18+

ЗАХВАТ БИТКОЙНА

СКРЫТАЯ ИСТОРИЯ BTC

РОДЖЕР ВЕР И Стив Паттерсон

Роджер Вер

Захват Биткойна. Скрытая история BTC

«Издательские решения»

Вер Р.

Захват Биткойна. Скрытая история BTC / Р. Вер — «Издательские решения»,

ISBN 978-5-00-657273-7

Биткойн обещал стать технологией, которая принесет свободу, станет рыночной альтернативой государственным валютам. Но это обещание не было выполнено после того, как небольшая группа инсайдеров захватила проект и кардинально изменила Биткойн.Мало кто знает подлинную истоию Биткойна и о его первоначальном дизайне из-за многолетней строгой цензуры и жесткого контроля информации в сети. Книга Захват Биткойна разрушает самые популярные представления о Биткойне и проясняет историческую картину.

ISBN 978-5-00-657273-7

Содержание

Захват Биткойна
Скрытая история BTC

Роджер Вер
Стив Паттерсон

Дизайнер обложки Феликс Диас де Эскауриас
Редактор Анастасия Полозова
Переводчик Дмитрий Бондаренко

ISBN 978-5-0065-7273-7
Создано в интеллектуальной издательской системе Ridero

Захват Биткойна

ЗАХВАТ БИТКОЙНА
СКРЫТАЯ ИСТОРИЯ BTC

РОДЖЕР ВЕР И СТИВ ПАТТЕРСОН

Опубликовано Роджером Вером

Написано в соавторстве со Стивом Паттерсоном

Взгляды, мысли и мнения, выраженные в этой книге, принадлежат исключительно автору, а не какой-либо другой группе или лицу. Сценарии, обсуждения и взгляды являются выражением мнения и не предназначены для окончательного анализа сложных механизмов работы Биткойна или криптовалютного рынка. Хотя исторические факты и повествования в этой книге основаны на исследованиях и личном опыте автора, они приводятся исключительно в информационных целях и не являются финансовыми, юридическими или профессиональными советами.

Автор приложил все усилия, чтобы обеспечить точность информации, содержащейся в этой книге, на момент публикации. Автор не принимает на себя и настоящим отказывается от любой ответственности перед любой стороной за любые потери, ущерб или сбои в работе, вызванные ошибками или упущениями, независимо от того, являются ли эти ошибки или упущения результатом небрежности, несчастного случая или любой другой причины.

Дизайн обложки: Феликс Диас де Эскауриас
Перевод на русский язык: Бондаренко Дмитрий
Редактор: Полозова Анастасия

Предисловие
От Джеффри Такера

История, которую вы прочтёте, – это трагедия, хроника денежной технологии, которая могла принести свободу, но была искажена ради других целей. Книгу, безусловно, больно читать, и впервые эта история рассказана с такими подробностями и во всех деталях. У нас был шанс освободить мир. Этот шанс был упущен, скорее всего, отнят и испорчен.

Те из нас, кто следил за Биткойном с первых дней его существования, с восхищением наблюдали за тем, как он набирает обороты и, казалось, предлагал жизнеспособный альтернативный путь будущего денег. Наконец-то, после тысячелетий коррупции правительств, у нас появилась технология, которая была неуязвимой, надёжной, стабильной, демократичной, неподкупной – воплощение видения борцов за свободу на протяжении всей истории. Наконец-то деньги можно было освободить от государственного контроля и таким образом достичь экономических, а не политических целей – процветания для всех, в противовес войне, инфляции и росту государственной машины и её влияния.

Во всяком случае, так было задумано. Увы, этого не произошло. Биткойн используется сегодня меньше, чем пять лет назад. Он находится не на траектории окончательной победы, а на пути постепенного роста цены для тех, кто приобрёл его раньше. Короче говоря, технология была предана из-за небольших изменений, которые в то время почти никто не понимал.

Уж точно, не я. Я пользовался Биткойном несколько лет и был глубоко поражён скоростью расчётов, низкой стоимостью транзакций, а также возможностью для любого человека, не имеющего банковского счёта, отправлять или получать Биткойн без посредников. Это чудо, о котором я восторженно писал в то время. Я организовал конференцию CryptoCurrency в Атланте, штат Джорджия, в октябре 2013 года, которая была посвящена интеллектуальной и технической стороне вопроса. Это была одна из первых национальных конференций по этой теме, но даже на ней я заметил, что формировались две стороны: те, кто верил в денежную конкуренцию, и те, кто был привержен развитию одного протокола.

Впервые я понял, что что-то пошло не так, через два года, когда впервые увидел, что сеть серьезно перегружена. Комиссии за транзакции взлетели, расчеты замедлились, а огромное количество способов входа и выхода закрывалось из-за высокой стоимости обслуживания. Я ничего не понимал. Я обратился к нескольким экспертам, которые объяснили мне, что в криптовалютном мире началась тихая гражданская война. Так называемые «максималисты» выступили против широкого распространения технологии. Им нравились высокие комиссии. Они не возражали против долгого времени расчетов. И многие из них приняли участие в работе криптовалютных бирж, число которых сократилось из-за репрессий со стороны правительства.

В то же время появлялись новые технологии, значительно повышающие эффективность и доступность обмена фиатных долларов. Среди них были Venmo, Zelle, CashApp, FB payments и многие другие, а также приложения для смартфонов и планшетов iPad, которые позволили магазинам любого размера принимать кредитные карты. Эти технологии полностью отличались от Биткойна, поскольку они были основаны на получении разрешения, их использование было возможно благодаря посредничеству финансовых компаний. Но для пользователей они казались отличными, и их присутствие на рынке вытеснило Биткойн в то самое время, когда моя любимая технология превратилась в неузнаваемую версию самой себя.

Форк Биткойна в Bitcoin Cash произошёл два года спустя, в 2017 году, и сопровождался резкими высказываниями и негодованием, как будто происходило что-то ужасное. На самом деле это было восстановление того, как задумывал технологию её основатель Сатоши Накамото. Он, как и исследователи монетарных политик прошлого, полагал, что ключ к превра-

щению любого товара в широко распространённые деньги – это принятие и использование. Невозможно даже представить себе условия, при которых любой товар мог бы принять форму денег, если бы не было жизнеспособного и востребованного на рынке способа его использования. Bitcoin Cash стал попыткой восстановить это.

Время для активного внедрения этой новой технологии наступило в 2013—2016 годах, но на тот момент было две сложности: намеренное ограничение способности технологии к масштабированию и натиск новых платёжных систем, вытесняющих её из сферы использования. Как показано в этой книге, к концу 2013 года захват Биткойна уже готовился. К тому времени, когда Bitcoin Cash пришла на помощь, сеть полностью изменила свой фокус с использования на удержание того, что есть, и создание технологий второго уровня для решения проблем масштабирования. И вот мы в 2024 году, индустрия пытается найти свой путь, свою нишу, в то время как мечты о цене «до луны» исчезают из памяти.

Эта книга должна была быть написана. Это история об упущенной возможности изменить мир, трагическая история об интригах и предательстве. Но это и обнадёживающая история о том, какие усилия мы можем предпринять, чтобы захват Биткойна не стал последней главой. У этой великой инновации ещё есть шанс освободить мир, но путь окажется более извилистым, чем кто-либо из нас мог себе представить.

Роджер Вер не преувеличивает в этой книге, он действительно герой этой саги. Он не только глубоко разбирается в технологии, но и придерживается видения, что Биткойн может нести свободу с самых первых дней и по сей день. Я разделяю его приверженность идее валюты без посредников для масс, наряду с конкурентным рынком для денег свободного предпринимательства. Это важная документальная история, и её аргументация бросит вызов любому, кто придерживается другой точки зрения. Несмотря ни на что, эта книга должна существовать, какой бы болезненной она ни была. Это подарок миру.

Джеффри Такер
Президент Института Браунстоун

Введение

Последние тринадцать лет моей жизни были посвящены тому, чтобы сделать Биткойн и другие криптовалюты деньгами будущего. Эта технология способна сделать мир значительно более свободным и процветающим, и в итоге она станет одним из важнейших изобретений всех времен. Я провел более десяти лет, рассказывая о преимуществах Биткойна, финансировал многочисленные стартапы в этой отрасли, строил свой собственный бизнес на его основе и видел, как его цена выросла более чем на 6 500 000%. Однако эта книга – не любовный роман, и я предпочёл бы, чтобы ее не пришлось писать. Проект, в котором я участвовал в 2011 году, был захвачен и изменен в худшую сторону.

Биткойн был задуман как цифровые наличные, пригодные для повседневной торговли, с минимальными комиссиями и быстрыми транзакциями, и он работал так в течение многих лет. Но сегодня Биткойн считают «цифровым золотом», не предназначенным для повседневной торговли, с высокими комиссиями и медленными транзакциями – полная противоположность первоначальному замыслу. Его называют «хранилище стоимости», мало заботясь о его полезности в качестве платежной системы. Некоторые люди даже утверждают, что Биткойн не может работать как платежная система, потому что он не масштабируется. Эти распространенные идеи просто не соответствуют действительности. Причина, по которой Биткойн больше не используется для цифровых расчетов, не имеет ничего общего с технологией, лежащей в его основе. Все дело в том, что группа разработчиков программного обеспечения захватила проект, решила изменить его дизайн и намеренно ограничила его функциональность – будь то из-за некомпетентности, злого умысла или сочетания того и другого. Захват произошел примерно в 2014—2017 годах, и в итоге сеть разделилась на две части, а криптовалютная индустрия разлетелась на тысячу осколков. Оригинальный проект все еще существует и остается чрезвычайно перспективным, но он больше не торгуется под тикером «BTC».

По мере того как я путешествую и продолжаю рассказывать по всему миру о преимуществах криптовалюты, выяснилось, что почти никто не знает историю захвата Биткойна. Основные дискуссионные площадки в сети уже много лет подвергаются жесткой цензуре и тщательно контролируют информацию, которую получают люди. Биткойн-максималисты – громкие голоса, настаивающие на том, что все проекты, кроме BTC, являются мошенничеством, – также помогают препятствовать критическому исследованию, в основном запугивая людей в социальных сетях. Любой, кто ставит под сомнение их версию, немедленно подвергается насмешкам, и это оказалось эффективной тактикой для подавления инакомыслия. Поскольку никто не высказывается, у новичков практически нет шансов узнать о реальной истории и устройстве Биткойна. Эта книга предоставляет такую информацию.

Книга *«Захват Биткойна»* состоит из трех частей. В первой части подробно рассматривается первоначальный дизайн Биткойна и радикальные изменения, внесенные в него. Вторая часть – это история захвата, включая многочисленные грязные приемы, такие как цензура, пропаганда и нападения на компании, которые не соглашались с новым курсом. Заключительная третья часть посвящена спасению Биткойна от захватчиков и реалистичному видению будущего.

Стать частью прорывной технологии на ранней стадии – мечта многих предпринимателей, и мой путь был наполнен захватывающими моментами и интересными историями. Но эта книга – не мемуары. Ее цель – просвещение. Последние несколько лет я делился этой информацией в частных беседах, публичных выступлениях и онлайн-видео, но теперь настало время изложить все это в письменном виде. Цель – помочь людям понять текущее положение Биткойна и то, как он к этому пришел. Предпринимателям и инвесторам, которые заинтересованы в том, чтобы в мире появились быстрые, дешевые, надежные и защищенные от инфляции циф-

ровые деньги: мы все еще можем это сделать. Нужно только работать вместе над правильным проектом.

Часть I: Гениальный дизайн

1. Изменение видения

Криптовалютная революция началась, когда в 2009 году миру был представлен Биткойн. За прошедшее десятилетие Биткойн превратился из совершенно неизвестной технологии в международную сенсацию, породившую новую индустрию. Предприниматели пытаются использовать эту технологию для решения широкого круга проблем – от простого улучшения онлайн-платежей до восстановления мировой финансовой системы. Благодаря освещению в новостях, спекуляциям на Уолл-стрит и энтузиазму в Интернете криптовалюта, пожалуй, стала самой популярной технологией XXI века. Однако, несмотря на шумиху и астрономический рост цен, её влияние на реальный мир было незначительным. В будущем криптовалюты могут послужить основой новой финансовой системы или стать альтернативой государственным деньгам, но на сегодняшний день основное применение криптовалют – это финансовые спекуляции.

Ситуация напоминает мне то время, когда я жил в Кремниевой долине во время интернет-бума 1990-х годов. Прогнозировалось, что интернет-технологии произведут революцию в коммерции по всему миру, а это означало, что любая «интернет-компания», не имеющая ни инфраструктуры, ни правдоподобного бизнес-плана, могла собрать миллионы, просто владея доменным именем премиум-класса. Спекуляции были просто умопомрачительными. Многие из крупнейших стартапов обанкротились всего через несколько лет после выхода на биржу. И всё же, несмотря на печально известный крах «пузыря доткомов», интернет действительно произвёл революцию в мире. Технология стала важнейшей инфраструктурой глобальной экономики и неотъемлемой частью современной жизни, хотя процесс её становления занял больше времени, чем многие надеялись. Криптовалюты идут по схожему пути. Несмотря на бурные спекуляции и относительную невостребованность, они кажутся неизбежной частью нашего будущего.

Любой рассказ о современной криптовалюте должен начинаться с Биткойна, дедушки всех криптовалют. Моя собственная жизнь связана с Биткойном с тех пор, как я открыл его для себя в 2010 году. Мои первые монеты были куплены в начале 2011 года по цене менее 1 доллара за штуку. Через несколько месяцев цена взлетела до 30 долларов, а к ноябрю того же года упала до 2 долларов – это было первое из многих экстремальных колебаний цены, которые с тех пор стали обычными для индустрии. Стремительный рост цены, за которым следует обвал на 80% и более, – это регулярный цикл, который повторялся несколько раз за короткую историю Биткойна. Волатильность служит хорошим поводом для новостных заголовков, поскольку широкая общественность ориентируется почти исключительно на цену. Но для меня Биткойн всегда был больше, чем просто финансовая инвестиция. Это великолепный инструмент для повышения уровня экономической свободы в мире.

Первоначально Биткойн-сообщество было наполнено эксцентричными людьми и необычными идеями. Как и многих других, меня Биткойн особенно привлек из-за моих политических и философских идеалов. Я очень ценю свободу человека и считаю, что люди должны иметь максимальный контроль над своей жизнью. Чем больше власти у любого правительства, тем меньше власти у отдельных людей, а из экономики и истории я знал, что контроль центральных банков над денежной массой даёт правительствам огромную власть. Поэтому Биткойн пришёлся мне по душе, так как он был спроектирован без центрального управляющего органа. Людям не нужно спрашивать разрешения на его использование. Не существует «Центрального банка Биткойна», который контролирует предложение монет, а сама техноло-

гия не признаёт международных границ. Немногие вещи имеют больший потенциал для увеличения глобальной свободы, чем быстрые, дешевые в использовании, не требующие разрешения, защищённые от инфляции цифровые деньги.

Футуризм – это ещё один ведущий философский мотив моего энтузиазма по отношению к криптовалютам. Такие мыслители, как Рэй Курцвейл, рисуют убедительные картины будущего, в котором люди радикально улучшат своё благосостояние с помощью передовых технологий. Возможно, достигнув достаточного уровня экономического и технологического развития, мы сможем значительно сократить количество страданий в мире и даже увеличить продолжительность своей жизни, чтобы наслаждаться большим количеством времени на Земле. Чтобы достичь этого, необходимо достаточное богатство и процветание, чтобы продолжать финансировать исследования, а также постоянная свобода для инноваций. На мой взгляд, Биткойн ещё на один шаг приближает нас к более технологически развитому будущему, в котором жизнь каждого человека станет лучше.

Эти убеждения не были уникальными для раннего Биткойн-сообщества. Онлайн-форумы и мессенджеры были центрами для дискуссий, и если бы вы посетили их, то увидели бы бесконечные обсуждения того, что Биткойн – это нечто большее, чем простая платежная система или спекулятивная инвестиция. Мы все знали, что эта технология может быть использована для кардинального улучшения мира. Брайан Армстронг, соучредитель и генеральный директор Coinbase, прекрасно отразил это настроение в статье под названием «Как цифровая валюта изменит мир», заявив:

> Цифровая валюта может стать самым эффективным способом повышения экономической свободы, который когда-либо видел мир. Если это произойдёт, последствия будут огромными. Это может избавить многие страны от бедности, улучшить жизнь миллиардов людей, ускорить темпы развития инноваций в мире… уменьшить количество войн, сделать беднейшие 10% населения более обеспеченными, свергнуть коррумпированные правительства и повысить уровень счастья.[1]

Мой энтузиазм быстро перерос в евангелизм, и я получил прозвище «Биткойн Иисус» за то, что проповедовал Евангелие от Биткойна всем, кто хотел слушать, и многим, кто не хотел. Мои друзья и семья, средства массовой информации и компании, которым я покровительствовал, слышали одно и то же послание: Биткойн – это быстрые, дешёвые, надёжные деньги, созданные для интернета. С его помощью вы можете мгновенно отправить любую сумму денег в любую точку мира за один цент США или меньше. В действительности, в первые дни большинство транзакций с Биткойном были совершенно бесплатными и включали небольшую плату только в том случае, если ваши монеты были недавно переведены. Люди сразу поняли ценность такой технологии, независимо от их личных убеждений. Одним из лучших маркетинговых ходов было просто заставить людей *использовать* Биткойн, поскольку пользовательский опыт был просто фантастическим по сравнению с другими платёжными системами. Я просил людей загрузить кошелёк на телефон, чтобы отправить им несколько долларов. После первой транзакции с использованием Биткойна нужно было всего несколько секунд, и вы слышали неизбежное «Вау!» после того, как новые пользователи были ошеломлены своим первым впечатлением.

К 2015 году Биткойн набрал такой оборот, что казалось, его уже не остановить. Известные компании, от Microsoft до Expedia, начали принимать его в качестве оплаты, и молодая индустрия росла в геометрической прогрессии. Успехи начали накапливаться. Венчурный капитал увеличился. Средства массовой информации стали позитивно освещать события. Биткойн начинал прямой полёт на Луну.

Провал запуска

Перенесёмся в сегодняшний день. Несмотря на громкое имя, Биткойн ещё не захватил мир. На самом деле, за заголовками и графиками цен скрывается мрачная правда: фактическое использование Биткойна снизилось с 2018 года, а многие компании и вовсе отказались от него в качестве средства оплаты. Неоднократно сеть давала сбои и становилась практически непригодной для использования из-за огромных комиссий за транзакции и ненадёжных платежей. В моменты перегрузки сети средняя комиссия может достигать более 50 долларов, а обработка транзакций может занимать дни или даже недели. И, пожалуй, хуже всего то, что эти сбои подтолкнули индустрию к принятию так называемых «***кастодиальных кошельков***», которые представляют собой просто счета клиентов, управляемые третьей стороной, подобно обычному банковскому счёту.

Массовое использование кастодиальных кошельков подрывает всю цель Биткойна, поскольку полный контроль передаётся третьей стороне, которая может цензурировать, отслеживать и даже конфисковывать монеты – как счета в Venmo. Мошенничество также становится проще. Например, когда в 2022 году рухнула биржа FTX, более миллиарда долларов клиентских средств мгновенно исчезли. Это стало возможным только потому, что FTX в конечном итоге контролировала деньги своих клиентов. Интеграция Биткойна в PayPal – ещё один яркий пример того, как пользователи переходят на кастодиальные кошельки вместо того, чтобы иметь полный контроль над своими средствами. Если люди будут пользоваться кастодиальными кошельками, Биткойн потеряет ключевое свойство, которое сделало его таким революционным.

Высокие комиссии, ненадёжные платежи, кастодиальные кошельки и сокращение случаев использования в коммерции – по другим показателям, кроме цены, Биткойн не улетел на Луну; он даже не сошёл с орбиты. Так что же произошло?

Официальная версия

Традиционное объяснение этих негативных тенденций заключается в том, что Биткойн стал жертвой собственного успеха. По мере роста популярности сеть исчерпала свои возможности. Присущие ей технологические ограничения привели к резкому росту комиссий, ненадёжности платежей, уходу магазинов и переходу индустрии к кастодиальным кошелькам. Вследствие этих проблем нарратив вокруг Биткойна сместился в сторону «цифрового золота» и «хранилища стоимости», а не цифровой валюты. Если Биткойн не предполагается использовать в повседневной коммерции, то не имеет значения, функционирует ли он как платёжная система.

Несмотря на то, что эти идеи часто повторяются в прессе и среди популярных комментаторов, они совершенно неверны. Реальная история гораздо более драматична. Биткойн был создан для использования в огромных масштабах и не столкнулся с присущими ему технологическими ограничениями. На самом деле проект был захвачен небольшой группой разработчиков программного обеспечения, которые переделали всю систему. Они намеренно ограничили её возможности и функциональность, а также открыто выступают за высокие комиссии и отставание в проведении транзакций – противоположность первоначальному замыслу.

Когда я рассказываю об этом людям сегодня, они часто думают, что я преувеличиваю, но разработчики говорят об этом сами. Например, влиятельный разработчик Биткойна Грег Максвелл совершенно открыто заявил: «Я не считаю, что комиссия за транзакции имеет значение – это не неудача, это успех!» Марк Фриденбах, ещё один разработчик Биткойна, заявил, что «медленные платежи и высокие комиссии будут нормой при любом благополучном

исходе». Когда в декабре 2017 года сеть почти остановилась, а средняя комиссия за транзакцию превысила 50 долларов, они отпраздновали это событие, «доставая шампанское», и были рады перегруженности, утверждая, что постоянное наличие бэклога – это «необходимый критерий стабильности».

Если бы вы сказали мне в 2012 году, что разработчики Биткойна в конечном итоге захотят высоких комиссий и медленных транзакций, я бы не поверил вам, как и ни один из ранних предпринимателей, которые помогли создать эту индустрию. Это просто нелепо. Дорогие транзакции и перегруженность сети не нужны для безопасности или стабильности. Наоборот, высокие комиссии и долгое время исполнения платежей подталкивают людей к использованию кастодиальных кошельков, а это в свою очередь подрывает весь смысл идеи Биткойна.

В текущих обстоятельствах Биткойн не может расширить возможности обычного человека. За последние несколько лет проект застопорился не из-за технологических сбоев, а из-за человеческих ошибок. В частности, плохого руководства и несовершенной модели управления. Когда я узнал о Биткойне в 2010 году, это было настолько захватывающе, что я почти чувствовал моральное обязательство рассказать о нём людям и поделиться хорошими новостями. Сегодня, учитывая произошедшие изменения, я чувствую моральное обязательство рассказать людям плохие новости: Биткойн был захвачен и больше не похож на первоначальный проект, вдохновивший меня и многих других. Но его история ещё не закончена.

Обходной путь

Оригинальный, масштабируемый дизайн Биткойна всё ещё существует, но он не торгуется на криптовалютных биржах под тикером BTC. Он называется «Bitcoin Cash» и торгуется как BCH. В течение многих лет разработчики BTC препятствовали развитию индустрии, пока в 2017 году не была создана новая сеть, призванная сохранить первоначальное видение Биткойна как цифровой валюты с низкими комиссиями, быстрыми транзакциями и отсутствием необходимости в кастодиальных кошельках. Сеть BCH гораздо менее известна, чем BTC, но она уже увеличила свою пропускную способность более чем в тридцать раз по сравнению с BTC и планирует продолжить расширение ещё в будущем.

События, приведшие к созданию Bitcoin Cash, были противоречивыми и с тех пор получили название «Гражданской войны Биткойна», и по сей день сообщества BTC и BCH часто враждебно относятся друг к другу. Если вы следите за Биткойном лишь вскользь, то слышали лишь версию событий от BTC-сообщества; эта книга рассказывает о другой точке зрения, она наполнена историческими подробностями, выдержками и цитатами других участников событий, которые разделяли видение Биткойна как цифровой валюты.

Чтобы разобраться, какие есть сети и группы, полезно установить чёткую терминологию. Сеть BTC часто называют «Bitcoin Core», а сеть BCH – «Bitcoin Cash». Именно эти термины будут использоваться далее. Слово «Биткойн» само по себе относится к технологии, которая используется в обеих сетях. И Bitcoin Core, и Bitcoin Cash используют технологию Биткойна и имеют одинаковую историю транзакций до их разделения в августе 2017 года. Разработчики Bitcoin Core решили отойти от первоначального дизайна, в то время как разработчики Bitcoin Cash придерживались его.

Избегание опасностей

Если эта технология действительно революционна, то она угрожает власти существующих финансовых и политических институтов. Но при нынешнем развитии событий, если ничего не изменится, эти институты ассимилируют криптовалюты и нейтрализуют их. Если Биткойн собирается сделать мир более свободным, то наше окно возможностей закрывается.

Индустрия приближается к двум сценариям провала. Первый – это полный захват существующими финансовыми и регуляторными системами. Массовое внедрение кастодиальных кошельков делает это возможным, поскольку транзакции легко отслеживаются и контролируются, а правительства могут без труда заставить компании соблюдать требования.

Другой сценарий провала – люди просто сдадутся и откажутся от идеи создания цифровых денег, не подверженных инфляции. Я видел, как многие талантливые умы и компетентные бизнесмены преждевременно пришли к выводу, что Биткойн не может масштабироваться из-за провала Bitcoin Core. Этого разочарования можно избежать, если люди поймут, что оригинальная технология Биткойна всё ещё существует, хорошо работает и может масштабироваться для глобального принятия. Bitcoin Core просто отклонился от этой концепции. Прежде чем потерять веру в технологию блокчейн, предприниматели и разработчики должны сначала испытать её оригинальную версию. Я постоянно пробую новые криптовалюты, и Bitcoin Cash по-прежнему оставляет наилучшее впечатление спустя всё это время.

Поскольку Биткойн находится в области пересечения международных финансов, политической власти и революционных технологий, его история должна быть одной из самых драматичных во всех отраслях, и материала для неё хватит на несколько голливудских постановок. Эта книга – лишь одна из частей этой истории: захват процесса разработки Биткойна и последующее отделение Bitcoin Cash с точки зрения бизнесмена, который использовал эту технологию в коммерции, возможно, больше, чем кто-либо другой в мире.

2. Основы Биткойна

Мир переполнен плохой информацией о Биткойне, во многом благодаря силе социальных сетей. Честные расследования в сети не поощряются, и если любопытный ум задаёт неправильные вопросы или высказывает неправильное мнение, он может ожидать волну гневных комментариев, критикующих его интеллект, репутацию или даже бизнес. Биткойн-максималисты – те, кто утверждает, что BTC – единственная легитимная криптовалюта, – печально известны тем, что используют эту тактику. Они выкладывают список причин, по которым любой альтернативный проект вроде BCH является мошенничеством, настаивают на том, что спор уже решён, и ставят под сомнение здравомыслие любого, кто с ними не согласен. У большинства людей нет времени на расследование этих утверждений, да и не хочется становиться мишенью для онлайн-троллей, поэтому они в итоге принимают общепринятую версию.

Чтобы понять разницу между Bitcoin Core и Bitcoin Cash, мы должны понять, как изначально создавался Биткойн. История может нам помочь, потому что создатель Биткойна, Сатоши Накамото, много раз публично рассказывал о своём изобретении, объясняя его дизайн. Другие великие умы и инженеры, пришедшие ему на смену, такие как Гэвин Андресен и Майк Хирн, также доходчиво объясняли основные идеи. Их работы, цитаты из которых приводятся в этой книге, обязательны к прочтению каждому, кто пытается понять Биткойн не только на поверхностном уровне. Прежде чем погрузиться глубже, полезно ознакомиться с тремя ключевыми понятиями: *блокчейн*, *майнеры* и *полные узлы*.

Блокчейн

Биткойн вращается вокруг технологии «блокчейн». Блокчейн – это просто публичная бухгалтерская книга, в которой хранятся все записи баланса Биткойн-кошельков, и она обновляется данными с новыми транзакциями примерно каждые десять минут. Эти новые транзакции упаковываются в «блоки», которые затем «соединяются» в цепочку, один за другим, образуя «блокчейн». Уникальность блокчейна заключается в том, что он не поддерживается централизованным органом. Нет какого-либо органа, который бы обрабатывал все транзакции или совершал записи в бухгалтерской книге. Вместо этого записи поддерживаются и обновляются децентрализованной сетью компьютеров по всему миру, что исключает возможность централизованного контроля или сбоя.

Сами блоки являются центральным элементом для понимания различных философий в Биткойне, которые можно условно разделить на два лагеря: сторонники больших блоков и сторонники маленьких блоков. Чем больше блоки, тем больше пропускная способность сети по транзакциям и тем больше ресурсов требуется для обработки каждого блока. Сторонники маленьких блоков хотят, чтобы блоки были маленькими, чтобы их мог обрабатывать каждый. Более подробно мы рассмотрим это различие позже.

Майнеры

Добавлять блоки в блокчейн может не каждый. Эту работу выполняют исключительно *майнеры*. Майнеры обновляют бухгалтерскую книгу, объединяя транзакции в блок, а затем добавляют специальное доказательство. Это доказательство представляет собой решение математической головоломки, которая настолько сложна, что для её решения требуется значительная компьютерная мощность. По всему миру существуют склады, заполненные специальными машинами, предназначенными для решения этих головоломок. Каждая из этих машин потребляет электроэнергию, а это значит, что быть майнером Биткойна стоит денег!

Майнеры получают финансовое вознаграждение за свои услуги с помощью двух механизмов: *комиссии за транзакции* и *вознаграждения за блок*. Комиссия за транзакции – это просто плата пользователей за добавление их транзакций в блок. Вознаграждение за блок – это способ добычи новых Биткойнов. Каждый раз, когда майнер добавляет блок в цепочку, он получает небольшое количество новых Биткойнов. Примерно раз в четыре года это вознаграждение сокращается вдвое. В первые дни майнеры получали по 50 новых Биткойнов за блок, но на момент написания книги вознаграждение за блок снизилось до 6,25 монеты. В конце концов, вознаграждение станет незначительным, и единственным источником дохода для майнеров останутся комиссии за транзакции.

Сторонники больших блоков считают, что майнеры выполняют важную функцию в индустрии Биткойна, защищая сеть от атак, поддерживая бухгалтерскую книгу и обрабатывая все транзакции. Майнеры часто инвестируют миллионы и даже десятки миллионов долларов в модернизацию более мощного оборудования. В 2018 году компания Bitmain объявила о планах построить крупнейший в мире майнинг-центр в Техасе и оценила общий объём инвестиций более чем в 500 миллионов долларов[1]. Майнинг Биткойнов требует больших инвестиций и затрат на обслуживание. Из-за этого большинство сторонников больших блоков считают, что майнеры должны иметь наибольшее влияние на развитие Биткойна. В зависимости от успеха монеты, которую они добывают, их вложения могут быть полностью потеряны или могут принести значительную прибыль. Поэтому у них есть серьёзный стимул следить за тем, чтобы Биткойн оставался полезным и ценным.

Сторонники малых блоков, как правило, относятся к майнерам более скептически или даже враждебно. Поскольку майнеры – единственные, кто может добавлять блоки в сеть, они обладают значительной властью и могут стать системной угрозой, если майнинг станет слишком централизованным. Если на рынке будут доминировать лишь несколько крупных игроков, это может привести к тому, что сам Биткойн станет слишком централизованным. Крупные майнинговые предприятия также создают политический риск для системы. Если правительства решат атаковать, регулировать или контролировать крупнейших майнеров, они смогут остановить или контролировать Биткойн. Роль майнеров – одно из главных разногласий, которое привело к расколу и формированию Bitcoin Cash.

Полные узлы

К счастью, если вы хотите использовать Биткойн, вам не нужно быть майнером или запускать сложное программное обеспечение. Обычные пользователи могут получить доступ к сети более простыми способами. Сатоши Накамото описал метод упрощённой верификации платежей (УВП), который позволяет пользователям отправлять, получать и подтверждать собственные транзакции с минимальными усилиями. На протяжении большей части истории Биткойна большинство кошельков использовали либо УВП, либо другие подобные методы доступа к блокчейну. В BTC эта тенденция меняется на противоположную из-за распространения кастодиальных кошельков, но в BCH она остаётся нормой.

Есть и другой вариант доступа к сети Биткойн, который требует больше усилий. Некоторые пользователи запускают программное обеспечение «полный узел», которое загружает весь блокчейн и проверяет каждую транзакцию, которая когда-либо происходила. Весь блокчейн BTC содержит около 800 миллионов транзакций и в настоящее время имеет размер около 450 гигабайт. Пользователям, впервые запускающим программное обеспечение полного узла, может потребоваться несколько часов, чтобы синхронизироваться с остальной сетью. Кроме того, если полный узел отключается от сети, его нужно будет подгружать и проверять все последние блоки, чтобы снова использовать Биткойн. Вот почему УВП стало таким важным изобретением. Его использование практически не требует времени и усилий, но при этом обес-

печивает отличную безопасность. УВП позволяет вам подтверждать собственные транзакции, в то время как полные узлы позволяют подтверждать все транзакции в блокчейне.

Пожалуй, самое большое различие между философиями больших и малых блоков заключается в роли полных узлов. Сторонники больших блоков считают, что подавляющее большинство операций в сети должно происходить между майнерами и лёгкими кошельками, использующими УВП или аналогичную технологию. Они считают, что полные узлы полезны только в особых случаях, когда нужно подтвердить транзакции многих людей за короткий промежуток времени, например, если вы управляете криптовалютной биржей или платёжным процессором. Поскольку сеть не выплачивает операторам полных узлов никакого финансового вознаграждения, а у большинства людей нет необходимости подтверждать чужие транзакции, у обычных пользователей нет стимула запускать такое мощное программное обеспечение. Сатоши был однозначным сторонником больших блоков, и, как он сказал, «дизайн позволяет пользователям просто быть пользователями»[2].

Сторонники малых блоков, напротив, считают, что полные узлы необходимы для сети. Они уверены, что пользователи должны сами управлять своими узлами, поэтому наличие небольших блоков крайне важно, так как стоимость управления узлом увеличивается с ростом размера блоков. Основная причина, по которой сторонники малых блоков утверждают, что Биткойн не может масштабироваться, заключается в том, что большие блоки обходятся операторам узлов дороже. Вместо того чтобы принять тот факт, что обычные пользователи не должны запускать полные узлы, они пришли к выводу, что Биткойн не может масштабироваться. С моей точки зрения, это одна из самых больших путаниц, связанных с Биткойном, и она будет подробно проанализирована.

Фундаментальная пятерка

О первоначальном видении Биткойна Сатоши Накамото было сказано немало. Сторонники этой идеи, такие как я и другие ранние последователи, считали, что он создал блестящую систему, которая доказала свою эффективность в реальном мире. Благодаря этому успеху мы не видели причин для её кардинального изменения. Критики первоначального видения считали, что Сатоши ошибся в некоторых ключевых областях и хотели изменить протокол соответствующим образом. Разработчики Bitcoin Core были такими критиками, несмотря на то что в конечном итоге они возглавили проект.

Биткойн-максималисты часто сравнивают приверженность первоначальному видению с некой слепой верой, в которой не допускаются никакие отклонения от основополагающих идей. Но это слабая критика. Желание придерживаться замысла Сатоши далеко не догматично. Биткойн – сложная система с множеством подвижных частей. Помимо программного обеспечения и компьютерной сети, это целая *экономическая* система, для понимания которой необходим экономический анализ. Если рассматривать не только экономические, но и программные компоненты, становится ясно, что Биткойн хорошо настроен и вмешательство извне нежелательно.

Вместо того чтобы масштабировать Биткойн за счёт увеличения размера блока для повышения пропускной способности транзакций, разработчики Core решили, что Биткойн должен масштабироваться за счёт использования нескольких слоёв. По их мнению, первый слой должен состоять из транзакций, которые будут записаны ончейн, на них строятся дополнительные слои. Эти дополнительные слои будут «вне цепи», то есть транзакции не будут записываться в блокчейн, что избавит от необходимости масштабировать базовый слой. Широко разрекламированная сеть Lightning Network является одним из таких вторых слоёв, но у неё есть множество фундаментальных проблем, которые подробно рассматриваются в главе 9. Одна из существенных проблем заключается в том, что для её использования необходимы

транзакции ончейн. Чтобы просто подключиться к Lightning Network, необходимо совершить хотя бы одну транзакцию на базовом уровне, а это может стоить сотни долларов при высоком уровне загрузки BTC. Несмотря на то что это критический недостаток, решение проблемы пока не предложено.

Bitcoin Core ставит всё на жизнеспособность этих дополнительных уровней. Они перевернули первоначальную систему, сделав транзакции базового уровня медленными и дорогими, но не создали удовлетворительной альтернативы, обеспечивающей простые и надёжные платежи. Текущая версия Lightning Network не является ни надёжной, ни безопасной (именно поэтому самые популярные кошельки Lightning теперь являются кастодиальными). Таким образом, все надежды на то, что BTC станет деньгами будущего, дающими свободу, полностью зависят от технологии, которая ещё не создана.

На конференции в июле 2021 года Илон Маск также отметил, что пропускная способность транзакций BTC может быть проблемой, и подчеркнул важность идеи масштабирования криптовалюты путём увеличения размера её базового слоя:

> Есть определённые преимущества в том, чтобы рассмотреть что-то, что имеет более высокую максимальную скорость транзакций и более низкую стоимость транзакций, и посмотреть, как далеко вы можете зайти в одноуровневой сети… Я думаю, что вы можете пойти дальше, чем люди думают[3].

Маск – видный сторонник BTC, но его интуиция инженера подсказывает, что философия BCH верна. Масштабирование базового слоя – правильная идея, и она всегда была частью первоначального дизайна.

Сатоши не был совершенен, но, как будет показано в последующих главах, его идеи убедительны, хорошо продуманы и заслуживают честного изучения. Его дизайн не требует сложности дополнительных слоёв, хотя они совместимы. Вместо того чтобы слепо следовать за каким-либо человеком, группой разработчиков или символом тикера, попробуйте оценить идеи по их собственным достоинствам. Послушайте, как Сатоши создал Биткойн, послушайте разработчиков Core и сформируйте собственное мнение.

Различия между оригинальным дизайном и новым дизайном Bitcoin Core можно отразить с помощью пяти главных идей:

1) Биткойн был разработан как цифровая валюта, используемая для совершения платежей через Интернет.

2) Биткойн был разработан для того, чтобы иметь чрезвычайно низкие комиссии за транзакции.

3) Биткойн был разработан для масштабирования с увеличением размера блоков.

4) Биткойн не был создан для того, чтобы обычный пользователь мог управлять своим собственным узлом.

5) Экономический дизайн Биткойна так же важен, как и его программное обеспечение.

Каждый из этих пунктов является центральным в первоначальном видении Биткойна, которое разделяли Сатоши и другие участники. Но сегодня преобладающая точка зрения не совпадает ни с одним пунктом. Если вы слушаете комментаторов на телевидении или блогеров, авторов популярных подкастов, вы можете считать, что:

1) Биткойн был разработан как хранилище стоимости, даже если он не работает как средство обмена.

2) Предполагается, что у Биткойна высокие комиссии за транзакции.

3) Биткойн не масштабируется с увеличением размера блоков.

4) Безопасность Биткойна зависит от обычных пользователей, управляющих своими собственными узлами.

5) Экономический дизайн Биткойна был сломан и должен был быть исправлен инженерами-программистами.

Все это неверно. Даже если вам нравятся изменения, внесённые Bitcoin Core, историческая справка ясно показывает, что они радикально отличаются от первоначального дизайна. В следующих главах мы подробно рассмотрим каждое из этих утверждений.

3. Цифровые наличные для платежей

Интернет – это самый мощный инструмент распространения информации, который когда-либо видел мир. Люди могут узнать практически обо всём, используя Google, YouTube, Wikipedia и даже социальные сети. Однако эти каналы могут быть легко замусорены или даже предоставлять заведомо ложную точку зрения. Например, если вы упомянете криптовалюту в Twitter, вы гарантированно услышите от целой толпы случайных пользователей, которые будут рекламировать свою любимую монету и ругать все остальные. Если присмотреться, у многих из этих аккаунтов фальшивые фотографии профиля, нет подписчиков, и, похоже, они целыми днями пишут в Twitter о своих любимых криптопроектах. По отдельности они могут казаться неважными и беспомощными, но когда так поступают сотни или тысячи аккаунтов, это может повлиять на общественное мнение. Я убедился в этом на собственном опыте. Криптовалютная индустрия постоянно страдает от кампаний в социальных сетях и дезинформации в Интернете. В Биткойне эти методы имеют особенно уродливую историю.

И хотя эта тактика аморальна, она, несомненно, эффективна. Свидетельством эффективности риторики Bitcoin Core является то, что сейчас существуют разногласия и путаница в отношении самого назначения Биткойна. Вместо того чтобы быть признанной платёжной системой для повседневной торговли, о Биткойне говорят почти исключительно как о «хранилище стоимости», полезность которого не зависит от использования его в качестве наличных. Это утверждение можно услышать повсюду, даже от учёных. Описание популярной книги The Bitcoin Standard гласит:

> Реальное конкурентное преимущество Биткойна может заключаться в том, что он является хранилищем стоимости и сетью для окончательного расчёта по крупным платежам – цифровой формой золота со встроенной инфраструктурой расчётов.[1]

Мне нравилась аналогия с цифровым золотом, пока её не перевернули с ног на голову. Мы говорили, что Биткойн – это цифровое золото, поскольку его не может напечатать центральный банк и его можно мгновенно отправить в любую точку мира почти без затрат. Теперь же под «цифровым золотом» подразумевают обратное – Биткойн похож на золото из-за высоких комиссий на сделки и ограниченного использования как средства обмена. Вместо того чтобы подчёркивать сильные стороны золота, Биткойн ассоциируется с его слабыми сторонами.

Некоторые сторонники Bitcoin Core пошли ещё дальше. Вместо того чтобы просто утверждать, что Биткойн лучше выполняет роль хранилища ценности, чем платёжной системы, они заявляют, что Биткойн был намеренно разработан как хранилище ценности, а не как средство обмена. По словам Дэна Хелда, директора по развитию бизнеса компании Kraken:

> Те, кто продвигают версию о том, что «Биткойн был создан в первую очередь для платежей», настойчиво и избирательно цитируют фразы из академической работы и сообщения на форуме, чтобы отстаивать свою точку зрения… Биткойн был специально создан, чтобы сначала стать хранилищем ценностей.[2]

Хотя это дерзкое утверждение может получить лайки в социальных сетях и похвалу от криптовалютных комментаторов, оно не выдерживает критики. Исторические факты свидетельствуют о том, что Биткойн был создан для повседневных платежей.

Словами Сатоши

Какие у нас есть доказательства того, что Биткойн специально создавался как платёжная система? Ну, всё, что его создатель написал на эту тему. Помимо основополагающего документа, в котором Биткойн был представлен миру, у нас есть сотни сообщений на форумах и более пятидесяти публичных писем Сатоши. Они рисуют чёткое видение технологии. Давайте начнём с научной работы, выпущенной в 2008 году, в которой впервые был представлен и описан Биткойн. Я рекомендую прочитать весь документ онлайн. Работа хорошо написана, и многие ключевые концепции можно понять без технических знаний. Мы проанализируем первые несколько разделов, начиная с заголовка:

Биткойн: система электронных денег без посредников.

Сатоши мог бы назвать её «электронным хранилищем ценностей», если бы именно так и задумывал, но вместо этого он назвал её системой электронных денег. Далее, самое первое предложение аннотации гласит:

> Версия электронных денег без посредников позволит отправлять онлайн-платежи напрямую от одной стороны к другой, минуя финансовые учреждения.[3]

«Онлайн-платежи» упоминаются буквально в первом предложении документа, представляющего миру Биткойн. После аннотации начинается введение:

> Торговля в Интернете стала почти полностью зависеть от финансовых учреждений, выступающих в качестве доверенной третьей стороны при обработке электронных платежей. Хотя эта система достаточно хорошо работает для большинства транзакций, она всё же страдает от недостатков, присущих модели, основанной на доверии…

В первых двух предложениях вступления Сатоши упоминает «коммерцию в интернете», «электронные платежи» и «транзакции». Далее он продолжает:

> Полностью необратимые транзакции на самом деле невозможны, поскольку финансовые учреждения не могут избежать посредничества в спорах. Стоимость посредничества увеличивает транзакционные издержки, ограничивая минимальный практический размер сделки и отсекая возможность для мелких случайных сделок, а более широкие издержки связаны с потерей возможности совершать необратимые платежи за необратимые услуги. С появлением возможности обратного платежа потребность в доверии возрастает… Этих издержек и неопределённости платежей можно избежать при личном использовании физической валюты, но не существует механизма, позволяющего осуществлять платежи по каналу связи без доверенной стороны.

Другими словами, существующие методы онлайн-платежей имеют высокую стоимость транзакций из-за присущего системе доверия. Кредитные карты, PayPal и так далее – все они зависят от компаний с дорогостоящими механизмами разрешения споров. Эти издержки делают «мелкие случайные транзакции» в интернете фактически невозможными. В отличие от этого, платежи физическими наличными не требуют доверия к третьим лицам, но нет возможности использовать физические наличные в Интернете. Появляется Биткойн:

> Необходима электронная платёжная система, основанная не на доверии, а на криптографическом доказательстве, позволяющая двум

> заинтересованным сторонам совершать сделки напрямую друг с другом без участия доверенной третьей стороны. Транзакции, которые невозможно отменить, с помощью вычислений, защитят продавцов от мошенничества, а для защиты покупателей можно будет легко внедрить обычный механизм эскроу.

Другими словами, Биткойн похож на наличные деньги, потому что участники сделки могут обмениваться друг с другом напрямую, не прибегая к услугам посредников. В первых нескольких абзацах документа ясно сказано, что Биткойн – это «коммерция», «транзакции», «платежи», «магазины», «покупатели» и «продавцы». О «хранилище ценностей» в документе не упоминается ни слова.

Даже в электронных письмах Сатоши и сообщениях на форумах концепция Биткойна как хранилища стоимости встречается лишь несколько раз. Сэм Паттерсон, соучредитель криптовалютной компании OB1, написал популярную статью, в которой он отметил все упоминания Биткойна как платёжной системы, а не как хранилища стоимости. Он заключил:

> Изучив все труды Сатоши, я могу с уверенностью заявить, что Биткойн не был создан для того, чтобы сначала стать хранилищем ценностей. Он был создан для платежей… Сатоши упоминал о платежах в четыре раза чаще, чем о хранении ценностей… Этих доказательств может быть достаточно, чтобы вы не принимали во внимание утверждение «Биткойн был создан для того, чтобы сначала стать хранилищем ценностей». Я не могу представить, чтобы кто-то, честно взглянув на слова Сатоши, поверил, что он создал его не для платежей.[4]

Не только в научной работе ясно сказано, что Биткойн – это платежи. Сатоши не менее ясно выражался на онлайн-форумах:

> Биткойн подходит для более мелких транзакций, лучше чем существующие методы оплаты. Он достаточно мал, чтобы обеспечивать то, что можно назвать верхней частью диапазона микроплатежей.[5]

Микроплатежи

Насколько малы «микроплатежи»? Универсального определения не существует, но в данном контексте это транзакции меньше одного доллара США. Гэвин Андресен, разработчик, которого Сатоши выбрал в качестве своего преемника, поделился похожими мыслями:

> Я по-прежнему считаю, что сеть Биткойна – это неправильное решение для платежей меньше цента. Но я не вижу причин, по которым она не могла бы продолжать хорошо работать для платежей на небольшие суммы (от 1 до 0,01 доллара США).[6]

Раньше Биткойн считался практичным для транзакций в диапазоне от пары центов до пары долларов. Но с тех пор как комиссия за транзакции выросла, зачастую невозможно отправить такую маленькую транзакцию, поскольку комиссия в итоге оказывается больше, чем сама отправляемая сумма. Если у адреса Биткойна недостаточно средств для оплаты комиссии майнера, его фактически нельзя использовать. Сатоши подробно говорит о микроплатежах:

> Хотя я не думаю, что сейчас Биткойн практичен для небольших микроплатежей, со временем он станет таковым, поскольку стоимость хранения данных и пропускной способности каналов связи продолжает снижаться. Если Биткойн будет использоваться в больших масштабах, то, возможно, к тому времени это уже будет так. Ещё один способ сделать их более

> практичными – если я реализую режим «только для клиентов», а количество узлов сети объединится в меньшее число профессиональных серверных ферм. Какой бы размер микроплатежей вам ни понадобился, в конечном итоге они станут практичными. Думаю, через 5 или 10 лет пропускная способность и хранение данных покажутся тривиальными.[7]

Эта цитата интересна по двум причинам. Во-первых, Сатоши представляет себе, что Биткойн в конечном итоге будет использоваться для «любого размера микроплатежей, который вам нужен», а во-вторых, он предсказывает, что сетевая инфраструктура трансформируется в «профессиональные серверные фермы», что особенно актуально для дебатов о больших блоках.

> Как только Биткойн начнёт работать, появится множество способов применения, в частности вы сможете заплатить несколько центов веб-сайту с той же легкостью, будто опускаете монеты в торговый автомат.[8]

Сатоши хотел, чтобы Биткойн использовался для «лёгкой оплаты нескольких центов на веб-сайте». В противоположность этому вот что говорит разработчик Bitcoin Core Питер Тодд:

> Я был бы очень счастлив, если бы мог перевести деньги в любую точку мира, полностью освободившись от централизованного контроля, всего за 20 долларов. В равной степени я с радостью приму более централизованные методы перевода денег, когда я просто покупаю шоколадку.[9]

Видение Сатоши и Тодда несовместимы друг с другом, поскольку они расходятся во мнениях относительно приемлемого уровня комиссии более чем на три порядка. Комиссионные в размере $20 разрушают все возможности использования Биткойна, кроме переводов большой стоимости, – это своего рода крайность цифрового золота. У нас есть одна цитата Сатоши, в которой он напрямую сравнивает Биткойн с золотом. Он отвечал на вопросы об очевидной расточительности потребления электроэнергии для добычи Биткойна:

> Это та же ситуация, что и с золотом и золотодобычей. Предельные затраты на добычу золота имеют тенденцию оставаться на уровне цены золота. Добыча золота – это расточительство, но это расточительство гораздо меньшее, чем польза от того, что золото доступно в качестве средства обмена. Я думаю, что с Биткойном будет то же самое. Полезность обмена, возможного благодаря Биткойну, намного превысит стоимость используемой электроэнергии. Поэтому отсутствие Биткойна будет чистым расточительством.[10]

Золото используется в качестве аналогии, чтобы проиллюстрировать, что его полезность *как средства обмена* перевешивает затраты на его добычу. Иронично, если оглянуться назад.

В одном из сообщений на форуме также обсуждаются покупки в торговом автомате, что подчёркивает способность Биткойна осуществлять мгновенные платежи небольшой стоимости. Поскольку мгновенные платежи не являются абсолютно безопасными, Сатоши предполагал, что платёжные процессоры возьмут на себя незначительные риски, чтобы справиться с ними:

> Я полагаю, что компания, занимающаяся обработкой платежей, сможет предоставлять в качестве услуги быстрое распространение транзакций с достаточно хорошей проверкой за 10 секунд или меньше.[11]

Он был прав, и оказалось, что процессорам Биткойн-платежей требуется всего пара секунд, чтобы провести достаточную проверку.

Все о коммерции

На форумах можно найти множество подобных обсуждений использования Биткойна в коммерции. Сатоши и другие говорили о создании интерфейсов для онлайн-магазинов, инструментов для физических магазинов, транзакций в точках продаж, случаев, когда клиент не хочет использовать кредитную карту, хранения небольших сумм Биткойна на мобильных устройствах для случайных расходов и так далее. Нет никаких сомнений в том, что Сатоши планировал использовать Биткойн для платежей, даже таких небольших, как несколько центов. На самом деле, первоначальная версия 0.1.0 содержала незаконченный код для торговой площадки без посредников и даже базовую основу для виртуального покера.

Биткойн-индустрия в целом тоже строилась, основываясь на принципе, что Биткойн – это быстрая, дешевая и надежная платёжная система для интернета. Успешные компании, такие как BitPay, крупнейший в мире процессор Биткойн-платежей, столкнулись с тем, что вся их бизнес-модель была поставлена под сомнение из-за необоснованно высоких комиссий. В одном из интервью в 2017 году генеральный директор Стивен Пэйр сказал:

> В компании BitPay блокчейн Биткойна перестал работать… и у нас есть несколько вариантов. Первый – начать использовать форк Биткойна. Второй вариант – мы начнём использовать форк Биткойна. И третий вариант – мы начинаем использовать форк Биткойна. Мы действительно находимся в безвыходном положении, и мы должны это сделать.[17]

По этой причине BitPay стала одной из первых компаний, интегрировавших Bitcoin Cash после раскола. Брайан Армстронг, генеральный директор Coinbase, также разделял видение Биткойна как цифровой валюты для всего мира, и в интервью 2017 года он объяснил, почему неспособность BTC масштабироваться «разбила ему сердце».

> Причина моего увлечения Биткойном и цифровыми валютами заключается в том, что я хочу, чтобы в мире существовала открытая финансовая система… где все платежи были бы быстрыми, дешевыми, мгновенными и без границ… А Биткойн в итоге оказался неспособным к масштабированию.[18]

Далее он объясняет, что другие проекты, такие как Bitcoin Cash, с большей вероятностью достигнут этой цели:

> Я считаю, что вы могли бы управлять сетью Биткойн, даже с таким объёмом транзакций как у Visa, за комиссии на два-три порядка меньше, чем Visa берёт сегодня. Таким образом, отправка всех платежей в мире могла бы стоить порядка одного цента или даже меньше… Но я думаю, что другие сети, такие как Bitcoin Cash или Ethereum, работают над этим, и поэтому это видение будет реализовано, но было немного обидно не увидеть, что первоначальный Биткойн достигнет этого.[18]

Мнение Армстронга было распространённым среди первых Биткойн-предпринимателей и вообще первых пользователей Биткойна. Я помню, как интернет-сообщество часто сравнивало Биткойн с Western Union, чтобы подчеркнуть его превосходство в качестве платёжной системы. В одной из самых популярных инфографик (на фото ниже) реклама Western Union была помещена рядом с аналогичной рекламой Биткойна. Реклама Western Union гласила: «Отправьте тёплые пожелания сегодня. Всего за 5 долларов вы можете отправить до 50 дол-

ларов с доставкой по США. „Перемещаем деньги к лучшему“». Реклама Биткойна гласила: «Отправляйте тёплые пожелания 24 часа в сутки 7 дней в неделю. Всего за 0,01 доллара вы можете отправить любую сумму и получить её в любой точке мира. „Перемещаем деньги гораздо лучше“».

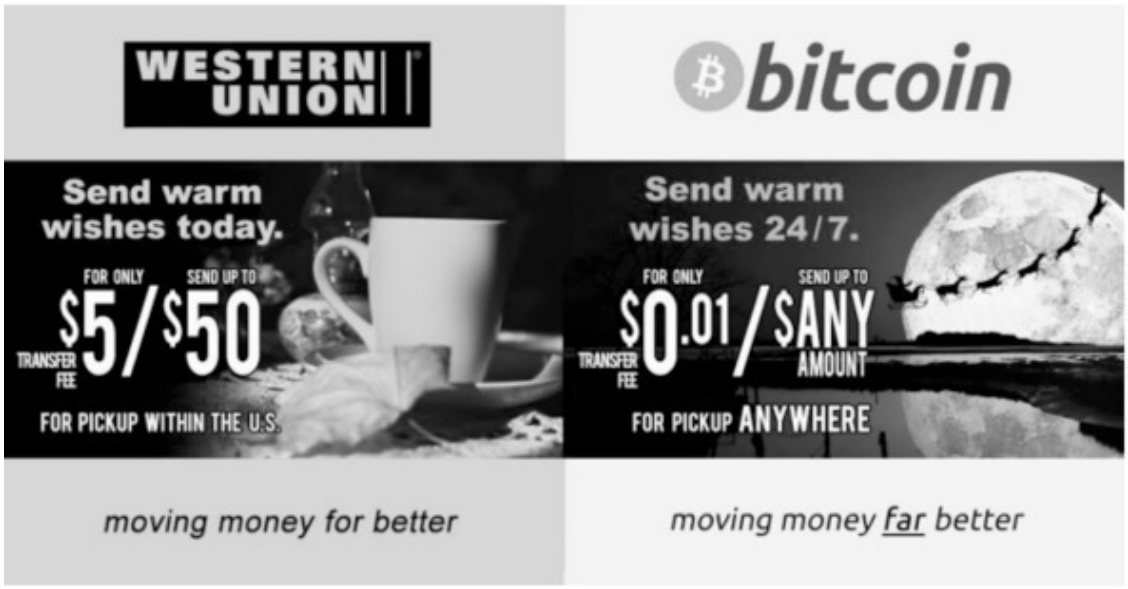

Рисунок 1: Ранняя инфографика, сравнивающая Western Union и Биткойн.

На сайте Bitcoin.org также рассказывалось о преимуществах использования Биткойна в повседневной коммерции. В архивной версии 2010 года говорилось, что «транзакции с использованием Биткойна практически бесплатны, в то время как кредитные карты и системы онлайн-платежей обычно стоят 1—5% за транзакцию плюс различные другие комиссии продавцов, достигающие сотен долларов». Даже в 2015 году сайт рекламировал «нулевые или низкие комиссии за обработку» и «мгновенные транзакции без посредников». [20]

Предположить, что Биткойн никогда не создавался для повседневных платежей, – дерзкая попытка переписать историю. Любой честный человек, участвовавший в проекте до 2014 года, подтвердит, что изначально планировалось создать недорогую цифровую денежную систему. Люди, которые считали, что Биткойн должен быть дорогим, эксклюзивным хранилищем ценностей, были в крайнем меньшинстве.

4. Хранилище стоимости или средство обмена

Настоящее преимущество биткойна заключается в том, что он является надежным инструментом сохранения стоимости… а не в его способности предоставлять безграничные или дешевые транзакции.[1]

– Сайфедеан Аммус, The Bitcoin Standard

Удивительно, что так много людей некритично восприняли идею о том, что Биткойн будет сохранять стоимость, даже если он не будет работать как цифровая валюта. Скорее всего, верно прямо противоположное: если Биткойн сможет доказать, что является лучшей валютой в течение длительного периода времени, то рынок может принять его в качестве хранилища стоимости. Но для этого потребуются годы демонстрации полезности и стабильности. Называть любую существующую криптовалюту «надежным долгосрочным хранилищем стоимости» преждевременно, учитывая дикие колебания цен, которые происходят регулярно. Тот факт, что BTC значительно вырос в цене за последние десять лет, не означает, что он является хранилищем ценности.

Не трогайте его

Сайфедеан Аммус придерживается одной из самых радикальных версий «максимализма цифрового золота». Он представляет будущее, в котором обычные люди даже не будут прикасаться к блокчейну, а транзакции на цепочке будут предназначены только для очень крупных переводов. В книге The Bitcoin Standard он пишет:

> Биткойн можно рассматривать как новую резервную валюту для онлайн-транзакций, где онлайн-эквивалент банков будет выдавать пользователям токены, обеспеченные Биткойнами, а свои запасы Биткойнов хранить в холодном хранилище…[2]

А в онлайн-дискуссии он пишет:

> Биткойн-платежи ончейн – не для магазинов, они для центральных банков. На базе Биткойна можно построить все платежные сети мира, но расчеты будут осуществляться ончейн. BTC – это как золото центрального банка при золотом стандарте.[3]

Похожие идеи разделяет известный комментатор Биткойна Туур Деместер:

> При должном развитии использование блокчейна Биткойна станет таким же редким и специфическим, как фрахтование нефтяного танкера.[4]

Сейчас эти идеи обсуждаются так, как будто они всегда были доминирующим видением. Но по сравнению с первоначальным проектом они дикие и ненужные. Я, конечно, никогда не подписывался на такую версию Биткойна, как и бесчисленное множество других предпринимателей, с которыми я работал в первые дни. На самом деле, главная прелесть Биткойна заключается именно в том, что блокчейн доступен всем, а не только банкирам. Как и многие другие публичные личности, уверенно говорящие о Биткойне, Аммус и Деместер просто предполагают, что дополнительные слои без проблем решат проблемы с удобством использования BTC. Однако, если взглянуть на технологии второго слоя, их жизнеспособность остается под вопросом, особенно если базовый слой не масштабируется. Эти проблемы часто не осозна-

ются энтузиастами BTC, которые вместо этого верят, что инженеры все исправят в будущем, несмотря на то что у них мало что получается на данный момент.

Более того, будущее «токенов, обеспеченных Биткойном», – это гарантия того, что произвольная инфляция будет и дальше мучить тех из нас, кто не является центральным банком. История показывает, что валюты неизбежно теряют свою поддержку со временем, и если люди вынуждены торговать обещаниями Биткойна вместо реального Биткойна, то это лишь вопрос времени, пока обещания не будут раздуты до уровня, значительно превышающего реальное предложение Биткойна. Вторые слои только облегчают эту инфляцию.

Смена повествования

В Биткойн-сообществе в течение нескольких лет происходило смещение повествования от цифровых денег к хранилищу стоимости. Даже в 2016 году большинство сторонников Биткойна все еще говорили о технологии как об онлайн-валюте – или, как они любили ее называть, «волшебные интернет-деньги», – поэтому каждый раз, когда очередная компания объявляла о том, что принимает Биткойн к оплате, начинались празднования. С каждым новым магазином, Биткойн становился все более авторитетным и полезным. Но после скачка комиссии за платежи в конце 2017 года, вместо того чтобы признать наличие проблемы, самые влиятельные сторонники BTC начали ловко менять точку зрения: мол, если Биткойн – это только хранилище стоимости, то высокие комиссии не имеют значения. В последние годы людей даже призывали не тратить свои монеты в коммерческих целях, потому что BTC можно покупать и хранить бесконечно долго. Я цинично отношусь к идее «купить, хранить и никогда не использовать», это отличный способ поднять цену, создав искусственный дефицит. Если достаточно людей убедить в том, что они могут разбогатеть, покупая и удерживая актив с конечным предложением, экстремальный рост цен будет неизбежным результатом.

По моему мнению, единственная надежда криптовалюты стать настоящим хранилищем стоимости – это *ее полезность в реальном мире*. Криптовалюта должна быть более полезной, чем другие денежные системы, доставшиеся нам по наследству, а высокие комиссии за переводы сразу же подрывают полезность любой монеты. Если бы BTC была единственной доступной криптовалютой, то, возможно, она еще могла бы работать в качестве хранилища стоимости, но поскольку на рынке есть из чего выбирать, маловероятно, что самая медленная, дорогая и наименее масштабируемая криптовалюта в итоге будет выбрана в качестве надежного долгосрочного хранилища стоимости. Например, Bitcoin Cash обладает практически всеми свойствами Bitcoin Core, более того, вы можете использовать её в качестве цифровой валюты. В долгосрочной перспективе рынок в конце концов поймет, что он платит чрезвычайно высокие комиссионные за BTC без всякой причины, поскольку тот же самый продукт может быть предложен за меньшую цену.

Экономика хранения ценности

Чтобы увидеть проблемы, связанные с идеей использования как лишь «хранилища стоимости», мы должны глубже погрузиться в экономику. Мне повезло, что я рано познакомился с Австрийской Школой Экономики. Такие великие мыслители, как Людвиг фон Мизес и Мюррей Ротбард, помогли мне понять мир через призму экономики, и я знал, что Биткойн станет популярным, потому что ранее читал их рассуждения о деньгах. Я видел, что Биткойн обладает свойствами чрезвычайно качественных денег, а это означало, что я должен немедленно купить несколько штук.

Потенциал Биткойна как хранилища стоимости – интересная экономическая загадка. Да и само понятие стоимости – интересная загадка, которая веками ставила экономистов в тупик.

Почему вообще что-либо имеет ценность? Один из выводов Австрийской Школы Экономической, который с тех пор вошел в мейнстрим экономики, заключается в том, что ценность субъективна. Ценность не находится в материальных товарах, она находится в человеческом сознании. Вещи не обладают ценностью сами по себе. Мы придаем им ценность, потому что считаем, что их можно использовать для удовлетворения наших желаний.

«Хранилище ценности» не может в прямом смысле «хранить» ценности, как если бы это был физический ящик, в который ценности помещаются для последующего извлечения. Скорее, если что-то является хранилищем ценности, это означает, что оно уже давно ценится людьми. И благодаря успешной истории люди имеют все основания полагать, что оно будет цениться и в будущем. Таким образом, оно сохраняет свою покупательную способность с течением времени. Многие вещи используются для хранения ценности. Например, крупный рогатый скот долгое время служил хранилищем ценности.

У людей есть все основания полагать, что скот можно использовать для удовлетворения своих желаний. Его можно доить, есть, использовать для работы на ферме и многое другое. Благодаря этой полезности, если вы захотите продать свой скот, вы наверняка найдете покупателей. Недвижимость – еще один популярный способ сохранения ценности с хорошей репутацией. У людей есть все основания полагать, что владение землей принесет им пользу. Они могут жить на этой земле, использовать ее для производства продуктов питания, развивать ее, сдавать в аренду и так далее. Скорее всего, и через тысячу лет скот и недвижимость будут попрежнему цениться людьми. Самым популярным хранилищем ценности являются *деньги*.

Деньги как экономическое явление несколько сложнее, чем скот или недвижимость. Чтобы понять его, нам необходимо усвоить еще одно понятие: разницу между *прямым* и *непрямым обменом*. Представьте себе ситуацию, когда фермер разводит кур, а по соседству с ним живет портной, который производит рубашки. Если фермеру нужна рубашка, а портному – пара кур, они могут вступить в простейший вид экономического обмена, который называется «прямой обмен» или «бартер», когда фермер напрямую обменивает своих кур на рубашку портного. Бартер, как правило, не очень удобен и неэффективен, так как требует от обеих сторон конкретного желания получить предмет, которым торгует другой человек. Если бы вместо рубашки фермеру нужны были туфли, обмен бы не состоялся.

В отличие от бартера, «косвенный обмен» происходит, когда обмениваемые товары не являются конечными товарами. Так, фермер может обменять своих кур на бензин не потому, что ему нужен бензин, а потому, что он может обменять бензин у портного на желаемую рубашку. В этой ситуации мы бы назвали бензин «средством обмена» – промежуточным этапом между фермером и конечным товаром, который он желает получить.

Средства обмена – удивительная вещь. Они позволяют огромным сетям людей торговать и сотрудничать без необходимости знать друг друга, говорить на одном языке или разделять одни и те же предпочтения. Самым популярным средством обмена в экономике являются *деньги*, и они, по сути, позволяют обменять любой товар на любой другой. Фермер может превратить своих кур в Ламборджини, если сначала обменяет достаточное их количество на деньги.

С помощью денег гораздо легче планировать, экономить и инвестировать. Фермер может продать своих цыплят летом за деньги, которые он планирует использовать зимой. Или же он может вложить свои деньги в проекты, которые принесут прибыль. Без денег управлять инвестициями гораздо сложнее – фермеру придется искать проекты, которые принимают цыплят непосредственно в качестве инвестиций. Используя деньги, он может продать своих цыплят, скажем, за евро, а затем вложить эти евро в другие проекты. Действительно, деньги – это прекрасное изобретение, которое делает всех нас богаче.

Деньги также являются отличным хранилищем стоимости. Австрийская школа экономики дает наилучшее объяснение этому. Согласно Людвигу фон Мизесу:

> Функции денег как передатчика стоимости во времени и пространстве также могут быть напрямую связаны с их функцией средства обмена. [5]

К такому же выводу пришел и Мюррей Ротбард:

> Во многих учебниках говорится, что деньги выполняют несколько функций: средство обмена, способ ведения учета, или «мера ценностей», «хранилище стоимости» и т. д. Но должно быть ясно, что все эти функции являются лишь методами одной большой функции – средства обмена.[6]

Другими словами, именно *потому, что* деньги являются общепринятым средством обмена, они хранят ценность. Таким образом, если Биткойн должен быть деньгами, то утверждать, что он может хранить ценность, не являясь средством обмена, значит ставить телегу впереди лошади.

Можно думать о «хранении ценностей» как о способе прогнозирования. Вы пытаетесь угадать, какие товары будут цениться в будущем. Если что-то полезно для людей – например, недвижимость, – оно, скорее всего, будет цениться. Если что-то уже используется в качестве средства обмена – например, бумажная валюта, – это верный признак того, что она будет цениться и в будущем. Это не гарантия, поскольку мы знаем случаи, когда бумажная валюта обесценивается из-за раздувания денежной массы центральными банками, но это все же положительный сигнал.

Если люди менее уверены в том, что что-то будет использоваться в качестве средства обмена в будущем, они с меньшей вероятностью будут использовать это в качестве хранилища ценности. Представьте, что вы живете на острове, где в качестве средства обмена обычно используются морские ракушки. Однажды вы слышите по радио, что новое революционное исследование показало, что ракушки опасно держать в руках и они могут вызвать рак. Вы ожидаете, что гораздо меньше людей будут принимать эти ракушки в качестве средства обмена, а значит, они станут худшим хранилищем ценности. Даже если исследование было ошибочным и ракушки не вызывают рак, простого убеждения общественности в том, что они *могут* вызывать рак, достаточно, чтобы превратить функционирующие деньги в нечто бесполезное. Сбои в работе сети Bitcoin Core в 2017 и 2021 годах и последующие отказы компаний от его использования в качестве платежного средства дают основания сомневаться в том, что BTC может работать как средство обмена, что снижает вероятность его превращения в реальное хранилище ценности в будущем.

Деньги и ценность

Хотя все деньги хранят ценность, не все хранилища ценности являются деньгами. Скот и недвижимость часто считаются хранилищами ценности, не являясь деньгами, поскольку они имеют другое, неденежное назначение. В связи с этим возникает ключевой вопрос: похож ли Биткойн на деньги, которые хранят ценность, поскольку используются в качестве средства обмена, или же Биткойн похож на скот и недвижимость, которые хранят ценность по немонетарным причинам? В 2010 году Сатоши обсуждал эту тему на форумах, где люди спорили о том, как Биткойн может приобрести ценность и почему. Он написал:

> В качестве эксперимента представьте, что существует некий металл, такой же редкий, как золото, но обладающий следующими свойствами:
>
> – обычного серого цвета;
> – плохой проводник электричества;
> – не особенно прочный, но и не вязкий и легко податливый;

> – не пригодный ни для каких практических или декоративных целей;
> – и одно особенное, волшебное свойство: может передаваться по каналу связи;
>
> Если бы он по какой-то причине приобрел хоть какую-то ценность, то любой человек, желающий передать богатство на большое расстояние, мог бы купить его, передать, а получатель продать.
>
> Возможно, он мог бы набрать начальную стоимость циклично, как вы предположили, благодаря людям, предвидящим его потенциальную полезность для обмена. (Я бы определенно купил). Может быть, коллекционеры, или любая случайная причина может послужить толчком к этому.
>
> Я думаю, что традиционная классификация денег была составлена в рамках убеждения, что в мире существует множество конкурирующих товаров, которые являются дефицитными, и что товар с наличием преимущества себестоимости обязательно опередит те, которые себестоимости не имеют. Но если бы в мире не было ничего, что обладало бы себестоимостью, что можно было бы использовать в качестве денег, а были бы только дефицитные, но не обладающие себестоимостью товары, я думаю, люди все равно выбрали бы что-нибудь.[7]

Это замечательная цитата по нескольким причинам. Во-первых, в данном контексте Сатоши использует термин «себестоимость» для обозначения неденежной потребительской стоимости. Золото и серебро, например, являются отличными средствами обмена, а также могут использоваться в промышленности. Табак и соль, другие исторические средства обмена, можно потреблять напрямую. Биткойн действительно имеет некоторую неденежную ценность, о чем будет рассказано ниже, но мысленный эксперимент Сатоши показывает, что *даже если бы* Биткойн не имел никакой неденежной пользы, одного факта, что он дефицитен и может быть отправлен по каналу связи – то есть стоимость транзакции крайне низка – было бы достаточно, чтобы придать ему ценность из-за «его потенциальной полезности для обмена». Другими словами, Сатоши считал, что Биткойн может сам создать свою стоимость, если люди поймут, что он может стать отличным средством обмена. Это делает Биткойн довольно уникальным изобретением. Это специально созданная платежная система, использующая валюту, которая была разработана таким образом, чтобы обладать лучшими денежными свойствами, чем все существующие деньги.

Другие способы использования

На первый взгляд кажется, что с Биткойном нельзя ничего сделать, кроме как отправить кому-то. Но у него есть и другие возможности. Блокчейн Биткойна – это публичная онлайн-бухгалтерия, которая поддерживается децентрализованной сетью компьютеров, а транзакции Биткойна становятся записями в этой бухгалтерии. Данные функции могут быть использованы в различных неденежных целях. Например, блокчейн можно использовать для хранения ценных данных, хотя это значительно дороже, чем другие способы хранения информации. Новые компании, работающие в сфере социальных сетей, используют эту функцию для создания платформ без цензуры на блокчейне. Другими сферами применения могут быть реестры активов, новые системы голосования или проверка личности для повышения безопасности в Интернете.

По сравнению с полезностью Биткойна как общей платежной системы эти способы применения кажутся малозначимыми, но они существуют.

Думать, что Биткойн можно считать хранилищем ценности из-за его немонетарных свойств, все равно что считать долларовые купюры хранилищем ценности, потому что их можно использовать в качестве хвороста или туалетной бумаги. Хотя такая польза и существует, она ничтожна по сравнению с ценностью безопасного, международного средства обмена. Сатоши понимал, что способность Биткойна к пересылке – это главная особенность, которая придает ему ценность. Однако эта особенность была намеренно уничтожена разработчиками Bitcoin Core в результате чего BTC практически не имеет уникального преимущества по сравнению с другими криптовалютами. Другие монеты не только имеют более низкие комиссии, но и превосходят Биткойн по немонетарной функциональности.

Учитывая субъективную природу ценности, можно *предположить*, что рынок может выбрать BTC в качестве хранилища ценности. Но также возможно, что рынок выберет в качестве хранилища ценности старые вонючие спортивные носки. Возможно, но маловероятно. Разумнее считать, что криптовалюта, имеющая наилучшие шансы стать хранилищем ценности, должна усилить все свои положительные свойства и минимизировать отрицательные. Неудобные и дорогие транзакции – не самая желательная черта любого хранилища ценности или средства обмена. Известный интернет-предприниматель Ким Дотком, основатель MegaUpload, выразил схожие чувства в беседе в январе 2020 года, сказав:

> Чтобы стать очень успешной криптовалютой, вам нужно обеспечить быстрые и дешевые транзакции, без этого никак не обойтись. Приятно быть хранилищем ценности, но если вы действительно хотите преуспеть, вам нужно быть электронными деньгами.

Ким также отметил, что подавляющее большинство людей до сих пор не имеют опыта использования криптовалют, и для того, чтобы привлечь их, необходимо, чтобы комиссии были низкими, а надежность – высокой.

> Большинство людей ничего не знают о текущих войнах и о токсичности внутри криптосообщества. Они выбирают ту валюту, которая дает им самые дешевые комиссии, самые быстрые транзакции, наибольшую надежность, и в настоящее время, к сожалению, это не Биткойн.[8]

Представьте себе криптовалюту, обладающую всеми свойствами BTC, но в дополнение к этому позволяющую проводить мгновенные, почти бесплатные транзакции по всему миру и являющуюся специально созданным средством обмена для XXI века. Ее полезность была бы на порядки выше, чем у валюты без этой функциональности. Таков был первоначальный план создания Биткойна, и он остается планом для Bitcoin Cash и других криптовалют.

5. Ограничение размера блока

Если бы вы сказали мне в 2011 году, что в 2017 году мы не увеличим размер блока,
я бы ответил: «Этого не может быть». [1]

– Стивен Пэйр, генеральный директор BitPay

Один-единственный технический параметр позволил разработчикам Bitcoin Core превратить Биткойн в совсем другой проект: «ограничение размера блока». Ограничение по размеру блока – это просто максимальный размер блока, допустимый в сети. Помните, что транзакции объединяются в блоки, поэтому чем больше транзакций, тем больше блоки. Это делает ограничение размера блоков фактически максимальным ограничением пропускной способности Биткойна. Bitcoin Core использовал крошечный лимит размера блоков, чтобы искусственно ограничить пропускную способность сети до малой части её потенциала.

Ограничение размера блока не должно было быть важным параметром, и оно не должно было быть достигнуто. Размер блока должен был оставаться намного выше среднего. Блоки никогда не должны были быть полностью заполнены, за редким исключением.

Требуется дополнительное пространство

Полный блок означает, что транзакций, которые необходимо обработать, больше, чем может поместиться в одном блоке, что немедленно приводит к росту комиссий и образованию задержек. В настоящее время один блок BTC вмещает 2 000—3 000 транзакций и создается каждые десять минут. Если 18 000 человек пытаются совершить одну транзакцию в течение десяти минут, то для обработки всех транзакций сети потребуется не менее шести блоков. Это один час на обработку каждой транзакции в очереди. Если 150 000 человек пытаются использовать Биткойн одновременно, то для обработки всех транзакций потребуется не менее пятидесяти блоков. Это более восьми часов ожидания.

Задержка обработки – не единственная проблема при перегрузке сети. Когда блоки переполнены, комиссия начинает расти. Более высокая комиссия не гарантирует, что ваша транзакция будет обработана быстро; она лишь позволяет вам сократить очередь перед другими транзакциями. Поскольку сеть не может обрабатывать более 3 000 транзакций в одном блоке, образуется очередь. Повышение комиссии увеличивает шанс того, что майнеры включат вашу транзакцию в следующий блок, но если достаточно людей заплатят больше, чем вы, ваша транзакция будет отодвинута дальше в очереди. Это приводит к росту платы и создает ужасные условия для пользователей. Как только блоки переполняются, комиссия может вырасти с десяти центов до доллара, затем до пяти, десяти, двадцати, пятидесяти долларов или даже больше, если эту комиссию готовы платить достаточное количество людей. Во время скачков платы в 2017 и 2021 годах некоторые сложные транзакции стоили более 1000 долларов, и в итоге мне пришлось платить несколько раз. Быстрый поиск в блокчейне транзакций с комиссией от 900 до 1100 долларов дает почти 35 000 результатов.[2]

Биткойн часто сравнивают с электронной почтой за его способность мгновенно соединять людей через интернет. Представьте себе, что электронная почта не могла бы выдержать 150 000 человек и требовала бы восемь часов на отправку и получение сообщений. Это, несомненно, считалось бы досадным недостатком системы. Однако при таких сбоях в сети транзакции могут зависнуть на несколько дней, а то и на целую неделю на пике нагрузки. Именно поэтому предполагалось, что предельный размер блока будет намного превышать

спрос на транзакции, как отдаленное техническое ограничение, которое не повлияет на функциональность системы. Биткойн будет масштабироваться по мере использования, а лимит будет либо увеличен, либо вообще снят.

Разрешение блокам расти естественным образом позволило бы сохранить Биткойн в качестве цифровой денежной системы с низкими комиссиями за транзакции и всеобщим доступом к блокчейну. Но разработчики Core хотели превратить Биткойн в расчетную систему для крупных переводов, поэтому они отказались увеличивать размер блока. Единственная причина, по которой комиссии выросли до астрономических уровней, а сеть стала ненадежной, заключалась в том, что блоки были слишком малы, чтобы удовлетворить спрос.

Бесчисленное множество разработчиков, предпринимателей и энтузиастов знали, что лимит размера блока необходимо увеличить. Они знали, что переполненные блоки приведут к ужасному пользовательскому опыту, и видели, что блоки становятся все более заполненными по мере роста популярности Биткойна. Однако, несмотря на бесконечные споры и просьбы пользователей, разработчики Core отказались увеличить лимит. Они до сих пор не смогли значительно увеличить максимальную пропускную способность транзакций по сравнению с уровнем 2010 года. Одна фотография на вашем смартфоне по размеру больше целого блока BTC, иногда значительно больше, в зависимости от качества изображения. В конечном итоге это повлекло раскол в криптовалютной индустрии и стало причиной создания Bitcoin Cash.

Причина ограничения размера блока

К тому времени, когда Сатоши Накамото покинул Биткойн, над проектом работало множество увлеченных и талантливых разработчиков, но двое из них были исключительными: Гэвин Андресен и Майк Хирн. Сатоши выбрал Андресена в качестве своего преемника и ведущего разработчика проекта. Естественно, он также был сторонником больших блоков. На протяжении многих лет он писал в своем блоге[3] популярные статьи о Биткойне и масштабировании, культуре разработчиков, экономике и других темах.[4] Он был мягким человеком, возможно, даже в ущерб себе. Хирн, напротив, был более прямолинейным разработчиком, который более открыто выступал против сторонников малых блоков, которые, по его мнению, подрывали проект. Его предыдущий опыт работы был особенно важен. Хирн ушел из Google, чтобы работать над Биткойном. Работая в Google, он три года занимался планированием пропускной способности Google Maps – одного из самых популярных сайтов в мире. Таким образом, он был хорошо знаком с проблемами пропускной способности сети. Как и Сатоши, Андресен и Хирн были сторонниками больших блоков и не считали, что у Биткойна будут проблемы с масштабированием. В своих сообщениях в блогах, электронных письмах, беседах на форумах и публичных интервью Андресен и Хирн лучше, чем кто-либо другой, отразили первоначальное видение Биткойна. Их комментарии рекомендуются к прочтению и цитируются в этой книге.

Когда писался первоначальный код Биткойна, не было четкого ограничения на размер блоков, которые можно было бы создавать. Все изменилось в 2010 году, когда Сатоши добавил ограничение на размер блока, чтобы предотвратить потенциальную атаку типа «отказ в обслуживании», пока Биткойн был еще молод. В своем блоге Гэвин Андресен объяснил причины первоначального ограничения:

> «… Ограничения были введены для предотвращения атаки „ядовитого блока“ на отказ в обслуживании сети. Мы должны были беспокоиться об атаках типа „отказ в обслуживании“, пока они были недороги для злоумышленника… Атака, которую блокировало это ограничение, сегодня стоит гораздо дороже…»

> 15 июля 2010 года на бирже торговалось около одиннадцати тысяч Биткойнов по средней цене около трех центов за штуку. Вознаграждение за блок тогда составляло 50 BTC, поэтому майнеры могли продать блок монет примерно за 1,50 доллара.
>
> Это дает приблизительное представление о том, во сколько злоумышленнику обойдется создание «ядовитого блока» для нарушения работы сети – доллар или два. Многие люди готовы потратить доллар или два «ради забавы» – им нравится доставлять неприятности, и они готовы потратить либо много времени, либо скромную сумму денег, чтобы доставить неприятности.[5]

Первоначальный лимит был установлен на уровне одного мегабайта, что позволяло теоретически ограничиться семью транзакциями в секунду. На практике реальный лимит составляет около трех-четырех транзакций в секунду, что соответствует 2000—3000 транзакций на цепочке за блок – намного выше фактического использования сети в те дни. Планировалось просто увеличить лимит или полностью его отменить. Андресен отметил на форумах:

> С самого начала планировалось поддерживать огромные блоки. Жесткое ограничение в 1 МБ всегда было временной мерой по предотвращению отказа в обслуживании.[6]

Рэй Диллинджер, еще один ранний сторонник Биткойна, сказал то же самое:

> Я тот парень, который изучил блокчейн в первой версии кода Биткойна, созданной Сатоши. У Сатоши не было ограничения в 1 МБ. Изначально ограничение было идеей Хэла Финни. И Сатоши, и я возражали, говорили, что оно не будет масштабироваться с 1 МБ. Однако Хэл был обеспокоен потенциальной DoS-атакой, и после обсуждения Сатоши согласился… Но все трое согласились, что ограничение в 1 МБ должно быть временным, потому что иначе оно никогда не будет масштабироваться.[7]

Единодушное согласие Сатоши, Хэла и Рэя особенно интересно, поскольку Хэл Финни часто считается сторонником небольших блоков. Но даже он согласился с тем, что ограничение в 1 МБ должно быть временным. Однако по сей день разработчики Bitcoin Core отказываются существенно увеличить размер блоков сверх первоначального уровня, установленного в 2010 году, несмотря на масштабные улучшения в программном обеспечении, оборудовании и сетевых технологиях. Практически все крупнейшие компании индустрии неоднократно пытались увеличить лимит, но разработчики Core отказались, даже после публичного согласия на увеличение. Вместо этого они изменили метрику размера блока на «вес блока» и заявили, что новый лимит составляет 4 МБ, но это в значительной мере трюк и не соответствует увеличению пропускной способности в четыре раза.

Искаженный дизайн

Простой причиной, по которой разработчики Core отказались увеличить лимит, – заключается в том, что они хотели изменить дизайн Биткойна. Чем быстрее заполнятся блоки, тем быстрее вырастут комиссии за транзакции, они считали это желательным. Жорж Тимон, разработчик Core, заявил: «Я согласен с тем, что увеличение лимита не только не плохо, но и даже хорошо для такого молодого и незрелого рынка, как комиссии Биткойна». [8] А Грег Максвелл

прямо заявил: «Нет ничего плохого в полностью заполненных блоках… Заполненные блоки – это естественное состояние системы». [9]

Чтобы понять, насколько радикальны эти идеи, сравните их с идеями, с которыми вы могли бы столкнуться в первые дни существования Биткойна, когда сеть Visa часто использовалась в качестве сравнения по пропускной способности транзакций. Еще в 2009 году Сатоши спросили о способности Биткойна к масштабированию, и он ответил:

> Существующая сеть кредитных карт Visa обрабатывает около 15 миллионов интернет-покупок в день по всему миру. Биткойн уже может обработать гораздо больше, чем это, используя существующее оборудование за долю стоимости. Он никогда не достигнет потолка масштабирования.[10]

Это было общепринятым пониманием в течение многих лет. Хотя сегодня мы бы назвали это частью «видения Сатоши», тогда это было почти всеобщим видением. Например, если бы вы изучали Биткойн в 2013 году, то, скорее всего, наткнулись бы на его страницу в Wiki. Вот что говорилось в разделе «Масштабируемость»:

> Основная сеть Биткойн может масштабироваться до гораздо более высоких объемов транзакций, чем сегодня, при условии, что узлы сети работают в основном на высококлассных серверах, а не на настольных компьютерах. Биткойн был разработан для поддержки легких клиентов, которые обрабатывают только небольшие части цепочки блоков…
>
> Конфигурация, в которой подавляющее большинство пользователей синхронизируют легковесные клиенты с более мощными магистральными узлами, способна масштабироваться до миллионов пользователей и десятков тысяч транзакций в секунду…
>
> Сегодня сеть Биткойна ограничена устойчивой скоростью в 7 транзакций в секунду благодаря некоторым искусственным ограничениям. Они были введены для того, чтобы не дать людям увеличить размер цепочки блоков до того, как сеть и сообщество будут к этому готовы. Как только эти ограничения будут сняты, максимальная скорость транзакций значительно возрастет… При очень высокой скорости транзакций размер каждого блока может превышать пол гигабайта.[11]

Это было общеизвестно. Все понимали, что система рассчитана на масштабирование с помощью больших блоков, и это даже не вызывало споров. Андресен заявил, что масштабируемость Биткойна была частью той причины, которая привела его в проект:

> Когда я впервые услышал о Биткойне, он был достаточно небольшим проектом, чтобы я мог прочитать все, и я прочитал, включая все эти сообщения в рассылке. Обещание системы, которая по масштабам может сравниться с Visa, – это часть того видения, которое помогло мне выбрать Биткойн.[12]

В 2013 году Visa обрабатывала, в среднем, около 2 000 транзакций в секунду. Чтобы получить 2 000 транзакций в секунду в Биткойне, блоки должны были быть примерно по 500 МБ, что является вполне возможным объемом. Современные мобильные телефоны могут легко записывать и загружать HD-видео размером в 1 гигабайт, что в несколько раз превышает размер блока Биткойна, содержащего более миллиона транзакций. Масштабирование до такого уровня требует большего, чем простое увеличение максимального размера блока,

но нет никаких фундаментальных причин, почему это нельзя сделать. На самом деле Bitcoin Cash уже успешно создал несколько блоков размером 32 МБ, а недавнее ответвление Bitcoin Cash, Bitcoin SV, даже создало блок размером 2 ГБ. Эти сети не сломались. У Сатоши был простой и окончательный ответ на вопросы о размере блоков:

> Было бы неплохо, чтобы файлы блокчейна оставались небольшими, пока это возможно. Конечное решение будет заключаться в том, чтобы не беспокоиться о том, насколько большими они станут.[13]

Высокие тарифы и медленные транзакции

Зачем разработчикам Bitcoin Core высокие комиссии? Для начинающего энтузиаста Биткойна или даже для обычного человека очевидно, что это плохая идея. Но на самом деле высокие комиссии – это неизбежный результат философии сторонников малых блоков. Чтобы понять почему, нам нужно более внимательно проанализировать систему. Как объяснялось в главе 2, майнеры получают вознаграждение двумя способами. Они получают комиссионные за обработку транзакций и вознаграждение за новый блок. Поскольку вознаграждение за блок со временем уменьшается, единственным источником дохода в конечном итоге будут транзакционные сборы. А поскольку разработчики Bitcoin Core стремятся к созданию малых блоков, единственный способ для майнеров заработать в их системе – это чрезвычайно высокие комиссии за транзакции. Биткойн не может работать без оплаты труда майнеров, а если они могут обрабатывать только 3 000 транзакций в одном блоке, то для поддержания безопасности комиссии должны составлять сотни или тысячи долларов за транзакцию. Разработчик Bitcoin Core Жорж Тимон открыто говорил об этой проблеме:

> В долгосрочной перспективе Биткойну нужен конкурентный рынок комиссий, чтобы поддерживать [доказательство работы] после сокращения вознаграждений [за блок]. Я очень рад, что теперь он у нас есть…[14]

Питер Вуйль, другой Bitcoin Core разработчик, сказал:

> Мое личное мнение заключается в том, что мы, как сообщество, должны позволить рынку комиссий развиваться, и чем раньше тем лучше.[15]

Они тактично называют задержки транзакций и высокие комиссии «рынком комиссий», где пользователи торгуются друг с другом за крошечное пространство внутри блоков. И эта странная и ненужная модель безопасности является поводом для празднования, где разработчики Core хвалят высокие комиссии и медленные транзакции. Грег Максвелл заявляет:

> Бремя комиссии является преднамеренной частью дизайна системы и, насколько мы понимаем, необходимо для ее долгосрочного выживания. Так что, да. Это хорошо.[16]

А когда в декабре 2017 года плата выросла до 25 долларов, Максвелл пресловуто отреагировал:

> Лично я пью шампанское за то, что поведение рынка действительно обеспечивает уровень активности, позволяющий оплачивать безопасность без инфляции, а также создает очередь на оплату комиссий, необходимых для стабилизации прогресса консенсуса по мере уменьшения вознаграждений за блоки.[17]

Конечно, Сатоши Накамото не разрабатывал Биткойн таким образом. Предполагалось, что майнеры будут окупать свои затраты за счет обработки большого количества низкооплачи-

ваемых транзакций в больших блоках. На форумах Сатоши спросили о долгосрочной модели доходов для майнеров. Он объяснил:

> Через несколько десятилетий, когда вознаграждение станет слишком маленьким, плата за транзакции станет основным вознаграждением для майнеров. Я уверен, что через 20 лет объем транзакций будет либо очень большой, либо его не будет вообще.[18]

Заметьте, он не сказал: «Через 20 лет будет либо большой объем транзакций, либо маленький объем с чрезвычайно высокими комиссионными за транзакции». Это показалось бы сомнительным любому здравомыслящему человеку. Он предсказал либо большой объем, либо его полное отсутствие.

Новый Биткойн

Искусственно ограничив размер блока, разработчики Bitcoin Core нашли способ полностью изменить динамику системы. Мало того, что пользовательский опыт изменился с «почти мгновенных и бесплатных транзакций» на «дорогие и ненадежные транзакции», радикально изменилась и базовая экономическая модель. BTC теперь делает ставку на то, что будущие пользователи будут готовы платить сотни или тысячи долларов за транзакцию на цепочке, несмотря на наличие более совершенных альтернатив. В противном случае майнерам придется закрыть большую часть своего оборудования, потому что оно не будет приносить прибыль.

Учитывая это – не будет преувеличением сказать, что BTC был захвачен, а первоначальный дизайн был заменен на новый, спекулятивный. Именно поэтому Виталик Бутерин, сооснователь Ethereum, публично заявил:

> Я считаю BCH «законным» претендентом на имя Биткойна. Я считаю, что неспособность Биткойна увеличить размер блока, чтобы сохранить разумные комиссии, является большим (несогласованным) изменением «первоначального плана», что с моральной точки зрения равносильно хард форку.[19]

Неспособность Bitcoin Core увеличить лимит размера блоков не была просто научной. Она имела реальные последствия для бизнесов, работающих на Биткойне или просто принимающих его к оплате. После скачка комиссий в 2017 году индустрия Биткойна впервые столкнулась с проблемой отторжения. Когда популярная игровая платформа Steam объявила о том, что больше не принимает Биткойн, она публично объяснила причины этого[20]:

> С сегодняшнего дня Steam больше не будет поддерживать Биткойн в качестве способа оплаты на нашей платформе из-за высоких комиссий и волатильности стоимости Биткойн… [Комиссия за транзакции, взимаемая с клиента сетью Биткойн, резко выросла в этом году и на прошлой неделе достигла почти $20 за транзакцию (по сравнению с примерно $0,20, когда мы первоначально добавили Биткойн)]…
>
> При оформлении заказа в Steam покупатель переводит сумму X Биткойнов за стоимость игры, плюс У сумму Биткойнов для покрытия комиссии за транзакцию, взимаемой сетью Биткойн. Стоимость Биткойна гарантируется только на определенный период времени, поэтому если транзакция не будет завершена в течение этого времени, то сумма Биткойна, необходимая для покрытия транзакции, может измениться. В последнее время сумма может измениться настолько, что может значительно отличаться.

> Обычным решением в этом случае является либо возврат пользователю первоначального платежа, либо просьба перевести дополнительные средства для покрытия оставшегося баланса. В обоих случаях пользователь снова оплачивает комиссию за транзакцию в сети Биткойн. В этом году мы наблюдали, как все большее число клиентов попадает в такое положение. Поскольку комиссия за транзакцию сейчас так высока, возвращать деньги или просить клиента перевести недостающий баланс нецелесообразно (что само по себе чревато повторной недоплатой, в зависимости от того, насколько изменится стоимость Биткойна, пока сеть Биткойн будет обрабатывать дополнительный перевод).
>
> На данный момент поддержка Биткойна как способа оплаты стала невозможной. Мы можем пересмотреть вопрос о том, имеет ли Биткойн смысл для нас и для сообщества Steam, позднее…
>
> – Команда Steam

Невозможно винить Steam за их решение. Попытка использовать Биткойн, когда блоки переполнены, могла стать ужасным опытом. Клиенты, желающие получить возврат, гарантированно потеряют деньги. Если они возвращают деньги за игру стоимостью 30 долларов, а комиссия за транзакцию стоит 10 долларов, пользователи могут потерять 20 долларов и ничего не получить. На мой взгляд, если бы вы хотели сломать Биткойн, лучшим способом было бы заполнять блоки записями о транзакциях до отказа. Если бы высокие комиссии и задержки в обработке были вызваны техническим сбоем, это, возможно, было бы лучше для Биткойна, поскольку это новая технология и проблему можно было бы считать случайностью. Но вместо этого общественности внушили, что высокие комиссии – это вполне нормально, что не стоит использовать Биткойн для повседневных покупок и что блокчейн на самом деле не может масштабироваться.

У сторонников BTC есть несколько стандартных ответов на эту критику. Если они не знают, что высокие комиссии являются частью намеренного редизайна Биткойна, они часто любят говорить: «На самом деле комиссии – это не проблема. Посмотрите, в этот самый момент комиссии низкие!» Но это слабый аргумент. В любой момент времени плата за пользование BTC может быть низкой, но только потому, что в сети мало трафика. Если её будет использовать больше людей, то загрузка быстро увеличится, и плата снова подскочит. Это похоже на автомобильное движение. Если в три часа ночи дороги пустые, это не значит, что Лос-Анджелес решил свои проблемы с пробками. Если блоки BTC не заполнены, то сборы будут низкими, но если блоки будут заполнены и активность возрастет, то сборы неизбежно вырастут до экстремальных уровней.

А что насчет вторых слоев?

Другая попытка оправдать философию малых блоков заключается в обращении ко вторым слоям, поскольку, если большинство транзакций происходит вне цепи, то, возможно, на вторых слоях комиссии могут быть низкими. Хотя в Биткойне действительно имеет смысл создавать несколько уровней, для правильной работы базовый уровень должен быть масштабируемым. Если базовый уровень может обрабатывать только семь транзакций в секунду, он даже близко не будет достаточно надежным для создания дополнительных уровней. Вторые уровни все равно должны взаимодействовать с базовым, поэтому высокие комиссии остаются фундаментальной проблемой. Например, для использования Lightning Network все еще тре-

буются периодические транзакции на первом уровне цепи, и комиссии за записи на первом уровне кто-то должен оплачивать. Сейчас многие популярные кошельки субсидируют эти расходы для своих пользователей, но если плата в $50+ станет нормой, такая модель будет просто нежизнеспособной.

Илон Маск – один из тех, кто, похоже, понимает ценность масштабирования базового уровня для криптовалют. В своем Twitter, посвященном дизайну сети, он как инженер поделился мыслями:

> BTC и ETH используют многоуровневую систему транзакций, но скорость транзакций на базовом уровне медленная, а стоимость транзакций высокая… Есть смысл в увеличении скорости транзакций на базовом уровне и минимизации стоимости транзакций… Размер и частота блоков должны постоянно увеличиваться, чтобы поддерживать высокую пропускную способность.[21]

Если бы Маск был в то время рядом, похоже, он согласился бы с Сатоши, Андресеном, Хирном и большинством первых предпринимателей, использовавших Биткойн, таких как я. Замены для дешевых транзакций на цепочке не существует.

Техническим параметром, который в итоге разделил Биткойн на две части, стал лимит размера блока. До того как блоки стали заполняться, доля BTC на рынке криптовалют составляла около 95%. Как только блоки начали заполняться, доля рынка быстро сократилась. На пике сбоя сети в январе 2018 года она упала до 32%, и многие пользователи, бизнесы и разработчики полностью покинули BTC. По состоянию на март 2023 года доля рынка BTC составляет около 40% и, скорее всего, снова упадет при новых сбоях в сети. Если бы разработчики Bitcoin Core просто увеличили лимит размера блока до разумного уровня, я уверен, что многие конкурирующие криптовалютные проекты просто не существовали бы, индустрия осталась бы объединенной вокруг одной монеты, а BTC продолжал бы оставаться главной цифровой денежной системой в интернете. Вместо этого разработчики Bitcoin Core переключились на расчетную систему с высокими комиссиями и ненадежными транзакциями, оставив для цифровой валюты пустое место, которое до сих пор не заполнено.

6. Пресловутые узлы

Биткойн был разработан для масштабирования с помощью больших блоков. Так почему же кто-то считает, что большие блоки – это проблема? Хотя невозможно узнать внутренние мотивы разработчиков Bitcoin Core, в этой главе мы рассмотрим заявленные ими причины, по которым блоки остаются малыми. Все возражения против больших блоков вращаются вокруг одной основной идеи: с увеличением размера блока увеличивается и стоимость запуска полного узла. Чем дороже содержание узла, тем меньше людей будут иметь возможность управлять им, и тем более централизованной станет сеть. Таким образом, благодаря тому, что блоки остаются малыми, больше людей могут управлять узлами, что позволяет сохранить децентрализованность сети. Разработчик Bitcoin Core Владимир ван дер Лаан четко сформулировал это в 2015 году:

> Я понимаю преимущества масштабирования, я не сомневаюсь, что увеличение размера блока будет *работать*. Хотя могут возникнуть непредвиденные проблемы, я уверен, что они будут решены. Однако это может сделать Биткойн менее полезным в том, что отличает его от других систем: возможность для людей «быть собственным банком» без особых инвестиций в связь и вычислительное оборудование.[1]

С этой идеей связано несколько проблем. В первую очередь, идея о том, что пользователям нужно запускать собственные полные узлы, чтобы «быть собственным банком», неверна. Биткойн был разработан таким образом, чтобы обычным людям *не нужно* было запускать свои собственные полные узлы. Они могут использовать более легкое программное обеспечение. Помните, что полный узел загружает копию всего блокчейна и проверяет каждую транзакцию в сети. В этом нет необходимости почти ни для кого. Сатоши разработал Биткойн с учетом упрощенной верификации платежей (УВП), которая позволяет пользователям проверять собственные транзакции с помощью небольшого количества данных. Используя УВП, вы не сможете проверить транзакции другого человека, как и не сможете проверить все транзакции, которые когда-либо совершались, но у большинства людей нет причин, чтобы делать это. Сатоши не был настолько глуп, чтобы разрабатывать денежную систему, в которой каждый пользователь должен был загружать и проверять транзакции всего мира. Такая система никак не сможет масштабироваться.

Во-вторых, тот факт, что стоимость проверки увеличивается с ростом размера блоков, не является проблемой. Сатоши не мог выразиться яснее, когда писал:

> Текущая система, в которой каждый пользователь является сетевым узлом, не предназначена для крупномасштабной конфигурации. Это было бы, как если бы каждый Usenet-пользователь запустил свой собственный NNTP-сервер. Дизайн позволяет пользователям просто быть пользователями. Чем больше нагрузка на узел, тем меньше их будет. Эти несколько узлов будут большими серверными фермами. Остальные будут клиентскими узлами, которые только выполняют транзакции и не генерируют.[2]

А также когда он заявил:

> Только людям, которые пытаются создать новые монеты, потребуется запускать сетевые узлы. Поначалу большинство пользователей будут управлять сетевыми узлами, но по мере того, как сеть будет расти дальше

> определенного предела, она будет все больше и больше переходить в руки специалистов с серверными фермами и специальным оборудованием.[3]

Сатоши говорил настолько ясно, что его слова невозможно неверно интерпретировать. В его идее был огромный смысл. В любой отрасли бизнесы специализируются в том, что у них получается лучше всего. Обслуживание сети Биткойна ничем не отличается в данном случае. Сатоши представлял себе «большие серверные фермы» в центре сети, к которым будут подключаться обычные пользователи. Можно не соглашаться с этой идеей, но именно так и был задуман Биткойн. Это аналог электронной почты. Технически любой человек может создать свой собственный почтовый сервер и подключиться к глобальной почтовой сети. Но зачем? Его сложно настроить и поддерживать, и у подавляющего большинства людей нет причин делать это. Поэтому в большинстве случаев мы оставляем это специалистам.

Мнение большинства

Гэвин, Майк и Сатоши были не единственными, кто так думал. Ранние форумы переполнены сообщениями других разработчиков и пользователей, которые также понимали, что система не требует от большинства запуска собственного узла. Алан Рейнер, создавший популярный кошелек Armory, сказал в 2015 г.:

> Цели «глобальная сеть транзакций» и «каждый должен иметь возможность запустить полноценный узел на своем ноутбуке Dell за 200 долларов» несовместимы. Мы должны признать, что глобальная система транзакций не может быть полностью/постоянно проверена каждым человеком и его матерью.[4]

Даже сторонники Bitcoin Core признали, что их взгляд на ноды сильно отличается от первоначального. «Theymos» – это псевдоним владельца самых популярных дискуссионных платформ для Биткойна, который впоследствии сыграл центральную роль в цензуре сторонников больших блоков, признал:

> Сатоши определенно намеревался увеличить жесткий максимальный размер блока… Я считаю, что Сатоши ожидал, что большинство людей будут использовать что-то вроде легкого узла, и только компании и настоящие энтузиасты будут использовать полные узлы. Мнение Майка Хирна схоже с мнением Сатоши.[5]

Более того, даже не совсем ясно, уменьшится ли общее число людей, управляющих узлами, если затраты возрастут. Общее число *любителей*, управляющих узлами, будет меньше, но если бы Биткойн стал новой финансовой сетью мира, тысячи компаний имели бы финансовый стимул для запуска собственных узлов. Как говорит Сатоши в научной работе:

> Бизнесы, которые часто получают платежи, вероятно, все же захотят запустить собственные узлы для более независимой безопасности и быстрой проверки.[6]

Религия полного узла

Давайте углубимся в причины, по которым сторонники малых блоков считают, что полные узлы так важны. На странице Bitcoin Wiki есть статья о полных узлах, которая хорошо объясняет их философию. Этот длинный отрывок – отличное резюме:

> Полные узлы составляют основу сети. Если бы все использовали легкие узлы, Биткойн не смог бы существовать… Легкие узлы делают все, что скажет большинство майнеров. Поэтому, если бы большинство майнеров объединились, чтобы, например, увеличить вознаграждение за блок, легкие узлы слепо согласились бы с этим. Если бы это произошло, сеть раскололась бы так, что легкие и полные узлы оказались бы в разных сетях, использующих разные валюты…
>
> Если все предприятия и многие пользователи держат полные узлы, то такое разделение сети не является критической проблемой, потому что пользователи легких клиентов быстро заметят, что они не могут отправлять или получать Биткойны от/к большинству людей, с которыми они обычно ведут бизнес, и поэтому они перестанут использовать Биткойн, пока злые майнеры не будут побеждены…
>
> Однако если в этой ситуации почти все в сети используют легкие узлы, то все продолжат совершать транзакции друг с другом, а значит, Биткойн вполне может оказаться «захваченным» злобными майнерами. На практике майнеры вряд ли будут пытаться осуществить что-то подобное описанному выше сценарию, пока в сети распространены полные узлы, потому что они потеряют много денег.
>
> Но стимулы полностью меняются, если все будут использовать легкие узлы. В этом случае у майнеров определенно есть стимул изменить правила Биткойна в свою пользу. Использование легкого узла является достаточно безопасным, потому что большая часть экономики Биткойна использует полные узлы. Поэтому для выживания Биткойна очень важно, чтобы подавляющее большинство экономики Биткойна поддерживалось полными, а не легкими узлами.[7]

Эти идеи стали ортодоксальными. Тот, кто пытается разобраться в Биткойне сегодня, может даже не знать, что эта статья сильно предвзята и придерживается точки зрения сторонников малых блоков, с которой сам создатель Биткойна не согласился бы. Здесь есть два основных момента:

1) У майнеров есть стимул «захватывать» Биткойн, изменяя правила в свою пользу, например, увеличивая вознаграждение за блок.

2) Майнерам не позволяют случайно менять правила, потому что полные узлы не «слепо подчиняются» большинству майнеров.

Оба эти утверждения неверны. Во-первых, у майнеров нет стимула произвольно менять правила Биткойна. На первый взгляд может показаться, что майнеры могут получать прибыль от создания новых монет из воздуха. Однако при этом упускается из виду причина, по которой Биткойн вообще имеет ценность. У Биткойна нет себестоимости; ценность возникает благодаря сложной сети убеждений, которые люди имеют обо всей сети Биткойн. Если бы майнеры решили добыть миллиард новых Биткойнов для себя, они бы уничтожили базовое доверие к системе, что уничтожило бы ценность каждого Биткойна. У них может быть еще миллиард Биткойнов, но каждый из них не будет ничего стоить. Майк Хирн понимал эту динамику:

> Рациональные майнеры не должны подрывать основы своего собственного богатства. Делать вещи, которые значительно снижают полезность системы, очевидно, даже в среднесрочной перспективе, потому что это приведет к тому, что люди просто откажутся от системы и с отвращением продадут свои монеты, снизив цену. Думаю, будет справедливо сказать, что невозможность лично покупать такие базовые вещи, как еда или напитки, снизила бы полезность Биткойна для многих.[8]

Хирн понимал, что майнеры не представляют угрозы для системы. Майнеры *меньше* всего заинтересованы в том, чтобы ломать Биткойн, поскольку их единственный доход – это плата за транзакции и вознаграждение за блок, которые выражаются в Биткойнах, которые должны быть проданы на рынке.

Второе основное утверждение статьи в Wiki – это то, что полные узлы могут каким-то образом предотвратить изменение правил сети. Это невозможно. Помните, что полные узлы не могут добавлять блоки в цепь. Они могут только проверять, действительны ли блоки и транзакции. Представьте, что в протоколе обнаружена новая ошибка, которая существенно ломает Биткойн, и программное обеспечение должно быть обновлено за короткий промежуток времени. Майнеры обновятся немедленно, поскольку их прибыль зависит от работы сети. Но что произойдет, если все остальные, у кого есть полные узлы, не обновят их? Помешают ли майнерам обновляться вообще? Вовсе нет. Майнеры продолжали бы исправно добавлять блоки в цепочку, а полные узлы просто отделились бы от основной сети и создали свою собственную новую сеть. Если в их новой сети не будет майнеров, они даже не смогут добавлять новые блоки в свою цепь, и никакие транзакции не будут обрабатываться. Это повод *использовать* легкие кошельки, так как вы не рискуете быть отделенными от основной сети.

Полные узлы не имеют власти, чтобы ограничить майнеров и не дать им изменить правила. Но правильнее будет сказать, что у них есть возможность *уведомлять* людей о том, что правила изменились. Согласно статье в Wiki, «злым майнерам» мешает изменить правила то, что они знают, что полные узлы остановят их, и как только мир узнает об их злых делах, ценность всей системы будет уничтожена. Поэтому бдительное око полных узлов держит майнеров в узде. В поверхностном смысле это верно. Майнеры действительно заинтересованы в том, чтобы не менять правила Биткойна произвольно, потому что это уничтожит стоимость их монет. Однако для того, чтобы уведомить людей о том, что правила изменились, не нужна большая сеть полных узлов. Для этого достаточно одного честного майнера или даже одного честного узла. Любой человек может доказать всему миру, что конкретный блок или транзакция не соответствует старым правилам. Даже если 100% майнеров были в сговоре, один-единственный честный узел все равно сможет доказать, что правила изменились. Это означает, что любой майнер, предприятие, криптовалютная биржа, исследователь или платежный процессор могут доказать, что правила изменились. Таким образом, гарантируется, что все узнают об этом.

Однако было бы чрезмерным упрощением утверждать, что полные узлы буквально не имеют власти, поскольку не все узлы созданы одинаковыми. Некоторые операторы полных узлов являются значимыми экономическими субъектами. Если любитель, управляющий узлом в своем подвале, будет вычеркнут из сети, это не имеет значения. А вот если выкинут крупный бизнес или криптовалютную биржу, это будет иметь значение, и стоимость монеты может пострадать. Таким образом, у майнеров есть серьезный стимул убедиться, что соответствующие экономические субъекты поддерживают предлагаемые ими изменения.

Честные и нечестные майнеры

Также было бы чрезмерным упрощением утверждать, что майнеры никогда не могли бы представлять риск для целостности Биткойна. Существует один четкий сценарий, при котором действия майнеров могут нанести ущерб. Как объясняется в техническом описании, Биткойн требует, чтобы большинство майнинговых мощностей – также называемых «хэшрейтом» – были честными, то есть не пытались намеренно разрушить систему. Честные майнеры стремятся получить прибыль, увеличивая полезность монеты и размер сети. Нечестные или злонамеренные майнеры, с другой стороны, представляют собой угрозу иного рода. Биткойн был специально разработан для работы даже среди нечестных майнеров, но только если они составляют меньшинство. Если бы большинство хешрейтов стали нечестными, то у Биткойна действительно возникли бы проблемы. Например, если враждебное правительство возьмет под контроль большинство хешрейтов, работа Биткойна может быть нарушена. Но даже при таком сценарии полные узлы не обеспечивают никакой защиты. Поскольку они не могут ни добавлять блоки в цепочку, ни контролировать поведение майнеров, они просто будут отброшены от основной сети. Как бы ни старался полный узел, у него просто не хватит сил спасти сеть с большинством нечестных майнеров.

Тот факт, что Биткойн требует, чтобы большая часть хешрейта была честной, не является уникальным недостатком дизайна. Все блокчейны, работающие по принципу proof-of-work, имеют такую же уязвимость. Реальная защита от нечестных майнеров – экономическая. Это стоимость майнинга. Чем дороже становится майнинг, тем выше издержки для недобросовестных участников, пытающихся получить большую часть хешрейта. Поэтому чем успешнее становится Биткойн, тем выше общий уровень его безопасности. Правительства, как правило, являются единственными, кто представляет реальную угрозу получения большинства вредоносного хешрейта, поскольку им не приходится действовать в рамках ограничений, связанных с прибылью и убытками. Если бы хорошо финансируемый государственный субъект попытался взломать Биткойн таким образом, сеть столкнулась бы с реальной проблемой, независимо от количества полноценных узлов.

Исторические факты очевидны. Биткойн не был создан для того, чтобы обычные пользователи могли управлять своими собственными узлами. Сатоши неоднократно открыто заявлял об этом, говоря:

> В проекте описывается легкий клиент, которому не нужна полная цепочка блоков… он называется УВП. Легкий клиент может отправлять и получать транзакции, он просто не может генерировать блоки. Ему не нужно доверять узлу для проверки платежей, он может проверять их сам.[9]

Масштабирование всегда было возможно с помощью больших блоков, а инфраструктуру должны были поддерживать специализированные «серверные фермы». Несмотря на это, разработчики Bitcoin Core посчитали, что дизайн Сатоши им не нравится, и решили, что могут улучшить его, заставив обычных пользователей загружать весь блокчейн и проверять каждую транзакцию, которая проходит по нему, даже если у них нет в этом финансовой заинтересованности. В настоящее время эта идея является основной в сети BTC, и именно по этой причине пропускная способность транзакций ограничена, а комиссии высоки.

7. Реальная стоимость больших блоков

> *«Я хочу иметь возможность запускать полный узел с моего домашнего компьютера». Кому это надо? Сатоши об этом не думал. Он считал, что в домашних условиях пользователи будут запускать узлы УВП, а полные узлы размещались в центрах обработки данных.*[1]
>
> *– Гэвин Андресен, 2015 г.*

Чрезмерное беспокойство по поводу стоимости больших блоков выглядит иррациональным, если проанализировать цифры. Не нужно делать никаких дополнительных расчетов, чтобы понять, что Биткойн может масштабироваться далеко за пределы блоков размером 1 МБ без существенного увеличения стоимости. На самом деле, учитывая крутую траекторию снижения расходов, даже при огромных масштабах они не будут запредельными для домашних пользователей, хотя Сатоши и не ожидал, что обычные пользователи будут запускать свои собственные узлы.

Чтобы иметь базовые возможности полного узла, необходимы две основные затраты: на хранение данных и на пропускную способность, которые за десятилетия резко упали вместе со стоимостью технологий в целом. Я наблюдал за этими тенденциями из первых рядов; моя компания MemoryDealers была создана для продажи компьютерного оборудования.

В книге *The Bitcoin Standard* Аммус пытается объяснить, почему масштабирование на цепочке нецелесообразно, опираясь на цифры:

> «Чтобы Биткойн мог обрабатывать 100 миллиардов транзакций, которые обрабатывает Visa, каждый блок должен быть размером около 800 мегабайт, то есть каждые десять минут каждый узел Биткойна должен был бы добавлять 800 мегабайт данных. За год каждый узел Биткойн добавит в свой блокчейн около 42 терабайт данных». [2]

Это верно. Если Биткойн обрабатывает примерно четыре транзакции в секунду на блок размером в один мегабайт, то 800 МБ блоков равны примерно 3200 транзакциям в секунду или ста миллиардам транзакций в год. Любой человек, знакомый с компьютерами, знает, что 800 МБ каждые 10 минут – это удивительно мало, учитывая, что это обеспечивает пропускную способность на уровне Visa. Однако Аммус приходит к противоположному выводу:

> «Такое количество полностью выходит за рамки возможной вычислительной мощности коммерчески доступных компьютеров сейчас или в обозримом будущем». [3]

Я не знаю, откуда Аммус взял эту информацию, но он, очевидно, не знаком с технологическими затратами. Даже при огромной пропускной способности ни затраты на хранение данных, ни затраты на пропускную способность не будут значительными для работы базового полного узла.

Расходы на хранение

Начнем с самых простых расчетов, а затем покажем, как еще больше сократить расходы. В сентябре 2023 года при быстром поиске жестких дисков объемом 8 ТБ на сайте Newegg.com первым результатом будет диск Seagate Barracuda, продающийся по цене 119.99[4] доллара, то есть 15 долларов за ТБ. Если Биткойн использует 42 ТБ в год, то это 630 долларов, или 52.50 доллара в месяц. Если учесть стоимость устройства NAS потребительского класса

с 6 отсеками для подключения накопителей, которое в настоящее время стоит около $670[5], то для хранения 100 000 000 000 транзакций это составит мизерные $1 300 в год – чуть больше ста долларов в месяц.

Конец ознакомительного фрагмента.