколько-нибудь серьезный майнинговый бизнес.

Полагаю, для вас теперь уже не станет сюрпризом известие о том, что большинство индивидуальных пользователей давно отошли от майнинга биткойнов на собственном оборудовании и переключились на облачный майнинг (и это даже при том, что существует масса рисков, связанных с нелигитимностью множества компаний облачного майнинга биткойнов). Читайте предыдущие разделы об облачном майнинге, в которых описывается, какие меры предосторожности необходимо предпринять, чтобы не попасть впросак.

Рассчитываем стоимость

Вне зависимости от того, хотите вы приобрести собственное оборудование или подписать контракт с провайдером облачного майнинга, предварительно вам следует выполнить домашнюю работу по определению уровня затрат, прибыли и ожидаемого времени возврата инвестиций вплоть до момента, когда вы начнете выходить в прибыль.

Стоимость майнинга выходит далеко за пределы первоначальных инвестиций в оборудование, цену логистики и импортные пошлины. Поскольку цены на электричество рознятся от страны к стране, один из главных факторов, которые нельзя упускать из виду, – это потребление электроэнергии.

В большинстве стран цена за киловатт-час (кВ/ч) электроэнергии делает майнинг биткойнов занятием бесприбыльным. Проверьте свой недавний счет за электричество и найдите в нем цену за киловатт-час, а затем посчитайте, сколько киловатт-часов в день будет потреблять ваш биткойн-майнер.

Например, биткойн-майнер, потребляющий из энергосети мощность 600 Вт, будет потреблять 12,4 кВт/ч в день. Это очень просто рассчитать: 600 Вт х 24 ч в день = 12 400 Вт или 12,4 кВт/ч. Если цена за киловатт-час составляет 10 центов, то ваш дневной чек за электричество будет составлять 1,24 доллара.

Необходимо сопоставить эти затраты с дневным доходом, который вы сможете заработать на майнинге. Этот дневной доход будет силы-но зависеть от цены биткойна, которая на момент написания книги была относительно невысока. Повышение цены биткойна может существенно повысить прибыль от майнинга при условии, что тариф за электроэнергию останется на прежнем уровне (до тех пор, пока энергоснабжающая организация не решит его повысить).

Однако оплата электроэнергии – далеко не единственная статья в списке расходов. Владеть биткойн-оборудованием означает постоянно поддерживать его в работоспособном состоянии и восстанавливать, если что-нибудь вдруг сломается. Некоторые АСИК-майнеры биткойнов поставляются без блока питания, и вам предстоит купить его самостоятельно.

Но самый большой и наиболее важной составляющей затрат будут инвестиции вашего времени и усилий по оптимизации прибыли от майнинга. Как правило, перед отправкой клиенту оборудование для майнинга настраивают для работы с максимально возможной производительностью, и тем не менее всегда остается место для тюнинга. Большинство производителей регулярно выпускают свежие прошивки для майнингового оборудования с целью исправить выявленные баги и выжать из железа еще немного дополнительной вычислительной мощности.

Использование калькулятора расчета прибыльности

К счастью, расчет цены и потенциальной доходности майнинга биткойнов не требует научной степени по математике или даже бумаги и ручки. Некоторые веб-сайты специализируются на точных расчетах прибыльности биткойн-майнинга. Вам всего лишь потребуется ввести некоторые исходные данные о параметрах оборудования вашего оборудования и цене электроэнергии.

Присмотритесь к этим веб-сайтам по расчету прибыльности майнинга. Они покажут вам ожидаемую рентабельность майнинга не только на текущий момент, но и на ближайшее будущее Сложность биткойн-майнинга изменяется каждые 2016 блоков, что тоже будет оказывать непосредственное влияние на ваш доход. Если сложность возрастает, ваш доход слегка уменьшается, и наоборот: если сложность уменьшается, то ваш доход возрастает

Чтобы воспользоваться калькулятором расчета прибыльности майнинга, просто введите в поисковике ключевую фразу “калькулятор прибыльности майнинга биткойна”. Один из русскоязычных калькуляторов предлагается вашему вниманию по адресу https://bits.media/calculator/.

Часть IV
Великолепные десятки

В этой части…
• Знакомимся с десятью наилучшими способами использования биткойнов
• Выясняем, какие существуют интересные альтернативные валюты
• Узнаем, какие еще доступные источники информации о технологии биткойна имеются в Сети и не только

Глава 12. Десять способов использования биткойна

В этой главе…
• Изучаем возможности для инвестиций
• Исследуем образовательный потенциал
• Тратим биткойны!

Биткойн можно использовать множеством различных способов, и единственной проблемой здесь является лишь его ограниченная приемлемость в качестве платежного средства. Однако с ростом популярности этой цифровой валюты, когда все больше продавцов начнут принимать биткойны, вы сможете покупать за них что угодно. Ура!

Не важно, хотите ли вы использовать биткойн в образовательных целях, для получения дополнительного дохода или изучать его с инвестиционной точки зрения. – эта цифровая валюта позволяет делать практически все. В этой главе мы опишем десять способов применения биткойна, хотя на самом деле их количество измеряется сотнями.

Биткойн в качестве инвестиционного инструмента

Большинство людей рассматривают биткойн в качестве инвестиций в будущее. Учитывая, что его предложение ограничено 21 миллионом монет (что будет достигнуто к 2140 году), а цена пока что все еще относительно низка, существует достаточно много возможностей быстро заработать, инвестируя в него.

Нет ничего плохого в попытках заработать на ценовых колебаниях, но учтите, что вы можете и потерять.

Существуют и другие формы использования биткойна в качестве инвестиционного инструмента. Инвестиции в биткойн можно рассматривать как часть долгосрочного плана, а не возможность быстро заработать (или прогореть). Биткойн все еще находится на заре своего развития, радуя нас своим присутствием всего лишь около восьми лет. Подавляющему большинству людей все еще только предстоит научиться использовать биткойн, что, в свою очередь, создаст новые возможности для инвестиций.

Использование биткойна в образовательных целях

Главной задачей биткойна, как мы ее видим, всегда была демонстрация людям возможностей блокчейна, позволяющих взять в свои руки контроль над финансами и всеми другими аспектами жизни, а также полностью пересмотреть взгляд на мир.

Куда бы вы ни посмотрели, везде можно увидеть мошенничество, коррупцию, бесхозяйственность, подавление свобод и прав собственности, финансовые ограничения и много других вещей, неприемлемых в наши дни. Когда Сатоши Накамото создавал биткойн, его главной идеей было не просто разработать новую подрывную технологию, но также показать обычным людям, как децентрализация позволяет победить коррупцию и самодурство.

До сих пор основное внимание было приковано к цене и финансовому аспекту биткойна. Эти сферы в своем нынешнем виде далеки от идеала, и биткойн позволяет показать людям, как можно – и нужно – изменить нашу текущую финансовую систему.

Но и это не все, поскольку образовательная сила биткойна выходит за границы финансов и технологии. Потенциальные возможности блокчейна и Биткойна 2.0 способны изменить все аспекты нашей жизни (об этом мы уже говорили в главе 7). Как только вы осознаете все возможности биткойна и блокчейна, вы поймете, что они способны коренным образом перевернуть нашу повседневную жизнь. К примеру, он может исключить человеческий фактор из многих вещей, включая цифровое голосование, ведение переговоров, подписание контрактов и осуществление пиринговых транзакций. И это лишь малая часть возможностей блокчейна, которые можно и нужно продвигать на примере биткойна.

Биткойны для ежедневных покупок

Биткойн – это электронная форма оплаты, и именно этим он привлекает к себе так много людей. За последние годы появилось множество мест, принимающих биткойны в качестве альтернативы стандартным платежным средствам – главным образом благодаря низким комиссиям, быстрым транзакциям и отсутствию риска мошенничества или возврата денег.

В результате биткойн становится вполне жизнеспособной формой оплаты как в Интернете, так и в магазинах по всему миру. Экосистема биткойна главным образом держится на осуществлении международных транзакций – это означает, что торговля является ключевым фактором поддержания ее жизнеспособности.

Учитывая большой выбор продавцов, принимающих биткойны в качестве оплаты за самые разнообразные товары и услуги, эта цифровая валюта постепенно завоевывает самую широкую популярность.

Один из интересных способов потратить биткойны – заказать за них доставку еды на дом. Или почему бы не оплатить ими ваш любимый кофе в Starbucks? Возможности поистине безграничны.

Быстрый поиск в Интернете по этой теме показывает, что способов потратить свои монеты гораздо больше, чем вы могли бы представить. Если вы хотите получить больше информации, выполните поиск по следующим запросам.

- “Потратить биткойны”
- “Использовать биткойны”
- “Оплатить биткойнами”
- “К оплате принимается биткойн”

Шикарная жизнь за биткойны

Биткойн смог привлечь к себе людей из совершенно разных социальных групп. Помимо предоставления людям возможности стать частью новой финансовой экосистемы, он может использоваться и для более редких покупок, таких как авиабилеты и бронирование гостиниц. Хотя пока еще далеко не каждый о гель и билет на самолет можно оплатить биткойнами, уже существует много сервисов, облегчающих этот процесс (например, BTCtrip – https://btctrip.com).

Один из интересных феноменов, обнаруженных этими компаниями, заключается в том, что биткойн-клиенты готовы больше тратить на отели и полеты. Возможно, причина этого кроется в том, что владельцы биткойнов в целом больше тратят на путешествия, а может быть, свою роль сыграли заниженные при покупке курсы. Точная причина этого феномена до сих пор неизвестна, но это убедительное доказательство преимуществ биткойна как для покупателей, так и для продавцов.

Поддержите биткойнами благотворительные организации

Одним из важных социальных аспектов жизни является возможность оказывать помощь нуждающимся людям. Биткойн может использоваться для пожертвований во многие благотворительные организации, включая Красный Крест и Гринпис. Некоторые организации даже помогут вам с отчислением суммы пожертвования из ваших ежегодных налогов, если вы перечислите им биткойны.

Однако главное преимущество биткойна с точки зрения благотворительности – возможность отправлять деньги напрямую нуждающимся, не полагаясь в этом на сторонние организации. К примеру, после недавнего землетрясения в Непале энтузиасты отправляли свои биткойны напрямую в местный фонд помощи, не прибегая к услугам благотворительных организаций в своих странах. В результате средства дошли до пострадавших районов быстрее и в большем объеме, и члены биткойн-сообщества смогли помочь тысячам людей.

Азартные игры в Интернете

Азартные игры в Интернете запрещены в некоторых государствах, поэтому, прежде чем следовать этому совету, внимательно изучите законодательство своей страны.

Если вы не нашли никаких запретов на этот счет, учтите, что биткойн предлагает прекрасную альтернативу стандартным платежным средствам. Для депозитов не требуется предоставлять ни личные детали, ни сканы документов – просто отправьте деньги на кошелек казино и начинайте играть.

Транзакции в сети биткойна проходят быстро и не подлежат возврату, что делает их хорошим выбором для поставщиков услуг в Интернете, включая онлайн-казино.

Ну, конечно, мы знаем, что вы – здравомыслящий и сознательный человек, но на всякий случай еще раз напоминаем вам о необходимости играть в азартные игры ответственно. Все, лекция закончена!

Инвестиции в драгметаллы: изобретаем заново золотой стандарт

Хотя технически это ничем не отличается от использования биткойна в качестве инвестиционного инструмента, очень мало людей знают, что его можно использовать для покупки драгоценных металлов, в частности – золота и серебра.

В дополнение к вышесказанному различные онлайн-платформы позволяют пользователям торговать биткойнами и приобретать за них драгоценные металлы в формате дей-трейдинга. Некоторые из таких платформ успешно существуют на протяжении уже нескольких лет: однако не забывайте проводить собственные расследования, прежде чем доверяться одной из них.

Например, самая популярная платформа на момент написания этих слов – Vaultoro (https://www.vaultoro.com), сосредоточенная на торговле золотом за биткойны. Среди других – MidasRezerv (https://midasrezerv.com), Uphold (https://uphold.com) и BitGold (https://bitgold.com). Всегда изучайте репутацию компании, прежде чем вложить свои биткойны.

Раздавайте их! Радость дарения биткойнов

Цифровая валюта является идеальным подарком для друзей, родственников и любимых.

Существуют также сайты, предлагающие купить подарочные сертификаты за биткойны. Среди них – Gyft (https://gyft.com) и eGifter (https://egifter.com). Магическая сила подарочных сертификатов позволяет оплачивать покупки биткойнами даже в магазинах, не принимающих цифровую валюту напрямую.

Оплата счетов

Возможность оплачивать счета биткойнами зависит от вашего места жительства. Однако есть много платформ, позволяющих заплатить биткойны за что угодно в обмен на небольшую комиссию.

В ближайшем будущем каждый сможет оплатить счета за телефон, ипотеку и коммунальные услуги биткойнами. Так, в некоторых странах мира уже можно использовать биткойн для оплаты услуг сотовой связи.

Использование биткойна в качестве социального эксперимента

Давайте предположим, что вы неровно дышите к биткойну и вас удручает его недостаточная распространенность. Почему бы не попытаться убедить продавцов и покупателей начать его использовать?

В конце концов, расширение экосистемы отнимает много времени и усилий, и поскольку у биткойна нет централизованной власти, способной взять решение этого вопроса в свои руки, каждый член сообщества несет определенную ответственность за его продвижение.

Все вышеописанное – лишь малая часть возможностей, открывающихся благодаря биткойну. Вы очень поможете сообществу, если придумаете свой креативный способ использования этой цифровой валюты. Поэтому не стесняйтесь делиться рассказами о том, как вы использовали биткойн, с его сторонниками.

Глава 13. Десять (или около того) других криптовалют

В этой главе…
- Торгуем разными криптовалютами
- Заглядываем в сообщество альткойна
- Азартные игры и краудфандинг

Мир цифровых валют полон нетерпеливых разработчиков, считающих себя способными создать “следующий биткойн”. В течение нескольких лет были созданы многие тысячи альтернативных криптовалют (альткойнов), но многие из них пропали, так как были ни чем иным, как созданными с целью быстрой наживы надувательскими схемами “памп-дамп”. Однако, помимо биткойна, есть несколько других альткойнов, имеющих некоторое значение даже несмотря на то, что в ближайшее время они никак не сумеют свергнуть биткойн с престола.

В данной главе рассматривается десять цифровых валют с разными преимуществами. (Чтобы выстроить весь список до десятого пункта, мы хотели добавить в нею и биткойн, потому что считаем его классным прежде всего и перво-наперво, но наш редактор не допустил бы это к печати. Так что здесь будет описано лишь девять криптовалют.)

Litecoin: серебро для золота биткойна

Возможно, самый широко известный альткойн – это Litecoin, или лайткойн (https://litecoin.org/), в котором используется совершенно другой алгоритм (Scrypt), чем в биткойне (SHA-256). Лайткойн был первым альткойном, использующим алгоритм Scrypt, что дало майнерам биткойна повод оставить в работе, а не выбросить свои устаревшие после прихода АСИКов видеокарты и сгенерировать прибыль, направив их мощность на майнинг лайткойна.

Лайткойн сумел остаться на плаву на протяжении длительного периода времени просто потому, что был первым, кто попробовал и сделал нечто новое. Внутренняя идеология привела к созданию заметного сообщества лайткойна, остававшегося лояльным на протяжении всех этих лет.

Единственный дополнительный плюс лайткойна, помимо применения устаревших видеокарт для майнинга, заключается во времени между нахождением новых блоков, примерно равном 5 минутам, в сравнении с 10 минутами у биткойна.

Огромная доля успеха лайткойна может быть приписана всем криптовалютным биржам, добавившим соответствующие торговые пары, таким образом создавая вторичные торговые рынки. На самом деле лайткойн может торговаться практически на любой современной криптовалютной бирже, однако лишь несколько бирж предлагают опцию лайткойн/фиатные валюты. Разные платежные процессоры добавили лайткойн к своим спискам альткойнов, давая сообществу способ траты LTC в большинстве тех мест, где уже принимается биткойн.

Многие из существующих на сегодняшний день альткойнов основаны на алгоритме Scrypt.

Ethereum и Ethereum classic: смарт-контракты на блокчейне

Блокчейн биткойна записывает только транзакции – кто сколько монет кому отправил. Но что если добавить

к этим транзакциям полноценный язык программирования? Мы получим “умные контракты”, в которые можно вложить практически любую логику управления денежными потоками. Ethereum стал первым блокчейном, реализовавшим данную идею.

Идея полностью программируемых денег завоевала серьезную популярность, привлекла многих разработчиков, за которыми последовали и серьезные инвестиции в экосистему эфириума. Возникли даже инвестиционные фонды, реализованные в “коде на блокчейне”, крупнейший из которых, TheDAO, привлек 150 миллионов долларов инвестиций, рекламируясь под громким лозунгом “Код есть закон!” Ирония этого лозунга стала очевидной очень скоро, когда неизвестные злоумышленники воспользовались уязвимостью в программном коде TheDAO и извлекли из фонда около 50 миллионов долларов.

Шок от этого взлома привел к тому, что часть эфириум-сообщества решила пожертвовать неизменностью блокчейна и переписать историю транзакций, чтобы “вернуть деньги” незадачливым инвесторам. Другая же часть сообщества наотрез отказалась нарушать базовый принцип неизменности блокчейна (https://ethclassic.ru/2016/07/14/a-crypto-decentralist-manifesto/). В результате этого разногласия единый до того времени блокчейн раскололся на неизменный Ethereum classic и модифицируемый Ethereum. которые сохраняют техническую совместимость, но являются теперь различными криптовалютами, ETC и ETH, сообщества которых придерживаются противоположных философии и принципов.

Узнать больше об этой захватывающей истории, а также о смарт-контрактах и децентрализованных приложениях можно на сайте https://ethclassic.ru.

Dogecoin: такая очень “Вау”, просто дико веселая монета

Когда произошел запуск системы Dogecoin (https://dogecoin.com/), она должна была стать криптовалютой-“мемом”, так как была презентована публике в очень мультяшном стиле. Догекойн не имел фиксированной денежной массы и использовал алгоритм Scrypt, так что никто даже и не ожидал от нее последующего присоединения к ряду основных криптовалют.

Но неожиданно эта прикольная криптовалюта оказалась весьма популярной среди тинейджеров. Догекойн гордится собой за то, что является общественной криптовалютой, это даже привело к различным попыткам сообщества собирать средства на хорошие дела.

Два положительных случая сбора средств с догекойн – включение Ямайской команды по бобслею в Олимпийские игры 2014 года в Сочи, а также сбор средств для участия Джоша Уайса в Супергонке NASCAR.

Dash, ранее известная как Darkcoin

Вы могли заметить, что на протяжении всей книги устойчиво продолжает всплывать тема анонимности. Биткойн, по сути, предоставляет не полную анонимность, а скорее псевдосанимность, когда пользователи могут маскировать свои личности с помощью адреса в кошельке. Такая недостача анонимности позволила разным разработчикам альткойнов предложить потенциальные решения данной проблемы, в результате чего были разработаны усовершенствования, способные (или не способные) выстроить свой будущий путь в рамках ПО биткойна.

Дарккойн, или дэш (https://dash.org/), как он зовется в наши дни, входит в группу криптовалют, делающих акцент на анонимность. Эван Даффилд, главный разработчик дэш, выступил с несколькими творческими решениями по созданию полностью автономных и анонимных транзакций в сети Дэш. Эта криптовалюта продолжает быть одной из самых популярных анонимных альткойнов. Впрочем, на пятки ему наступают

окучивающие ту же грядку анонимности конкуренты, такие как ZCash и Monero.

Ripple: криптовалюта для банкиров

С какой бы криптовалютой вы ни столкнулись, все они поддерживают идеологию децентрализации. А вот валюта “риппл” (https://ripple.com) сделана из другого теста, так как не предусматривает ни майнинга, ни децентрализации. Она была полностью эмитирована в самом начале (в количестве 100 миллиардов), а теперь поддерживается и управляется корпорацией Ripple Labs. По рыночной капитализации монета “риппл” сегодня занимает значительное пространство в мире криптовалют.

Целью разработки системы Ripple является предоставление криптовалютной платформы с целью улучшения технологии межбанковских расчетов. В этом качестве риппл постоянно вызывает интерес журналистов. Протокол криптовалюты был внедрен Fidor Bank и другими банками по всему миру в качестве эксперимента по внедрению криптотехнологии. По мнению банковских специалистов, технология распределенных кошельков, представленная системой Ripple, имеет ряд преимуществ перед технологией блокчейна биткойна, при этом в их число входят как безопасность, так и цена.

Peercoin: представляем proof-of-stake

У биткойна и лайткойна есть одна общая черта: новые монеты могут генерироваться лишь через процесс майнинга. Валюта “пиркойн” (https://peercoin.net/) была одним из первых “клонов” биткойна, предложивших новую систему генерации монет, названную proof-of-stake (доказательство владения). Она работает на базе того условия, что у вас в кошельке находится некоторое количество монет на протяжении определенного промежутка времени, которые вы не тратите.

Как только эти монеты достигнут определенного возраста – периода времени, на протяжении которого их не отправляли, – они генерируют небольшой процент прибыли. В целом этот принцип работает так же, как и банковские депозиты, но в полностью децентрализованной манере, и пользователь имеет полный контроль над своими средствами в любой момент времени.

Генерация новых пиркойнов через алгоритм proof-of-stake также предоставляет дополнительный уровень сетевой стабильности, ведь количество майнеров может уменьшаться со временем, но несмотря на это всегда найдутся пользователи, хранящие свои PPC. Разработчики пиркойна определили постоянный коэффициент инфляции в 1 % в год без установки фиксированной денежной массы.

StartCOIN: краудфандинг

Старткойн нацелен на краудфандинг и основан на системе наград. Монета вознаграждает пользователей, которые делают ставки, делятся, а также хранят свои старткойны на отдельном веб-сайте, названном StartCOIN (https://startcoin.org/).

Краудфандинг набирает популярность, которую система старткойна превращает в преимущество, позволяя сообществам финансировать идеи, разработки и проекты. Те, кто пересылает или получает средства через указанный веб-сайт, позднее вознаграждаются дополнительными старткойнами для поддержания их энтузиазма.

NXT: используем механизм proof-of-stake для достижении консенсуса по транзакциям

В отличие от консенсуса биткойна, достигаемого через майнинг, в системе NXT (https://nxt.org/) для достижения консенсуса по транзакциям используется метод proof-of-stake. Кроме того, валюта NXT является одной из немногих криптовалют, не имеющих процесса майнинга – все монеты были распределены во время запуска данного альткойна в обращение. Наличие постоянного источника монет, доступного в любое время, создало новую экосистему в мире криптовалют.

Что делает валюту NXT действительно интересной, так это наличие опции создания пользователем собственной криптовалюты внутри экосистемы NXT. Все созданные монеты подкреплены валютой NXT и могут распространяться разными способами.

Относительно недавно в системе NXT были постепенно введены в эксплуатацию новые функции, такие как умные контракты, служба произвольных сообщений и действительно децентрализованная платформа обмена, получившая название “MultyGateWay”.

CasinoCoin: брэндинг для пользователей казино

Есть монета, которая начинает ощущать прибыль от правильно выбранного названия уже сейчас, и это – казинокойн (https://casinocoin.org/). Судя по ее названию, можно сделать очевидное предположение, что эта криптовалюта имеет отношение к рынку казино.

Казинокойн позиционирует себя при использовании той же технологии, что и лайткойн (алгоритм Scrypt), однако за счет брэндового имени позволяет публике немедленно осознать, где пролегает область действия монеты и кто ее целевая аудитория.

Глава 14. Список онлайн-ресурсов

В этой главе…
- Учимся искать дополнительную информацию
- Следим за новостями в Сети и в обычных СМИ
- Держим руку на пульсе последних новостей биткойн-торговли

Узнать больше о биткойне, блокчейне и о том, как развивается эта цифровая валюта, можно самыми разными путями, а не только со страниц этой книги, хотите – верьте, хотите – нет.

В действительности в вашем распоряжении имеется довольно много ресурсов, которые ставят своей целью предоставление вам самой свежей информации об экосистеме биткойна. В этой главе вы найдете информацию о десяти (или около того) наиболее интересных источниках новостей о биткойне и биткойн-сообществе.

Биткойн и Википедия

Наличие объективного и независимого источника информации о биткойне является ценным достоянием для сообщества виртуальных валют, поскольку в этой области постоянно появляются изменения, обновления и новые сервисы. Одним из наиболее часто используемых источников информации в Интернете является Википедия, в которой биткойн имеет собственный подраздел. Вся специальная терминология этой системы объясняется здесь достаточно подробно.

В разделе Википедии, посвященном биткойну, вы найдете любую информацию от сведений о его создателе Сатоши Накамото (хотя его фигура до сих пор остается почти мистической и довольно загадочной) до объяснения всех тонкостей майнинга, особенностей управления узлом биткойна и многое-многое другое. Определенно, это источник информации, за которым нужно постоянно следить, так как всегда есть вероятность узнать из него что-то такое о биткойне, чего вы еще не знали.

Страница в Википедии: https://ru.wikipedia.org/wiki/Биткойн.

Англоязычный вариант: https://en.wikipedia.org/wiki/Bitcoin.

Форумы BitcoinTalk

Одним из самых популярных мест для ведения дискуссий по теме биткойна и обзоров предлагаемых в этой среде услуг являются форумы на сайте bitcointalk.org. Эти форумы, посвященные биткойну и созданные много лет назад, являются самым популярным местом для публикации новостей, запуска и разработки биткойн-проектов, предоставления информации об услугах и товарах, а также многого другого. Если в системе биткойна есть что-то, что вы хотели бы обсудить с другими заинтересованными лицами, то форумы сайта BitcoinTalk являются как раз тем местом, где это можно было бы с успехом осуществить.

Следует отметить, что вовсе не все, что размещено на форумах BitcoinTalk, обязательно связано исключительно с биткойном. Здесь также имеются отдельные разделы, выделенные для обсуждения альтернативных виртуальных валют, включая Litecoin, Dogecoin и др. Кроме того, существуют специальные подфорумы для некоторых популярных языков, включая голландский, французский, русский и китайский.

Чтобы посетить эти форумы, воспользуйтесь ссылкой https://bitcointalk.org.

Официальный сайт биткойна Bitcoin.org (и bitcoin.com)

Можно считать, что сайт bitcoin.org всегда был “домашней” страницей биткойна в Интернете. Краткое описание биткойна, несколько демонстрационных видеороликов и набор ссылок для скачивания соответствующего программною обеспечения биткойн-кошельков – вот что представляет собой этот портал. Благодаря подаче информации в простой и удобной манере, вполне доступной даже для начинающих пользователей, этот сайт – отличное средство представить биткойн всему внешнему миру. Официальный сайт биткойна на русском языке (это один из 26 языков, доступных на сайте) вы найдете по адресу https://bitcoin.org/ru/.

Оригинальная работа создателя биткойна Сатоши Накамото доступна по адресу https://bitcoin.org/files/bitcoin-paper/bitcoin_ru.pdf

В числе первых результатов поиска – когда информация о биткойне запрашивается в поисковых машинах Google или Bing – всегда присутствует сайт bitcoin.com. Этот сайт (на английском языке) содержит много полезной информации, включая раздел новостей, содержимое которого обновляется каждый день, а также предоставляет доступ к биржам как к источникам приобретения биткойнов, форумам, магазинам и т. д. Для перехода на этот сайт воспользуйтесь ссылкой https://bitcoin.com.

Новостные сайты и блоги биткойна

В Интернете для любой значимой или перспективной темы всегда появляется несколько специализированных новостных сайтов, посвященных исключительно соответствующей тематике. И биткойн здесь не исключение – этой теме также посвящено несколько новостных блогов, которые являются преимущественно хобби-проектами, а значит, их содержимое обновляется нерегулярно, от случая к случаю. Биткойн – тема относительно новая, и здесь пока еще достаточно места для здоровой конкуренции в отношении публикации новостей.

В Сети существует немало источников новостной информации обо всем, что происходит в мире биткойна. Из англоязычных наиболее значащими из них можно считать следующие.

- https://bitcoinmagazine.com – сайт журнала Bitcoin magazine
- https://insidebitcoins.com/news – новостной сайт Inside Bitcoins
- https://www.coindesk.com – портал Coin Desk
- https://bitcoinist.net – портал Bitcoinist, предоставляющий также доступ к своему форуму
- https://bitcoin.com – этот сайт упоминался в предыдущем разделе

На русском языке почитать новости из мира биткойна можно на следующих сайтах.

- https://bitnovosti.com/ – новости мира биткойна
- https://ru.newsbtc.com/ – новости биткойна и блокчейна
- https://bits.media/calculator/ – новостной сайт и калькулятор для майнинга биткойнов
- https://www.facebook.com/bitcoinru/ – биткойн-сообщество в Facebook
- https://ethclassic.ru/ – все о смарт-контрактах и блокчейн-приложениях
- https://blockchain.community/ru/ – блокчейн-сообщество в России

Средства массовой информации

Несмотря на то что у основных СМИ есть привычка относить биткойн к негативной стороне бытия, в последнее время теме виртуальных валют в них уделяется больше внимания, чем когда-либо прежде. И интерес к этой теме постоянно растет.

Этот интерес вполне понятен. Революционная технология, положенная в основу биткойна, в перспективе может иметь большое значение для финансовых учреждений и инновационных компаний, а сам биткойн как валюта может помочь гражданам законно обходить тотальный контроль над капиталом, осуществляемый всеми правительствами.

И хотя общая оценка системы биткойна по-прежнему остается в большинстве случаев отрицательной, основные средства массовой информации внимательно следят за развитием виртуальных валют. Все больше людей во всем мире узнают о существовании биткойна и его удивительных возможностях, поэтому основным СМИ так или иначе придется идти в ногу с этой тенденцией, если они намерены сохранять свою актуальность. Как пример можно привести следующие источники.

- Онлайн-видео о криптовалютах: http://www.bitnovosti.tv/
- Документальный фильм Криптовалюты. Золото цифрового века: https://www.youtube.com/watch?v=Aybt-UZb4kk

Диаграммы цены биткойна

Биткойн – это нечто большее, чем просто текущая цена его обмена на ту или иную валюту, но многие люди предпочитают сосредоточить свое внимание именно на колебаниях текущего значения курса биткойна. Существуют различные сайты, на которых можно следить за текущей ценой биткойнов, средним объемом торгов и диаграммами, представляющими различия в заказах на покупку и продажу.

Сайт BitcoinWisdom является одним из наиболее часто посещаемых. На нем объединяются данные с различных бирж по всему миру, распределенные по основным парам торговли валютой. Вся информация на нем

бесплатна для использования и обновляется в режиме реального времени.

Интересным для вас также может быть сайт Coinmarketcap.com, на котором отражается текущая рыночная капитализация для всех существующих виртуальных валют.

Для доступа к указанным выше источникам используйте следующие ссылки.

- https://bitcoinwisdom.com – сайт Bitcoin Wisdom
- https://coinmarketcap.com – сайт компании Coinmarketcap

Сайт FiatLeak

Для тех, кто не любит весь день смотреть на скучные финансовые графики, существует сайт FiatLeak.com – интересное средство наблюдения за происходящим на биржах в режиме реального времени. Сайт FiatLeak (доступен также на русском языке) выдает визуальное представление поступающих заказов на продажу биткойнов в реальном времени. На его странице символы биткойнов летают по карте всего мира, наглядно показывая, какая страна отвечает за самый большой объем торгов в каждый момент времени.

Наблюдать за таким веб-сайтом довольно забавно, и в то же время эта картинка просто завораживает: ведь в действительности имеет место гораздо больший объем торговли биткойнами, чем этого можно было ожидать. Количество биткойнов, участвующих в продажах по всему миру, просто потрясает, и сайт FiatLeak дает отличную визуализацию того, откуда берутся эти деньги. Ссылка на сайт: http://fiatleak.com.

Сайты CoinMap и CoinATM Radar

Если бы когда-нибудь заинтересуетесь тем, где можно найти банкомат для биткойнов, чтобы удобным способом купить или продать биткойны в обмен на фиатную валюту, обратитесь на сайт CoinATM Radar. На нем вы найдете постоянно обновляемый список банкоматов биткойнов по всему миру. В действительности таких устройств больше, чем можно было бы подумать, хотя еще очень далеко до того, чтобы считать такие автоматы явлением столь же обычным, как привычные всем банковские банкоматы.

С другой стороны, сайт CoinMap представляет посетителям обзор мест, где биткойны можно так или иначе потратить, например в магазинах, по всему миру. В зависимости от вашего местоположения количество таких мест может быть более или менее ограниченным, но с течением времени их число только увеличивается. Сайт CoinMap строит свои диаграммы, опираясь на информацию, предоставляемую биткойн-сообществом, и эта информация постоянно поддерживается в состоянии актуальности. Поэтому, если вам станет известно о новых местах, где можно потратить биткойны, обязательно сообщите о них на сайт CoinMap.

Ссылки на упомянутые выше сайты:

- https://coinmap.org/ – сайт CoinMap
- https://coinatmradar.com – сайт CoinATM Radar

Примечания

1

На момент выхода этой книги на русском языке (лето 2017 года) цена биткойна возросла почти до 2500 долларов США.

2

Англоязычные версии тех же программ можно найти на сайте https://bitcoin.org/en/choose-your-wallet.

3

Можно также порекомендовать некоторые англоязычные источники, например https://howtobuybitcoins.info/#1/ или www.coindesk.com/how-can-i-buy-bitcoins/.

4

В оригинальном американском издании также указаны сайты https://www.bitstamp.net/ и https://kraken.com.

5

На момент подготовки русскоязычного издания к печати стало ясно, что правы были оптимисты – в начале 2017 года цена за биткойн вернулась к уровню 1150 долларов за единицу, а к началу лета уже перевалила за 2500 долларов за один биткойн (https://blockchain.info/ru/charts/market-price). – Примеч. ред.