

Андрей Остальский

# НОВАЯ ИСТОРИЯ ДЕНЕГ



*От появления  
до криптовалют*

ТАЙНАЯ СТОРОНА

Тайная сторона (Феникс)

Андрей Остальский

**Новая история денег. От  
появления до криптовалют**

«Феникс»

2023

УДК 821.161.1-34  
ББК 84(2=411.2)6

**Остальский А. В.**

Новая история денег. От появления до криптовалют /  
А. В. Остальский — «Феникс», 2023 — (Тайная сторона  
(Феникс))

ISBN 978-5-222-40755-4

Возможно, самый захватывающий триллер «всех времен и народов» – история денег, универсального средства обмена между людьми – в живом и порой парадоксальном изложении Андрея Остальско-го (р. 1955), известного журналиста, главного редактора (2001–2009) Русской службы Би-би-си. Написанная увлекательно и популярно, книга читается легко, будет интересна как экономистам, так и обычным читателям, не изучавшим финансовые дисциплины. В тексте читатель встретит два способа написания слова биткоин. Когда оно пишется с заглавной буквы, имеется в виду платежная система или само явление. Если же имеется в виду биткоин как денежная единица, то слово пишется со строчной буквы.

УДК 821.161.1-34  
ББК 84(2=411.2)6

ISBN 978-5-222-40755-4

© Остальский А. В., 2023  
© Феникс, 2023

# Содержание

Пролог	6
Часть первая	8
С рогами и копытами	8
Кто же он?	12
Что скрывает биткоин?	16
Конец ознакомительного фрагмента.	17

# Андрей Остальский

## Новая история денег

© Остальский А. В., 2023

© ООО «Феникс», оформление, 2023

*Деньги... по сути, служат... тонким инструментом,  
соединяющим настоящее с будущим.*

*Джон Мейнард Кейнс*

*Доверие – это сырьё, из которого изготавливаются все виды денег.*  
*Юваль Ной Харари*

## Пролог

Завораживающее зрелище: огромные, могучие печатные прессы с умопомрачительной скоростью – глаз не успевает следить – извергают оранжевые, зеленые и желто-коричневые листы; специальный нож молниеносно разрезает их на яркие бумажные полоски, при ближайшем рассмотрении оказывающиеся банкнотами в 50, 100 и 200 евро. Потом бумажки эти громятся на столах, лежат высокими стопками на полу, валяются под ногами, и люди просто ходят по ним, как по мусору. Это кадры из испанского «Бумажного дома» – одного из самых популярных телесериалов всех времен и народов. Деньги – во множестве значений этого многогранного термина – его главная тема.

И дом в названии на самом деле не просто бумажный. Это мадридский Монетный двор, где уже не столько чеканят монету, сколько печатают банкноты в валюте ЕС – евро. Преступный гений по кличке Профессор придумал, как, перехитрив испанские власти и захватив это учреждение вместе с заложниками, похитить не готовые дензнаки, а драгоценное время тех самых огромных печатных станков, на которых банда сотворяет из ничего невероятную уйму наличности – около миллиарда евро.

Эта захватывающая сказка-утопия завораживает не только бешеными поворотами сюжета и яркими характерами, но и своим анархистским месседжем. Современные испанские Робин Гуды не только заняты личным обогащением, но и бросают вызов финансово-кредитной системе капитализма, объявляя ее порочной и несправедливой. Вот что говорит Профессор в своеобразной программной речи налетчиков: «В 2011 году Европейский центральный банк произвел из ничего 171 миллиард евро... И знаете, куда ушли все эти деньги? Они пошли банкам, то есть напрямую... в карманы богачей. Кто-нибудь назвал ЕЦБ вором? Нет. Они назвали это инъекцией ликвидности. Ну вот и я делаю такую инъекцию, но только я вливаю ликвидность не в банки, а в реальную экономику».

Ну, насчет «карманов богачей» – это, конечно, риторический перехлест, пропагандистское передергивание в духе вульгарного, не очень грамотного марксизма. Те миллиарды, временно добавленные в денежную массу ЕЦБ, пошли не в чьи-то частные кошельки, а на поддержку банковской системы и экономики в целом. И кстати, с 2010 по 2015 таких «инъекций» было на самом деле произведено на гораздо бóльшую сумму – два триллиона (!) евро с лишним. Но без этих вливаний Европа не вылезла бы из рецессии и кризиса, и это ударило бы больше всего по беднякам и среднему классу, а не по богатым. Другое дело, что банки и банкиры долгое время вели себя вопиюще безответственно и более других виноваты в жестоким кризисе 2008–2009 годов, последствия которого не до конца преодолены до сих пор. Обидно и несправедливо, что расхлебывать заваренную банкирами кашу, расплачиваться за их жадность и преступную беспечность пришлось всем нам. Но все же не надо путать причину со следствием и лечение – с болезнью.

Но в чем Профессор совершенно прав, так это в том, что нелегально напечатанные и ловко вывезенные из мадридского Монетного двора наличные действительно влились бы в реальную экономику. До того, как пандемия коронавируса перевернула мир вверх тормашками, многие экономисты считали, что в условиях низкого роста и стагнации последних лет финансовую систему было бы весьма полезно слегка разогреть, увеличив денежную массу в обращении; одного миллиарда, впрочем, для этого было бы явно мало. Но коронавирус все изменил, и вот уже правительства и центробанки вбрасывают в финансовые системы своих стран чудовищные, небывалые суммы, от которых глаза на лоб лезут, и никто не знает, чем такая беспрецедентная щедрость закончится – не новой ли Великой депрессией? Некоторые правительства даже напрямую одаривают население безвозмездной помощью на крупные суммы. Впрочем, пророк монетаризма Милтон Фридман писал о «сбрасывании денег с верто-

лета» как необходимом в особых случаях методе наращивания количества денег в обороте; так государства практически этим и занялись.

К Фридману и его теории мы еще вернемся, но пока снова о красивых банкнотах. «Бумажный дом» вновь усиливает общераспространенное мнение, что именно они, эти разноцветные фантики, и есть деньги нашего мира. Разве не так? Не совсем. Вернее, совсем уже не так. Подавляющую часть денег – около 90 процентов – творят банки, выдавая кредиты. А наличные теряют свою роль и значение и в некоторых странах могут скоро превратиться в анахронизм. Но совсем недавно, лет 10 с небольшим назад, появился еще один – и какой! – «производитель денег». Самый модный, самый таинственный и интригующий. Это блокчейн, он же распределенный леджер (или реестр), создатель биткойна, вслед за которым родились и другие криптовалюты. Таковых сейчас в мире насчитывается уже несколько тысяч, и любому дилетанту понятно, что такого их количества человечеству явно не нужно. Большая часть наверняка обречена на скорую гибель, не до конца понятно, сколько сумеет уцелеть, некоторые не видят долговременной перспективы ни у одной из них.

Поклонники криптовалют уверены, что их появление – это великая революция в мире финансов, что они способны заменить деньги банков и правительств, став доступными каждому, у кого есть смартфон в любом конце мира. Ведь крипто не знает границ! А если вложиться в такую валюту в правильный момент, то можно на ней сильно и быстро разбогатеть.

Мне показалось, что было бы интересно начать эту книгу как бы с конца: с разговора именно об этих недавних пришельцах – странных, таинственных и никому до конца не понятных квазиденьгах. А потом уже вспомнить о том, с чего все начиналось и во что превращалось. Ведь внимательно посмотрев на новорожденные деньги в их первоначальном виде, легче разглядеть их голую суть. И понять, чем криптовалюты от денег отличаются и на что они исторически похожи. Потому что все ново – и в то же время ничто не ново под луной.

Итак...

## Часть первая Тайна биткоина

### С рогами и копытами

Но как, как выглядит этот чертов биткоин? Он еще неуловимей, еще призрачней, чем проклятый коронавирус. Тот, по крайней мере, материален, хотя его тоже не увидишь глазом и не пощупать руками. Но в сильнейший микроскоп его все же можно разглядеть, у него есть какое-никакое, пусть суперкрохотное, тельце, из которого торчат омерзительные рога – их тоже можно увидеть в электронном увеличении и даже сфотографировать. А у биткоина нет ни веса, ни массы, ни высоты, ни длины. Если вы его увидите, то будете сильно разочарованы. Какие-то бледные строчки высыпаются на компьютерный экран – не понять, где они начинаются и где кончаются. Крохотные единички да нолики. И ничего больше ведь там нет, разве что буквы иногда беспорядочно и бессистемно туда еще вставлены, по крайней мере, так кажется с первого взгляда. Да и они, эти строчки, – лишь след чего-то другого, происходящего в потустороннем электронном мире. И вот ЭТО, этот невнятный, эфемерный призрак навязывается человечеству в качестве денег новой эпохи? И неужели он может стоить тысячи и тысячи долларов? Да с какой такой стати?

Людям понадобилось нечто, что могло бы примирить их психику с этой несообразностью. Нечто материальное, понятное, осязаемое. Сначала явился внятный символ – #. Посмотрите на него: по-моему, похоже на латинскую букву В, но с рогами и копытами, разве нет? Поклонники криптовалюты, впрочем, с этим не согласны и уверяют, что это – след двух вертикальных линий, перечеркивающих знак, а значит, отсыл к доллару США, который биткоин намерен потеснить. Потом придумали знак почему-то наклонить на 14 градусов вправо, и вышло вот что:

Но этого было мало, и кто-то создал сувенирные монеты, латунные, а затем даже серебряные и золотые. Красивые, тяжелые штуки, евро может позавидовать. Подержать такую монету в руках было очень приятно, она придавала биткоину некий смысл. Монеты те имели и кое-какую материальную ценность – в том числе коллекционную. Но на самом деле они соотносились с настоящими биткоинами примерно как придуманные фантастами зеленые человечки с где-то наверняка существующими, но неизвестными нам внеземными цивилизациями. В 2011 году появились монеты Casascius. Это было уже нечто принципиально иное, попытка соединить виртуальное с материальным: в монете были записаны коды, удостоверяющие реальное владение одним биткоином, который мог соответственно колебаться вместе с курсом самой криптовалюты. Но это все равно подмена, игра. Монета та играла роль лишь кошелька для настоящего биткоина, но никакого иного финансового смысла в ней не было. Чистая психология – попытка облегчить человеку взаимодействие с чем-то труднопознаваемым, чужеродным и странным.

Но вообще-то, если бы меня заставили определить биткоин как можно короче, я бы рискнул сказать: это интернетные деньги. Шифрованный метод перемещения средств в киберпространстве. (Хотя кто-то скажет иначе: технология.) Да-да, в итоге это и то и другое. Но в любом случае эта шифротехнология наделала всемирного шума.

Создатель Биткоина дал своему детищу определение ненамного длиннее моего: «Одноранговая система электронных денег». Но лапидарная эта дефиниция требует множества непростых пояснений. Для начала – что такое одноранговая? С этим нам еще предстоит разобраться.

И кто он сам, этот сумрачный гений? Тоже призрак? Тоже лишь символ, не имеющий физического тела и облика? Якобы 36-летний, якобы японец, якобы по имени Сатоши Накамото. 3 января он якобы пробежал пальцами по клавиатуре, и самое поразительное явление XXI века родилось на свет. «Бит», понятное дело, это единица измерения информации, а «коин» произошел от английского слова coin, монета. В том, что сотворил таинственный программист, было очень много битов – 31 тысяча линий кода, но никаких, разумеется, монет. Появился на свет и «ник», аббревиатура, которая станет самым употребимым именем в криптовалютных кругах – BTC.

Мало кто за пределами узкого круга специалистов обратил в тот момент на произошедшее внимание, а в числе тех, кто его заметил, большинство скептически крутило носами. Гораздо более известные и уважаемые в тех кругах люди уже достаточно давно пытались создать нечто подобное, например b-money, придуманные блистательным американцем китайского происхождения, создателем легендарной библиотеки криптографических алгоритмов сгупто++ по имени Вей Дай (Wei Dai); или же bit gold, бит-золото, основанное не менее легендарным Ником Сабо (Nick Szabo). Все это было очень занимательно и забавно для просвещенных специалистов, но практического применения не имело. А тут вдруг является некий самозванец, мутный тип со странным, претенциозным именем – вернее, псевдонимом. И выступает с неслабыми претензиями: что он ни много ни мало, а создал принципиально новый вид денег для цифровой эпохи. Деньги эти, утверждал он в опубликованной ранее «Белой книге», освободят людей от навязчивого контроля банков и государств, позволят анонимно оплачивать товары и услуги, а также накапливать капиталы и инвестировать их. В общем – полная свобода и неприкосновенность частной жизни! Лозунг этот звучал в унисон господствовавшим в тот момент в мире настроениям: в разразившемся всемирном финансовом кризисе общественное мнение винило прежде всего банки, а во вторую очередь – правителей, не сумевших или не захотевших защитить простого человека, но мигом пришедших на выручку жадинам-банкирам. В код, опубликованный 3 января 2009 года, был вмонтирован заголовок с первой страницы лондонской газеты «Таймс»: The Times 03/Jan/2009 Chancellor on brink of second bailout for banks – «Канцлер казначейства готов предоставить второй пакет финансовой помощи банкам». Это был и своеобразный «таймстэмп» – временная метка, и идеологическое послание: вот до чего довели дело власти и финансисты, Биткоин – наше спасение.

Тем не менее проект не вызвал восторга у подавляющего большинства экономистов. Я и сам в то время поддался их уверениям, что Биткоин – пустое дело и будущего у него нет. Да и невозможно спорить с фактом: создавать локальные или отраслевые денежные суррогаты пытаются с незапамятных времен, и эти квазиденьги часто провозглашались великими революционными открытиями, но неизбежно заканчивались пшиком.

Ко всему прочему, и настоящее имя свое изобретатель новой валюты скрывает, прячется – то ли шарлатан, то ли изощренный мошенник, нашедший новый способ ободрать наивных и легковверных, рассуждали знатоки. Да пусть покажет свое лицо и раскроет тайну псевдонима. А пока он этого не сделает, есть все основания предполагать худшее, говорил один из самых известных в Британии экономистов.

Я, как и многие, как абсолютное большинство, не поверил в биткоин – и не разбогател, как те немногие, кто поверил. Как, например, юный американец, мальчишка Эрик Финман: в 2011 году он вложил в биткоины тысячу долларов, подаренную бабушкой к 12-летию, и теперь, глядите на него, ходит в мультимиллионерах, важный, как Илон Маск. Эх, знать бы, где упадешь, соломку бы подстелил, знать бы, какой актив подорожает в сотни или тысячи раз (не говоря уже о миллионах), и можно свой путь не то что солодкой, а розами или золотом устилать. Но есть, наверно, высшая справедливость в том, что этого, как прикупа в преферансе, не дано знать никому. Угадать можно только по дикому везению, а то и вообще просто по глупости, как в разработанной (кажется, на спор) уже упоминавшимся американско-китайским

гением криптографии Вей Даем забавной игре: она так устроена, что побеждает, как правило, самый глупый игрок.

Первая сделка с биткоином – покупка двух пицц за 10 тысяч биткоинов – была произведена в мае 2010 года. Надеюсь, что программист из Флориды Ласло Хэнич (Laszlo Hanyecz), его друзья и родственники слопали те пиццы с особенным аппетитом, но подозреваю, что он пропал бы, знай они, что через семь с половиной лет, в декабре 2017 года, стоимость того ланча приблизится к 200 (двумстам!) миллионам долларов. А через несколько лет и через 600 миллионов перемахнет – правда, чтобы тут же снова упасть – почти в два раза. Вот они, казалось бы, верили в биткоины, но не сильно, не до конца, допускали, что они подорожают, но не в миллионы же раз, черт возьми! Неизвестно, впрочем, что сделал с тем электронным «уловом» пользователь форума [bitcointalk.org](http://bitcointalk.org) из Великобритании с ником Jercos (ему было тогда всего 18 лет). Именно он заплатил пиццерии Papa John's кредитной картой, получив от Хэнича за это биткоины. Так или иначе, а с тех пор поклонники криптовалют отмечают 22 мая как праздник Bitcoin Pizza Day – ведь та, кажущаяся сегодня безумной, покупка впервые наглядно показала, что за биткоины можно что-то реально покупать и продавать. В интернете нетрудно найти ежедневно меняющийся «Индекс пиццы биткоина», показывающий, сколько «стоят» теперь те две достославные пиццы (иначе говоря, сколько долларов можно получить в настоящее время за 10 тысяч биткоинов). Цифра эта то и дело очень резко – в разы – взлетает и падает вместе с изменениями курса криптовалюты (к теме волатильности Биткоина мы еще вернемся). Что же касается Хэнича, то он участвовал потом в нескольких криптопроектах, в том числе работал над усовершенствованием системы Lightning Network, специально созданной для ускорения сделок с применением биткоинов. И вот с ее помощью снова купил две такие же пиццы в том же заведении – на этот раз они обошлись ему всего в 0,00649 биткоина, – да и то некоторые пишут в соцсетях, что переплатил.

Еще одно имя вошло в историю криптовалюты в том же ряду: Джеймс Хауэллз (James Howells). Этот программист из Уэльса обратился в Биткоиновскую веру очень рано – прямо в начале того же достославного 2009 года. Он стал одним из первых «криптошахтеров», освоивших так называемый «майнинг» (к этому термину мы тоже еще вернемся) – то есть производство, «добычу», с помощью электронно-компьютерной силы, новых биткоинов. Но вера его была, видно, недостаточно тверда: когда его девушка стала жаловаться на то, как раздражает ее компьютерное гудение, он уступил возлюбленной и прекратил это занятие, о чем жалеет до сих пор. Впрочем, он полагал, что «намайнил» уже и так немало: семь с половиной тысяч биткоинов. Хранил он их на жестком диске своего ноутбука марки Dell. В какой-то момент разобрал его на части, диск спрятал в шкаф. И надолго забыл о нем. Настолько забыл, что через несколько лет при очередной разборке машинально выбросил его в мусор вместе с прочим компьютерным хламом. И опомнился только в тот момент, когда цена одного биткоина превысила 500 долларов. Вот тогда он стал мучительно вспоминать, куда делись его электронные деньги, стоившие к тому моменту уже порядка четырех миллионов долларов. И вспомнил! Но было уже поздно: на общественной свалке в районе города Ньюпорт за четыре минувших года накопились тонны и тонны всевозможного мусора, похоронившего компьютерный диск и записанные на нем строчки – нанизывания большого числа букв и цифр. Это так называемые «ключи» к электронным «кошелькам», в которых «хранятся» (видите, сколько слов приходится ставить в кавычки – ведь все это лишь сравнения-уподобления чему-то известному нам из нормального быта) те самые строчки кода. Вам нужен частный, секретный «ключ», который надежно запирает ваш «кошелек», но также и «ключ» публичный, он же «адрес», который вы используете для транзакции, посылая его через интернет покупателю или продавцу.

Вот, например, как такой частный «ключ»-пароль может выглядеть:

5KVb8kLf9zgWQnodigDA76MzPL6TsYYZ36hWXMssSzNydYXYB9K

Кстати, в русском языке со словом transaction случился жесткий «форк» – то есть насильственное, принудительное ответвление. (Об этих терминах в применении к Биткоину чуть позже.) То есть теперь в традиционных финансовых текстах надо писать: транзакция (через «с»), а в программно-компьютерных – через «з» – транзакция.

«Ключи» надо как-то записывать – либо электронно, либо на бумаге. Одно из железных правил, которым обучают новичков в мире криптовалют, гласит: «Если вы потеряли ваши частные ключи, вы потеряли и свои биткоины – необратимо и навсегда». Да-да, если вы уронили на улице бумажник или несколько банкнот, есть невеликий, но реальный шанс, что вам их вернут (особенно если вы в Скандинавии). Если вы потеряли кредитную карточку, банк вам ее обязательно восстановит и даже, есть шанс, возвратит деньги, которые сумеют снять с нее злоумышленники. Но «ключи» восстановлению не подлежат, ваши электронные деньги будут или пожизненно погребены в эфирных безднах интернета, или же похищены мошенником, если тот сумел найти ваши записи, хотя бы на мусорной свалке. Владеть биткоинами – значит просто знать невыносимо длинные комбинации цифр и букв.

Есть, как известно, редкие самородки с абсолютной памятью – они могут просто взять и запомнить несколько десятков (или сотен) таких строчек, и ничего записывать не надо, ни в какой форме. Но таких среди нас единицы, и Джеймс Хауэллз к ним не относится. Он, бедолага, обречен на пожизненную муку: то и дело вспоминать о том, что его жизнь могла быть совсем другой, если бы не злополучная рассеянность. Иногда ему удается и забыть об этом. «У меня бывают хорошие и плохие дни», – говорит он. Но можно себе представить, что он испытывал, скажем, в декабре 2017 года. Читая финансовые новости, он не мог не поддаться коварному соблазну и не подсчитать, сколько стоили в тот момент выброшенные биткоины. Около 150 миллионов долларов! Но не это самое главное его сожаление. Больше всего он не может себе простить, что поддался уговорам возлюбленной и прекратил «майнинг», который в те времена требовал совсем немного времени и электричества, не то что сейчас. «Я был в двух шагах от того, чтобы заработать 10 миллиардов, и не сделал этих шагов», – сказал он в интервью журналу «Ньюсуик». При этом Хауэллз уверяет, что всегда верил в будущее биткоина, знал, что он поднимется в цене, но... Значит, делаю я вывод, верил не совсем всерьез, для него, как и для многих, тогда это была скорее игра. Энтузиасты делали вид, что верили, ведь это было так круто, так весело. Но можно и бросить производить деньги, если девушку раздражает жужжание. Если женщина просит...

Но все это я говорю в основном к тому, что по-прежнему вопрос веры остается центральным. Главное, в чем нуждаются деньги, чтобы стать деньгами, – чтобы в них свято поверила достаточно большая часть населения. Финансы – это прежде всего психология. Нам только кажется, что деньги у нас в руках или кошельках (а теперь еще и в компьютерах), нет, они на самом деле в наших головах. А то, что мы принимаем за их физическое, а теперь уже и электронное воплощение, есть лишь вспомогательные опорные, сигнальные символы. В таком случае и набор электрических импульсов стодится в качестве платежного средства, лишь бы доверие к ним было массовым. Достигли ли уже биткоины необходимого уровня народной веры? На этот счет есть большие сомнения. Достигнут ли его когда-нибудь? Может быть, да, а может быть, и нет. Но то, что они поразили воображение миллионов людей, не вызывает сомнений. Все эти невероятные цифры, миллионы, полученные из грошовых вложений, которые любой мог бы себе позволить, рассказы о вдруг разбогатевших или о тех, кто легко мог бы разбогатеть, но вот потерял свои биткоины или продешевил, истратив их на какую-то ерунду, от всего этого у людей глаза лезут на лоб. И тайна, окружающая личность изобретателя первой криптовалюты, только дополнительно разогревает любопытство.

## Кто же он?

О Сатоши Накамото достоверно известно только одно, что такого человека не существует, иначе многочисленные энтузиасты, перерывшие все мыслимые базы данных, давно бы его разыскали. Мало того, в русском языке по крайней мере даже и с произношением его имени есть проблемы.

Satoshi было бы грамотнее произносить по-русски как Сатоси. Причем произошло недопонимание по одной-единственной причине: по-английски ведь пишется «sh», а мы привыкли произносить это сочетание звуков как «ш», хотя в данном случае это неверно, ведь так английские японисты пытались передать необычный, как бы немного шепелявый звук. Русская транслитерация, забавно прозванная «россиядзи», была разработана в 1917 году великим лингвистом и востоковедом Евгением Поливановым, который разъяснял, что звук этот гораздо ближе к русскому «с», но в слегка шипящем варианте, нечто между «си» и «щи». Если писать «ш», уверяют специалисты, то пропадает всякая «японскость». Получается подражание неправильно прочитанному английскому варианту. Но знатоки и эксперты российского криптомира убедили меня, что для них привычнее, ближе, роднее пусть неточное, но уже вошедшее в сердца и умы «ш». Значит, придется пожертвовать «японскостью».

Тем более что относительно происхождения имени изобретателя Биткоина тоже есть сомнения. Он вроде бы позиционировал себя как американского японца, но при этом, видимо, давно уже живущего в англосаксонском мире, стиль его письма и владение языком безупречны. Правда, еще одна странность: первые его публикации написаны на американском, а более поздние – на британском английском. Из чего напрашивается вывод: это два разных человека. Как минимум два...

В тот достопамятный день, 3 января 2009-го, условный Накамото опубликовал программу и создал первый, официально именуемый нулевым блок («Генезис-блок»). Сотворил первые 50 биткоинов. Первая транзакция между ним и известным программистом Хэлом Финни в июне 2009 года была произведена по курсу 0,0001 – одна десятитысячная доллара (или одна сотая цента) за один биткоин. В блоке номер 70 последний «намайнил» себе 10 биткоинов. Несколько лет спустя он так вспоминал о своем взаимодействии с Накамото, которого «живьем» так никогда и не видел: «Я понял, что имею дело с молодым человеком японского происхождения, очень умным и искренним. Мне посчастливилось за свою жизнь познакомиться со многими блестящими людьми, поэтому я узнаю их по некоторым признакам».

Как считает кое-кто из знатоков, сам создатель Биткоина успел обзавестись почти миллионом (!) электронных «монет». (По другим подсчетам, эта сумма несколько скромнее – около 700 тысяч биткоинов.) По какому курсу пересчитывать это состояние? Если по декабрю 2017 —то это двадцать миллиардов долларов. Но если бы Накамото дождался апреля 2021 года, то смог бы реализовать свои запасы криптовалюты по цене 55 тысяч долларов, выручив невероятную сумму – 55 миллиардов. Но даже если бы у него не хватило терпения, и он продал бы монеты весной 2020 (по цене 5 тысяч долларов), то получил бы около пяти миллиардов. Тоже не слабо. Но вот что интересно: биткоинов тех он так и не «отоварил» и ни на что не поменял. Ни по какому курсу. Сидел себе на них, как Скупой рыцарь. Ни себе ни людям... Но может, и слава богу, что эти гигантские средства остаются без движения, должны сказать поклонники виртуальной валюты. Ведь если этот некто когда-нибудь вздумает выбросить на рынок значительную часть своего «капитала», Биткоин может рухнуть, возможно и навсегда. Некоторые аналитики называют этот огромный массив электромонет «дамокловым мечом Накамото». В любой момент может, если захочет, уничтожить свое детище. Тогда получится: я тебя породил, я тебя и...

Но так или иначе, примерно из 18 с половиной миллионов биткоинов, созданных на настоящий день, почти два миллиона считаются «заснувшими», то есть владельцы ими почему-то очень давно не пользуются, то ли потеряв частные ключи, то ли по каким-то технологическим или личным причинам. Есть и другие подсчеты: по ним получается, что чуть ли не четыре миллиона электронных монет «утрачены навсегда». Сам Накамото когда-то объявил такие утраченные биткоины «пожертвованием в пользу сети». Принято считать, что он и сам делал такие альтруистические дарения для поддержки своего проекта, не исключено, что и весь миллион – или 700 тысяч – тоже были им «усыплены», то есть фактически уничтожены во имя благородных криптоанархических целей.

Но даже если забыть о ранней эпохе становления Биткоина и обратиться к 2014 году, то выясняется, что с тех пор владельцы 11 крупных «кошельков» не производили никаких оплат, накопив в них больше 270 тысяч биткоинов. Это, конечно, не миллион. Но даже по исторически не самым высоким ценам весны 2020 года, например, это два с половиной миллиарда долларов. Год спустя эта сумма выросла почти в десять раз. Если один из этих «китов» начнет активно продавать криптовалюту, ее цена резко пойдет вниз, что может заставить включиться многочисленных ботов, которые тоже ринутся в быструю распродажу, потом начнется общая и обычная в таких случаях паника, и тогда уже курс биткоина упадет катастрофически – вплоть до полного краха. Такого рода опасения, кстати, весьма распространены и заставляют пессимистов сомневаться в том, есть ли у криптовалют серьезное будущее...

...Настал момент, и Накамото взял и исчез. Написал на форуме, что решил заняться другими делами. И вот с 2010-го о нем ни слуху ни духу. Но зато его с тех пор усердно ищут другие. Множество людей. Кто с познавательными целями, из любопытства, а кто, возможно, и с корыстными. Охота за Накамото для многих стала чем-то вроде хобби, если не профессии. Каких только теорий на этот счет не выдвигалось!

Подозревали уже упомянутых Вей Дая, Ника Сабо и Хэла Финни. Известный исследователь и знаток всего, что связано с биткоинами, Джошуа Дэвис доказывал, что Накамото – это на самом деле некий юный, но, судя по всему, очень талантливый криптограф из Дублина по имени Майкл Клир (Michael Clear). Австралийский компьютерщик Крейг Райт утверждает, что он и есть создатель концепции Биткоина. Он даже использует в соцсетях ник Craig Wright (SATOSHI). И периодически представляется как: «Я – Крейг Райт, создатель Биткоина, самый богатый человек в мире и отец всей этой криптоиндустрии». Но другие авторитетные фигуры в мире виртуальных валют и криптографии подвергают эти утверждения сомнению. В общем, в списке эвентуальных претендентов на роль Накамото довольно много людей, и список продолжает расти.

А кто-то увидел в имени изобретателя Биткоина аббревиатуру и, расчленив его на части, получил не слишком сложно зашифрованное послание: **Sa** – от Samsung, **Toshi** – от Toshiba, **Naka** – от Nakamichi и **Moto** – от Motorola. То есть получается, что четыре всемирно известные компании по производству электроники – одна южнокорейская («Самсунг»), одна американская («Моторола») и две японские («Тошиба» и «Накамиши») совместными силами создали Биткоин, спрятавшись под псевдонимом Сатоши Накамото. И при этом весьма прозрачно прокламировали этот факт в придуманном имени.

Дурацкое совпадение, конечно, но смешное...

Еще экстравагантнее (и ближе сердцу истинных любителей теорий заговора) звучит предположение, что на самом деле изобретение Биткоина – творение американского шпионского ведомства. Вот как рассуждают сторонники этой версии: по-японски фамилия идет впереди. «Накамото» значит «внутренний» или «центральный». А «Сатоши» – «ясно мыслящий», «умный», «интеллектуальный», короче говоря. То есть можно понять это сочетание слов как «центральный ум или интеллект». Но ведь по-английски intelligence – это не только ум, но еще и разведка. То есть получается Central Intelligence, добавим еще слово Agency, и готово – Цен-

тральное разведывательное управление, ЦРУ. Которое тоже почему-то решило при этом себя выдать с помощью неуклюжего ребуса.

Всякие теории – сомнительные и не очень – можно перечислять еще долго. Но самое солидное и интересное расследование провел, на мой взгляд, профессор журналистики Нью-Йоркского университета Адам Пененберг. Во-первых, он рассмотрел уже упомянутую гипотезу Джошуа Дэвиса, пытавшегося доказать, что Накамото – это 23-летний Майкл Клир, и показал ее безосновательность. Но он использовал кое-какой интересный материал, собранный Дэвисом. Например, интервью со знаменитым Дэном Каминским – великим, знаменитым антихакером. Свой талант тот использует для защиты компьютерных сетей от злоумышленников. Он находит слабые места, показывает, как ими могут воспользоваться мошенники, и помогает эти бреши заделать. Считается, что в свое время чуть ли не весь интернет спас, когда возникла опасность, что им может завладеть некий зловещий хакер. Каминский был уверен, что запросто взломает сеть Накамото, настолько на первый взгляд уязвимой казалась эта структура. После многих дней напряженной работы с применением большого числа мощных компьютеров Каминский нашел девять слабых мест. Но когда он пытался туда вторгнуться, то каждый раз наткнулся на прочный заслон. А на экране монитора появлялись слова: «Нападение отбито». Каминский говорит, что это был шок: ни до, ни после он не встречал ничего подобного. И намекнул, что, возможно, за созданием такой гениальной сети должны стоять несколько необычайно талантливых и умных людей. Ведь для того, чтобы сотворить нечто подобное, надо быть не только программистом высшего класса, досконально, до тонкостей, владеющим языком программирования «С++», но и обладать глубочайшими познаниями в области криптографии, экономики и строительства одноранговых виртуальных сетей (о том, что это такое, смотрите ниже). И ведь сколько лет прошло с момента создания сети Биткойна, а взломать ее так никому и не удалось, а уж в том, что лучшие хакерские умы трудились над этим долго и больно и продолжают трудиться и по сей день, можете не сомневаться. Удивительный феномен в зыбком виртуальном мире, где никто и никогда не чувствует себя в безопасности...

Профессор Пененберг вспомнил об этом намеке Каминского, когда перешел к следующей стадии своего расследования. А именно: он стал выбирать отдельные, необычные, редко встречающиеся словосочетания из «Белой книги» и постов Накамото на форумах и так далее и вбивал их в поисковик Гугла, причем ставил эти фразы в кавычки, чтобы поиск находил только буквальное совпадение. Надежда была на то, что Накамото мог выдать себя в какой-нибудь другой публикации, под другим, возможно, своим подлинным именем. Ведь людям свойственно повторять показавшиеся им удачными формулы в разных публикациях и жанрах. Долго ничего толком не находилось, кроме прямых или косвенных цитат из работ Накамото, касающихся Биткойна, как вдруг... Бинго! Диковатая фраза «computationally impractical to reverse» («вычислительно практически невозможно развернуть в противоположную сторону») обнаружилась в документе, вроде как никоим образом с Биткойном не связанном, – в описании патентной заявки, поданной, между прочим, 15 августа 2009 года, то есть за три дня до того, как был зарегистрирован накамотовский домен Bitcoin.org!

Авторами той заявки на изобретение «Обновления и распределения ключей шифрования» числились трое: обитатели Мюнхена Нил Кинг (Neal King) и Чарлз Брай (Charles Bry), а также живущий в США Владимир Оксман (Vladimir Oksman). Все они оказались очень замкнутыми людьми, не светящимися в соцсетях и избегающими паблисити, про которых мало что можно было выяснить. Но в итоге все трое категорически отрицали свою причастность к Биткойну. (Причем Нил Кинг даже высказал серьезную критику самой концепции криптовалюты.) Тем не менее Пененберг считает, что его изыскания указывают на весьма высокую вероятность того, что он нашел людей, скрывавшихся за псевдонимом Накамото. Вероятность гораздо более серьезную, чем все другие предположения. Но вероятное – не есть доказанное. И, будучи в

высшей степени ответственным расследователем, он готов признать, что его гипотеза остается лишь гипотезой, хоть и весьма правдоподобной.

Обратил я внимание и еще на несколько цитат в той интригующей патентной заявке. В первом, черновом варианте этой части книги я дальше рассуждал на технологические темы, приходя в итоге к выводу, что авторы патентной заявки предвосхитили важнейшие элементы системы Биткоина – за три дня до его рождения! Но, прочитав текст вслух, понял, что выходит тяжеловато. Внимание читателя неизбежно начнет блуждать. Да и насколько важно нормальному человеку, не слишком интересующемуся криптографией, вдаваться в такие дебри? Наверно, не очень. Поэтому для желающих помешаю подробности в Приложение в конце этой книги. Здесь же сразу перескакиваю к выводу. Трудно поверить в такие совпадения. Или эти трое, авторы заявки, и есть коллективный Накамото, или же они действовали в его интересах и под его прямым руководством. Другого объяснения я придумать не мог.

## Что скрывает биткоин?

Каждый сегодня слышал, что Биткоин – это так называемая криптовалюта. От греческого слова κρύπτω (krúptō, «скрывать»). Так что же, значит, все же это нечто скрытое, зашифрованное? Да, разумеется, – от посторонних, но частично – и от своих. Секрет разделен, конечно, но не до конца. И в этом весь смысл. Даже солидные СМИ до сих пор путаются, называют криптовалютой любые цифровые деньги, например экспериментальную шведскую электронную Э-крону (E-krona – см. главу «Ближние и дальние перспективы»). Но есть принципиальное, важнейшее отличие. Шведскую электронную валюту намерено гарантировать шведское государство. В то время как настоящая криптовалюта – это децентрализованная система платежного обмена, основанная на криптографии и не имеющая ни внешнего, ни внутреннего администратора. Что позволяет обеспечить безопасность финансовых транзакций, контроль за созданием дополнительных денежных единиц и проверки трансфера (передачи) активов. Впрочем, с безопасностью, возможно, все еще лучше обстоит у шведов, но существенное отличие любой криптовалюты от других электронных денег состоит в том, что она никоим образом не контролируется ни банками, ни государствами.

Далее в черновом варианте я обильно цитировал Накамото, описавшего основные принципы своей криптовалютной концепции. Это был мой перевод с английского. Но Накамото пишет для посвященных, для своих. Для всех этих сдвинутых криптографов и программистов. Для нормальных людей требовался второй перевод – пересказ – на нормальный язык. Я попробовал это сделать, но, прочитав получившийся текст вслух невинным подопытным кроликам, увидел, что у них стекленеют глаза. Поэтому вычеркиваю несколько абзацев – вернее, переношу их в приложение в конце книги. Здесь же обойдусь самым общим и до предела упрощенным описанием.

Когда говорится об одноранговой платежной системе, то имеют в виду полное равноправие всех участников (на профессиональном жаргоне все участвующие в функционировании сети компьютеры называются нодами – узлами). Над нодами нет начальника или администратора, они сами контролируют друг друга. И сами же они производят новые монеты. Но ведь деньги становятся средством платежного обмена только тогда, когда завоевывают универсальное доверие в обществе. Обычно оно обеспечивается через высокий статус банков или государства, печатающего банкноты (или пусть даже, как в случае с Э-кронной, производящего деньги в виде электронного импульса). Однако в сети Биткоина, пишет Накамото, ни тому ни другому места нет. Весь смысл криптовалюты в том, что ни тех ни других она не признает. Но как же быть с доверием? Его, как предполагается, должны обеспечить сами участники, заключив негласный общественный договор, утверждающий достоинство Биткоина. Вступая в сеть, ты тем самым под тем договором как бы подписываешься. А дальше вся сила – во всеобщем контроле за всем происходящим. Это еще называется на языке криптовалютчиков словом «консенсус».

Вспоминают еще и логическую задачу, так называемую «проблему византийских генералов». Представьте себе: большое число дивизий, каждая со своим генералом во главе, готовится к наступлению, от которого зависит, уцелеет ли вся византийская армия. Но некоторые из этих генералов, вполне возможно, предатели. Так вот, должна в теории существовать такая система связи между всеми командирами и главнокомандующим, которая подстрахует, не даст предателям погубить всю цепь. Даже если предатель – сам главком! Но ведь для решения этой задачи необходим математический алгоритм, система ВФТ, «Византийской отказоустойчивости».

## **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.