

Алексей Гольшев



Инвестиции в криптовалюты от А до Я

Практическое руководство
начинающего инвестора

Алексей Гольшев

**Инвестиции в криптовалюты
от А до Я. Практическое
руководство
начинающего инвестора**

«Издательские решения»

Гольшев А.

Инвестиции в криптовалюты от А до Я. Практическое руководство начинающего инвестора / А. Гольшев — «Издательские решения»,

ISBN 978-5-00-514222-1

Если вы давно задумывались о вложении собственных средств в криптовалюту, но не знали, с чего начать, то эта книга станет для вас практическим руководством к действию. Автор расскажет о возможных способах покупки, о том, как хранить и обменивать криптовалюту, как определять рыночный тренд, а также даст обзор самых перспективных инвестиционных стратегий. Полученные знания помогут вам сделать первый шаг в инвестировании и разработать стратегию для получения прибыли и приумножения своего капитала.

ISBN 978-5-00-514222-1

© Гольшев А.
© Издательские решения

Содержание

Об авторе	6
Благодарность	7
Введение	8
Глава 1. Блокчейн	9
Что такое блокчейн	9
Глава 2. История создания биткоина	11
История создания	11
В чем же особенность биткоина?	12
Принцип работы биткоина	13
Поведение биткоина до и после халвинга	14
Глава 3. Как и где хранить криптовалюту	17
Официальный кошелек Ethereum	23
Конец ознакомительного фрагмента.	37

Инвестиции в криптовалюты от А до Я

Практическое руководство

начинающего инвестора

Алексей Гольшев

Корректор Александра Макарова

© Алексей Гольшев, 2020

ISBN 978-5-0051-4222-1

Создано в интеллектуальной издательской системе Ridero

Об авторе

- Окончил в 2003 г. Университет нефти и газа им. Губкина.
- Работал в крупных IT-компаниях по разработке и внедрению ERP-систем более 15 лет.
- Бизнес-практик с опытом более 10 лет.
- Более 10 запущенных с нуля успешных бизнес-проектов в разных сферах (event-индустрия, недвижимость, оптовые продажи инновационной автохимии, франшиза автомойки, автострахование, сервис доставки правильного питания, онлайн-школа похудения, производство и продажа корпусов для майнинг-ферм).
 - Инвестировал более 1 млн р. в свое образование по инвестициям в фондовый и криптовалютный рынки, интернет-маркетингу, продажам и продолжает постоянно учиться.
 - Занимается инвестициями с 2010 года.
 - С 2017 года занимается инвестированием в криптовалюты, формированием инвестиционных портфелей и консультированием.

<https://vk.com/agolshev>

<https://www.facebook.com/alexey.golshev>

<https://t.me/agolshev>

Благодарность

Хочу выразить большую благодарность и признательность моему другу **Вадиму Голику** за первичную рецензию материала. За корректировки и обсуждение тем, которые интересны начинающим инвесторам в криптовалюты. Он задал вопросы, на которые я постарался дать ответы в своей книге, надеюсь, мы неплохо поработали и собрали качественную и актуальную информацию, которая будет полезна читателям и поможет начать успешно инвестировать без больших рисков и избежать первичных ошибок, которые совершают все новички при инвестировании в криптовалюты.

<https://vk.com/id22018709>

<https://t.me/vadslavin>

Введение

Данная книга написана для тех, кто хочет больше узнать о криптовалютах, способах инвестирования и использовать возможности для формирования капитала.

Цель этой книги – дать практические советы и решения для инвестирования в криптовалюту без воды, теории и громоздких описаний. В этой книге не будет воды и абстрактных знаний, которые вряд ли могут пригодиться обычным людям, которые являются лишь пользователями экосистемы блокчейна и криптовалют.

Эту книгу можно сравнить с машиной, где водителя не интересует, как устроен двигатель внутреннего сгорания или подвеска и как все это взаимодействует в этой «системе», для водителя важно понимание, как управлять машиной и доехать из точки А в точку Б. Так и задача этой книги – дать начальные практические знания и инструменты для инвестирования в криптовалюту, которые доказывают свою эффективность уже несколько лет подряд.

Эта книга пишется в начале 2020 года, когда в мире разыгралась пандемия COVID-19 и люди в своем большинстве столкнулись с проблемами, которые до этого казались лишь больным воображением. Мир поменялся навсегда. Возможно, это еще мало кто понимает, но это так. В ближайшие годы процессы цифровизации будут только ускоряться и охватывать все больше и больше областей нашей жизни. Идет смена технологических укладов, где цифровая экономика будет играть одну из основных ролей.

Поэтому чем раньше вы познакомитесь с новыми цифровыми способами обмена и криптовалютой в частности, тем более подготовленными вы войдете в новый мир и сможете использовать те возможности, которые откроются перед нами во благо себе и окружающим.

Глава 1. Блокчейн

Что такое блокчейн

Блокчейн представляет собой цепочку из блоков, которые формируют собой базу данных. Устройства, на которых хранятся эти распределённые данные, не имеют общего сервера. Каждый блок – это упорядоченная запись, которая содержит в себе ссылку на предыдущий блок и метку времени. Список блоков внутри базы данных постоянно растёт.

Принцип блокчейна заключается в объединении цифровых записей в блоки. Сложные математические алгоритмы связывают эти блоки между собой в хронологическую криптографическую цепочку – новые блоки находятся в конце этой цепочки. Переставить блоки местами невозможно – система отвергнет такое действие по причине несоответствия временной метки и структуры.

Блокчейн – это универсальный инструмент для построения различных баз данных, который обладает следующими преимуществами:

- **Децентрализация.** Отсутствует главный сервер хранения данных. Все записи хранятся у каждого участника системы.
- **Полная прозрачность.** Любой участник может отследить все транзакции, проходившие в системе.
- **Конфиденциальность.** Все данные хранятся в зашифрованном виде. Пользователь может отследить все транзакции, но не может идентифицировать получателя или отправителя информации, если он не знает номера кошелька. Для проведения операций требуется уникальный ключ доступа.
- **Надёжность.** Любая попытка внесения несанкционированных изменений будет отклонена из-за несоответствия предыдущим копиям. Для легального изменения данных требуется специальный уникальный код, выданный и подтверждённый системой.
- **Компромисс.** Данные, которые добавляются в систему, проверяются другими участниками. Если говорить умными словами – они пересчитывают хеш. Хеширование – процесс шифрования данных.

Позволяя цифровой информации распространяться, но не копироваться, технология блокчейн создала основу нового вида интернета. Технология была первоначально разработана для цифровой валюты, биткоина, но теперь уже повсеместно используется практически во всех сферах жизни – от производства до различных услуг, включая государственные.

Со 100% уверенностью уже можно заявить, что технология блокчейн – это технология будущего, которая прочно вошла в нашу жизнь и будет развиваться ближайшие десятилетия. Блокчейн – это Интернет 3.0.



Принцип работы технологии блокчейн можно сравнить с работой сети Интернет. Вы размещаете в сети какую-либо информацию, и пользователи Интернета могут получить к ней доступ, независимо от места своего нахождения. Так и здесь: информацию, содержащуюся в блоке цепочки, могут получить все пользователи сети, которые имеют к ней доступ, в любой точке мира. Чтобы получить доступ к этой информации, вы должны иметь специальный закрытый ключ, который создан согласно криптографическому алгоритму. Это делает хранение данных в цепочке блокчейна защищённым и полностью безопасным.

Чтобы передать кому-либо денежную сумму, хранящуюся в блоке цепочки, достаточно передать пользователю системы этот закрытый ключ. В обороте биткоинов такой закрытый ключ открывает доступ к адресу, по которому хранится определённая сумма в криптовалюте и представляет собой финансовую ценность. По сути, это способ регистрации произведённых в криптовалюте транзакций, которую в обычной жизни производит банковская система.

Посредством внедрения технологии блокчейн между пользователями сети устанавливаются доверительные отношения, ведь, не имея соответствующего ключа, никто не сможет внести изменения в цепочку из блоков. Любые неподтверждённые закрытыми ключами изменения отклоняются системой. Теоретически закрытый ключ может быть украден. Но защитить его от такой вероятности с помощью нескольких строчек компьютерного кода не представляет особой сложности. Защитить же от кражи физическую валюту гораздо сложнее.

Глава 2. История создания биткоина

История создания

Создателем биткоина считается **Сатоши Накамото** – до сих пор точно не известно, кто скрывается за этим псевдонимом, предположения ходят разные: от просто гиков-энтузиастов до МВФ и мирового правительства. Кем бы он ни был, но 31 октября 2008 года вышла статья «Биткоин: одноранговая система электронной наличности», в которой Сатоши изложил основные принципы работы криптовалюты.

Однако стоит отметить, что еще в августе 2008 года трое энтузиастов подали заявки на патент технологии блокчейн, и был зарегистрирован домен Bitcoin.org. Но все трое полностью отрицают свою связь с Сатоши Накамото и его статьей.

3 января 2009 года в 18:15 по Гринвичу был сгенерирован первый блок в блокчейне биткоина и получена награда в 50 BTC. После этого энтузиасты и активные пользователи сети начали заниматься новым процессом – майнингом.

Майнинг – это процесс добычи (генерирования) криптовалюты.

Криптовалюта получается как вознаграждение за каждый вновь созданный блок, и в самом начале давали по 50 BTC за 1 блок, а сложность сети была настолько низкой, что любой на своем домашнем компьютере мог заниматься майнингом и по текущим ценам стать долларовым миллионером со своего старенького ноутбука.

Эти времена уже давно прошли, и сейчас майнинг на обычном компьютере невозможен, а профессиональные майнеры используют специальные устройства ASIC или фермы (системы из видеокарт для добычи криптовалют на GPU), которые потребляют много электричества и создают очень много шума и тепла, что делает их содержание в домашних условиях крайне затруднительным.

Про майнинг отдельно поговорим в следующих главах.

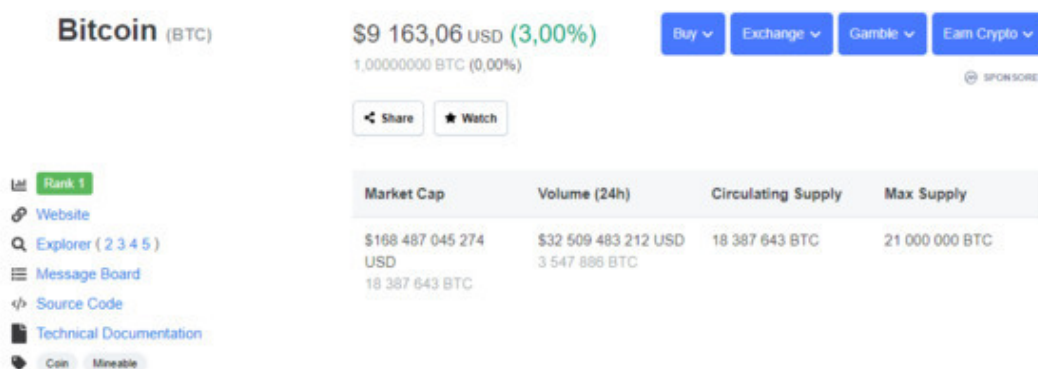
Уже 12 января в 170-м блоке была произведена первая транзакция – перевод криптовалюты с одного кошелька на другой между самим Сатоши Накамото и Хэллом Финли. В 2009 году биткоин еще не приобрел популярности, а курс криптовалюты был крайне низкий – к концу года он колебался между 800 и 1600 BTC за 1 доллар США.

Только представьте себе: вы могли просто запустить программу у себя на компьютере дома или на работе и, пока он включен, заработать себе целое состояние по сегодняшним меркам. Вот он – великий шанс, если вы думаете, что вы его упустили, то это далеко не так. Сегодня звучат заявления о возможной стоимости биткоина в 100 000 \$ и даже 1 000 000 \$, и эти заявления вовсе не лишены здравого смысла, и дальше в книге я расскажу вам почему.

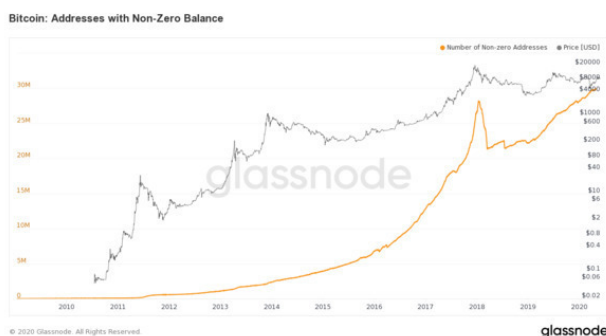
Актуальную цену биткоина вы можете всегда узнать по ссылке: <http://preev.com/>.

В чем же особенность биткоина?

Дело в том, что в его коде стоит ограничение, – существует только 21 миллион биткоинов. В этом заключена его основная ценность как актива – ограниченное предложение. В отличие от фиатных денег (доллара, рубля, евро и других валют), его невозможность взять и напечатать, его никогда не станет больше, а раз в 4 года предложение биткоина сокращается в 2 раза. На текущий момент за каждый найденный блок майнерам выплачивается вознаграждение **6,25 BTC**, хотя на протяжении последних 4 лет выплачивалось 12,5 BTC.



На текущий момент доступно **18 387 643** биткоинов из **21 000 000**. Последний биткоин будет добыт в 2140 году, а значит, за следующие 120 лет будет добыто всего чуть больше **2,5 миллионов** биткоинов, это в 7 раз меньше, чем за 10 лет существования. Как видите, предложение очень сильно уменьшается, а спрос за последние годы только растет, что видно по количеству кошельков биткоина с ненулевым балансом.



Но, несмотря на это, данная валюта может делиться на более мелкие части – до стомиллионной частички.

0,00000001 BTC – это 1 сатоши.

1 BTC – 100 000 000 сатоши.

Главный плюс биткоина в том, что торговать (покупать и продавать) можно не только целыми единицами, но и ее частями.

Принцип работы биткоина

В случае с биткоином, который не имеет Центрального банка, уровень инфляции регулируется согласно общему консенсусу сети криптографическим алгоритмом, который определяет время и количество выпускаемых монет. Каждые 10 минут майнеры добывают новый блок, в котором записываются транзакции сети и который содержит в себе информацию о предыдущих блоках. Чтобы сгенерировать новый блок, майнерам необходимо решить математическую задачу, но для этого требуются большие вычислительные мощности. За генерирование нового блока майнер получает вознаграждение от сети, заложенное в алгоритм, которое по своей сути и является эмиссией биткоина. Каждые 210 000 блоков, на добычу которых уходит 4 года, размер вознаграждения или эмиссия уменьшается в 2 раза. Это «уполовинивание» и называется **халвинг**.

До халвинга в 2012 году майнеры получали 50 BTC за добытый блок, после чего вознаграждение уменьшилось до 25 BTC. После халвинга в 2016 году размер вознаграждения снизился до 12,5 BTC. В мае 2020 года, после третьего по счету халвинга, эмиссия за добытый блок составляет уже 6,25 BTC. В 2138 году за 2 года до последнего добытого биткоина, состоится последний халвинг в истории, после которого вознаграждение майнеров будет составлять 0,000000005820766091 BTC. Это будет не такая большая награда как сегодня, даже если биткоин будет стоить 1 млрд долларов, но последние добытые монеты могут стоить целое состояние. Основным источником дохода майнеров к тому времени будет комиссия за транзакции.

Таким образом, **задача халвинга** – это увеличение сложности добычи биткоина и распределение его эмиссии на 130 лет. Халвинг сдерживает гиперинфляцию, делает биткоин более дефицитным, что положительно сказывается на его стоимости в будущем. Соответственно, криптовалютное сообщество небезосновательно ждет нового халвинга, за которым должен последовать новый буллран биткоина.

Поведение биткоина до и после халвинга

Аналитик регулируемой криптовалютной биржи Currency.com Михаил Кархалёв изучил поведение биткоина до и после халвинга за все 10 лет существования монеты и обнаружил определенные закономерности. Основываясь на них, аналитик сформировал модель роста биткоина и поделился своими предположениями с сообществом.

С полной версией статьи вы можете ознакомиться по ссылке: <https://ru.investing.com/analysis/article-200263302>.

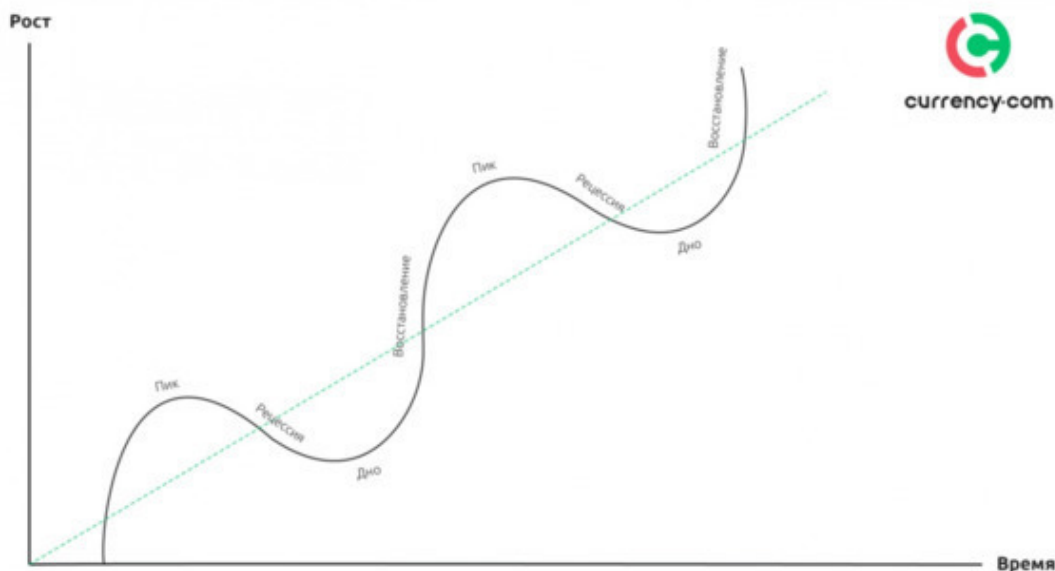
Экономические циклы

Один из постулатов Чарльза Доу, создателя технического анализа, гласит, что история всегда повторяется. Это касается не только фондовых рынков, но и любой экономической модели или системы. За ростом всегда следует падение, за падением – дно, за дном – восстановление и за восстановлением – пик.

Есть 4 наиболее известные циклические модели:

- циклы Китчина – 2—4 года;
- циклы Жюгляра – 7—11 лет;
- циклы Кузнеца – 11—25 лет;
- циклы Кондратьева – 45—60 лет.

Выглядят эти циклы так:



И здесь появляется первое интересное наблюдение.

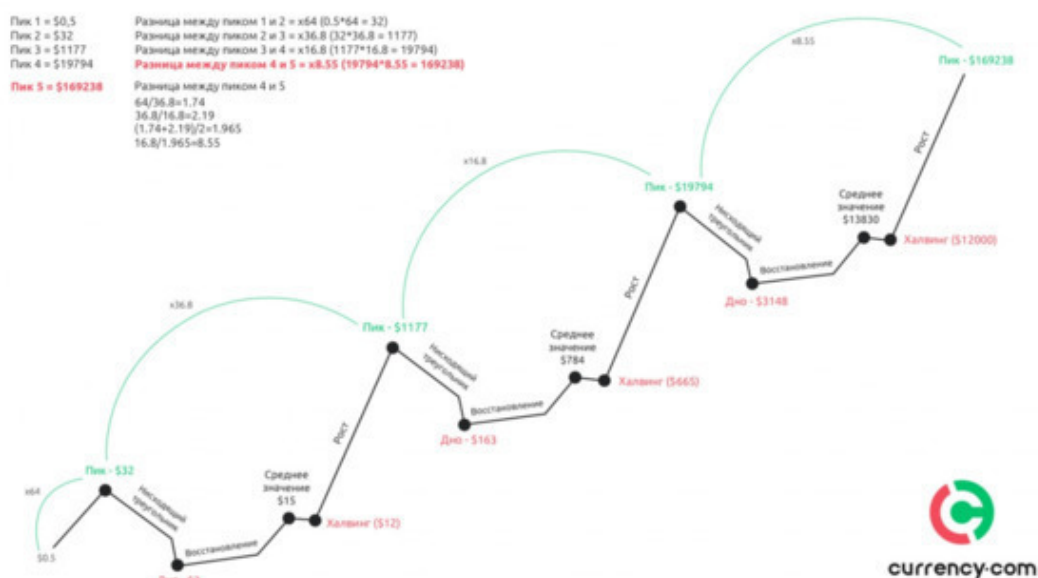
Циклы Китчина – это краткосрочные экономические циклы с характерным периодом 2—4 года, которые сам экономист связывал с краткосрочными циклами колебаний мировых запасов золота. Создавая биткоин, Сатоши Накомото разрабатывал самоподдерживающуюся систему, которая была бы похожа на золотодобычу и снижала эмиссию монеты каждые 4 года. Соответственно, весь экономический цикл «пик – рецессия – дно – восстановление» должен проходить за 4 года от халвинга до халвинга, что очень похоже на циклы Китчина.

Далее следует обратить внимание на то, как вел себя биткоин перед каждым новым халвингом и после него. Сценарий был всегда один и тот же: пик – нисходящий треугольник (рецессия) – дно – восстановление к среднему значению – халвинг.

Сначала цена достигает пиковых значений после мощного бычьего ралли. Добравшись до вершины, биткоин начинает падение по модели технического анализа «Нисходящий треугольник». Прежде чем пробить уровень поддержки, цена несколько раз отскакивает от него, после чего происходит пробой и движение на «дно». Далее происходит постепенный процесс восстановления цены к околосредним показателям от предыдущего пика. Оставшийся период времени до халвинга цена движется разнонаправленно, но к халвингу возвращается к среднему показателю от предыдущего пика. После халвинга биткоин постепенно переходит к росту и вскоре покоряет новый пик.

Модель роста биткоина

После визуализации в целую картинку всех наблюдений складывается следующая модель роста биткоина, с помощью которой можно прогнозировать новый пик, который будет покорен после халвинга 2020 года.



Первый серьезный рост биткоина произошел в 2010 году, когда цена достигла 50 центов за монету. Второй пик был на отметке в 32 \$, что в 64 раза больше, чем предыдущий пик в 50 центов. Третий пик был на отметке в 1 177 \$, что в 36,8 раз больше, чем предыдущий пик в 32 \$. Четвертый пик на 19 794 \$ больше в 16,8 раз, чем пик в 1 177 \$. Обратите внимание, что сила роста с каждым разом фактически уполовинивается:

- отношение силы роста между пиком 1—2 и пиком 2—3 составляет 1,74 ($64 \div 36,8 = 1,74$);
- отношение силы роста между пиком 2—3 и пиком 3—4 составляет 2,19 ($36,8 \div 16,8 = 2,19$).

Чтобы выяснить будущую силу роста и новый пик, необходимо узнать среднее значение отношения между предыдущими силами роста:

$$(1,74 + 2,19) \div 2 = 1,965.$$

Соответственно, если последняя сила роста 16,8 уменьшится в 1,965 раза, то следующая сила роста составит 8,55.

$19\,794 * 8,55 = 169\,238$ \$ – следующий пик биткоина.

По статистике, после халвинга рост начинается практически сразу, но движется постепенно, обновляя исторический максимум через 5—7 месяцев. После небольшой коррекции, которая длится несколько недель, рост продолжается, в течение года переходя в новый bullrun («бычье ралли»), после чего достигается новый пик. Соответственно, обновление ценового максимума можно ждать примерно через полгода после халвинга или к концу 2020 года, а новый пик – через 18 месяцев или к концу 2021 года.

Резюме

Исходя из данного наблюдения и расчетов, можно сделать следующие выводы:

- По статистике, в день халвинга цена находится на околосредних значениях от предыдущего пика или на уровне 11 836—12 034 \$ в день халвинга в мае 2020 года.
- Рост после халвинга начинается практически сразу, но идет постепенно, обновляя исторический максимум только через 5—7 месяцев.
- Предположительно, если наблюдения и расчеты верны, то через 18—20 месяцев цена биткоина может составить 169 238 \$.

Обращаем ваше внимание, что данная модель является личным наблюдением и мнением аналитика Currenсу.com Михаила Кархалёва и ни в коем случае не является истиной в последней инстанции и тем более руководством к действию. Помните, что криптовалюты – это высокорисковые активы, цена которых в будущем непредсказуема.

ВАЖНО!

Стоит отметить, что халвинг состоялся 11 мая 2020 г. и цена биткоина составила в течение дня 8200—9168 \$. А значит, расчеты, с одной стороны, близки к реальным показателям, но в то же время **не являются абсолютом** и могут не сбыться в будущем.

Глава 3. Как и где хранить криптовалюту

Прежде чем купить криптовалюту, надо сначала понять, как и где ее хранить. Поэтому первое, с чего следует начать работу с криптовалютами, – это завести себе кошелек. Они бывают разными: горячими и холодными, для одной валюты или мультивалютные, мобильные или десктопные, аппаратные или на бумажном носителе. Разберем основные типы и сразу перейдем к описанию рекомендуемых вариантов, которые сочетают в себе оптимальное решение удобства, доступности и безопасности.

Что такое криптовалютный кошелек?

Это всего лишь адрес, на котором висит баланс той или иной криптовалюты. Это не аккаунт и не физическое хранилище! К этому адресу (его еще называют «публичный ключ») у вас должен быть приватный ключ (или закрытый), с помощью которого вы можете отправлять монеты, подписывая криптографическую функцию в блокчейне.

Важно! В кошельке вы не храните свои монеты! Монеты хранятся в блокчейне и никуда оттуда не пропадают.



Поэтому **кошелек** – это, по сути, **способ хранения** вашего приватного ключа!

Это также означает, что, если вы когда-нибудь потеряете кошелек, вы необязательно потеряете свои средства, если у вас остался приватный ключ. Пока вы записываете свои закрытые ключи где-то в другом месте, вы можете получить к ним доступ с другого кошелька в любое время.

Приватный ключ – это пароль, который позволяет вам осуществлять транзакции, а еще криптографическая функция, которая создает общедоступный адрес для вашего кошелька.

Адрес и приватный ключ связаны друг с другом. Если вы создаете новый кошелек, то вы фактически создаете определенный пароль, в комплекте к которому идет адрес, который ассоциирован с этим паролем и куда можно присылать криптовалюту.

Сид-фраза (seed – мнемоническая) – это своеобразный пароль, который используется для восстановления доступа к кошельку в случае его утери по каким-либо техническим причинам (например, выход из строя жесткого диска). Как правило, состоит из 12 или 24 слов, которые генерирует сам кошелек.

ТИПЫ КОШЕЛЬКОВ (варианты хранения приватных ключей)

Горячие кошельки – это кошельки, где у вас нет доступа к приватному ключу. Такой способ чаще всего используется на биржах и различных сервисах. Сами понимаете, что в этом случае вы полностью доверяете свои деньги бирже или сервису, а они отвечают только своей репутацией. Так что на таких кошельках нельзя хранить большие суммы и делать долгосрочные инвестиции. Деньги с такого кошелька можно вывести, только создав транзакцию через этот сервис.

Если сервис перестает работать, то вы просто теряете свои деньги.

Самый рискованный и ненадежный способ хранения. По сути, ваши средства вам не принадлежат и зависят от надежности системы, на которой они хранятся.

Программные кошельки – приватный ключ хранится на сервисе и на вашем устройстве в зашифрованном виде, у вас есть к нему доступ. Это тоже горячие кошельки, но более надежные и с возможностью восстановления.

Стоит отметить, что для хранения небольших сумм в краткосрочном или среднесрочном варианте неплохо зарекомендовали себя мультивалютные кошельки, которые можно назвать отчасти и холодными. Их можно установить на компьютер или планшет – без доступа к интернету. При этом сид-фраза для восстановления хранится у вас, а приватный ключ хранится в зашифрованном виде на вашем устройстве и серверах производителей, что является довольно безопасным способом.

Холодное хранение (бумажный кошелек) – приватный ключ находится только у вас, никто не имеет к нему доступа. Надежный способ для хранения криптовалюты. Нужно хранить вне устройства сид-фразу для восстановления.

В 2009 году, когда биткоин только начинался, первые закрытые ключи были созданы генератором случайных чисел, а затем записаны на листе бумаги. Их называли бумажными кошельками, так как закрытые ключи хранились на бумаге. Бумажные кошельки все еще существуют сегодня и считаются одними из наиболее безопасных способов хранения ваших закрытых ключей. Я рекомендую использовать бумажный кошелек только в качестве резервной копии или в качестве холодного хранения больших сумм монет, иначе это не стоит тех хлопот, с которыми придется столкнуться при постоянном использовании.



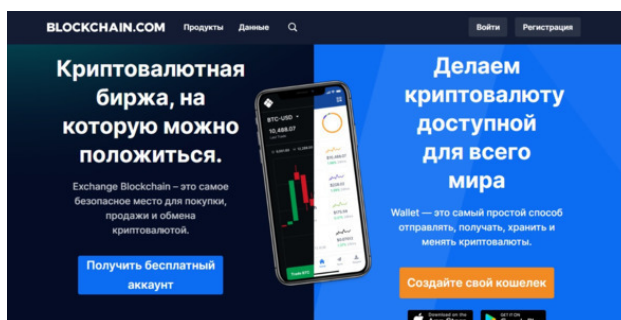
Холодное хранение – способ хранения ключей отдельно на флешке или внешнем диске без доступа к интернету. На него можно установить операционную систему, загрузить программный кошелек и использовать только при крайней необходимости. Опять же, сид-фразу хранить лучше отдельно в надежном месте.



Аппаратные кошельки с холодным хранением. Специализированные устройства (аналог флешки), которые хранятся у вас в безопасном месте без подключения к интернету. Самый удобный и надежный способ на текущий момент для хранения криптовалюты на долгосрок.

Если же вам нужен только биткоин, или эфириум, или какая-то другая криптовалюта, то проще всего воспользоваться их собственными кошельками.

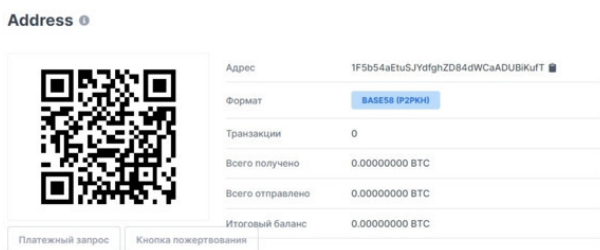
Самым популярным кошельком биткоина, который считается практически официальным (но не является таковым, потому что у биткоина нет своего официального кошелька), является сервис <https://www.blockchain.com/>.



Этот сервис постоянно развивается и дополняется новыми инструментами: кошельками других криптовалют (Ethereum, Bitcoin Cash и Stellar), обменником, информацией по рынкам, API для разработчиков. Вы можете установить приложение на свой телефон, скачав его в App Store или Google Play.

Кроме самих кошельков, есть обозреватель блоков и много еще полезной статистики по хешрейтам и нагрузке сети.

Обозреватель блоков, транзакций и кошельков – <https://www.blockchain.com/ru/explorer>.



Здесь вы можете указать любой кошелек или транзакцию и проверить баланс, движения и что вообще происходит на этом адресе.

Интересны и графики (<https://www.blockchain.com/charts>), где вы можете посмотреть много аналитической информации по хешрейту сети, сложности, майнингу, комиссиям майнеров.

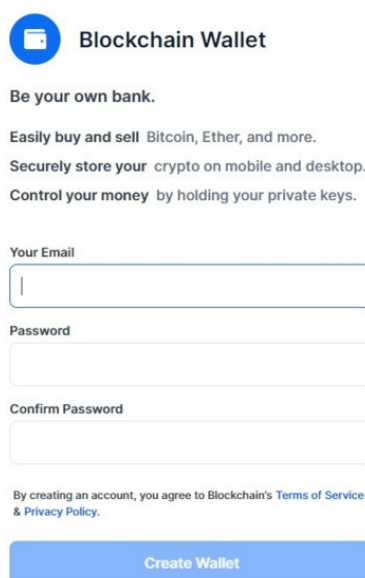


Это целый информационный портал по первой криптовалюте. Сам кошелек – лишь небольшое дополнение к этому. Несмотря на всю надежность и доверие к сайту, стоит отметить, что тут приватный ключ будет находиться в совместном доступе, то есть у сервиса есть к нему доступ, и они хранятся на сайте.

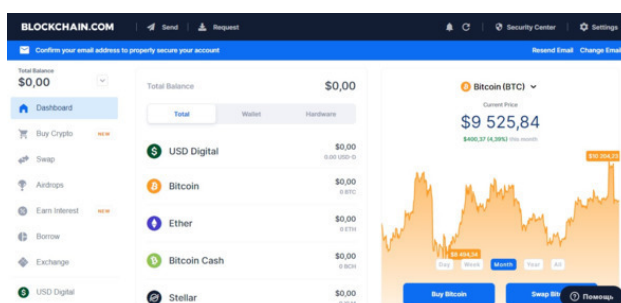
А это значит, что в случае хакерской атаки они могут быть похищены, они, конечно же, зашифрованы, и ранее никому не удавалось их взломать, но теоретическая вероятность существует.

Зарегистрировать свой кошелек довольно просто: нажимаете «Создайте свой кошелек» или «Регистрация». Вводите свой email и пароль.

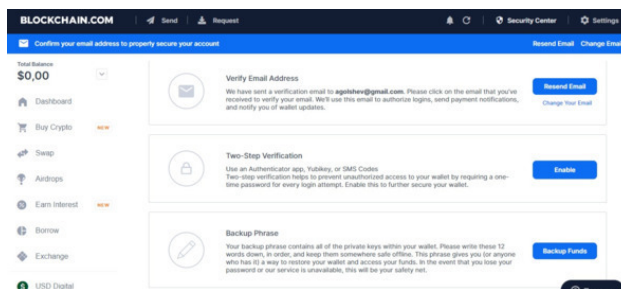
Автоматически вам создается ваш кошелек, и вы попадаете в свой личный кабинет, где у вас есть различные криптовалюты – Bitcoin, Ether, Bitcoin Cash и Stellar.



The image shows the registration page for Blockchain Wallet. At the top, there is a blue circular icon with a white wallet symbol and the text "Blockchain Wallet". Below this, the text reads "Be your own bank.", "Easily buy and sell Bitcoin, Ether, and more.", "Securely store your crypto on mobile and desktop.", and "Control your money by holding your private keys." The registration form consists of three input fields: "Your Email", "Password", and "Confirm Password". Below the form, there is a blue button labeled "Create Wallet". At the bottom, there is a small disclaimer: "By creating an account, you agree to Blockchain's Terms of Service & Privacy Policy."



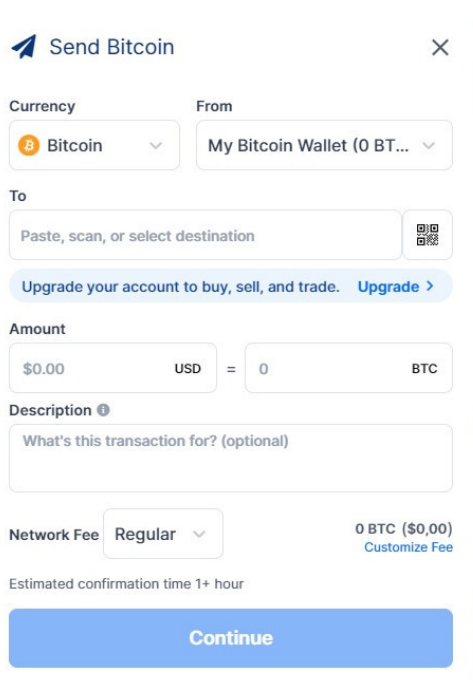
Первым делом зайдите в Security Center – подтвердите свой email, установите двухфакторную верификацию и создайте backup-фразу.



Также вы можете сразу купить биткоин по выгодному курсу, если у вас есть дебетовая/кредитная карта в долларах, единственное ограничение – 1 000 \$ за один раз.



Чтобы отправить свой биткоин, нажмите «Send» в верхней части экрана. Вставьте адрес, кому вы хотите отправить биткоин, укажите количество и выберите комиссию. Если хотите, чтобы средства пришли быстро, указывайте повышенную, если готовы подождать – выбирайте обычную.





Чтобы получить свой биткойн, нажмите «**Request**» в верхней части экрана и скопируйте адрес своего кошелька.

Request Bitcoin ×

Currency:

Receive To:



Address:
 

Done

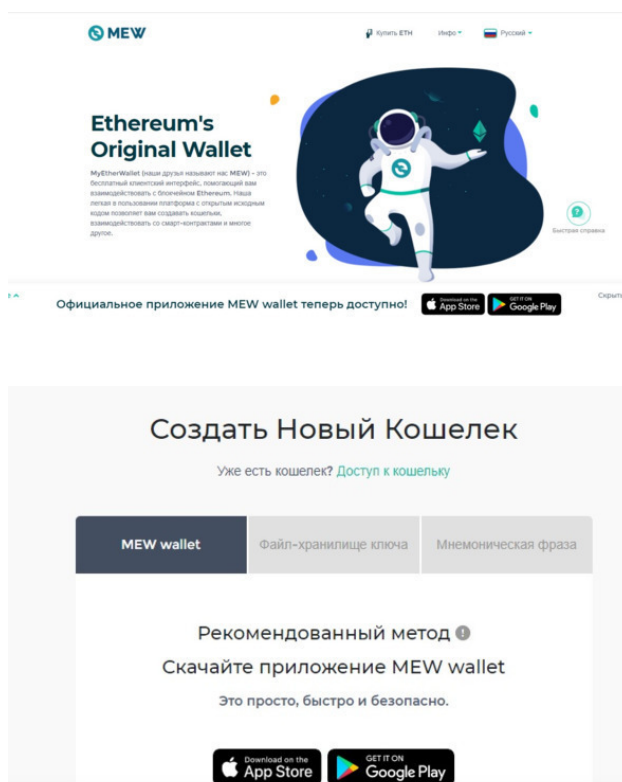
Create Shareable Request Link

Официальный кошелек Ethereum

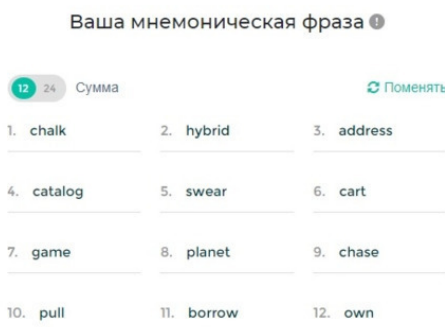
Рассмотрим кошелек для эфира, который также используется для всех токенов на блокчейне эфириума стандарта ERC-20 – <https://www.myetherwallet.com/>.

Разработчики уже выпустили мобильные приложения для IOS и Android и очень рекомендуют воспользоваться именно такой версией.

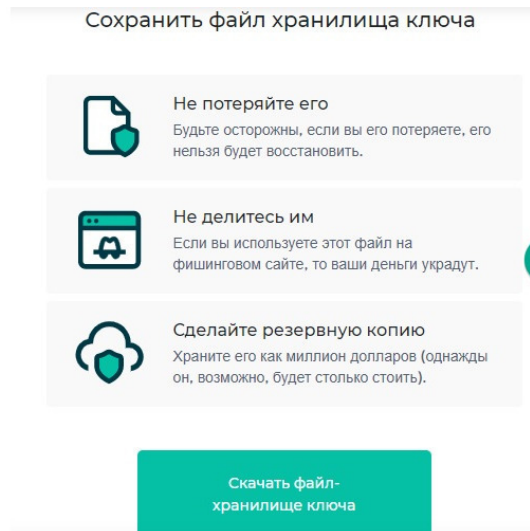
Для создания кошелька надо выбрать вариант: либо скачать приложение, либо воспользоваться установкой на устройстве через создание файл-хранилища ключа или мнемонической фразы.



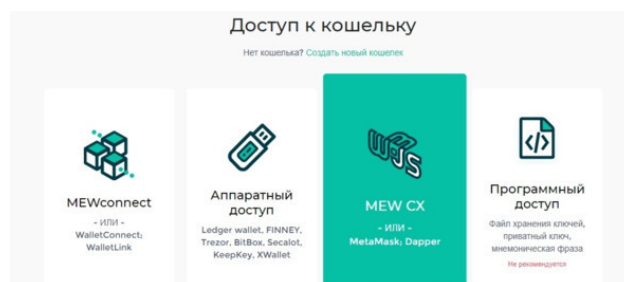
Создание через мнемоническую фразу. Записываем фразу, и в дальнейшем подключение к кошельку происходит с помощью этой сид-фразы.



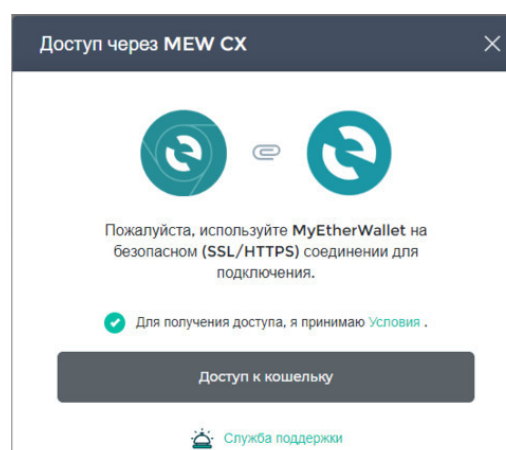
Для хранилища ключа. Придумываем пароль и создаем файл-хранилище.



Скачиваем файл и через него в дальнейшем подключаемся к кошельку.

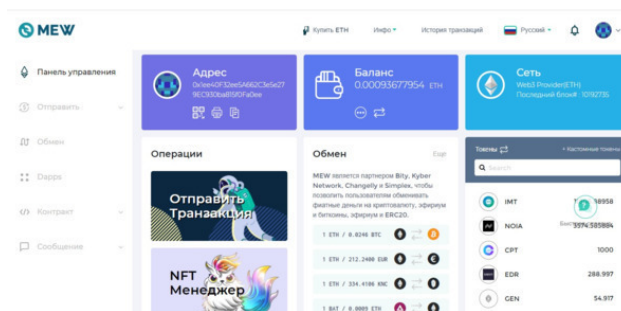


Рекомендуемый способ. Установить расширение Mew CX для браузера Chrome, и в дальнейшем легко и просто можно подключаться уже без постоянного ввода ваших ключей или фразы.



ВАЖНО! Файл-хранилище ключей лучше хранить отдельно на флешке без доступа к интернету. Сид-фразу также можно хранить на флешке или на бумаге в безопасном месте!

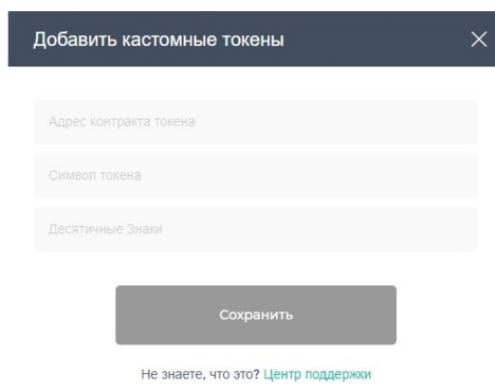
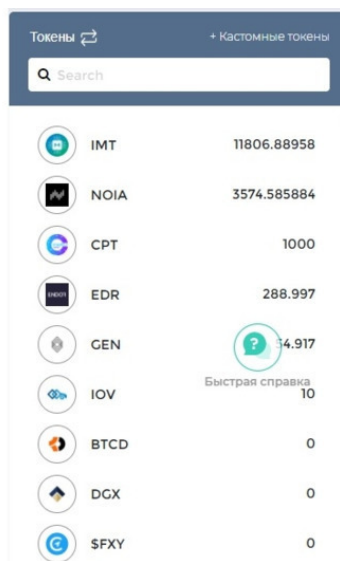
Вот так выглядит интерфейс кошелька для Ethereum и токенов:



Справа в нижнем углу отображаются ваши токены, привязанные к этому адресу эфира. Токены не имеют собственного блокчейна и привязаны к вашему адресу в системе эфириум, так что он становится и их адресом тоже.

Вы можете добавлять нужные вам токены. Если у вас есть токены, но кошелек не нашел их автоматически, то нужно выполнить их поиск, если поиск их не находит, то нужно вручную ввести адрес смарт-контракта.

Для этого переходим по ссылке <https://etherscan.io/tokens>, там находим ваш токен и копируем адрес из строки Contract (адрес контракта токена), Decimals (десятичные знаки) и краткое значение токена (символ токена). Если все сделали правильно, то токен появится в вашем списке.



ПРОГРАММНЫЕ КОШЕЛЬКИ

Стоит отметить, что для хранения небольших сумм в краткосрочном или среднесрочном варианте неплохо зарекомендовали себя мультивалютные кошельки, которые можно назвать отчасти и холодными. Их можно установить на компьютер или планшет без доступа к интернету. При этом сид-фраза для восстановления хранится у вас, а приватный ключ хранится в зашифрованном виде на вашем устройстве и серверах производителей, что является довольно безопасным способом.

Рассмотрим один из таких вариантов, который мне очень нравится.

Программный онлайн-кошелек Exodus

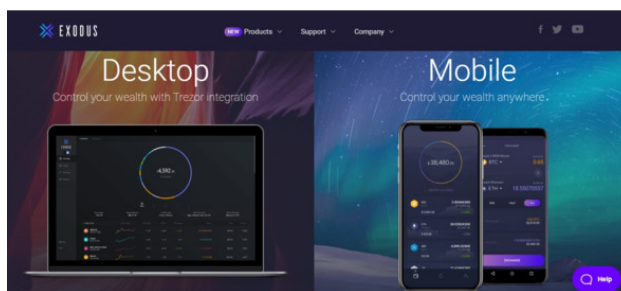
Exodus – это мультивалютный кошелек смешанного типа хранения приватного ключа. Ключ в зашифрованном виде хранится на вашем устройстве и сервисе. Поддерживается как desktop-версия для Mac и Windows, так и мобильная для IOS и Android.

В кошельке на текущий момент можно хранить более 110 криптовалют с возможностью их обмена прямо в приложении, и список постоянно расширяется. В отличие от большинства аналогичных решений, интерфейс этого кошелька настолько прост и понятен, что им могут пользоваться даже новички в криптовалютной сфере.

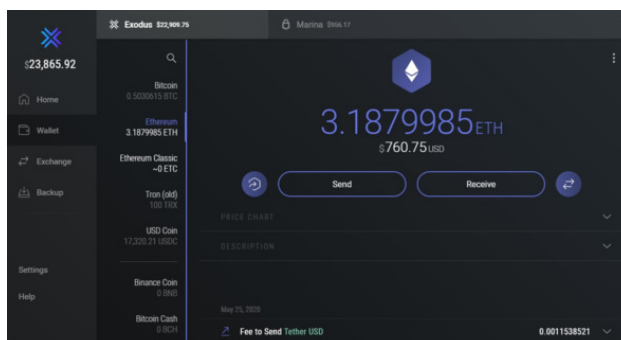
Многих пользователей кошелька Exodus привлекает возможность работы с большей частью своих криптовалютных сбережений в одном инструменте без необходимости использования множества сложных кошельков и хранения огромной базы приватных ключей или сид-фраз от каждого из них.

Запущенный в 2016 году после краудфандинговой кампании на 300 000 € Exodus позиционировался как один из самых удобных и безопасных универсальных кошельков для компьютера. И пока что его разработчикам вполне удается удерживать эту позицию.

Установить кошелек можно по ссылке: <https://www.exodus.io/>.



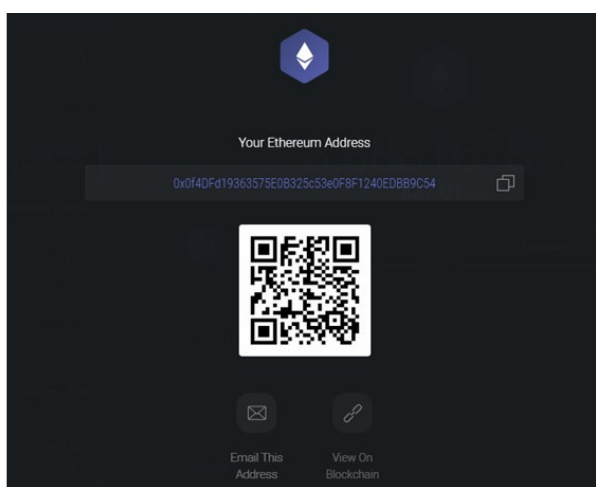
Для начала работы необходимо установить кошелек на устройство. У вас сразу появится список доступных криптовалют, который можно расширить через добавление.



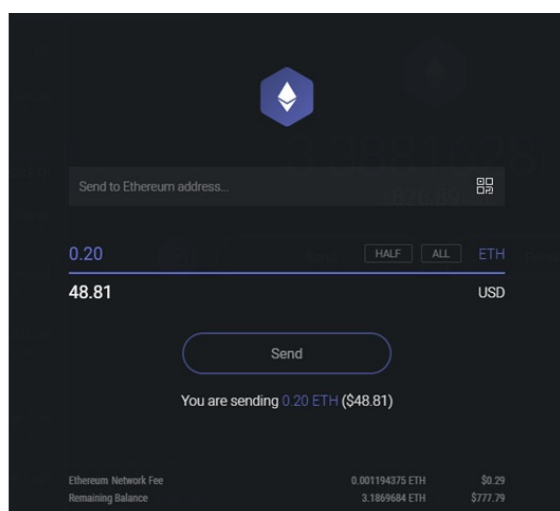
Как только вы пополните свой кошелек любой криптовалютой, программа попросит вас зашифровать данные – придумать пароль, записать recovery-фразу из 12 слов и секретное слово для восстановления. Запишите эту фразу и сохраните в надежном месте. Если что-то произойдет с вашим устройством, то вы всегда сможете восстановить доступ к своим криптоактивам.

В Exodus вы можете получать, отправлять и мгновенно обменивать свои криптовалюты, формировать свой портфель и отслеживать изменения на графиках.

Чтобы пополнить свой кошелек, надо нажать кнопку «**Receive**», и отобразится ваш адрес. В случае с пересылкой монет, работающих на собственных блокчейнах (BTC, ETH, XRP и пр.), на балансе должно оставаться достаточно средств для оплаты комиссии за пересылку. Если же речь идет об отправке токенов ERC-20, на счету должно быть достаточно для этой цели количество эфира. В обоих случаях расчетный размер комиссии указывается внизу окна формирования операции по отправке средств.



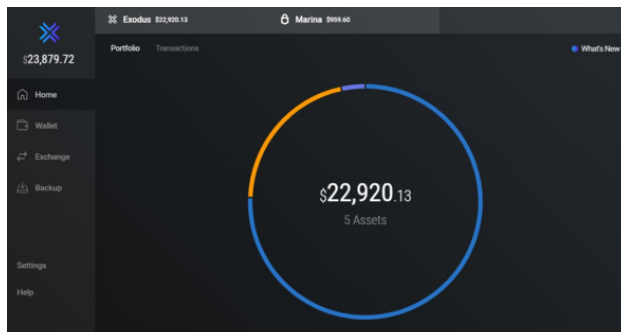
Чтобы отправить средства, необходимо выбрать в списке нужный криптоактив и нажать кнопку «**Send**». В открывшемся окне указывается адрес кошелька получателя и количество пересылаемых монет.



В кошельке реализовано портфолио и список криптовалют с их курсами и графиками. Вы можете отслеживать свой портфель как в валюте, так и в отдельных криптовалютах. Там же

можно посмотреть историю изменений общей стоимости активов в портфеле пользователя в виде графика, выбрав один из доступных временных промежутков.

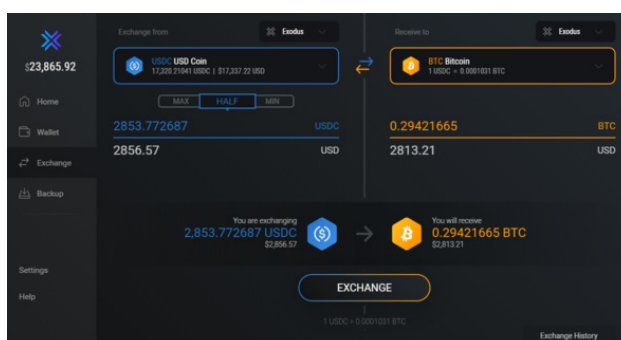
Внутренний обмен криптовалют является отличительной особенностью Exodus и доступен в меню **Exchange** (обмен). Этот функционал работает на базе обменника ShapeShift и доступен только для активов, поддерживаемых кошельком.



ASSET NAME	PRICE	24H CHANGE	MARKET CAP	30 DAY TREND	BALANCE	VALUE	PORTFOLIO %
USD Coin (USDC)	\$1.00	-0.05%	\$79M		17,320.21 USDC	\$17,327.22	75.68%
Bitcoin (BTC)	\$9,561.70	-0.41%	\$176B		0.5009615 BTC	\$4,810.12	20.99%
Ethereum (ETH)	\$238.63	+1.19%	\$26.5B		3.1879985 ETH	\$760.75	3.32%
Tron (old) (TRX)	\$0.016622	+3.44%	\$1.11B		100 TRX	\$1.66	0.01%
Ethereum Classic (ETC)	\$6.90	+0.17%	\$799M		-0 ETC	\$0.00	<0.01%
XRP	\$0.20287	-1%	\$8.97B		0 XRP	\$0.00	0%

Правда, курс обмена не очень выгодный, поэтому большие суммы лучше так не менять, но в целом это очень нужная и удобная функция. Вы можете приобрести только биткоин, а в кошельке обменять частично на другие криптовалюты, тем самым составив себе сбалансированный портфель. Кстати, в этом кошельке есть практически все криптовалюты из топ-10, 20 и даже топ-30.

Процесс обмена средств производится очень просто: слева выбирается исходная монета и ее количество, справа – валюта, которую желает получить пользователь. Конечная сумма монет на выходе подсчитывается автоматически (минус комиссия) и зависит от курса обмена на ShapeShift.



Преимущества и недостатки криптокошелька Exodus

Достоинств у Exodus, на которые стоит обратить внимание при выборе универсального криптовалютного кошелька, довольно много:

- интуитивно понятный и удобный интерфейс, позволяющий выполнять операции с криптовалютами даже тем, кто является новичком в этой области;
- мультиплатформенность – desktop-версия для всех ОС, мобильное приложение для IOS и Android.
- поддержка более 100 различных криптоактивов избавляет от необходимости использования множества заточенных под отдельные монеты кошельков;
- безотказная работа приложения;
- надежная защита хранящихся криптоактивов (за всю историю существования кошелька не было ни одного взлома);
- быстрое проведение транзакций;
- встроенный криптообменник;
- удобное портфолио и графики;
- регулярное расширение списка поддерживаемых криптовалют и добавление нового функционала;
- разработчики непрерывно работают над совершенствованием приложения, о чем свидетельствуют частые обновления (по несколько раз в месяц);
- отзывчивая техподдержка, оперативно решающая трудности, с которыми сталкиваются пользователи Exodus.

Недостатков у проекта **Exodus** значительно меньше, чем преимуществ, да и серьезными недостатками это не назовешь.

Можно выделить разве что:

- отсутствие функции двухфакторной аутентификации, которая считается нормой для обеспечения безопасности средств;
- невозможность ручной установки комиссий за проведение транзакций, т. к. кошелек рассчитывает их автоматически с учетом пропускной способности сети, чтобы обеспечить высокую скорость перевода средств;
- закрытый исходный код приложения (некоторыми расценивается как лазейка для разработчиков);
- отсутствие возможности смены языка интерфейса.

По сути, последние перечисленные пункты с натяжкой можно назвать недостатками. Это скорее нюансы, доставляющие лишь небольшие неудобства отдельным пользователям, которые с лихвой компенсируются многочисленными преимуществами кошелька.

АППАРАТНЫЕ КОШЕЛЬКИ

Аппаратные холодные кошельки – это баланс между безопасностью и удобством. Высокая степень безопасности, нет подключения к интернету напрямую, ключи хранятся отдельно. Операции проводить не очень удобно, но безопасно. Приоритетное назначение – хранение, как в сейфе. Не для ежедневного использования. Хранение значительного количества на долгосрок.

Аппаратный кошелек похож на USB-флешку, но с одним важным отличием: закрытый ключ хранится на USB-накопителе, но при этом к нему нельзя получить доступ с компьютера и, как следствие, из интернета.

Это действительно важно, так как некоторые мошенники пытаются продать людям обычные флешки (которые, конечно же, подключаются к компьютеру) по цене аппаратных кошель-

ков. Причина, по которой аппаратный кошелек хорош, состоит в том, что ваш закрытый ключ постоянно остается в офлайн-режиме. Вы можете получить доступ к закрытому ключу только с помощью PIN-кода, который вам нужно физически ввести на устройстве. Если вы когда-либо потеряете устройство, никто не сможет его использовать, так как не знает PIN-кода. Если же вы заблокируете его по неосторожности, то с помощью сид-фразы вы сможете все восстановить.

Важно! Помните, что вы должны относиться к своему закрытому ключу и сид-фразе как к деньгам, потому что это так и есть. Хотя это всего лишь строка букв или слов, но она может стоить миллионы.

Два самых распространенных и зарекомендовавших себя устройства – это кошельки от компаний Trezor и Ledger.

Trezor (сайт: <https://trezor.io/>) – чешская компания, которая первая в начале 2014 г. выпустила свой аппаратный кошелек. Следом за ней французская компания Ledger (сайт: <https://www.ledger.com/>) спустя год выпустила свою версию криптовалютного аппаратного кошелька.

Компания Ledger продала более миллиона своей бюджетной модели Nano S, что говорит о популярности кошелька и его качествах.

В целом эти две компании успешно конкурируют, а их модели мало чем отличаются друг от друга. Поэтому сравнивать их довольно тяжело, и различия практически никакой нет. Выбор больше идет на вкус и цвет.

У каждого бренда есть по 2 модели кошельков. У Trezor это **Trezor One** и **Model T**. У Ledger это **Nano S** и **Nano X**.

Младшие модели – **Trezor One** и **Nano S** и старшие **Model T** и **Nano X**. Более уместно сравнивать их между собой, потому что там больше отличий, чем между конкурентными моделями. Однако отличия незначительные все-таки есть, и мы их разберем.

В чем разница между аппаратными кошельками?

- **Стоимость** – практически одинаковая.
- **Безопасность** – принцип хранения ключей, ввод PIN-кода.
- **Поддержка платформ** – PC, MAC, IOS, Android и т. д.
- **Мультивалютность** – поддержка числа криптовалют.
- **Функционал** – наличие дополнительных возможностей: обмен криптовалюты, аналитика, инфографика.

Если сравнивать Trezor и Ledger, то существенной разницы нет. У каждого производителя есть свои плюсы и минусы. Если использовать кошелек только для хранения одной или двух основных валют, то для этого прекрасно подойдет Trezor One. Если же использовать кошелек для более широкого количества монет, более часто совершать транзакции, тогда есть смысл обратить внимание на **Ledger Nano S** с их приложением **Ledger Live** для компьютера или телефона, которое позволяет просматривать свой баланс без подключения аппаратного кошелька.

Trezor One поддерживает более 1 000 + монет, при этом он не поддерживает такие топовые криптовалюты как Ripple, EOS, Cardano, Monero, Tezos. Но в модели Model T такой проблемы нет. Список поддерживаемых криптовалют вы можете посмотреть по ссылке: <https://trezor.io/coins/>.

Еще одно неудобство, что вы должны использовать Trezor со сторонним кошельком Myetherwallet для хранения Ethereum или токенов ERC-20, поскольку Trezor в своем интерфейсе не дает такую возможность. В **Ledger Nano S** с их приложением Ledger Live такой проблемы нет.

Что же касается **Ledger Nano S**, то он вмещает только от 1 до 18 приложений (криптовалют), которые вы можете видеть и управлять одновременно. Поэтому если криптовалют больше, то придется удалять неиспользуемые и добавлять новые. В старшей модели **Nano X** можно хранить одновременно до 100 приложений.

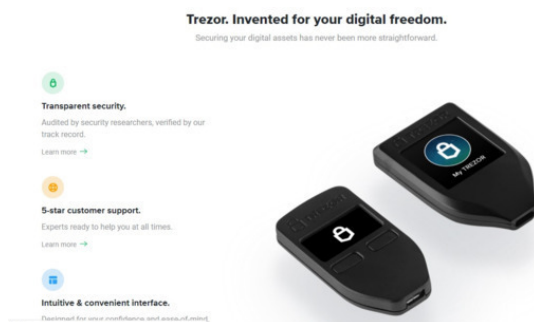
Основное отличие кошельков **Trezor** от **Ledger** – это то, что код моделей кошельков **Trezor** является открытым и выложен на GitHub. Все желающие могут его посмотреть, убедиться в его безопасности, найти ошибки и отправить производителю. Также с **Ledger** было связано несколько историй с уязвимостью, но это давно уже в прошлом, и за последнее время они активно развиваются и шагнули довольно далеко.

ВАЖНО! Ни в коем случае не покупайте кошелек на AliExpress или «Авито». Только на официальных сайтах производителей или у официальных дилеров.

Мало того что там можно купить просто поддельный кошелек, который не будет работать, там могут продать, что еще хуже, перепршитое устройство, которое будет работать, но отправлять данные о вашем Private Key злоумышленникам. Поэтому заказывайте на официальном сайте или у официальных дилеров в РФ.

Аппаратный кошелек Trezor

Рассмотрим отдельно, как установить кошелек **Trezor One** и пользоваться им. Ссылка на официальный сайт, где можно заказать кошелек с доставкой по РФ: <https://trezor.io/>.

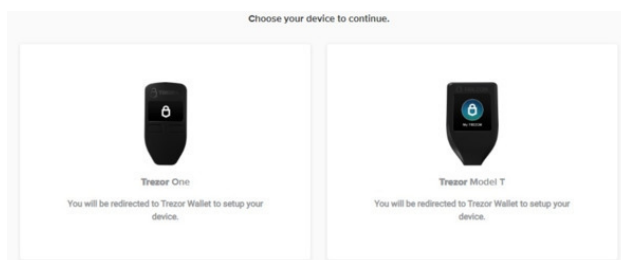


Надежный аппаратный кошелек. Есть две модели – **Trezor One** (вполне подойдет для хранения нескольких основных валют) и **Trezor Model T** (более продвинутая модель с большим количеством функций и криптовалют).

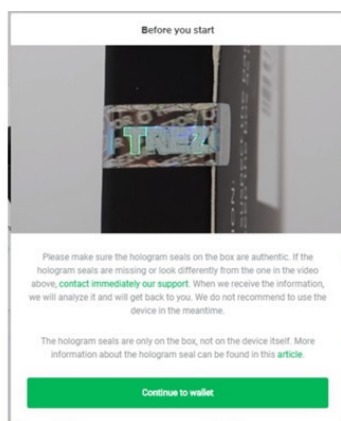
Основное преимущество этих кошельков – поддержка большого количества криптовалют, цена, совместимость с программным кошельком **Exodus** и отсутствие прецедентов со взломом и различными ошибками.

Между моделями есть еще отличие в системе безопасности, такая как ввод PIN-кода. В модели **Trezor One** ввод и проверка кодовой фразы могут выполняться на компьютере. В модели **Trezor T** все выполняется исключительно на устройстве, что исключает риск похищения ваших паролей с компьютера, если он у вас заражен.

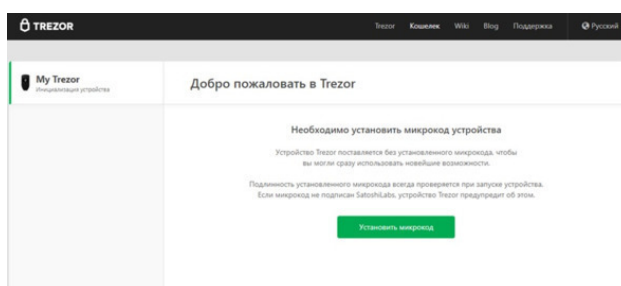
Для начала работы и активации необходимо подключить устройство к компьютеру, перейти на основной сайт в раздел кошелька (<https://trezor.io/start/>), выбрать модель и нажать кнопку «Продолжить».



Перед тем как начать работу с кошельком, убедитесь в том, что голографическая наклейка хорошо наклеена, когда вы ее снимите, все равно останутся следы, и это нормально, это нужно для вашей безопасности. Нажмите зеленую кнопку «Продолжить».

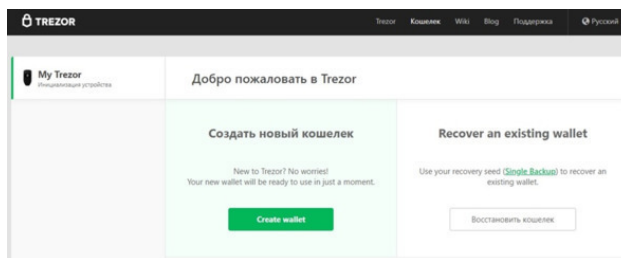


При первоначальном входе на кошелек необходимо установить программное обеспечение. Программное обеспечение устанавливается на кошелек через компьютер, первоначально кошелек чист.

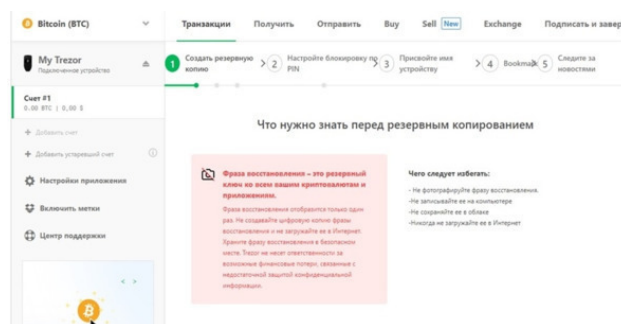


Нажимаете «Установить микрокод» и следуете дальнейшим инструкциям. В процессе установки микрокода следите за тем, что будет появляться на экране компьютера и кошелька. Его придется отключать, и заново подключать, и подтверждать свои действия нажатием на кнопки.

После установки микрокода необходимо создать кошелек или восстановить прежний.



После того как кошелек создан, вам предложат сделать резервное копирование. Это на самом деле важный момент, где нужно создать сид-фразу для восстановления из 24 слов. В комплекте к кошельку идет специальный бумажный кошелек с уже готовыми полями, куда надо будет вписать эти слова. Принимайте условия и начинайте процесс.



Отнеситесь к этому очень серьезно и внимательно. На экране дисплея кошелька будут появляться слова, их надо записывать в бумажный кошелек в той последовательности, в которой они идут, и подтверждать нажатием на кнопку кошелька. Как только вы запишете слова, проверьте повторно внимательно каждое слово – такая возможность будет.

Запишите фразу восстановления

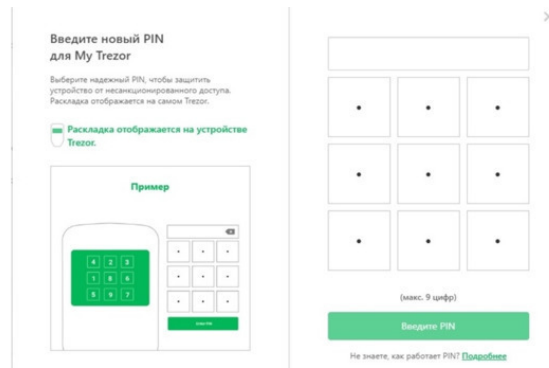
На устройстве Trezor отобразится уникальная комбинация из 24 слов, которая позволит восстановить счета в случае потери устройства. Порядок слов в ней очень важен. Внимательно перепишите с экрана эти слова.

Запишите 6-е слово из Trezor на карточку фразы восстановления.

Не отключайте устройство от сети.

Следующий этап защиты – это создание PIN-кода для быстрого доступа к кошельку. Он может состоять из 4—9 цифр – чем больше, тем надежнее.

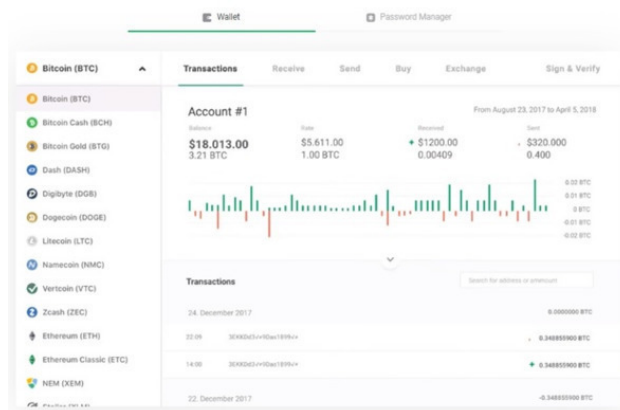
Цифровое поле будет высвечиваться на дисплее кошелька, а на компьютере в окне вам нужно будет эти цифры нажатием в соответствии с тем, как они расположены на дисплее кошелька.



После этого останется задать имя кошельку (но это по желанию), добавить страницу <https://trezor.io/> в закладки браузера, чтобы обезопасить себя от фишингового сайта, и подписаться на новости!

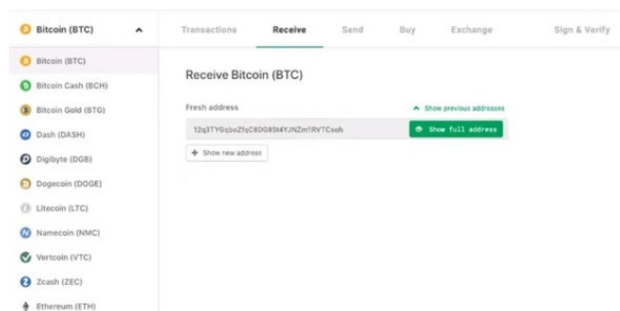
После этого вам откроется личный кабинет кошелька, и можно будет совершать первые транзакции.

Функционал кошелька несложный, тут нет необходимости зачислять кошельки для каждой валюты на кошелек, они просто выбираются из списка в самом сервисе. На основном экране вы увидите свой баланс, транзакции, а также можно сменить свой PIN-код, сделать обмен криптовалют, купить и подтвердить/верифицировать свой кошелек.



Для того чтобы пополнить свой кошелек, вам нужно в левом столбце выбрать криптовалюту, например биткоин, и перейти в закладку «**Receive**».

Здесь показывается публичный адрес вашего кошелька для получения средств, именно по нему можно будет пополнить ваш кошелек.

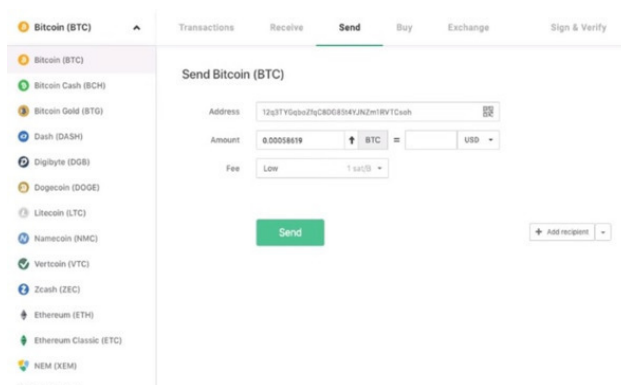


Чтобы отправить кому-нибудь криптовалюту, необходимо перейти в следующую закладку «**Send**».

Здесь можно отправить деньги с вашего кошелька на любой другой адрес. Вам нужно указать адрес получателя, количество и выбрать комиссию в зависимости от срочности отправки и получения средств.

Также есть функции покупки и обмена криптовалюты, но, честно говоря, ими я не пользовался, поскольку есть более проверенные варианты с более низкой комиссией. Но эти функции – это, безусловно, плюс и могут пригодиться в дальнейшем.

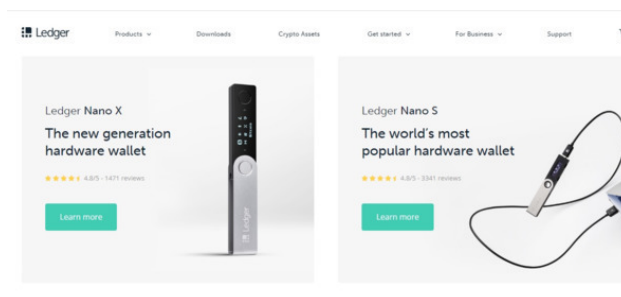
Подпись и верификация – это функция нужна, когда на каком-либо сервисе или бирже просят подтвердить, что этот кошелек действительно ваш.



Собственно, вот мы и разобрали ключевые функции, которые нужно знать. Теперь разберем еще один популярный холодный криптокошелек – Ledger.

Аппаратный кошелек Ledger

Ссылка на официальный сайт, где можно заказать кошелек с доставкой по РФ: <https://www.ledger.com/>.



Наверное, один из самых распространенных аппаратных кошельков. Есть две модели: **Nano S** (начальный вариант) и старшая модель **Nano X** с большим количеством функций и криптовалют.

Основное преимущество – свое приложение **Ledger Live** для гаджетов на iOS и Android, с помощью которого можно управлять криптовалютами без подключения устройства. Но транзакции делать нельзя.

Недостатки – прецеденты с уязвимостью и возможностью взлома, однако достоверных фактов этого нет, это всего лишь потенциальные угрозы, которые были обнаружены довольно-таки давно. С тех пор Ledger шагнули далеко и довольно неплохо доработали свой кошелек,

вопросы безопасности и удобства. Выпустили свое приложение Ledger Live, которое добавило функциональности и удобства в повседневном использовании.

Заказать можно на официальном сайте с доставкой по России.

Первым делом вас попросят задать PIN-код (до 8 цифр), его вы будете вводить каждый раз при подключении и для подтверждения операций. Затем начнут появляться по одному 24 слова – все эти слова в верном порядке (так, как они появляются) нужно записать на бумажку, по ней, в случае чего, вы сможете восстановить доступ к своему аккаунту в системе Ledger и всем вашим кошелькам. Бумажку стоит хранить в надежном месте. Для продолжения работы кошелька попросит вас ввести все эти слова в нужном порядке.

Одно из преимуществ кошелька Ledger в том, что там все делается на кошельке физическим способом, то есть все вводится без участия компьютера и программ на нем, так что если ваш компьютер заражен, то мошенники никак не смогут получить ваши деньги. Но с точки зрения удобства эксплуатации тут есть минус, так как на устройстве всего 2 кнопки и вводить и PIN, и уж тем более сид-фразу (те самые 24 слова) придется дольше.

После этого заходим на официальный сайт Ledger Wallet, там скачиваем программу Ledger Live, регистрируем свое устройство и делаем себе личную запись. Этот сервис не будет владеть вашими приватными ключами, он только агрегирует всю информацию по переводам по публичным ключам, то есть будет позволять вам просматривать ваши балансы на компьютере, и для этого не нужно будет соединения с устройством, но никакие переводы без подключения устройства сделать нельзя.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.