

Криптовалюта. Учебное пособие по работе с цифровыми активами

Автор:

[Дмитрий Приходько](#)

Криптовалюта. Учебное пособие по работе с цифровыми активами

Дмитрий Приходько

Эта книга изменит вашу жизнь раз и навсегда. В ней содержится информация, без которой полноценная жизнь современного человека невозможна. Дочитав до конца, узнаете историю возникновения и основные правила работы с криптовалютами. Также будете знать топовые монеты на рынке и многочисленные способы заработка на них. Данный бестселлер просто необходимо прочитать новичкам криптоиндустрии, а также всем, кто работает в сфере современной экономики и финансов.

Криптовалюта

Учебное пособие по работе с цифровыми активами

Дмитрий Приходько

© Дмитрий Приходько, 2020

ISBN 978-5-4496-8654-1

Создано в интеллектуальной издательской системе Ridero

Слова благодарности

В первую очередь, хочу поблагодарить своих родителей. Они научили меня быть ответственным за свои поступки в очень раннем возрасте. Эта самостоятельность дала свободу для роста, приобретения знаний и развила интуицию. Их труд внес неизмеримый вклад в моё воспитание, формирование характера и личности.

Отдельную благодарность хочу выразить своей старшей сестре, без ее помощи я бы вряд ли преодолел самые темные периоды своей жизни. Она всегда помогала словом и делом. Моя семья всегда верила в меня, даже тогда, когда я сам сомневался в том, чем занимаюсь. Их поддержка и понимание в те моменты, когда рассказы про blockchain технологии портили семейные ужины, была очень важна для меня.

Признателен своим друзьям за то, что не отвели к психотерапевту, после того как я продал свой мотоцикл, что – бы на вырученные деньги собрать майнинг ферму. Помогали мне с настройкой компьютерного оборудования.

Относились с пониманием, когда пропускал праздники и дни рождения общих знакомых, сидя в гараже и осваивая азы майнинга. Ездил в соседние населенные пункты для обмена опытом с коллегами по криптовалютному ремеслу. А потом и вовсе начал писать эту книгу, которая отнимала много свободного времени.

Я благодарен всем за то, что принимаете меня таким, какой я есть. Это дает стимул двигаться вперед с немыслимой скоростью, разрушая все препятствия на своем пути.

Предисловие

«Дайте мне управлять деньгами страны, и мне нет дела, кто будет устанавливать там законы»

Майер Амшель Бауэр (Ротшильд)

Приветствую коллеги!

Очень рад, что вас заинтересовали технологии, которые изменят мир раз и навсегда. Эта книга в руках – уникальный шанс заглянуть в будущее версии 2.0 раньше остальных. Мы с вами пройдем путь познания экосистемы blockchain и криптовалют от истоков до современных, передовых финансовых технологий.

Рассмотрим основные преимущества, уникальность и перспективы развития топовых криптовалютных проектов. Вы узнаете какие монеты сегодня используются для передачи ценности в системе интернета вещей, как работают анонимные криптовалюты, когда за Bitcoin можно будет купить колбасы в магазине у дома и еще очень много других ништяков. Не узнаете эту информацию сейчас, возненавидите себя потом.

По окончании курса, будете объяснять знакомым истинный смысл непонятных для обычного человека слов: токен, форк, хэш, майнинг, атомарный своп, фиат. Кстати, фиат – это не марка автомобиля, а слово напрямую связанное с цифровой экономикой. Гарантирую одно – в процессе чтения ваше мировоззрение изменится раз и навсегда.

Но прежде чем отправляться в мир цифровой экономики, я расскажу вам историю возникновения этого бессмертного произведения. Готовы?! Тогда поехали.

Для начала позвольте представиться, зовут меня Приходько Дмитрий, имею 2 высших образования, одно из них экономическое. Мне 32 года, и большую их часть прожил не зная, что такое цифровые деньги и распределенный реестр. Все изменил 2016 год, год в котором я встретился на перекрестках интернета с криптовалютой под названием Bitcoin.

Мои знакомые, делились по отношению к «крипте» на 2 лагеря. Одни говорили, что это наше будущее, другие что это «пузырь хайпа», который скоро лопнет,

мотивируя свои слова тем что это какие-то цифровые деньги и их нельзя пощупать. А значит и доверять им не стоит.

Я привык доверять фактам, а не слухам и проверять все на себе. В начале ознакомился с первоисточником «white paper» первой цифровой валюты под названием Bitcoin: система цифровой пиринговой наличности. В целом там отражаются основные принципы функционирования, безопасности и защиты транзакций в распределенной сети.

Далее проанализировал всю информацию в глобальной сети, которую смог отыскать об этом «чуде» человеческой мысли. И пришел к выводу что да, это все-таки прорывная технология и за ней будущее. В это время интерес к сфере криптовалют нарастал. Я продолжал изучать данное направление финансовых технологий, ибо, не зная броду в воду не хожу.

Я заходил в любой новый проект, общался с разработчиками и сообществом. Попробовал, наверное, все что доступно в мире blockchain нашего времени. Торговал на криптовалютной бирже, занимался майнингом монет на обычном компьютере, строил фермы для майнинга, участвовал в ICO новых проектов и пытался проводить собственные ICO. Так же мне были близки арбитражные сделки покупки – продажи монеток на разных криптовалютных биржах.

Виды информации: текстовая, графическая и «смартфон»

Отдельным направлением моего развития была интернет – безопасность при производстве транзакций. Ибо набил себе немало шишек, пока не понял, как этим заниматься просто и безопасно. Мне пришлось перепробовать все кошельки для хранения криптовалют от WEB версии до аппаратного кошелька холодного хранения, чтобы выработать для себя основные правила работы с цифровыми активами.

Каждый день находил новое для себя направление исследования и вникал в его самую суть. Время шло... наступил 2017 год, думаю самый безбашенный и головокружительный год для новейшей истории криптовалютного рынка.

Здесь и там появлялись новые монетки, капитализация рынка росла как сумасшедшая, и, следовательно, были те, которые хотели на этом заработать.

В You – Tube и социальных сетях массово стали появляться люди, которые знали где находится та самая пресловутая кнопка «бэбло» и могли поделиться ее координатами за умеренную сумму в 15—50 тысяч рублей. Псевдокоучи разного разлива и мошенники расцвели пышным цветом. Большинство из них рассказывали мотивирующие сказки, про то что вы все можете, стоит только захотеть. И какие-нибудь основы рынка, базовые понятия.

В общем эти ребята продавали воздух, и неплохо зарабатывали на этом. «Хайп» и истерика вокруг Bitcoin нарастала, в клиентах у них не было дефицита. Что еще говорить, если один раз при поездке в такси марки ВАЗ – 2101 доисторического года выпуска в городе Ростов – на – Дону я увидел на ящике бардачка надпись «Bitcoin accepted here». Сами понимаете, у меня был легкий шок от увиденного.

Естественно поинтересовался у водителя в курсе ли он что за наклейка висит у него в машине, как переводится надпись и что она означает?! Сказать, что я был удивлен ответом, ничего не сказать... Мужичек средних лет по имени Валерий поведал, что у меня есть возможность рассчитаться за поездку новой интернет – валютой «бетховенами»! Да, да вам не показалось, именно бетховенами. Конечно при наличии таковых. Что он знает актуальный курс пересчета рублей в эти самые «бетховены» и у него есть на телефоне кошелек, на который он принимает платежи. Вот это приколы?! За композитора таксосу безусловно лайк!

Эта встреча перевернула мою жизнь с ног на голову. Валера конечно не знал английского языка, где-то услышал про бетховены, так и стал их называть. Но по сути... таких скоростей внедрения технологии в массы населения я никак не ожидал. Буквально за один 2017 год почти каждый гражданин России и СНГ знал примерно, кто такой Bitcoin и что его стоимость растет!

Наступил 2018 год, курсы криптовалют снизились, в индустрии наступило равновесие. Но все равно, имидж самой высокотехнологичной сферы в истории человечества был подпорчен скамерами, мошенниками и коучами которые сами ничего толком не знали. Из-за них тысячи людей потеряли свои последние сбережения, по причине того, что не знали азы работы с «криптой», и доверялись первому попавшемуся «гуру».

Многие вкладывали последние деньги в криптовалюту, представляя, что они утратят свои сбережения за месяц. Но увы... Парни, которые собирали деньги у доверчивых обывателей скрывались в неизвестном направлении. И таких становилось все больше и больше....

Я не мог смотреть на такую ситуацию сквозь пальцы... Было досадно слышать упаднические отзывы о своей судьбе тех, кто рискнул сбережениями и потерял все. Почти каждый день приходилось сталкиваться с такими людьми, им было действительно не просто... После одной такой встречи, когда мне рассказал свою историю несбывшихся инвестиций Всеволод, учитель младших классов, я и принял решение - остановить этот беспредел!

В этот же день создал сообщество «blockchain академия» в социальной сети Вконтакте, стал консультировать всех желающих по вопросам, в которых компетентен. Я не брал деньги за свои услуги, мне нравилось, что человек, которому помог уже вряд ли попадет на удочку мошенников. И не потеряет свои активы.

Наше сообщество «blockchain академия» растет и развивается. В данный момент количество участников насчитывает порядка 2000. Мы делимся своим опытом друг с другом, разбираем передовые новинки технологий мира криптовалют. Поверьте, в одиночку выжить, заработать и развиваться на этом рынке практически невозможно!

Теперь о книге. Весь объём информации представленный в ней это мой практический опыт и опыт моих учеников по «blockchain академии». Все наши наработки с 2016 года я упаковал в «кейсы» и необходимые знания для вас, будущие коллеги. Вооружившись ими, вы сможете найти себя в любой сфере нашего общего цифрового будущего!

Данная книга рассчитана на широкую массу людей, которые только соприкасается с этим огромным и необъятным миром экономики завтрашнего дня. В качестве писателя я выступаю первый раз, поэтому если вы найдете какие - либо стилистические недочеты, не судите строго.

Изложение материала будет происходить таким образом, что мы будем двигаться от простого к сложному. В начале вы узнаете, как безопасно создать кошелек для хранения ваших монет, или торговать на криптовалютной бирже,

так же узнаете, как вывести средства в фиатную, не цифровую валюту (рубли, доллары, евро, тенге). Тут разложено по полочкам все что нужно знать для базового навыка обращения с любыми цифровыми криптовалютными активами.

Схемы отображения бизнес процесса

Обычно интернет проекты по обучению работе с криптовалютой за подобную информацию попросят с вас от 500\$ и выше за курс обучения. Этот материал достается вам бесплатно. Та цена которую вы заплатили за книгу в магазине полностью расходуется на оплату услуг по продвижению, дистрибуции и маркетингу.

Я не зарабатываю на этой книге. Моя мотивация состоит в популяризации новой цифровой экономики и развитии своего сообщества криптоэнтузиастов, которые без страха смотрят в будущее и знают, как там жить и получать доход от любимого дела.

В курс обучения входит история возникновения и развития технологии. Мы с вами разберем основные термины, практическое применение и тренды развития данного сектора финансовых технологий. Ну кажется все, ан нет... еще один организационный момент.

Для полного, комфортного и легкого обучения вам нужно установить приложение для считывания QR кодов на смартфон. Скачать его можете абсолютно бесплатно в магазинах приложений Google Play если у вас смартфон работает под управлением операционной системы Android, или в Apple Store для iOS.

Посредством штрих кодов буду давать проверенные, безопасные ссылки на полезные интернет ресурсы, с их помощью можно легко регистрироваться на официальных сайтах сервисов, которые проверены от фишинга и прочих уловок интернет мошенников.

Общий вид QR кода на экране смартфона

Большинство этих ссылок будет реферальные. Что это значит? Той или иной сервис, платформа будут фиксировать, что регистрация выполнена по приглашению. Это даст возможность видеть сквозную аналитику посещения ресурсов, смотреть статистику. Если партнерских регистраций будет много, то на основании полученной информации буду вести переговоры с администрацией сервисов, чтобы «выбить» дополнительные плюшки для наших пользователей.

В тексте ссылки в виде QR кодов выглядят так:

Пример ссылки для считывания смартфоном

Итак, для старта необходимо держать в руках эту книгу, смартфон с предустановленным приложением для считывания QR кодов и соединение с интернетом. Если все в наличии, тогда погнали!

Введение

Данная книга написана бессонными ночами для всех, кто только начинает своё знакомство с миром криптовалют. Она не претендует на лавры профессиональной или научной литературы. Здесь описаны основы, благодаря которым, любой сможет значительно ускорить и обезопасить свои первые шаги в мире цифровых денег.

Этот труд – настольная книга каждого человека, криптоконцентрат, собранный в одном месте для вашего удобства. Не буду утверждать, что иметь дело с криптовалютой и зарабатывать на ней это 100% прибыльное дело. Всегда

имеет место так называемый человеческий фактор. Один человек зарабатывает, другой теряет деньги. Мои алгоритмы и правила работы на этом рынке, научат делать верный выбор в любой экстренной ситуации. Это уменьшит шансы на провал к минимуму.

Решение работать с криптовалютами и получать прибыль, или просто прочитать книгу для общего развития вы принимаете сами. Я не экстрасенс и не могу знать, что будет завтра с рынком. Однако сегодня могу утверждать точно, что, имея базовые навыки работы с рынком криптовалют вы можете организовать себе один из самых высокодоходных видов заработка в мире. За короткое время с минимальными инвестициями каждый из вас может заработать кратный прирост капитала. Который можно сравнить только с торговлей оружием, либо наркотиками.

Желаю вам приятного и познавательного чтения. Надеюсь, что благодаря мне и этой книге вы с лёгкостью откроете для себя мир криптовалют и blockchain технологий. Самая большая награда для меня, ваша признательность!

Глава 1. Blockchain по русски

Вы наверняка уже не раз слышали слово blockchain, но объяснить что это за штука врятли сможете. Просто употребляете его в разговорах как еще одно модное западное слово. Пришлось перерыть тонны литературы что бы разобраться как это все работает. Вам важно знать одно – это основа, на которой основана любая криптовалюта. Технология blockchain – это революция, которая затронет не только сферу финансов, но и многие другие отрасли. Для начала выясним общую концепцию построения системы.

Blockchain (цепочка блоков) – это распределённая база данных, у которой компьютеры с базой данных не подключены к общему серверу. Каждый участник сети на своем жестком диске хранит файлы с постоянно увеличивающимся списком записей, называемых блоками, которые в реальном времени синхронизируются и обновляются.

Это значит, что на каждом компьютере сети есть своя актуальная копия базы данных. Это самый главный принцип децентрализации. Каждый блок содержит

метку времени и ссылку на предыдущий блок.

Использование шифрования гарантирует, что пользователи могут изменять только те части цепочки блоков, которыми они «владеют» в том смысле, что у них есть закрытые ключи, без которых запись в файл невозможна. То есть если обладаешь «закрытым» ключом от зашифрованной информации, ты ее полноправный владелец.

А значит можешь делать с этими данными все что угодно. Кроме того, шифрование обеспечивает синхронизацию копий распределённой цепочки блоков у всех пользователей. Кстати из-за применения шифрования цифровая валюта и стала иметь приставку «крипто».

А теперь перенесемся на миг в будущее. Где уже во всю используется технология распределенного реестра. Представьте себе цифровой паспорт технического средства (ПТС), например, автомобиля: каждая запись о владельцах этого автомобиля и есть такой блок.

У этой записи есть метка: дата и время внесения. Изначальным законом, по которым функционирует сеть считается обязательный запрет на изменение записей задним числом, потому что нужно, чтобы записи о покупке, продаже автомобиля не допускали разных толкований и оставались в исходном виде.

К записям могут получить доступ только госавтоинспекция, у которой есть один закрытый ключ, и текущий владелец автомобиля, у которого есть другой. Затем к этой информации получают доступ только те, кому один из этих пользователей предоставит свой закрытый ключ (например, следующий счастливый обладатель авто).

В основы технологии blockchain заложена безопасность на уровне лучших современных баз данных. Концепцию цепочек блоков предложил в 2008 году некий Сатоши Накамото (Satoshi Nakamoto). До сих пор этого парня никого не видел, но говорят, что он существует... Первый блок был сгенерирован в 2009 году как компонент цифровой валюты – Bitcoin, где blockchain используется как общий децентрализованный реестр всех транзакций.

Благодаря этому Bitcoin стал первой криптовалютой, которая решает проблему двойных расходов (в отличие от «деревянных рублей», электронные деньги

могут тратиться дважды) так как при платежах не используется посредник, такой как банк.

Решение заложено в исходный алгоритм сети, если будет проведена транзакция «двойной траты», то вторая транзакция отправки монет, которых у вас уже нет будет отвергнута сетью. Перенесемся опять в будущее... допустим вы, не являясь человеком отягощенным моральными принципами имея в своем распоряжении 1 Bitcoin купили себе Lamborghini Diablo, соответственно отдали за него одну монетку.

Затем захотели себе еще приобрести личный коучинг Тони Робинса, но вот при оплате произошла проблема. Ваша трата была отвергнута сетью, так как этих средств у вас уже нет. В целом ничего страшного. Вы уедете к себе домой на крутой тачке, смотря на стоящего в стороне грустного Тони.

Причем двойная трата будет возможна в одном теоретическом случае. Если у вас под контролем будет 51% вычислительной мощности сети и при помощи нее вы сможете «пропихнуть» свою транзакцию, но в этом случае все узлы системы узнают о вашем поведении и сразу же прекратят операции и транзакции. Проще говоря даже если кто-то совершит атаку на сеть, это не будет иметь смысла.

Безопасность технологии blockchain обеспечивается через децентрализованную сеть серверов, проставляющие метки времени, и одноранговые сетевые соединения. В результате формируется база данных, которая управляется автономно, посредством алгоритма языка программирования C++. Это делает blockchain удобным для фиксирования событий (например, внесения сведений о праве собственности на дома, квартиры или земельные участки, учет выпуска товаров) и операций с данными, управления идентификацией и подтверждения подлинности.

Глава 2. Что такое Bitcoin?

Что такое Bitcoin?! Большинство людей, у которых вы спросите этот вопрос ответят: «интернет валюта», «деньги из даркнета», «это что-то непонятное». Bitcoin по меркам криптовалют достаточно стар, годом его рождения как

упоминалось ранее был 2009, а вот 2013—2014 годы стали самыми информационно насыщенными в его истории.

«Монета» Bitcoin

Причина достаточно проста: за один Bitcoin стали давать больше 1000 баксов, что не могло не вызвать ажиотажа у мировых спекулянтов. В это время сама тема криптовалют начала набирать колоссальную популярность. У всех возник вопрос... что ты такое Bitcoin?!?

Начнем с того, что следов инопланетян и рептилоидов в появлении крипты не зафиксировано. Все же история появления первого блока Bitcoin окутана тайной. Сеть Bitcoin это технологичная пиринговая сеть. Пиринговые сети (от англ. P2P, peer-to-peer) в интернете известны давно и распространены практически повсеместно. Например, торренты. Каждый из вас неоднократно скачивал фильмы или музыку через трэкер. Общее в любой пиринговой сети – отсутствие центрального сервера, узла, на который всё завязано. Стоит только исключить этот узел, как вся сеть перестает существовать.

В пиринговой сети такого уязвимого места нет. Bitcoin – такая же пиринговая сеть, как и торрент. В ней точно так же пересылается информация. Только эту информацию можно копить и тратить. Эти данные в сети blockchain Bitcoin являются криптовалютой.

На этом остановимся поподробнее... Валюта – то, что принято большой группой лиц как мера стоимости. Мы можем обменять деньги на материальные блага только потому, что в обществе существует подобная установка. То есть все функции, которыми, как утверждают экономисты, обладают деньги, являются следствием договорённости большинства людей в обществе.

Включим нашу воображаемую машину времени и перенесемся снова в прошлое. С собой прихватим чемодан, набитый стодолларовыми купюрами, не возражайте это для тренировки воображения. На данную сумму в нашем времени мы можем приобрести виллу на Гавайях, яхту и шампанское. Но вот в чем загвоздка... мы

в прошлом.

Ребята в 17 веке с непониманием смотрят на меня как на не совсем психологически здорового человека при попытке приобрести продукты на рынке. Они требуют золотые или серебрянные монеты! Для них это деньги! Максимум что мы сможем сделать с баксами это сжечь их в костре, хотя бы погреемся в прохладную ночь.

То есть ценность денег зависит от места и времени их использования. В истории было много денег, которые со временем лишались своих функций, становились прикольным сувениром. Возможно, у вас где-то завалялась советские или перестроечные рубли, банкноты номиналом 50 или 100 рублей. На них в своё время можно было безбедно прожить целый месяц. Но вот рухнуло государство-эмитент, или произошла девальвация рубля – и эти сто рублей интересны только нумизматам.

Делаем вывод: деньгами может быть назначено что угодно согласно общественному сговору, все функции денег придуманы и назначены обществом, ценность денег определяется исключительно доверием к ним. А доверие – штука не постоянная. С этой точки зрения будет проще понять, почему Bitcoin можно называть валютой. Да, это всего лишь цифровые данные. Но сейчас почти все деньги в банках лишь цифры на экране компьютера.

Со времен бреттон-вудского соглашения ни один банк не держит в хранилище эквивалентный запас наличности или тем более золота для покрытия своих обязательств. Когда вы производите перечисление в онлайн банкинге, на самом деле никакого перечисления не происходит, деньги не перемещают физически – просто меняются значения сумм на счетах.

У фиатных денег (рубли, доллары) имеется паритет покупательной способности. Вы можете их на что-то обменять, получить что-то вам нужное (или не нужное – такие покупки для девчонок совсем не редкость).

Но как я куплю картохи у бабульки на даче, скажите вы? Никак... если бабулька не имеет внука, который ее просветил в вопросах крипты и установил на ее смартфон Bitcoin кошелек. И эта бабулька имеет таких же продвинутых подруг. У которых она сможет покупать другие товары и услуги за эту крипту.

Таким образом, с точки зрения потребителя основное отличие Bitcoin от фиата – сложность в обмене на товары и услуги. Если бы Bitcoin начали принимать для оплаты все привычные нам товарные точки, то у него были бы все функции привычных денег.

Современный человек 50% своей жизни проводит за компьютером

История не стоит на месте. Bitcoin становится платежным средством для многих товаров и услуг. На сегодняшний день много видео блоггеров делали челлендж «выжить за крипту», все остались живы и здоровы. А значит, процесс цифровизации денег потихоньку идет. Появляется все больше сервисов в которых вы можете расплатиться криптовалютой.

Активно развивается интернет вещей. В его работе как воздух необходима криптовалюта для взаиморасчетов гаджетов между собой. Допустим вы заказали пиццу, к вам вылетел квадрокоптер и привез пиццу по адресу, у него есть заданная заранее точка посадки. В нее встроен платежный терминал, который привязан к вашему криптовалютному счету. Дрон прилетел к вам, приземлился, оставил пиццу и через терминал принял оплату в Bitcoin после этого улетел восвояси. ВСЕ!! Вы без всяких заморочек получили пиццу и не потратили лишнего времени.

Глава 3. В чем уникальность криптовалюты Bitcoin?

Весь тот хайп, который творится вокруг Bitcoin и других криптовалют происходит по причине массового распространения информации в обществе о революционности идеи цифровых денег.

Ранее гегимония фиатных денежных расчетов была непоколебима. Теперь есть альтернатива, убрать очень большую часть посредников из денежных расчетов. Уверен, что Bitcoin – та технология, которая перевернет весь наш привычный мир

вверх тормашками. Он уже никогда не будет прежним.

Первая черта, из-за которой первая криптовалюта уникальна это ее децентрализованная сеть, которая защищает сама себя от произвола властей, или отдельного нерадивого участника сети. У нее нет «уязвимого места» которое можно уничтожить и вывести из строя всю сеть.

При общении с коллегами я ни раз слышал, что Bitcoin называют «канализационной крысой», расскажу почему. Канализация – это то место где есть в наличии все известные миру вирусы и бактерии, что не мешает крысе жить в таких условиях долго и счастливо. Плюс у нее нет каких-либо «хозяев», у которых можно что ни будь украсть для пропитания, как у обычных крыс.

Теперь проведем аналогию. Местом обитания сети Bitcoin является интернет и даркнет. А вы сами понимаете, что творится в последнее время на этом поприще... миллионы вирусов, хакеров, червей, троянов, рукитов и прочего еще неизвестного болезнетворного живет в цифровом пространстве. Что не мешает системе распределенного реестра Bitcoin работать как часы, без сбоев и зависаний. Не имея какого-нибудь суперсистемного администратора, который за всем следит в режиме «БОГ».

Теперь о живучести. В связи с децентрализацией и трансграничностью системы, которая работает на тысячах серверов по всему миру, бессмысленно принимать законы о запрете Bitcoin в отдельно взятом государстве. Отсутствие какого-либо центрального сервера или дата-центра делает невозможным его штурм агентами ЦРУ.

Bitcoin в виде физической монеты

Bitcoin в отличие от фиатных валют, можно хранить у себя в кармане, при помощи смартфона или аппаратного кошелька для хранения крипты. Вы скажете с банками та же история. Но это не так. В случае с банками вам дают просто удаленный доступ к вашим средствам.

Bitcoin или альткоины физически хранятся на вашем кошельке, жёстком диске, или любом другом носителе информации. Причём украсть Bitcoin с этих носителей невозможно. Для операций с ним нужен специальный буквенно – цифровой код (приватный ключ), который позволяет совершать операции по отправке Bitcoin или другой криптовалюты другим участникам сети.

Bitcoin кардинально отличается от привычных нам денег механизмом эмиссии. Печать новых банкнот в госбанках на сегодняшний день никем и ничем не ограничено. Знаете ли вы, сколько выпущено российских рублей? Уверю вас, этого не знает даже центральный банк Российской Федерации.

Печать денег автоматически их обесценивает, потому что рынок их использования остаётся прежним. Вот вам простой пример... как вы думаете, сколько будет стоить бутылка пива в ближайшем ларьке, если у каждого пацанчика на районе будет по два чемодана с пятью миллионами долларов наличными?! Правильно. Очень высокой!

Количество Bitcoin ограничено. В соответствии с алгоритмом программирования будет создан всего 21 миллион Bitcoin. Именно этим количеством монеток и будет располагать человечество. Несложно представить, что если каждый десятый житель России прикупит себе по одному «битку», то все остальные жители планеты не получат ничего. Процесс эмиссии Bitcoin растянут во времени до 2140 года, от года к году количество добытых Bitcoin будет уменьшаться.

В цифровом мире нет риска купить поддельный Bitcoin. Если только у цыган на курском вокзале в Москве. Да, да. Была такая история. Во время пика спроса на криптовалютном рынке цыгане покупали на aliexpress физические круглые монетки с символикой Bitcoin и продавали в несколько раз дороже необразованным нашим согражданам на пероне вокзала, прямо на выходе из вагонов. Вот что значит предпринимательская жилка!

Алгоритм blockchain сети Bitcoin защищен от эмиссии монеты вне сети, и потом отправки ее к себе на счет. Невозможно просто напечатать себе в кошельке несколько лишних нулей. Хакерам и другим мошенникам проще придумать как обмануть напрямую владельца заветного приватного ключа, чем взламывать сеть. Поэтому вопросам безопасности я советую уделять повышенное внимание.

Так же следует иметь ввиду, что реальное итоговое количество монет Bitcoin окажется меньше 21 миллиона штук. Все дело в человеческом факторе... да да как ни странно в нашем общечеловеческом разгильдяйстве.

Bitcoin безопасно хранить на аппаратном кошельке в надежном месте, или на флешке у себя под рукой. Однако если потеряете флэшку, или отформатируете ее, повредите файлы на ней, – вы лишитесь своих Bitcoin. Что нельзя сказать об аппаратном кошельке. Но об этом речь пойдет чуть позже.

Если вы теряете приватный ключ от вашего Bitcoin кошелька, то вы больше никогда не увидите своих кровных монеток! Будьте осторожны! Каждая криптовалюта создается один раз, и если она потеряна, то взамен ее новой создано не будет. В истории уже известны случаи потери монет глобального масштаба.

Вот вам пример, Джеймс Хауэллс из Англии будучи местным системным администратором выменял в сети более 7000 Bitcoin (тогда еще биток стоил сущие копейки). Соответственно местом хранения их был жёсткий диск ноутбука. Со временем он позабыл о них. Во время эксплуатации винчестер имеет свойство изнашиваться, вот и диск Джеймса пришел в негодность. Он его выбросил на свалку. Зачем дома складировать поломанную технику.

Но как вы понимаете все изменилось, когда курс Bitcoin вырос уже более 5000\$ за монету, лицо Джеймса надо было видеть. Он смекнул сколько бабулесиков выбросил и ринулся этот диск искать. Но шансы перекопать свалку площадью в десятки гектар и отыскать там свой HDD, как вы понимаете, равны нулю.

С учётом подобных потерь следует, что монет Bitcoin, хоть они и генерируются регулярно не очень много, и после того, как будет создан последний «биток», их общее количество начнёт уменьшаться вследствие безалаберности владельцев.

Современный компьютер изнутри

Криптовалюты хороши для совершения платежей тем, что каждая транзакция в сети записывается в «публичный реестр». Данные об адресах получателя и отправителя, сумме перевода доступны для просмотра всеми желающими в любое время. Таким образом, обмануть друг друга при переводах невозможно по определению.

Отправив перевод, вы можете в реальном времени отслеживать состояние вашей транзакции в реестре. По завершении процесса будете точно уверены в том, что сделка прошла успешно. Она длится больше или меньше времени, в зависимости сколько вы отдали монеток за комиссию. Чем больше сумма комиссии сети, тем быстрее завершится ваша операция.

Если провести аналогию с банковской системой, «крипта» выигрывает. При совершении перечисления рублей между различными банками зачастую нельзя быть уверенным, что реквизиты получателя указаны верно.

У Bitcoin легко можно определить, существует ли адрес в сети, сколько там монет онлайн в любое время без проблем и пересылки монет. Если в системе интернет банкинга средства с неверно указанными реквизитами могут «блукать» неделями, то в сети Bitcoin это невозможно.

Все ныне существующие платёжные системы, зависят от централизованной базы данных. В любой момент времени ваши финансы могут заблокировать, списать в пользу государства или иного контрагента. В сети Bitcoin подобного безобразия произойти не может ни при каких обстоятельствах. Всё, что вы отправляли и получали, сохранено в памяти узлов – компьютеров в разных странах. Это максимально диверсифицированная штука для ваших финансов.

Кстати для отслеживания транзакций в сети Bitcoin был создан сервис под названием `blockchair`. Там вы можете проследить всю историю платежей через сеть, так же текущий уровень сложности и текущую комиссию за перевод, ссылка на него вот:

Сервис `blockchair`

Итак, можно подвести промежуточный итог... Сегодня Bitcoin можно назвать настоящим первопроходцем, стоящим у истоков будущей финансовой системы. Признание криптовалюты, как денежной единицы для расчетов, говорит о том, что цифровая монета уже заняла свою нишу в мировой экономике. Это своего рода цифровое золото нашего времени. Уникальное и суперфункциональное. Уверен, что времена, когда купить Bitcoin будет нельзя даже за очень большие деньги скоро наступит. Люди, которые смогли приобрести себе «битка» за ранее будут очень и очень рады. Он со временем не обесценивается, как доллар, рубль или евро. Поэтому как инвестиция в долгую это очень достойный финансовый инструмент.

Глава 4. В чем отличие криптовалюты от традиционных (фиатных) денег?

Можно ли прожить в современном мире без денег? Вопрос скорее философский. Но если вы не живете в джунглях или на необитаемом острове, то ответ я полагаю будет отрицательным.

Все экономические процессы выстроены таким образом, что в случае нештатной ситуации в мире финансов все риски ложатся на конечного потребителя. То есть нас.

Ежегодные кризисы в экономике, которые вынимают из наших карманов бабулесик вынуждают нас быть недовольными денежной политикой государства. А куда нам деваться? Все мы так или иначе пользуемся валютой, которая в современном обществе является монополистом при передаче ценности от одного человека к другому.

В финансовом сегменте экономики много скрытых от посторонних взглядов механизмов, которые день за днем обесценивают деньги. А значит и наш с вами труд. Вы слышали об инфляции? Думаю, уже почти все знают, что это такое.

По сути это увеличение денежной массы на рынке, при сохранении его объёмов. То есть количество продаваемых товаров и услуг остается прежним или уменьшается, а вот цена на них уже подрастет. Эта ситуация невыгодна населению, но выгодна банкирам.

Они «печатают» дополнительные деньги, без которых вам не обойтись. Инфляция заставляет вас нуждаться в большем количестве денег, которые вам с удовольствием предоставят... в кредит.

Peer – 2 – peer платеж

Криптовалюты во главе с Bitcoin – это попытка народа уйти из плена «печатного станка». Центральные банки всех стран давно работают по принципу «деньги ради денег», а не «деньги для экономики». Всевозможные средства массовой информации каждый день, говорят нам что инфляция – это естественно и нормально, а также неизбежно, что они с ней борются, но с переменным успехом.

Горькая правда заключается в том, что инфляция – это заранее спланированная игра банковского картеля, ее регулируют по оговоренному плану и очень скрупулезно. Создают специально, но они никогда не признаются в этом.

«Хозяева денег» озабочены вовсе не нашими пенсиями и зарплатами, а поддержанием уровня инфляции на нужном для них уровне. Она стимулирует каждого из нас все время искать бабулесик. Потому что со временем прожить на одну зарплату, становится невозможно. Сами знаете.

Большинство людей видит только один выход искать подработку к текущей, или вторую работу. Что ведет к проблемам со здоровьем и отношением с семьей. Кстати, ничего капиталисты для себя не выигрывают. В смысле, если человек «хреначит» на двух работах, то как работник он весьма посредственен на обеих, и как правило «спит на ходу».

Посредством механизма инфляции покупательская способность зарплаты каждый месяц снижается. Допустим, ваш доход каждый месяц составляет сорок тысяч рублей. Вы получаете по сорок тысяч в январе, феврале, марте, ... декабре. И наверняка согласитесь с тем, что в январе на сорок тысяч вы могли себе позволить больше, чем в декабре того же года.

Подозрительно, не правда ли? А ваша зарплата наверняка не индексируется на уровень инфляции ежемесячно. В этом и заключается один из «фокусов» инфляции – вас можно обобрать почти незаметно.

Многие из вас помнят дефолт 1998 года, пол страны осталось без средств к существованию. А ведь такая ситуация может повториться в любой момент. Если центральный банк захочет, вас оставят с бесполезными бумажками на руках. Таким образом, если вчера вы могли купить на деньги что угодно, то сегодня можете ими, только потереться.

В связи с вышесказанным Bitcoin и остальные криптовалюты очень выгодно отличаются от привычных денег, стоит только чуть-чуть вникнуть в тему. Что бы пресловутая инфляция не «сожрала» ваши накопления вы вынуждены держать их в банке. Но банк – это очень непрозрачная и мутная структура. Вы никак не сможете управлять или проследить за движением своих средств.

Если кто-то захочет лишить вас сбережений – это будет сделано по букве закона. Банк заблокирует все ваши карточки, вы не сможете воспользоваться своими кровными. Кроме того, процентная ставка по вкладам в банке, как правило, ниже уровня инфляции. А именно вам кажется, что вклад прирастает процентами, тогда как на самом деле вы понемногу теряете ваши накопления.

Еще один самый сильный инструмент против нас у «хозяев денег» это девальвация. Девальвацией можно в одночасье поставить население любой страны на колени. Массовое обесценивание накоплений людей в стране увеличивает число алкоголиков и самоубийств в сотни раз. Рушит множество семей. С девальвацией обокрасть народ проще простого – и гораздо быстрее, чем с инфляцией. Правда, если инфляцию растягивают на долгие года и народ привыкает к кражам из своего кармана. Девальвация же, как чума, просто убивает.

Криптовалюты во главе с Bitcoin не дают никаких инструментов в руки экономической «мафии». Никто, включая массонов, или мирового закулисья не может девальвировать Bitcoin или навязать ему инфляцию 26% в год. Не в их силах запретить Bitcoin и обязать принимать в качестве платёжного средства только доллар.

Естественно, у сильных мира сего есть возможность скупать Bitcoin, потом продавать по дорожке. Но, во-первых, создание Bitcoin растянуто во времени, и завершить эмиссию BTC одновременно невозможно, соответственно, тупо скупить весь «биток» нереально.

Во-вторых, те, кто «генерируют» Bitcoin (майнеры), часть монет оставляют себе, продавая лишь то что необходимо для покрытия издержек производства. «Вытащить» их можно только баснословными ценами на бирже. А это означает беспрецедентный рост его стоимости. Кроме того, монетки Bitcoin которые находятся у долгосрочных инвесторов способствуют росту цены – спрос есть, а предложения в разы меньше. Это, одна из причин, позволяющих прогнозировать увеличение цены BTC в долгосрочной перспективе.

Bitcoin на вашем кошельке – только ваш, целиком и полностью. Он лежит на холодном кошельке аппаратного хранения, который вы храните в сейфе. Если вы его сами не потеряете, никто у вас его не отнимет. Никакое правительство, при помощи законов не сможет обязать вас отдать Bitcoin.

По-простому, Bitcoin не подвержен инфляции, ему не страшна девальвация, его «производители» не могут единолично принять решение об отмене валюты. Подумайте немного над этим, и вы наверняка согласитесь, что ваши сбережения в виде банковских депозитов – не такой уж и безопасный способ сохранения заработанного.

Купленные банкирами СМИ пугают население, которое интересуется Bitcoin и другими криптовалютами словом «дефляция». Как вы понимаете это явление противоположное инфляции. При дефляции стоимость денег растёт, соответственно, с течением времени одна и та же валюта получает всё большую покупательную способность. Следовательно, выгодно становится не тратить баблес, а сберегать. Снижение объёма трат населения означает снижение спроса на товары, а это как говорят по телевизору очень плохо.

При такой ситуации банкротятся предприятия, увольняют сотрудников, а это чревато «кризисом» в экономике. Кстати, слово «кризис», самое любимое в речи экономистов. Но экономисты усиленно скрывают, как устроен реальный сектор экономики. На самом деле повышение покупательной способности денег и привлекательности сбережений не означают что люди перестанут тратить бабулесики на товары повседневного спроса.

На самом деле дефляция – это спасение планеты и наше будущее. Я не шучу. Представьте на минуту что мы перенеслись в дефляционное будущее. Тут почти нет толстяков, которые стали худыми по причине того, что не покупают чизбургеры и вредную колу что бы захватить это на ночь, экономят.

Почти все по городу передвигаются пешком или ездят на велосипедах и самокатах. Это лучше, чем толкаться в пробках на автомобиле (т.е. экономят на бензине). Мужья не тратят лишние средства на покупки жены, которая покупает то, что нафиг не нужно (т.е. тратит деньги впустую), а откладывают на совместный отдых летом. Да, перепроизводство ширпотреба при дефляции снизится.

Чего в этом всем негативного? Ничего. Только позитив. В этом будущем производители товаров вынуждены корпеть над тем, что бы их продукт как можно дольше работал и не ломался. То есть продают изделие с целью дальнейшего использования, а не с целью продажи любой ценой.

Рыночные котировки

Уверен что истощение ресурсов планеты и развращение людей сверхизобилием приведет к краху человеческой цивилизации. Да, я – за умеренность во всём. Дефляция этому способствует.

Она снижает цены. Поднимать цены в условиях снижающегося спроса – невыгодно. Привычным спекулянтам, включающим тучу посредников, приходится удалять особо зажавшиеся звенья. Чтобы убедить редкого покупателя купить свой продукт, продавцы выпускают все более совершенную продукцию. Потребитель понимает, что покупать телефон раз в год и чинить машину раз в месяц очень дорого, и было привычным когда-то в далеком прошлом.

Дефляция «очистила» экономику от паразитов, выросших как на дрожжах благодаря инфляции. Оптимизированы органы власти, департаменты, ведомства. Их содержание в условиях дефляции невозможно – средств на всех

у государства нет. Люди ценят родственников и друзей по-настоящему. Количество свалок сократилось наполовину. Экология стала восстанавливаться. В мегаполисах легко дышать и приятно передвигаться. Нет автомобильных пробок.

Ответьте себе на вопрос хотели бы вы жить в таком будущем? Без мусора, кредитов и посредников? Если да, тогда самое время начать пользоваться криптовалютами.

Bitcoin хотя это и передовое изобретение, пока не сможет заменить деньги полностью ввиду своих технических характеристик. Объем торговли товарами и услугами только в нашей стране больше в несколько раз, чем конечная сумма добытых Bitcoin к 2140 году. Плюс надо учитывать, что некоторая часть выпущенных «битков» безвозвратно утеряна. Из всего вышесказанного можно сделать вывод: Bitcoin – это цифровое золото, революционная инвестиционная идея «для тех, кто понимает», которая будет дорожать в будущем, но не заменит деньги как таковые.

Не Bitcoin единым живет общество. Как я уже говорил «биток» – это первая крипта, которая увидела свет. У нее есть свои преимущества и недостатки с точки зрения криптовалютной индустрии. Уже известны более 2000 монет, которые применяются как средство расчета. Никто не знает, когда и какая криптовалюта займет первое место и станет расчетным средством во всем мире. Как говорится поживем – увидим.

Вводный блок на этом закончен. Теперь мы с вами перейдем к изучению основ, необходимых для работы с «криптой». Будем учиться методикам работы с криптовалютами, как сохранить свои активы и преумножить капитал.

Глава 5. Правила безопасности при работе с криптовалютными активами

Уделите этой главе особое внимание! Перед тем, как начать работу с криптовалютой, поговорим о кибербезопасности. При операциях с цифровыми источниками информации приватность и защита ваших личных данных важна как никогда. В самом начале своей карьеры, я относился к этим вещам

скептически. Не уделял особого внимания антивирусным программам, устанавливал на компьютер пиратский софт, заливал операционную систему с торрент трэкера.

Впоследствии это сыграло злую шутку со мной. Я три раза подвергался атакам хакеров и шпионского программного обеспечения. Что привело к неоднократной потере честно заработанных криптовалют. Этот «пинок под зад» со стороны судьбы заставил разбираться в вопросах безопасности.

Уверен, что изначально правильный подход к делу – залог успеха в будущем. Не повторяйте моих ошибок! Эта глава одна из основных, которые необходимо освоить. Я сформулировал несколько простых правил, которые помогут сохранить ваши сбережения в целостности и сохранности.

При транзакциях криптовалют нет третьей стороны, например, банка. Следовательно, в случае если у вас пропадут ваши бабулесики претензий предъявить будет не кому. Вы и только вы в полной мере отвечаете за сохранность своих приватных данных.

Злоумышленников, которые хотят завладеть вашими деньгами, намного больше, чем вы можете себе представить. Только выполнение всех нижеперечисленных пунктов может гарантировать максимальную безопасность ваших криптоактивов.

Для работы с криптовалютами рекомендую приобрести самый простенький новый ноутбук, что бы там точно отсутствовало предустановленное шпионское ПО. Поверьте, это вложение сэкономит кучу потерянных денег и нервов в будущем! Далее выполняем рекомендации, описанные ниже.

Лицензионное ПО

На компьютере должна быть установлена лицензионная версия операционной системы Windows. Так же остальные продукты, например, Microsoft Word или Excel должны быть лицензионными.

Я понимаю, что гораздо проще скачать это же самое с явными вирусами, или с неявными троянами или рукитами и работать дальше, но эта экономия может выйти вам боком в будущем. Потому что никто не знает какие еще программы и утилиты защиты в пиратские наборы программ. Нельзя до конца быть уверенным в своей безопасности.

Пароль

Установите максимально сложный пароль для входа в операционную систему windows. Даже если комп стоит у вас дома и ни у кого кроме вас нет к нему доступа. Пароль должен содержать буквы, цифры и специальные символы.

WEB камера

Необходимо выполнить защиту вашей вэб камеры на ноутбуке или персональном компьютере. Когда вы ей не пользуетесь ее нужно закрывать защитным непрозрачным кожухом, или просто заклевать скотчем с матовым оттенком, что бы через него не было ничего видно.

Не подумайте, что это мания преследования. Просто были доказанные случаи, когда люди через вэб камеры теряли свои приватные ключи от кошельков, и их монеты просто оседали в карманах мошенников. Как это происходит?

Люди вслух произносят свои пароли от кошельков их записывают хакеры, либо в поле зрения камеры попадает QR код или приватный ключ от кошелька. Так же были случаи, через общение по вэб камере приятели просто передавали друг другу приватную информацию, что приводило к ее компрометации и краже активов.

Современный человек и камеры наблюдения за ним

Антивирус

Необходимо установить любую из существующих антивирусных программ на ваш смартфон и компьютер. Обновить ее до актуального состояния базы данных вирусных сигнатур. Потом проведите полное сканирование компьютера на наличие вирусов и шпионского ПО.

Браузер

Установите удобный и быстрый интернет браузер. Лично я пользуюсь Google Chrome и всем рекомендую.

AdBlock

Установите AdBlock расширение для браузера. Оно обезопасит от посещения фишинговых сайтов, собирающих ваши данные, а также будет блокировать всплывающие окна и навязчивую рекламу. Расширение можно скачать с официального сайта разработчика абсолютно бесплатно.

Отключение автозапуска

Отключите автозапуск на съемных носителях данных (USB флеш карты или внешние жесткие диски). Операционная система при подключении внешнего носителя информации пытается проверить наличие файла autorun.inf на диске и при его наличии выполняет инструкции, которые содержатся в нем.

Этой функцией воспользовались создатели различного вредоносного программного обеспечения, которые выпустили целое семейство опасных программ под названием autorun-вирусы. Конкретную инструкцию по отключению этой функции найдете в сети, там информации более чем достаточно.

Чистка устройств

Удалите с компьютера и смартфона все подозрительные программы и приложения. Этим действием, вы не только сократите риски вирусной атаки, но и освободите память гаджета, а также ускорите его производительность.

E-mail

Заведите себе новый e-mail адрес. Его вы будете использовать для регистрации на биржах и создания аккаунта для криптовалютных кошельков. Если у вас браузер Google Chrome, то и почту рекомендую заводить на www.gmail.com. Вы сможете синхронизировать формы авто заполнения, логины и пароли и прочую информацию со своим аккаунтом Google. Это значительно упростит и ускорит вашу работу в сети.

Обязательно используйте сложный пароль при регистрации e-mail адреса! Минимум 16 символов, содержащий спецсимволы, цифры, а также буквы верхнего и нижнего регистра. Пароль должен выглядеть примерно так «X!w;KVER7878bW». Рекомендую записать пароль и сохранить в нескольких безопасных местах.

Например, в своей записной книжке, и, где-нибудь, в текстовом файле на компьютере, среди текста, но без отсылки на свой email адрес. Ни в коем случае не храните такой текстовый файл на рабочем столе в компьютере!

Не используйте одинаковые пароли! Для каждого email адреса пароль должен быть оригинальным и не использован где-либо ещё. Так же не используйте

одинаковые пароли, при регистрации на биржах и криптовалютных кошельках.

Указывайте при регистрации действительный номер своего мобильного телефона! Если вдруг потеряете пароль, это будет единственный способ для восстановления доступа к вашему e-mail! Берегите свой номер. Если вы меняете свой номер телефона, не забудьте изменить в настройках e-mail свой старый номер на новый. Это важно!

Wi - Fi

При работе с криптовалютами нежелательно использование беспроводного доступа к интернету, только кабельный ввод в сетевую карту. У ПК и ноутбука рекомендую отключить вайфай адаптеры, или сделать их неактивными. В противном случае есть угроза доступа к вашим данным через взлом вайфай протокола.

Вредоносные или фишинговые ссылки

Будьте внимательны к ссылкам на сайты, на которые переходите. Многие, в том числе я, используют сервис <https://goo.gl> для создания коротких ссылок. Например, вот такая ссылка:

https://www.coinex.com/account/signup?refer_code=bkmpq58 Пройдя через сервис сокращения, превращается в <https://goo.gl/qweRt>.

Кликнув по короткой ссылке, вы заметите, что она переносит вас туда же, что и ссылка выше. Бывали случаи, что этот сервис использовали злоумышленники, перенаправляя трафик на фишинговый сайт, с целью завладеть вашими данными.

Чтобы расшифровать ссылку, используйте сервис unshorten. Ссылка на него вот:

Сервис unshorten

Просто вставьте в поле короткую ссылку, например, <https://goo.gl/MxFSrT> и нажмите кнопку «Un-Shorten». Ниже увидите адрес, на который ведет короткая ссылка.

Проверяйте абсолютно все ссылки, даже те, которые присылают вам ваши знакомые. Мошенники часто используют контакты своей жертвы, для отправки фишинговых ссылок от взломанного лица.

Добавляйте ссылки таких сайтов, как биржи, банки и платёжные системы в «закладки» вашего браузера. Один из самых распространённых видов мошенничества в сети – создание копии сайта (например, сайта биржи) с трудно отличимым названием адреса.

Чаще всего, злоумышленники оставляют название и меняют домен сайта. Например, если ссылка на официальный сайт крипто биржи binance выглядит так «binance.com», при желании можно ввести вас в заблуждение, создав сайт с аналогичным названием и контетом на другом домене, допустим «ru». Тогда ссылка будет выглядеть следующим образом – «binance.ru».

Еще один из методов обмана пользователей – изменение похожих букв в названии. Я поменял две буквы местами, что практически незаметно с первого взгляда – «banince.com».

При помощи SEO оптимизации и платной контекстной рекламы, можно вывести фейковый сайт в топ поисковой системы. Тогда при запросе «биржа бинанс», на первом месте в поиске появится ссылка на фейковый сайт, но большинство будет думать, что он настоящий.

Вывод: перед вводом личных данных (логины, пароли, номера карт, приватные ключи и. т. д.) на любом интернет ресурсе предварительно убедитесь, что это официальная страничка нужного продукта, а не красивая обманка мошенников!

Для вашего удобства все ссылки на интернет ресурсы, указанные в этой книге проверены на фишинг и прочие уловки хакеров, и являются официальными версиями сайтов! Необходимо только считать соответствующий QR код смартфоном и перейти на сайт. После этого – сделайте себе закладку в браузере, под адресной строкой, чтобы потом не искать.

Двухуровневая аутентификация

Используйте двухуровневую аутентификацию везде, где есть риск потери денежных средств. Существует два вида аутентификации, это смс на ваш номер телефона и google authenticator. Для первого варианта надо указать номер телефона в своем аккаунте, на него будут приходить одноразовые коды доступа, то есть всегда после логина и пароля необходимо будет вводить код из смс.

Для второго варианта необходимо установить приложение google authenticator на смартфон. После этого в вашем аккаунте, надо выбрать способ двухфакторной аутентификации – google authenticator. Затем появится QR код, который надо отсканировать приложением смартфона. Только обязательно где-нибудь его сохраните. А то в случае пропажи смартфона вы потеряете доступ к своим средствам.

Все! Аккаунт этой площадки сохраняется в смартфоне автоматически. Учтите, что код доступа к сервисам в google authenticator меняется каждую минуту. То есть всегда для доступа в ваш аккаунт после логина и пароля необходимо будет вводить одноразовый код из приложения.

Соблюдение вышеперечисленных правил безопасности критически важно для вас. Только при выполнении всех без исключения можете рассчитывать на спокойный сон. Далее переходим к изучению законов построения цепочек распределенного реестра blockchain. А это значит, что в следующей главе будем изучать «анатомию» криптовалюты.

Глава 6. Основные термины криптовалютной индустрии

Ну что братья и сестры по криптосообществу, готовы «впитывать» информацию? Тогда, пожалуй, начнем повествование. Современная история криптовалют довольно короткая, но наполнена до отказа важными событиями. Это сверх динамичная отрасль цифровых финансовых технологий.

Каждый день в индустрии появляется что-то новое, и охватить весь этот объем информации в одиночку невозможно. Тем более описать все в одной главе книги. Но я старался... честно... Выбрал самое важное, ту информацию без которой просто нельзя развить бурную деятельность в финансовой сфере цифрового будущего.

Перевел на русский язык материалы, которые в оригинале были написаны на английском. Максимально все структурировал для вашего удобства. Что из этого получилось читайте ниже.

Криптография

Использование математики для создания кодов и шифров с целью скрыть информацию. Технология blockchain использует криптографию в качестве средства защиты личности пользователей, обеспечивая безопасность транзакций.

Криптовалюта

Цифровые деньги, созданные по определённым алгоритмам с применением криптографии (шифрования). Применение техники шифрования позволяет ей быть защищённой от мошенничества. У нее есть создатель (программист, написавший код), но нет владельца, который мог бы у всех всё отобрать, принудительно обесценить, или запретить к использованию.

Блокчейн (blockchain)

Дословный перевод с английского – цепочка блоков.

Представляет из себя реестр, состоящий из непрерывной последовательной цепочки блоков с информацией. Блокчейн Bitcoin представляет из себя базу данных, состоящую из всех когда-либо совершённых транзакций, находящуюся в свободном доступе.

Цепь выстроена по определённому алгоритму. Каждый новый блок связан с предыдущим, содержит в себе набор записей и добавляется всегда строго в конец цепочки. Копии цепочек хранятся параллельно и независимо друг от друга. Обработываются сразу на множестве компьютеров, что предотвращает возможный сбой или вмешательство в один из блоков.

Выглядит это примерно так:

Модель blockchain сети

Если попытаться изменить информацию в блоке на одном компьютере, то все остальные узлы, находящиеся внутри сети, подтвердят, что данная операция изменена, а значит недействительна, сеть отвергает эту цепочку, и операции происходят дальше.

Это никак не отразится на blockchain сети в целом. Любой пользователь имеет возможность свободного доступа к информации, используемой в ней, что делает распределенный реестр абсолютно прозрачным. В любой момент вы можете скачать к себе на компьютер весь blockchain и синхронизировать его в реальном времени, иметь актуальную информацию о всех транзакциях.

Несмотря на полную прозрачность, также сохраняется максимальная анонимность. Совершая перевод криптовалют с одного кошелька на другой, в реестре blockchain остаётся лишь информация о сумме отправленных монет, адреса кошельков отправителя и получателя, без какой-либо информации об участниках сделки.

Блок (Block)

Каждый блок цепочки содержит случайное число, которое является ответом на математическую задачу. Решение конкретно этой задачи происходит перебором случайных чисел множеством компьютеров, используемых «майнерами» это люди или организации у которых имеется оборудование и вычислительные мощности.

Когда задача решена и число совпадает, сеть подтверждает решение и блок присоединяется к цепочке. Это необходимо для того, чтобы исключить нахождение двух и более блоков одновременно. Теперь рассмотрим один из блоков подробнее, на рисунке ниже я показал схему его построения.

Упрощенная модель одного блока цепочки

Вся информация проходит шифрование, что бы злоумышленники не могли перехватить и заменить данные в блоке. Шифрование идет по специальным алгоритмам с использованием хэша.

Хэш

Процесс математического преобразования любой информации в буквенно – цифровую фразу. Например, хэшировать слово «KUKOIN» алгоритмом SHA-256, то получим следующее

«18833da39fb9b7f8c917fe0220x8l4df8fb16e39f04dbe827e2d200». Этот процесс называется хэш-функция. Хеширование широко применяется в криптографии.

Чтобы визуально представить блок – включите свое воображение. Блок появляется благодаря майнерам, которые создают его, решив на своём оборудовании сложную задачу, выданную сетью. Когда самому удачливому из майнеров удаётся найти решение задачи, сеть подтверждает, что решение верно. Майнер в свою очередь получает награду в виде заданного количества криптовалюты как говорится за труды праведные.

Блок содержит в себе информацию, которая была передана вам в зашифрованном виде от предыдущего блока. Перед тем, как предыдущий блок передал вам шифр, вы обменялись паролями как разведчики на задании, чтобы удостовериться, что перед вами действительно не мошеннический блок.

Современное сетевое оборудование

Теперь блок может начать записывать в себя транзакции, подтверждая их. Эти транзакции уже были проведены, но находились «вне закона», а как только появился новый блок в цепочке, они поместились внутри, тем самым став подтверждёнными.

Теперь наш воображаемый блок стал частью длинной цепочки и бережно хранит в себе данные, которые не могут быть изменены! Я намерено упустил технические тонкости, оставив лишь основную суть, чтобы сформировать чёткое представление, что такое блок.

Майнинг

Процесс добычи криптовалюты на всём, что в состоянии производить необходимые вычислительные операции. Для этой цели пригодны как специализированные устройства ASIC так и персональные компьютеры, ноутбуки. Соответственно человек который контролирует этот процесс называется майнером.

Почти все криптовалюты, в том числе и Bitcoin поддерживаются майнерами. Но есть так называемые «не добываемые монеты», например, монетка Ripple (XRP). Она не подтверждает свои транзакции майнингом, а рыночная цена актива зависит от ценности проекта, что является негативом для лиц, предпочитающих иметь дела только с «добываемыми» монетами.

Майнинговая ферма

Оборудование, предназначенное для майнинга криптовалюты. Фермы могут быть различными по размеру, виду и мощности. Обычный системный блок персонального компьютера, четыре видеокарты с блоком питания и огромный ангар со стеллажами ASIC – это всё фермы.

Производительность ферм разнится в зависимости от оснащения, но все они характеризуются высоким потреблением электроэнергии и большим тепловыделением, поэтому нуждаются в охлаждении. Устройства, на которых криптовалюта майнится в промышленных масштабах, размещаются в местах с дешёвым электричеством и холодным климатом с целью продления срока жизни оборудования.

Алгоритм консенсуса и протокол сети

В контексте криптовалют, алгоритмы консенсуса являются решающим элементом каждой blockchain сети, поскольку они отвечают за поддержание целостности и безопасности этих распределенных систем.

Алгоритм консенсуса – это механизм, с помощью которого сеть достигает консенсуса. Публичные (децентрализованные) blockchain цепочки построены как распределенные системы, и поскольку они не полагаются на центральный сервер, распределенные узлы должны согласовывать валидацию (подтверждение) транзакции между собой.

Именно здесь вступают в силу алгоритмы консенсуса. Они уверяют, что соблюдаются правила протокола, и гарантируют, что все транзакции происходят доверенным способом, и отсутствует возможность двойной траты монет. Очень часто путают понятие алгоритм консенсуса и протокол сети. Хочу внести немного ясности.

Эти термины используются взаимозаменяемо, но это не одно и то же. Проще говоря, мы можем охарактеризовать протокол как первичные правила blockchain сети, а алгоритм консенсуса – механизм, с помощью которого они будут выполняться.

Существует несколько типов алгоритмов консенсуса. Наиболее распространенными являются Proof of Work и Proof of Stake. У каждого есть свои преимущества и недостатки, при попытке добиться баланса безопасности, с функциональностью и масштабируемостью.

Например, алгоритмом консенсуса сети, является то, что определяет в ней валидацию транзакций и блоков. Таким образом, Bitcoin и Ethereum являются протоколами, а Proof of Work и Proof of Stake являются их алгоритмами консенсуса. Теперь разберемся поподробнее с ними...

Proof of Work (PoW) – первый алгоритм консенсуса, который был создан. Он используется Bitcoin и многими другими криптовалютами. Алгоритм Proof of Work является основой майнинг процесса.

Внешний вид майнеров

Майнинг PoW включает в себя бесчисленные попытки хеширования, поэтому чем больше вычислительная мощность, тем больше попыток в секунду. Другими словами, майнер с высоким хешрейтом имеет больше шансов найти правильное решение для следующего блока.

Алгоритм консенсуса PoW объединяет майнеров, которые подтверждают новые блоки транзакций и добавляют его в blockchain цепочку, далее распределенные узлы сети достигают консенсуса и соглашаются с тем, что хеш блока, предоставленный майнером, является подтвержденным.

Алгоритм консенсуса Proof of Stake (PoS) разработан в 2011 году в качестве альтернативы PoW. Хотя PoS и PoW имеют похожие цели, но имеют некоторые кардинальные различия. В нескольких словах, алгоритм консенсуса Proof of Stake заменяет технологию майнинга PoW механизмом, в котором блоки проверяются в соответствии с долей монет участников в сети.

Валидатор транзакций вносит свои монетки в blockchain, и количеством этих монет определяется его вес в сообществе майнеров, а не количеством его вычислительной мощности. Каждая система PoS может реализовать алгоритм по-разному, но в целом цепочка блоков обеспечивается псевдослучайным процессом отбора, который учитывает баланс монет узла сети и возраст монеты (как долго монеты заблокированы или находятся в доле), наряду с фактором рандомизации.

Вышеперечисленные протоколы консенсуса отнюдь не все, которые применяются на сегодняшний день. Попадаются и довольно экзотичные, которые мы рассмотрим в следующей главе книги.

Генезис блок

Самый первый блок в цепочке blockchain. Точнее сказать это даже не первый, а нулевой блок. Любая криптовалюта начинает добываться с нулевого блока, то есть с генезис блока.

Нода

Любой компьютер, подключенный к сети blockchain той или иной криптовалюты. Ноды децентрализованной сети контактируют посредством одно ранговой пиринговой сети для обмена информацией о блоках и транзакциях. Нода, в зависимости от ее типа, хранит только часть или все данные blockchain.

Полная нода – это компьютер, постоянно подключенный к сети blockchain и полностью синхронизированный с ней. Он хранит все данные распределенного реестра, начиная с генезис-блока.

Полные ноды не берут платы за обслуживание сети, загружают и валидируют (подтверждают) каждый блок с транзакциями, руководствуясь исключительно алгоритмом консенсуса и являются полностью независимыми. Полные ноды отфильтровывают противоречащие консенсусу блоки или отдельные транзакции.

Мастерноды – это специально настроенные полные ноды, разделяющие майнерам вознаграждение за обслуживание сети. Они с успехом используются для поддержания сети криптовалюты Dash. Так же они обеспечивают повышенную анонимность, поскольку информация о транзакциях не находится в общем доступе, а записывается только на мастернодах.

Сверхмощные серверные стойки с оборудованием

Подтверждение транзакции

Процедура, выполняемая автоматически сетью. При отправке монет некоторое количество произвольно выбранных компьютеров подтверждают подлинность транзакции, после получения нескольких подтверждений транзакция считается действительной и более никто никогда не сможет утверждать, что такой транзакции не было.

Транзакции в blockchain сети сохраняются навечно в «открытой книге», называемой «public ledger». Все криптовалюты предоставляют приватность для пользователей, но данные о задействованных кошельках, суммах, датах платежей записываются в «открытой книге» и доступны к просмотру любым человеком, когда угодно. «Открытую книгу» можно в любой момент скачать к себе на компьютер и иметь под рукой записи о всех транзакциях в сети, когда-либо совершённых.

Майнинговый пул

Пулom, также майнинг пулом, называют сервер, распределяющий майнинг между множеством участников, что упрощает и ускоряет добычу нового блока. При коллективной добыче блоков, майнеры делят награду за рассчитанный блок между собой.

Он распределяет награду в зависимости от мощности, выделенной тем или иным майнером. То есть, если вы майнили на пуле с одной видеокартой, а другой майнер с десятью такими картами, то после нахождения блока, майнер с десятью картами получит в десять раз больше вознаграждения.

Награда за блок

Премия, которую получает майнер или группа майнеров, работающих в пуле, за добавление очередного блока в цепочку blockchain.

Премайн

Это монеты, которые были намайнены до официального запуска криптовалюты разработчиками. На низкой сложности майнится некоторое количество блоков и монет, а затем валюта выходит публично. Это дает возможность быстрого

и незатратного майнинга, получается много монет, с которыми потом можно манипулировать рынком.

Инстамайн

Это монеты, которые находятся в генезис блоке. Количество монет закладывается алгоритмически, их может быть больше, чем будет в последующих блоках. Иногда это понятие используется для раннего майнинга первых блоков на простой сложности.

Криптовалютная транзакция

Транзакция Bitcoin или другой криптовалютой, это передача средств с одного кошелька на другой. Отправитель указывает необходимое для передачи количество криптовалют, вводит адрес кошелька получателя, который одновременно является публичным ключом кошелька получателя, подписывает транзакцию приватным ключом от своего кошелька и отправляет средства.

Как только транзакция подтвердится, Bitcoin или другие монетки поступят на кошелек получателя. При этом берется комиссия. Чем она выше, тем быстрее средства дойдут до получателя.

Комиссия сети

Плата за транзакцию по blockchain сети.

Криптовалюта и девушка

Криптовалютный кошелек и его адрес

ВНИМАНИЕ! ВАЖНАЯ ИНФОРМАЦИЯ!

Я прошу отнестись как можно серьезнее к правилам работы с криптокошельком описанным ниже. По статистике незнание именно этих основ работы с валютой приводит к потере ваших криптовалют.

Принцип работы любой криптовалюты основан на асимметричном шифровании данных. Оно происходит посредством публичного и приватного ключа. Монетки имеют цифровую природу и как будто «вшиты» в блоки blockchain сети. Что бы их куда-либо перевести необходимо иметь в своем распоряжении те самые публичные и приватные ключи. Именно за ними охотятся мошенники.

Знай, кто владеет публичным и приватным ключом от криптовалютного кошелька тот его хозяин! Система криптовалют децентрализована, если злоумышленники завладеют обеими ключами от вашего кошелька они смогут отправить ваши кровные куда угодно. Вы никак не вернете их. Так как откатить назад транзакции невозможно! Теперь давайте разберемся, что это за ключи такие ценные?

Публичный ключ вы передаете партнерам для отправки на него монет, его могут знать многие, это нормально. Если кто-то знает ваш публичный ключ от кошелька он сможет только посмотреть его баланс, или кинуть туда бабулесиков и больше ничего. Для более простого понимания дам простую аналогию. Все включаем воображалку!

Представьте, что криптовалютный кошелек – это то же самое что ящик e-mail. Электронная почта имеет свой адрес, это как раз публичный ключ. Его может знать много людей, без угрозы безопасности. А вот пароль доступа от ящика имеет только его хозяин, это приватный ключ. Таким образом для почтового сервера все равно кто пришел, если он знает адрес и у него есть пароль, то он хозяин почты! Вывод: необходимо как зеницу ока хранить ваш приватный ключ, и никогда, ни при каких обстоятельствах никому не давать его.

Обычно люди думают, что для криптовалюты адрес кошелька (или публичный ключ) от этого кошелька выглядит примерно одинаковым для всех валют, но это не так!!!! Адрес кошелька эфира (ETH) выглядит так:

«0xAQW5890622FCF21fE69ff99E62090E9c9ci1CU89»

Когда адрес кошелька Bitcoin (BTC), выглядит таким образом
«587NBzjqbuENEo9utGC7kjYepMrf3gXfge».

Обратите внимание, адрес ETH начинается с «0x», имеет от 40 до 44 произвольных латинских букв и цифр, адрес BTC не содержит такие символы как (0, O и I), и состоит из 26 до 35 буквенно-цифровых латинских символов, начинающийся с «1» или «3».

Это только пример двух основных криптовалют. Запомните обязательно одно правило. Всегда отправляете транзакции в пределах одной сети, т.е. вы пересылаете средства с кошелька Bitcoin на кошелек Bitcoin, с кошелька эфира на кошелек эфира, с кошелька рипл на кошелек рипл. Если вы отправите, например, с кошелька Bitcoin монеты на кошелек Bitcoin cash, то ваши средства пропадут безвозвратно! Будьте очень осторожны!

Приватный ключ может быть представлен в виде сид (seed) фразы, которая представляет из себя рандомный набор слов, расположенных в определенном порядке. Сид также может выступать гарантом сохранности ваших средств. Зная сид, вы сможете в любой момент получить доступ к своему балансу.

Теперь мы с вами знаем, что такое адрес криптовалютного кошелька, а что же такое сам кошелек? Криптовалютный кошелек – это программа клиент blockchain сети, с помощью которой пользователь управляет своими счетами. Основные правила безопасности при хранении монет и виды лучших на сегодняшний день кошельков мы рассмотрим далее в этой книге.

Seed-фраза

Фраза, состоящая из 12, 18 или 24 слов, которая используется для восстановления криптокошелька. Если вы, например, удалите программу кошелька со своего смартфона или ПК, это никак не скажется на балансе вашего счета. Информация о ваших балансах монет хранится в blockchain и защищена шифрованием. Seed-фраза – это мастер-ключ, зная который можно получить функции управления счетом, выполнив процедуру восстановления.

Внимание! Тот, кто знает seed, имеет полный доступ к кошельку и может распоряжаться средствами на свое усмотрение. Поэтому сид нельзя никому говорить. Хранить его тоже нужно таким образом, чтобы никто не смог его обнаружить. К примеру, в сейфе. А еще лучше, переписать на бумажку и разделить на несколько частей.

Хранение seed фразы на устройствах, подключенных к интернету не рекомендуется. Потому что данные могут быть уничтожены из-за технического сбоя или похищены компьютерным вирусом.

Crowdfunding

Финансирование проекта большим количеством участников.

ICO (Initial Coin Offering), IEO (Initial Exchange Offering) и STO (Security Token Offering)

Все это способы «первичного предложения монет». ICO является одной из форм привлечения инвестиций в виде продажи инвесторам фиксированного количества новых единиц криптовалют, полученных разовой или ускоренной эмиссией.

IEO тот же самый процесс, только при поддержке криптовалютных бирж. А STO это «предложение токенов как ценных бумаг» то же самое что и ICO, только проекты проходят более тщательную проверку в комиссии по ценным бумагам.

Софт кап, soft cap

Минимальный порог сбора средств в ICO, IEO или STO, необходимый для полноценного развития и запуска проекта.

Хайп, hype

В переводе английского high yield investment program высоко прибыльный инвестиционный проект, как правило такие проекты платят недолго, а потом превращаются в обман и надувательство.

Токены

Единица стоимости и расчетная единица, чаще всего применяемая в ICO. Этот внутренний актив проекта – своеобразный аналог акций компании.

Использование токенов ограничено рамками определенного проекта, но они многофункциональны: их можно использовать как валюту внутри проекта. Или как показатель владения акциями для права голоса за изменения в проекте.

В зависимости от особенностей и назначения можно выделить два основных типа токенов:

– utility-токены, которые позволяют владельцу использовать сервисы и услуги эмитента токенов. Их используют для финансирования проектов общей инфраструктуры.

– security-токены, которые дают владельцу право на реализацию его инвестиционных интересов. Это может быть право на участие в капитале, прибыли, и.т.д.

Также у токенов есть стандарты, без них токены не смогут выполнять свои функции. Их очень много, но основные сосредоточены на платформе Ethereum. Наиболее известный из них – ERC20.

Альткоины

Альтернативные монеты. Альткоинами называются все криптовалюты, выпущенные после Bitcoin. Ими являются, например, etherium, litecoin, monero, dash которые достаточно известны и широко применяются в криптосообществе, хотя их стоимость во много раз меньше, чем стоимость «битка».

Эмиссия криптовалюты

В экономике этим термином называют выпуск денег. Обычно эмитентом национальной валюты является центробанк страны. Результатом эмиссии может быть также создание ценных бумаг, или, как в нашем случае – криптовалюты.

Конец ознакомительного фрагмента.

Купить: https://tellnovel.com/ru/prihod-ko_dmitriy/kriptovalyuta-uchebnoe-posobie-po-rabote-s-cifrovymi-aktivami

Текст предоставлен ООО «ИТ»

Прочитайте эту книгу целиком, купив полную легальную версию: [Купить](#)