ТОТ САМЫЙ ИНТЕРНЕТ-БЕСТСЕЛЛЕР

КРИПТВОЮ МАТЕМАТИКА

АЛЕКСЕЙ МАРКОВ

АЛЕКСЕЙ АНТОНОВ

18+

ВРЕМЕНА

КАК ПОТЕРЯТЬ ВСЕХ ДРУЗЕЙ И ЗАСТАВИТЬ ВСЕХ СЕБЯ НЕНАВИДЕТЬ

Звезда Рунета. Бизнес

Алексей Марков

Криптвоюматика. Как потерять всех друзей и заставить всех себя ненавидеть

«АСТ»
2018

УДК 336
ББК 65.264

Марков А.

Криптвоюматика. Как потерять всех друзей и заставить всех себя ненавидеть / А. Марков — «АСТ», 2018 — (Звезда Рунета. Бизнес)

ISBN 978-5-17-109364-8

Криптовалюта – это уже не просто новое словечко из интернета или ругательство, а настоящий бум XXI века. Уже не осталось никого, кто бы не знал о существовании криптовалюты, однако людей, которые знают, что с ней делать, с каким соусом подавать и как благодаря ей стать вечно счастливым и здоровым, – почти нет. Но не беспокойтесь – в ваших руках сейчас находится книга «Криптвоюматика», в которой вы найдете не только пищу для ума, но и ответы на самые важные вопросы. Книга содержит нецензурную брань

УДК 336
ББК 65.264

ISBN 978-5-17-109364-8

© Марков А., 2018
© АСТ, 2018

Содержание

Об авторах 6
Благодарности 7
Вступление 8
Хайп 2017-го 9
Истории успеха 12
Истории провала 15
Глава 1 21
1.1 22
1.2 26
1.3 29
1.4 34
1.5 38
Глава 2 42
2.1 43
Конец ознакомительного фрагмента. 44

Алексей Марков, Алексей Антонов
Криптвоюматика
Как потерять всех друзей и заставить всех себя ненавидеть

Серия «Звезда Рунета. Бизнес»

© А. Марков, текст
© А. Антонов, текст
© ООО «Издательство АСТ»

* * *

Об авторах

Алексей Марков – создатель лучшего в мире учебника по финансовым рынкам для гопников-интеллектуалов (бестселлер «Хулиномика»), кандидат экономических наук, преподаватель престижного вуза. Заслуженный рокер Российской Федерации.

Алексей Антонов – видный покупатель и продавец токенов на бирже, инвестор, кофаундер SONM, публичный спикер со сцены. Отдал маме «Порше Кайен».

Благодарности

Авторы пока никого не благодарят. Наоборот – ждут, пока их самих отблагодарят.

Вступление

Хайп 2017-го

Скорее всего, вы услышали про биткоин в прошлом году. Но за последние пару месяцев тема уже успела вас достать. Вот и мы больше не можем молчать, ибо кто будет спасать отечество? Биток по 8 тыщ! По 15 тыщ! По 17, 18, и вот уже и по 20 тыщ долларов. А теперь опять по 8! Простые ребята, вроде нас с вами, только кусают локти, пока криптоолигархи сказочно обогащаются. То и дело приходят новости о новых миллионерах и даже миллиардерах. Люди стали искать крипту даже в «Гугле»: слово bitcoin искали в 6 раз чаще, а ethereum – в 8 раз чаще, чем в 2016 году.

И вправду, 2017-й стал дико удачным годом для криптовалют: бешеный рост, статьи в газетах, высказывания банкиров, запреты центробанков, халявные миллионы у каких-то молокососов (это как раз самое обидное!), да еще какой-то канадец Виталик со своим эфиром…

ПОГОВАРИВАЮТ, ЧТО ОН ВСТРЕЧАЛСЯ С ПУТИНЫМ И ДАЖЕ ДАЛ ЕМУ ДЕНЕГ НА ИЗБИРАТЕЛЬНУЮ КАМПАНИЮ; НУ ИЛИ НАОБОРОТ, МЫ НЕ ЗНАЕМ, КАК ТАМ У НИХ УСТРОЕНО В КУЛУАРАХ ВЛАСТИ.

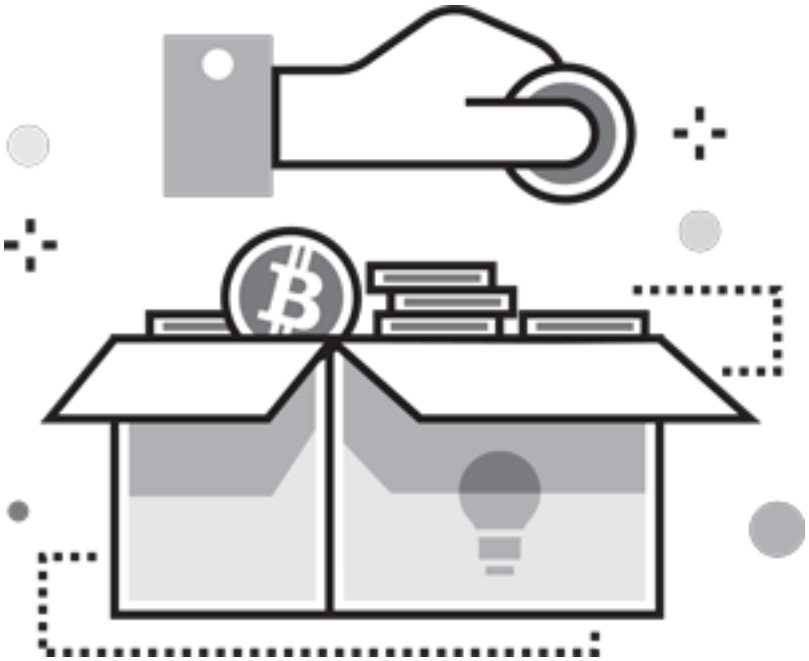
Рост казался нереальным: за год биткоин надулся почти в 20 раз! Правда, потом припал. Все сразу закричали про очередной пузырь, МММ и аферистов, но втайне все равно плакали, что не купили по три; хотели-хотели, да вот почему-то не смогли. Хотя шансы были: начав год с 1000 баксов, биток проседал до 770 долларов, потом с 1250 до 900 долларов, короче колбасило нормально. Закупиться можно было много раз. Но вы не стали.

Да, рос ведь не только биткоин. Как выяснилось, у него еще есть друзья: эфиры, лайткоины, риплы, дэши, монеро – даже зеки какие-то. Все они дико, яростно ломились вверх, и в один прекрасный момент общая капитализация всех криптовалют перевалила цену «Фейсбука» (не говоря о наших карликовых народных достояниях типа «Газпрома» и «Сбербанка»). За 2017 год общая капитализация крипторынка выросла в 30 раз!

Потом вдруг все дико начали майнить. Из магазинов пропали видеокарты. Что за херня? Почему они всем внезапно понадобились? Как это – добывать деньги на своем компе?

ПОЧЕМУ ЭТО МОЖНО? ПОЧЕМУ НАМ НЕ СКАЗАЛИ РАНЬШЕ, СУКА?! ВЕДЬ КОМПЬЮТЕРЫ У НАС С 13 ЛЕТ!

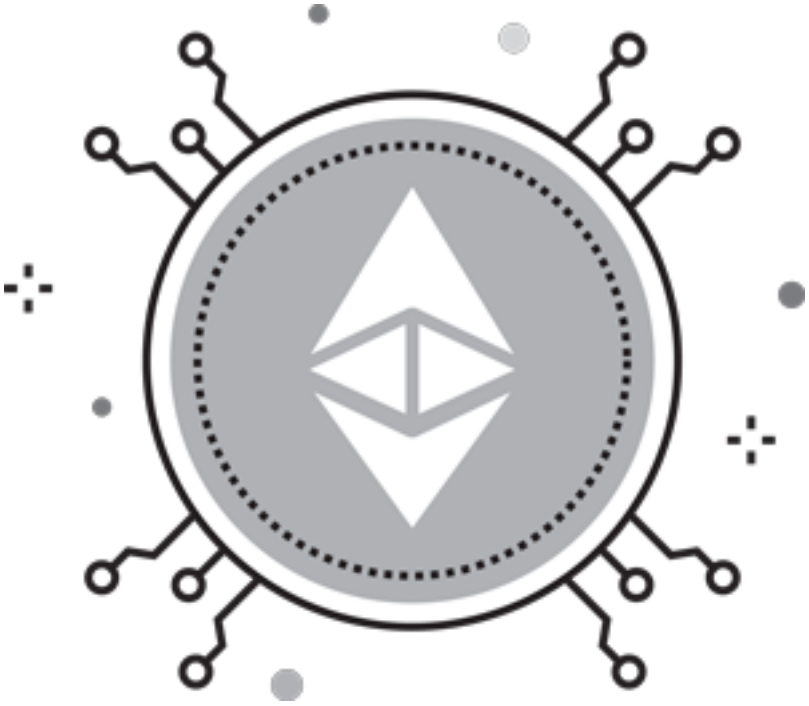
Потом все резко заговорили про какие-то айсио (ICO) – тут вообще черт ногу сломит: люди собирают криптовалюту, пишут какие-то вайтпейперы, издают свои токены – что это? Зачем? Почему их так много? В начале семнадцатого года ICO проходили одно в неделю, в конце уже по 10 штук в день. Потом Китай их запретил, а японцы разрешили. А потом, вроде, наоборот. Но где же деньги, Зин?



Лукашенко в конце года вообще отмочил: отныне в Белоруссии криптовалюты абсолютно легальны, и бизнес, с ними связанный, приветствуется и крышуется самим Батькой. Набиуллина вздрогнула.

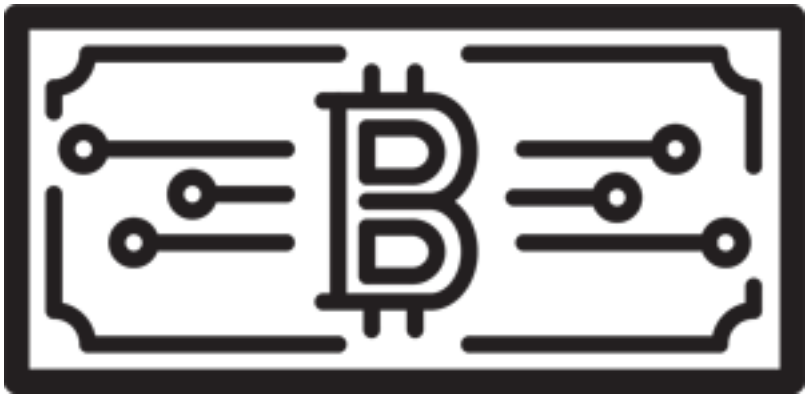
Короче говоря, событий было много. Сначала фейсбучным братьям Винклвоссам не дали создать биржевой фонд биткоинов – американский регулятор сказал, что это бяка, нельзя. Биток от огорчения припал, но быстро восстановился. В апреле японцы внезапно разрешили платить биткоином по всей стране – теперь он считается там обычной валютой наравне с йеной. Хотя курсу это не сильно помогло, что странно: это было-таки первое признание крипты на государственном уровне.

В мае-июне выстрелил новый герой крипторынка – эфир, – да так, что чуть не обогнал биткоин по капитализации. В конце лета стало понятно, что биток завоевывает мировую популярность, но все еще полон подвохов: то он разделялся на части (точнее будет сказать, отпочковывал от себя некий «биткоин-кэш» и прочие мерзкие порождения дьявола), то вдруг всем стало понятно, что транзакции очень дороги, да еще и дико тормозят. Но курс неумолимо продолжал расти.



В сентябре очередной удар по крипте нанес Китай, запретив проводить ICO и торговать цифровалютами у себя на территории. Курс биткоина упал чуть ли не в два раза за несколько дней. Но в декабре произошло чудо, хотя и давно ожидаемое: американские биржи начали торговать фьючерсами на биткоин. Теперь даже умудренные сединами банкиры могут вложиться в биток. Хотя мы догадываемся, что они-то как раз вложиться уже успели – через многочисленные венчурные криптовалютные фонды, которые тоже в этом году цвели и пахли.

Похоже, что криптовалюты вообще и биткоин в частности становятся неотъемлемой частью мировой финансовой системы, а значит, пора и вам узнать о нем все необходимое. Мы тут как раз для этого.



Истории успеха

Некто Кристофер Кох из Норвегии вложил 150 крон (примерно 27 американских баксов), купив 5000 биткоинов в 2009 году. Он писал диплом по шифрованию и, понятное дело, наткнулся на эту технологию в самом зародыше. Столь значительную покупку трудно было забыть, но он смог. К счастью для себя. Вспомнил он о ней только в начале 2013 года. Пароль свой он-таки подобрал и продал первую тысчонку биточков, приобретя замечательную квартиру в центре Осло. Сейчас у него все хорошо.

Другой норвежец по имени Кристофер Хансен, айтишник из Тронхейма, продал все свои сраные акции[1] и закупился битком в середине 2017 года по $2800. Все сбережения конвертнул, до последней кроны. «Я пошел ва-банк», – пишет смельчак. Ну, упятерился за полгода, про него даже в газете написали. Не знаем, зафиксировал ли профит. Может, уже и повесился после падения.

Но были и более крупные ребята, которые нажились так, что глаза на лоб лезут. Два братца-акробатца Винклвосса, про которых все узнали из увлекательного фильма про Цукерберга, оказывается, вложили в биток 11 миллионов долларов – еще в 2013 году[2]. Новость вышла 3 декабря, когда вложение этих мурзилок из илитных американских универов превратилось в миллиард долларов. Самое забавное, что спустя лишь 2 недели, их вложение стоило уже 2 миллиарда долларов; а еще через месяц – обратно миллиард. Forbes подсчитал[3], что средний криптомиллиардер (которому 42 года) заметно моложе обычного, гетеросексуального миллиардера – тому сейчас 67 лет. Ну как тут не заволноваться? Мы тут, понимаешь, использованные чайные пакетики боимся выбрасывать, а они там в своей Омерике вона чо.

Но, оказывается, не только в Омерике все хорошо, но и в славном Сент-Китсе и Невисе. Сам наш Паша Дуров (тамошний гражданин) знатно обогатился на биточке[4]. Вложил он в 2013 году 1.5 миллиона долларов и в конце 2017 его 2000 монет стоили почти $40 лямов.

Что тут хулиномически архиважно, так это размер их вложений. Если зеленоплющелиговые Винклвоссы получили от Цукерберга 65 миллионов долларов, то, выходит, в биток они вложили 1/6 своего состояния. Ну ладно, мы не знаем про их состояние *до* получения отступ-

[1] https://news.bitcoin.com/scandinavian-investor-pivots-sells- all-shares-and-buys-bitcoin/

[2] https://lenta.ru/news/2017/12/03/billionaires

[3] https://www.forbes.com/richest-in-cryptocurrency

[4] http://www.forbes.ru/milliardery/354251-cifrovoe-zoloto-pavel-durov-zarabotal-na-bitkoinah-bolshe-30-mln

ных, но в стародавние времена студенты вложили в Фейсбук, кажется, ровно миллион – наверное уж, не все свои деньги. Ну пусть не 1/6, а 1/10 ушла в крипту.

ТО ЕСТЬ РЕБЯТА СЕРЬЕЗНО РИСКНУЛИ – КАК, КСТАТИ, И В СЛУЧАЕ С ФЕЙСБУКОМ – И КРУТО ЗАРАБОТАЛИ. А МОГЛИ И ПОТЕРЯТЬ.

В случае же с Дуровым ситуация совсем иная. Павел, обладая капиталом в полмиллиарда долларов (сейчас уже под миллиард, слава «Телеграму»), вложил в биток всего полторашечку – 0,3 % от своего капитала. Тут не надо обладать никаким даром визионария, чтобы понять: его новый блестящий сорокет – это просто удачный эксперимент. Это для него было все равно, что нам купить на базаре серебряный николаевский рубль – в качестве инвестиций в антиквариат, – а тот бы оказался дико редким и стал бы стоить не 100 долларов, а 10 тысяч. Даже для наших скромных читателей, большинство из которых обладает в лучшем случае небольшой квартирой, это не показательно и жизнь, увы, не изменит.

«Уолл-Стрит Джорнал» сообщает[5], что венчурный фонд Founders Fund, который основал миллиардер Питер Тиль в далеком 2005 году, вложил чуть ли не 20 миллионов долларов в биточек. Вложения уже выросли до сотен миллионов, хотя когда именно они закупились, издание умалчивает; вообще фонд Питера немногословен. Хотя один из их криптофондов был запущен совсем недавно – в середине 2017 года. Также неизвестно, фиксили они профит или нет. Самое забавное, что сама по себе заметка столь уважаемого в буржуазных кругах журнала вызвала некоторую эйфорию среди покупцов, и биток в очередной раз взлетел на 100–200 миллионов процентов. Не, ну а чо, Питер не ошибается.

ОН ДАЖЕ КОГДА-ТО СТИПЕНДИЮ ДЛЯ ГЕНИАЛЬНЫХ СТУДЕНТОВ ОСНОВАЛ. ЧТОБ ЕЕ ПОЛУЧИТЬ, НАДО БРОСИТЬ ИНСТИТУТ. КРУТО, А?

[5] https://www.wsj.com/articles/peter-thiels-founders-fund-makes-big-bet-on-bitcoin-1514917433

Чему же нам надо поучиться у этих олигархов? Естественно, распределению активов по классам. Есть кое-где один популярный канал, где чел инвестирует 52 биткоина по разным криптоактивам и полагает, что его «инвестиционные» действия имеют какой-то волшебный эффект. Товарищи, если у вас два года назад появилось 52 биткоина, не имеет значения, вложили вы их куда-то или нет: они выросли в *пятьдесят*, сука, раз! Ну ок, вы там разложили их по разным эфирам, зекам и риплам и умножили ваши 20 тысяч не в 50 раз, а в 52 раза. Ну охуеть теперь! Просто надо понять, что криптовалюта уже успела стать отдельным классом активов и немного странно его не использовать в своем портфеле. Если он у вас, конечно, есть.

Истории провала

Первый «официальный» фейл, он же и самый знаменитый – покупка пиццы за битки в мае 2010 года. Некто Лазло Хейнич предложил 10 тыщ биткоинов за 2 больших пиццы стоимостью 42 бакса. По нынешним меркам это примерно 100 миллионов долларов. Сука, дорого. С другой стороны, нынче и пицца уже не та.

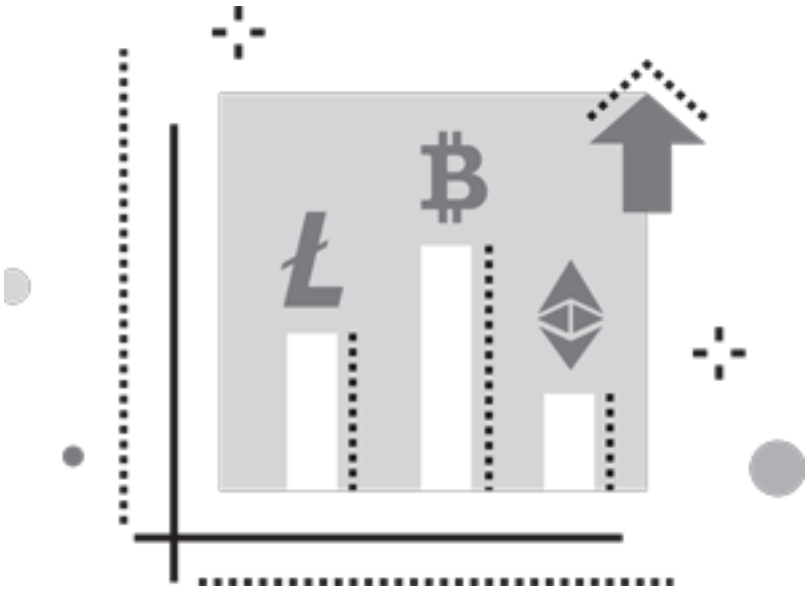
Самое забавное, что многие будущие какбе-миллионеры не получили даже и пиццы. Около четверти всех биткоинов утеряно. Слито. Проебано. Спизжено. Навсегда. Безвозвратно. Ха-ха-ха!

Сноб.ру опубликовал[6] целую серию откровений, читать их одно удовольствие. Один неудачник купил в 2011 году 70 битков, потому что увлекался киберпанком, – вложил 100 баксов. Хранил биточки он на старом ноуте, а тот, понятное дело, издох. Ну он его и выкинул на помоечку. Вспомнил товарищ про крипту только в 2013 году, когда курс перерос $1000. Чуваку так поплохело, что он до сих пор не ест и не пьет. Шутка ли – миллион долларов на новую прекрасную жизнь отправились в помойку. Не можем не процитировать героя: «*Если бы монеты удалось сохранить, я бы сделал ремонт у родителей, купил бы автомобиль, квартиру, путешествовал бы. Своей неудачей я навсегда обрек себя работать за гроши, пока счастливчики будут прожигать свою жизнь*». Аминь.

[6] https://snob.ru/selected/entry/131898

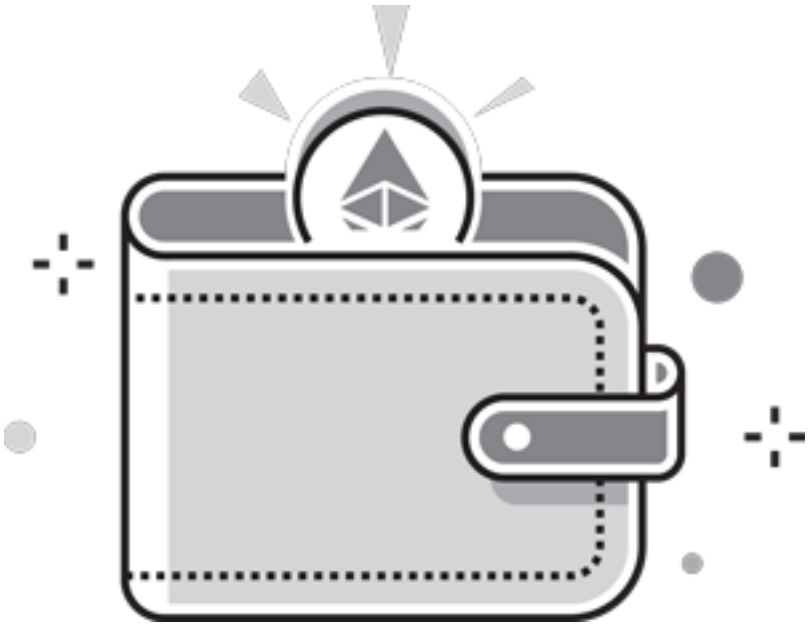
Второй счастливчик закупился битками в 2013-м году – купил аж 18 монет. Он терпеливо ждал, пока они превратятся в заветный миллион – и действительно, курс рос как на дрожжах. Он не спекулировал, не нервничал, не принимал поспешных решений. Но хранил он биткоины на знаменитой японской бирже Mt. Gox, которая в те времена была самой большой в мире – с огромным отрывом от преследователей. В феврале 2014-го биржа наебнулась и все его биточки сгинули. Основателя до сих пор судят: хотя тот заявлял про ужасных хакеров, расследование показало, что деньги с биржи выводились несколько лет, а в 2014 на счетах клиентов уже ничего и не было. Тем временем этот Марк Карпелес, руководитель и главный подозреваемый в крахе Mt. Gox, прославился тем, что всю дорогу жил в жырнейшем пентхаусе в центре Токио, упиваясь саке и гейшами.

В июле 2017-го взломали еще одну большую биржу, на этот раз южнокорейскую – BitHumb, умыкнув больше миллиона долларов. Ну, с Mt. Gox не сравнить – там было своровано чуть ли не 500 миллионов долларов (это на тот момент – на февраль 2018 это около миллиарда долларов). На BitHumb было забавное продолжение – с биржи слили еще и личные данные ее пользователей, и кто-то повелся на развод от «ее сотрудников», которые хитростью выманивали пароли и уводили оставшиеся деньги на свои кошельки.



КОМЕДИЯ ПРОСТО. У ВАС ПРОПАЛИ ДЕНЬГИ, СКАЖИТЕ НАМ СВОЙ ПАРОЛЬ, И МЫ ВАМ ИХ ВЕРНЕМ.

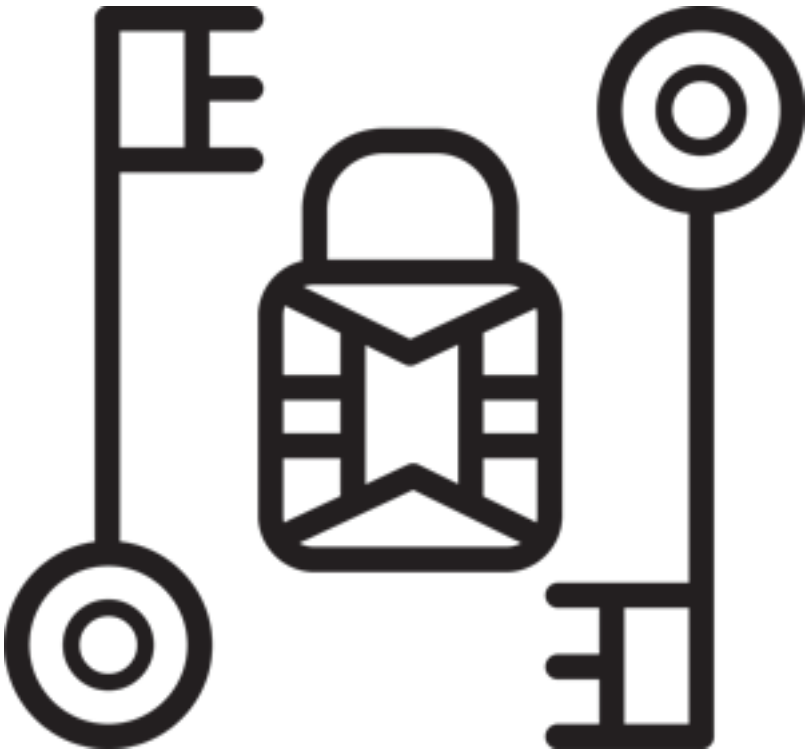
Но зачем такие сложности? Самая уморительная история развода – это, конечно, ICO израильского (а может быть, даже еврейского – как посмотреть) стартапа CoinDash. Номер кошелька для сбора «инвестиций» был подло подменен прямо на сайте компании. Действительно, зачем взламывать какие-то биржи, когда можно ломануть хостинг и просто подставить свой адрес для сбора средств? Злодеи успели собрать 7,5 миллионов долларов, ну а потом горе-стартаперы встрепенулись и поняли, что что-то не то. Хотя они уверяли, что все равно будут дальше развивать проект. Ну, бог им судья: кошельки-то все анонимные, и кто на самом деле подменил номер кошелька, мы никогда не узнаем. Хотя история эта еще не закончилась: хакер сначала вернул им 10 тыщ эфиров, потом еще 10. Номер кошелька-то у всех на виду! То ли он им так выдает вознаграждение за их труды, то ли это реально один из них… Загадка. Но факт в том, что потратить денежки ему будет сложно – все же следят, куда уходит спизженный эфир.



Немало доставила и история NiceHash. Это майнинговый пул – площадка, на которой отдельные пользователи собираются для совместной добычи криптовалют. Добытые валюты выплачиваются не мгновенно, а порциями, плюс там продается свободная мощность. И в один прекрасный момент (как раз после очередного взлета курса) невыплаченных и вложенных осталось чуть ли не 5 тысяч биткоинов – это больше 60 миллионов долларов. Надо сказать, что на подобных (да на всех облачных) сервисах деньги каждого пользователя хранятся на общем кошельке, а распределяет их система биллинга. Оно бы, конечно, и ничего, просто, видимо, кто-то посчитал, что «традиционным» способом, взимая небольшую комиссию с каждого юзера, 60 лямов набирать будет слишком долго. И проклятые «хакеры» вдруг взломали площадку. Сайт прекратил работу на несколько дней, но потом восстановился и даже объявил награду за поимку злодеев.

НУ-НУ. ЗА ЯЙЦА СЕБЯ УКУСИТЕ – МОЖЕТ, ПОЛЕГЧАЕТ.

А первое место в списке адских криптофейлов получает некто Джеймс Хауэллс из старого доброго Уэльса. Парень по забывчивости отправил на помойку жесткий диск, на котором хранился ключ к его кошельку. Так 7500 биткоинов оказались на свалке, хотя сам Джеймс навсегда вошел в историю.



Но это, в общем, понятная херня: кому-то не везет, кто-то пароль забыл, некоторые – тупые. Но, бывает, люди просто промахиваются по кнопкам. Недавно (прямо у всех на глазах!) на аукционе майнинговых мощностей Hashing24 кто-то поставил бид на 2800 гигахэшей в 0,83 биткоина. Беда в том, что он забыл один нолик – хотел-то поставить 0,083. Так вместо $1400 за контракт человек заплатил $14 тысяч (по тогдашнему курсу). Такая криптономика, братцы. Хулиматика.

Кто-то считает, что появление биткоина по значимости сравнимо с появлением Интернета. Кто-то говорит, что это очередной ммм-пузырь.

В основной части книги 5 глав:

1. Теория: шо за блохчейн такой?

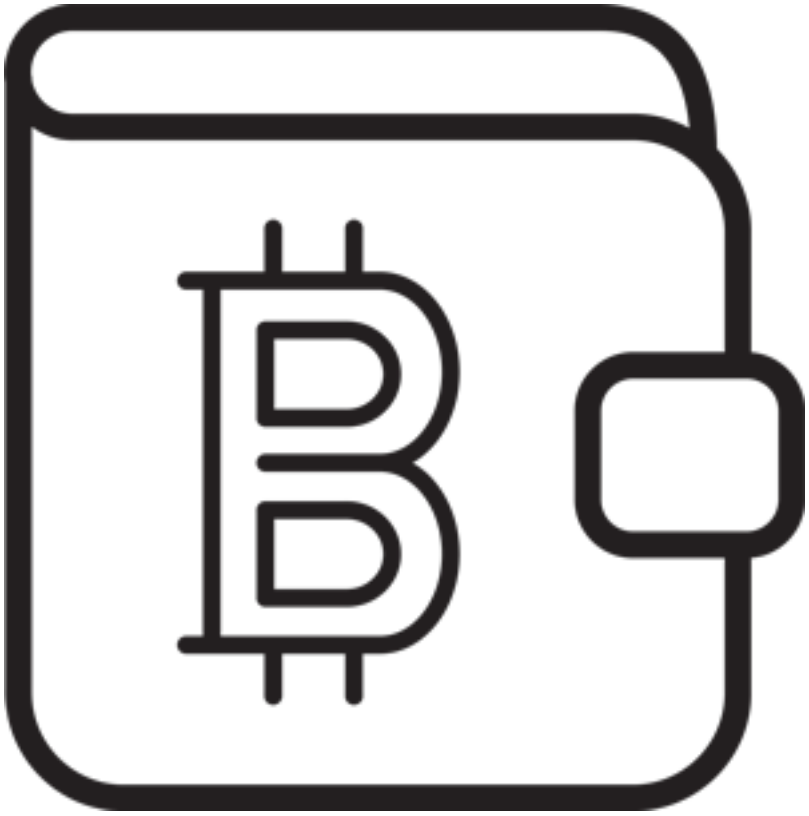
Сначала расскажем про саму технологию: как устроен блокчейн, что в нем хорошего и – вы удивитесь! – что плохого, для чего он пригодится, а для чего бесполезен.

2. Проекты на блокчейне: биткоин и все остальное

Во второй главе мы подробно рассмотрим биткоины, потом самые известные альтернативные монеты, прикладные возможности и перспективы блокчейна как глобальной технологии.

3. Инфраструктура: где купить и как хранить?

Кошельки, криптобиржи, обменники, информационные сайты и Телеграм-каналы – вся обслуживающая система для спекулянтов и криптокомьюнити. Как купить крипту и куда ее девать? Как сохранить? Где основные подвохи?



4. ICO: как появляются проекты на блокчейне

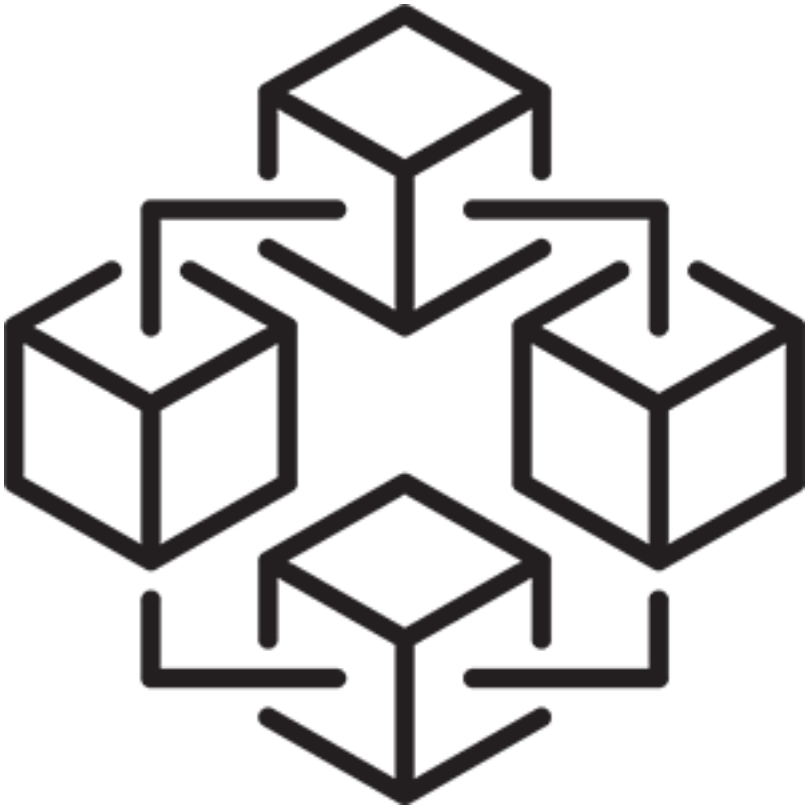
Четвертая глава – про ICO, самую хитроумную и весьма прибыльную в прошлом тему в крипте. Как появляются новые криптовалюты? Какими приемами пользуются аферисты? Как не прогореть, вложившись в новый проект?

5. Криптостратегия: чо делать-то?

В пятой главе мы ответим на созревшие у молодых спекулянтов вопросы: как торговать криптой, да и надо ли вообще?

Глава 1
Теория: шо за блохчейн такой

1.1. Что нового и что особенного в этом вашем блокчейне
1.2. Зачем оно вообще надо
1.3. Как это работает
1.4. Почему это работает плохо
1.5. Все равно все спиздят хакеры и бандиты



1.1
Что нового и что особенного в этом вашем блокчейне

Про блокчейн вы узнали, конечно, благодаря биткоину – новой чудесной цифровой валюте, которая показала небывалый рост за прошедшие три года и сразу всем очень понадобилась. Первое, что нужно понять – блокчейн может содержать не только записи о том, сколько у кого денег (например, биткоинов), а вообще любую информацию: списки, файлы, документы и даже программы.

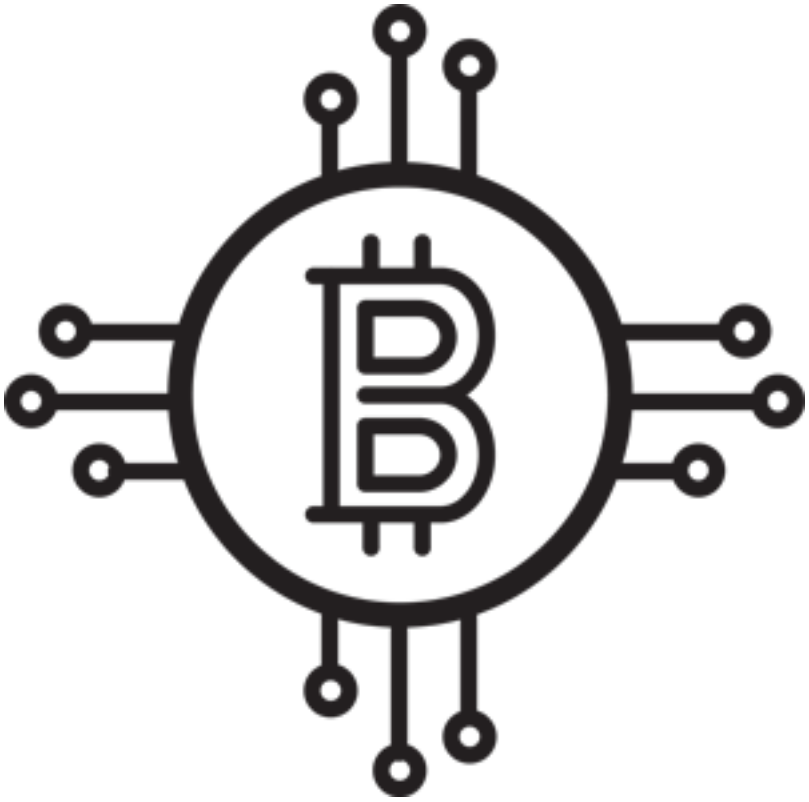
Мир держится на контрактах, сделках и записях о них. Это важная часть современной экономической и бюрократической машины. Они защищают наши активы и устанавливают барьеры для злоумышленников. Они идентифицируют участников процессов и управляют взаимодействием между странами, организациями, компаниями и простыми людьми.

Блокчейн справляется с этими задачами гораздо лучше, чем все, придуманное человечеством ранее. Это открытый распределенный журнал, который записывает операции между участниками эффективно, проверяемо и без сбоев. При этом журнал этот может быть запрограммирован на нужные нам автоматические действия. Например, он может высылать 30 серебренников каждый раз, когда с какого-то адреса поступает полезная информация. Но начнем с более простых вещей.

Как мы понимаем, что курс рубля к доллару рухнул? Особенно, если телевизор талдычит об обратном? Вроде понятно: есть обменники, есть публичные курсы, которые всем видны. Или возьмем что-нибудь более интригующее: например, депутат обосрался на Красной площади. Если вокруг него было несколько тысяч человек, никакой телевизор не заставит их думать, что депутата там не было.

ВСЕ ЭТО ВИДЕЛИ, А ЕСЛИ И НЕ ПОВЕРИЛИ СВОИМ ГЛАЗАМ – ВСЕГДА МОГУТ ДРУГ У ДРУГА ПЕРЕСПРОСИТЬ И УДОСТОВЕРИТЬСЯ.

В блокчейне так все примерно и устроено: каждый видит происходящее и никто не может подменить правду, потому что она у всех одинаковая, а все ходы записаны. При этом нет необходимости обращаться к какому-то местному царьку для проверки: все сделано таким образом, что все друг другу доверяют благодаря технологии, которая, к тому же, открыта – то есть все видят, как она устроена.



Технически это выглядит следующим образом. Вместо того, чтобы записывать всю информацию в одно место, которому все вынуждены доверять (например, в банк, чтобы понять, у кого сколько бабла), информация записывается в цепочку блоков, тот самый **блокчейн**. Каждый блок содержит в себе кусочек предыдущего, поэтому какой-то старый блок нельзя взять и подменить – это сразу же станет известно, ведь цепочка, идущая дальше, просто перестанет подходить. Все это хозяйство хранится не на одном, а на тысяче компьютеров одновременно, фактически у любого желающего. И любой желающий может получить к ней доступ. Когда происходят какие-то изменения (см. депутат обосрался), информация об этом записывается в новый блок и разлетается на каждый компьютер – «ноду» или узел сети. Таким образом наступает всеобщее благоденствие и непорочность.

ПРАВДА, ЦЕНОЙ ИЗБЫТОЧНОГО ХРАНЕНИЯ КОНСКОГО КОЛИЧЕСТВА ИНФОРМАЦИИ И ТАКОГО ЖЕ КОНСКОГО КОЛИЧЕСТВА ИЗБЫТОЧНЫХ ОПЕРАЦИЙ, НО ОБ ЭТОМ ПОЗЖЕ.

Если говорить еще более формально, принципы работы такие:

1) Блокчейн – это распределенная база данных. Правила доступа, хранения и добавления новой информации в блокчейн устанавливаются участниками и полностью открыты.

2) Все, что происходит в децентрализованном блокчейне, происходит между его участниками и непосредственно друг с другом.

3) Степень раскрытия личности участника устанавливается правилами сети. В 95 % блокчейнов (например, в блокчейне биткоина) у вас есть только адрес[7], без имени и фамилии. Можно этот адрес раскрыть соседям, а можно никому не показывать. Все сделки проходят между этими адресами.

4) Вернуть и исправить ничего нельзя. Как только операция записана в базу, удалить ее невозможно – все уже о ней узнали и запомнили. Записи связаны друг с другом, рассортированы хронологически и постоянно видны всем. Блоки соединены в цепочку и для изменения любого из них требуется изменить вообще все, а это не по силам даже Эрнсту или Чурову.

[7] Например, вот такой – 1EkaseA9wJmPxFLaBtSfuqAPRaaHRLStZB.

Получается, что блокчейн – это, прежде всего, новый формат *доверия*, для которого не нужны посредники и авторитеты.

1.2
Зачем оно вообще надо

Итак, блокчейн – это криптографически защищенный распределенный реестр. Он оберегает нас от того, чтобы кто-то незаметно не продублировал свою запись о наличии чего-либо, при этом не надо доверять никакому специальному регулятору – все и так верят всем. Поэтому и записать в блокчейн можно все, что вообще можно записать списком. Логичное приложение – регистрировать собственность на землю, наличие диплома[8] или рецепта[9] на лекарство. Некоторые из этих идей – гениальные (без шуток). Удобно же зарегистрировать сделку по квартире не за 10 дней, а за 10 минут; вроде как в Грузии оно уже так и работает. Или в аптеке проверить наличие у человека рецепта, ткнув в базу, – при этом человек точно знает, что никакой регулятор не сможет у него этот рецепт отобрать и бумажку с ним он не потеряет. А фармацевт точно знает, что рецепт не поддельный – он видит, кто его выдал. Работодатель может автоматически проверить резюме на наличие какого-то сертификата или диплома, и будет уверен, что они настоящие.

Или представьте, что вы покупаете песню непосредственно у ее создателя. Посредников нет, комиссия минимальна, он сразу получает ваши деньги, а вы автоматически получаете права на нее. Все всегда могут проверить, что такой-то адрес у такого-то музыканта эту песню купил и может ее слушать. Или смотреть фильм. Или читать книгу. Не нужен никакой Михалков со своим РАО, чудо-то какое! Все и так без него знают, что кому принадлежит и сколько кому причитается. Более того, не только сколько причитается, а оно уже и перечислено

[8] http://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017

[9] http://www.healthcareitnews.com/news/next-big-thing-pharmacy-supply-chain-blockchain

и уплочено, и все довольны – композитор, автор текста, продюсер. Кроме издателей, которые стали не нужны.

Правительства и регуляторы могут снять с себя функции регистрации и проверки чего бы то ни было. При этом уровень анонимности можно менять по консенсусу сторон. Все сделки проходят очень быстро и нет никакой системы Visa или MasterCard: марокканец покупает фильм у бразильца напрямую, минуя таможню и банки!

И ОТОБРАТЬ ЕГО ТОЖЕ НИКТО НЕ МОЖЕТ. ПРОСТО СКАЗКА.

Внезапно для удостоверения документов не требуется нотариус, да и вообще какие-либо государственные учреждения. Голосовать можно на дому, и всегда можно проверить, кому достался твой голос – он зачислится «на счет» твоему кандидату, и директор какой-то дагестанской школы не сможет спиздить голос простого пастуха после подсчета.

Так со всем: патенты, разрешения, браки и разводы, паспорта, доверенности – без подвохов, подделок и черных риэлторов. По поликлиникам не надо будет таскать свою карту! Дал пароль нужному врачу – он сразу видит не то что твою историю болезни, а еще и какой-нибудь геном впридачу – в любой больничке любого Таиланда!

Благотворительность тоже выйдет на новый уровень. Можно же сделать так, чтобы никто не видел жертвователей – а настоящая благотворительность всегда анонимна, – зато вот жертвователи всегда знали бы, куда уходят деньги со спонсорского счета, на какие операции расходуются и кто их получает.

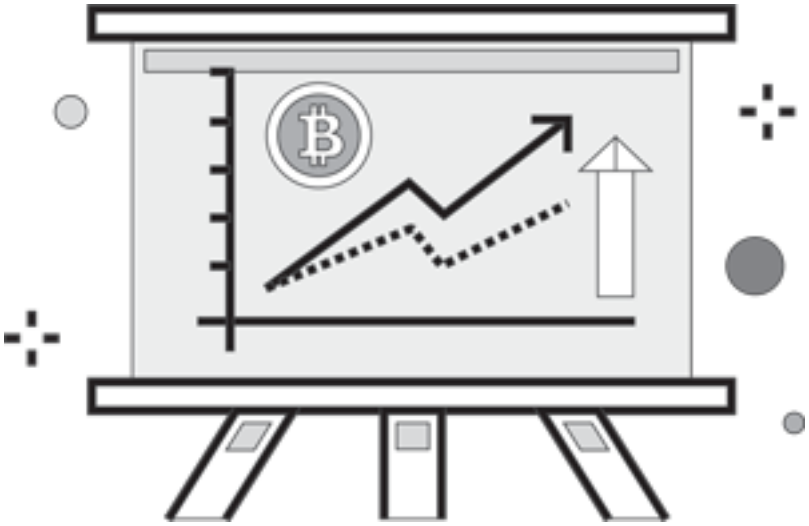
Можно и еще хитрее: если вы своему ребенку обещали подарить миллион на свадьбу, это можно записать в смарт-контракт с доступом к вашему счету. Как только контракт видит, что у сына зарегистрирован брак, он переводит ему деньги напрямую, а вы сами, может быть, уже даже и померли, не дождавшись этого счастливого момента (речь о переводе денег, конечно).

ДЛЯ ЭТОГО НЕ НУЖЕН БАНКИР, ЗАГС, НОТАРИУС И ЗАВЕЩАНИЕ. НЕ НУЖНО НИЧЕГО ЖДАТЬ ИЛИ ПРОВЕРЯТЬ. ВСЕ СРАБОТАЕТ САМО.

Хотя некоторые идеи криптоноваторов – абсолютно бредовые (без шуток). Нужен ли блокчейн, чтобы завести какую-то новую энциклопедию[10] на блокчейне или читать платные новости, которые – ничего себе! – нельзя исправить задним числом[11]? Вы часто перечитываете прошлогодние новости? Из-за бешеного притока инвестиций в эту отрасль люди пробуют совершенно невменяемые идеи на предмет сбора бабла с инвесторов.

[10] https://www.wired.com/story/everipedia-blockchain/

[11] http://www.niemanlab.org/2017/10/



А у инвестора логика простая: биткоин растет, может и еще что-то вырастет? Это совершенно нормальный процесс. Технология молодая и скоро все поймут, для чего она подходит хорошо, а для чего нет. Кому-то, правда, это понимание встанет в копеечку.

1.3
Как это работает

Мы изучили херову тучу объяснений того, как работает блокчейн. Проблемы две: либо эксперт держит читателей за идиотов и объясняет это так примитивно, что суть процесса остается за кадром, либо текст рассчитан на айтишника с деревьями Меркла и схемами Шнорра, и простой человек его уже не воспринимает. Самое лучшее объяснение встретилось нам в блоге «Лаборатория Касперского»[12]. Его мы и взяли за основу, но постарались сделать *еще* понятней.

Сначала изучим несколько основных понятий, первое из которых – цифровая подпись. Зачем нужна обычная подпись? Она удостоверяет того, кто подписал документ. Цифровая в этом плане даже лучше – она делает то же самое, только ее нельзя (точнее, невероятно трудно) подделать. То есть автор документа определяется однозначно, и подписать его мог только он.

> ПРИ ЭТОМ ОДИН ЧЕЛОВЕК (ИЛИ ФИРМА) МОЖЕТ СГЕНЕРИРОВАТЬ НЕСКОЛЬКО ВПОЛНЕ ЗАКОННЫХ ПАР ИМЯ-ПОДПИСЬ – ДЛЯ РАЗНЫХ ЦЕЛЕЙ.

Второй термин, который нам потребуется – это хэширование. С подписью понятно: если мы видим подпись, мы точно знаем, что автор документа (транзакции, программы) – именно тот, кто свою подпись под документом поставил. Но что, если в документе подменили что-то важное? Например, количество отправленных денег (приписали нолик в конце?). Стало быть, крайне важно проверять не только автора документа, но и его целостность и неизменность.

[12] https://www.kaspersky.ru/blog/bitcoin-easy-explanation/12668/

Есть много способов это сделать, начиная с простых, – которые легко обойти. Например, пересчитать все буквы в сообщении и потом проверить это количество. Если цифра не сходится, то сообщение было изменено какими-то злодеями, либо не дошло до нас целиком. Но этот метод легко обходится, если злоумышленник знает, какого рода проверку мы будем применять.

Простейший пример такой антиподделочной проверки находится в бланке ОСАГО об аварии. Там внизу нужно отметить, сколько квадратиков заполнены галочками (типа «я выезжал со стоянки», «я стоял на светофоре»). Это чтоб кто-то после получения подписанной копии не натыкал новых, нужных ему вариантов происшествия. Но криптографическая проверка или, иначе говоря, «хэш», гораздо круче. В нашем (примитивном) варианте при перестановке букв в сообщении контрольная сумма не изменится. А в правильно сделанном хэше при малейшем изменении сразу понятно: это не оригинал. При этом сам «хэш» занимает одну строчку даже для очень больших файлов или документов[13].

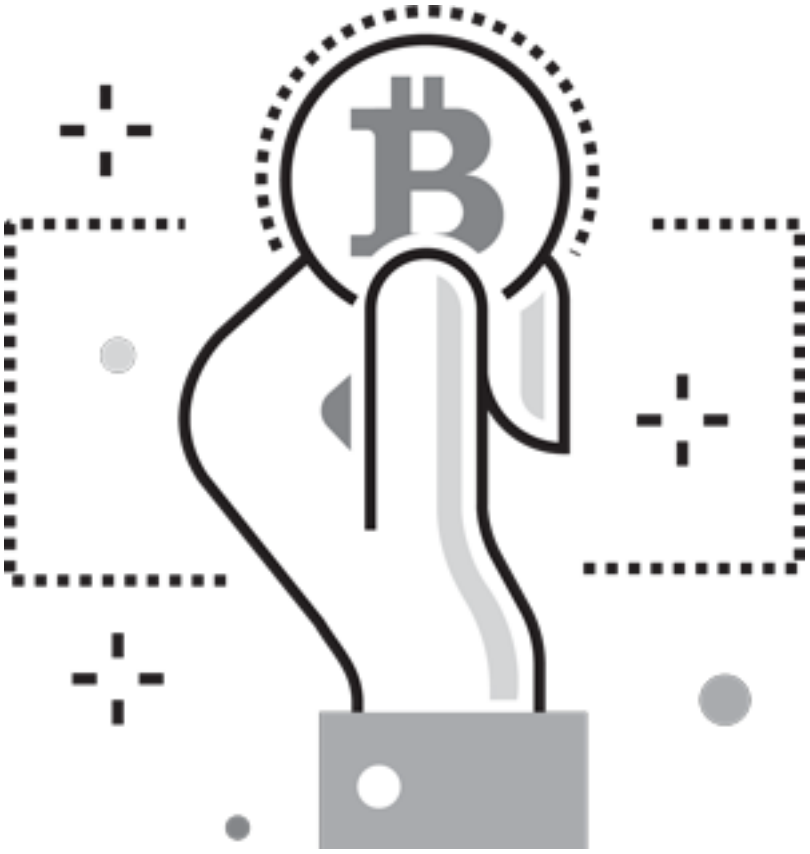
У хэша есть одно очевидное свойство: он односторонний. То есть по хэшу невозможно подобрать изначальное сообщение (только перебором всех вариантов – так и работает майнинг; но об этом позже). Да, у некоторых типов хэшей была такая проблема, что у разных сообщений мог получится одинаковый хэш, но сейчас это либо уже решено, либо не играет особой роли.

[13] Например, на нашем сайте по адресу **криптвоюматика.рф** будет хэш этой книги, и ты, дорогой читатель, всегда можешь проверить, что тебя не наебали и не подсунули какую-то другую, мерзкую книгу про скам-проекты вместо нашей доброй и светлой литературы.

ГЛАВНОЕ, ВЫ ПОНЯЛИ, ЧТО ЭТА ФУНКЦИЯ РАБОТАЕТ ТОЛЬКО В ОДНУ СТОРОНУ.

Теперь к самому блокчейну. Как использовать подписи и хэши? Представим себе одноклассников, которые хотят завести виртуальную валюту. Они ведут запись на школьной доске: сколько у кого было монет и кто кому сколько отправил, ставят подписи для подтверждения сделок, и все эту доску видят. Потом приходит учитель и говорит: «*Вы тут совсем распоясались, поди уже и клей друг другу толкаете втихаря*». Стирает все записи мокрой тряпкой и насаждает веру в светлое будущее.

Ученикам такая херня не нравится. Им нужна своя валюта, и так, чтобы с доски никто не мог ничего стереть. И на одной общей бумажке тоже писать нельзя – тот, у кого она находится, может там наисправлять всего. Поэтому у каждого бумажка будет своя, но у всех одинаковая. На перемене все сверяют записи и добавляют новые – кто кому сколько передал и сколько теперь монет у каждого.



Как понять, хватает ли у Васи денег на передачу Маше? Надо перечитать весь журнал, и станет понятно: вот 10 монет Вася получил от Пети на прошлой неделе, а 40 ему вчера перечислил Олег. После этого сделок не было, поэтому вписываем в журнал новую строчку: «Забрать 50 монет у Васи и добавить 50 монет Маше», – заверяем васиной подписью и дописываем хэш. Да, проверять все – это долго, но у каждого же есть компьютер! Он сразу поймет, если подпись не та или история неправильная.

ИСПОРЧЕННУЮ СДЕЛКУ ОН В ЖУРНАЛ ЗАПИСЫВАТЬ НЕ СТАНЕТ, А ПРОСТО ВЫКИНЕТ КАК ФАЛЬШИВУЮ.

Совокупность сделок на одной странице назовем блоком, допишем в конец хэш всего блока, чтоб не проверять страницу заново (а сверить только хэш) и начнем новую страницу-блок. Цепочка таких блоков – это и есть блокчейн.

Осталось только понять, кто заполняет страницу на перемене, чтобы раздать всем остальным (просто для справки – у биткоина эта «перемена» каждые 10 минут). Для этого все решают задачку по нахождению «красивого» хэша с нулями впереди. Если вы еще помните, что такое хэш, то станет ясно, что задача это не просто трудная, но и абсолютно бессмысленная (ведь для подтверждения подлинности не имеет значения, *как именно* выглядит подпись и красива ли она, а речь именно об этом). Решение требуется лишь для того, чтобы случайно определить победителя. Ведь если блок будет все время оформлять кто-то один, он сможет, например, чьи-то сделки подло не учитывать.

Сложность задачи при этом настолько высока, что решается она только перебором всех вариантов и «хэширования» каждого из них, а перебирают варианты участники одновременно. У кого-то компьютер помощней, ну у того и шансов побольше. Если участников становится слишком много и красивый хэш находится слишком быстро, то новая задачка выбирается потруднее (и наоборот); об этом все договорились заранее.

Все желающие решать эту задачу называются «майнерами», а решение записывается на страницу вместе со всеми операциями. Это делается для того, чтобы в будущем какой-нибудь хитроумный китаец не пришел и не сказал: «*Ребята, вот на самом деле правильный журнал, у меня все подсчитано*», – тогда ему придется предъявить *решения* всех подделанных задачек сразу, а это нереально. Хотя будем честны: если у него под контролем большинство компьютеров в сети – то возможно.

В итоге мы имеем новую крутую систему децентрализованных операций, где все доверяют всем – потому что все всегда могут все проверить.

ИСТОРИЮ СДЕЛОК НЕЛЬЗЯ ПЕРЕПИСАТЬ И ИСПРАВИТЬ ЧТО-ТО ЗАДНИМ ЧИСЛОМ. УЧАСТНИКОВ МОЖЕТ БЫТЬ ОЧЕНЬ МНОГО, И НАДЕЖНОСТЬ СИСТЕМЫ ОТ ЭТОГО ТОЛЬКО ВЫРАСТЕТ.

По подписи нельзя вычислить ее владельца – если только он сам не заявит о ее принадлежности. А если не учитывать траты сил на постоянное дописывание журнала сделок, все еще и бесплатно.

Но есть и занимательные побочные эффекты. Во-первых, становится удобно торговать оружием и давать взятки, потому что схему трудно отследить и прикрыть, никаких саквояжей с меченой колбасой тут нет. Во-вторых, любую сделку невозможно оспорить или отменить – если ты выслал кому-то свою крипту по ошибке, то это навсегда. И в-третьих, вся информация дублируется 100500 раз, что немного перебор. Это только то, что на поверхности.

Разберем поподробнее.

1.4
Почему это работает плохо

Скажем прямо: блокчейн – технология крутая. Но недостатков у нее хватает. Для их исправления в системе и проводятся так называемые *хардфорки* – разветвления или перезагрузки. Поэтому нельзя сказать, что все участники всем всегда довольны. Да, блокчейн решает проблему доверия без единого центра, но пока не очень эффективно. Почему?

1) За счет открытости анонимность не такая уж и анонимная, как кажется. Если все транзакции можно проверить, а вы перевели немного бабла своему дилеру, то он узнает, сколько денег у вас в кошельке и куда вы их деваете. Конечно, для этого ему надо знать, кому принадлежат и другие кошельки, но это тоже со временем решается. При этом он может узнать все не только о прошлых, но и о всех будущих платежах с известного ему кошелька.

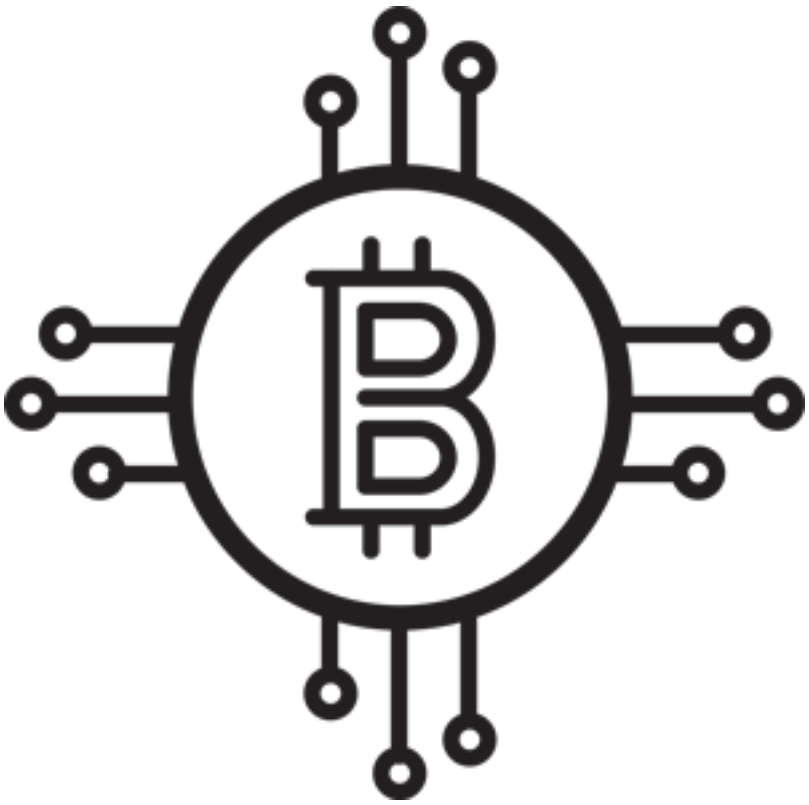
ЕСТЬ ДАЖЕ КОНТОРА, КОТОРАЯ ЭТИМ СПЕЦИАЛЬНО ЗАНИМАЕТСЯ – И СРЕДИ ЕЕ КЛИЕНТОВ, КОНЕЧНО, СПЕЦСЛУЖБЫ И ПРОЧИЕ ПОДОЗРИТЕЛЬНЫЕ ЛИЦА.

2) Децентрализация не так уж велика. Да, копии реестра хранятся в каждом полноценном кошельке, общего сервера нет, поэтому закрыть все сразу нельзя. Но майнеры, обеспечивающие функционирование сети, объединены в пулы. Сейчас для добычи требуется настолько большая вычислительная мощность, что по одному намайнить, например, биткоин просто невозможно. А 70 % всех майнинговых пулов биткойна (по мощности) сейчас находятся в Китае. А там ведь повсюду проклятые коммунисты! Кто знает, что скажет партия? То же самое можно сказать и про другие криптовалюты. Некоторые из них «децентрализованы» только у себя на сайте.

3) Каждый участник сети хранит у себя копию реестра. Изначально так все и задумывалось, в этом весь цимес. Но сейчас получается, что информация дублируется миллионы раз.

Более того, каждый новый участник должен скачать себе историю с подтверждением всех сделок, а она нарастает, как снежный ком: на начало 2018-го для биткоина это 150 гигов. В телефон, например, уже не влезет и на старый комп тоже. И блокчейн продолжит расти. Поэтому многие пользуются «легкими клиентами», которые не скачивают весь блокчейн на компьютер, а только необходимую в данный момент часть. Или, боже упаси, пользуются онлайн-кошельками, то есть доверяют свои ключи кому-то другому.

В РЕЗУЛЬТАТЕ ИСТИННЫХ ХРАНИТЕЛЕЙ ПОЛНОЦЕННОГО УЗЛА ЖИРНЫХ БЛОКЧЕЙНОВ НЕ ТАК УЖ И МНОГО.



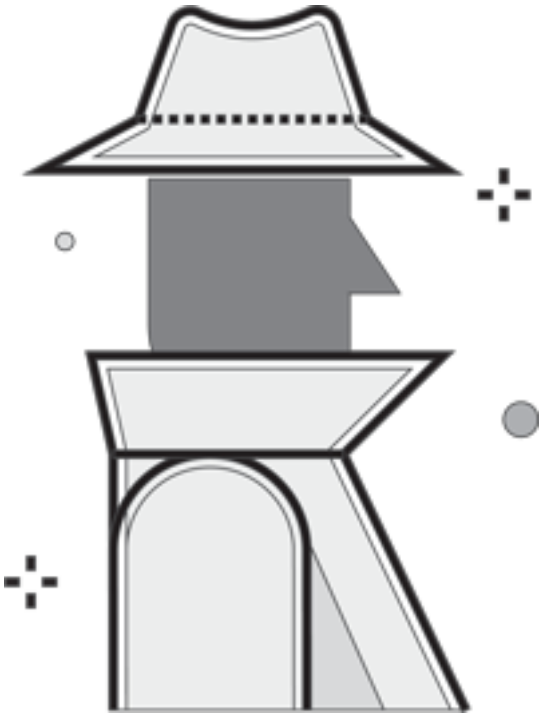
4) Блокчейн по своей сути – довольно медленная технология, а самая первая, что в основе биткоина, – очень медленная. Сейчас в системе проходит примерно 6–7 операций в секунду. Для сравнения – Visa может обрабатывать 24 тысячи операций в секунду. У биткоина на начало 2018-го около 350 тысяч операций в сутки, но очевидно, что близок предел – порядка 600 тысяч в сутки (7 в секунду × 60 с × 60 мин × 24 ч). Подтверждения перевода иногда приходится ждать час-полтора, если сеть перегружена или кто-то «шатает» блокчейн преднамеренно[14] миллионом микротранзакций. Если деньги вам нужны здесь и сейчас, биткоин никуда не годится. Справедливости ради нужно сказать, что новые криптовалюты эту проблему предвидели и заранее подумали о масштабируемости. Тем не менее, проблема существует.

5) Большинство текущих централизованных процессов и реестров не готово к переходу на блокчейн тупо технически – там, где один мощный сервер справлялся неплохо, сотня обычных персональных компьютеров заглохнет в первый же день от объема обрабатываемых данных. К радости различных IT-директоров, мало кто в руководстве корпораций это понимает, поэтому они уже насоздавали себе блокчейн-лабораторий и вовсю пилят бюджеты на блокчейнизацию всего и вся.

[14] Обычно это делает известный криптовалютный инвестор Роджер Вер в рамках рекламной кампании Bitcoin Cash

КАК ИЗВЕСТНО, МАЛО ЧТО СРАВНИТСЯ С ВОЗМОЖНОСТЬЮ ПОТРАТИТЬ ДЕНЬГИ НА БЕСКОНЕЧНЫЙ ПРОЦЕСС НЕПОНЯТНОЙ СТОИМОСТИ.

6) К сожалению, помимо технических и концептуальных ограничений, претворению влажных блокчейн-фантазий в жизнь вовсю мешают те, кому это невыгодно. Те, кому не нужна прозрачность, неподделываемость, неизменность операций и прочие радости честной жизни. Когда ты удачно работаешь посредником не один десяток лет, а потом появляется технология, которая делает тебя ненужным и убивает твой бизнес, мало кому это понравится. Также мало кому понравится, когда больше нельзя подделывать результаты выборов или отбирать у граждан собственность, как раньше. Врагов у новой технологии уже сейчас немало, а будет еще больше. Они просто пока не разобрались, что готовит им светлое технологическое будущее.



Есть и технологические уязвимости, о которых мы, вероятно, еще не знаем. В 2010 году кто-то смог зачислить себе на кошелек 92 миллиарда биткоинов. Потратить не успел: баг нашли, всю систему откатили. Но кто знает, что будет дальше?

Криптовалюты, которые появились после биткоина, стараются предложить какие-то решения перечисленных проблем, но в основе-то все равно лежит блокчейн, и какие-то из его недостатков автоматически достаются всем. Факт остается фактом: на данный момент для привычных вещей, типа, перевести деньги соседу существующие (централизованные) технологии удобнее, дешевле и быстрее. Возьмите хотя бы тиньковские (ну или сберовские) переводы с карты на карту. Что, есть какая-то проблема, что негодяи умудряются потратить деньги с карты два раза? Или биткоины нельзя украсть? Крадут только в путь. Еще вопрос, где держать деньги безопаснее, – в обычном онлайн-банке или на криптобирже.

И БАНКОВСКИЙ СЕРВЕР НЕ ЖРЕТ ТАКОЕ ЦИКЛОПИЧЕСКОЕ КОЛИЧЕСТВО ЭЛЕКТРИЧЕСТВА ДЛЯ ПОДТВЕРЖДЕНИЯ ОПЕРАЦИЙ.

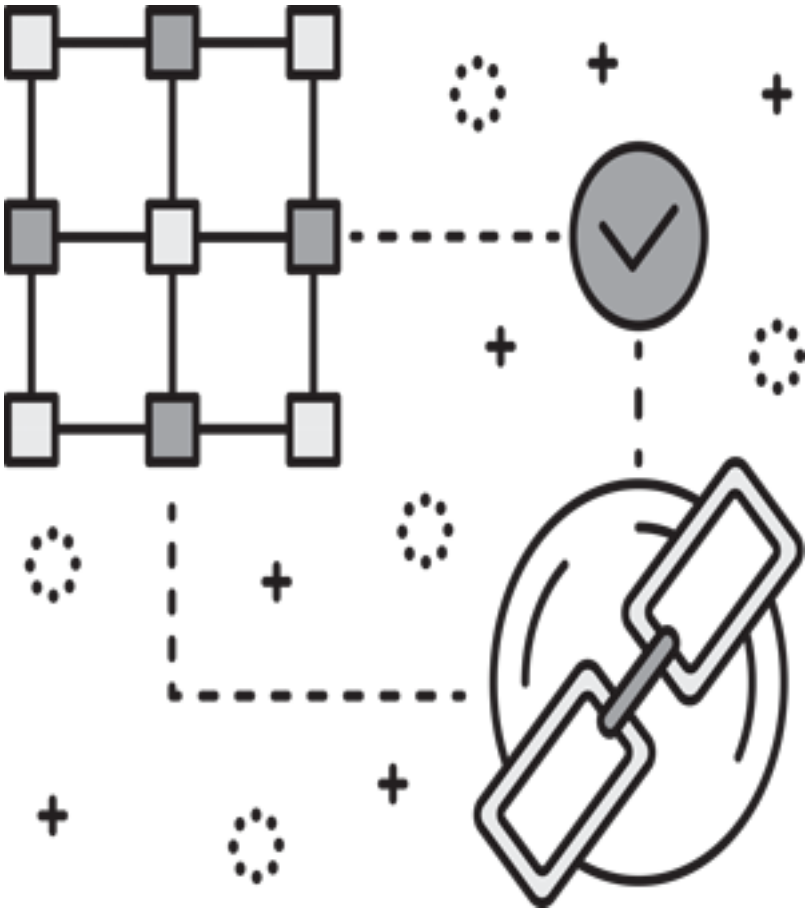
Можете представить себе текущее практическое применение технологии блокчейн чем-то вроде первых попыток приручить дикую лошадь древними людьми. Вот, вроде бы, конь. Кажется, на него даже можно как-то влезть и поскакать. Вот только ездить никто не умеет. А

еще он пока брыкается, покусал всю деревню за жопы и насрал в костер. А еще он жирный и грустный. Но зато конь, да! Конь.

Есть и еще один вполне закономерный нездоровый эффект: те, кто вложился в крипту, волей-неволей начинают ее пропагандировать (как мы этой книжкой). Поэтому мало кто честно рассказывает о недостатках технологии. Кроме нас, конечно. Мы наступили себе на горло и сообщили о потенциальных проблемах. А что дальше делать – решать вам.

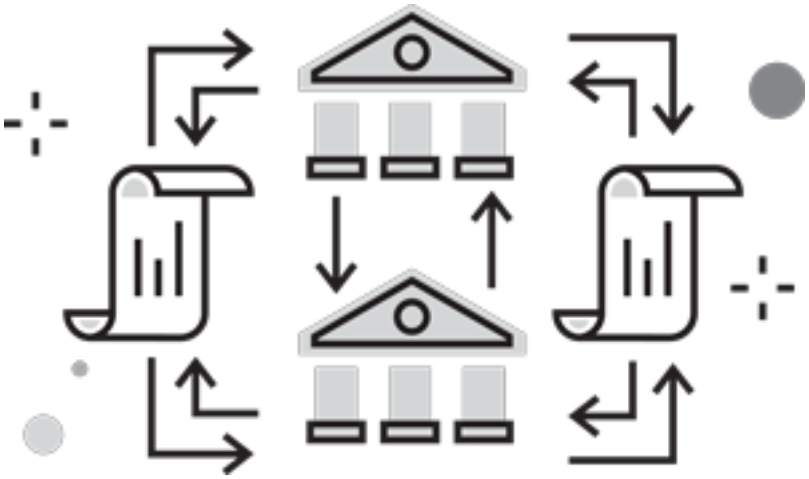
1.5
Все равно все спиздят хакеры и бандиты

Еще одна огромная проблема наступления прекрасного цифрового будущего – новые потенциальные уязвимости и новые ловкачи-преступники, которые будут эти уязвимости эксплуатировать. Хотя, ладно, ловкачи-то по большей части старые, просто жизнь устроена так, что эти паскуды учатся быстрее, чем средняя пенсионерка. И быстрее, чем силы правопорядка. Поэтому, впервые попадая в волшебный мир цифровой собственности, граждане любой страны мира априори меньше преступников понимают, как не проебать сладкие бетховены и какое действие (или какое бездействие) таит в себе наибольшую угрозу.



Не претендуя на создание супермануала по безопасности в блокчейне, тем не менее опишем некоторые ситуации, в которые лучше не попадать. Итак, что плохого может случиться?

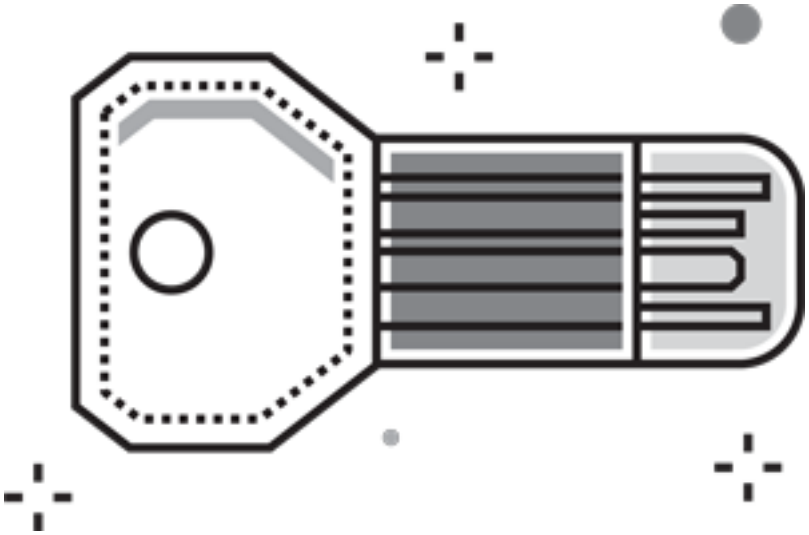
В самом общем смысле, проблема лежит на поверхности, в самой сути технологии: деньги лежат не в банке, где доступ к ним контролируется какими-никакими, но все же людьми, а в виде ключа на бумажке. Или когда доли в стартапах записаны на ваш паспорт не у брокера, а в блокчейне Ethereum, где есть только цифры и несколько букв (не очень много). Все это создает совершенно новые риски: проебать все деньги (вообще все!) можно теперь в результате пожара, скачка напряжения или неловкости племянника, который «случайно» переустановил Windows. Бумажку с фразой для восстановления сожрал кот, а потом блеванул в прихожей. Так или иначе, никакой возможности восстановить ваши цифровые деньги и доли в компаниях нет, вся ответственность возложена исключительно на вас.



ПОЭТОМУ ПЕРВЕЙШИЙ ВРАГ КРИПТОИНВЕСТОРОВ – ИМЕННО ЧЕЛОВЕЧЕСКИЙ ФАКТОР. САМ ВСЕ ПРОСРЕШЬ, ЕСЛИ НЕ БУДЕШЬ ВНИМАТЕЛЕН И ОСТОРОЖЕН.

Окей, пусть куча бэкапов создана, флешка в сейфе, копия на компе, комп в утке, утка в яйце, племянник в Адлере. Возникает обратный эффект: чем больше у вас резервных копий, тем проще их украсть. Только представьте, насколько интересно быть хакером в прекрасном светлом блокчейн-будущем! Раньше вы крали голые фотки знаменитостей, чтобы теребонькать, добавляли компьютеры в ботнеты, чтобы заработать на ddos-атаках, крали кредитные карты, чтобы выслать себе какие-то товары с Ebay, взламывали сайты за деньги конкурентов. Да, заработать своими скиллами взломщика было вполне возможно, хотя и непросто.

Но представьте себе, какие возможности для красивой жизни открываются, если на каждом втором компьютере можно поживиться реальными, анонимными деньгами?! Или долями в блокчейн-компаниях – тоже анонимными? Это же просто праздник какой-то! Поэтому не только мы (инвесторы) ожидаем прихода блокчейна в народ, но и романтики с большой хакерской дороги ждут всех с распростертыми. И вы даже представить себе не можете, на что способны их пытливые умы, и какие дыры оказываются в самом надежном и популярном программном (и аппаратном – недавняя критическая уязвимость абсолютно всех процессоров Intel тому пример) обеспечении. Это первая беда.



Вторая беда не менее серьезна, чем первая: преступления с цифровой собственностью на данный момент непонятно как классифицируются и непонятно как расследуются. Их как бы вообще не существует. Потому что нигде нет таких законов и такой практики, которая бы в достаточной мере описывала товарищу майору эти ваши биткоины. А значит, если в подворотне вам встретилась пара крепких ребят, они вам дали леща, и к вашему удивлению, вместо того, чтобы отобрать мобильный телефон, потребовали перевести всю крипту с вашего в этом мобильном телефоне находящегося крипто-кошелька (а это гораздо ценнее, чем все, что у вас с собой, включая шубу) – значит новая цифровая эпоха наступила и в Бутово. Вашу мобилу даже забирать не будут – зачем создавать состав преступления? Ведь с физическим аппаратом все понятно, а где там какие цифры в Интернете – поди разбери.

ДО СОЗДАНИЯ КИБЕРПОЛИЦИИ ОСТАВАЛОСЬ ЕЩЕ 77 ЛЕТ. СУДЬЯ ДРЕДД, ВОССТАНЬ, ГОПОТА УЗНАЛА О КРИПТЕ!

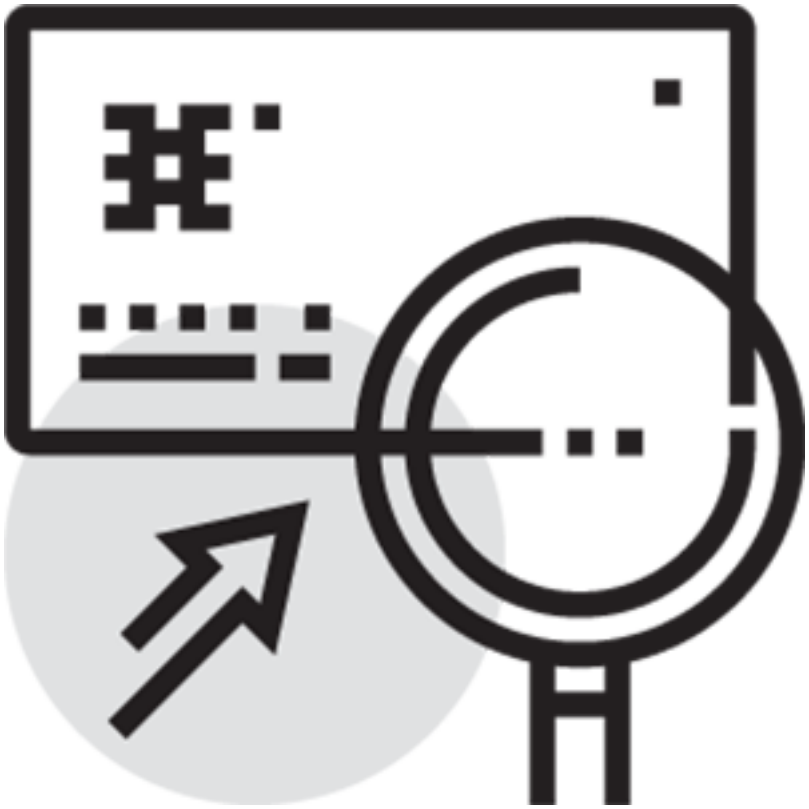
Это не шутки. Граждан грабят, похищают, угрожают и силой заставляют перевести значительные суммы неведомо куда. Процесс этот плохо отслеживаемый, а как вести расследование – непонятно. Добавьте сюда взятки в крипте, оплату наркотиков, оружия и прочих криптовалютных пакостей, и вот криминал уже плотно следует за прогрессом, вбирая самое лучшее. Как всегда и происходит, когда придумывают что-то клевое.

Что же делать, как же быть? Если ты наш криптобратишка или хочешь им стать, для начала будь очень внимателен и осторожен. Поменьше рассказывай о своих богатствах, не стоит вести мощные видеоблоги и вещать со сцены о заработанных миллионах. Помни: чем большую ценность для тебя представляет твоя цифровая собственность, тем более внимательно нужно подойти к ее (и своей) защите!

Базовые советы по компьютерной безопасности очень просты. Заведи несколько резервных копий, и чем дальше друг от друга, тем лучше. Разные города и страны лучше, чем разные комнаты. Все диски и ноутбуки зашифрованы, базовых средств ОС будет достаточно. Для работы с криптовалютой, биржами и кошельками выдели отдельный компьютер или ноутбук. Не скупись, если занимаешься этим всерьез – потери будут больнее, чем поход в компьютерный супермаркет. Занимайся криптой только с этого устройства, поставь платный антивирус с файрволом. Не ходи ни на какие сомнительные сайты, не устанавливай лишние программы – этим всем можно позаниматься с обычного рабочего компа, где Ворд, Эксель, игры, сериалы и порнушка.

ЭТО БАЗОВАЯ МЕРА, КОТОРАЯ ПОМОЖЕТ СОЗДАТЬ НУЖНЫЙ КОНТУР БЕЗОПАСНОСТИ.

Ну и главный совет против хакеров – внимательность. Смотри, на тот ли ты сайт зашел, правильно ли он написан в адресной строке? Скопировал биткоин-адрес где-то и вставил в кошелек, уже приготовился отправлять – проверь, не подменили ли его злоумышленники через буфер обмена? Скачиваешь новую версию кошелька? Проверь, правильный ли сайт, совпадает ли контрольная сумма… ну и так далее.



Базовые советы по физической безопасности тоже несложные. Надо усвоить одну простую концепцию: даже если у тебя в компьютере миллион долларов, взять с тебя в моменте должно быть нечего. Ни поймав тебя на улице, ни вломившись в квартиру: к основным богатствам у тебя у самого не должно быть доступа. Это усложнит разбойную операцию вплоть до полной невыгодности. Заведи себе ключ с подписями «две из трех», одну себе, а две раздай близким родственникам. И предупреди, что это и зачем. И копию ключа у бабушки на даче в сундуке прикопай. Но только одного, чтобы обладание сундуком или бабушкой не дало злоумышленником легкой наживы!

Любой расклад для преступников должен заканчиваться тем, что им придется красть кого-то из родственников и шантажировать тебя как минимум сутки, чтобы получить твои жалкие гроши, потому что один ты ничего перевести не сможешь. Либо выкрасть одновременно и тебя, и сейф взломать на работе. Или в банке ячейку. Короче, делает операцию по отъему денег у населения слишком сложной. А вот жить за городом в неохраняемом (да даже и охраняемом) поселке с кучей наличности и всеми приватными ключами и компом на руках – очень, очень плохая затея. Особенно в светлом криптовалютном будущем.

НО ЧТО ЭТО МЫ ВСЕ О ПЛОХОМ И О ПЛОХОМ? НА БЛОКЧЕЙНЕ СДЕЛАНО МНОЖЕСТВО ЗАМЕЧАТЕЛЬНЫЙ ВЕЩЕЙ. О НИХ – В СЛЕДУЮЩЕЙ ГЛАВЕ.

Глава 2
Проекты на блокчейне: биткоин и все остальное

2.1. Биткоин: откуда он взялся и куда девается
2.2. Монеро, дэш, зкэш, рипл и другие финансы
2.3. Платформы: эфир, вейвс, кутум
2.4. Айдентити и авторские права
2.5. Децентрализация использования ресурсов

Авторы книги не ставят себе задачу сделать обзор абсолютно всех проектов на блокчейне или структурировать их тем или иным образом. В первую очередь, потому, что варианты реального применения развиваются слишком стремительно. Кроме того, таких обзоров хватает. Главное, чего мы хотим, – чтобы вы увидели несколько ярких примеров того, как работает блокчейн. Учитывая уровень нынешних «конференций» и «крипто-митапов», после прочтения этой главы вы сможете выступать на них в качестве эксперта.

2.1
Биткоин: откуда он взялся и куда девается

Биткоин – первая цифровая валюта на основе блокчейна. Изначально она хранилась в кошельках, которые как раз и содержали в себе весь блокчейн, но потом появились легкие кошельки, которые хранят только часть блокчейна и ваши приватные данные, а также онлайн-кошельки, которые хранят и ваши приватные данные в том числе, вы им как-бы полностью доверяете[15]. Самое главное отличие биткоина от, скажем, Яндекс-Денег или Вебмани – никто не контролирует их эмиссию, а информация о переводах не хранится в каком-либо конкретном учреждении.

Для осуществления перевода вам не нужен центробанк и вообще кто бы то ни было – вы просто отправляете криптовалюту на адрес получателя, без посредников типа Visa, Webmoney или PayPal. В любой момент любой человек может проверить каждую сделку, потому что все они записаны в блокчейн, соответственно, подделать информацию нельзя.

[15] Наиболее надежно выбрать себе кошелек можно, как это ни странно, на официальном сайте Bitcoin Core – https://bitcoin.org/ru/choose-your-wallet.

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.