ЦИФРОВОЕ ЗОЛОТО

НЕВЕРОЯТНАЯ ИСТОРИЯ БИТКОЙНА, ИЛИ КАК ИДЕАЛИСТЫ И БИЗНЕСМЕНЫ ИЗОБРЕТАЮТ ДЕНЬГИ ЗАНОВО

НАТАНИЕЛ ПОППЕР

Натаниел Поппер

Цифровое золото: невероятная история Биткойна, или Как идеалисты и бизнесмены изобретают деньги заново

«Диалектика-Вильямс»

2015

УДК 681.3.07
ББК 88.575

Поппер Н.

Цифровое золото: невероятная история Биткойна, или Как идеалисты и бизнесмены изобретают деньги заново / Н. Поппер — «Диалектика-Вильямс», 2015

ISBN 978-5-8459-2079-9

Биткойн – это пиринговая платежная система и финансовая технология, которая ломает многие привычные представления о деньгах и их роли в обществе. Многих ставит в тупик сама мысль о цифровой валюте, за которой не стоит мощное государство или Центробанк и поддержка которой осуществляется совместно всеми ее пользователями. Но это не помешало Биткойну вырасти в технологический феномен с миллионами сторонников и капитализацией в миллиарды долларов. Его фанаты считают Биткойн важнейшим изобретением человечества, сравнивая его с Интернетом по потенциалу воздействия на общество.В этой книге рассказана невероятная история о том, как идея, изначально интересная лишь маленькой группке энтузиастов, постепенно привлекла к себе внимание всего мира. История, в которой важную роль играют самые неожиданные персонажи: финский студент; аргентинский миллионер; китайский предприниматель; создатель Netscape; неудавшийся физик, ставший онлайн-наркобароном; близнецы-плейбои, засудившие главу Facebook; акулы венчурного капитала; прокуроры и спецагенты; сенаторы США и руководители крупнейших мировых банков. Конечно, повествование не могло обойти стороной и таинственного отца-основателя Биткойна, выступавшего под псевдонимом «Сатоши Накамото». Так ли он на самом деле анонимен и неуловим, как кажется широкой публике? Энтузиасты Биткойна во всем мире – от Пекина до Буэнос-Айреса – верят в способность этой полностью пиринговой финансовой системы стать всемирно признанными деньгами цифровой эпохи. Как минимум стремительное восхождение криптовалютных технологий поднимает серьезные вопросы о том, чем на самом деле являются деньги, как они работают сейчас и как им предстоит измениться, чтобы отвечать будущим потребностям

общества.Книга номинирована Financial Times в категории «Лучшая бизнес-книга 2015 года»

УДК 681.3.07
ББК 88.575

ISBN 978-5-8459-2079-9

Содержание

Натаниел Поппер
Цифровое золото

Nathaniel Popper
DIGITAL GOLD
THE UNTOLD STORY OF BITCOIN

* * *

Предисловие

Что такое деньги? Мы пользуемся ими каждый день, мы много о них говорим, мы их хотим. Но попробуйте прямо сейчас дать им определение: «Деньги – это…» Если вы столкнулись с затруднением, то знайте – вы не одиноки. Большая часть людей привыкли к некоему интуитивному пониманию этой сущности, но не более того. Вопросы наподобие «Что это такое?», «Почему у них именно такие форма и свойства?» и «Есть ли варианты лучше?» звучат гораздо реже, чем вопрос «Как их заработать?»

Исторически сложилось так, что практически везде деньгами заведуют государства, начиная от их выпуска и заканчивая правилами обращения и утилизации. Несомненно, у данного подхода есть свои плюсы, но есть и минусы. Те, кого минусы не устраивают, зачастую не имеют возможности что-либо изменить, улучшить, так как это может быть незаконно.

При этом нужно понимать, что законы появляются во вторую очередь, а в первую – само явление, которое они описывают. Иногда бывает так, что появляется новая сущность, а законов для нее еще нет. Так было с радио, автомобилями, Интернетом и многими другими технологиями, когда они появлялись. То же самое происходит сейчас с *криптовалютами*.

Криптовалюты появились на стыке экономики, криптографии и идеологии. Притом первая криптовалюта – *биткойн* – была инновацией «снизу», а не «сверху», т. е. не инициативой государств, а решением от народа. Тем интереснее следить за историей возникновения и развития этой инновации, описанной в данной книге.

Что же такого нового было предложено? Фактически были предложены модель и практическая реализация децентрализованного взаимодействия, при котором комиссии или отсутствуют, или минимальны. В этой модели без желания участников сделок никакая третья сторона не может ни помешать им, ни навязать свои услуги, ни заблокировать или конфисковать чужие средства. Это система с заранее запрограммированной эмиссией, которая исключает политические манипуляции или злоупотребления, связанные с возможностью управлять выпуском денег. Это транснациональная система без единой точки отказа, через которую можно было бы управлять ею в обход желания ее пользователей. Это система, которая не требует *доверия*: ее правильная работа гарантируется математикой и криптографией, а не правовыми контрактами, что полностью исключает человеческий фактор.

Биткойн стал первым практическим доказательством успешной работы блокчейн-систем. Однако сама технология блокчейна гораздо шире криптовалют; она позволяет создавать практически любые распределенные системы учета. К примеру, это могут быть земельные реестры, нотариальные сервисы, удостоверения личности, системы учета акций и иных прав собственности и так далее.

Кроме надежной распределенной базы данных, технология блокчейна позволяет создавать смартконтракты, которые выполняются автоматически, и использовать мультиподписи –

например, когда для проведения транзакции требуются две подписи из трех, – а также предоставляет другие удивительные возможности.

Конечно же, с новыми возможностями приходят и новые риски. Возможная анонимность, мгновенные переводы любых сумм в любую точку мира, невозможность блокировки счетов и другие особенности криптовалют ставят перед государственными структурами новые задачи в борьбе с преступностью, терроризмом и незаконным отмыванием средств.

Государства стоят сейчас перед выбором: как регулировать это новое явление, как использовать плюсы новой технологии, при этом минимизировав риски, как встроить это новое явление в текущую финансовую систему. Понятно, что варианты полного разрешения, как и полного запрета, не оставят возможности как-то управлять новыми явлениями, это скорее отказ от ответственности. При этом примера внедренного удачного регулирования нигде в мире еще нет, а значит, нет и возможности им воспользоваться.

А технология уже есть, она уже работает. Как когда-то электронная почта пришла на смену обычной или интернет-мессенджеры – на смену телефонной международной связи. Фактически джинн блокчейна уже выпущен из бутылки, и долго его игнорировать не удастся.

Бизнес уже готов внедрять криптовалюты, крупнейшие мировые банки изучают возможности блокчейн-технологий. Финтех-индустрия называет блокчейн одним из самых перспективных трендов современности. И лишь отсутствие правовой определенности не дает этим технологиям развернуться по-настоящему. В свою очередь, блокчейн-сообщество готово помогать всем желающим в изучении этих новых систем. Мы призываем быть не просто пассивными наблюдателями за происходящими переменами, но и активно участвовать в изменении мира к лучшему.

Иван Тихонов

Введение

Blockchain Community

Было уже за полночь, и многие гости отправились спать, оставив на столах стаканы с недопитым дорогим виски.

Дилеры для игры в покер, нанятые в местном казино, ушли полчаса назад. Оставшиеся игроки убедили их не забирать фишки и карты, чтобы можно было продолжить игру. Пока что они не собирались покидать свои места за дорогим столом под сводчатым деревянным потолком. За стеной из стекла был виден длинный причал, уходящий в глубь озера Тахо.

Глядя на двадцатидевятилетнего Эрика Вурхиса, сидящего спиной к озеру, никто не смог бы сказать, что всего три года назад он был безработным, перебивался случайными заработками и едва мог заплатить за аренду жилья, не говоря уже о том, чтобы вернуть долги по кредитным картам. За столом Эрик, надевший на вечер дорогую замшевую рубашку и заказные джинсы, непринужденно разговаривал с менеджером хедж-фонда. Волосы Эрика уже редели, но он сохранял моложавый бодрый вид. Эрик пошутил насчет своего вчерашнего проигрыша и сказал, что все идет по плану. «Вчера была разминка, я настраивался на сегодняшнюю битву», – сказал он с широкой улыбкой, прежде чем передвинуть стопку фишек в центр стола.

Эрик мог позволить себе такие шутки. Совсем недавно он выгодно продал сайт для азартных игр, на котором использовались загадочные цифровые деньги под названием «Биткойн». Эрик приобрел этот сайт в 2012 году за 225 долларов, поработал над его фирменным стилем, раскрутил его и через год продал примерно за 11 миллионов долларов. Он также владел немалой суммой в биткойнах, которые начал покупать несколькими годами ранее, когда каждый биткойн стоил всего несколько долларов. Теперь один биткойн стоил около 500 долларов, что делало Эрика долларовым миллионером. Крупные инвесторы и серьезные бизнесмены, которые первоначально относились к Эрику с пренебрежением, признали его за своего, и Дэн Морхэд, тот самый менеджер хедж-фонда, пригласил его в свой дом у озера Тахо, чтобы лучше узнать, о чем думают те, кому уже удалось разбогатеть на криптовалютной лихорадке.

Как и многие другие люди, собравшиеся в доме Морхэда, Эрик заинтересовался криптовалютами не только из желания разбогатеть, хотя и это было для него очень важно. Узнав о Биткойне из сообщения в Facebook, Эрик сообразил, что его курс имеет все шансы вырасти до астрономических высот, но этот рост будет следствием куда более серьезных трансформаций. Программный код и технология Биткойна могли коренным образом преобразовать традиционные властные структуры во всем мире, включая банки Уолл-стрит и национальные правительства, и сделать с деньгами то же самое, что Интернет сделал с обычной почтой и СМИ. Эрик рассчитывал, что Биткойн не просто сделает его богатым. По его мнению, Биткойн вполне мог создать для всех новый, более справедливый мир, в котором государства не смогут более финансировать бесконечные войны, а люди получат контроль над собственными деньгами и судьбой.

Неудивительно, что при таких амбициях жизнь Эрика уже несколько лет напоминала американские горки. Он долго сидел без работы в Нью-Гэмпшире, а переехав в Нью-Йорк, основал один из первых биткойн-стартапов под названием «BitInstant». Он убедил братьев-близнецов Уинклвоссов, заработавших капитал благодаря участию в создании Facebook, вложить в проект BitInstant миллион долларов. Однако это партнерство завершилось полным провалом, после которого Эрик ушел из компании и переехал в Панаму.

В последние месяцы Эрик проводил много времени в своем панамском офисе, отвечая на вопросы следователей из Комиссии по ценным бумагам и биржам США – одного из главных регуляторов в финансовом мире. Они интересовались, на каких условиях Эрик продал за бит-

койны долю в одном из своих стартапов, которая в итоге принесла инвесторам большой доход. По мнению Эрика, регуляторы даже не понимали, как работает Биткойн, но были правы в том, что он не зарегистрировал свои сделки с ценными бумагами должным образом. Как бы то ни было, стать фигурантом расследования было все же лучше, чем попасть в тюрьму, которая угрожала одному из бывших партнеров Эрика по BitInstant, арестованному двумя месяцами ранее по обвинению в отмывании денег.

Однако Эрик не поддавался давлению – в основном благодаря тому, что, в отличие от многих сторонников Биткойна, он с юмором относился и к себе, и к этому экзотичному движению, в центре которого оказался.

«Я часто напоминаю себе, что Биткойн может потерпеть полный крах, – как-то обмолвился он. – Каким бы неизбежным ни казался мне рост его курса, я все же стараюсь не забывать о том, что инновационные проекты обычно проваливаются».

Тем не менее Эрик продолжал работать над продвижением Биткойна, и не только из-за богатства, которое быстро накапливалось на его банковском счете. Еще больше Эрика интересовала сама природа новых денег, которые, как он считал, изменят мир.

ИНФОРМАЦИЯ О БИТКОЙНЕ впервые появилась в Интернете пятью годами ранее, когда загадочный автор по имени Сатоши Накамото опубликовал сообщение о нем в малоизвестной почтовой рассылке.

В своем сообщении Сатоши описывал новые универсальные деньги, которыми мог бы владеть любой человек в мире, используя их для каких угодно трат. Больше всего такие деньги напоминали цифровой аналог золота. Как и золото, эти новые цифровые монеты стоили бы лишь столько, сколько кто-то был бы готов за них заплатить (на первых порах – нисколько). Но система была спроектирована так, чтобы, как и золото, биткойны были редкими и их невозможно было подделать. Как и в случае с золотом, для «добычи» новых биткойнов требовалось выполнить определенную работу, в данном случае – компьютерные вычисления.

Биткойн имел даже ряд преимуществ перед золотом. Так, чтобы переместить биткойны из Лондона в Нью-Йорк, не требовалось ни корабля, ни самолета: достаточно было ввести цифровой ключ и сделать несколько щелчков мышью. Для обеспечения же безопасности использовались надежные математические формулы, а не вооруженная охрана.

Но сравнение с золотом не может полностью объяснить, почему Биткойн в итоге привлек к себе такое внимание. Каждый слиток золота и каждая золотая монета существует независимо от других слитков и монет, тогда как биткойны интегрированы в хитроумно сконструированную децентрализованную сеть, подобно тому как все веб-сайты в мире находятся в Интернете. Как и Интернет, биткойн-сеть не находится под контролем какого-либо центрального учреждения; ее совместно обслуживают все люди, подключившие к ней свои компьютеры, что в действительности может сделать кто угодно. Интернет связывают воедино правила, или интернет-протоколы, которые регламентируют передачу информации. У Биткойна тоже есть свой протокол, определяющий все правила, по которым работает эта сеть.

Технические подробности реализации Биткойна достаточно сложны и включают сложные математические и криптографические формулы, но уже с самого начала проекта немногие преданные сторонники видели, что в своей основе Биткойн – это простой, удобный и элегантный способ создания, хранения и перевода денег. Биткойны не похожи на доллары и евро,

которые находятся под контролем центробанков и крупных транснациональных финансовых организаций. Это деньги, которые создают и поддерживают сами пользователи, а эмиссия медленно распределяется среди пользователей, которые помогают работе сети.

Биткойн ставит под угрозу существование некоторых могущественных институтов общества, поэтому многие энтузиасты с самого начала описывали его в утопических терминах. Интернет отобрал изрядную долю власти у крупных СМИ, наделив ею блогеров и диссидентов, а Биткойн обещал сделать еще больше: отобрать власть над деньгами у банков и правительств и передать ее самим людям, использующим деньги.

Такие идеи не могли не вызвать множества обвинений и презрительных насмешек, но большинство людей в первые годы существования Биткойна вообще ничего не слышали о нем. А те, которые слышали, чаще всего думали, что это какая-то разновидность финансовой пирамиды (или новая блажь вроде Тамагочи).

Однако Биткойну повезло появиться в мире в идеальный момент, вскоре после мощнейшего финансового кризиса, который обнажил многие недостатки финансовой и политической систем и породил много дискуссий об альтернативном устройстве общества. Проекты Tea Party, Occupy Wall Street и WikiLeaks имели разные цели, но все они были объединены желанием отнять власть у привилегированной коррумпированной элиты. Биткойн предоставил одно из возможных технологических решений этой проблемы. Потенциал Биткойна как нельзя лучше подтверждает поразительное разнообразие его сторонников, которые бросили свои прежние занятия, чтобы посвятить себя его популяризации. Конечно, не следует думать, что они были лишь бескорыстными альтруистами: успех Биткойна сделал бы их богачами. Как часто говорил Эрик, «это первый известный мне проект, который одновременно позволяет и разбогатеть, и изменить мир».

Возможность создания собственных денег привлекла к Биткойну не только диссидентов и революционеров. Прежде чем запустить свой хедж-фонд, Дэн Морхэд получил образование в Принстоне и проработал много лет в Goldman Sachs. Он был одним из главных инвесторов с Уолл-стрит, которые недавно начали вливать десятки миллионов долларов в биткойн-экосистему в надежде сорвать большой куш. Венчурные инвесторы и предприниматели из Кремниевой долины, в свою очередь, спешно изучали Биткойн в поисках возможностей потеснить воротил с Уолл-стрит и отнять долю рынка у платежных систем, таких как PayPal, Visa и Western Union.

Даже для людей, которые не испытывали симпатии к проектам Occupy Wall Street или Tea Party, были очевидны многие преимущества Биткойна. Универсальные деньги, которые не требовалось обменивать на каждой границе, платежи без необходимости отправки персональных данных, невозможность манипулирования денежной эмиссией, международные переводы почти без комиссии, возможность жителям беднейших уголков мира получить онлайн-доступ к финансовой системе, микроплатежи, позволяющие блогерам и журналистам монетизировать контент без рекламы – вот лишь некоторые из тех волнующих возможностей, которые замаячили на горизонте благодаря Биткойну.

Многие из тех, кого интересовали лишь сугубо практичные способы применения Биткойна, тоже осознавали его революционный потенциал. Ведь возможность создавать собственные деньги по-настоящему угрожала сложившемуся статус-кво. За ужином перед игрой в покер Морхэд пошутил, что все биткойны в мире стоят на данный момент примерно столько же, сколько и производитель рваных джинсов Urban Outfitters – около 5 миллиардов долларов.

«Странно, да? – сказал Морхэд. – Но я думаю, когда археологи или инопланетяне раскопают наши города через несколько веков, выяснится, что Биткойн оказал куда большее влияние на мир, чем Urban Outfitters. Мы лишь в самом начале пути».

Многие банкиры, экономисты и чиновники игнорировали биткойн-энтузиастов, воспринимая их как наивных фанатиков, которые поддались новомодной версии тюльпаномании,

охватившей Голландию четыре века назад. И действительно, несколько инцидентов подтвердили опасения критиков, продемонстрировав обратную сторону децентрализованных денег. Всего за несколько недель до собрания в доме Морхэда руководитель биржи Mt. Gox, крупнейшей на тот момент биткойн-компании в мире, объявил, что потерял биткойны своих клиентов на сумму около 400 миллионов долларов. И этот скандал был далеко не единственным ударом по пользователям Биткойна.

Но никакие кризисы не смогли погасить энтузиазм сторонников Биткойна, который продолжал привлекать новых пользователей, несмотря ни на что. Ко дню собрания в доме Морхэда на различных криптовалютных веб-сайтах было создано более 5 миллионов биткойн-кошельков, и разнообразие интересов их владельцев было очевидно по участникам собрания. Среди них были бывший руководитель Wal-Mart из Китая, недавний выпускник колледжа из Словении, лондонский банкир и два выходца из студенческого братства Технологического института Джорджии. Кто-то из них увлекся Биткойном из-за недоверия к правительству, кто-то разочаровался в банковской системе, а кого-то к Биткойну привели личные мотивы. Например, предки китайского руководителя Wal-Mart бежали от коммунистической революции, захватив с собой только золото, и он обоснованно считал, что Биткойн как нельзя лучше подходит для защиты сбережений в этом ненадежном и непредсказуемом мире.

Эти люди со всего мира сделали Биткойн тем, чем он является сейчас, и именно им посвящена эта книга. Сатоши Накамото, создатель Биткойна, исчез в 2011 году, оставив после себя ПО с открытым исходным кодом, который другие пользователи могли свободно обновлять и улучшать. По некоторым оценкам на пятом году существования Биткойна он содержал лишь 15 % исходного кода Сатоши, но от этого ПО стало только надежнее и эффективнее. Как это верно для любых денег, полезность и ценность Биткойна зависит от того, насколько велико сообщество использующих его людей. Каждый новый пользователь криптовалюты повышает общие шансы Биткойна на успех.

В общем, это не типичная история о революционном стартапе или гении-одиночке, которому удалось преобразовать мир, прославиться и по ходу дела заработать много денег. Это история о коллективном изобретении, в котором отразились многие актуальные проблемы и тенденции нашего времени: недовольство правительством и банками, разногласия между Кремниевой долиной и Уолл-стрит, мечты о технологических утопиях, способных защитить нас от наших же слабостей, и страх, что технологии выйдут из-под контроля. Эти и многие другие мотивы породили в недрах криптовалютного сообщества огромное количество интересных проектов, которые превратили Биткойн из теоретических рассуждений в многомиллиардную индустрию.

Одни из ранних энтузиастов Биткойна заработали целые состояния, другие потеряли все и даже очутились в тюрьме. Сам Биткойн постоянно находится под угрозой краха, если в нем вдруг будет обнаружен какой-то критический изъян. Но даже в этом случае Биткойн стал бы одним из самых впечатляющих практических исследований природы денег и возможных способов их улучшения. Вряд ли он полностью заменит доллар в обозримом будущем, но он хотя бы в общих чертах рисует альтернативное будущее, в котором мы можем оказаться, если центробанки прекратят печатать физиономии давно умерших президентов или национальные достопримечательности на дорогой бумаге.

Утром после игры в покер, когда остальные гости собирались уходить, Эрик Вурхис сидел у причала для яхт за домом Морхэда. Вчерашняя радость покинула его. Оторвавшись на секунду от размышлений, он сказал, что решил отказаться от должности исполнительного директора своего же панамского биткойн-стартапа. Его позиция в компании не позволяла ему рассказывать о революционном потенциале Биткойна, потому что это могло навредить бизнесу.

«Моя подлинная страсть – это не развитие бизнеса, а создание криптовалютного мира», – пояснил он.

Кроме того, его подруге надоело жить в Панаме, да и сам Эрик скучал по семье в США. Он планировал перебраться через несколько недель в Колорадо, где вырос. Однако благодаря Биткойну он вернется домой совсем другим человеком. То же самое вполне могли бы сказать о себе и многие его новообретенные друзья.

Часть I

Глава 1

10 января 2009 года

В этот субботний день у Хэла Финни был праздник – день рождения его сына. Погода в Санта-Барбаре была прекрасной, и в гости приехала сестра жены из Франции, но Хэл надолго застрял за компьютером. Этого дня он ждал много месяцев, а в каком-то смысле и почти всю жизнь.

Хэл редко делился со своей женой Фрэн подробностями работы. Как врач она мало что понимала в его компьютерных делах. Вот и на этот раз он даже не пытался что-то объяснить. Да и что бы он сказал? «Дорогая, я собираюсь поучаствовать в создании нового вида денег?»

А ведь именно такими были его намерения, когда после утренней пробежки он расположился за компьютером в своем скромном домашнем офисе – уголке гостиной со старым столом, на котором громоздились четыре разномастных монитора, подключенных к жужжащим компьютерным блокам. Во всех местах, не занятых компьютерным оборудованием, возвышались стопки бумаг, книги и старые руководства по программированию. Сидя за столом, Хэл мог видеть примыкающее к гостиной патио, даже в середине января щедро залитое калифорнийским солнцем. Слева от него на ковре лежал Арки, преданный пес, названный в честь звезды в созвездии Волопаса – Арктур. Здесь Хэл чувствовал себя дома и именно здесь он написал большинство своих программ.

Он запустил свой громоздкий IBM ThinkCentre, устроился поудобнее и щелкнул на ссылке, которую получил по электронной почте днем ранее. Еще несколько секунд, и на экране появилась главная страница сайта www.bitcoin.org.

Хэл узнал о Биткойне пару месяцев назад из сообщения, отправленного в одну из многочисленных почтовых рассылок, на которые он был подписан. Хэл много лет знал большинство участников этой специализированной группы для программистов, но то письмо было отправлено незнакомцем. Некто по имени Сатоши Накамото описывал «электронную наличность» со звучным названием «Биткойн». Хэл давно экспериментировал с цифровыми деньгами – достаточно для того, чтобы скептически отнестись к очередной подобной идее, – но все же что-то в этом письме привлекло его внимание. Сатоши описывал цифровые наличные, для работы которых не требовалось ни банка, ни какого-либо другого посредника. Предлагаемая им система могла функционировать за счет работы компьютеров рядовых пользователей. Хэла особенно заинтересовало заявление Сатоши о том, что пользователи могут владеть биткойнами и отправлять их друг другу, не предоставляя своих персональных данных никаким центральным организациям. Хэл и сам бóльшую часть профессиональной жизни посвятил разработке программ, помогавших людям защититься от всевидящего и всепроникающего ока «Большого брата».

Девятистраничный документ Сатоши, написанный в строгом академическом стиле, вызвал у Хэла неподдельный прилив энтузиазма. «Когда был запущен сайт Wikipedia, я думал, что из этого ничего не выйдет, но проект оказался очень успешным, и во многом по тем же причинам», – написал он в группу. Однако остальные участники переписки отнеслись к предложению скептически.

Хэл посоветовал Сатоши запрограммировать описанную им систему, чтобы проверить ее потенциал в действии. Через несколько месяцев, как раз в этот январский день, он скачал код Сатоши с веб-сайта Биткойна. Запустив обычный EXE-файл, Хэл установил биткойн-программу, и она автоматически открыла окно на рабочем столе его компьютера.

При первом же запуске программа сгенерировала для Хэла список биткойн-адресов и закрытый ключ – своеобразный пароль для доступа к каждому адресу. Кроме того, программа имела еще пару-тройку функций. Самая интересная, «Отправить монеты», была Хэлу недоступна, потому что у него еще не было никаких монет, которые можно было бы кому-то отправить. Увы, прежде чем Хэл смог поэкспериментировать с программой, она завершилась из-за какого-то сбоя.

Это не остановило Хэла. Просмотрев файлы журналов, он написал Сатоши письмо, в котором объяснил, что именно произошло, когда его компьютер попытался связаться с другими узлами сети. Как выяснилось, кроме компьютера Хэла к сети были подключены лишь два компьютера Сатоши с одним и тем же IP-адресом, принадлежащим калифорнийскому интернет-провайдеру.

Вскоре Сатоши прислал ответ, в котором не скрывал своего разочарования. Он написал, что тщательно тестировал весь код и давно не сталкивался с какими-либо проблемами. Причиной сбоя могло стать лишь то, что он сжал программу, чтобы ускорить ее передачу по сети. «Видимо, я зря это сделал», – написал Сатоши и предложил продолжить эксперимент.

Сатоши отправил Хэлу одну из прежних версий программы и поблагодарил его за помощь. Эта программа тоже завершилась сбоем, но Хэл не привык отступать. Наконец ему удалось запустить код на компьютере с другой операционной системой. Когда все заработало, он выбрал в меню наиболее интригующую команду, «Генерировать монеты». Как только он это сделал, вентилятор процессора в его компьютере заметно ускорился и зашумел.

Довольный собой, Хэл решил сделать перерыв и присоединиться к семейному празднику. В инструкциях, которые Сатоши выслал вместе с программой, говорилось, что на генерирование монет могут потребоваться «дни или месяцы, в зависимости от производительности компьютера и конкуренции среди участников сети». Хэл уведомил Сатоши, что все работает и что он пока не будет выключать компьютер с запущенным на нем биткойн-узлом.

К тому времени Хэл прочитал достаточно, чтобы понять, что делает его компьютер. Как только биткойн-программа запустилась, она зарегистрировалась в специальном канале чата, чтобы найти другие компьютеры, на которых выполнялось такое же ПО, – в то время там были только компьютеры Сатоши. Все подключенные к биткойн-сети компьютеры пытались получить новые биткойны, которые создавались пакетами по 50 монет. Каждый новый пакет биткойнов отправлялся тому пользователю, который выиграл последний раунд своеобразного конкурса на решение специальной вычислительной задачи. Когда один из компьютеров побеждал в очередном раунде конкурса и получал новые монеты, все остальные узлы сети обновляли свою копию данных о количестве биткойнов, принадлежащих владельцу соответствующего адреса. После этого узлы сети автоматически приступали к решению очередной задачи в попытке выиграть следующий пакет из 50 монет.

Вернувшись вечером к компьютеру, Хэл увидел, что тот в его отсутствие заработал 50 биткойнов, которые были зачислены на один из его биткойн-адресов и зарегистрированы в общедоступном журнале, служащем для отслеживания всех когда-либо созданных биткойнов. Этот блок стал 78-м по счету, и хотя на тот момент заработанные Хэлом биткойны не стоили

ровным счетом ничего, это ничуть его не смутило. В поздравительном письме к Сатоши, копию которого Хэл отправил в группу подписчиков, он позволил себе немного помечтать.

> «Представьте, что Биткойн станет главной платежной системой в мире, – дал он волю фантазии. – Тогда его общая стоимость сравняется со стоимостью всего богатства в мире».

По его подсчетам в этом случае каждый биткойн должен был бы стоить около 10 миллионов долларов.

«Даже если шансы Биткойна достичь такого уровня призрачны, неужели они меньше, чем 1 против 100 миллионов? – написал он, прежде чем покинуть группу. – Есть над чем подумать».

ХЭЛ ФИННИ давно интересовался тем, как технологии формируют облик будущего.

Один из четверых детей инженера-нефтяника, Хэл в юности прочитал много классических научно-фантастических романов, позже перешел на книги по высшей математике и в итоге поступил на учебу в Калифорнийский технологический институт. Сложные задачи никогда не пугали его, а скорее раззадоривали. Достаточно сказать, что уже в первый год учебы в институте он записался на курс по теории гравитационного поля, предназначенный для аспирантов.

Но он не был и типичным компьютерным гиком. Высокий и атлетично сложенный, Хэл любил покататься на лыжах в калифорнийских горах и не имел никаких проблем с социальной адаптацией, бывших частым явлением среди студентов Калтеха. Активный творческий дух распространялся и на интеллектуальные увлечения Хэла. Читая романы Ларри Нивена, в которых обсуждалась возможность замораживания людей с целью их последующей реанимации, Хэл не просто оценивал реалистичность таких технологий. Он нашел фонд продления жизни Alcor, который занимался подобными исследованиями, и подписался на его журнал. Позднее он заплатит за сохранение своего тела и тел членов его семьи в криохранилищах Alcor неподалеку от Лос-Анджелеса.

Изобретение Интернета Хэл воспринял как величайшее благо: сеть позволила ему свободно общаться с теми немногими людьми, которые увлекались подобными радикальными идеями. Еще до появления первого веб-браузера Хэл вступил в интернет-сообщества «шифропанков» и «экстропианцев», участники которых страстно обсуждали возможные способы влияния на будущее с помощью технологий.

Мало что волновало участников этих групп больше, чем вопрос, как технологии изменят баланс власти между корпорациями и государствами с одной стороны и отдельными людьми – с другой. Безусловно, информационные технологии предоставили людям беспрецедентные возможности продвижения своих взглядов и поиска единомышленников. Но в то же время постепенное проникновение цифровых технологий в нашу жизнь позволило государствам и крупным компаниям усилить контроль над наиболее ценным и опасным товаром информационной эпохи – самой информацией.

Конечно, правительства всех стран пытались следить за своими гражданами и в докомпьютерную эпоху, но собрать много информации о большинстве людей было просто невозможно. Однако уже в 1990-е годы – задолго до того как выяснилось, что АНБ прослушивает телефонные разговоры обычных граждан, а политика конфиденциальности Facebook стала предметом национальных дебатов – шифропанки ясно увидели, что компьютеризация всех сфер жизни значительно упрощает для властей сбор сведений о людях и манипулирование ими. Больше всего шифропанков беспокоил вопрос, как люди могут защитить свою личную информацию и конфиденциальность. Достаточно сказать, что «Манифест шифропанка», который в 1993 году опубликовал Эрик Хьюз, математик из Беркли, начинается словами «В электронную эпоху конфиденциальность стала для открытого общества необходимостью».

Эти воззрения во многом произрастали из либертарианских взглядов, которые приобрели популярность в Калифорнии в 1970- и 1980-е годы. Подозрительное отношение к государству было естественным для программистов, которые на работе самостоятельно создавали новый мир, не полагаясь на чью-либо помощь. Хэл проникся этими идеями еще в Калтехе, отчасти благодаря романам Айн Рэнд. Однако проблема конфиденциальности в эпоху Интернета вызывала немалый интерес и вне либертарианских кругов, в том числе среди защитников прав человека и активистов других протестных движений.

Конечно, никто из шифропанков не призывал к отказу от технологий – напротив, именно в технологиях, а особенно в науке о шифровании (криптографии) они видели решение проблемы. Шифрование исторически было привилегией лишь самых влиятельных организаций. Частные лица могли попытаться кодировать свои данные тем или иным способом, но спецслужбы и военные прекрасно научились взламывать такие шифры. Однако в 1970- и 1980-е годы математики из Стэнфорда и MIT сделали ряд открытий, которые впервые в истории позволили обычным людям шифровать сообщения так, что их невозможно было взломать даже с помощью самых мощных суперкомпьютеров. Новая технология получила название «криптография с открытым ключом».

Чтобы зашифровать данные с ее помощью, пользователь должен сгенерировать открытый ключ – уникальное случайное сочетание букв и чисел, служащее чем-то вроде адреса, который можно свободно сообщать кому угодно – и соответствующий закрытый ключ, который нужно сохранить в секрете. Эти два ключа связаны математическим отношением, которое гарантирует, что только обладатель закрытого ключа – Алиса, как ее традиционно зовут криптографы – может расшифровывать сообщения, отправленные ее открытому ключу. Уникальное отношение между открытым и закрытым ключами определяется с помощью сложных математических уравнений, которые исключают возможность вычислить закрытый ключ по открытому даже на самом мощном суперкомпьютере. Подобные криптографические хитрости позже будут положены в основу Биткойна.

Хэл узнал о потенциале криптографии с открытым ключом в 1991 году благодаря Дэвиду Чому – талантливому криптографу, который экспериментировал с технологиями защиты конфиденциальности.

«Все показалось мне совершенно очевидным, – рассказывал Хэл другим шифропанкам о своем первом впечатлении от работы Чома. – Мы думаем, как решить проблемы утраты конфиденциальности, всеобъемлющей компьютеризации, централизации баз данных, но ищем решения не там, где следует. Чом предлагает двигаться в другом направлении, чтобы отнять власть у правительств и корпораций, наделив ею простых людей».

Как обычно, обнаружив новую захватывающую идею, Хэл не ограничился чтением о ней, а начал в свободное время помогать проекту PGP (Pretty Good Privacy). Участники проекта разрабатывали ПО, позволявшее отправлять и получать сообщения, зашифрованные с помощью криптографии с открытым ключом. Основатель PGP Фил Циммерман был категорическим противником ядерного оружия и хотел, чтобы диссиденты могли общаться без контроля со стороны государства. В скором времени Циммерман принял Хэла на работу в PGP.

Идеалистические проекты наподобие PGP обычно получают совсем малую известность, но и ее оказалось достаточно, чтобы федеральная прокуратура инициировала уголовное расследование относительно деятельности Циммермана и PGP. Дело в том, что ранее правительство США засекретило надежные технологии шифрования, что сделало их экспорт нелегальным. Хотя иск в итоге был отозван, Хэлу пришлось годами скрывать свое участие в работе над PGP, из-за чего его вклад в проект так и не получил должного признания.

БОРЬБА ЭКСТРОПИАНЦЕВ и шифропанков с традиционными формами власти принимала разные формы, но все же с самого начала в центре их внимания были деньги. Для рыночной экономики деньги – это такой же базовый элемент, как вода или огонь для человечества. Представить экономику без денег практически невозможно. Все существовавшие валюты, действительные только в пределах конкретного государства и контролируемые некомпетентными банкирами, казались программистам-шифропанкам безнадежно устаревшими и ограниченными, особенно в сравнении с возможными альтернативами. Далеко ходить за примерами не требовалось: во многих научно-фантастических романах, на которых выросли Хэл и его соратники, описывались те или иные универсальные деньги, например в «Звездных войнах» это были галактические кредиты.

Даже если вынести за скобки эти причудливые амбиции, шифропанки видели в финансовой системе одну из опаснейших угроз для конфиденциальности. Мало что характеризует человека точнее, чем его финансовые операции. Получив доступ к выпискам по кредитной карте, можно узнать, чем увлекается ее владелец, какие магазины и рестораны посещает, что для него важно и что ему безразлично… Неслучайно финансовые записи – один из главных способов отслеживания беглых преступников. В «Манифесте шифропанка» Эрик Хьюз описывает проблему гораздо подробнее: «Если механизмы транзакции таковы, что моя личность раскрывается, значит, конфиденциальности у меня нет. У меня нет возможности раскрывать себя избирательно, я вынужден делать это всегда… Для сохранения конфиденциальности в открытом обществе требуются системы анонимных транзакций».

Анонимные платежи возможны испокон веков благодаря наличным деньгам, но мы не смогли взять с собой наличные в цифровой мир. Как только деньги переводились в цифровую форму, они попадали под контроль банков или других организаций, которые получали возможность с легкостью отслеживать транзакции. Чего хотели Хэл, Чом и шифропанки, – так это создать наличные для цифровой эпохи, которые были бы безопасными и защищенными от подделки, но при этом не вынуждали людей жертвовать конфиденциальностью. В тот же год, когда Хьюз опубликовал свой манифест, Хэл отправил в группу единомышленников сообщение с описанием цифровых наличных, позволяющих не хранить никакие записи о том, где и на что кто-то их потратил. Предполагалось, что банк будет лишь знать, сколько денег его клиент снял за конкретный месяц. Хэл даже придумал для цифровых наличных звучное название: «CRASH», или «CRypto cASH».

К тому времени, когда проблемой финансовой конфиденциальности заинтересовались шифропанки, Чом уже изобрел DigiCash – интернет-деньги, которые можно было тратить без обнародования каких-либо личных сведений. Для сохранения личности в секрете в DigiCash использовались так называемые слепые подписи, также основанные на криптографии с открытым ключом. Когда один из американских банков решил поэкспериментировать с DigiCash, Хэл тут же открыл в нем счет.

К сожалению, работы Чома обозначили не совсем правильный путь к решению проблемы. В DigiCash каждую цифровую подпись должна была проверять центральная организация, принадлежавшая Чому, а это означало, что она требовала доверия со стороны потенциальных клиентов. Когда компания Чома обанкротилась в 1998 году, с ней пришел конец и всему проекту DigiCash. Этот печальный опыт показал, что никакая центральная организация не должна контролировать цифровые наличные. На первый взгляд, проблема казалась нераз-

решимой: если бы никакая организация не контролировала цифровые деньги, ничто не мешало бы людям тратить их дважды, ведь скопировать данные в цифровом мире проще простого. Некоторые из шифропанков сочли задачу неразрешимой и оставили проект, но Хэл не привык отступать.

Как ни странно, человек, приложивший столько усилий ради создания нового вида денег, вовсе не стремился к богатству: PGP и другие программы, которые писал Хэл, распространялись в основном бесплатно. Его недоверие к государству также не было обусловлено желанием уклониться от уплаты налогов; напротив, в 1990-е годы Хэл каждый год выплачивал налоги с полного дохода, не пользуясь какими-либо вычетами или льготами, чтобы как можно меньше возиться с бумагами. Много лет он прожил в скромном домике на окраине Санта-Барбары. Казалось, его совершенно не заботит то, что он вынужден работать в углу своей гостиной или что обивка на его кресле прохудилась. Хэл был движим, прежде всего, интеллектуальным любопытством, которое буквально сочилось из каждого написанного им письма, и осознанием права каждого человека на достойную жизнь.

«Главная цель того, чем мы занимаемся, – это отправить Большого брата на свалку истории, – писал Хэл своим единомышленникам. – Не стоит недооценивать эту задачу. Возможно, когда-нибудь мы оглянемся и увидим, что это было самое важное из всего, что мы сделали».

Глава 2

1997 год

Создание денег нового типа может показаться странным и бессмысленным начинанием. Большинство людей в современном мире даже не могут представить себе деньги, отличные от выпускаемых государством купюр и монет. Право печатать деньги – один из фундаментальных признаков суверенного государства, пусть даже такого крошечного, как Ватикан или Микронезия.

Однако так было не всегда. До гражданской войны в США почти все американские деньги выпускали частные банки, что создавало сумасшедшую финансовую мозаику из конкурирующих купюр, которые могли потерять всю свою ценность в случае банкротства банка-эмитента. Многие государства в те времена вообще использовали во внутренней торговле монеты других стран.

Еще раньше люди пробовали использовать в качестве денег золото, ракушки и даже каменные диски. Поиск лучших форм денег всегда в той или иной мере был связан со стремлением изобрести более точный и надежный способ оценки стоимости окружающих нас вещей – единую метрику, которая позволяла бы с легкостью сравнивать ценность поленницы дров, часа работы плотника и написанного художником пейзажа. Как сказал социолог Найджел Додд, хорошие деньги «преобразуют качественные различия вещей в количественные различия, позволяя обмениваться ими».

В своих исследованиях шифропанки пытались довести стандартизирующую функцию денег до логического завершения, чтобы создать универсальные деньги, которые можно было бы тратить везде, не обменивая на новые бумажки на каждой границе. Шифропанки прекрасно знали свойства, присущие успешным деньгам. Хорошие деньги должны быть долговечными (только представьте себе доллар, напечатанный на салфетке), портативными (представьте монету весом в 20 килограммов), делимыми (если бы у нас были только стодолларовые купюры и не было монет, экономике тут же пришел бы конец), единообразными (если бы все купюры выглядели по-разному, пользоваться ими было бы невозможно) и редкими (если бы купюры было легко скопировать, они не имели бы никакой ценности).

И все же, помимо всех этих качеств, для создания денег всегда требовалось что-то неуловимое, а именно – доверие со стороны использующих их людей. Чтобы фермер был готов принимать доллары за выращенный урожай, он должен верить в то, что они не утратят ценность через месяц или год. Как показало время, наиболее важным свойством денег является не то, кто их выпустил, и даже не то, насколько они портативны или долговечны, а количество людей, готовых их использовать.

В XX веке доллар получил и сохранил статус глобальной валюты во многом потому, что большинство людей в мире считали, что США и их финансовая система имеют лучшие шансы

выстоять в любых кризисах, чем другие страны. Это объясняет, почему многие люди предпочитают хранить свои сбережения в долларах.

Связь денег с доверием наделяет людей, уполномоченных создавать и защищать деньги, почти религиозным статусом. Само слово «деньги» («money») происходит от имени римской богини Юноны Монеты, в храме которой монеты и выпускались. В США к руководителям Федерального резерва, которые управляют денежной системой, относятся, как к оракулам, – сотни, если не тысячи, экспертов анализируют их заявления так же тщательно, как когда-то пророки изучали внутренности жертвенных животных. Чиновники Федорезерва настолько влиятельны и независимы, что им могли бы позавидовать любые госчиновники, а защита национальной валюты США доверена специально созданному агентству, Секретной службе, которой лишь намного позже в довесок поручили еще и охранять президента США.

Самый известный глава Федерального резерва, Алан Гринспен, знал, что деньги могут создавать не только центробанки. В 1996 году, когда шифропанки с головой погрузились в свои эксперименты, Гринспен заявил, что технологическая революция может привести к возврату частных денег и что он не видит в этом ничего плохого.

> «Вполне возможно, что в ближайшем будущем эмитенты электронных платежных обязательств, таких как карты предоплаты или „цифровые наличные“, смогут создать специализированные корпорации с надежными балансами и открытыми кредитными рейтингами».

В годы, последовавшие за этим заявлением Гринспена, мир шифропанков буквально бурлил от кипевшей в нем активности. В 1997 году британский исследователь Адам Бек опубликовал в почтовой рассылке для шифропанков описание проекта Hashcash, который решил проблему неограниченного копирования цифровых денег. Позднее идея Бека стала важным элементом Биткойна.

Проект Бека был основан на еще одной концепции из мира криптографии, а именно – на криптографических хеш-функциях. Так называют математические уравнения, которые легко решить, но почти невозможно восстановить, зная ответ. Например, числа 2903 и 3571 можно легко перемножить с помощью карандаша и бумаги, но чтобы вручную разложить число 10 366 613 на эти множители, нужно по-настоящему постараться. Именно этот принцип лег в основу Hashcash, хотя задачи, назначаемые узлам Hashcash, были гораздо сложнее, чем нахождение множителей числа 10 366 613. Когда компьютер, перепробовав множество догадок, находил в итоге правильный ответ к задаче Hashcash, он зарабатывал некоторое количество монет.

Применение такого алгоритма стало важным шагом потому, что он гарантировал редкость Hashcash. Как мы уже выяснили, редкость – важное свойство успешных денег, но исключить дублирование файлов не так-то просто, ведь именно легкостью копирования данных славится цифровой мир. Для создания каждого нового блока Hashcash компьютер должен был выполнять много работы, что дало новому алгоритму название «подтверждение работы» (именно этот процесс позднее станет одной из главных инноваций в Биткойне). Главная проблема системы Бека состояла в том, что каждую единицу Hashcash можно было использовать лишь однократно. Из-за этого каждый участник должен был создавать новые монеты всякий раз, когда он хотел совершить какую-то операцию. Другой проблемой было то, что пользователь, располагающий большой вычислительной мощностью, мог создавать для себя все больше и больше единиц Hashcash, сокращая ценность каждой монеты.

Через год после выпуска программы Бека два участника шифропанковского сообщества независимо друг от друга разработали цифровые токены с подтверждением работы, которые можно было использовать повторно. Одну из систем, названную «bit gold», изобрел Ник Сабо, эксперт по безопасности. Он поделился своими идеями с единомышленниками вроде Хэла Финни в 1998 году, но не попытался реализовать проект на практике. Другую

систему, получившую название «b-money», придумал американец по имени Вэй Дай. Хэл тоже создал собственный вариант подобной системы, но не стал напрягать фантазию и назвал ее «RPOW» («повторно используемые подтверждения работы»).

Обсуждение этих идей в сообществе для шифропанков и похожих группах иногда напоминало перебранки конкурентов, пытающихся обойти друг друга в своеобразном состязании. Особенно усердствовал Сабо, который находил множество изъянов в чужих предложениях, чрезмерно, по его мнению, привязанных к специализированному компьютерному оборудованию. Однако все шифропанки испытывали глубокое уважение друг к другу, и, несмотря на многие неудачные эксперименты, их амбиции вскоре вышли за пределы создания анонимных денег. Бек, Сабо, Финни и другие участники стали уделять больше внимания дефектам финансовой системы, взимающей огромные комиссии за любые транзакции и при этом неспособной быстро перевести деньги в другую страну.

«Мы хотим создать полностью анонимные средства обмена с минимальной комиссией, – написал Бек вскоре после выпуска Hashcash. – Если у нас это получится, банки постигнет участь динозавров, чего они в полной мере заслужили».

В 1999 году Нил Стивенсон опубликовал книгу «Криптономикон», и у шифропанков, наконец, появился идеал, на который они могли ориентироваться. В этом романе, получившем в хакерском сообществе культовый статус, описан теневой мир со своеобразным цифровым золотом, позволяющим людям сохранять свою личность в тайне. Роман включает подробные описания криптографических схем, благодаря которым это возможно.

Однако в реальном мире эксперименты шифропанков были гораздо менее успешными. Ни у кого не получалось создать деньги, не полагаясь на центральные организации, которые, как все уже прекрасно поняли, подвержены кризисам, сбоям в работе и могут быть уничтожены государством. Со временем обозначилась и более фундаментальная проблема – как убедить людей использовать и ценить эти цифровые токены. К моменту, когда на сцене появился Сатоши Накамото, многие потенциальные сторонники Биткойна уже устали от неудач. Создание цифровых денег стало казаться такой же несбыточной мечтой, как преобразование свинца в золото.

В АВГУСТЕ 2008 ГОДА Сатоши написал Адаму Беку письмо, в котором просил его взглянуть на краткое описание чего-то под названием «Биткойн». Бек не слышал ни о Биткойне, ни о Сатоши и, по большому счету, проигнорировал письмо, но все же указал Сатоши на другие эксперименты шифропанков, которые тот мог пропустить.

Шестью неделями позже, на Хэллоуин, Сатоши отправил более подробное описание своего проекта в специализированную академическую рассылку, посвященную криптографии. Рассылка для шифропанков к тому времени приказала долго жить, но большинство ее участников следили за криптографическими новостями. В типичном для сообщества стиле Сатоши ничего не сообщил о себе, а спрашивать об этом среди криптографов не принято – для них важны идеи, а не личности высказывающих их людей. В своем письме, написанном сухим лаконичным языком, Сатоши смело заявлял, что решил многие из проблем, препятствовавших созданию универсальных денег. «Я работаю над электронной пиринговой денежной системой, не нуждающейся в доверенных сторонних организациях», – так начиналось письмо.

Прикрепленный к письму девятистраничный PDF-файл ясно давал знать, что Сатоши прекрасно осведомлен обо всех предыдущих усилиях по созданию автономных цифровых денег. В своем документе Сатоши цитировал Бека, Вэя Дая и приводил выдержки из нескольких малоизвестных журналов по криптографии. Собрав идеи многих своих предшественников, Сатоши каким-то образом умудрился объединить их в систему, которая радикально отличалась от всего, что было предложено до него.

Вместо того чтобы доверять эмиссию и отслеживание денег центральной организации, как это реализовано в существующей финансовой системе и в DigiCash Чома, Сатоши предложил отслеживать все биткойн-транзакции с помощью общедоступной базы данных, совместно обслуживаемой самими пользователями новых денег.

Впоследствии даже экспертам потребовались месяцы, чтобы разобраться в нюансах работы Биткойна, но базовые элементы системы можно за пару десятков минут объяснить любому человеку. На таком уровне и была написана работа Сатоши, которую впоследствии стали называть официальным документом Биткойна.

Согласно этому документу каждый пользователь Биткойна может создать один или несколько общедоступных биткойн-адресов – аналогов банковских счетов – и по одному закрытому ключу для каждого адреса. Монеты, связанные с конкретным адресом, может потратить только владелец закрытого ключа, соответствующего этому адресу. Закрытый ключ несколько отличается от традиционного пароля, который обычно хранится в некоторой центральной организации, проверяющей, имеет ли пользователь право на доступ к ресурсу. В Биткойне Сатоши задействовал чудеса криптографии с открытым ключом, чтобы уже знакомая нам Алиса могла подписывать свои транзакции, не сообщая никому свой закрытый ключ.

Итак, подписав транзакцию закрытым ключом, Алиса отправляет ее остальным узлам биткойн-сети, которые затем проверяют, действительно ли у Алисы есть монеты, которые она пытается потратить. Они проверяют платежеспособность Алисы, сверяясь с общедоступным журналом всех биткойн-транзакций – так называемым блокчейном, копию которого может хранить у себя каждый узел сети. Убедившись, что по адресу Алисы действительно хранится нужная сумма, компьютеры-узлы подтверждают транзакцию и добавляют ее в список («блок») недавних биткойн-транзакций.

Пожалуй, самой сложной частью системы является алгоритм добавления блоков с транзакциями в блокчейн. Он представляет собой что-то вроде соревнования между биткойн-узлами, которое во многом напоминает решение задачи, придуманной Адамом Беком для Hashcash. Компьютер, победивший в конкурсе, получает право записать блок недавних транзакций в блокчейн. Зачем ему эта сомнительная честь? Дело в том, что победитель конкурса также получает в награду новые биткойны, и это единственный способ эмиссии новых биткойнов в системе. Именно награда в виде новых монет мотивирует пользователей направлять вычислительные ресурсы своих компьютеров на обработку биткойн-транзакций.

При возникновении разногласий по поводу того, какой компьютер победил в конкурсе, приоритет отдается блоку, принятому большинством узлов сети. Например, если большинство узлов считает, что в последнем раунде конкурса победила Алиса, но какие-то узлы-диссиденты отдают победу Бобу, сторонники Алисы будут игнорировать блоки от компьютеров, поддержавших Боба, пока те не присоединятся к большинству. Этот поистине демократичный способ принятия решений хорош тем, что он предотвращает махинации со стороны «плохих» узлов, которые могли бы попытаться записать на свои счета много новых биткойнов. Благодаря реализованной в Биткойне защите злоумышленникам, задумавшим неладное, пришлось бы заручиться поддержкой большинства узлов сети.

Решения об изменении ПО, работающего на биткойн-узлах, также принимаются демократически. Любой пользователь может внести изменение в ПО Биткойна (исходный код которого открыт), но изменения вступят в силу только в том случае, если новая версия ПО будет

установлена на большинстве компьютеров в сети. Если один компьютер ни с того ни с сего перейдет на другую версию ПО, другие узлы просто станут игнорировать его.

Давайте подытожим сказанное, кратко описав процесс в пяти шагах.

1. Алиса инициирует перевод биткойнов со своего счета, подписав транзакцию своим закрытым ключом и сообщив о ней остальным пользователям сети.

2. Узлы сети убеждаются в том, что по адресу Алисы достаточно средств, и добавляют транзакцию в список (блок) недавних транзакций.

3. Компьютеры-узлы соревнуются за право добавить блок в блокчейн.

4. Компьютер, победивший в конкурсе, удостаивается права добавить блок в блокчейн и получает в награду новые биткойны.

5. Компьютеры составляют новый список неподтвержденных транзакций, и начинается новый раунд конкурса.

Объединение всех этих процессов дает нам нечто, чего никогда ранее не существовало, – финансовую сеть, способную создавать и перемещать деньги без банков, эмитентов кредитных карт, регуляторов и вообще каких бы то ни было центральных организаций. Система спроектирована так, чтобы никто, кроме владельца закрытого ключа, не мог потратить деньги, связанные с конкретным биткойн-адресом. Более того, в любой момент времени существует один и только один общедоступный неизменяемый журнал со сведениями о суммах, принадлежащих каждому участнику системы. Чтобы пользоваться Биткойном, не нужно верить Сатоши, в отличие от DigiCash или доллара, которые вынуждают их пользователей доверять Дэвиду Чому или Федеральному резерву. ПО узлов Биткойна работает на собственных компьютерах пользователей, а написанный Сатоши код открыт, и кто угодно при наличии соответствующих знаний и навыков может проверить, все ли с ним в порядке. Если кому-то из пользователей не нравится что-то в правилах, реализованных в Биткойне, никто не мешает ему изменить правила и попытаться убедить других пользователей следовать им. Пользователи биткойн-сети в буквальном смысле являются и клиентами, и владельцами монетного двора и банка. Однако на момент публикации предложения Сатоши ничего этого в реальности еще не существовало. Он лишь вынес на обсуждение описание своей революционной схемы.

Несмотря на все описанные в документе инновации, за неделю, прошедшую после его публикации, он получил всего лишь два отзыва, и оба отрицательных. Джон Левин, известный эксперт в вопросах компьютерной безопасности, заявил, что хакеры-злоумышленники легко смогут подделать блокчейн. «У хороших ребят гораздо меньше вычислительной мощности, чем у плохих, – написал он 2 ноября. – Есть и другие моменты, которые кажутся мне сомнительными, но и одного этого достаточно, чтобы поставить на проекте крест».

Опасения Левина были обоснованными, потому что в системе Сатоши предполагалось, что компьютеры принимают решения большинством голосов. На ранних этапах развития сети, пока в ней еще было мало компьютеров, злоумышленники легко могли бы получить контроль над сетью. Однако Сатоши надеялся, что в начале ни у кого не будет серьезной мотивации захватывать контроль над системой. Ну а если такая мотивация возникнет позднее, то сеть к тому моменту привлечет достаточно участников, чтобы организовать такую атаку стало гораздо труднее.

Другой ветеран шифропанковских дискуссий, Джеймс Дональд, заявил, что такая система нужна всем как воздух, но блокчейн быстро станет слишком большим, из-за чего пользователи не захотят загружать его из сети.

В последующие недели Хэл оставался единственным защитником Сатоши. Он написал, что почти не беспокоится по поводу атак, о которых упомянул Левин, но при этом признал,

что не знает, как система проявит себя на практике, и выразил желание увидеть реальный компьютерный код, а не концептуальное описание.

«Идея кажется оригинальной и многообещающей, и мне очень хотелось бы увидеть ее дальнейшее развитие», – написал он в сообществе.

Вероятно, то, что Хэл встал на защиту Биткойна, и побудило Сатоши отправить ему раннюю бета-версию ПО для тестирования. В ходе нескольких тестовых запусков в ноябре и декабре они выявили и устранили несколько багов, и в январе 2009 года Сатоши отправил полный код системы в криптографическое сообщество.

Окончательная версия кода немного отличалась от оригинального документа и содержала несколько интересных дополнений. Например, в коде было прописано, что новые монеты будут выпускаться примерно каждые 10 минут, а при сокращении этого интервала из-за роста общей вычислительной мощности сети хеш-функция, вычисляемая в конкурсе, будет становиться сложнее.

Кроме того, в коде окончательно определялся график эмиссии биткойнов. Сатоши решил, что в первые 4 года победитель в гонке за право создать новый блок будет получать 50 монет, после чего каждые 4 года награда будет уменьшаться вдвое, пока объем эмиссии не достигнет окончательного значения в 21 миллион биткойнов.

Когда Хэл запустил биткойн-узел в первый раз, сеть уже работала. В следующие несколько дней не случилось ничего примечательного. Каждые 10 минут один из компьютеров (обычно компьютер Сатоши) выигрывал 50 монет. Однако воскресным вечером в блокчейне была зарегистрирована первая транзакция – в рамках тестирования Сатоши отправил Хэлу 10 биткойнов. Чтобы выполнить транзакцию, Сатоши подписал ее своим закрытым ключом, отправил в сеть (состоявшую на тот момент только из компьютеров Хэла и Сатоши), и несколько минут спустя транзакция была сохранена в блокчейне, когда один из компьютеров Сатоши победил в очередном раунде конкурса. Любой, кто после этого устанавливал биткойн-узел на своем компьютере, мог видеть в блокчейне запись о 10 монетах, которые Сатоши перевел Хэлу.

В первые недели потенциальные пользователи не торопились присоединяться к сети, поэтому для ее обслуживания Сатоши использовал собственные компьютеры. Он также делал все возможное для популяризации Биткойна и старался быстро отвечать всем, кто проявлял хотя бы малейший интерес к проекту. Когда однажды ночью какой-то программист из Техаса написал Сатоши письмо, в котором продемонстрировал знание цифровых денег и криптографии, он получил ответ уже утром.

«У нас определенно схожие интересы, – написал Сатоши с явным энтузиазмом, прежде чем пожаловаться на отсутствие какого-либо интереса к Биткойну. – Знаете, мне кажется, что в девяностые этой темой интересовалось гораздо больше людей, но после многолетних неудачных попыток создать систему с доверием к сторонним организациям (DigiCash и т. д.) они сочли дело безнадежным. Надеюсь, они поймут, чем уникально мое предложение. Насколько мне известно, это первая попытка создать финансовую систему без доверия».

Пока что все выглядело так, что программа Сатоши была всего лишь очередным набором кода, готовым разделить печальную участь многих других перспективных, но заброшенных и всеми забытых проектов. Чтобы выжить, Биткойн должен был как-то привлечь больше пользователей и защитников вроде Хэла, но вступать в их ряды никто особенно не торопился. Скорее наоборот: через неделю после выпуска программы один из участников криптографического сообщества написал, что никакое государство не позволит Биткойну в его текущей форме достигнуть мало-мальски значимых размеров.

Хэл признал, что автор этого сообщения может оказаться прав, но снова выступил в защиту Сатоши. «В пользу Биткойна говорит следующее, – написал Хэл. – Он распределен и не имеет единой точки сбоя, в нем нет монетного двора, и он не принадлежит никакой компа-

нии, сотрудников которой можно было бы привлечь к ответственности, заставить замолчать или арестовать».

Однако казалось, что временами даже Хэл теряет энтузиазм. Слушая, как шумит его компьютер, пытающийся получить право сгенерировать новые монеты, он начал беспокоиться о том, сколько углекислого газа начнут выбрасывать все узлы, если Биткойн окажется успешным. Когда его сын Джейсон пожаловался на износ компьютера, Хэл вообще отключил функцию генерирования монет. Кроме того, выяснилось, что из-за открытости и доступности журнала транзакций – пусть даже каждый пользователь представлялся в нем непонятным адресом – Биткойн вовсе не так анонимен, как могло показаться.

А затем дело приняло совсем плохой оборот. У Хэла начались быстро прогрессирующие проблемы с речью, и вскоре все свое свободное время он был вынужден уделять общению с врачами. У него диагностировали боковой амиотрофический склероз – неизлечимый дегенеративный процесс, который приводит к увяданию всех мышц в теле. Ко времени, когда был поставлен диагноз, Хэл из-за свалившихся на него бед покинул биткойн-сообщество. Спустя месяцы он вернется ради нескольких памятных сообщений, но за это время он уже потеряет способность ходить; Биткойн же, напротив, прочно встанет на ноги.

Глава 3

Май 2009 года

В начале мая, через несколько месяцев после исчезновения Хэла Финни, Сатоши получил письмо, написанное на слишком правильном английском, обычно характерном для иностранцев.

Конец ознакомительного фрагмента.