Где хранить биткоины: Как выбрать и защитить биткоин-кошелек

Автор: Тая Арянова

Наличные деньги мы держим в физическом кошельке, а как хранится биткоин, если его и потрогать-то нельзя? Рассказываем обо всех нюансах биткоин-кошельков, их разновидностях и степени защищенности.

Если вы хотите начать работать с биткоинами (Bitcoin), прежде всего вам понадобится биткоин-кошелек. Он позволяет совершать транзакции, то есть покупать и продавать криптовалюту. Главная задача биткоин кошелька — хранить секретный ключ, который нужен для доступа к биткоин-адресу и соответственно вашим средствам.

С технической точки зрения, сами биткоины нигде не хранятся, хранятся только секретные цифровые ключи, дающие доступ к публичным биткоин-адресам и возможность «подписывать» транзакции. Именно для этой информации и нужен биткоин-кошелек.

Кошельки бывают разными, в зависимости от устройства, для которого они предназначены — можно даже вообще не пользоваться компьютером и записывать ключи на бумаге. И, конечно, очень важно, чтобы кошелек имел резервную копию и был защищен от доступа посторонних.

Биткоин-кошельки делят на десктопные, мобильные, онлайновые и аппаратные. Они доступны практически на всех популярных операционных системах — Windows, Linux, OS X, Android, iOS, Windows Phone — и совместимых с ними. Кроме того, существуют даже бумажные клиенты.

Биткоин-кошелек для ПК

ПК-кошельки (они же десктопные или локальные) хранятся на вашем компьютере, как и файл с ключами. Существует два вида биткоин-клиентов для ПК: «толстые» («тяжелые») и «тонкие» («легкие»).

«Толстые» скачивают весь блокчейн, а это значит, что вам потребуется много места для хранения данных на достаточно мощном ПК.

«Тонкие» кошельку обращается к блокчейну через сторонние сервисы и не требует скачивания и хранения.

Один из самых популярных «толстых» кошельков — Bitcoin Core. Это «официальный» клиент сети Bitcoin, который разрабатывается и продвигается Bitcoin Foundation — некоммерческой организацией, объединяющей разработчиков ядра. Bitcoin Core не только обслуживает транзакции сети, но и позволяет создать биткоин-адрес для отправки и получения биткоинов, а также хранить закрытый ключ.

Также известен кошелек Armory, который работает поверх Bitcoin Core и расширяет его функциональные возможности. Этот клиент больше подходит для продвинутых пользователей: здесь требуется гибкости в управлении и умение обеспечить безопасность ключей.

Среди «тонких» кошельков лучшим считается Electrum. Он требует от вас минимальных усилий: после установки нужно лишь выбрать сервер. Вы получаете фразу, которую необходимо записать или распечатать — это станет своеобразной гарантией в случае утери пароля. Кроме того, Electrum предлагает работу не только с биткоинами, но и другими криптовалютами, в том числе лайткоином.

Есть и другие кошельки для компьютера — все они немного отличаются функционально. MultiBit работает под Windows, MacOS X и Linux. Hive — это кошелек на базе OS X с некоторыми уникальными функциями, включая магазин приложений, который напрямую подключается к биткоин-сервисам.

В некоторых кошельках сделан упор на анонимности. Например, с DarkWallet поставляется расширение для браузера с дополнительными возможностями, включая микширование биткоинов, когда токены разных пользователей смешиваются для затруднения отслеживания.

Мобильный кошелек

К сожалению, кошелек для компьютера не слишком полезен, если вы вышли на улицу и хотите за что-то заплатить в магазине — в этой ситуации пригодится мобильный кошелек. Это приложение для смартфона, которое хранит секретные ключи для ваших биткоин-адресов и позволяет платить прямо с телефона.

Некоторые кошельки задействуют протокол NFC, позволяя не вводить никакую информацию и оплачивать покупки, просто прикладывая смартфон к считывателю.

Впрочем, у мобильных кошельков есть общая особенность: все они не являются полноценными биткоин-клиентами. Такой клиент должен загружать и хранить весь постоянно растущий блокчейн, занимающий несколько гигабайт. Во-первых, это привело бы к огромным счетам за мобильную связь, а во-вторых, в памяти многих телефонов просто не хватит места.

Поэтому обычно в мобильных кошельках обычно реализована упрощенная проверка платежей (SPV). В этом случае клиент загружает лишь небольшую часть блокчейна и отчасти полагается на другие, доверенные узлы сети биткоин.

Среди мобильных кошельков на Android популярны Bitcoin wallet, Mycelium, Xapo и Blockchain (он хранят ключи на телефоне в зашифрованном виде, а кроме того, создает резервную копию на сервере).

Apple известна своим параноидальным отношением к биткоин-кошелькам. В ноябре 2013 года мобильное приложение кошелька Coinbase было удалено из App Store, а в феврале 2014-го та же участь постигла версию Blockchain для iOS. Впрочем, в июле 2014 года в магазине для iOS снова начали появляться подобные приложения, и теперь почти все ведущие авторы кошельков выпустили версии под эту систему.

Есть и другие типы кошельков, которые также можно использовать на мобильном устройстве — к примеру, Aegis Bitcoin, поддерживающий умные часы на Android.

Онлайн-кошельки

Онлайновые, или интернет-кошельки хранят секретные ключи в интернете, на сервере, который сам пользователь не контролирует. Есть несколько таких серверных сервисов, и ими пользуются в том числе и мобильные кошельки и кошельки для компьютеров — для синхронизации данных между устройствами.

Одно из преимуществ веб-кошелька — доступ из любого места и с любого устройства. Впрочем, с этим связан и главный недостаток: если реализация кошелька окажется не совсем правильной, организация, хранящая ваши ключи, может ими завладеть, лишив вас доступа.

Один из примеров такого рода кошелька — решение Coinbase. Компания управляет биржей обмена биткоинов, и ее услуги интегрированы прямо в кошелек.

Circle предлагает пользователям по всему миру возможность хранить, отправлять, получать и покупать биткоины. Пока напрямую привязывать к аккаунту банковский счет могут только граждане США, но остальные могут пользоваться кредитными или дебетовыми картами.

Кроме того, веб-кошелек есть у Blockchain, а компания Strongcoin предлагает так называемый гибридный кошелек: здесь личные ключи шифруются прямо в браузере перед отправкой на сервер.

Есть также кошелек Xapo — авторы стремятся объединить удобство простого биткоин-кошелька и надежность офлайн-хранилища.

Аппаратный кошелек

Сегодня аппаратных кошельков на рынке представлено немного. Это специализированные устройства, предназначенные для хранения секретных ключей в электронном виде и облегчения платежей.

Аппаратный кошелек Trezor

Это решение предназначено для биткоинеров с крупными запасами криптовалюты, которые не хотят полагаться на сторонние службы хранения биткоинов или на надежные, но непрактичные офлайн-хранилища.

USB-флешка Ledger

Компактный Ledger USB Bitcoin Wallet использует защиту с помощью смарт-карты, при этом он не слишком дорог.

В сентябре 2015 года в продажу поступили кошельки KeepKey. В них используется ПО, некогда отделившееся от проекта Trezor.

Mycelium разрабатывает мультивалютные кошельки и недавно объявила о партнерстве с Dash, в результате которого пользователи смогут покупать и продавать эту популярную криптовалюту непосредственно внутри приложения.

Бумажный кошелек

Это одно из самых популярных и дешевых решений, и подобные услуги предлагают несколько сайтов. Они создают для вас биткоин-адрес и картинку с двумя QR-кодами: один — это общедоступный адрес, по которому можно получить биткоины, а второй — закрытый ключ, который можно использовать для пересылки хранящихся по этому адресу биткоинов.

Преимущество правильно организованного бумажного кошелька в том, что личные ключи нигде не хранятся в цифровом виде, а значит, им не угрожает опасность кибератаки или аппаратного сбоя.

Анонимны ли биткоин-кошельки?

С одной стороны, биткоин полностью анонимен, с другой — полностью прозрачен и отслеживаем, поэтому часто эту криптовалюту называют псевдоанонимной.

В связи с этим некоторые компании занимаются отслеживанием транзакций, и, чтобы этому противостоять, в биткоин-сообществе были разработаны различные техники: предотвращение слияния (merge avoidance), скрытые адреса и микширование монет.

Безопасны ли биткоин-кошельки?

Зависит от обращения. Личные ключи в вашем кошельке — единственный способ доступа к данным транзакции, хранящимся в биткоин-адресе, так что, если вы их потеряете, то потеряете и свои средства.

Таким образом, если никто другой не может получить к ним доступ, и вы их не теряете, это безопасно.

Как защитить свой кошелек?

Шифрование

Кошелек можно зашифровать надежным паролем — это затрудняет взлом, но не дает стопроцентной защиты. Если ваш компьютер заражен вирусом, записывающим нажатия клавиш, пароль может стать известен злоумышленнику.

Резервное копирование

Важно создать резервную копию всего кошелька. Дело в том, что некоторые адреса используются для хранения изменений в транзакциях и могут быть не видны пользователю. Так что необходимо создать резервную копию всего кошелька в нескольких местах.

Мультиподпись

В последнее время появляется все больше сервисов, поддерживающих транзакции с несколькими подписями. Такой подход позволяет нескольким пользователям частично подписать один адрес публичным ключом, и, если кто-то хочет потратить биткоины, нужно, чтобы в дополнение к его подписи транзакцию подписали еще несколько пользователей. Сколько именно подписей необходимо, устанавливается заранее, при создании адреса.

Такая форма подписи может быть удобна в случае взаимной договоренности между, например, деловыми партнерами или членами семьи. Также вторым участником может выступать второе устройство, принадлежащее тому же пользователю.

Офлайн-кошелек

Если хранение биткоин-ключей в цифровом виде кажется вам слишком опасными, например, есть еще один способ: кошелек, который хранится на носителе, не подключенном к интернету.

Можно хранить основные средства в таком офлайн-кошельке, а небольшой оперативный запас — в более удобном кошельке, подключенном к интернету. Таким образом, даже если вы потеряете мобильный телефон или кошелек на ноутбуке будет поврежден в результате сбоя жесткого диска, пропадет лишь небольшая часть биткоинов.