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/`[1]).
- ✓ 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.

[1] Англоязычные версии тех же программ можно найти на сайте `https://bitcoin.org/en/choose-your-wallet`.

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:

```
http://www.bitfinex.com
http://www.bitstamp.net
http://coinbase.com
http://kraken.com
http://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[2]:

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

Основная цель биткойн-биржи — упростить процесс конвертации фиатной валюты в цифровую, например в биткойны, и обратно. Кто угодно 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

[2] Можно также порекомендовать некоторые англоязычные источники, например `https://howtobuybitcoins.info/#1/` или `www.coindesk.com/how-can-i-buy-bhitcoins/`.

(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 паспорта 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 значительные 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 национальную 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:

  `http://bitcoinwisdom.com`
  `http://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 б*о*льший 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 свободного 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 вают 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://localbitcoins.net`[3].

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.

[3] В оригинальном американском издании также указаны сайты `www.bitstamp.net` и `https://kraken.com`.

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 говорить 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 децентрализованных 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 дольно 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 то 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 угрозой 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 `http://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 по 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 поступившими 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 сигнал 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. Однако 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 купить 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 торговых площадках для операций с биткойнами, вам следует познакомиться с двумя терминами: *горячие кошельки* и *холодное хранение*.

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 которого 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 платформу взломают, потери будут довольно катастрофичными.

  По этой причине большинство бирж не станет делать *крупные* выводы биткойнов из горячего кошелка, а скорее, выведет 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.