Андреас М. Антонопулос

Интернет денег

Посвящается биткойн-сообществу

Эта книга – сборник расшифрованных и отредактированных записей лекций. Большая часть ее содержания основана на личном опыте и неофициальных данных. Она призвана побудить к всесторонней оценке содержащихся здесь идей, подстегнуть к философским дискуссиям и проведению независимых исследований. Здесь нет советов, куда вложить деньги; не используйте данную работу в качестве руководства по принятию решений, связанных с инвестициями. Книга не может рассматриваться в качестве пособия по юридическим вопросам; по вопросам, связанным с применением законодательства конкретной страны, следует обращаться за консультациями к юристам. В этой книге, несмотря на все старания автора и издательства, могут содержаться и ошибки, и упущения. Андреас М. Антонопулос, Merkle Bloom LLC, редакторы, корректоры, наборщики текста и дизайнеры не несут никакой ответственности за допущенные ошибки или пропуски. В сферах Биткойна и Блокчейна всё очень быстро меняется; пользуйтесь данной книгой как справочником, но не единственным источником!
Ссылки на работы, защищенные авторским правом, даются исключительно в целях критической оценки либо комментирования. Все права на товарные знаки принадлежат их законным владельцам. Упоминания людей, компаний, продуктов, сервисов и услуг даются только как примеры и не должны рассматриваться в качестве рекламы.

Предисловие

Когда я только начинал свой путь в мире Биткойна[4], я даже не предполагал, во что это выльется. Книга, которую вы держите в руках, – что-то вроде сокращенного дневника о моем исследовании Биткойна; он представлен в виде лекций, которые я прочитал в период с 2013 года по начало 2016-го.

За эти три прошедших года я выступал более 150 раз перед людьми по всему миру, записал более 200 роликов для подкастов, ответил на несколько сотен вопросов, дал более 150 интервью для радио, газет и телевидения, снялся в восьми документальных фильмах и написал книгу «Осваиваем Биткойн» – технический справочник о
принципах работы Биткойна
. Практически все эти работы доступны в интернете бесплатно (на условиях лицензий на ПО с открытым исходным кодом). Лекции, вошедшие в эту книгу, – лишь небольшая часть моей работы; они были отобраны командой редакторов, чтобы дать читателю представление о Биткойне, о том, как его использовать и какое влияние он окажет на будущее.

Каждая из этих лекций была прочитана на публике, без заранее написанного текста, без демонстрации каких-либо слайдов и другого визуального подспорья. Перед началом лекции у меня имелась только ее тема, а вдохновение я получал при общении с аудиторией. От лекции к лекции темы развиваются, я пробую новые подходы, наблюдаю за реакцией зала и делаю выводы. Поэтому некоторые идеи, которые сначала умещались в одном предложении, спустя несколько лекций могли развиться в отдельную тему.
Такой процесс «нащупывания», конечно, не идеален. Мои лекции содержат немало мелких фактических ошибок. Я говорю о датах, событиях, числах и технических деталях по памяти, и иногда она меня подводит. В тексте книги мои спонтанные ошибки, оговорки и слова-паразиты были вычищены

редакторами. Осталась только суть каждой лекции – лишь то, что я хотел сказать; это не дословная расшифровка всего сказанного. Но и такое сокращение имеет свою цену: чтение не позволяет ощутить реакцию и энергию публики, вы не услышите мою оригинальную интонацию и спонтанные смешки – как мои, так и людей в зале. Чтобы всё это почувствовать, посмотрите видео, ссылки на которые приведены в Приложении А.

И книга, и мои выступления за последние три года – нечто большее, чем просто исследование Биткойна. Эти лекции отражают мое восприятие мира, политические убеждения и надежды, мои технические увлечения и то, какой я программист. Они раскрывают мой энтузиазм по отношению к этой технологии и к удивительному будущему, которое я себе представляю. И это видение начинается с Биткойна – необычного эксперимента любителей криптографии, который привел к цепной реакции инноваций, созданию «Интернета денег» и радикальной трансформации человеческого общества.

От редакторов

Практически всё биткойн-сообщество знает, как много сделал Андреас для популяризации Биткойна. Помимо его работы в СМИ, он – востребованный лектор, прославившийся своими инновационными, захватывающими лекциями, которые дают пищу для размышлений. В настоящей книге собрана лишь небольшая часть работ Андреаса в области Биткойна и Блокчейна за последние три года. При таком богатстве выбрать материал для книги – задача не из легких. Мы отобрали именно эти лекции, поскольку они соответствуют цели данного сборника. Это издание лишь первый том; надеемся, что следующий не заставит себя ждать.

Наш издательский проект мы начали с того, что сформулировали идею. Нам хотелось создать несложный для восприятия сборник рассказов, в котором были бы рассмотрены вопросы: почему так важен Биткойн, почему он интересует стольких людей? Мы стремились сделать такую книгу, которую захотелось бы дать почитать родным, друзьям и коллегам; чтобы можно было быстро ознакомиться с основными понятиями и углубиться в проблему на пару часов. Книга должна быть увлекательной (с аналогиями из повседневной жизни для понимания технической части) и одновременно вдохновляющей, демонстрирующей, как все эти вещи могут позитивно повлиять на человечество. К тому же книга должна быть честной, с признанием всех недостатков современных систем и самой технологии.

Несмотря на наши старания, мы уверены в том, что многое можно и улучшить, и изменить, – это ведь первое издание лекций. Отдельные расшифровки лекций подверглись серьезной редактуре, чтобы информация лучше воспринималась при чтении, но при этом мы старались сохранить эффект звучащей лекции. Как нам кажется, мы добились равновесия и в целом книга удалась; надеемся, вы с этим согласитесь. Если у вас появятся замечания по содержанию или идеи, как улучшить эту книгу, пишите нам по адресу: errata@merklebloom.com.

Несколько советов по чтению

По замыслу автора, каждая лекция носит самостоятельный характер. Читать книгу с самого начала не обязательно, но, если вы незнакомы с Биткойном, лучше всё же сразу обратиться к первой лекции «Что такое Биткойн?», где содержится общий обзор этой темы. Вы заметите в книге сквозные темы и аналогии: например, несколько раз упоминается британский «Закон о красном флаге» (Red flag act), несколько раз приводится беседа о деньгах между отцом и сыном. Но несмотря на то, что примеры изредка повторяются, они призваны иллюстрировать совершенно разные идеи.

В конце сборника вы найдете тщательно подготовленный указатель. Честно говоря, мы им очень гордимся! Мы вложили в него много труда, и он позволит вам увидеть логические связи и уяснить для себя основные нюансы и темы лекций.

Что такое Биткойн?

«Взрывай, создавай новое, расширяй масштаб»; Афины, Греция; ноябрь 2013 года

Примечание издателя для читателей: лекция прочитана в конце 2013 года. Транзакции в системе Биткойн теперь уже не бесплатные, хотя тарифы минимальны. На сегодня тариф примерно 10 центов за одну транзакцию, от суммы транзакции он не зависит.

Добрый день, Афины! Спасибо, что пригласили меня выступить с лекцией. Вы хотите всё до основания разрушить? (Одобрительные возгласы из зала) Хорошо, сейчас разрушим! У меня для вас припасена самая настоящая революция. Сегодня я расскажу вам о суперволнующем, суперинтересном и, возможно, суперважном технологическом изобретении в информатике за последние 20 лет. Я расскажу вам о Биткойне.

Биткойн – это гораздо больше, чем цифровые деньги. Сказать, что Биткойн – цифровые деньги, всё равно что за явить, будто интернет – это такой новый модный телефон. Или утверждать, что функции интернета сводятся к обмену электронными письмами. Деньги – это просто первое реализованное приложение. Биткойн же на самом деле – это и технология, и валюта, и международная сеть для платежей и обмена, причем совершенно децентрализованная. Она не опирается ни на банки, ни на правительство.

«Сказать, что Биткойн – цифровые деньги, всё равно что заявить, будто интернет – это такой новый модный телефон».

В истории человечества ничего подобного не было. Биткойн – изобретение по-настоящему революционное. Оглядываясь назад, мы увидим, как момент его создания стал историческим и положил начало социальной политической революции. Итак, давайте приступим к делу.

Изобретение Биткойна

Биткойн – это цифровые деньги. Такие же деньги, как евро и доллары, только никакое правительство не причастно к их выпуску. Их можно мгновенно и совершенно безопасно отправить из одной точки мира в любую другую, и стоить это будет совсем мало или вообще ничего. Два дня назад в сети Биткойн произошла самая крупная транзакция: кто-то перевел 150 миллионов долларов между двумя счетами в биткойнах, за секунду, по нулевому тарифу. Этот пример поможет вам понять, насколько прорывной станет данная технология в аспекте международных платежных систем. И это только начало.

Биткойн – это цифровая валюта, которая начала входить в оборот с 2008 года после ее изобретения неким господином Сатоши Накамото (Satoshi Nakamoto). Он опубликовал статью, где сообщил, что ему удалось создать децентрализованную сеть, в которой возможно достижение согласия без участия какого-либо органа власти или третьей стороны. И если вы изучали информатику или проходили курс по распределенным системам, то вы знаете, что эта проблема называется «задача византийских генералов» (или «задача двух армий»). Впервые эта задача была описана в 1982 году, и вплоть до 2008 года задача оставалась нерешенной. И вот Сатоши Накамото заявил: «Я ее решил!» – угадайте, что за этим последовало? Его подняли на смех, его игнорировали, от него стали отмахиваться. Сначала он выступил с этим заявлением, а через три месяца выпустил программное обеспечение, которое позволило людям начать построение сети Биткойн.

Биткойн – это не компания и не организация. Это стандарт, или протокол, – такой же, как TCP/IP или интернет. Им никто не владеет. Он работает на основании простых правил математики, с которыми согласны все, кто использует эту сеть. Благодаря изобретению Сатоши Накамото, Биткойн позволяет полностью децентрализованной сети компьютеров прийти к согласию по вопросу, какие именно

транзакции произошли в сети, и еще по одному существенному вопросу: кто в данный момент обладает деньгами?
Так что, посылая в этой одноранговой и полностью децентрализованной сети деньги со своего аккаунта на чей-нибудь еще аккаунт, я совершаю операцию, подобную отправке электронного письма. Между владельцами двух аккаунтов никого нет. Каждые десять минут вся сеть приходит к согласию по поводу того, какие произошли транзакции, без участия какой-либо централизованной власти, путем простого выбора, совершаемого в электронном виде.
Это изобретение гораздо больше чем просто валюта. Валюта – лишь первое приложение, первое применение, которое может быть создано на основе системы с распределенным консенсусом. Среди других возможностей использования можно назвать распределенное честное голосование, ведение реестра акций, регистрацию прав, нотариальное заверение и еще много того, о чем мы раньше даже не думали.
Я узнал о Биткойне в 2011 году, и впервые за много лет, прошедших с того дня, как открыл для себя интернет, я был ошеломлен новыми возможностями. С интернетом я познакомился в 1991 году, еще до того, как он превратился в коммерческую площадку. Мне было ясно, что он изменит мир, но мне никто тогда не верил. И точно такое же ощущение у меня сейчас по отношению к Биткойну.
Наверняка некоторые из вас слышали про биткойн: такая, дескать, валюта, которая сегодня котируется очень высоко, а завтра не будет стоить практически ничего. Я здесь, чтобы сказать вам: не обращайте внимания на котировки, забудьте, что это деньги! Вам нужно понять суть Биткойна, какую сеть можно создать на его основе. Если мы будем считать Биткойн только деньгами, мы просто запустим еще одну валюту. Изобретение Биткойна, технологии, которая сделала это возможным, уже нельзя отменить. Она позволяет создать децентрализованную организацию в невиданных масштабах для нашей планеты.

«Изобретение Биткойна, технологии, которая сделала это возможным, уже нельзя отменить. Она позволяет создать децентрализованную организацию в невиданных масштабах для нашей планеты».

Народные деньги

Я расскажу, почему изобретение Биткойна представляется мне столь важным. Сегодня приблизительно один миллиард человек имеют доступ к банковской системе, кредитам и другим услугам международной финансовой системы; в основном это люди с западной культурой. Шесть с половиной миллиардов людей на нашей планете никак не связаны с мировыми деньгами. Они живут при общественно-экономическом строе, в основе которого наличные расчеты; возможности выхода на международные ресурсы у них ограниченны. Банки им не нужны. Однако два миллиарда из этих шести с половиной уже имеют доступ к интернету. Установив приложение, они получат возможность в один миг стать участниками мировой экономики и пользоваться международной валютой, которую можно передавать куда угодно без сборов и без какого-либо контроля со стороны правительств. Они могут подключиться к миру международных финансов (или расчетов) напрямую, без посредников. Биткойн – это народные деньги; он основан на простых математических правилах, с которыми соглашаются участники сети и которые никто не контролирует. Подключение этих шести с половиной миллиардов людей к миру финансов имеет революционный потенциал.
Пострадают платежные системы и провайдеры. Эти огромные компании осуществляют платежи и взимают повышенную комиссию за то, что переводят деньги в более бедные страны. Такое состояние дел попахивает эксплуатацией и коррупцией. Компании получают огромные доходы за операции, которые могут быть совершены в биткойнах практически безвозмездно. Однажды кто-то пошутил в интернете, написав: «Я только что заменил всю вашу отрасль сотней строчек кода на Python», – это именно то, что мы сейчас и делаем с помощью Биткойна.

Валюты, бизнес и международные платежи

Как сегодня можно использовать Биткойн? Если объяснять просто, то Биткойн работает как валюта. Представьте, что вы покупаете иностранную валюту: заходите на биржу в интернете, зачисляете на счет несколько евро и используете их для покупки биткойнов по текущему обменному курсу. Но это всё еще не лучший способ его использования. Мы ведь предприниматели, верно? И мы хотим всё изменить. Так что лучший способ – найти продукт или услугу, которые вы можете предложить в обмен на биткойны, и того, кто готов заплатить за них биткойнами, – и начать зарабатывать.

Решение проблем с платежами

Если вы подумываете основать международный бизнес, то на пути к глобальному рынку вам предстоит преодолеть два барьера. Первый – сложности с перемещением продуктов и услуг через границы. С появлением интернета эта проблема решена. Теперь можно создавать виртуальные продукты и услуги – и продавать их где угодно. Продукт у нас есть, но остается еще одна большая проблема: как получить оплату? И эту проблему решает Биткойн. Он дает возможность мгновенно получать платежи из любой точки мира. Сеть Биткойн позволяет отправить даже малую сумму – как одну стомиллионную биткойна[5], а это на сегодня – совсем крошечные деньги[6]. С традиционными деньгами и платежными системами вам такого не сделать. Банковские карты были введены в оборот в 1950-х годах, и они совершенно точно не были предназначены для эпохи интернета. Для нее был создан Биткойн.

«Банковские карты были созданы в 1950-х годах, и они совершенно точно не были предназначены для эпохи интернета. Для нее был создан Биткойн».

Итак, если платежи в размере сотой или даже тысячной доли евро реальны, то уже появляется возможность продавать контент. Вы можете осуществлять микротранзакции, собирать микроплатежи от миллионов людей, и в совокупности они будут уже что-то стоить. Та же сеть, в которой можно переслать тысячную долю евро или целый миллион евро, способна переслать и миллиард, и триллион евро! Комиссия за осуществление транзакции будет одинаковой[7], поскольку тариф зависит от размера транзакции в килобайтах, а не от суммы, являющейся контентом транзакции.

Нейтралитет, преступники и Биткойн

Вспомним историю интернета и подумаем, какие уроки можно извлечь из нее для понимания Биткойна. Один из самых важных принципов интернета – это нейтральность. Ему всё равно, крупная вы организация или мелкая. Для интернета нет разницы между CNN[8] и египетским блогером. У египетского блогера и CNN равные возможности быть услышанными в мире.
Биткойн тоже нейтрален по отношению к отправителю, получателю и стоимости транзакции. Это означает, что любой гражданин, любой пользователь Биткойна получает возможность реализовать свой инновационный потенциал в сфере финансовых инструментов, платежных систем и банковских услуг. Вы можете вести деятельность на том же уровне, на каком ее ведет Citibank. И это воистину революция!

«Биткойн нейтрален по отношению к отправителю, получателю и стоимости транзакции. Это означает, что любой гражданин, любой пользователь Биткойна получает возможность реализовать свой инновационный потенциал в сфере финансовых инструментов, платежных систем и банковских услуг».

Биткойн переворачивает с ног на голову иерархически выстроенную систему международных финансов. До сих пор безопасность данной системы была построена на ограничении доступа, поскольку именно такой метод обеспечения доверия в основном используется в наших платежных системах. Вы как пользователь не сможете войти в систему без проверки. Благодаря Биткойну можно создать полностью горизонтальную и децентрализованную сеть, где все узлы равны, протокол нейтрален по отношению к транзакциям. Такие возможности благоприятствуют инновациям в Биткойне, порождая такой же феномен, как мы видим в интернете, где внедрение инноваций не требует какого-либо разрешения. Не

надо спрашивать никого, можно ли разместить ваше приложение в интернете, можно ли произвести революцию в целой индустрии с помощью вашей информационной технологии, запустить в биткойн-сети новый финансовый инструмент, новую платежную систему или сервис. Вы имеете право просто взять и всё это сделать. Вы можете просто написать код и стать частью международной финансовой сети, которая будет исполнять этот код и позволит вам вступить в контакт с миллионами потребителей.
Сегодня мы наблюдаем зарождение технологии. Еще нет доведенных до совершенства интерфейсов, да и система сложна в использовании. Некоторым она помогает достичь преступных целей. Ее применяют разные организации по всему миру, и точно узнать, кто именно пользуется Биткойном, непросто. Всё это я уже слышал. Когда в 1991 году я впервые вышел в интернет, он был просто каким-то прибежищем разбойников, любителей порнографии, пиратов и преступников. Но как тогда это не имело никакого значения, так и сейчас. Это не столь важно потому, что та же мощная технология, которую могут использовать для своих темных дел преступники, служит во благо всем остальным людям, чтобы творить добро, чтобы совершать невероятное, – везде, во всем мире! А нас гораздо больше, чем их!
Биткойн создает среду, которая полностью готова к инновациям, поскольку это не только валюта – это технология, сеть и валюта. Признаюсь, я рад, что курс биткойна растет, поскольку у меня есть биткойны, – ощущение от этого довольно приятное. Но здесь важен не только биржевой курс. Если даже завтра курс биткойна обвалится, революционная технология всё равно никуда не денется. Точно так же, как если вдруг обрушится какой-нибудь веб-портал или приложение, интернет от этого не исчезнет.

«Биткойн создает среду, которая полностью готова к инновациям, поскольку это не только валюта – это технология, сеть и валюта».

Биткойн как механизм согласия и отказа

Поняв, что Биткойн – это технология, а не только деньги, вы тут же осознаете его поистине огромное значение. Повторюсь: это не совсем про нас с вами, это касается шести с половиной миллиардов людей. Всё дело в возможности такого уровня мировой финансовой интеграции, которого еще никогда не было на свете. С нашей точки зрения, с точки зрения привилегированной части населения планеты, это великая технология. Мы сможем осуществить взрывные инновации. Мы создадим интересные и привлекательные сервисы. Но с точки зрения кенийского фермера, которому нужны деньги на покупку семян и который теперь имеет возможность взять заем у любого участника децентрализованной пиринговой сети, причем кредитор может быть из любого уголка света, эта новая технология способна изменить жизнь.
Большая часть населения мира живет в странах с репрессивными и коррумпированными режимами, центральные банки которых устраивают гиперинфляцию на уровне 30 процентов в месяц. Очень важно понять, как именно Биткойн может поменять жизнь этих людей. Из них два миллиарда имеют доступ к интернету, и лишь у одного миллиарда из них есть банковский счет. Это можно изменить. Будет непросто, не надо обольщаться. Когда вы вводите прорывную технологию прямо в центр сильнейших в мире организаций, им это вряд ли понравится. В настоящий момент мы всё еще в самом начале пути. Повторю избитую фразу: «Сначала они будут нас игнорировать, затем будут над нами смеяться, затем начнут с нами бороться – а потом мы победим!» Пока что мы на стадии их насмешек. Так и должно быть, поскольку к тому времени, когда они начнут с нами бороться, они уже проиграют этот бой. Биткойн уже приобрел глобальный масштаб – китайские инвесторы вложили в него 2,5 миллиарда долларов, увидев в нем противовес глобальному доминированию мировой резервной валюты – американского доллара.

Альткойны: криптовалюты для всех

В мире существует около 200 валют, но международной является лишь одна. Существует около 200 валют, контролируемых центральными банками и правительствами, но математическая валюта лишь одна, и это – биткойн.

Мы создадим их гораздо больше. Криптовалюты станут частью будущего нашей планеты, потому что их уже изобрели. Ничего сложного, всё просто. Невозможно не изобрести эту технологию, как невозможно повернуть время вспять. В сети существует более сотни криптовалют[9], что говорит о быстроте распространения инноваций, и даже за пределами Биткойна. Существует много других альтернативных криптовалют – альткойнов, которые используют ту же базовую технологию децентрализованного реестра на основе базы консенсуса «алгоритма Сатоши». Некоторые из этих валют подвержены инфляции, некоторые – дефляции, в некоторых применяется демерредж[10] или отрицательные процентные ставки. Некоторые являются благотворительными и перераспределяющими часть доходов в благотворительные организации.
Мы можем придумывать деньги бесконечно, создавать новые формы денег и финансовые инструменты.

Программируемые деньги для каждого из нас

По большому счету, Биткойн – это программируемые деньги. Когда появляются программируемые деньги, возможности становятся действительно безграничными. Можно взять многие базовые принципы современной системы, построенной на регулируемых законом обязательствах, и конвертировать их в подчиняющиеся алгоритмам обязательства, в транзакции, которые можно применять в сети Биткойн. Как я уже говорил, нет никаких третьих сторон, нет никаких контрагентов. Если мне хочется отправить некую сумму из одной части сети в другую, это будет произведено без каких-либо посредников. Если я изобрел новую валюту, я смогу распространить ее на весь мир и пригласить других людей присоединиться ко мне и пользоваться ею.

«Биткойн – это интернет денег. Криптовалюта – лишь одна из сфер его применения. В своей основе Биткойн имеет революционную технологию, которая навсегда изменит наш мир».

Биткойн – это мгновенные безопасные транзакции с минимальной комиссией. Но Биткойн больше, чем только деньги, – это интернет денег. Криптовалюта – лишь первое его применение. Если вы ухватили суть и видите не одни лишь котировки и волатильность, то понимаете, что это не просто дань моде. В своей основе Биткойн имеет революционную технологию, которая навсегда изменит наш мир.
Присоединяйтесь. Давайте вместе делать эту революцию.
Спасибо за внимание!

Одноранговая денежная система

[11]

«Изобретаем заново деньги»; лекция прочитана в Университете им. Эразма Роттердамского, Голландия; сентябрь 2015 года

Меня обычно просят рассказать о том, что нового происходит в мире Биткойна, но сегодня я хочу порассуждать о древней истории. Я хочу поведать вам о деньгах в историческом контексте и поговорить, почему в этом контексте важен Биткойн.

Как давно появились деньги?

Сначала позвольте задать вам один вопрос: если рассматривать деньги в качестве технологии – пусть это будет изобретенная человеческой цивилизацией технологическая система, – ответьте, давно ли эта технология появилась? Кто что думает?
(Из зала звучат разные ответы.)
Да, есть много разных вариантов ответа. Мне всегда странно, когда люди отвечают что-то вроде: 400 лет, 1000 лет, 2000 лет. Ведь на самом деле это неизвестно. Мы не знаем, давно ли появились деньги, поскольку пока еще не обнаружена культура столь древняя, чтобы денег в ней не было. Известно одно – деньги появились вместе с человеческой цивилизацией.

«Деньги появились вместе с человеческой цивилизацией».

Люди часто удивляются, когда узнают, что деньги появились раньше письменности. В археологических находках с образцами письменности есть иероглифы, есть клинопись. А когда найденные архаичные формы письменности были расшифрованы, попробуйте угадать – о чем тогда писали? О деньгах! Это древние рукописные реестры[12]. Поэтому деньги древнее письменности.
Изобрели ли деньги раньше колеса? Я не знаю; зато известно, что колёса использовались в качестве меновой стоимости. В ходе археологических раскопок стоянок каменного века тоже были обнаружены деньги – в форме ракушек, перьев и бусин.
Доказано, что обезьяны способны пользоваться деньгами. Во время исследований ученые демонстрировали шимпанзе камни определенного вида, которые можно обменять на бананы. Затем исследователи наблюдали, что станут делать обезьяны с новой информацией. А обезьяны довольно быстро додумались до… вооруженного ограбления! Они смекнули, что если побить другую обезьяну и отобрать у нее камни, то за них можно будет получить бананы. Вторым же их изобретением стала… проституция. Шимпанзе догадались, что за сексуальные ласки тоже можно получить камешки и обменять их на бананы. Не объясняет ли нам это природу денег?
Мне кажется важным, что при взгляде на природу денег выясняется: деньги – это форма взаимодействия. На своем самом базовом уровне деньги не несут ценности. Деньги представляют собой абстракцию ценности, способ сообщить о ней. Это определенный язык. Вот почему деньги такие же древние, как сам язык. Во многих аспектах деньги обладают характеристиками, превращающими их в лингвистическую концепцию. Это также форма взаимодействия.

«Мы используем деньги для того, чтобы сообщать друг другу о ценностях, показать, насколько высоко оцениваем продукт, услугу, поступок».

Мы используем деньги для того, чтобы сообщать друг другу о ценностях, показать, насколько высоко оцениваем продукт, услугу, поступок. Мы пользуемся ими как фундаментом социального взаимодействия, поскольку сообщение друг другу о ценности создает социальные связи. Так что деньги еще и очень важный социальный компонент. Это древняя технология[13]. Правда, по иронии судьбы – одна из наименее изученных с исторической и технологической точек зрения. Взгляните на Биткойн – это изобретение новой формы денег. Давайте об этом и поговорим.

Технологическая эволюция денег

Как часто в результате изобретений трансформировались технологии денег? Сколько существует различных форм денег? На базовом уровне способ передачи ценности – это обмен вещами, которые, по нашему мнению, обладают одинаковой ценностью. «Вот, например, у меня есть коза. Ты мне отдаешь 20 бананов, а я тебе – мою козу». Здесь деньги не участвуют (поскольку наша сделка – бартер или обмен), зато мы видим одну из первых форм коммуникации по вопросу ценности.

Средство обмена на драгоценные металлы

Затем появились абстрактные формы денег. Первой значительной технологической эволюцией стало начало обмена вещей на нечто такое, что нельзя было съесть: на перышко, бусину, шнурок с завязанными на нем узелками, на какую-нибудь цветную штуку, которую можно было использовать в эстетических целях. Первый значительный момент трансформации технологии произошел, когда в качестве денег перестали выступать исключительно предметы, сами по себе ценные или пригодные для потребления, – деньгами же сделались предметы, символизирующие ценность, то есть абстрактные символы.

«Первый значительный момент трансформации технологии денег произошел, когда в качестве денег перестали выступать исключительно предметы, сами по себе ценные или пригодные для потребления, – деньгами же сделались предметы, символизирующие ценность, то есть абстрактные символы. Одной из самых популярных форм таких символов стало использование драгоценных металлов для выражения ценности».

Одной из самых популярных форм таких символов стало использование драгоценных металлов для выражения ценности. В металлах скомбинированы некоторые из важнейших характеристик денег: их сложно найти (они редкие); их легко перемещать (по крайней мере, по сравнению с гигантскими камнями либо целым бочонком перьев); их легко поделить (можно расколоть золотую монету на части); их эстетическая ценность универсальна. Вот что такое вторая значительная трансформация технологии денег. Внедрение драгоценных металлов заняло сотни тысяч лет. В истории мы начинаем сталкиваться с драгоценными металлами в самом раннем периоде «плодородного полумесяца»[14], когда было положено начало развитию тех сельскохозяйственных традиций, на основе которых сложились цивилизации Ближнего и Среднего Востока. Использовать в обращении драгоценные металлы продолжили вавилоняне, египтяне и греки.

Замена драгоценных металлов бумагой

Так произошли две значительные технологические революции, и в течение нескольких тысяч лет ничего не менялось. А затем кому-то пришла в голову блестящая идея: передать золото на хранение кому-нибудь заслуживающему доверия, кто взамен даст документ о том, что золото лежит в его надежном хранилище. И вместо золота можно обмениваться этими документами, которые удобнее носить с собой. Пока я могу доверять свои деньги владельцу хранилища, у меня есть новая форма денег.
Любая технологическая эволюция в области денег вызывает всеобщий скептицизм. Но мне кажется, что самый глубокий скепсис человеческая цивилизация испытала именно на этом этапе. У многих введение бумажных денег в оборот вызывало противоречивые чувства. Вы думаете, что люди паникуют по поводу биткойнов? Но задумайтесь, какая должна была подняться паника, когда людям сказали, что вместо обмена на золото будет обмен на листочки бумаги! Для многих это было немыслимо. Ведь, в конце концов, бумага явно не обладает какой-либо реальной ценностью. Примерно 400 лет понадобилось, чтобы бумажные деньги получили широкое распространение. Это было очень серьезное изменение.

«Вы думаете, люди паникуют по поводу биткойнов? Но задумайтесь, какая должна была подняться паника, когда людям сказали, что вместо обмена на золото будет обмен на листочки бумаги!»

Бумагу сменяет пластик

Затем (примерно 60 лет назад) появилась новая форма денег – пластиковые банковские карты. Фактически первые пластиковые карты были той же самой бумагой. В США первой компанией, создавшей кредитную карту, стала компания Diners Club[15], и это было что-то вроде «дорожного чека». В те времена люди брали банковскую карту в руки и говорили: «Какие же это деньги? Дайте мне лучше старые добрые бумажные купюры, к которым я привык». И это была еще одна великая трансформация денег.

Биткойн заменит пластик

Теперь появился Биткойн. В моем понимании Биткойн – довольно радикальная трансформация денег. Такая же, как переход от драгоценных металлов к бумажным деньгам, а возможно, даже более радикальная. Так что же такое Биткойн? Основная фундаментальная проблема в описании Биткойна в том, что если использовать отсылки к предшествующему опыту, то этот опыт основан на тысячелетнем понимании того, что такое деньги в их материальной форме. Сейчас нам нужно описать новую форму денег, являющуюся абстракцией. «Это токен, обозначающий принятие и отправление транзакций в сети, – сетецентрическая форма денег». Но это ведь даже не начало того, что я хочу рассказать о Биткойне.
При описании Биткойна чаще всего вызывает непонимание то, что это не просто новая платежная система и не новая форма денег. Биткойн – цифровые деньги. Но какой в этом смысл – цифровые деньги и так уже есть. Все вы ежедневно пользуетесь цифровыми деньгами – и пользовались еще задолго до того, как появилась сеть Биткойн. У всех есть банковские счета. Банки ведут электронные реестры с данными этих счетов. Вы пользуетесь ими, чтобы отправлять электронные платежи. Вот это и есть цифровые деньги. Биткойн же представляет собой фундаментальную трансформацию денег.
Биткойн – это не только цифровые деньги. Биткойн – фундаментальная трансформация технологии денег. Это сложно понять, поскольку такое утверждение сильно отличается от всего, что мы знаем. И я попробую использовать другой подход. Давайте на минуточку взглянем на архитектуру построения вычислительных сетей.

В сторону сетецентрической эпохи, основанной на протоколах

Биткойн существует не сам по себе, он встроен в контекст текущей финансовой реальности. Биткойн был создан в исторический момент, когда происходят преобразования социальных институтов, которые положили начало великой сетецентрической эпохе.
Социальные институты на протяжении столетий были организованы в иерархические структуры: существовали организации, демократия, банковская система, образование. Все наши социальные взаимодействия строились путем обращения к вышестоящим уровням этой иерархии, то есть полномочия власти сосредоточены у прослойки бюрократически настроенных чиновников. Но изобретение интернета что-то изменило. Мы видим, что всё большее количество социальных институтов стали превращаться из закрытых, непрозрачных иерархических комплексов с собственными правилами в платформы. Мы стали видеть появление систем с интерфейсами, открытыми API[16], к которым мы можем получить доступ и обмениваться информацией. Таким образом, от институтов мы перешли к платформам.
Сейчас мы видим более важную трансформацию: переход от платформ к протоколам. Самое интересное в переходе от платформы к протоколу кроется в том, что у протокола отсутствует единый центр. Протокол TCP/IP[17] не ссылается на конкретного провайдера услуг связи, он работает по всему миру без учета внутреннего контекста. Не нужно проводить регистрацию и авторизацию (например, в личном кабинете на платформе), чтобы использовать протокол TCP/IP; нужно просто применить язык, который используется в данном протоколе. И как только вы переходите от платформы к языку, вам открываются колоссальные возможности.
Биткойн – это первая сетецентрическая форма денег, работающая на базе протокола. Это означает, что она существует безотносительно какого-либо институционального либо платформенного контекста. Чуть позже я еще к этому вернусь – это крайне важный момент.

Одноранговая архитектура

Биткойн, по моему мнению, одноранговые деньги. Что же это значит? Здесь используется термин «архитектура» в аспекте компьютерных наук, построения сетей или распределенных систем, который

описывает взаимодействия между участниками и системой. Архитектура биткойн-сети является одноранговой, поскольку каждый участник в сети использует биткойн-протокол на равных с остальными. Специальных нод (узлов) не существует; все ноды Биткойна «одинаковы».
«Одноранговый» означает, что когда вы отправляете транзакцию в сеть, то при обработке она равнозначна, то есть все транзакции в сети обрабатывают ее совершенно одинаково. В подобной системе отсутствует внутренний контекст как таковой, за исключением того, что будет получено из сети. Интересной проблемой распределенных систем является именно эта проблема: контекст и состояние. Если вы заходите в свой аккаунт на Facebook, вы не используете протокол. Все действия, всё, что касается состояния, контролирует Facebook: все данные находятся у него, а для вас просто открывается сессия доступа к сервису социальной сети. Такая архитектура называется «клиент-серверной».
Биткойн построен иначе, поскольку это одноранговая сеть: точно так же построены электронная почта или протоколы TCP/IP.

Клиент-серверная архитектура

Мы неохотно разговариваем о деньгах. Удивительный факт: практически во всех странах мира обучение финансовой грамотности не входит в программу школьного образования. Самые интересные вопросы о деньгах обычно задают пятилетние дети. Большинство родителей на эти вопросы ответить не могут. «Мама, а что такое деньги? Как работают деньги? Почему у нас мало денег? Как сделать так, чтобы их было много? Почему не все могут иметь большие деньги?» Но вы ведь не говорите: «Мария, ну-ка быстро иди к себе в комнату, будь паинькой, садись читать об инфляции и не вздумай показываться на глаза, пока не узнаешь ответы на все эти вопросы!»
О деньгах мы не разговариваем. Весьма любопытно: практически в любом аспекте социального взаимодействия мы используем деньги как основу, но тем не менее эта тема считается табуированной. Все притворяются, будто им нет никакого дела до денег и этот вопрос не принципиальный. У нас ведь есть высшие цели и стремления. Деньги мы используем ежедневно, но никогда о них всерьез не беседуем. Такие разговоры считаются «неудобными».
Мне кажется, что в этом отчасти виновата история. Предшествовавшая Биткойну форма денег – когда их выпускали взамен хранящихся в сейфах драгоценных металлов – являлась олицетворением долгового обязательства. Это действительно важная мысль, которую нужно понять, поскольку она добавит красок нашей дискуссии.
У многих ли из вас хранятся деньги в банках? Ни у кого из вас нет денег в банке! Вы храните физически банкноты в сейфовой ячейке банка? Ну, если храните, тогда, пожалуй, можно сказать, что деньги в банке у вас есть. А все остальные просто отдали свои деньги банку взаймы. И за привилегию принять ваши деньги банк начислит вам просто потрясающее вознаграждение в размере 0,00001 процента от полученной суммы за каждый год. Ваш банк берет у вас деньги, тут же выдает их в качестве займа тому, кто сейчас стоит рядом с вами, – в среднем под 24,99 процента в год!
Вот что такое «клиент-серверные» отношения. Поскольку эти деньги существуют лишь в форме долгового обязательства в реестре счетов, находящемся вне вашего контроля. Данные этого реестра хранятся на сервере, а вы – простой клиент. В реальности вы не имеете никакого контроля над ними. У вас нет даже базовых интерфейсов доступа к этим деньгам – ну разве только сам сервер предоставит вам такой опосредованный интерфейс… Вот так работает клиент-серверная архитектура.

Master-Slave архитектура

В распределенных системах существует и другой термин, описывающий частный случай клиент-серверной архитектуры, когда второстепенная сторона владеет лишь редуцированной копией данных, не обладающей важным значением. Такая архитектура называется master-slave (или «ведущий-ведомый»). Если на предыдущем шаге денежная система покажется вам выстроенной по принципу «ведущий-ведомый», то у вас наверняка возникнет малоприятный вопрос: кто же в этом случае выступает

«ведомым»? Ведь в системе, основанной на долговых обязательствах, одна из сторон обязательно должна быть «ведомой».

«В системе, основанной на долговых обязательствах, одна из сторон обязательно должна быть „ведомой“».

Вы клиент, а не сервер. Сервер на самом деле вас не обслуживает, поскольку он обслуживает сам себя – он «ведущий»! Так выглядит архитектура денежной системы, с которой мы живем в настоящий момент. Именно такая архитектура денежного взаимодействия используется нашей цивилизацией: в данной архитектуре вы ничего не контролируете; в ней любое взаимодействие производится при посредничестве третьей стороны, обладающей полным контролем над денежными средствами.
Если вы сегодня подойдете к банкомату и вставите карточку, банкомат будет решать, выдать ли ваши деньги. Однажды – как в этом убедились за последние несколько десятилетий и даже столетий жители Кипра, Греции, Венесуэлы, Аргентины, Боливии, Бразилии и далее по списку – вы приходите в банк, а банк не хочет отдавать вам ваши деньги, потому что он, оказывается, вправе так поступить. Вот это и есть суть отношений «ведущий-ведомый».

«Фундаментальное отличие Биткойна заключается в том, что вы никому ничего не должны и вам никто ничего не должен. Взаимоотношения в данной сети не основаны на долговых обязательствах».

Фундаментальное отличие Биткойна заключается в том, что вы никому ничего не должны и вам никто ничего не должен. Взаимоотношения в данной сети не основаны на долговых обязательствах. Они основаны на праве владения абстрактным токеном. Абсолютном праве владения. В Соединенных Штатах есть такая поговорка: «Собственность – это девять десятых закона». В Биткойне «собственность диктует законы, владелец на девять десятых прав». Если вы владеете ключами к биткойн-кошельку – это ваши биткойны. Если у вас нет ключей – это не ваши биткойны. Вы возвращаетесь к отношениям «ведущий-ведомый».

Биткойн – фундаментальная трансформация денег

Биткойн представляет собой фундаментальную трансформацию денег. Эта инновация перестраивает древнейшую из существующих технологий, радикально меняя основные принципы ее построения на новые, когда каждый из участников сети имеет равные права. Транзакция внутри сети не контролируется государством или какими-то общими положениями, за исключением необходимости подчинения алгоритму консенсуса, с которым соглашаются участники сети, – сама же сеть не подчиняется ее участникам. Здесь ваши деньги – именно ваши. Вы полностью контролируете свои деньги с помощью приложения с цифровой подписью; никто не способен это изменить, не сумеет их перехватить, не сможет их «заморозить». Никто не диктует, что вам делать (или не делать) с вашими деньгами.
Это транснациональная и трансграничная денежная система. У нас еще никогда не было подобной. Внутри нее транзакции совершаются мгновенно, и в их обработке может участвовать кто угодно, обладая простейшим устройством вроде телефона с возможностью передачи текстовых сообщений.
Подобное положение дел многих пугает, ведь это фундаментальная трансформация денег. Люди будут говорить, что они встревожены. Конечно, они опасаются, что биткойны могут использовать преступники. Но правда такова: гораздо больше их беспокоит то, что пользоваться биткойнами будут все остальные люди.
Спасибо за внимание!

Конфиденциальность, идентификация, надзор и деньги

Семинар по Биткойну в FabLab; Барселона, Испания; март 2016 года

В этой лекции я собираюсь вам рассказать о концепциях нейтралитета, децентрализации, конфиденциальности и о том, что делает Биткойн таким особенным. Когда я произношу «Биткойн», я имею в виду не только криптовалюту – для меня это более широкое понятие. Это концепция полностью децентрализованной сети с горизонтальными связями, обеспечивающими работу доверенных приложений. Если вам посчастливилось построить полностью децентрализованную сеть, логика подсказывает, что первым приложением станет ее применение как валюты. Но «платежи» – всего лишь первое применение.

Банковская система: от свободы к ограничению

Общество изменяется, когда мы переустраиваем его институты. Традиционно наши институты выстраивались по принципу иерархии. Таким путем шли со времен индустриализации XVIII века: люди объединялись и взаимодействовали в крупных сообществах, чтобы разрушить феодальную систему. Такой подход сейчас не работает.
Меня иногда спрашивают, каково мое политическое кредо; объяснить это довольно сложно, но попробую выразиться в двух словах: думаю, что «я – разрушитель»! Я имею в виду следующее: каждые 30–40 лет необходимо разрушать (в хорошем смысле слова, то есть менять на что-то новое) те социально-экономические процессы, что успели за это время устояться. Поскольку устоявшиеся процессы аккумулируют в себе силу и власть, в них происходит централизация, а при наличии централизованной силы всегда появляется коррупция. Мысль эта не новая. Мои предки – а я родом из Греции – уже давно поняли, что коррупция зарождается во власти, «власть развращает, абсолютная власть развращает абсолютно»[18]. Сегодня нет власти более абсолютной, чем власть над деньгами.

«Каждые 30–40 лет необходимо разрушать те социально-экономические процессы, что успели за это время устояться. Поскольку устоявшиеся процессы аккумулируют в себе силу и власть, в них происходит централизация, а при наличии централизованной силы всегда появляется коррупция. Сегодня нет власти более абсолютной, чем власть над деньгами».

Мы живем в мире, который приобрел независимость благодаря банковской системе. Управление системой финансов перешло от монархов к обычным гражданам. Данная система стала либеральной и сделала свободными миллиарды людей. Затем она начала стремиться к централизации, обрела власть, и эта власть привела к внутреннему разложению. Та система, которая в свое время освободила людей, уже далеко не либеральная; пришло время ее разрушить. Биткойн – изобретение, которое сможет остановить централизацию власти. Я расскажу, почему это так.

Негативные результаты в силу неудачной архитектуры

Как специалиста по компьютерным наукам, работающего с распределенными системами, меня интересует их архитектура. Архитектура – отличная тема для обсуждения, потому что именно она принципиально влияет на результаты работы всей системы.
Мне доводилось работать со многими банкирами. Они прежде всего люди: им нужно обеспечивать семьи, выплачивать ипотеку, держаться за свое место. Среди них встречаются и социопаты, которые неизбежно взбираются на высшие позиции корпоративной лестницы управления, поскольку социопатия в иерархических структурах является преимуществом. Но большая часть проблем с традиционной концентрацией власти в деньгах не имеет ничего общего со злым умыслом людей. Эти проблемы появляются из-за того, что все эти институты – в силу своих особенностей, структуры и архитектуры – создают неудовлетворительные результаты, сужающие нашу свободу действия.

Рост коммуникаций при снижении доступности банковской системы

За последние 15 лет интернет стал мощным инструментом, который позволяет свободно взаимодействовать. Он направлен на устранение ограничений. Но если взглянуть на вовлечение людей в экономику и на то, как работает банковская система, становится ясно: эти возможности никак не используются. Доступность банковской системы не выросла. Наоборот, сегодня мы движемся в обратную сторону. Интеграция в экономику снижается.
Причина снижения уровня вовлеченности людей в экономику – изолированная структура финансового сектора; архитектура этой системы возводит барьеры: национальные границы, классовое разделение, различия подходов к оценке и учету денег и коммерческой деятельности. Мы живем в мире, который становится всё более глобальным и взаимосвязанным. Появилась особая глобальная интернет-культура. Наши финансовые системы остаются ограниченными, локальными и разобщенными.
Если посмотреть на финансовые системы со стороны сетевой структуры организации, то можно увидеть системы денежных переводов для небольших и крупных сумм, денежные транзакции для потребительских нужд от обычных потребителей услуг и переводы между компаниями, где работает бизнес для бизнеса. Все системы платежей разделены географически, они учитывают границы и юрисдикции различных стран и регионов. Результатом работы такой структуры организации является разобщенность. А для нас, людей, это означает, что мы всё в меньшей и меньшей степени свободны совершать сделки со всем остальным миром. Геополитика оказывает очень сильное влияние на финансы, поскольку союз государства и денежной системы в итоге создает негативную среду.

Всё это мы сейчас и хотим разрушить.

Новая архитектура, новый доступ

Архитектура Биткойна дает нам новый способ организации глобального взаимодействия – точно так же, как интернет уравнял возможности связи для всех пользователей сети, сделав их равноправными. Если у меня есть IP-адрес[19], то отправляемые мною пакеты[20] будут обработаны точно так же, как и любые другие пакеты в сети. В большинстве случаев каждый имеет право голоса. У каждого пользователя появляется сила, сравнимая с силой мировых печатных изданий. Биткойн делает то же самое, предоставляя каждому всю мощь банковской системы в глобальном масштабе.

«Архитектура Биткойна дает нам новый способ организации глобального взаимодействия – точно так же, как интернет уравнял возможности связи для всех пользователей сети, сделав их равноправными».

Представим, что у вас есть «банк на рабочем столе» компьютера. По аналогии с печатью на домашнем принтере и возможностью публикации на веб-сайтах, ваш «банк на рабочем столе» – индивидуально-контролируемая банковская система с такими же возможностями, которые есть у крупнейших банков мира, – приведет к их разрушению.
Представьте себе мир, где каждый имеет возможность не только выполнять транзакции, но и создавать сложные финансовые системы и инструменты, не спрашивая никаких разрешений, не получая банковских лицензий. Просто подключившись к сети, каждый может запустить новое приложение. В централизованной системе невозможно сделать это. В такой системе чем дальше вы находитесь, тем меньше у вас возможностей контроля. Чем ближе вы к системе, чем выше вы взобрались по иерархической лестнице, тем большему контролю и ограничениям подвержен ваш доступ. В Биткойне всё иначе. Здесь каждая нода (узел сети) обладает равными правами доступа ко всем финансовым сервисам.
Если вы хотите создать новое приложение в централизованной системе, то сначала необходимо запросить разрешение. Его вам выдадут только в том случае, если ваше приложение будет распространено на очень большую аудиторию и принесет доход.

В интернете или Биткойне для запуска приложения необходимо лишь наличие двух нод, двух пользователей и двух систем. После чего они могут начать взаимодействие, создавать свои собственные протоколы, свои собственные системы; и приложение, используемое лишь двумя пользователями, будет работать, как и любое другое приложение в сети.

Сетевой нейтралитет и отсутствие дискриминации

Люди, имея дело с интернетом, часто заблуждаются, думая, что его главное преимущество состоит в мгновенной передаче информации. Но на самом деле истинная мощь интернета – равноправие. Идея равноправия заключается в том, что здесь невозможна никакая дискриминация по источнику информации, ее назначению и содержанию.

«Биткойн – это первая финансовая сеть, демонстрирующая нейтралитет».

Биткойн – это первая финансовая сеть, демонстрирующая нейтралитет. При проведении транзакции в сети Биткойн не имеет значения ни источник, ни назначение, ни сумма, ни тип поддерживаемого финансового приложения. Единственный вопрос, который имеет значение, – заплатили ли вы достаточную сумму за использование ресурсов сети. Если заплатили, то ваше приложение «будет работать».

Отсутствие спама в биткойн-транзакциях

Сегодня в криптосообществе идут довольно интересные дискуссии относительно Биткойна. Возможно, некоторые из вас слышали термин «спам-транзакция». Знаете, что это такое? Мне кажется, данный термин недостаточно корректен, поскольку для того, чтобы решить, является ли транзакция спамом, нужно поставить себя на уровень выше и дать этому оценку. В аспекте архитектуры вы таким образом вводите правила в отношении допустимого статуса отдельно взятого приложения. Сразу возникает вопрос: допустимого для кого? Для конечного пользователя? Всё просто – никаких спам-транзакций не существует, поскольку если отправитель криптовалюты заложил в транзакцию комиссию, то это означает, что транзакция обладает достаточной ценностью для ее передачи (выполнения), – таким образом, подобные транзакции становятся допустимыми. Простой рыночный механизмом заменяет все концепции контроля и содержания, с принятием решений о том, что хорошо, а что плохо, что допустимо, а что недопустимо, какое приложение имеет ценность, а какое – нет. Если вы платите небольшую комиссию за транзакцию, это происходит в силу того, что Биткойн делает финансы по-настоящему демократичными, ваша транзакция имеет ценность и не является спамом.

Деньги «в сети»

Начиная с 1970-х годов мы видим постепенный переход мира на цифровые деньги. Когда люди называют биткойн «цифровыми деньгами», они упускают суть данного понятия. Цифровой валютой можно назвать евро или американский доллар. Менее восьми процентов этих валют существуют в материальной форме; всё остальное – это биты[21] в электронных реестрах. Но фундаментальной разницей является то, что эти реестры контролируются централизованно организациями, а биткойн – нет. В основе биткойна лежит децентрализованная сеть, открытый протокол.

«Биткойн не цифровая валюта – это криптовалюта. Это деньги, расположенные „в сети“».

Биткойн не цифровая валюта – это криптовалюта. Это деньги «в сети». Мне действительно нравится идея таких денег. Биткойн позволяет выстраивать доверие на основе правил, которые установила сеть, заменяя

доверие к институтам и управление на основе иерархии! Сама сеть выступает в качестве третейского судьи, который способен урегулировать любые споры о транзакциях и безопасности, не находясь ни под чьим контролем.

Мечта о тотальном контроле над всеми финансовыми транзакциями

Начиная с 1970-х годов мировые валюты стали переходить в цифровую форму, но это не та же концептуальная форма, что есть у Биткойна. Все правительства вынашивают мечту о контроле любой финансовой транзакции каждого человека на планете: сделать так, чтобы они были прозрачными для структур власти. Если это произойдет, то право на неприкосновенность частной жизни будет полностью уничтожено. Возможность моментального проведения платежа поставит вас под наблюдение со стороны системы. Мы длительное время создавали систему тотального финансового надзора, действующую по всему миру.

«Все правительства вынашивают мечту о контроле любой финансовой транзакции каждого человека на планете: сделать так, чтобы они были прозрачными для структур власти. Если это произойдет, то право на неприкосновенность частной жизни будет полностью уничтожено».

Именно эта система, которой требуется идентификация, проверка кредитной истории и ограниченные права доступа, несет ответственность за то, что количество вовлеченных в экономику людей снизилось. Она также несет ответственность за то, что два с половиной миллиарда людей на планете вообще не имеют доступа к банковской системе. Это только цифры по числу домохозяйств, без учета всех членов их семей. Не были учтены и те, кто имеет ограниченный доступ к банковской системе с возможностью использования только одной валюты в пределах одного государства. Если посчитать всех, то их наберутся миллиарды.

Надзор за финансовыми транзакциями

Я представитель верхушки общества развитой страны[22], и у меня есть возможность открыть брокерский счет за один день в электронном виде! В течение суток я могу начать торговать японской йеной на токийской бирже или отправлять и получать деньги куда угодно и откуда угодно, по всему миру, без каких-либо лимитов и ограничений. Для этого требуется лишь одно – я должен пожертвовать своей конфиденциальностью и свободой.
Даже несмотря на то, что я способен совершать столь значимые действия, есть кое-что, чего я сделать не в состоянии. Я не имею в виду покупку наркотиков – это не так интересно. Речь идет об очень простых действиях: я не вправе пожертвовать деньги некоторым организациям с активной общественной позицией – например, WikiLeaks[23]. Несколько лет назад WikiLeaks была полностью отрезана от всемирной финансовой системы путем внесудебного давления, оказанного с помощью платежных операторов (Visa, MasterCard, система межбанковских платежей, PayPal и др.). Без каких-либо судебных разбирательств, без каких-либо доказанных обвинений и (как считаю лично я) без каких-либо вмененных правонарушений, кроме раскрытия правды о преступлениях, WikiLeaks была отрезана от мировой финансовой системы. Такое сейчас происходит не только с организациями с активной гражданской позицией, – это случается даже с целыми странами!
Мечта государственных аппаратов о создании финансовой системы под тотальным контролем умерла 3 января 2009 года – в тот самый день, когда появился блок генезиса[24], то есть в день создания Биткойна.

«Мечта государственных аппаратов о создании финансовой системы под тотальным контролем умерла 3 января 2009 года – в день создания Биткойна».

Деньги «в сети» не подвержены внешнему контролю

Биткойн устойчив к внешнему контролю. Возможно, вы об этом слышали. В биткойн-сети нельзя контролировать адрес[25] назначения платежа. Этот адрес не содержит никакой идентификации, как и привязки к географии (региону, стране). Неподверженность какому-либо внешнему надзору как одно из неотъемлемых свойств Биткойна обусловлено сетевым нейтралитетом и архитектурой глобальной сети с горизонтальными связями. Архитектура сети, реализующая принципы сетевого нейтралитета, где нет дискриминации по источнику информации, ее назначению и содержанию, обеспечивает отсутствие внешнего надзора.

«Взаимное наблюдение» – это не надзор сверху

Конфиденциальность (от
англ
. privacy) – понятие крайне важное и зачастую имеющее глубокое политическое значение. Давайте сопоставим его с другим термином – «секретность». В чем разница между «конфиденциальностью» и «секретностью»? На практике конфиденциальность – это право миллиардов людей жить без внешнего наблюдения. Секретность – это возможность, предоставленная властью весьма ограниченному числу людей, позволяющая ни перед кем не отчитываться и вести свою деятельность негласно.

Мы живем в финансовом мире, где каждая отдельная транзакция, которую вы проводите, каталогизируется, анализируется и передается в сотрудничающие между собой секретные службы по всему миру, – но мы при этом всё равно понятия не имеем, что делают с деньгами наши правительства. Финансовые системы, находящиеся у власти, непрозрачны. А все наши транзакции для них прозрачны благодаря имеющейся системе постоянного надзора. Весь мир перевернут с ног на голову. Но Биткойн это исправит.
Конфиденциальность является правом каждого человека. Секретность – привилегия людей, находящихся у власти; нам хочется жить в мире, где каждому человеку предоставлены права и гарантии, поскольку в этом и заключается суть свободы самовыражения, свободы слова, свободы участия в ассоциациях, участия в политических партиях – и всех остальных свобод, которые прочно связаны с конфиденциальностью. Нам хочется жить в мире, где секретность может быть нарушена, где власть обязана быть подотчетной, а информация о ее действиях – публичной. Мы должны перевернуть функционирование этой системы, поставив ее «на ноги».

«Конфиденциальность является правом каждого человека. Секретность – привилегия людей, находящихся у власти. Нам хочется жить в мире, где секретность может быть нарушена, где власть обязана быть подотчетной, а информация о ее действиях – публичной».

В списке моих любимых слов есть одно из французского языка – sousveillance, что в переводе означает «взаимное наблюдение»; оно противоположно слову surveillance, которое подразумевает наблюдение (или надзор). «Наблюдать» означает смотреть на что-либо сверху; «обратное наблюдение» означает взгляд снизу. В своих мечтах о тотальном контроле всей нашей финансовой жизни правительства допустили один серьезный просчет. Они не учли, что нескольким сотням тысяч людей будет крайне затруднительно наблюдать за остальными семью с половиной миллиардами. Как вы думаете, что произойдет, когда эти 7,5 миллиарда, наоборот, начнут присматривать за теми, кто наблюдает за ними? Когда «в глазок» можно будет заглянуть и с другой стороны? Когда наши финансовые системы, системы связи будут построены по принципам конфиденциальности, а возможность «быть секретным» превратится в иллюзию? Когда преступления, совершаемые во имя интересов государств и крупнейших корпораций, станут уязвимы для хакеров, бдительных граждан и любителей раскрывать секреты? Когда всё со временем вскроется, выплывет наружу? У нас появляется громадное преимущество, поскольку

естественный баланс системы – это когда человек обладает правом на конфиденциальность, а у власти больше нет права на сохранение секретности. Биткойн – один из первых шагов на пути к этому.

«У нас появляется громадное преимущество, поскольку естественный баланс системы – это когда человек обладает правом на конфиденциальность, а у власти больше нет права на сохранение секретности. Биткойн – один из первых шагов на пути к этому».

Банки для каждого

Возможность совершать трансграничные переводы между странами означает, что теперь мы сможем предоставить финансовые услуги миллиардам людей, которые не имели их ранее. Необязательно это делать с помощью изощренной технологии! Я иногда выступаю в различных банковских учреждениях разных стран, которых не пугает Биткойн. Мне там рассказывают интересные вещи: например, 80 процентов местного населения находятся примерно в полутора сотне километров от ближайшего отделения банка – и нет возможности предоставить им банковские услуги. Как-то раз мне сказали, что банк находится «в сотне миль, если плыть на каноэ». Сами угадайте, в какой стране было дело. Тем не менее даже в самых отдаленных уголках Земли сегодня есть вышка сотовой связи. Даже в беднейших регионах планеты на крышах хижин ставят небольшие солнечные батареи, которые нужны для зарядки телефонов модели «Nokia 1000». По количеству произведенных экземпляров эта модель стала абсолютным рекордсменом в истории промышленности – с заводов вышли миллиарды таких телефонов. Каждый из этих телефонов мы можем превратить не просто в банковский счет, а даже в целый банк!

«У меня нет в кармане счета в швейцарском банке. У меня там находится целый швейцарский банк».

В марте 2016 года действующий на тот момент президент США Барак Обама выступил на фестивале South by Southwest[26]; его речь была посвящена конфиденциальности граждан. Он сказал: «Если у нас нет возможности разблокировать ваш телефон, это означает, что у каждого в кармане есть счет в швейцарском банке». Это не совсем точно. У меня нет в кармане счета в швейцарском банке. У меня там находится целый швейцарский банк, с возможностью генерации двух миллиардов адресов с одним seed-паролем[27] и с возможностью использования разных адресов для каждой из транзакций. Транзакции этого банка полностью зашифрованы, так что даже если вы разблокируете мой мобильный телефон, то у меня всё равно сохранится доступ к моему банку. Происходит когнитивный диссонанс между возможностями, которые есть у власти, и новой силой, находящейся практически у нас в руках. Если вам кажется, что эту силу вам так запросто и без всякой борьбы отдадут, – вы сильно ошибаетесь.

Биткойн – «валюта-зомби»?

Почитайте, что пишут о Биткойне, – там всё то же самое, что писали об интернете в начале 1990-х годов. Это рай для педофилов, террористов, наркомафии и бандитов. Сколько среди нас людей с биткойнами в кармане? А сколько здесь террористов, педофилов, наркобаронов и бандитов? (Смех в зале.)
Видите ли, тут есть одно интересное обстоятельство: пока людям продолжают настойчиво внушать про негативные последствия, даже те, кто никогда не интересовался Биткойном, начинают замечать, что он не «умирает» – и это удивительно, ведь каждые два-три месяца появляется статья, уведомляющая о его скором исчезновении. Это прекрасная реклама. Ведь слыша, что Биткойн мертв, а спустя три месяца слыша, что он всё еще не умер, люди задумываются и говорят себе: «Н-да, а эта штука, кажется, живее всех живых». Я называю Биткойн интернетом денег, но, может быть, его стоит назвать «валютой-зомби». Потому что эту валюту «невозможно убить».

«Я называю Биткойн интернетом денег, но, может быть, его стоит назвать „валютой-зомби“. Потому что эту валюту „невозможно убить“».

Сейчас мы создаем систему, которая угрожает крупнейшей мировой индустрии – финансам. Правительства, разумеется, против, потому что хотят вернуть свои позиции и используют самую распространенную и эффективную тактику игры на страхе. Они считают вас идиотами и попытаются убедить в том, что вам есть чего бояться. Люди слышат такие утверждения, а на следующий день приходят на мои лекции; затем они знакомятся со стоматологом и архитектором, которые готовы принять оплату в биткойнах, с таксистом, посылающим деньги родным в биткойнах, – то есть с самыми обычными людьми, которые используют криптовалюту, чтобы получить финансовые преимущества и обеспечить себе финансовую свободу. Каждая попытка СМИ посеять сомнения в людях разбивается о противоречия, Биткойн выигрывает. Ему надо просто выжить, только и всего.

И до сих пор это у него отлично получается!

Эволюция валют

В новом сетецентрическом мире валюты занимают активно развивающиеся ниши. Они эволюционируют, словно биологические виды, реагируя на воздействие окружающей среды. Биткойн – это динамическая система с сообществом программистов, которые могут изменять ее. Вопросов лишь несколько. В каком направлении движется его эволюция? Какую нишу он может занять? Каким образом на него может повлиять власть? Если власть атакует Биткойн, то он будет эволюционировать, чтобы защититься от хищников, как это делает любой вид животных. А если она начнет атаку на анонимность Биткойна, то он сделается еще более анонимным. Если целью атаки окажется устойчивость Биткойна, то, эволюционируя, он будет стремиться к большей децентрализации. В конце концов, Биткойн – несмотря на все страшилки – это такой «милый плюшевый мишка» в мире валют, и вам не захочется его обижать. Потому что, как и в случае биологической эволюции, если вы наступите на маленькую ящерку, она эволюционирует и в итоге превратится в большого варана с острова Комодо, на которого вы уже вряд ли сможете наступить.
Меня иногда спрашивают: «Как вы считаете, органы власти запретят Биткойн? Как вы считаете, им удастся его зарегулировать „до смерти“? Как думаете, они будут устраивать DoS-атаки[28] против него?» Ответить на все эти вопросы несложно, поскольку любые атаки на сетецентрические системы – динамические и адаптирующиеся, проявляющие антихрупкость[29] – заставляют их самоадаптироваться, эволюционировать и становиться более устойчивыми. Задумайтесь об этом на минутку.

«Любые атаки на сетецентрические системы заставляют их адаптироваться, эволюционировать и становиться более устойчивыми».

Атаки повышают устойчивость

Моя жизнь с 1989 года связана с интернетом. В первые годы после его появления выходило множество статей о том, что сеть интернет неустойчива, немасштабируема для передачи голосовой информации, а также небезопасна. Я помню те времена, когда DoS-атаки на сервисы Yahoo, AltaVista и даже Google выводили их из строя на целые часы, а порой и дни. Что же произошло с тех пор? Сколько раз за последние пять лет вы видели, что Google не работает? Думаете, хакеры перестали атаковать его сервисы? Ничего подобного. Просто сегодня Google выдерживает гигабиты DoS-атак из любой точки мира и умеет динамически перестраивать маршрутизацию. То же самое относится ко всем интернет-приложениям. Атаки не прекратились. Но системы приобрели иммунитет по аналогии с иммунной системой человека: если в нее попадает вирус, который не убивает, то в организме вырабатываются защитные антитела – и в следующий раз этот вирус уже не нанесет никакого вреда.
Будут ли органы власти пытаться запретить Биткойн? Попытаются его регулировать? Атаковать? Они уже это делают! Они делали это практически с самого начала. Эта система подвергается постоянной DoS-

атаке, ее атакуют хакеры, агенты, другие системы – и это происходит круглосуточно. Но Биткойн становится лишь сильнее.

Эта система подвергается постоянной DoS-атаке, ее атакуют хакеры, агенты, другие системы – и это происходит круглосуточно. Но Биткойн становится лишь сильнее».

В информационной безопасности мы используем забавный термин: ловушка «горшочек с медом» (от англ
. «honeypot»). Такая технологическая ловушка предназначена для привлечения внимания хакеров. Сложно представить приманку масштабнее, чем финансовая сеть размером в шесть миллиардов долларов[30]. Если вы найдете способ, как взломать Биткойн, то вас ждет награда в шесть миллиардов! Но никто еще эту награду не получил, и вовсе не потому, что никто не пытался. Кто-то постоянно атакует сеть. Но системы, подобные Биткойну, оказались довольно устойчивыми.

Добро пожаловать в мир будущих финансов

Помните, что блокчейн – не просто новая криптовалюта. Это перестройка структуры общественных систем, которые нам уже не подходят. Иерархические системы XVIII столетия, которые неприменимы для решения проблем глобального взаимосвязанного мира, будут заменены информационными системами с одноуровневой архитектурой (то есть сетецентрическими системами), – неважно, будет ли это сама сеть интернет или любое приложение, работающее на ее основе либо на основе биткойна (или другой криптовалюты блокчейн-сети). Валюта – лишь первое приложение. Когда появляется равноправная сеть, внутри которой пользователи доверяют друг другу, то возможно построить с помощью нее бесчисленное количество приложений – для чего не потребуется спрашивать никакого разрешения у кого-либо.
Биткойн – гораздо больше, чем просто валюта. Когда я говорю, что Биткойн – это интернет денег, то акцентирую внимание не на деньгах, а на слове «интернет». Добро пожаловать в мир денег будущего!
Спасибо за внимание!

Инноваторы, разрушители, «белые вороны» и Биткойн

«Ярмарка изобретений»; музей им. Генри Форда, Детройт, штат Мичиган; июль 2014 года

Перед началом выступления аудитории был продемонстрирован подготовленный музеем фильм об истории автомобилестроения. Этот фильм упоминается несколько раз во время лекции.

Доброе утро! Забавное видео. Вам тоже понравилось? Месяц назад я продал свою машину за биткойны. Довольно интересный опыт, прямо новый мир! Скажите, у кого из присутствующих есть биткойны? А теперь вопрос тем, у кого их нет: слышали ли вы о них? Девяносто пять процентов присутствующих о биткойнах слышали. Тут есть такие, кто никогда не слышал о них? Хорошо, разговаривать будет проще, чем я думал.

Признание инноваций

Биткойн – это интернет денег, но не только. Здесь и сейчас – для всех собравшихся и для посетителей «Ярмарки изобретений» – я бы хотел поговорить о нем с точки зрения «белых ворон», чудаков и фриков. С позиции тех, кто отказывается мыслить, как все остальные люди; кто видит работающую не в полную силу, но элегантную технологию и сосредоточен на ее развитии. Именно такие пользователи обеспечивают инновациям признание. Это признание приходит за несколько месяцев или несколько лет до того, как его признают все остальные, иногда на целое десятилетие раньше. Именно такие люди приходят на «Ярмарку изобретений». Так что это отличное место, чтобы начать разговор о Биткойне.

Никто не ждал появления Биткойна. Биткойн – не те деньги, к которым мы привыкли. Он не должен был появиться и стать популярным, не должен был заработать[31]. Биткойн относится к такой категории изобретений, которая не работает в теории – и при этом работает на практике. Так же как Wikipedia, как Linux, как интернет. Странные идеи, рожденные бородатыми парнями с длинными волосами. Чудаками, которых никто не воспринимал всерьез.

Биткойн пользуется спросом потому, что он работает. Как технология он обладает элегантностью. Я хочу сказать о присущем ему духе маргинальности. Представьте, что вы входите в зал заседаний совета директоров промышленной корпорации и произносите: «Эй, знаете что? Мы тут сейчас всё поменяем!», – и вас под смех присутствующих оттуда выпроваживают. А вы продолжаете свое дело, идете своей дорогой, – и так до тех пор, пока действительно всё не изменится. В мире технологий такое происходит постоянно. Мы просто об этом забываем, игнорируем. Мы переписываем историю в «более радужном свете».

Опасности, которые несут в себе автомобили, электричество и Биткойн

Мы только что посмотрели фильм о заре автомобилестроения. Знаете, что писали газеты и журналы о первых автомобилях в то время? Они их высмеивали. Машины ехали медленнее лошадей, постоянно ломались. Им необходим был дорогой бензин, который еще и не так просто было найти. Для них требовалась инфраструктура. Газеты сосредоточились на историях, которые гарантировали высокие тиражи: автопроисшествиях, авариях с участием пешеходов. Больше двадцати лет после появления первых автомобилей о них писали только одно: это дьявольские, отвратительные, грязные и шумные машины, значительно уступающие лошадям; никакое развитие автомобилей невозможно, их всегда будут использовать только чудаки, и всегда они будут нести смерть своим водителям и любому, кто к ним хотя бы приблизится.

Истерия достигла такой степени, что в 1865 году в Великобритании приняли закон, который остался в истории под названием «Закон о красном флаге». Этот закон требовал, чтобы любое лицо, отправляющееся в путь на самодвижущемся экипаже, обеспечило для эксплуатации экипажа бригаду в составе трех человек – водителя, инженера и знаменосца. Водитель должен был управлять автомобилем, инженер – наблюдать за его управлением (как на железной дороге), а знаменосец с красным флагом – бежать впереди автомобиля на расстоянии 100 ярдов (91 м 44 см) и предупреждать пешеходов о грядущем появлении дьявольской машины, которая вот-вот их убьет.

Угадайте, что после этого случилось в Британии? Она проиграла промышленную гонку в автомобилестроении. Вместо того чтобы оценить ее потенциал, англичане просто испугались. Они создали такую среду, в которой возможности автомобиля нельзя было реализовать в полной мере. Ведь заставив автомобиль двигаться со скоростью бегущего впереди него пешехода с красным флагом, вы уничтожаете все преимущества автомобиля. Если для поездки необходима бригада из трех человек, автомобиль теряет все свои преимущества. Они рассматривали автомобиль с точки зрения перспективы того будущего, где транспорт – это железные дороги и лошади. Британцы ошиблись и проиграли гонку!

В фильме не было показано, что вплоть до этого момента англичане в этой гонке вели. Они уже выиграли гонку «индустриальной революции» с паровым двигателем. Первые работающие автомобили были созданы именно в Великобритании. В те времена именно Англия являлась движущей силой промышленных инноваций. Англичане выигрывали до тех пор, пока не решили выделить для грязных машин весьма ограниченное пространство и подчинить их набору правил. Они зарезали курочку, и золотые яйца закончились.

«Первые работающие автомобили были созданы именно в Англии. В те времена именно Англия являлась движущей силой промышленных инноваций. Англичане выигрывали до тех пор, пока не решили выделить для грязных машин весьма ограниченное пространство и подчинить их набору правил».

Эта история поучительна, поскольку она вновь и вновь повторяется в мире технологий. Не думайте, что, когда появилась возможность использовать электричество в быту, люди стали подключать дома к электрическим подстанциям, а газеты – выходить с заголовками «Блестяще! Эдисон – гений! Электричество перевернет этот мир!». Газеты кинулись писать, что это опасная технология, от которой сгорят жилые дома. Раз за разом повторялись истории о том, как людей бьет током, как полыхают жилища. Разумеется, какое-либо масштабное использование электричества сначала было невозможно, поскольку для этого требовалась капитальная перестройка жилищ. Нужно было завести в дом провода – а от проводки дом мог загореться. Нужно было покупать специальные устройства, которые работали бы от этих проводов, – ну, пока ваш дом не сгорел, конечно… Такое могли себе позволить только богачи. Совершенно очевидно: эта технология – всего лишь очередная причуда богачей! Просто игрушка без какого-либо практического применения.
Мэр города Парижа на Всемирной выставке 1900 года заявил: «Новая повальная мода на электричество кончится сразу же по окончании выставки – в один миг, как гаснет свет!» Мир технологий слышал много «авторитетных» приговоров, впоследствии вызывавших смех. Например, заявление главы корпорации IBM: «Я предвижу, что для всего мира будет вполне достаточно пяти компьютеров». Или высказывания тех, кто утверждал, будто новому изобретению под названием «телефон» никогда не стать массовым.

«Мир технологий слышал много „авторитетных“ приговоров, впоследствии вызывавших смех».

Угадайте – что сейчас говорят о Биткойне? Вам рассказывают, что это технология непривычная и чересчур сложная. Что она обслуживает неудачников и преступников. Я тут подобных людей что-то не вижу, но вы на всякий случай будьте начеку – а вдруг они появятся?
Разумеется, всё это неправда. Биткойн – это просто технология. Как это часто случается с технологиями, первыми их начинают применять преступники. Первые автомобили использовались, чтобы скрыться с места преступления. Первые телефоны были нужны для секретных переговоров и тайных заговоров, а первые телеграммы – для отправки на дальние расстояния мошеннических сообщений и для организации финансовых пирамид («схем Понци»). Электричество в первые годы после его появления часто использовали жулики для обмана и мистификаций. Такие вещи всегда случаются с новыми технологиями, и Биткойн не исключение.
Попытаемся найти причины, по которым преступники одними из первых используют новые технологии. Их деятельность связана с повышенным риском и поэтому должна давать очень высокую доходность. В этой среде процветает яростная конкуренция. И раз вы и так уже готовы брать на себя огромный риск, то использование новейших технологий – не вопрос. Если вы выигрываете, то получаете огромное преимущество. История учит нас тому, что самые безумные технологии первыми применяют именно преступники. Не думаю, что стоит включать эту мысль в маркетинговые планы по Биткойну, но всё же хорошо бы знать, что сейчас использует преступный мир – ведь лет через десять это станет распространенной технологией. Здесь наблюдается определенная динамика.
Биткойн давно прошел начальную стадию развития, когда он мог быть интересен только злоумышленникам. И, по правде говоря, нет никаких доказательств, будто на первых порах там был сплошной криминал, что бы ни утверждали СМИ. Сегодня Биткойн уже широко используется в самых разных областях, всё очень быстро меняется.

«В технологии Биткойн сейчас происходит нечто очень важное. Это нечто встряхнет финансовые и банковские системы – подобно тому, как появление автомобиля изменило всю отрасль перевозок на лошадях, и подобно тому, как производство масел повлияло на китобойный промысел, а электричество – на производство дровяных печей».

Я хочу рассказать о технологии Биткойн, поскольку в ней сейчас происходит нечто очень важное. Это нечто встряхнет финансовые и банковские системы – подобно тому, как появление автомобиля изменило всю отрасль перевозок на лошадях, и подобно тому, как производство масел повлияло на китобойный промысел, а электричество – на производство дровяных печей. Банковская система вот-вот будет разрушена. Некоторые утверждают, что она уже разрушается. Честно говоря, к тому времени, когда они смогут оценить масштаб бедствия[32], их песенка уже будет спета.

Обычно так всё и происходит.

Как компании реагируют на инновации

Когда солидная и крепкая индустрия впервые сталкивается с прорывной технологией, она ее игнорирует, не видя для себя угроз. С позиции действующего игрока отрасли, с высот прочно стоящего на ногах монополистического бизнеса все эти инновации выглядят детскими игрушками. С точки зрения JPMorgan Chase[33] Биткойн – это как киоск с лимонадом, конкурирующий с сетью супермаркетов Walmart[34]. Если технология продолжает свое существование, то происходит переход к новой стадии, когда игроки отрасли принимаются ее высмеивать. Внезапно инновационная технология появляется везде – и они начинают по этому поводу шутить. Так же, как высмеивали первых покупателей машин. В самом начале автомобильной эры их изображали вечно стоящими на коленях с гаечным ключом в руках и ремонтирующими свои автомобили, которые постоянно ломались. Таким был образ автомобилиста в те годы.
Пока они смеются, Биткойн продолжает расти и совершенствоваться. Через некоторое время вы заметите перемены. Сначала отдельные игроки отрасли скажут: «Кажется, нам тоже стоит попробовать. Возможно, надо присмотреться получше». Затем наступает паника: они вдруг осознают, что это новшество навсегда изменило их отрасль. Но в этот момент будет уже слишком поздно, так как они превратятся в компанию Kodak, которая занимала первое место в мире в своей области и за три года уступила рынок объемом 12 миллиардов долларов компании, которая прежде никогда не занималась производством фотоаппаратов! Знаете, кто разрушил Kodak? Маленькая финская компания Nokia. За три года она выпустила полмиллиарда камер и разрушила бизнес Kodak.
Компания Tower Records доминировала в музыкальной индустрии. Она исчезла за четыре года. Почему? Потому что с возникновением нового формата хранения аудиоинформации MP3 у людей появился выбор.
Компания IBM занимала незыблемые позиции в мире компьютеров. Они гарантировали качество. Честно говоря, если вы покупали компьютер и это был не IBM, все считали вас неудачником. Затем появился Linux[35], который встряхнул IBM до основания, опровергнув то, что лишь машины IBM годятся для решения задач банковской сферы, инженерного дела и государственного управления, поскольку это лучшие из возможных машин, – когда заказчикам была нужна закрытая, управляемая и продуманная система, построенная серьезными инженерами, у которых есть научные степени.
Когда в далеком 1992 году Линус Торвальдс[36] произнес: «Я создам свою операционную систему, не выходя из спальни, так как не могу себе позволить купить лицензионную операционку», – звучало это крайне нелепо. Операционные системы представляли собой огромные махины такой сложности, что для их создания требовались усилия тысяч инженеров. Линус Торвальдс приступил к разработке новой операционной системы. Через шесть лет созданная им Linux уже доминировала в компьютерной индустрии, и компания Sun Microsystems[37] стала испытывать трудности. Через восемь лет компания Sun Microsystems вплотную приблизилась к банкротству, компания HP была перепродана, их компьютерное подразделение закрылось, а IBM ушла с рынка персональных компьютеров.
Сегодня 80 процентов сотовых телефонов в мире работает под управлением ОС Android – которая, между прочим, тоже Linux. Серверы, к которым она подключается, работают под управлением Linux. Банковские системы, которые мы используем, также работают под управлением Linux, – и развлекательные порталы, на которых мы играем, и машины, которыми мы управляем. Всегда, когда они перестают работать, появляется приветствующий вас маленький синий экран, на котором написано: «Упс! Прошу прощения! Ошибка! Неправильно выбрана операционная система». Вы входите в самолет, вы загружаете программу, – всё это Linux. Если бы 15 лет назад вы сказали инженеру из IBM: «Ваша компания будет разрушена с появлением операционной системы, которую создал финский студент в своей спальне», – вас бы подняли на смех.

«Если бы 15 лет назад вы сказали инженеру из IBM: „Ваша компания будет разрушена с появлением операционной системы, которую создал финский студент в своей спальне“, – вас бы подняли на смех».

Но вот настало будущее, и Биткойн конкурирует со всей банковской системой – с самой мощной индустрией в мире. Угадайте, чем всё это кончится? Биткойн победит по одной простой причине. Не просто потому, что он лучше, и даже не потому, что банковской системой заправляют гангстеры, мошенники и люди в пиджаках, с полным отсутствием морали. А потому, что за последние полвека банковская система выдала ровно две инновации для потребителей: банкоматы и кредитные карты, – а всё остальное время потратила на изобретение новых способов ободрать вас как липку. Биткойн победит, потому что это открытая технология. В мире ремесленников, экспериментаторов и создателей нового побеждает открытость. Залог успеха в том, что это качество позволяет процветать инновациям повсюду.

«Биткойн победит, потому что это открытая технология. В мире ремесленников, экспериментаторов и создателей нового побеждает открытость. Залог успеха в том, что это качество позволяет процветать инновациям повсюду».

Открытые инновации и системы подписок

Позвольте пояснить, что я имею в виду под этим названием. Любая финансовая система в мире использует модель безопасности и доверия, в которой требуется исключение опасных участников из работы системы. Я не могу подключиться к сети Visa и внести изменения в работу программы, поскольку это поставит под угрозу ее безопасность. Я не могу подключиться к сети SWIFT, международной межбанковской системе платежей, поскольку это поставит под угрозу безопасность данной сети. Все эти сети построены как закрытые, их безопасность обеспечивается контролем доступа. Проводится очень тщательная проверка любого лица, которому требуется предоставить доступ к сети и к программному коду. Очень тщательно проверяются все приложения, работающие в системе, поскольку безопасность может быть нарушена при получении доступа к системе хотя бы одного злоумышленника. Как это случилось в 2008 году, когда мы обнаружили, что хакеры получили контроль над банками[38].
Их жадность разорила миллионы домовладельцев, пенсионеров и тех, кто годами копил деньги, – и это коснулось всего мира.

«Биткойн устроен по-другому: для поддержания безопасности сама сеть не использует принцип контроля доступа, – она опирается на простую математическую формулу расчета стимулов и вознаграждений».

Биткойн – это другая история. Но не потому, что нам вдруг удалось обнаружить самых честных в мире людей. И не потому, что здесь отсутствуют «глюки» или эту сеть никто не атакует. Особенность Биткойна в том, что, несмотря на мошенников в сети, для поддержания безопасности сама сеть не использует принцип контроля доступа[39], – она опирается на простую математическую формулу расчета стимулов и вознаграждений. Чтобы стать участником сети Биткойн и работать (для обеспечения защиты данной сети) в качестве майнера[40], нужно иметь возможность использовать компьютер со значительной вычислительной мощностью. Если вы выигрываете соревнование, то получаете биткойн в качестве награды. Простое уравнение создает систему стимулов, в которой выгоднее играть по правилам, чем пытаться эти правила обойти. Нечто вроде гигантского судоку или теории игр.
Если вы посмотрите на ситуацию с точки зрения специалиста по информатике или даже банкира, то скажете: «Разве это может работать?! Что вы имеете в виду под конкуренцией каждого с каждым и этим гигантским судоку? Такая система не может быть основой системы безопасности, она способна привести только к хаосу». Звучит примерно так, как если бы автор-составитель «Британской энциклопедии»[41] заявил: «Неужели вы всерьез считаете, что энциклопедию может редактировать кто угодно? Такое совершенно невозможно!» Ну а если вам еще нет сорока, то вы вряд ли когда-либо пользовались «Британникой»…
Биткойн – полностью открытая сеть. Возможность подключиться есть у кого угодно, вы прямо сейчас можете написать приложение и научить пользователей сети делать что-нибудь новое, можете создать финансовый сервис или финансовый инструмент. Вам не нужно будет идентифицировать вашу личность в сети и получать какое-либо разрешение, вас никто не будет проверять, вам не нужно думать о защищенности. Сеть вас не боится, поскольку ее безопасность не нуждается в том, чтобы отказывать в доступе потенциально опасным участникам. В реальности Биткойн прекрасно работает при наличии

множества этих участников даже в самом ядре системы – потому что это полностью децентрализованная система. Что будет, когда вы создаете сеть, где возможен открытый доступ к финансовым сервисам? Где впервые в истории любой пользователь может подключиться к сети и написать приложение?

«Биткойн – это интернет денег, а валюта – лишь первое применение».

Биткойн не валюта. Это очень важно понять. Валюта – приложение, которое выполняется в сети Биткойн; Биткойн – это интернет денег, а валюта – лишь первое его применение. Сегодня тысячи компаний занимаются созданием новых приложений. Они нанимают десятки тысяч человек, работая в одной из наиболее активных отраслей за последние двадцать лет. В 2014 году связанные с Биткойном стартапы получили инвестиции в размере более чем 250 миллионов долларов. И замечательно то, что деньги в Биткойн вкладывают охотнее и быстрее, чем в интернет в 1995 году! Мы впереди всей планеты! Биткойн развивается быстрее, чем Twitter и Facebook в первые несколько лет. Причина в том, что любой неудачник, чудак, фрик или программист из какой угодно точки мира может подключиться к Биткойну, не спрашивая разрешения; он может придумать свою безумную идею и запустить новый финансовый сервис, банковское приложение, приложение для покупок или же приложение для условного депонирования. Именно этим люди и занимаются – создают инновационные вещи, которых никогда бы не создали в обычном банке, потому что саму идею зарубили бы на корню.

«Когда бок о бок существуют две среды – банковская, в которой любое действие требует одобрения руководства, и полностью открытая система, где внедряются инновации без предоставления каких-либо разрешений, – угадайте, какая из них выиграет? Где происходит всё самое передовое и интересное?»

Биткойн является также одной из систем подписок. Вы выбираете, какие приложения будете использовать, с кем будете взаимодействовать. Выбираете правила взаимодействия. Если приложение вам не нравится, вы его не загружаете. Если нравится – загружаете и рассказываете о нем друзьям. Вот почему Биткойн победит. Он предоставляет пользователям необходимые решения.
Никто в Биткойне не пытается найти способ опередить алгоритм высокочастотного трейдинга, чтобы выжать три микроцента из четырех микроцентов быстрее, чем другой гигантский банк, который тоже играет с алгоритмами. Никто не пытается найти новый способ лишить вас вашего права на овердрафт – эту «инновацию» впервые применил один из крупных банков в 2007 году. Они придумали вот что: в момент, когда вы приближаетесь к пороговому значению овердрафта, они, вместо того чтобы сначала провести вашу крупную транзакцию, а потом мелкие, меняют порядок транзакций и первыми проводят мелкие – и вы платите комиссию в 25 долларов за каждую, а они получают максимум комиссионных. Вот какие инновации их интересовали! Так что изобретали банкиры лишь новые способы облапошить своих клиентов.
В Биткойне никто такими инновациями не занимается, потому что в этой сети никто не может никого заставить пользоваться каким-либо приложением. Если вы клиент крупного банка, то должны пользоваться его сетью на его условиях, – а если вам не нравится, можно обратиться в другой банк (чтобы выяснить, что все они одинаковы).

Вовлечение шести с половиной миллиардов людей в глобальную экономику

Вот еще одна причина, по которой Биткойн победит. Существует значительный дисбаланс, который мало кто замечает. У каждого в этом зале есть доступ к банковскому счету, который не находится под валютным контролем. С этого банковского счета можно покупать и продавать валюту, перечислять деньги в любую точку мира, получить доступ к международным рынкам – например, к Токийской или Немецкой фондовым биржам. Эти рынки предоставляют доступ к кредитным средствам и оборотным капиталам. Автоматические займы, залоговые займы… Это мощный банковский счет. И эта мощь доступна примерно миллиарду людей на планете. Миллиард людей имеет доступ к полноценным, международным и высоколиквидным банковским услугам.
Но у двух миллиардов людей нет никакого банковского счета. Еще у четырех миллиардов имеется такой доступ, но с ограничениями, то есть без международных валют, без международных рынков, без доступа к оборотным средствам. Биткойн создан вовсе не для того единственного миллиарда. Биткойн – сеть для

остальных шести с половиной миллиардов. Для тех, кто сего дня отрезан от международных банковских услуг. Как вы думаете, что будет, когда прямо посреди нигерийской деревни появится возможность превратить простой телефон – с одной лишь функцией передачи СМС и аккумулятором, заряжающимся от солнечной батареи, – в банковский терминал? В терминал пересылки денег Western Union? В международную систему по выдаче кредитов? В биржу? В средство размещения акций? Поначалу ничего особенного, а вот через несколько лет…
Мы уже представляем, что именно произойдет, на примере развития технологии сотовой связи: в Африке эта технология была развернута быстрее, чем какая-либо другая в истории человечества. Мы видели маленькие деревушки, в которых отсутствует водопровод, где пищу до сих пор готовят на кострах и где нет электричества; даже там на крыше какой-нибудь глинобитной хижины ставят небольшую солнечную батарею, и эта батарея предназначена отнюдь не для освещения. Она нужна, чтобы заряжать телефон Nokia 1000. Этот телефон сообщает им прогнозы погоды, текущие цены на зерно на местном рынке и соединяет их со всем остальным миром. Так что же произойдет, когда этот телефон превратится еще и в банк? Благодаря Биткойну он может стать банком. Что произойдет, когда шесть с половиной миллиардов людей станут участниками глобальной экономики без каких-либо ограничений доступа?

Денежные переводы влияют на жизнь людей во всем мире

Биткойн не валюта – это интернет денег. Как технология он может предоставить экономические возможности миллиардам людей. Я покажу вам лишь один пример конкретного использования Биткойна, которое фундаментально изменит жизнь более чем миллиарда человек в ближайшие пять – десять лет.
Ежедневно трудовые мигранты в Америке получают свои зарплатные чеки, обналичивают их и становятся в очередь, чтобы отправить часть денег домой семьям. Здесь, в США, у 60 миллионов человек нет банковских счетов, но эти люди получают деньги и посылают их за границу. Во всем мире из развитых стран ежегодно отправляется в виде денежных переводов 550 миллиардов долларов. Большая часть этих денег пересылается в пяти основных направлениях: в Мексику, Индию, на Филиппины, в Индонезию и Китай. В некоторых из этих стран денежные переводы составляют до 40 процентов местной экономики! На этом 550-миллиардном потоке сидят компании вроде Western Union; в среднем они забирают себе девять процентов от каждой из этих транзакций – забирают прямо из карманов беднейших в мире людей!

«Представьте, что будет, когда один из этих мигрантов додумается, что всё то же самое он может проделать с помощью Биткойна – и не за 15 процентов, не за десять и даже не за пять, а заплатив всего лишь пять центов? Не процентов, а центов – комиссию по фиксированному сбору».

Представьте, что будет, когда один из этих мигрантов додумается, что всё то же самое он может проделать с помощью Биткойна – и не за 15 процентов, не за десять и даже не за пять, а заплатив всего лишь пять центов? Не процентов, а центов – комиссию по фиксированному сбору. Что будет, когда они смогут это сделать? Уже сейчас это возможно. Создан стартап, который осуществляет денежные переводы из США на Филиппины. Сегодня их оборот составляет несколько миллионов долларов, и они не намерены останавливаться. В перспективе эта цифра может достичь 500 миллиардов долларов. Если вы мигрант и можете изменить ваше финансовое будущее, не отдавая девяти процентов за пересылку денег семье, подумайте, что будет, когда каждый месяц вместо отправки домой 91 доллара вы сможете отправлять по 100 долларов. Разница налицо. Сегодня у миллиарда человек есть доступ в интернет и есть смартфон, они могут воспользоваться Биткойном в качестве сервиса международных денежных переводов.

Биткойн изменит мир

Подводя итог, скажу: Биткойн – самая захватывающая технология, с которой я когда-либо сталкивался. Я познакомился с интернетом в 1989 году, когда был подростком. Задолго до того, как об этом догадались другие, я уже знал, что эта технология изменит мир. Я говорил всем вокруг: «Мы будем покупать в интернете. Все банки будут в интернете». Реакция окружающих была довольно предсказуемой: «Да-да,

Андреас. Делай-ка лучше уроки и не забудь навести порядок в комнате». Когда я впервые увидел Linux, то сказал: «Вот это да! Это навсегда изменит все операционные системы, IBM „катится вниз“». Все надо мной смеялись. Когда я впервые увидел веб-браузер и зашел на первый веб-сайт, то сказал: «Через десять лет у каждой американской компании будет сайт». Все снова надо мной смеялись. Что ж, позвольте теперь вам кое-что сказать. Я не знаю, что будет с Биткойном, но уверен: система криптовалют, в которую не входят банки и правительства, система, которая не имеет централизованного контроля и доступ к которой может получить любой, причем без всяких разрешений, – изменит наш мир!
Спасибо за внимание.

«Упрощенные» сети, инновации и «процветание ресурсов общего пользования»

Лекция прочитана в рамках проекта O’Reilly Radar Summit
[42]
; Сан-Франциско, штат Калифорния; январь 2015 года

В самом начале видео Андреас благодарит компанию O’Reilly за публикацию его книги «Осваиваем Биткойн» на условиях лицензии на свободное распространение. Он благодарит слушателей и всё сообщество за то, что помогли ему написать книгу. Она распространяется на канале github, есть на Amazon и на сайте bitcoinbook.info.

Сегодня я хочу рассказать вам об «упрощенных» и «умных» сетях. Я хочу рассказать о ценности доступности свободного программного обеспечения в финансовом секторе и о «процветании ресурсов общего пользования».
Биткойн одновременно и денежная единица, и сеть, и технология. Вы не можете разделить эти определения. Консенсус[43] этой сети, ценность которой базируется на валюте, не работает без самой валюты. Нельзя выстроить Блокчейн без криптовалюты, так же как любая криптовалюта не будет работать без блокчейн-сети. Биткойн – это и то и другое. Это точка, где сходятся сеть с коллективным консенсусом и глобальной, не признающей границы, безопасной криптовалютой.
Сегодня я хочу немного рассказать о сети Биткойн и подробнее остановиться на концепции, которая во многом напоминает интернет в его самом раннем периоде.

«Умные» сети против «простых»

Биткойн – это «простая», а не «умная» сеть[44], и в этом одна из ее важнейших особенностей. Биткойн – это «упрощенная»[45] сеть, которая создана для обработки транзакций, для верификации простого языка сценариев. Он не предлагает широкого спектра финансовых сервисов и продуктов, его функционал ограничен.
Когда вы разрабатываете сети и выстраиваете архитектуру сетевых систем, перед вами встает выбор: будет ли это сеть с поддержкой умных устройств или же сеть с поддержкой более простых устройств?

«Умная» сеть: телефония

Телефонная сеть создавалась как «умная» сеть. Сотовый телефон как оконечное устройство сети является оборудованием с ограниченным набором функций. Если у вас был телефон с импульсным набором

номера, то внутри него имелось максимум четыре электронных детали. Практически это был просто выключатель на проводе с присоединенным к нему громкоговорителем. Для набора номера следовало отправлять с определенной скоростью несколько электрических импульсов, чередуя их с паузами.
Когда-то телефон был очень простым устройством, и телефонная сеть имела лишь несколько функций: определение номера и ожидание вызова. Если вам хотелось улучшить качество услуг, нужно было улучшить сеть, а не модернизировать сами мобильные устройства. Решение в отношении такого дизайна сети являлось принципиально важным, поскольку в то время господствовало убеждение, что «умные» сети лучше: ведь для внедрения новых услуг достаточно было усовершенствовать только сеть, в интересах сразу всех пользователей.

«В результате проектирования „умных“ сетей новые сервисы добавляются только тогда, когда это потребность выявлена у всех пользователей данной сети, когда она достаточно востребована и убедительна для того, чтобы изменить функциональность работы всей сети с помощью ее обновления».

У «умных» сетей есть лишь один недостаток: модернизация идет строго в одном направлении – от центра к периферии. Это означает, что инновация (или новый сервис) внедряется централизованно, одним участником сети, с обязательным получением разрешения. В результате проектирования «умных» сетей новые сервисы добавляются только тогда, когда потребность в них выявлена у большинства пользователей.

«Упрощенная» сеть: интернет

Интернет – «упрощенная» сеть[46]. Она довольно примитивна. Всё, что данная сеть умеет делать, – это переносить данные из точки А в точку Б. Интернет не различает, когда вы делаете звонок по Skype и открываете какую-то веб-страницу; он не знает, какое устройство является конечным адресатом: персональный компьютер, мобильный телефон, пылесос, холодильник или автомобиль; он не знает, насколько это устройство мощное; он не знает, умеет ли устройство воспроизводить мультимедиа. Интернет всего этого не знает – для него это не важно.

«Чтобы запустить новое приложение или внедрить инновацию в „упрощенной“ сети, надо просто добавить сервис в само оконечное устройство. Поскольку данная сеть поддерживает „умные“ устройства, в сети вам ничего менять не потребуется».

Чтобы запустить новое приложение или внедрить инновацию в «упрощенной» сети, надо просто добавить сервис в само оконечное устройство. Поскольку данная сеть поддерживает «умные» устройства, в сети вам ничего менять не потребуется. Можно делать приложения хоть для пяти пользователей – лишь бы они обновили свои устройства, чтобы пользоваться ими. «Упрощенная» сеть будет также передавать данные пользователей, поскольку она не видит никакой разницы и для сети это не важно.

«Упрощенная» сеть: Биткойн

Биткойн – это пример «упрощенной» сети, поддерживающей «умные» устройства; идея Биткойна невероятно сильна, поскольку в нем все сведения сосредоточены на устройствах, образующих эту сеть.
Биткойну всё равно, принадлежит ли сетевой адрес мультимиллионеру, центральному банку или отдельному смарт-контракту[47], является ли он адресом устройства или конкретного человека. Сеть этого не знает. Не имеет значения, какая сумма передается в ходе транзакции, расположен ли адрес в Куала-Лумпуре или деловом центре Нью-Йорка.
Деньги передаются с одного адреса на другой по довольно простому сценарию. Если вы хотите создать новое приложение на основе протокола сети Биткойн, вам будет достаточно просто обновить само устройство и приступить к созданию приложения. Для разработки приложения вам не надо спрашивать

разрешения. Просто напишите приложение, запустите его на вашем устройстве, а сеть Биткойн возьмет на себя маршрутизацию трафика приложения, поскольку Биткойн – «упрощенная» сеть.
Вот в чем сила инноваций в интернете. Для них не нужны разрешения и одобрение какого-либо руководства. Это означает, что Биткойн – не специальная финансовая сеть для крупных или мелких, быстрых или медленных транзакций. Биткойн – сеть для чего угодно: всё зависит от того, что вы в вашей конечной точке сети хотите сделать.
Сравните Биткойн с существующей банковской системой, которая построена на «умных» сетях: передача данных здесь идет под абсолютным контролем предоставления доступа к приложениям на конечные устройства. Даже в самом сложноустроенном онлайн-банкинге всё, что вы можете сделать, – получить доступ к набору страниц, которые предоставляют спектр услуг вашего банка. У вас нет доступа к API[48], нет возможности запускать дополнительные приложения, делать обновления, вносить изменения, пока вся сеть не будет готова для технической поддержки вашего нового приложения. Существующая банковская система имеет сети для крупных и небольших платежей, для выполнения мгновенных платежей, – но не для всего перечисленного одновременно. Биткойн же не разделяет эти вещи.

«Существующая банковская система имеет сети для крупных и небольших платежей, для выполнения мгновенных платежей, – но не для всего перечисленного одновременно. Биткойн же не разделяет эти вещи».

Идея передать возможности интеллектуальных разработок конечным участникам сети без централизованного принятия решений позволяет всем пользователям самостоятельно создавать «нишевые» приложения, которые нужны разных группам людей по всему миру. Они могут создавать приложения без какого-либо разрешения.

«Трагедия ресурсов общего пользования»

У Биткойна есть еще одна уникальная черта; именно благодаря ей Биткойн существует и одерживает новые победы над прежними централизованными, закрытыми сетями. Я говорю о том, что Биткойн – это сеть с открытым исходным кодом.
Одна из ключевых концепций в экономической науке – «трагедия ресурсов общего пользования» (или «трагедия общин»[49]). Речь идет о том, что при наличии общего невозобновляемого ресурса, который может неограниченно потреблять любой участник рынка, ресурс в итоге истощается и вся система рушится. Такой рыночный «крах» и называется «трагедией ресурсов общего пользования». Обычно в пример приводят общинные (в традиционно английском смысле этого слова) травяные луга. Существует поле, на котором любой может пасти свой скот; и если все члены общины примутся без меры использовать его, то недалек тот час, когда луг превратится в грязное вытоптанное пространство и для скота не останется пищи. Из-за того, что все слишком увлеклись выпасом своего скота, ресурс исчерпался.

«Процветание ресурсов общего пользования»

В отличие от большинства финансовых сетей Биткойну не грозит «трагедия ресурсов общего пользования». Внедрять инновации в чужой сети я не могу. Если инновации внедряет Visa, то нововведение идет на пользу только Visa. Когда инновации внедряет MasterCard, пользу извлекает только MasterCard. Если в системе переводов SWIFT появилась новая функция – меня как потребителя она не касается. Если Bank of America внедряет нечто новое и привлекательное, они делают это лишь для повышения своей конкурентоспособности – чтобы исключить из числа своих конкурентов любой другой банк, у которого нет такой функции.
Биткойн – общий ресурс, использование которого только увеличивает его ценность, причем никого из числа пользователей исключать не нужно. Если какая-либо компания создает новую функцию в сети Биткойн на условиях лицензии с открытым исходным кодом, то эта функция может послужить всем участникам и обогащать их. Если какая-либо компания инвестирует деньги в Биткойн, в создание

протоколов, – выигрывает не только она, но и все остальные участники. Когда компания начинает играть на поле Биткойна, она получает выгоду и от инвестиций других компаний, которые вложились в Биткойн. Так что инвестиции возвращаются многократно. Возникает такая прекрасная синергия: каждая компания, инвестирующая в эту изумительную технологию, улучшает ее в интересах остальных участников сети. Здесь работает не принцип исключения, – вместо «трагедии ресурсов общего пользования» выходит, наоборот, «процветание ресурсов общего пользования». Общедоступные ресурсы становятся еще более качественными при использовании их большим количеством компаний.

«Работает не принцип исключения, – вместо „трагедии ресурсов общего пользования“ выходит, наоборот, „процветание ресурсов общего пользования“. Общедоступные ресурсы становятся еще более качественными при использовании их большим количеством компаний».

«Процветание ресурсов общего пользования», годы 2012–2014

Давайте рассмотрим несколько примеров. Две тысячи четырнадцатый год считается худшим годом для Биткойна. Но это так лишь с точки зрения котировок криптовалют; в том же году появились сразу две изумительные технологии. Первая – мультиподпись: для нее потребовалось внести небольшие изменения в основной протокол, что повлекло за собой создание огромного количество сервисов и продуктов, которые стало возможным создавать в конечных точках сети. Вторая – кошельки с иерархически детерминированными ключами: для них не понадобилось изменений протокола, они обеспечили появление невероятно сложных и богатых в функциональном плане опытов в сфере электронных кошельков.

Компании, которые придумали и разработали эти нововведения, начали работу в 2012 году, а возможности, которые они создали, мы используем сегодня. Эти два изобретения позволили создать целую инфраструктуру для новых продуктов и услуг. Средства, инвестированные одной компанией два года назад, дали мощный старт и потянули за собой создание целого диапазона продуктов в новой отрасли в настоящее время.

В 2014 году, во время худшего года для Биткойна, 500 стартапов получили 500 миллионов долларов инвестиций, создали десятки тысяч рабочих мест, но пока еще ни одно из их изобретений не «выстрелило» – потому что они только начали. Все поразительные технологические усовершенствования, которые мы увидели в 2014 году, стали результатами изобретений 2012 года. А теперь задумайтесь: что будет, если вы задействуете 500 компаний и 10 000 разработчиков для решения задачи? Дайте нам пару лет, и в мире Биткойна появится нечто поразительное! Это и есть преимущество принципа «процветания ресурсов общего пользования».

Ускоряя инновации

Пока журналисты пишут некрологи Биткойну, я вижу открытую экосистему, которая создает рабочие места в умирающей экономике. Я вижу экосистему, в которой работают умнейшие люди, создающие удивительные инновации. А самое поразительное здесь то, что выгоду получим мы все! Здесь никто ни с кем не конкурирует. Все работают на благо «процветания общин», и в результате скорость инноваций растет. Она уже и так предельная, но рост продолжается.

Создайте открытую, децентрализованную экосистему с «ресурсами общего пользования» – с открытым исходным кодом, открытыми стандартами, открытыми сетями; ум и изобретательность пробьются наружу и завладеют вниманием пользователей сети. Сравните такую экосистему с закрытой, которая контролируется центральным провайдером, чье разрешение непременно нужно для внедрения любой инновации… Мы их раздавим!

Меня спрашивают: «Ну ладно, а что будет, если банк Goldman Sachs создаст собственную криптовалюту – скажем, GoldmanSachsCoin?» Я вам отвечу: «Пусть создают!» Если их криптовалюта будет на основе открытой и децентрализованной системы, то они только подтвердят всё то, о чем я сейчас сказал, и мы с вами сможем разойтись по домам и отпраздновать победу. А если система будет закрытая, не допускающая открытого внедрения инноваций, то она умрет за несколько месяцев, мы же тем временем

продолжим ускоренное движение вперед, и каждое новое изобретение будет порождать всё больше и больше новых изобретений.
Этот процесс не остановить. Вот почему для меня настолько увлекательно быть частью биткойн-сообщества в «упрощенной» сети, где интеллект и инновации отданы на откуп устройствам и пользователям, где мы можем создавать и изобретать без всяких разрешений и участвовать в этом невероятном «процветании ресурсов общего пользования».
Спасибо за внимание!

Переворот в инфраструктуре

Цюрихский семинар по Биткойну; Цюрих, Швейцария; март 2016 года

Сегодня я расскажу о концепции под названием «переворот в инфраструктуре». Я расскажу о том, как всё изменяется, когда новой технологии сначала приходится использовать существующую инфраструктуру, и какой при этом возникает конфликт – и как потом он приводит к инверсии инфраструктуры.

Новые технологии работают на старой инфраструктуре

Биткойн – это нечто особенное! Я говорю о
Биткойне
в широком смысле; я говорю о децентрализованных сетецентрических платформах, которые можно использовать для работы с криптовалютами, выполнения платежей и для других надежных приложений. Платформа может быть Биткойн, а может быть и какая-то другая. В сегодняшней лекции я буду использовать термин
Биткойн
для обозначения целой категории уже существующих платформ. Мы пытаемся внедрить Биткойн в банковскую систему – и в результате наблюдаем беспорядок.

Этот хаос дает возможность тем, кто поддерживает традиционную банковскую систему, говорить: «Взгляните, Биткойн работает так себе». Ничего нового. Такое явление наблюдается всякий раз, когда появляется новая прорывная технология: в первые годы своего существования она вынуждена адаптироваться и работать в связке с существующей технологией, которую должна заменить.

«Такое явление наблюдается всякий раз, когда появляется новая прорывная технология: в первые годы своего существования она вынуждена адаптироваться и работать в связке с существующей технологией, которую должна заменить».

Давайте обратимся к истории и посмотрим, как развивались похожие события в прошлом. Когда мы читаем о прорывной технологии через 20, 30 или 40 лет после ее появления, нам кажется, что всё шло более-менее гладко. Само собой, ретроспективный взгляд позволяет видеть четче. Например, великим изобретением был автомобиль. И, конечно, когда в мире появились автомобили, все радостно воскликнули: «Ура! Лошади нам больше не нужны!» – правда? Нет – на самом деле всё было не совсем так. Люди говорили: «Это же просто какое-то безумие! Все эти шумные отвратительные машины – они нас всех доконают, они никогда не принесут никакой пользы. Разве только богатые дураки захотят ими баловаться, а на что они нормальному человеку, если есть на свете прекрасные лошадки?»
Вот что происходит в реальности, когда появляется новая прорывная технология. Первой реакцией становится сопротивление. Успеха добиваются те, кто продолжает верить в безумную идею, пусть все

вокруг и смотрят на них как на сумасшедших: так было и с автомобилями, электрификацией, интернетом – и с Биткойном. Первопроходцы, над чьими безумными идеями смеялись окружающие, продолжали делать свое дело до тех пор, пока общество не убеждалось в правильности их работы.

Инфраструктура для лошадей

В историческом аспекте самое интересное то, что на раннем этапе прорывные технологии вынуждены жить в мире, который был создан для старой технологии. Вы решили прокатиться в вашем новеньком автомобиле по городу – значит, придется ехать по дороге для гужевого транспорта; вся инфраструктура была создана для лошадей и ими же используется. Не существует светофоров. Нет правил дорожного движения. Дороги не вымощены.

«Вы живете в обществе, где все ездят на лошадях, – значит, это именно вы сошли с ума, решив кататься на безлошадном экипаже!»

У гужевого транспорта есть некоторые особенности, которых нет у автомобилей. Первые машины были с передним приводом – в движение их приводили два колеса. Лошади – транспорт с полным приводом, они движутся на четырех ногах, и это дает им определенные преимущества. Существовавшие дороги предназначались для поездок на лошадях. Отдельные участки были вымощены булыжником, но не большая часть дорог, поэтому обычно они были покрыты грязью и лошадиным навозом (поскольку лошадям свойственно производить навоз). Вот в какой инфраструктуре предстояло проявить себя первым автомобилям. Их путь не начинался с чего-то вроде: «Ура! Мы изобрели автомобиль! Позвольте продемонстрировать вам его возможности на автобане». Вместо этого безумные богачи, экспериментировавшие с новой технологией, должны были вести свои автомобили по дорогам с глубокими колеями от повозок, которые тащили лошади. По дорогам, которые не были предназначены для автомобилей, – прямо по грязи. И в итоге машины застревали.
Критики говорили: «Ха-ха, а мы ведь предупреждали, что автомобили непрактичны! Взгляните на себя! Вы даже из грязи выбраться не можете! А бензин вы где собираетесь брать? Ведь его продают на одной-единственной заправке, больше его нигде нет. Что будет, если бензин в машине кончится, а вы окажетесь вдали от заправки? Ведь если нужно накормить лошадь, она может потерпеть пару миль до кормушки, а если в вашем дурацком автомобиле кончится бензин, всё пропало – он не сдвинется с места. Вы и так уже застряли в грязи, а теперь вообще с места не сдвинетесь, потому что бензина нет.»

От лошадей к автомобилям

Очень часто на первом этапе новая технология должна использовать инфраструктуру той технологии, которую она впоследствии заменит. Автомобилям вначале пришлось ездить по дорогам, предназначенным для лошадей. Со временем дороги стали мостить камнем. Затем произошло нечто интересное. Если дорога замощена и пригодна для автомобиля, то и прежняя технология (лошадь) вполне может ею пользоваться. Если вам захочется объехать Цюрих на лошади и осмотреть окрестности, я уверен – поездка будет комфортной. Лошади отлично себя чувствуют на асфальте – не хуже, чем скейтбордисты, мотоциклисты, велосипедисты и любители кататься на сигвеях, хотя этих технологий тогда не существовало. На самом деле для того, чтобы эти технологии появились, сначала нужно было выстроить инфраструктуру для автомобилей.
Ровные асфальтированные дороги не только обеспечивают существование автомобиля, допуская и комфортное сосуществование гужевого транспорта, – наравне с этим они позволяют развивать новые транспортные технологии. Сегодня люди ездят на сигвеях, скутерах, скейтах, роликовых коньках, самокатах и на всем, что только может передвигаться по нашим улицам.
Вот что такое переворот в инфраструктуре. Всё начинается с новой технологии, которая использует старую инфраструктуру, а затем меняет ее. Вы строите новую инфраструктуру – и старая технология тоже начинает использовать новую инфраструктуру, предназначенную для новой технологии.

«Вот что такое переворот в инфраструктуре. Всё начинается с новой технологии, которая использует старую инфраструктуру, а затем меняет ее».

Давайте рассмотрим несколько таких случаев.

Инфраструктура для природного газа

У истории есть замечательные особенности: например, когда отдельные категорические заявления веками вызывают смех, хотя в них не было заложено и доли юмора. В 1889 году на Всемирной выставке в Париже впервые был представлен проект электрификации, и тогдашний мэр Парижа заявил: «Электричество – это просто забава, и как только закроется выставка и мы демонтируем Эйфелеву башню, электричество тут же канет в Лету». Попал в небо сразу двумя пальцами! И Эйфелева башня до сих пор стоит, и электричество одержало победу…

Но задумайтесь о том времени, когда электрификация только появилась: инфраструктуры для электричества не существовало. И как провести в дом это самое электричество? Единственной причиной желания иметь у себя электричество являлось то, что домовладелец принадлежал к числу тех самых безумных богачей, купивших себе автомобиль! А теперь он собрался впустить в дом молнии, от которых может случиться пожар! Вот что писали в газетах. Писали о каждом сгоревшем доме и о том, как эти умалишенные проводили электричество в свои дома.

Какой в то время была инфраструктура? В те времена инфраструктура в основном предназначалась для доставки в дома природного газа. Газовое освещение в крупных городах являлось самой обычной вещью. Существовали трубопроводы, по которым газ доставлялся к уличным фонарям; отводы от этих трубопроводов доставляли газ в дома для освещения и для отопления. Эту инфраструктуру для электричества использовать было нельзя. Она не годилась для передачи электроэнергии в дома.

Поначалу электричество стали масштабно применять на заводах и фабриках, поскольку именно на производстве электричество приносит больше всего пользы. До появления электричества на фабриках где-нибудь в углу устанавливали большие моторы, работавшие на газу. Мотор вырабатывал энергию и передавал ее другим фабричным машинам с помощью системы ремней и шкивов. С технической точки зрения это была газовая турбина. Электричество позволяло подвести электроэнергию непосредственно ко всему оборудованию, используя электромоторы.

Как видно, электричество давало фабрикам преимущество, но зачем оно в доме? Зачем вам пользоваться электричеством, если у вас уже есть прекрасно работающее газовое освещение и отопление? Да еще и инфраструктуры никакой нет! Газовая инфраструктура для электричества не годилась. Если вам требовалось электричество, приходилось строить новую инфраструктуру.

И здесь можно отметить еще один аспект, характерный для инфраструктурного переворота. Те, кто заинтересован (в том числе материально) в сохранении существующей инфраструктуры, говорят: «Распределительная сеть слишком мала, чтобы привлечь больше пользователей. А пользователей слишком мало, чтобы строить для них распределительную сеть. Всё безнадежно!» Ровно то же самое они говорили и про автомобили: «Бензозаправок недостаточно, чтобы заправить все машины, а желающих заправляться недостаточно, чтобы строить новые заправки. Не будет этого никогда!»

От природного газа к электричеству

Затем началась электрификация, и люди обнаружили: как только возникла инфраструктура для электричества, у них появилась возможность не только использовать новую электрическую силу, но и применять ее для прежних нужд. Электричество можно использовать для освещения и отопления, причем иногда с большей эффективностью, чем газ. Но появились и новые применения. Можно использовать

электричество для вентиляции, охлаждения, для двигателей и миксеров, с его помощью можно даже сушить волосы, – и, если взглянуть в общем и целом, не так уж и часто из-за электричества сгорают дома. Мы вновь увидели инфраструктурный переворот. Первые несколько лет приходится использовать старую инфраструктуру, что практически неизбежно. В теории можно, конечно, поставить дома газовый электрогенератор, подвести к нему газ и вырабатывать электроэнергию для дома, но это неэффективно. А потом возникает новая инфраструктура для новой технологии и позволяет вполне комфортно работать и старым технологиям: освещению, отоплению и, если говорить о дорогах, лошадям. Но при этом открываются возможности и для новых применений, о которых раньше и речи не заходило. И наш мир меняется.

«При смене инфраструктуры открываются новые сферы применения электричества, о которых раньше и речи не заходило. И наш мир меняется».

Инфраструктура передачи голоса

Мой третий пример связан с техникой. Именно сейчас присутствующие четко разделятся на тех, кому больше тридцати пяти, и на тех, кому еще нет тридцати пяти. Скажите, вы можете узнать эти звуки?

(Андреас воспроизводит звуки подключения телефонного модема.)

Те, кто младше тридцати пяти, смотрят на меня как на сумасшедшего, – а те, кому за тридцать пять, говорят: «Да это же модем! У меня такой раньше был! По нему можно было выйти в интернет». Что ж, простите, но сейчас мы поговорим о чем-то по-настоящему древнем. Слово «модем» получилось из слов «модулятор» и «демодулятор». Это устройство передает данные по телефонной линии. Если проводить аналогию, то телефонная линия – грязная дорога, по которой вы пытаетесь проехать на автомобиле.
Телефонная линия связи – это система, предназначенная для передачи голоса (голосовой информации). Когда я был подростком, телефонные линии были аналоговыми, и для связи у нас имелись аппараты с импульсным набором номеров. Иногда мы даже пытались проигрывать любимые песни друзьям по телефону. Если вы тоже пробовали, то знаете, что это невозможно. А невозможно потому, что передаваемый телефонной линией диапазон частот был очень узким.
Видите ли, телефонная сеть предназначена для выполнения одной-единственной функции. Это узкоспециализированная сеть – аналогично газовой сети, по которой в дома доставляется газ. Такая сеть создана только для доставки газа, а не воды, не электричества и не нефти. Телефония была придумана для передачи на расстояние исключительно голоса, а у человеческого голоса есть масса особенностей. Основная частота нашего голоса 1 КГц: мы все обычно говорим примерно с такой частотой, иногда уходя чуть выше или немного ниже. Довольно мало людей способны издавать звуки вне обычного диапазона. Подростки могут издавать звуки, которых я в свои годы даже и не услышу. Но из-за того, что голос используется людьми для конкретной задачи, а также потому, что возникают сложности в передаче голоса, особенно на большие расстояния, инженеры сузили допустимый диапазон. Если бы в системе был допустим весь диапазон звуков, вы смогли бы передать оттенки голоса, но при этом возникли бы статические шумы (электрические помехи на очень высоких частотах). Также слышалось бы жужжание (электрические помехи от моторов на очень низких частотах). И что делать, если в телефонной линии присутствуют статические шумы и жужжание? Добавляется фильтр, который отсекает нижние и верхние частоты. После этого связь становится чище, но человеческий голос начинает звучать непривычно, поскольку при передаче звук был сжат.
Такой сжатый канал – весьма неудобная среда для передачи данных, поскольку необходимо уместить большое количество информации в очень узком диапазоне частот. Именно поэтому модем издает свистящие звуки, так как для установления сеанса связи с другим модемом необходимо произвести тестирование доступной полосы частот. Весь шум – попытки установить соединение одного модема с другим на разной частоте: «Ты меня слышишь?», а второй отвечает: «Да, слышу. А ты меня слышишь?», – и так несколько раз, пока не будет установлен доступный диапазон.

Это был совершенно безумный способ передачи данных. Фактически у вас есть два устройства, которые

поют
друг другу по очень узкому каналу, стараясь пропустить как можно больше данных сквозь него. А затем мы начали их улучшать, и они стали справляться с задачей всё лучше и лучше.

Телефонным компаниям нововведения очень не нравились: «Разве для этого мы строили свои сети? У нас безупречная, высокотехнологичная сеть для передачи голосовых сообщений. Что вы творите?» У меня на родине – в греческих Афинах, – когда вы пытались совершить междугородний вызов с помощью модема, происходило следующее: сначала было слышно, как модемы начинают соединение, а затем раздавался резкий щелчок. Что такое? Что случилось? А просто линию отключали, когда обнаруживали модем. Почему? Потому что связь через интернет создавала конкуренцию бизнесу телефонной компании. Аналогично поступают банки, когда закрывают счета организаций, работающих с биткойном.
Что тогда про всё это говорили? «Мы можем построить сети для передачи данных и использовать оптоволокно, кабель или высокоскоростные выделенные каналы. Но, во-первых, никому не нужен широкополосный доступ – что с ним делать-то? Передавать голос? Но у нас уже есть великолепная сеть для общения! Нам все эти новинки не нужны. Во-вторых, откуда взять столько абонентов, чтобы прокладка кабеля для связи окупилась? Сети на коаксиальном кабеле нет, и больше клиентов привлечь не получится». Точно такая же мысль!

От передачи голоса к передаче данных

А далее имел место один из самых зрелищных примеров инфраструктурного переворота из всех, когда-либо произошедших в истории. Сначала интернет был никому не нужен; телефонные компании нехотя передавали его трафик своим сетям. Затем телефонные компании стали превращаться в интернет-провайдеров. И постепенно их магистральные линии начали ориентироваться преимущественно на передачу данных. А затем уже и сети сделались полностью цифровыми. После чего вся сеть связи стала работать по интернету, и телефонные вызовы – тоже передаваться по интернету. Сегодня любой телефонный вызов в мире, откуда бы вы его ни совершили, передается по интернету, не считая нескольких исключений в развивающихся странах. Произошел инфраструктурный переворот.

«Сегодня любой телефонный вызов в мире, откуда бы вы его ни совершили, передается по интернету, не считая нескольких исключений в развивающихся странах. Произошел инфраструктурный переворот».

Всё перевернулось: очень трудно втиснуть данные в узкий телефонный канал, но если поменять местами части уравнения, то выяснится: передавать телефонные вызовы по широкополосным каналам очень легко. В чем же разница? В том, что телефонная сеть – вещь узкоспециализированная. Единственное применение – голосовой вызов, а передача данных лишь исключение, которое приходится буквально «втискивать». В то время как сеть передачи данных лишена какой-либо избирательности. Данными может быть что угодно, и речь – это лишь один из видов данных, который без проблем можно передавать по новой сети.
По иронии судьбы, телефонным компаниям пришлось даже разработать специальную функцию, которая называется «генерация комфортного шума». Любой инженер связи знает, о чем я говорю, – действительно, такая ирония судьбы! За многие годы люди моего возраста привыкли говорить по телефону, в котором постоянно слышались статические шумы; с появлением сотовых телефонов и цифровых каналов связь стала совершенной, шумы исчезли. И в тот миг, когда ваш собеседник делал паузу в разговоре, на линии наступала абсолютная тишина. И вы думали: «Он, по всей видимости, повесил трубку».
Но ведь он не отключался! Он всё еще оставался на связи. Просто не было статического шума. И тогда телефонные компании разработали блестящую технологию создания «комфортного» шума. Генератор – устройство, которое находится в вашем аппарате и проверяет, поддерживается ли канал связи в настоящий момент; если связь работает, генератор «шепчет» вам в ухо, дабы вы не сомневались в том, что собеседник вас всё еще слышит. Устройство специально генерирует искусственный высокочастотный шум на вашей стороне канала; этого шума в канале связи нет, – и всё ради того, чтобы вы не думали, будто собеседник повесил трубку.
Те самые компании, которые раньше заявляли: «У нас никогда не будет возможности передавать голос через интернет в хорошем качестве. Нам не нужен никакой интернет в наших телефонных линиях», –

теперь нарочно шумят в процессе разговора, чтобы симулировать ужасное качество сетей предыдущего поколения, – потому что сегодня качество передачи звука с континента на континент не уступает качеству музыки на компакт-диске, а то и превосходит его. Произошел полный инфраструктурный переворот.

От банков к Биткойну

Теперь появился Биткойн – децентрализованная платформа, которая может проводить транзакции по всему миру без посредников. Но мы всё еще живем в старой системе. Сегодня мы вынуждены использовать биржи, привязанные к традиционным банковским счетам, либо пользоваться переводами по системе IBAN или кредитными картами. Мы вынуждены сегодня вести свой автомобиль по разбитым дорогам. Суперкар «Биткойн» – болид «Формулы-1» финансового мира – мчится по грязной дороге банковской системы, работающей на базе инфраструктуры 1970-х годов, и дорога сплошь в выбоинах.
Банки указывают на это и заявляют: «Не сработает! Вам придется ввести такое же регулирование, как и нам. Вам придется ввести идентификацию, как и нам. Вам придется замедлять процессы до скорости обычных банковских услуг, и у вас ведь недостаточно пользователей, чтобы построить новую инфраструктуру, и у вас нет достаточно развитой инфраструктуры, чтобы привлечь новых пользователей. Так что совершенно ясно: всё это никогда не заработает».
Но у нас, как и при изобретении автомобилей, электричества и интернета, – новая технология, и в будущем она получит тысячи других применений, которые пока невозможно даже вообразить.
Я предсказываю, что в следующие 15–20 лет мы увидим масштабный инфраструктурный переворот в финансовом секторе. Сначала банки будут противиться, затем смирятся. Они станут работать с системами Блокчейн и Биткойн, и в итоге вся традиционная банковская система превратится в приложение, работающее на распределенном реестре. Ведь несмотря на то, что его очень сложно реализовать, воспроизведение традиционных банковских услуг на распределенном реестре, в Биткойне, в открытом глобальном Блокчейне – задача тривиальная. Всё, что требуется, – взять все его возможности и замедлить. Например, я могу создать приложение, которое будет проводить транзакцию в срок от трех до пяти рабочих дней с комиссией в пять долларов, – так будет реализована традиционная банковская услуга. Напоминает генерацию комфортного шума, правда?

«Я предсказываю, что в следующие 15–20 лет мы увидим масштабный инфраструктурный переворот в финансовом секторе».

Ну а тем из нас, кто привык к банковским услугам предыдущего поколения и заявляет: «Не нравятся мне все эти шустрые финансы! Они вызывают у меня дискомфорт. Мне хочется сидеть по воскресеньям на кухне, сводить баланс в своей чековой книжке и думать о том, как бы мои чеки не отказались обналичивать. Не нравятся мне эти электронные мгновенные переводы по всему миру, они меня пугают», – мы сможем оказывать услуги обычным способом.
Инфраструктурный переворот позволяет функционировать традиционным банковским приложениям на глобальном распределенном реестре: на открытом Блокчейне – таком, например, как Блокчейн Биткойна. Одновременно этот переворот открывает дверь другим приложениям, доселе еще не виданным. Эти новые приложения будут отличаться от традиционных банковских услуг настолько же сильно, как отличаются сигвей или скейтборд от традиционных конных экипажей. Подобно электрификации традиционного викторианского жилища в эпоху газового освещения, выглядеть это будет столь же чужеродным, как комфортный шум в высококачественной голосовой связи через интернет, способной на большее.
Обеспечить будущее развитие, используя в качестве базы существующую систему, очень сложно. Стоит лишь попытаться, как все начинают вам указывать и говорить: «Глядите! Ведь не работает!» Но как только вы переворачиваете инфраструктуру, приспособление традиционных банковских услуг на сети будущего становится чрезвычайно простой задачей.
Все мы сегодня находимся на самой ранней фазе будущего денег – и лишь на первых фазах величайшего преобразования инфраструктуры, еще никогда доселе не виданного.
Спасибо за внимание!

Валюта как язык

«Биткойн-Экспо – 2014»; Торонто, провинция Онтарио, Канада; апрель 2014 года

Разговор сегодня будет с небольшим уклоном в философию – мы поговорим о будущем криптовалют и о том, что я узнал нового на выставке. Она называется «Биткойн-Экспо – 2014», но правильнее было бы назвать ее «Биткойн и Эфириум[50], Экспо-2014». Не знаю, заметили ли вы, но Эфириум представлен тут довольно широко. И возникает интересный вопрос, который мне задавало множество людей: «Угрожает ли Эфириум будущему Биткойна? Не перехватит ли он инициативу?» Эти вопросы задавались неоднократно, и я знаю, что люди обращаются к этой проблеме в попытке понять, что представляют собой альтернативные криптовалюты. Все задаются вопросами: не несет ли их существование угрозу доминированию Биткойна, не ослабляют ли они Биткойн, не «размывают» ли ценность и пользу сети?

Рожденная стать криптовалютой

Я довольно долго думал об этом и считаю, что сам вопрос порожден старой парадигмой понятия «валюта». Мы все выросли в мире, где валюта нам навязывалась как монополия, поскольку валюты определяются строго по географии своего возникновения – так что вы не можете выбрать себе валюту. Валюта, которой вы пользуетесь, зависит от места вашего рождения, а это случайность – как и многое другое в наших жизнях. Я, например, случайно родился в греческой семье, принадлежавшей к верхнему уровню среднего класса, и поэтому в моей жизни было немало привилегий. Кроме того, моя жизнь была связана с драхмой. Греческую драхму я не выбирал, как не выбирал родиться мужчиной белой расы; я не выбирал своих родителей, получивших высшее образование. Это просто случайные обстоятельства моего рождения.

«Валюта в нашем понимании – продукт деятельности национального государства. Это накладывает на нас определенные ограничения. Мы не выбираем нашу валюту, она выбирает нас».

Валюта в нашем понимании – продукт деятельности национального государства. И это накладывает на нас определенные ограничения. Мы не выбираем нашу валюту, она нас выбирает. И мы вынуждены ею пользоваться. У нас нет выбора – точнее, до 2008 года не было. Теперь мы живем в несколько ином мире, но наше мышление продолжает цепляться за устаревшую парадигму.
В мире, где валюта – монополистический продукт национального государства, находящаяся в рамках географического региона, получается игра с нулевым исходом, когда обязательно должен быть и победитель, и проигравший. Валюта – это еще один государственный флаг. Это выражение экономической ценности вашего государства. Она определяет все ваши взаимодействия в геополитическом мире, в глобальной борьбе наций за доминирование. Она не подлежит индивидуальному выбору. Она не имеет ничего общего с отдельной личностью, не считая ту личность, чей портрет на ней изображен; до недавних пор здесь, в Канаде, это был портрет одной старой леди, принадлежавшей к белой расе, по имени Елизавета.

Валюта как средство выражения

Сегодня мы живем в новом мире, где сами выбираем, какой валютой пользоваться. И дело не только в выборе. Речь о том, что это средство выражения. Любой из нас теперь может создать валюту с помощью инструментов, которые дает Блокчейн.
Раздумывая об эволюции альтернативных криптовалют, я пришел к выводу, что неверно ставил вопросы. Сколько всего будет существовать валют и альтернативных валют? Как по мере наступления будущего будут конкурировать альтернативные криптовалюты? Если существуют сотни альтернативных валют, что

это будет означать для стоимости каждой из них? Как они будут конкурировать? Этот метод размышления был неправильным. Я рассматривал валюту в качестве игры, в которой всегда только один победитель, – в навязанной моему мировоззрению перспективе валют, созданных национальными государствами. А затем я стал смотреть на нее по аналогии с мобильным приложением – как на средство выражения.
Видите ли, деньги в самой своей основе – это язык, который мы используем для выражения ценности чего-либо. Когда я даю вам банкноту в один доллар, я сообщаю, что передаю эквивалентную этой сумме ценность и тем самым заявляю о своем желании произвести обмен ценностями. Поскольку ценю нечто, что вы можете сделать для меня или дать мне.

Изобретение валюты

Люди изобретают валюту вне зависимости от наличия официально признанной денежной единицы. Если у вас не существует валюты с чьим-то изображением на банкноте, вы ее придумаете. Понаблюдайте за детьми в старшей группе детского сада в их, так сказать, естественной среде (хотя в большинстве школ эта среда скорее неестественная), у них никакой валюты нет, и что такое валюта, они тоже не понимают. Но они изобретают валюту! Они начинают обмениваться. Резинки для волос, карточки с покемонами, тамагочи, знаки любви, знаки популярности. Люди создают валюту в качестве средства выражения своих желаний, выражения своей индивидуальности. Я задумался: что же будет, если пятилетние дети в детском саду научатся пользоваться веб-сайтом для создания, например, Джо-койна, который будет конкурировать с Мэри-койном в игре завоевания популярности в рамках их детского сада?
И тут меня осенило: вопрос «Сколько будет существовать валют?» равносилен вопросу «Сколько может быть блогеров в интернете?». И ответ на эти вопросы очень простой: столько, сколько нас!

Сегодня валюта – это средство выражения. Но если валюту может создать кто угодно, то откуда у нее появится ценность и что она будет означать? В чем разница между валютами, если они выражают популярность, желание, представляют собой «мемы», результат чьей-то прихоти или являются брендом? Прямо сейчас вон там
(Андреас указывает за окно аудитории на улицу)
идет канадский конкурс «Кумир подростков». У одного из участников – его зовут Амир – много поклонников. Может, когда-нибудь он создаст валюту Амиркойн, чтобы его поклонники смогли выразить свое желание как можно больше видеть, как он танцует? Почему бы и нет? Меня многие спрашивают, не хотел бы я создать Андреаскойн. Мне кажется, что это как-то глуповато звучит, но почему бы и нет? Думаю, в скором будущем мы увидим подобные вещи.

Не будет нескольких сотен или тысяч альтернативных криптовалют. Они станут исчисляться сотнями тысяч, а потом и миллионами. Ежедневно будет создаваться несколько тысяч альтернативных криптовалют в целях организации местных сообществ и выражения каких-либо причуд, для проведения конкурсов красоты, для кодификации новейших сетевых «мемов».

«В мире не будет нескольких сотен или тысяч альткойнов. Они будут исчисляться сотнями тысяч, а затем миллионами».

Ценность валюты в силу производственных возможностей

Но если будет так много альтернативных криптовалют, то как определить, какие из них ценные, а какие – нет? Для ответа на подобные вопросы я обращусь к моменту появления первой в моей жизни децентрализованной системы – интернета. Что эта система сделала для устранения нехватки информации для ее усвоения и формирования мнений и авторитетов? Что сделал интернет для нас как для общества одним лишь своим появлением и глобальным распространением?

Были времена, когда для того, чтобы узнать авторитетное мнение, вам приходилось покупать у организации, владевшей печатными станками, лист бумаги; у организации было какое-нибудь славное имя, например «Нью-Йорк Таймс». Она имела возможность закупать чернила бочками – и в силу владения этой огромной производственной мощностью обладала весомым авторитетом. Мы сами наделяли полномочиями эти организации, и доверяли им, позволяя формировать наши взгляды.
А затем интернет всё изменил, поскольку вдруг оказалось, что печататься и публиковаться может кто угодно.

Заслуженный авторитет

В самом начале люди спрашивали: «Как узнать, чьи убеждения и взгляды значимы, если каждый может выразить свои?» Все думали, что скоро настанет конец света. Но вышло интереснее. Мы переместились из мира, в котором авторитет и мнение зависели от влиятельного издателя, – в мир, где о мнении нужно судить по присущим ему достоинствам, по содержанию этого мнения. Мы попали в мир, где «Нью-Йорк Таймс» печатает чушь, которая подталкивает целую нацию к войне, а египетский блогер в самой гуще революции пишет правду, которую никто не желает знать. Внезапно всё встало с ног на голову. Тот, кто владеет печатным станком, уже не обладает авторитетом. Влияние приобретает тот, кто обладает информацией. И мы только что сделали то же самое с валютой.

«Тот, кто владеет печатным станком, уже не обладает авторитетом. Влияние приобретает тот, кто обладает информацией».

Валюта приобретает ценность в силу использования

Сегодня авторитет возникает не в силу суверенности эмитента и не потому, что печатный станок принадлежит государству, которое благодаря своему монопольному приложению и силе объявляет вам, что вы будете пользоваться именно этой валютой. Сегодня валюту можно выбирать, и даже пятилетние дети могут создать валюту. И созданная ребенком валюта может иметь денежную стоимость, а может и не иметь. Скорее всего, она ее не имеет. Но некоторые валюты будут ее иметь. Нам еще нужно привыкнуть к миру, где о валюте следует судить не по тому, кто ее эмитировал, а по тому, кто ею пользуется. Точнее, по тому, сколько людей ею пользуется и для чего.

«Нам еще нужно привыкнуть к миру, где о валюте нужно судить не по тому, кто ее эмитировал, а по тому, кто ею пользуется. Точнее, по тому, сколько людей ею пользуется и для чего».

Давайте представим мир, в котором широко используется валюта, но никто не помнит, кто эту валюту создал и почему она была создана. Все знают лишь, что в пределах их местного сообщества у валюты есть покупательная способность.
Небольшая фантазия: представим, что через десять лет в глухой деревушке, вдали от развитых стран, деревенские жители меняются двумя валютами. На одной из них нарисована собака японской породы шиба-ину, и называется эта валюта догкойн. Не знаю точно, как это слово правильно произносить, да и неважно: важно, что за нее можно купить дюжину яиц. Вторая половина деревенских жителей использует другую валюту, на ней нарисована пожилая белая леди по имени Елизавета. Они понятия не имеют, кто такая Елизавета. Они не знают, почему ее портреты украшают монеты. Возможно, она написала хорошую песню, а может, выиграла канадский конкурс талантов Teen Idol. Никто этого уже не помнит, зато на эту валюту можно купить шесть яиц.

Этим людям всё равно, кто эмитировал валюту; им важно лишь, есть ли у нее покупательная способность. В такой ситуации валюта ценится исключительно по своей денежной сущности, в силу того, что она принимается, – в силу ее

использования
.

Между этими валютами существует одно фундаментальное различие. Для одной из них имеется предсказуемое, стабильное денежное предложение. А на второй просто есть портрет пожилой белой леди по имени Елизавета. Поэтому одна из валют обладает некой реальной и неотъемлемой ценностью – ведь в ней снижен уровень неопределенности, присущий традиционным валютам, – а вот вторая такой ценностью не обладает.
Нам нужно приготовиться к жизни в мире, где будет одновременно существовать множество валют.

Сосуществование множества валют

Валюта как средство выражения, как языковой инструмент теперь не зависит от эмитента. Всё теперь зависит от людей, которые совершили выбор, и ценность валюты рождается в процессе ее использования. Общество наделяет валюту ценностью самим фактом того, что готово ее использовать. Мы еще будем впечатлены валютами, которые появятся по чьей-нибудь причуде, в виде шутки (возможно, что и злой), и они войдут в массовое сознание интернет-пользователей, а затем обретут силу настоящих и широко используемых в сообществе денег.
Как же жить в таком мире? Что означает конкуренция валют, если этих валют – миллион? Будет ли существовать цифровой дефицит, хотя бы только на местном уровне и в контексте каждой из этих валют? Что, если дефицит не является функцией эмитента, а порождается в контексте приятия и в контексте знака как такового?

«Валюта как средство выражения, как инструмент выражения языка теперь не зависит от эмитента. Всё теперь зависит от личностей, которые совершили свой выбор и используют эту валюту: мы сами, используя конкретную валюту, делаем ее более ценной».

Появятся валюты для разных целей. Уже сегодня существует Биткойн, в котором реализована весьма специфическая денежная политика. Существует Эфириум, обеспечивающий договорную платформу. Существует Неймкойн для распределенных соглашений о присвоении имен. Существует множество других криптовалют, и появятся еще для решения других проблем: сворачивание белка, поиски внеземных цивилизаций… Возможно, возникнут криптовалюты, которые будут идеальны для микротранзакций и микроплатежей, где главное – скорость исполнения транзакции. Возможно, появятся валюты, подходящие для крупных транзакций вроде сделок с недвижимостью. Кто знает? Если рассматривать валюту как приложение, то становится ясно, что конкретное применение не так уж важно. В сети предком всех этих криптовалют была электронная почта. Она, как и Биткойн, стала приложением с убойной эффективностью, позволившим оценить всю мощь децентрализованного взаимодействия и принять новую платформу. Электронной почты оказалось достаточно, чтобы создать утилиту, распространившую сеть по всему миру, – и это было только первое приложение! Затем появились системы обмена мгновенными сообщениями, форумы, электронные доски объявлений, сервисы Facebook и Twitter. Беспокоит ли вас проблема полной замены электронной почты Twitter или полной замены систем мгновенных сообщений на сервис Facebook? Волнует ли вас, что польза и ценность электронной почты несколько снизились с появлением сервиса Twitter? Мы обо всем этом не думаем, поскольку понимаем, что каждый из таких сервисов нужен для разных целей. Некоторые из них обеспечивают выражение в поле мгновенной коммуникации в режиме реального времени. Другие обеспечивают асимметричные коммуникации: используя Twitter, можно говорить с многотысячными аудиториями и получать отклики в режиме реального времени без необходимости обеспечивать двунаправленную синхронную коммуникацию. Некоторые сервисы – например, электронная почта – позволяют организовать взаимодействие с ориентацией на более продолжительный срок передачи сообщений в асинхронном режиме.
Для возможности использования подобных функций мы строим интерфейсы, выстраиваем абстракции и разрабатываем средства унификации, которые позволяют нам использовать все эти разнообразные средства в едином интерфейсе с возможностью плавного переключения с одного сервиса на другой. Мы можем начать с передачи кому-либо короткого текстового сообщения, затем продолжить общение

голосом, потом переключиться на видеосвязь, а также организовать видеозвонок с участием кого-нибудь еще, а когда мы закончим общаться, можно подытожить все достигнутые договоренности электронным письмом. Таким образом, мы воспользовались пятью различными коммуникационными сервисами с помощью единого универсального интерфейса.

«Мы строим интерфейсы, мы выстраиваем абстракции, мы разрабатываем универсальные программы, позволяющие нам использовать разнообразные сервисы в едином интерфейсе с возможностью их плавного переключения».

Валюта как приложение

Вот что я думаю о будущем валюты. Мы будем рассматривать ее в качестве приложения, а для этого нам понадобятся интерфейсы, которые позволят унифицировать используемые валюты: у нас должен появиться один электронный кошелек – может быть, со 150 разными валютами. Благодаря изобретениям – например, «сайдчейнам», децентрализованным биржам, системам с высокой ликвидностью и полным отсутствием монополии, – благодаря синхронизации, благодаря ситуациям в мире валют, когда заложниками становятся обе стороны, мы сможем мгновенно и по минимальной цене проводить конверсию Биткойна и в Неймкойн, и в догкойн, и в Эфириум. И когда это станет возможным, то уже не будет иметь значения, поскольку заниматься этим будем не мы сами: этим будет заниматься интерфейс нашего универсального кошелька путем определения преследуемых нами при пользовании валютами целей. Если я хочу купить дом, то моя воля в виде транзакции будет выражена с помощью Биткойна, поскольку это самая подходящая для такого дела валюта. Если я хочу купить территорию (вокруг дома), то часть моей валюты будет конвертирована в неймкойны. Контракт (подразумевается смарт-контракт) будет оплачен через Эфириум. Если я хочу дать на чай бариста в кофейне, чаевые будут выплачены в догкойнах. И мой интерфейс скроет все их различия.

«Мы будем рассматривать валюту в качестве приложения, а для этого нам понадобятся интерфейсы, которые позволят унифицировать используемые валюты: у нас должен появиться один электронный кошелек – может быть, со 150 разными валютами».

Впереди нас ждет мир, в котором мы будем плавно перемещаться между валютами. Из этого следует кое-что еще: вполне реальная возможность отделить абстрактную стоимость обменного курса от фактической валюты. При наличии мультирежимной коммуникационной системы нам больше не нужно смотреть на индивидуальные стоимости и обменные курсы всех этих продуктов, ресурсов, валют – называйте как угодно.

Валюта как индекс

Имеется вполне реальная возможность появления отдельной валюты в форме индекса: такая валюта, которая сама по себе не торгуется, которую нельзя использовать отдельно в качестве товара, а лишь для выражения покупательной способности по отношению к другим криптовалютам и отображения стоимости в электронных кошельках. Универсальную валютную единицу купить нельзя. Можно купить биткойн, а затем сказать, сколько в нем универсальных валютных единиц. Я всё оцениваю в универсальных валютных единицах, а затем плачу в догкойнах, неймкойнах, биткойнах или эфириумах, в зависимости от цели использования мною валюты. Наши финансовые рынки уже так работают. К примеру, вы можете торговать на финансовых рынках, используя фондовый индекс S&P 500[51]. Вы не покупаете акций какой-то одной компании: вы покупаете агрегированное значение стоимости различных акций компании на фондовом рынке в виде выражения общей их рыночной стоимости. Этот метаинструмент можно использовать для оценки эквивалента стоимости транзакций.

Например, ставка предложения LIBOR[52] используется в качестве метапроцентной ставки для того, чтобы в договоре сделать привязку его положений к используемому в мире списку аббревиатур процентных ставок. Вам не нужно объяснять: «Я покупаю вот это по цене, объявленной „Бундесбанком“». Вы просто говорите: «Я покупаю это по цене LIBOR плюс два», – используя стабильную величину для фиксации стоимости и выполнения транзакции.
Думаю, вскоре мы увидим практически то же самое в мире криптовалют. Появятся метавалюты, единственной задачей которых будет агрегировать стоимости всех криптовалют во всех наших кошельках, что позволит понимать общий эквивалент стоимости всех валют в виде некоторой абстрактной единицы, существующей вне зависимости от каждой из валют, в виде которой она выражена.

Выбор валют и сообществ

Итак, это перспектива с небольшим философским уклоном. Вот почему я считаю, что различие валют не имеет значения: эфириум не конкурирует с биткойном, а биткойн не конкурирует с лайткойном. Все эти криптовалюты – механизмы транзакции, которые мы можем использовать в любой момент времени для достижения наших целей. Очень важное и мощное средство. А при выборе, который мы осуществляем в мире валют, мы также решаем, с каким сообществом себя отождествить.

«Принятие валюты – не просто действие по ее использованию: это также и отождествление себя с сообществом людей, которые принимают такую же валюту».

Принятие валюты – не просто действие по ее использованию: это также и отождествление себя с сообществом людей, которые принимают такую же валюту. Если мой выбор – принимать платежи в биткойнах, то вместе с этим я верю в денежную политику, выраженную в 21 миллионе денежных единиц[53]. Если мой выбор – принимать фрейкойны, это означает, что я верю в валюту с инфляционной базой, использующую отрицательную процентную ставку, которая стимулирует траты и делает невыгодным накопление. Я выбираю валюту и тем самым ассоциирую себя с глобальным сообществом людей, сделавших такой же выбор. Это же происходит, когда я использую приложение в интернете для общения. Я выбираю Twitter не потому, что он удобен для связи. Я пользуюсь им, так как соглашаюсь с философией сообщества людей, которые выбрали его.
В отношении валют подобный выбор становится серьезнее. Мы вышли на уровень метаполитики, в сферу возможностей формирования глобальных сообществ на базе общего политического согласия посредством выбора валюты. Хотите инфляцию? Пользуйтесь инфляционной валютой. Нравится золотой стандарт? Пользуйтесь дефляционной валютой. Хотите, чтобы валюта гарантировала минимальный доход для бедных? Хотите, чтобы при использовании валюты перечислялись деньги для сокращения выбросов диоксида углерода? Тогда выбирайте ту валюту, которая подразумевает вашу заботу об экологии. В конце концов, валюта – одна из форм языка, с помощью которого мы сообщаем о наших ценностях, и теперь мы можем делать это в огромном масштабе, поскольку валюту может создать каждый и в реальности значение имеет только наш выбор. Игра с нулевым исходом окончена. Теперь дело не в национальных государствах. И не в том, кто первым стал использовать Биткойн или криптовалюту, потому что ее принимают в интернете, а интернет – крупнейшая в мире экономика. Интернет – первая транснациональная экономика, и для нее требуется транснациональная валюта.

Валюта создает суверенитет

Давайте подведем итог: мы поменяли местами левую и правую части базового фундаментального равенства валют. Тысячелетиями, вплоть до 2008 года, валюта определялась суверенитетом, той базой, на которой создавались валюты, и они позволяли выражать этот суверенитет. Монополистический контроль валюты – базовая основа независимости любой страны мира. Сегодня интернет получил свою валюту и будет пользоваться ею, чтобы создать собственный суверенитет.

Начиная с 2008 года суверенитет обеспечивает валюта. У интернета есть своя собственная валюта: это означает, что интернет обладает покупательной способностью, то есть экономической свободой. Пользователь сети получает возможность игнорировать границы, лишая их прежнего значения. Если египетский блогер может не только писать у себя в блоге о революции, но и финансировать эту революцию с помощью Биткойна, общаться с людьми всего мира, разделяющими его убеждения в отношении самоопределения и свободы, то это означает, что, используя криптовалюту, он имеет возможность выразить личную независимость и независимость своего сообщества.
Вот в каком мире мы теперь живем; в таком мире валюты могут сосуществовать, а валюта и факт ее принятия пользователями создают суверенитет.
Спасибо за внимание!

Принципы работы Биткойна

Это выступление состоялось в июне 2015 года в Гарвардской лаборатории инноваций (Бостон, штат Массачусетс, США) в рамках проектного семинара IDEO Lab. Во время этого двухдневного семинара среди студентов проводился конкурс по созданию прототипов приложений на базе Биткойна и технологии Блокчейн.

С добрым утром! Да, задача у вас непростая. Но главное – вам нужно понять: что такое Биткойн? На данный вопрос я могу ответить одним предложением: Биткойн – цифровые деньги, хотя даже такое определение не отражает его истинной сущности. Скорее, это интернет денег. А в реальности – децентрализованная сеть, в основе которой лежит алгоритм консенсуса, на базе технологии Блокчейн и алгоритма доказательства работы, который позволяет организовать выдачу цифрового токена в качестве награды в соревновании с другими майнерами… И тут раздается: «Ой-ой-ой! Подождите, главное – не запутаться окончательно».
Даже через пару лет исследований на тему «Что такое Биткойн?» вы обнаруживаете, что всё еще находитесь в процессе обучения и пытаетесь осознать, что же это такое. Отчасти так происходит потому, что Биткойн – действительно новая прорывная технология и одновременно производная от одной древней технологии, которой уже очень много лет. Эта древняя технология – деньги. У нее много общего с лингвистикой, поскольку в нашем обществе она используется практически как язык, который мы используем, чтобы сообщить друг другу о ценностях.

История денег

Скажите мне: как долго существуют деньги?
(Реплика из зала: «Пять тысяч лет?»)
Да, хороший вариант. Правда, деньги существуют несколько дольше. Есть еще варианты? Главная проблема в истории денег – они древнее самой истории! Можно обратиться к письменным источникам, но деньги древнее письменности. Тут все начинают думать: «Что? Деньги древнее письменности? Да быть того не может!» Но на самом деле, если взглянуть на первые письменные источники, выяснится, что это бухгалтерские книги! Первое, что было нацарапано на табличках палочками и прочими подобными средствами, – бухгалтерская отчетность. Записывали, сколько амфор с маслом передано фараону. А если взглянуть еще дальше, то среди руин древнейших цивилизаций можно обнаружить и первые формы денег: это бусины, перышки, раковины и гигантские камни. Деньги обладали множеством форм, и существовали и существуют они практически с тех самых пор, как был придуман язык. Это воистину древнейшая технология. Так что ей не пять тысяч лет. Скорее, ей пятьсот тысяч лет, не меньше.

Приматы и деньги

В живой природе можно увидеть, как возникает понятие денег и у других биологических видов. Высокоразвитые животные – например, приматы, некоторые виды птиц (вороны) и даже морские животные (дельфины) – используют токены (жетоны) различных форм для сообщения друг другу о ценностях и очень легко обучаются технике применения денег. Если показать обезьяне, что в обмен на определенный камень она получит банан, в течение небольшого промежутка времени можно увидеть, что новый навык не только становится частью культуры приматов, но и передается ими последующим поколениям, и животные начинают изобретать способы получения «денег». Они организовывают ограбление: нападают на других обезьян и отнимают у них камни, чтобы получить за них бананы. Занимаются проституцией, обменивая сексуальные ласки на камни, за которые потом можно получить бананы. То есть придумывают формы экономических действий.

«Высокоразвитые животные – например, приматы, некоторые виды птиц (вороны) и даже морские животные (дельфины) – используют токены (жетоны) различных форм для сообщения друг другу о ценностях».

Деньги – очень древняя технология, и никто в действительности ее не понимает. Это легко доказать: попробуйте сесть и объяснить четырехлетнему ребенку, что такое деньги. Очень скоро вы обнаружите, что четырехлетний ребенок задает очень интересные вопросы, на которые вы не можете ответить. Понаблюдайте за родителями в процессе такой беседы – это довольно забавно.
– Мама, а откуда берутся деньги?
– Из банков.
– А как их там делают?
– Ну, их там печатают…
– А почему бы нам не взять их там побольше?
– Ступай наведи порядок у себя в комнате!
До «наведи порядок у себя в комнате» в разговоре о деньгах обычно успевает прозвучать не более четырех вопросов, поскольку взрослые плохо понимают, что такое деньги. Даже несмотря на то, что этот предмет материальной культуры существует в нашей популяции уже сотни тысяч лет, мы не понимаем, как он работает.

Характеристики денег

Деньги пережили несколько технологических эпох. Всё началось с простейших форм, которые обладали определенными уникальными характеристиками, благодаря которым эти формы могли служить в качестве денег. Почему какой-либо предмет может выполнять функцию денег? Потому что он редкий: раковины, перья… Можно применять ракушки в качестве денег, если вы, конечно, не живете на пляже, – потому что если вы живете на пляже, то раковины деньгами быть не могут. Большая часть предметов, являющихся деньгами, легко транспортируется. Ведь если сумма денег, необходимая для покупки коровы, тяжелее самой коровы, то это не очень хорошие деньги. Вот почему мы, например, нечасто видим использование золота в крупных сделках. Оно слишком тяжелое. Что касается остальных характеристик денег… Их должно быть трудно подделать – они не могут являться простыми в производстве. Необходимо, чтобы с первого же взгляда (по крайней мере, это не должно вызывать проблем) удавалось понять, что деньги настоящие. Предметы должны быть взаимозаменяемыми. Если мы используем раковины, то необходимо, чтобы и та раковина, и эта раковина – обе – могли являться деньгами. Если я даю вам доллар, не должно быть никакой разницы, какой конкретно доллар я вам даю: все доллары должны быть одинаковыми.

Деньги сами по себе – это абстракция. Если я дам вам бананы за вашу козу, то деньги здесь ни при чем. Бананы не деньги, потому что их можно съесть. Вы не станете использовать их для дальнейших обменов. Вот как получается бартер. Вы обмениваете один продукт на другой.
Всё это неизбежно приводит нас к одному умозаключению по поводу денег: деньги представляют собой всеобщую культурную иллюзию. Мы ходим и ассоциируем себя с другими людьми при помощи усеянных микробами кусочков бумаги с рисунками, нанесенными зелеными чернилами. И если бы мы посмотрели на этот процесс глазами прибывшего на Землю с другой планеты антрополога, нам всё это показалось бы очень странным. Путем обмена этими кусочками бумаги можно создавать социальные связи, совершать транзакции и вести торговлю; можно питаться, можно обеспечить себе убежище и т. д. Здравого смысла здесь немного, всё основано на коллективной галлюцинации. Всё базируется на предположении, что если вы мне сегодня дали доллар, то завтра кто-то еще примет у меня этот доллар в обмен на нечто ценное. Если я в это верю, то доллар имеет ценность. И данная ценность рождается из предположения, что я смогу использовать этот предмет снова.

Еще одна абстракция денег

Биткойн – новейшая абстракция денег. Абстракциями мы занимались и раньше, но всякий раз, когда она касается денег, общество впадает в панику: разве эта новая штуковина может быть настоящими деньгами? Можно оглянуться назад и вспомнить, что было, когда впервые возникли монеты из недрагоценных металлов, а затем и бумажные деньги. Когда в обращении появились первые банкноты, никто не верил, что они имеют ценность, то есть в тот момент всеобщая галлюцинация еще не овладела умами. Трудно было убедить людей обменивать монеты из настоящего золота или серебра на кусочки бумаги с надписями о том, что они обеспечены находящимся в хранилище золотом. Ведь если золото из хранилища исчезнет, то можно будет лишь сказать: «Да ведь это просто бумага!»
В разговорах о биткойне я часто сразу слышу от собеседников, что биткойн – не настоящие деньги, потому что он не обеспечен золотом, как американский доллар, – и это меня изумляет. Доллар не обеспечен золотом с 1936 года! Но большинство людей думают, что где-то там в хранилище – в Форт-Ноксе или в какой-нибудь другой кинодекорации – покоятся золотые слитки, которые вплоть до грамма соответствуют тем кусочкам бумаги, которые у всех лежат в карманах. Нет, это не так. Так почему же биткойн – это деньги? Потому что люди думают, что это деньги! Можно написать дюжину диссертаций с подробными объяснениями, почему биткойн не деньги. Но вот лично я живу на биткойны уже два года. Так что для меня это самые настоящие деньги. Таким образом, не имеет никакого значения, что написано в вашей докторской. Для меня это деньги, и тысячи других людей живут так же.

Биткойн и проектирование

Перед вами стоит задача создать дизайн и концепцию для древнейшей в мире технологии, которую мало кто хорошо понимает. Ее новейшая и наиболее абстрактная форма невероятно сложна в технологическом плане – куда сложнее, чем предыдущая. И когда вы подойдете к задаче вплотную, наилучшей техникой поиска решения будет использование архитектурных метафор (аналогий). Архитектурные метафоры в проектировании – очень мощное средство. Это инструменты, с помощью которых мы создаем ожидания потребителей. Если у вас есть компьютер, можно предположить, что произойдет, когда вы переместите какой-либо элемент на его «рабочем столе». Поскольку вы наверняка пользовались обычным письменным столом, то такое предположение ляжет в основу ваших ожиданий. Вы будете ожидать, что новая сущность станет вести себя так же, как и та сущность, которой она притворяется. Вот что такое архитектурные метафоры в проектировании. Это очень мощные инструменты, но также и весьма опасные, если их применить неправильно.

«Архитектурные метафоры – очень мощные инструменты, но также и весьма опасные, если их применить неправильно. В технологии Биткойн каждый термин и каждая архитектурная метафора некорректны».

Кошельки – это не кошельки на самом деле

В Биткойне каждый термин и каждая метафора некорректны и разрушают общий смысл. Давайте пройдемся по списку. Вы, скорее всего, уже столкнулись с этой проблемой, когда знакомились с технологией Биткойн и ее терминологией. Номер один: «кошелек». Что это такое? Кошелек – предмет для хранения денег. Но в Биткойне это не так. Деньги находятся не в самом кошельке: деньги находятся в распределенной сети. В биткойн-кошельке лежат ключи. Так что это не кошелек, а скорее брелок с ключами. Вот вам еще одно доказательство того, что это не кошелек: подумайте, можно ли скопировать кошелек. Конечно, нет. А сделать копию ключа – запросто! Поэтому брелок – гораздо более уместная метафора. Если у вас есть брелок – представьте себе такую огромную связку ключей; можно сходить в мастерскую и сделать их дубликаты, чтобы создать копии. Обе эти связки будут взаимозаменяемы для всех замков, к которым подходят ключи из оригинальной связки. И если вы понимаете, как работает брелок с ключами, то вы легко поймете, как работает кошелек в Биткойне. Его можно скопировать, можно сделать копии ключей. Если вы передадите кому-нибудь дубликат ключа, то этот человек сможет открыть дверь. Ему не понадобится ваше разрешение.

В Биткойне нет монет

Обратимся к основам: слово «Биткойн» состоит из двух частей, «Бит» и «койн» (coin от
англ.
«монета»). Что за ужасное слово «монета»! Монета… Нет, ну надо же! Взять наиболее абстрактную форму денег из созданных человечеством, основанную на полностью децентрализованной сети, в которой нет никаких монет, и назвать ее
монетой
. Наверное, чтобы враг не догадался. Ведь монета – это сущность, появившаяся в позапрошлой технологической эпохе, гораздо менее абстрактная и имеющая конкретное материальное воплощение; это осязаемое представление денег. И вот мы берем наиболее абстрактное представление денег и называем его именем самого что ни на есть материального представления. Лишь инженер может так обращаться с брендами!

Открою небольшой секрет: в Биткойне нет никаких монет. Когда майнеры майнят, они не создают никаких монет – они создают записи в распределенном реестре. В этих записях в реестре количество монет не указывается. В них заносятся результаты транзакций, представляющие собой фрагменты данных о ценности, которые могут делиться до бесконечности и снова комбинироваться. Монеты так не умеют. Монету в Биткойне отследить нельзя, потому что в Биткойне нет никаких монет.
Итак, у вас имеется «кошелек», в котором нет никаких «монет» – потому что эти «монеты» на самом деле находятся в сети, да это и не монеты, а результаты транзакций, – и в действительности вместо кошелька у вас есть брелок с ключами. Транзакции не инициируются отправителем и не направляются получателю. У адресов в Биткойне нет баланса. Для адреса не существует такого понятия, как баланс. Адрес управляет результатами транзакций, и если вы тщательно просмотрите весь блокчейн и просуммируете все результаты транзакций, то сможете вычислить некий номинальный баланс. Можно ли его расходовать или нет, сколько это в числовом выражении, – всё это в действительности довольно сложно определить. Нет такого понятия, как «баланс». В Биткойне у вас нет никакого «счета».
Вся терминология нарушена. Проблема в том, что описание архитектуры Биткойна вместо того, чтобы с помощью использования корректных метафор формировать у пользователя соответствующие действительности ожидания, только запутывает. Данная терминология создает почву для неправильного понимания, поскольку мы считаем, что, к примеру, «кошелек», должен работать вполне конкретным способом, а в итоге работает совершенно по-иному и довольно неожиданно. Вроде рабочего стола в Windows. Не знаю, приходилось ли вам сравнивать рабочие столы в системах Mac и Windows? Мне

кажется, что в Windows рабочий стол страдает отсутствием логики. Вы ждете, что произойдет одно, а он делает совершенно другое и ставит вас в тупик. Суть хорошего дизайна в том, чтобы каждая из выбранных метафор формировала реалистичные ожидания от применения системы.

«Суть хорошего дизайна системы в том, чтобы каждая из выбранных метафор формировала реалистичные ожидания пользователей при ее применении».

Скевоморфический дизайн

Существует большая проблема, связанная с метафорами и архитектурой сети, – это скевоморфический дизайн. Термин «скевоморфический» родом из греческого и означает «тень прежнего себя». При создании новых элементов их делают похожими на прежние формы чего-либо. Классический пример: в первом поколении iPad программное обеспечение iOS включало множество примеров скевоморфического дизайна. Например, при открытии «контактов» интерфейс напоминал ежедневник в кожаном переплете. Кожаный переплет был даже прошит нитками! Эти нитки не несли никакой функциональной роли. Это был просто нефункциональный элемент дизайна, призванный настроить пользователя на привычный ход мыслей, чтобы архитектурная метафора сработала. Когда вы играете на компьютере в карты, карты на экране выложены на зеленом сукне; этот элемент дизайна – метафора стола в казино. Дизайн в стиле скевоморфизма – исключительно мощная штука. Одновременно и очень опасная! Если вы используете его неправильно, то он становится причиной неверных прогнозов.
В Биткойне многие элементы имеют скевоморфический дизайн. Мой самый любимый и самый ненавистный пример подобного дизайна – это картинка, которую можно увидеть в каждой статье о Биткойне: куча золотых монет с буквой «В» на аверсе; как правило, это созданные Майком Калдвеллом физические монеты Casascius со знаком Биткойна, хотя встречаются и другие варианты. Майк взял наихудшую из метафор и придал ей красивую материальную форму при помощи скевоморфического дизайна, чтобы окончательно всех запутать. Люди заходят на онлайн-аукцион eBay и покупают там предметы, которые, как они думают, и есть тот самый «биткойн». На самом деле они покупают позолоченные металлические жетоны, которые не имеют ничего общего с Блокчейном, не считая отлитой на них буквы «В». «Глядите, я тоже присоединился к цифровой денежной революции!» – говорят покупатели, однако стоимость этих материальных предметов крайне редко имеет какой-либо эквивалент в Биткойне. Вот вам результат! Затем журналисты строчат статьи, люди смотрят на картинки и думают: «Так вот ты какой, биткойн!» Но биткойн вовсе не такой, поскольку (вы наверняка это помните, я уже об этом рассказывал) никаких монет в Биткойне не существует. Вот в чем опасность.

Проектирование дизайна для инноваций

Задача создания метафор, которые описали бы то, что происходит в Биткойне, крайне сложна, поскольку параллели отсутствуют. Мы никогда раньше такого не делали. И мы попадаем в ловушки, пытаясь экстраполировать прежний опыт – а он ничему не соответствует. С прорывными технологиями всегда так. В последовательно развивающейся технологии берется то, что может называться общими понятиями, добавляется чуточку перспективы и еще чуть-чуть расширяется точка зрения; новую технологию вы понимаете потому, что на самом деле она лишь слегка расширенное представление предыдущего этапа. Биткойн – это радикальный прорыв вперед, так что знания о механизме работы традиционных денег не помогут вам понять Биткойн, скорее даже затруднят. Люди, разбирающиеся в Биткойне, отнюдь не специалисты по монетарной экономической теории. Такие специалисты Биткойн не понимают. Они пишут объемные работы о том, что Биткойн не деньги, – даже несмотря на тот факт, что лично я уже два года живу на биткойны.

«Биткойн – это радикальный прорыв вперед, так что знания о механизме работы традиционных денег не помогут вам понять Биткойн, скорее даже затруднят».

Понимание прорывных технологий гораздо сложнее понимания поступательно развивающихся технологий, поскольку для всего самого интересного параллели отсутствуют. Попробую пояснить: вспомните американский сериал «Звездный путь» («Star Trek») 1970-х годов.
Что там смогли угадать? В сериале были «трикодеры» – портативные коммуникаторы. Там была видеотелефония. Там имелось всё, что удалось предсказать на базе технологий 1970-х годов. Интернета там быть не могло. Тогдашние сценаристы не обладали возможностью придумать идею сетевых хранилищ информации. В сериале были фантастические компьютеры, которые могли разговаривать с людьми, но эти машины не имели доступа к данным. Невозможно было предсказать появление сетевых средств массовой информации. И самое важное: если смотреть внимательно, можно заметить нечто очень странное – в мире «Звездного пути» деньги отсутствуют. Нигде во всем фильме нет денег! Почему? Потому что самой отдаленной перспективой, которую удалось разглядеть сценаристам, оказалось безденежное общество; в этом обществе нет языка сообщения ценностей, что является, возможно, наиболее радикальным отклонением фильма от реальности.

Предсказание будущего

Когда мы пытаемся предсказать будущее, возникает несколько абсолютно неизвестных областей. Это те области, которых мы никогда не видели. Приложения, которые нельзя представить, поскольку для того, чтобы они появились, должно совпасть множество факторов. Чтобы появился интернет, необходим общий стандартизированный протокол передачи данных. Чтобы в интернете зародились социальные сети, необходимо массовое проникновение базовых коммуникаций по электронной почте и соединений по TCP/IP. Проникновение этих сервисов должно быть таким, чтобы обеспечивалась ситуация постоянного подключения. Необходимо появление умещающихся на ладони мобильных устройств с возможностями высокоскоростных вычислений, причем устройства должны иметь возможность постоянного присутствия в интернете. Всем эти вещам пришлось осуществиться, чтобы возник феномен социальных сетей.
Взглянув на интернет из 1992 года, можно было сказать, что эта вещь заменит телефон. Ведь телефон являлся единственным опытом подобного рода. Возможно, это необыкновенный телефон/факс; может, это многофункциональный принтер/факс/телефон. Так что телефонные компании смотрели на всё это и говорили так: «Ну да, это просто необычный телефон. Мы вполне можем сделать то же самое». К счастью, они заблуждались. В противном случае всякий раз, когда мы звоним по Skype, пришлось бы раз в три секунды засовывать по монетке в боковой слот на компьютере. К счастью, правила игры в этой сети разрабатывали не телефонные компании. Они оказались неспособны спрогнозировать всё то, что мы видим в интернете, поскольку самое интересное было не в русле поступательного развития технологии и не в расширении существующих возможностей. Всё самое интересное являлось радикальным отходом от прошлого, поскольку создавались условия для того, что раньше было невозможно.
Давайте вернемся к Биткойну и на несколько секунд задумаемся. Подумайте, о чем мы только что говорили: о финансовых транзакциях, банковских услугах, платежах. «Ну да, это просто необычная кредитка! Практически то же самое, что и Paypal, только глобальнее». Но это не так. Это нечто совершенно иное, но мы пока не можем увидеть, к чему всё это придет. В Биткойне появятся новые приложения – и залогом их появления будет достаточная степень распространения данной технологии.
Сегодня у трех миллиардов людей на планете нет никаких возможностей для банковского обслуживания. Три миллиарда людей не имеют доступа к банковским услугам в силу географических и экономических факторов – абсолютно никакого доступа к международной кредитной и финансовой системе. Мы с вами прямо сейчас можем зайти на веб-сайт брокерской компании и в течение суток оформить счет в американских долларах, с которого можно торговать на Токийской фондовой бирже. Эта возможность доступна менее чем одному миллиарду людей. Только каждому седьмому жителю планеты. Как же остальные шесть миллиардов? Не у всех есть даже возможность выписать чек, если уж на то пошло. Большая часть людей живет в обществах, где используются только наличные деньги или натуральный обмен. Так что стоит задуматься над таким вопросом: что будет, когда кенийский крестьянин, у которого есть телефон Nokia 1000 с возможностью передачи СМС, вдруг обнаружит, что этот телефон имеет блумберг-терминал[54], терминал по выдаче кредитов, терминал для денежных переводов Western Union и даже банк? Не банковский терминал, а банк – прямо в этом телефоне? И что будет, когда всё это станет доступно шести миллиардам людей во всем мире?

Одна из причин, по которым Биткойн не удастся остановить, – наличие насущной необходимости в этой технологии. Банки в развивающихся странах не могут охватить своими услугами все слои населения. Я недавно беседовал с одним банкиром, который рассказал мне следующее: «Половина населения в наших краях проживает в 1660 километрах от ближайшего филиала, причем добраться туда можно только по реке на каноэ. У нас нет возможности их обслуживать». Но даже в самой далекой деревне бассейна Амазонки стоит вышка сотовой связи, и у кого-нибудь в этой деревне обязательно имеется солнечная батарея и телефон Nokia 1000 с функцией передачи текстовых сообщений. Таких телефонов Nokia в мире существует больше, чем каких-либо других электронных устройств. Это самая массовая модель за всю историю промышленного производства на планете. Практически пять миллиардов человек на Земле обладают доступом к мобильному телефону. Почти три миллиарда человек обладают доступом к мобильной связи, хотя у них нет доступа к источникам чистой питьевой воды. Задумайтесь об этом. На нашей планете сотовые телефоны распространены шире, чем питьевая вода! Так что будет, когда каждый сможет стать банкиром? Для меня перспектива Биткойна не в том, чтобы включить в банковскую систему эти оставшиеся шесть миллиардов, а в том, чтобы освободить от банков всех людей. И мы справимся! Банковские услуги – это просто приложение.

«Для меня перспектива Биткойна не в том, чтобы включить в банковскую систему эти оставшиеся шесть миллиардов, а в том, чтобы освободить от банков всех людей».

Инновации, навсегда меняющие прежний мир

Это лишь начало. Самое интересное в Биткойне происходит в области «внедренных инноваций», то есть когда изобретения встраиваются в такие ниши, куда существующим системам входа нет. Технологии обладают довольно интересным эффектом: им свойственно внезапно менять базовые предпосылки. Некоторые из наиболее важных вещей, случившихся в интернете, произошли не благодаря его возможностям по установлению соединений, а благодаря крайне низкой стоимости передачи информации на расстояние. До появления интернета передача информации из точки А в точку Б стоила дорого. Интернет понизил эту стоимость практически до нуля. В результате миллионы приложений, которые не могли появиться в прежней ситуации из-за высокой стоимости этих услуг (пусть даже мы и хотели их придумать), вдруг стало возможным реализовать. Зачем слушать музыку в режиме реального времени вместо того, чтобы покупать ее и хранить на компьютере? А затем, что это ничего не стоит! И как только это уже ничего не стоит и музыку можно слушать в потоковом аудио, вы внезапно понимаете, что ценность владения музыкальной коллекцией была вами несколько преувеличена. А если это понимание продлится целое поколение, то в итоге и права интеллектуальной собственности будут подвергнуты переоценке. И прощай, музыкальная индустрия! Такие эффекты наблюдаются, поскольку технология меняет фундаментальную стоимость выполнения действий.
Задумаемся о том, что будет, когда Биткойн изменит фундаментальную стоимость транзакции на большом расстоянии, с передачей ценности, с записью информации. Что будет, когда впервые появится система, которая сможет следить за выполнением правил без человеческого вмешательства и при этом пользоваться доверием без необходимости доверять какому-либо человеку? В Биткойне такая ситуация называется устранением рисков посредника. Если я создаю транзакцию и подписываю ее, то любой участник сети Биткойн может проверить корректность данной транзакции совершенно автономно – это всего 350 байт – и убедиться в ее корректности, никого не спрашивая. Это уже система с самопроверкой – система правил, существующая независимо от человеческого фактора на базе топологии этой сети.

«Что будет, когда впервые появится система, которая сможет следить за выполнением правил без человеческого вмешательства и при этом пользоваться доверием без необходимости доверять какому-либо человеку?»

Что это означает для коммерции и банковских услуг? Мы можем понять, что в ближайшее десятилетие Western Union полетит под откос. Если вы берете 30 процентов комиссии с беднейших в мире людей, то вы заслужили, чтобы прорывная технология вас уничтожила. В прошлом году руководитель Western

Union заявил: «В среднесрочной перспективе Биткойн нас не беспокоит». Я хочу записать это и повесить в рамке у себя на стене! Это одна из
тех самых
фраз; в том же духе говорили руководители Kodak, когда Nokia вытесняла их с рынка. Компания Kodak была крупнейшим производителем фотокамер в мире, пока не появилась компания, которая прежде камерами вообще не занималась; новая компания за год продала миллиард камер и разрушила индустрию Kodak. А они и не подозревали, что так может случиться. И то же самое ожидает Western Union. Ну а Nokia, между прочим, на сегодня крупнейший производитель фотокамер.

Всё очень просто. Что будет, когда у вас появится возможность проверять выполнение правил без участия третьей стороны? Такое положение дел изменит несколько существующих ныне фундаментальных социальных институтов. Это изменит так называемый «коэффициент Коуза», который выражает накладные расходы организации. Например, два человека могут сделать больше, чем один. Трое могут добиться еще большего. Но существует предел. Как только команда становится слишком крупной, накладные расходы делаются выше незначительного прироста производительности. А Биткойн это меняет. Сегодня можно привлекать примерно миллион людей, примерно пять тысяч компьютеров, чтобы достигать согласия по вопросу состояния реестра каждые десять минут, практически за копейки. Раньше такого никогда не было. Это открывает дверь возможностям, о которых прежде никто и не помышлял. Биткойн радикально уходит от прошлого.
Приведу один простой пример: понятие «идентификация». Идентификация отдельного лица – необходимое условие для работы с финансами. Чтобы владеть деньгами, контролировать средства, иметь банковский счет, чтобы получать счета, чтобы заплатить, – необходимо быть идентифицируемым лицом. Вез де в мире, в любой существующей платежной и финансовой сети, деньгами владеют лица. Лица могут быть физическими или юридическими, например, корпорацией, – но юридическое лицо сводится к группе физических лиц. Лица могут использовать заместителей, агентов и прочее, но в конечном счете это просто люди, которые работают вместе. Для Биткойна лицо не требуется. Деньгами может владеть программа-агент. Программа может в автономном режиме контролировать деньги без какого-либо вмешательства со стороны человека. В истории человечества это неслыханное дело! Мы еще не знаем, как будет развиваться эта ситуация дальше.
Давайте проведем мысленный эксперимент: возьмем три радикальные прорывные технологии и соединим их вместе. Биткойн, такси Uber и беспилотные автомобили. Что будет, когда эти три технологии соединятся? Получится автономный и принадлежащий самому себе автомобиль. Эта машина станет сама осуществлять платежи за лизинг (к примеру, компании Toyota), оплачивать страховку и бензин, зарабатывая извозом людей. Владельцем такой машины не окажется какая-либо организация. Эта машина будет сама себе организацией. Машина, являющаяся акционером и собственником своего юридического лица. Такого раньше никогда не было, и это лишь начало.
(Из зала доносится: «Вот это да!»)

«Возьмем три прорывные технологии и соединим их вместе. Биткойн, Uber и беспилотные автомобили. Что будет, когда эти три технологии соединятся? Получится принадлежащий самому себе автомобиль».

Я могу поручиться, что одной из первых автономных организаций станет полностью автономный компьютерный вирус-вымогатель на базе искусственного интеллекта, который будет вымогать у людей биткойны и использовать эти деньги для саморазвития, оплачивая услуги по программированию, услуги хостинга и услуги по распространению в сети. Вот так выглядит одна из перспектив. Другой будущей перспективой является цифровая автономная благотворительность. Представьте себе систему, которая собирает пожертвования у людей и с помощью этих пожертвований осуществляет мониторинг социальных сетей Twitter или Facebook. По достижении определенного порогового значения – если, например, 100 000 человек приняли участие в обсуждении природной катастрофы вроде тайфуна на Филиппинах – система производит распределение пожертвований и автоматически перечисляет средства в фонд помощи жертвам данной катастрофы, без участия какого-либо совета директоров или акционеров. Сто процентов пожертвований передаются непосредственно на благотворительность. Любой может проверить правила, по которым работает данная автономная благотворительная организация. Мы сейчас приближаемся к тому, чего никогда не было раньше. Это не просто новая валюта.
Теперь давайте посмотрим, как биткойн-сообщество с помощью своего выбора в проектировании и выбора метафор использует этот неслыханный потенциал. Да-а-а, ну и неразбериха!

Использование банкомата

Рассмотрим простой пример. Скольким из вас довелось пользоваться банкоматом Биткойна – так называемым биткойноматом[55]? И как вам опыт? Понравилось? Что, вообще никому? Ну да, всё правильно… Что такое банкомат? Этому изобретению уже 25 лет. Какую задачу решает банкомат, зачем его придумали?
(Из зала доносится: «Для выдачи наличных».)
Верно. Когда вы, как физическое лицо, взаимодействуете с банкоматом, у вас уже должны быть сложившиеся отношения с банком или финансовым учреждением, существовать счет, а вашей задачей является получение наличных. Двадцати секунд для этого слишком много. Три нажатия на кнопки – тоже много. За последние 25 лет самой радикальной инновацией в банкоматах стала функция «ускоренное получение наличных» (Fast Cash). Именно так! Но там мало что изменилось. Вы нажимаете кнопку – и получаете наличные после одного нажатия! Вот это да! Всего 15 секунд от начала и до завершения работы. Почему это так важно? Потому что банкоматы в первую очередь необходимы в ситуации, когда в час дня в центре города у нескольких банкоматов скапливаются очереди по 100 человек; каждому в очереди нужно взять 20 долларов на обед. И так во всем мире.

Так каково же назначение этого устройства? Для банка назначение банкомата – снижение накладных расходов по содержанию персонала и снижение до минимально возможной величины количества времени на взаимодействие с теми, кто уже является клиентом банка. И что же тут общего с банкоматом Биткойна? Да абсолютно ничего общего!

Использование банкомата для биткойнов

А теперь рассмотрим использование банкомата для биткойнов. Обычными пользователями банкомата для биткойнов являются те, кто никогда раньше биткойнов не видел. Как правило, такие люди не понимают, что это такое; не обладают кошельком, поскольку не знают, что он им нужен, и совершенно точно не знают, что на самом деле это не кошелек, а брелок с ключами. Люди подходят к биткойномату (инженеры создали дизайн, который напоминает обычный банкомат, даже несмотря на то, что он не имеет ничего общего с работой обычного банкомата), который должен выдать биткойны после минимального количества нажатий на кнопки с минимальным взаимодействием, но ничего подобного не происходит. Я имею в виду, что машина на вас просто набрасывается, и вы к этому не готовы! «Пожалуйста, откройте ваш телефон и продемонстрируйте полученный QR-код». И вы думаете: «Что? Какой еще QR-код?.. Так, минуточку, надо зайти на Google Play и поискать „QR-код“. Ага, есть приложение, которое эти коды сканирует… Наверное, надо вот это поставить. Или не ставить? Может, поставить биткойн-кошелек? Ого, да их тут 26 штук! И какой лучше? Неизвестно. Ладно, скачаем Circle… Н-да, для него нужно уже быть пользователем сети. Ладно, поставим Coinbase… И тут надо тоже быть пользователем сети…»
В конце концов я установил кошелек, показал QR-код, положил в него деньги – и мне выдали биткойны. А что с ними теперь делать? У меня сплошь вопросы: кто их принимает, где их можно потратить? Ничего не ясно. А почему? Потому что эта дьявольская машина ничего мне не рассказала! Она просто бросила мне биткойны и через 15 секунд занялась следующим клиентом.
Вот если бы я разрабатывал банкомат для биткойна, я бы в первую очередь поставил все машины в небольших магазинчиках в кварталах, где живут эмигранты из Мексики. Второе: в интерфейсе не было бы ни слова по-английски; весь интерфейс был бы на испанском, потому что я продвигал бы новую модель денежных переводов. Третье: первейшей функцией этого банкомата стала бы функция «Отправить деньги в Мексику». Вот так! Потому что я хочу, чтобы люди использовали биткойны в обычной жизни. Четвертое: на передней панели я бы установил большую кнопку «Поговорить с человеком». Берем устройство с выходом в интернет, подключаем веб-камеру и планшет для ввода… но нет, я не собираюсь устраивать видеоподдержку пользователей, что вы! «Что это еще за биткойн? Как его можно потратить?» Ответ: «Добрый день! Я вижу, что вы сейчас в магазине на 25-й авеню. Вблизи есть целых три магазина,

где принимают биткойны. Я вам сейчас поставлю небольшой видеоролик. Соберите всех детей в магазине, попляшем – для них сейчас прозвучит веселая песенка про Биткойн. А теперь посмотрите еще одно видео». Я не хочу взаимодействовать 15 секунд! Я хочу, чтобы взаимодействие длилось пару часов и чтобы все мои друзья сидели перед банкоматом Биткойна, смотрели видеоролики про Биткойн и узнавали, что это такое. Всё должно быть ярким, и пусть будет информация, где биткойны можно потратить. Должны быть советы по выбору кошелька, они могут приходить мне прямо на электронную почту. Вот так завоевывается лояльность, так формируется бренд и позитивный опыт использования. Это не 15-секундное взаимодействие! Для многих людей именно этот опыт станет первым знакомством с Биткойном. И у вас есть возможность превратить его в глубокий, важный и просвещающий опыт. Но никто этим не пользуется.

Дети пользуются Биткойном

Вот еще одна подсказка: использование Биткойна детьми. В среднем по миру самый ранний возраст, когда можно открыть банковский счет, – это 16 лет. И мне бы хотелось, чтобы к тому времени, как 16-летний подросток отправится в банк, у него уже был бы как минимум шестилетний опыт активного использования Биткойна. В таком случае, когда человек первые столкнется с традиционными банковскими услугами, он скажет: «От трех до пяти дней?! Рабочих дней?! Каких еще рабочих дней? И работаете вы только до 17:00 – серьезно, что ли? Да я в 17:00 только со своей работы ухожу! А что вот это значит – я вам должен платить за хранение моих денег, что ли? Это же смешно. Вы что, никогда тут про Биткойн не слыхали?!»

«Для многих молодых людей Биткойн станет первым опытом в экономике. К тому моменту, когда они придут в банк, они уже заранее с этими банками покончат».

Вот какой опыт мне бы хотелось иметь. Десятилетние дети открывают аккаунты в Биткойне. И знаете почему? Они могут загрузить приложение из интернета и впервые в жизни контролировать свои средства. Так что вам нужно будет не только поговорить про «тычинки и пестики», но и провести беседу о «секретных ключах». Тут пролегает широкая пропасть, разделяющая поколения. Для многих молодых людей Биткойн станет первым финансовым опытом. К тому моменту, когда они придут в банк, они уже заранее с этими банками покончат. И это огромное преимущество.

Новая технология, старая терминология

Итак, чем же можно заинтересовать новое поколение? Один из ключевых моментов – не пытайтесь создать нечто родственное традиционным банковским услугам. Всё это лишь испортит отношение новых пользователей. Нужно, чтобы они получили совершенно особый опыт в Биткойне, который не будет походить на любые банковские услуги. Вы ведь не хотите, чтобы ваши сервисы напоминали традиционный расчетный счет? Забудьте вообще слово «расчетный». Откройте любую из существующих обменных площадок, например Circle или Coinbase. Как называется ваш аккаунт в Coinbase? Это «расчетный счет», у него есть баланс, и в нем можно посмотреть «выписку». Кого, интересно, они наняли, чтобы сварганить такой дизайн? Что означает слово «расчетный»? Оно означает, что для этого счета вы можете выписать чек. Я, конечно, понимаю, что мы у себя в Америке лет на двадцать пять отстали от современных финансовых технологий. Весь остальной мир не пользуется чеками, это я вам точно говорю. Что такое чек? Чек – это такая штука, с помощью которой ваша бабушка может заставить застонать одновременно двадцать человек, стоящих за ней в очереди в супермаркете. Я лично пользуюсь чеками каждый месяц, чтобы платить за квартиру, и сам не знаю зачем. Просто никак иначе я заплатить за квартиру не могу. Это же безумие: в 2015 году я расписываюсь на бумажке и отправляю ее по почте в конверте. Чтобы потом мой квартирный хозяин сходил в банк и предъявил там этот чек. И по нему в срок от трех до пяти рабочих дней он сможет получить деньги – после того, как заплатит банку комиссию в пять долларов из собственных денег!

Чтобы Биткойн выиграл у банков, не надо никакой агрессивной рекламы. Всё, что требуется от Биткойна, – дать человеку недельку попользоваться Биткойном, а об остальном позаботятся сами банки. Они будут замораживать счета, они будут рассказывать, что сегодня праздник и они не работают, они будут обрабатывать транзакции от трех до пяти рабочих дней. Сами же банки продвигают Биткойн! И всякий раз, когда они работают как обычно, они продвигают его всё дальше.

Прелести международных денежных переводов

Меня недавно пригласили выступить в центральном банке Германии – «Бундесбанке». За выступление мне должны были заплатить, но как это сделать с помощью Биткойна, они не знали, и это стало серьезной проблемой – потому что гонорары я обычно принимаю в биткойнах. И мы договорились о международном банковском переводе. Это заняло 16 дней! Сначала они спросили у меня номер моего счета. На следующий день сказали, что им нужен номер в системе SWIFT. Но к этому моменту мой банк был уже закрыт, и номер SWIFT я узнать уже не мог. На следующее утро я узнал номер SWIFT и отправил его немцам. Но к тому моменту в свою очередь закрылся их банк. На следующее утро они ввели номер SWIFT и обнаружили, что это не тот номер SWIFT: мне дали номер для долларов США, а надо было номер для иностранной валюты. Так что они отправили мне электронное письмо, но, когда я его получил, мой банк был уже закрыт. На следующий день я узнал другой номер SWIFT и отправил его немцам, но к тому моменту их банк закрылся опять. И вот они отправили мне перевод. В моем банке посмотрели на перевод и сказали: «„Бундесбанк“? Никогда о таком не слышали. Как-то не внушает доверия. Давайте-ка заморозим транзакцию на 14 дней, мало ли что, вдруг будет отказ в оплате». А это, на минуточку, третий по величине в мире центральный банк, немецкий государственный банк! Как они могут не оплачивать чеки? Через 14 дней – внимание, сейчас будет кульминация! – в моем банке было сказано: «Деньги заблокированы. Деньги разблокированы». И выдали 80 долларов из всей суммы, которая была четырехзначной. Восемьдесят долларов. Почему восемьдесят? Что за чертовщина? Что мне делать? Они просто блокировали всю сумму. Просто глупость какая-то!

Проблема поиска метафор для традиционного банкинга

А вот что требует повышенного внимания в Биткойне. Подумайте: когда на рынок выводится новый продукт, то какие детали архитектурных метафор прошлого этапа следует использовать дизайнеру в новом продукте? Если посмотреть на архитектуру Биткойна, получается, что она спроектирована для того, чтобы убедить людей, будто это полный аналог обычного банка. Но привычных функций традиционного банка в новом продукте нет: отсутствует простая возможность отмены транзакции, нельзя получить компенсацию, если вы скомпрометировали ваш секретный ключ. Ничего этого нет! Хотя отсутствуют и неприятные стороны традиционного банка, но на этом внимание можно не заострять. В итоге пользователей вводят в заблуждение.

Инновации, дизайн и принятие

Биткойн отчаянно нуждается в понятной пользовательской архитектуре. Но у меня есть надежда, что всё изменится, поскольку так уже было раньше. Я в интернете с 1989 года, и в те времена не существовало никакой интернет-торговли. Интернетом владела организация «Национальный научный фонд» (National Science Foundation), сеть была предназначена только для академической среды (ну и для 15-летних подростков, которым удалось разжиться паролем к этой академической системе). В то время система DNS лишь начинала развиваться. Большинству систем еще не были присвоены имена DNS. Сеть была плохо структурирована. Самые интересные вещи удавалось найти, только зная точный IP-адрес ресурса. Я ходил

со списком IP-адресов в записной книжке, чтобы иметь доступ ко всем этим ресурсам. А чтобы их использовать, надо было обладать навыками работы с командной строкой UNIX.
Моя мама всем этим воспользоваться никак не могла. Однажды она позвала меня и сказала, что по неизвестной причине сломался проигрыватель. «Он показывает сообщение об ошибке! Мигает и показывает „0:00“». Мне понадобилось несколько минут, чтобы понять, что она случайно выключила проигрыватель, а после повторного включения требовалось заново установить время на часах. Я бы очень хотел поговорить с ней об интернете, но для этого ей надо было научиться им пользоваться, но такого, казалось, не случится никогда. С того дня, как я отправил свое первое электронное письмо, и до момента, когда моя мама наконец сумела отправить свое первое письмо по электронной почте, прошло двадцать лет. А чтобы это случилось, необходимо, чтобы произошло множество вещей. Самое важное – должен был появиться iPad. Ей удалось отправить письмо, просто проведя пальцем по экрану, и лишь это сделало возможным для нее использование данного сервиса. В 1989 году не было вообще никаких условий для того, чтобы интернетом могли пользоваться большинство обычных людей.

Пользовательские интерфейсы и общество

Существует просто отличный видеоролик, снятый в 1994 году «за кулисами» утреннего телешоу: куча журналистов готовятся к эфиру. Они обсуждают интернет и уточняют друг у друга информацию. Один спрашивает коллег: «Слушайте, так интернет – это та самая штука со значком @?» Ему отвечают: «Нет-нет, это ты про электронную почту. А интернет – это штука с „www“, там еще точки и слэши». Он: «А это точно не электронная почта?» Ему: «Да нет, это интернет». – «А может, это всё-таки „веб“?» И так далее по кругу. Система, разработанная инженерами… Непостижимая система! Но произошли две вещи. Первая: технологию удалось сильно упростить для понимания, она улучшилась, стала более гладкой. И второе: общество изменилось. Сегодня самый обычный человек точно знает разницу между сервисами со значком @ и с буквами «www», пусть это и пример ужасного дизайна. Общество выучило язык интернета, потому что сеть обрела ценность, оправдывающую изучение этого языка.

«Общество выучило язык интернета, потому что сеть обрела ценность, оправдывающую изучение этого языка».

И пока интернет становился проще, общество тоже развивалось и сумело разобраться в по-настоящему непостижимых частях интернет-технологий. То же самое происходит и с Биткойном. Выступая на конференциях для неспециалистов, которые никогда прежде о нем не слышали, я обычно говорю так: «Послушайте! Вам не о чем беспокоиться. Ваши дети обязательно всё вам объяснят про Биткойн. Как только наведут порядок у себя в комнатах, зовите их к себе и просите рассказать про него». Их дети, которым сейчас по десять лет, всё это поймут. Я лично знаком с детьми, которые пользуются веб-интерфейсами для создания собственных криптовалют.
Вот один из самых интересных вопросов, которые мне задают: «Сколько будет создано криптовалют?» Ответ на него представляет собой точный эквивалент ответа на вопрос, сколько в интернете блогеров. Да все мы! Все, кто есть в интернете. Криптовалют будет не сотня – появятся тысячи, десятки тысяч криптовалют. Когда шестилетний ребенок создает криптовалюту Джо-койн для того, чтобы запустить ее как критерий оценки популярности среди одноклассников, тот факт, что эта валюта также является глобальной, исключающей возможность подделки, масштабируемой и может использоваться по всему миру, Джо особо не волнует – его волнует лишь одно: нравится ли его друзьям пользоваться Джо-койном? К сожалению, тут на сцену выходит конкурент – Мэри-койн, и начинается старомодная война валют. Всё это будет. Доказательством служит тот факт, что дети в играх сами придумывают свою валюту. Посмотрите на детей в детском саду – у них есть своя валюта: резинки для волос, карточки с покемонами, кубики… Они начинают копить, торговать, менять предметы на знаки внимания, а затем могут даже устроить драку из-за своей воображаемой валюты. Это обычный человеческий опыт.
Мы только что придумали лучшую валюту в мире. Ваша задача – создать верные метафоры, чтобы она заработала для всех остальных людей.
Спасибо за внимание!

Деньги как один из видов контента

Южная конференция по Биткойну; Куинстаун, Новая Зеландия; ноябрь 2014 года

Всем доброго утра! Сегодня я хочу поговорить на новую тему, над которой сейчас работаю: давайте побеседуем о деньгах как об одном из видов контента. С появлением Биткойна произошла фундаментальная трансформация подхода к деньгам в перспективе будущего. Деньги стали абсолютно независимы от базовой среды их передачи и превратились в отдельный вид контента.
Что я хочу этим сказать? Транзакция в биткойн-сети – это подписанный структурированный фрагмент данных, который может быть выполнен где угодно. Многие думают, что такая транзакция должна передаваться исключительно в сети Биткойн. Это не так. Транзакция Биткойна должна достичь майнера и быть включена в блок, но передавать ее в сети Биткойн необязательно. Данная сеть не обладает какими-либо особенностями. Она всего лишь перенаправляет транзакции и формирует блоки. Сама транзакция может быть передана в среде любого типа.
Технология Биткойн обладает волшебным свойством: транзакция не включает никаких защитных механизмов. Безопасность достигается благодаря алгоритму «доказательство выполнения работы» (PoW), которое обеспечивается майнерами, а цифровая подпись в транзакции добавляется только конечными пользователями, которые сами у себя хранят ключи. В транзакции Биткойн нет уязвимых или секретных элементов. Сейчас я поясню это подробнее.

Пластиковые карты небезопасны

Сегодня, когда я обращаюсь в торговую точку с расчетным терминалом и предъявляю свою пластиковую карту, я передаю продавцу (через длинную цепочку посредников) номер карты, срок ее действия и код безопасности CCV2, указанный на оборотной стороне карты. Фактически я передаю секретные ключи. Я передаю коды доступа к моему счету. Это конфиденциальная информация. Если она будет перехвачена, мой счет окажется в опасности. С него могут неоднократно запрашиваться средства, это может сделать как продавец, так и один из посредников, а также любой хакер, который сумеет украсть информацию через разных посредников. Данные моей пластиковой карты необходимо очень тщательно охранять.
С момента, когда я достал карточку из кармана, и до момента, когда деньги поступят на счет продавца, информация фактически передается по сети через виртуальные «инкассаторские машины». Шифрование начинается с кассового терминала продавца, затем информация о транзакции в зашифрованном виде поступает в систему Visa для пакетной обработки. От системы Visa, опять в зашифрованном виде, информация поступает в банк-инициатор данной транзакции и в банк-получатель, вся информация шифруется на каждом этапе прохождения, поскольку везде передаются секретные ключи. Если шифрование на любом этапе будет взломано, то моя карта окажется в опасности.
Данные карты также хранятся во многих транзитных базах, для истории. Это просто ужасная идея, поскольку создаются централизованные секретные тайники, которые атакуют хакеры. О них мы уже не раз слышали. Достаточно вспомнить, как в США у крупных ритейлеров Target и Home Depot в результате кражи данных были скомпрометированы 50–60 миллионов карт. У фирмы JPMorgan Chase недавно были скомпрометированы 75 миллионов счетов! Всё это произошло не потому, что эти компании не выполнили своих обязательств по защите данных карт клиентов.

«На сегодняшний день все компании можно разделить на два типа: те, которым не удалось предпринять адекватных мер для безопасности кредитных карт, и те, которым в ближайшем будущем не удастся обеспечить необходимые меры безопасности».

На сегодняшний день все компании можно разделить на два типа: те, которым не удалось предпринять адекватных мер для безопасности кредитных карт, и те, которым в ближайшем будущем не удастся обеспечить необходимые меры безопасности. Либо вас уже «хакнули», либо вас скоро «хакнут», – есть лишь две категории. Никто не обладает иммунитетом. Никто не может изобрести способ защиты миллионов секретных кодов доступа от заинтересованных в наживе хакеров. Это просто невозможно. Никто не знает, как это сделать. В информационной безопасности нет метода, который сможет защитить от всех возможных видов и типов атак. Сама технология расчетов по пластиковым картам содержит в себе конструктивную брешь, так как сам токен является секретным ключом. И если вы передаете этот токен, то вы подвергаете риску весь счет, к которому он относится.

Транзакции в Биткойне: безопасность на основе архитектуры

Биткойн отличается от всего, что было ранее. Когда я совершаю транзакцию в этой сети, то передаю не ключ, а лишь простое подписанное сообщение. Это сообщение – авторизация. Авторизация содержит два внешних идентификатора: 1) откуда направляются деньги – этот параметр ссылается на непотраченный баланс в блокчейне; 2) куда направляются деньги – этот идентификатор формируется созданием нового обязательства, или ограничения с назначением того, кто может потратить деньги (обычно это публичный ключ или адрес в сети). В данной записи транзакции нет никаких конфиденциальных, персональных данных. Если информация из транзакции будет украдена, то всё, что можно узнать, – это адрес, с которого ушли деньги; адрес, на который идут деньги; сколько денег было переведено. Вот и всё. Подпись ничего вам не скажет. Адреса вам тоже ничего не сообщат. Какие-либо идентификаторы отсутствуют. Можно взять и распечатать транзакцию. Можно разместить ее на форуме. Можно нарисовать на асфальте. Биткойн-транзакцию можно передавать по незащищенному каналу связи, через Wi-Fi. С помощью пожарного датчика, световыми сигналами, голубиной почтой, – это не имеет ни малейшего значения. Никакая информация из данного сообщения не может быть скомпрометирована.

«Биткойн-транзакцию можно передавать по незащищенному каналу связи, через Wi-Fi. С помощью пожарного датчика, световыми сигналами, голубиной почтой, – это не имеет ни малейшего значения. Никакая информация из данного сообщения не может быть скомпрометирована».

Деньги как вид контента

Большинство людей не понимают, что означает превращение денег в один из видов контента. Мы взяли транзакцию, размер которой всего 250 байт, и отделили ее от среды передачи, чтобы она не зависела от степени защищенности этой среды[56]. Мы сделали так, что транзакция стала автономной, чтобы она могла быть проверена любым узлом сети, обладающим полной копией блокчейна. Проверена независимым образом на предмет возможности расхода указанной суммы, на подлинность записи и на действительность подписи в любой системе, обладающей полной копией блокчейна, – и даже в системе, которая обладает лишь частичной его копией. Проверка транзакции занимает секунды. Всё, что нужно сделать, – доставить ее к одному из узлов распределенной сети, который имеет канал взаимодействия с майнерами. Вот и всё. Как только транзакция попала в сеть Биткойн и начала распространяться, можно быть уверенным, что эта транзакция по прошествии какого-то времени будет включена в блокчейн и станет действительной. То есть, взглянув на любую транзакцию, я могу вычислить, достаточное ли она обещает вознаграждение, и сделать некоторые предположения о том, насколько быстро майнеры ее обработают, поскольку я знаю правила работы системы с алгоритмом консенсуса. И можно быть уверенным в том, что, как только транзакция получила достаточное распространение, она обязательно появится в каком-нибудь блоке поблизости от вас, причем довольно скоро.

Невозможно остановить транзакции в биткойн-сети

В биткойн-транзакции нет никакого волшебства. Давайте ненадолго над этим задумаемся. Как можно закодировать 250 байт и передать их по сети? Меня недавно об этом спросили – и я уже не в первый раз слышу подобный вопрос: «Разве правительственная диктатура не может блокировать или запретить передачу транзакций в Биткойне?» Ответ здесь один: нет, – но мне кажется, что почти никто не понимает, почему нет. Я приведу пару теоретических примеров, чтобы вы меня лучше поняли.

Передача биткойн-транзакций с помощью смайликов в Skype

Мой первый смешной пример кодирования биткойн-транзакции – это анимированные смайлы или просто символы эмоций (смайлики) в программе Skype. Skype имеет набор из 128 символов, которые вы можете отправить собеседнику: нахмуренные или смеющиеся лица, жесты одобрения и неприятия, изображение солнечной погоды, сердечек и праздничных тортиков. А теперь взгляните на всё это с точки зрения информационного содержания. Это же набор символов, верно? И специалист в области информатики сразу же скажет: можно сделать схему кодирования. Она позволит отправлять транзакцию размером 250 байт в виде сообщения длиной примерно 500 символов, то есть 500 смайликов. Таким образом получится биткойн-транзакция из смайликов.
С помощью простой математики я могу написать небольшой скрипт – это примерно пара строк кода на языке Python. У хорошего программиста выйдет всего одна строчка. Не нужно никаких библиотек. В этом скрипте я буду брать шестнадцатеричное представление биткойн-транзакции и кодировать его смайлами. Затем всё это я могу скопировать в диалоговое окно Skype, находясь в любой точке мира. И как только принимающая сторона получит эту строку смайликов, она скопирует ее в скрипт декодирования, запустит результат в Биткойн – и транзакция будет выполнена. Получателем может быть робот, или автоматически сканирующая станция, которая предназначена для декодирования последовательности смайликов в транзакции с передачей их в биткойн-сеть.
А теперь скажите мне, как это можно остановить? Ну, разве только заблокировав по всему миру Skype. А если будет заблокирован Skype, я воспользуюсь Facebook. Если заблокируют Facebook, я использую Craigslist[57]. Если заблокируют Craigslist, я отправлю транзакцию через TripAdvisor. Если закроют и его, то я размещу транзакцию в качестве комментария в статье на Wikipedia. Если и ее закроют, то я размещу транзакцию в качестве фона в файле JPEG с моими фотографиями из отпуска.

«Деньги сегодня – это ничем и ни с чем не связанный информационный контент».

Деньги сегодня – это ничем и ни с чем не связанный информационный контент. При имеющемся изобилии полностью взаимосвязанных мультимедийных механизмов коммуникации совершенно невозможно воспрепятствовать передаче информации откуда угодно и куда угодно.

Передача транзакций через коротковолновый радиоприемник

Но допустим, что у нас нет интернета. Я могу предложить еще более смешную и безумную схему: биткойн-транзакции мы будем передавать с помощью радиоприемника, со скачкообразным изменением частоты и в режиме импульсной передачи. Это на случай, если придется «уйти в партизаны».
Во время Второй мировой войны самолеты союзников сбрасывали на территорию оккупированной Франции тысячи коротковолновых радиоприемников, чтобы находившиеся на земле партизаны могли их подбирать и прятать в амбарах, в заброшенных зданиях, под мостами, а затем пользоваться ими для связи с союзниками по всей Европе, прямо под носом у оккупационных фашистских войск. Одним из преимуществ коротковолновой радиосвязи является огромный диапазон. В те времена радиоприемник использовался для передачи кодовых сообщений с помощью азбуки Морзе или для передачи коротких шифровок.

Сегодня я могу подключить простейший коротковолновый передатчик к ноутбуку через USB-порт. Всё, что мне для этого нужно, – антенна. Для коротких волн нужна антенна из достаточно длинного куска металла: это может быть железнодорожный рельс, металлическая перекладина, разбитая линия электропередачи, сетка ограждения или забор из колючей проволоки. Как я заметил, тут у вас в Новой Зеландии этого добра навалом. Везде, где пасутся ваши любимые пушистые овечки, расположены загоны. Так что для выполнения транзакции мы подключаем ноутбук, присоединяем его к столбу какой-нибудь изгороди, нажимаем Enter на клавиатуре и передаем в течение 25 секунд в импульсном режиме информацию о транзакции. И пока в радиусе полутора тысяч километров будет находиться какая-нибудь приемная станция, подключенная к Биткойну, вы можете провести транзакцию в сети. Представим, что я партизан и хочу что-то купить: я просто сформирую транзакцию офлайн, а когда всё будет готово, выбегу на спортивную площадку, подключу передатчик к перекладине проволокой, передам сообщение за 25 секунд и скроюсь вместе со всем своим оборудованием. Как можно этому воспрепятствовать? Ответ очень прост – никак! И это лишь начало.

Разделяем средства коммуникации и информацию

Как только наступает понимание, что деньги превратились в контент, а транзакции больше не связаны со средством их передачи, возникают довольно важные дополнительные характеристики. Однажды кто-то из знаменитых людей[58] произнес: «Средство коммуникации – это и есть сообщение [информация]». Главные доводы в пользу такого утверждения – это ограничения, а во многих случаях – искажение информации, которая передается через различные средства коммуникации.

Если ваше средство коммуникации – телевидение, то информация будет длиться около 18 минут, а затем прервется рекламным блоком. Информацию распространяют в соответствии с форматом медиа. Вы начинаете наделять информацию ценностью, исходя из неверного предположения о том, что эта ценность эквивалентна стоимости производства. Например, в сфере телевидения нужно понести определенные затраты на производство телешоу. Люди, работающие в этом бизнесе, ошибочно думают, что стоимость создания телевизионного контента равняется его ценности, то есть чем больше вы тратите на производство, тем ценнее результат.

Можете себе представить, какой они испытывают ужас, когда появляется что-то вроде YouTube и стоимость производства падает до нуля? О чем сразу же начинают думать те, кто работает на телевидении? Если затраты нулевые, то и контент тоже ничего не стоит. Вот вам фундаментальное непонимание того, что происходит, когда вы отделяете контент от формы медиа. При разделении средств коммуникации и информации ваше восприятие ценности перемещается со стоимости производства на ценность самой информации, которой оно обладает для его конечного потребителя.

Приведу один пример из истории. Когда стоимость печати астрономическая, а печатный станок доступен лишь немногим избранным, единственное, что печатается, – это библии Гуттенберга. Средство коммуникации очерчивает круг приемлемой информации и ограничивает его только самым важным для общества.

Интересно, что бы сказал Гуттенберг о Twitter, в котором стоимость производства информации нулевая? Мы прошли путь от печатных библий Гуттенберга до ответов на сообщение в Twitter короткими аббревиатурами, у меня даже есть любимая – это «SMH» (от
англ.
shaking my head), в онлайн-переписке означает «качаю головой в изумлении». Когда какой-нибудь «Профессор Биткорн» заявляет: «Котировка биткойна стремится к нулю», – я могу выразить весь диапазон своих мыслей символом, обозначающим «лицо, закрытое одной рукой», который в онлайн-переписке выражает безнадежность диалога. Если взглянуть на такой способ выражения объективно, то такая информация не имеет никакой ценности. Если сделать неверное предположение о том, что при нулевой цене производства и ценность получаемой информации минимальна, то тогда не имеют ценности и все медиа вместе с информацией: такая комбинация должна порождать пустоту и банальность; именно эту ошибку люди всегда совершают в моменты, когда история выходит на новый этап своего развития.

Когда впервые появился Twitter, люди решили, что его можно использовать только для пустяков. Но год назад я смотрел зарубежные новости по каналу CNN о революции в Египте; по телевидению передавали сообщения, которые египетские революционеры писали в Twitter с улиц Каира: участники событий рассказывали о том, что происходит в реальном времени. А журналисты CNN ничего не делали. Они тыкали пальцем в экран и приговаривали: «Смотрите, у нас новое сообщение». Их роль свелась к роли красотки из телешоу, которая произносит: «И этот чудесный холодильник станет вашим, если вы угадаете, что за приз спрятан за дверью номер один!» Мне доставило массу удовольствия наблюдение за тем, как одна из этих «говорящих голов» по имени Андерсон Купер сделалась всего лишь диктором, озвучивающим сообщения из Twitter на экране.

Потому что именно телевидение раньше насмехалось над Twitter. Журналисты и работники массовых коммуникаций заблуждались, считая, что если стоимость производства нулевая, то и ценность сообщения тоже равна нулю. Они ошибочно смешали понятия «средство коммуникации» и «средство информации» – и предположили, что контроль над средством коммуникации является залогом высокого качества информации. И еще долго после того, как качество исчезло, люди, работающие в СМИ, продолжали цепляться за рычаги управления и думать, что управление – единственный путь достижения высокого качества, и если убрать управление, то и качество тоже уйдет. А это уже дурно пахнущая и бессовестная элитарность в ее наихудшей форме! Потому что выходит, что источником качества являются блюстители среды, хотя они всего лишь блюстители. По их мнению, раз они владеют дорогостоящим производством, это автоматически означает, что их сообщения стоят того, чтобы их слушать.

В тот момент, когда вы отделяете сообщение от средства коммуникации и открываете его для всего диапазона выражений, среди сообщений обязательно появятся и самые банальные из существующих в вашей культуре – в том числе и «SMH». Но со временем эти сообщения обязательно будут выражать и самое интересное в вашей культуре.

В современных американских школах дети читают «Документы федералистов» – это сборник гражданских эссе, написанных в XVIII столетии отцами-основателями нации, в которых обсуждается значение демократии для новой республики. Через сто лет дети будут читать «Твиты федералистов», написанные каирскими революционерами. И это вовсе не безумная фантазия. Это часть человеческой цивилизации. Мы уже не раз видели, как это бывает.

Сегодня Twitter высмеивают за банальность, потому что не понимают, что информация и средство коммуникации неразрывно не связаны. Когда-то смеялись над телевидением, представлявшимся пустым времяпрепровождением, затмившим высокое искусство кинематографии. Кинематограф тоже был пустым времяпрепровождением, поскольку обесценил и вульгаризировал высокое театральное искусство. Театр в викторианские времена считался вульгарным и дешевым времяпрепровождением, поскольку являлся опошлением великих драматических пьес классиков Древнего Рима и Греции. Идя дальше по этому пути, можно дойти до Аристотеля, который говорил о смерти философии, потому что современная ему молодежь желала лишь смотреть театральные постановки, а не читать философские пергаменты! И, скорее всего, он нелестно высказывался о тогдашней молодежной моде отращивать длинные волосы. Каждое поколение совершает ошибку, приписывая ценность своему средству коммуникации и рассматривая средство коммуникации следующего поколения – расширяющее доступность, увеличивающее диапазон выразительных средств – как пустое и вульгарное.

«Каждое поколение совершает ошибку, приписывая ценность своему средству коммуникации и рассматривая средство коммуникации следующего поколения – расширяющее доступность, увеличивающее диапазон выразительных средств – как пустое и вульгарное».

Но ворчуны не понимают, что при удешевлении средств коммуникации сообщение обретает свободу. Для него появляется расширенный диапазон средств выражения. Да, первые сообщения будут банальными. Причина этой банальности в том, что среда предыдущего поколения не позволяла выражать подобные пустяки. В ней не было поддержки таких выражений. Так что появятся «SMH». Но появятся и сообщения в реальном времени о революции в Каире. И к тому времени, как до ворчунов всё это дойдет, новая среда будет уже заполнена сообщениями высокого качества. Ну а затем можно отвернуться и приступить к порицанию «вульгарного» средства коммуникации, обесценивающего сообщение.

Деньги – это тип контента, и мы только что разорвали связь денег со средствами коммуникации. Прежние представляли собой серию соединенных между собой сетей, «сортировавших» деньги в зависимости от их размера и получателя. Существовали платежные средства для небольших сумм. Существовали платежные сети как для крупных сумм и для быстрой передачи денег, так и для медленной передачи. Платежные сети для расчетов между организациями, между государствами, для расчетов физических лиц

с юридическими лицами, для расчетов между физическими лицами… Ой нет, прошу прощения! Таких как раз и не было! Платежных сетей для расчетов между физическими лицами у нас нет. Платежные сети не занимаются мелкими платежами, поскольку традиционная среда не дает такой возможности.
Я не могу отправить двадцать центов за границу, чтобы рассчитаться как обычный человек с другим человеком, поскольку средства коммуникации накладывают ограничение на разнообразие оказываемых услуг. Стоимость производства не дает мне такой возможности. Но мы разделили сообщение и средства коммуникации. Мы создали деньги в виде одного из типов контента, при практически нулевой стоимости производства. Проводить транзакции теперь возможно вне зависимости от размера суммы и конечного получателя, будь это физическое лицо или государство.
Что же будет дальше? Блюстители порядка примутся рассказывать, что сеть эта несерьезная. Они путают стоимость затрат на их платежную сеть с ценностью их услуг! Блюстители старых платежных сетей поведают нам, что эта новая форма платежей вульгарная и дешевая. Ее можно использовать только для пустяков. А все серьезные люди продолжат использовать традиционные банки. И поскольку они могут контролировать и ограничивать транзакции, то считают такую систему залогом высокого качества услуг. Но нет! Это просто раздутая величина производственных расходов, элитарность в наихудшем проявлении! Они цепляются за привычное им средство коммуникации и отказываются видеть, что сообщение теперь может быть передано при нулевых затратах и мгновенно.
Каким же окажется первое использование новой модели? Теперь мы можем обмениваться мелкими платежами в Twitter, мне уже поступают небольшие пожертвования[59]. Но для большинства людей это пустяки. Они не в силах понять, что эти средства годятся для всех транзакций, от минимальных до крупных.

«Блокчейн может работать со всем диапазоном: от десяти центов до стомиллиардного государственного долга».

Придет день, когда одна из стран впервые заплатит за поставку нефти с помощью Блокчейна; когда-нибудь в Блокчейн попадет покупка транснациональной корпорации или продажа авиаперевозчика. В Блокчейне возможно проводить любые транзакции – от десяти центов до стомиллиардного государственного долга. Общество просто пока не готово это осознать. Технология способна всё это выполнять без каких-либо ограничений, накладываемых каналом передачи. Суть не в том, что транзакция в форме контента может быть передана в виде смайликов в Skype. Это всего лишь признак, указывающий на суть: мы освободились от всех ограничений, которые накладывались средствами коммуникации предыдущих эпох. Мы сделали контент важнее остального.

Цикл зрелости технологий

Когда создание контента – прерогатива элит, тогда избранные мастера используют его для создания шедевров: Библия Гуттенберга; первые фотографии; полет на Луну, показанный по телевизору; великие киноленты прошлого. Все эти достижения – дело рук великих людей, мастеров своего дела.

Технологии становятся более доступными, изменяются средства коммуникации. Люди осваивают всё новые средства для выражения мыслей, идей, своих потребностей, а «блюстители порядка» продолжают цепляться за старое. Они по-прежнему пытаются создать нечто грандиозное при помощи средств коммуникации, которые у них в наличии. Они печатают массивные, тяжелые фолианты в кожаном переплете на латыни:
Principia Mathematica
. Появляются новые средства коммуникации, а вместе с ними – книги в мягких обложках, и пленка на 24 кадра, которая открывает дорогу в мир фотографии любому обывателю. Хранители старых традиций продолжают цепляться за прошлое, но им всё труднее делать вид, что у них в руках нечто грандиозное, – поэтому они просто играют на публику. Они заявляют: «В пленочной фотографии есть неуловимая магия», «У звука на виниле есть что-то, чего не передает CD», «Тележурналист – это же авторитет: вспомните Уолтера Кронкайта[60]!», «Газета – источник авторитетных мнений, и она стоит того, чтобы печатать ее именно на бумаге». Да, пафос! Вся грандиозность улетучилась. Качество ушло. И остается лишь цепляться за рычаги управления и притворяться, что управление – залог высокого качества.

В итоге, следуя по кривой вверх[61], технология достигает пика. Ближе к концу в величие этой технологии по-прежнему верит только поколение бабушек и дедушек. Развитие технологий идет по большой дуге, и то, что начиналось как шедевр, теперь используют лишь те, чья жизнь вступила в финальную пору. Первые чеки выписывались членами королевских фамилий для финансирования великих предприятий, например Остиндской компании, которая проложила дороги к специям и создала торговые пути на Восток. В те дни чековые книжки были лишь у членов королевской семьи. А если сегодня в супермаркете впереди вас стоит, дай бог ей здоровья, бабуля, которая достает из сумки чековую книжку, – вы услышите одновременный стон всех 15 человек, стоящих за ней в очереди, потому что они понимают: оформление этой транзакции займет 15 минут. В чековой книжке при покупке бобов и хлеба в супермаркете от грандиозности финансирования Ост-индской компании ничего не остается. Это финальная стадия технологии.

Сегодня новости по телевизору смотрят только старики, потому что остальные узнают новости из интернета. То, что когда-то считалось ничтожным, сегодня стало важным источником заслуживающих доверия новостей и информации. Но старикам вы этого не втолкуете. Мы читаем электронные книги. Некоторые говорят: «Есть нечто
этакое
в шуршании бумажных страниц». Ага, еще бы! Двадцать книг – нелегкая ноша, а я вот читаю примерно двадцать книг за четыре-пять недель, так что мне нужно именно столько таскать с собой. Ничего
этакого
в бумажных книгах нет – люди просто цепляются за прошлое.

Когда мы вступаем в этот мир, где деньги – одна из форм контента, блюстители старых платежных систем цепляются за иллюзию высокого качества традиционных банковских систем и утверждают, что они сами – залог высокого качества, которое зиждется на их контроле, цензуре, ограничениях. Однако качество обеспечивается не этим. Мы движемся дальше и открываем новые формы выражения, достигая того, чего никогда не было прежде. А они хватаются за свою идею величия: огромные старинные банки со сводчатыми потолками и хромированными сейфами, которые уже опустели: туда можно сходить на экскурсию в воскресенье, чтобы поглядеть, какими раньше были банки. Во многих городах мира огромные хранилища старинных банков теперь превращены в бары, и можно выпить в бывшем сейфе коктейль, потому что сегодня банки не могут себе позволить содержать свои огромные здания. Всё, чему они могут служить, – напоминание о былом величии. Они всё еще пытаются убедить вас, что, контролируя, оберегают нас от зла, от террористов, от отмывания криминальных денег… Но они лишь защищают свои насиженные места от конкуренции!
Нам удалось отделить сообщение от канала коммуникации. Теперь деньги – это одна из форм контента, и обратно мы не вернемся никогда.
Спасибо за внимание!
Примечание Андреаса для читателей:

В этом выступлении я, не подумав, попытался прямо во время разговора без подготовки приводить математические выкладки. Математик я посредственный. Как выяснилось. Но никакие неверные выкладки не меняют мою точку зрения, хотя текст был проверен редакторами, чтобы меня не позорить. Т-с-с! Пожалуйста, никому не говорите, что я не силен в математике.

Элементы доверия: свободная реализация креативных идей

Семинар по Блокчейну; Берлин, Германия; март 2016 года

Сегодня я расскажу об особенности технологии Биткойн, делающей ее такой привлекательной и интересной. Большинство людей эту особенность просто не замечают, не потратив год-другой на изучение Биткойна. Ведь он напоминает луковицу. С нее нужно снять шелуху, а когда вы снимете верхний слой, под ним обнаружится следующий. Я начал пять лет назад – и всё еще открываю для себя новое. Каждый день я узнаю о Биткойне всё больше и больше удивительных вещей.

Иллюзорные отправители, получатели и счета

Когда я впервые столкнулся с Биткойном, меня удивило, насколько всё было похоже на более-менее привычную банковскую систему. Я посещал известные сайты по Биткойну, например blockchain.info, и наблюдал за тем, как проходят транзакции. Я мог посмотреть отправителя, получателя и счет. Я думал: да, знакомая картина. Банковские услуги. Ну да, отлично, – а потом я решил посмотреть на исходный код и выяснить, как это работает.
Как специалист, работающий в области теории вычислительных машин, я подумал: взгляну на исходный код и попробую разобраться, как система всё это делает. Но когда я поискал в исходном коде отправителя, получателя или счет, то ничего такого там не нашел. Потому что все эти вещи в Биткойне не существуют. Это меня сильно удивило: когда я смотрел исходный код программы, ничего из того, что я ожидал там увидеть, не было! Думаешь, что система, по многим признакам похожая на банковскую, создана так, как и положено банковской. Но в Биткойне всё иначе.

«Когда я поискал в исходном коде отправителя, получателя или счет, то ничего такого там не нашел. Потому что все эти вещи в Биткойне не существуют».

Сколько из вас смотрели исходный код или разбираются в технических основах? Вижу, что немного. Так вот, когда вы изучаете код, то обнаруживаете, что в нем нет баланса, нет отправителя, а есть только UTXO (сокр. от англ. Unspent Transaction Output)[62], информация с выходными данными о непотраченных средствах, и inputs (англ.) – входящие данные. Данные об исходящих транзакциях невозможно сопоставить с получателями. Внезапно вы понимаете: то, что вы видите, – это простые элементарные частицы, выражающие квантовую или атомарную природу Биткойна.

Атомарная структура Биткойна

Химия изучает элементы: например, медь, железо или гелий. Она также изучает огромное множество составляющих вещество элементов, которые комбинируются, создавая интересные вещи. Например, людей – или тостеры. Но когда вы углубляетесь в изучение химии, то начинаете понимать, что медь – это не некая «вещь в себе». Это структура, состоящая из протонов, нейтронов и электронов. И никакой меди нет! Один протон точно такой же, как и любой другой протон; он может с таким же успехом быть частью гелия или любого другого вещества, ему всё равно. В данном конкретном протоне нет ничего особенного, что заставило бы его стать частью именно меди.
Химия – это верхний уровень; ниже лежит другой уровень, который изучает атомная физика. Этот уровень очень прост. Здесь существует небольшое количество элементарных частиц. И из этих нескольких частиц возникает вся известная нам химия, сто с лишним природных химических элементов, имеющих свои собственные уникальные свойства, совершенно различные. Одни из них являются жидкостями, другие

металлами, а третьи – газами. Они по-разному себя ведут. Но все эти свойства не относятся к их базовому составу. Всё это просто вариации.
Биткойн обладает такой же базовой атомной структурой, он строится из базовых элементов. Элементарные частицы Биткойна – это компоненты транзакций и элементы языка сценариев. Эти элементы не имеют ничего общего с традиционными банковскими сервисами. Нет счетов, баланса, отправителей, получателей. Вместо этого элементы биткойн-сети обращаются к фундаментальным математическим и криптографическим свойствам: например, проверяют, равна ли контрольная сумма (хэш) другой контрольной сумме, соответствует ли одна ECDSA-подпись другой, производят операции с числами и т. д. А то, что видно на поверхности, то есть транзакции, – это уже комбинации. Это особый способ сочетания элементов, позволяющий создать нечто вроде банка. И это прекрасно, поскольку новичку в Биткойне можно показать «счет, отправителя, получателя», и новичок думает: а, понятно, это мне знакомо.
Затем новичок узнаёт, что у него есть кошелек, но в кошельке нет никаких монет, а только ключи, и эти ключи можно копировать, – и теперь он думает: «Ничего не понимаю! Не похоже на то, как я делал это раньше». Всё становится сложнее, поскольку Биткойн – совсем не то, что вы думаете. Это платформа. Это не платежная сеть. Это не валюта. Это не банковская система. Это платформа, которой вы доверяете выполнение определенных функций. А если у вас появляется платформа, которой вы доверяете выполнение определенных функций, одно из полезных применений для нее – создать валюту и платежную сеть; но создать можно и другие вещи.

Конструктор «Лего»

В детстве моей любимой игрушкой был конструктор «Лего». Он нравился мне не потому, что я мог собрать из него изображенную на коробке игрушку. Я не собирал то, что там было нарисовано. Если на коробке была красная пожарная машина, я собирал дракона или жирафобегемота – нечто не существующее в природе или что-нибудь странное из того, что приходило мне в голову. Вот это мне и нравилось. Можно было взять эти детали и создать что пожелаешь.
Если взглянуть отвлеченно, конструирование из «Лего» – довольно беспорядочное занятие! И то, что я из него делал, не было похоже ни на пожарную машину, ни на космический корабль. Если бы из этой пластмассы отлили игрушечную пожарную машину – обтекаемой формы, без острых углов, просто пожарную машину, – да, это была бы прекрасная пожарная машина. Но она осталась бы лишь пожарной машиной, и через двадцать минут игры надоела бы мне. Потому что моя гладкая пластмассовая пожарная машина – всего-навсего пожарная машина, пусть и прекрасная. И ей никогда не стать жирафобегемотом, помидором или космическим кораблем. А «Лего» позволяет добиться большего!

Кулинарный конструктор

Я подрос, и у меня появилось хобби – кулинария. В приготовлении пищи мне нравится идеальное сочетание науки и искусства. Если вы понимаете основы работы ингредиентов, их поведение, как их трансформируют химические процессы, или когда вы добавляете катализатор (например, соль), или когда вы их нагреваете, то вы можете творить! Можете создавать что угодно. И если вы понимаете, как работают ингредиенты, то можете приготовить всё, что вам захочется.

Элементы креативных идей

Биткойн обладает такой же элементарной природой. Он не дает вам окончательного результата. Технология предлагает набор ингредиентов и рецепт – или, если провести аналогию с «Лего», набор элементов и фото предмета, напоминающего очертаниями красную пожарную машину. И когда мы

демонстрируем наш результат миру, финансовые компании смотрят и говорят: «Ну, у вашей пожарной машины слишком много острых углов, и она построена из каких-то дурацких деталей». А мы в Биткойне взяли ингредиенты, перемешали их и создали банковскую платежную систему. Банки смотрят и словно хотят сказать: «Ваш бургер неплохой, но вот у нас в „Макдональдсе“ делают такой же за 45 секунд, и мы продаем их миллиардами. Так зачем же повар, ингредиенты, рецепты, если можно просто штамповать их миллиардами?» И они упускают самое главное.

«Биткойн обладает элементарной природой. Он не дает вам окончательного результата. Технология дает набор ингредиентов и рецепт».

А главное вовсе не в том, чтобы создать миллиард экземпляров всё того же низкокачественного продукта. Главное не в том, чтобы у каждого появилась красная пластиковая пожарная машина, которая надоест через пять секунд. Главное – уничтожить барьеры для нашей креативности, дав нам инструменты и элементы, необходимые для построения чего-то уникального.
Я не приготовлю бургер так же быстро и дешево, как «Макдональдс», и моя маленькая пожарная машина не такая гладкая, как отлитая на конвейере пластмассовая игрушка. Зато я могу добавить томатный соус и приготовить альбондигас[63]. Могу создать жирафобегемота. А с готовой игрушкой этого сделать нельзя. И на кухне в «Макдональдсе» желаемого тоже не добиться. Но я уничтожил барьеры для своей креативности!

Биткойн как конструктор

Люди начинают понимать, что Биткойн – это набор ингредиентов и рецепт, но ведь рецепт можно взять и другой? Сегодня люди начинают искать новые комбинации ингредиентов.
Мы создаем краудфандинговые проекты, комбинируя несколько транзакций и цифровые подписи. Комбинируя эти элементы, мы можем создать одну транзакцию, которую финансируют несколько человек, но транзакция будет корректной лишь в случае достижения порогового значения финансового показателя. Это те же самые элементы, которые я использую для того, чтобы заплатить доллар по платежной сети Биткойн, но их можно скомбинировать по-другому – и получится краудфандинговая платформа.
Мы создаем платежные каналы, комбинируя подписи «2-из-2», используя мультиподпись, алгоритм остановки транзакций по расписанию. Это позволяет ввести посекундную тарификацию при просмотре потокового видео.
Мы строим приложения поверх платежных каналов, добавляя к ним новый ингредиент – контракты типа Hash TimeLocked Contract[64], – и тем самым можем соединять вместе несколько каналов. А затем получается сеть мгновенных платежей Lightning Network – новый невиданный рецепт!

«Мы пытаемся убрать барьеры для креативности нового поколения! Мы строим систему, поверх которой можно построить тысячи приложений».

Банки говорят: «У вашего грузовика острые углы, бургер ваш слишком дорогой и готовится дольше 45 секунд». Но на самом деле они хотят сказать вот что: «У вас слишком высокая стоимость транзакции, скорость очень низкая и нет никаких перспектив масштабирования». Они не улавливают главного. А главное то, что мы не пытаемся продать миллиард бургеров, потратив на каждый по 45 секунд: мы пытаемся разрушить барьер креативности для всего нового поколения! Мы строим систему, поверх которой можно построить тысячи приложений, для которых нужна система с доверием.

Экономика на базе фокус-групп

Когда у вас есть эти ингредиенты, то по какому рецепту вы станете их смешивать – уже ваше дело. Потому что, если заниматься производством красных пожарных машинок, будет создана целая фабрика, на

которой примутся штамповать сплошь одни красные пожарные машинки. И я уверен, что ее создатели скажут: «Послушайте! Наша статистика утверждает, что 95 процентов детей хотят играть красными пожарными машинками. Мы провели тестирование на фокус-группах и привлекли маркетинговую команду. Мы можем производить миллионы экземпляров стоимостью всего лишь по три цента. Надо совсем немного свинцовых белил и ядовитых, токсичных, канцерогенных углеводородов, – и никаких проблем. Мы всё сделаем очень дешево, доходность выйдет огромная». И они будут изготовлять только пожарные машинки.

Когда вы строите сеть общепита наподобие «Макдональдса», то получаете возможность штамповать бургеры раз в 45 секунд, но альбондигас вы на этих кухнях готовить не сможете. И что-нибудь другое – тоже нет! Вы налаживаете отличный конвейер под что-нибудь одно – и только. И пока это дает нужную доходность, всё в порядке. Ведь я уверен: вы обязательно протестируете продукт на фокус-группах и убедитесь, что именно он всем и требуется.

И это кошмарный способ построения экономики. Это ужасный способ построения финансовой системы. И это ужасный способ построения платежной сети!

Привилегии банков и банки-наблюдатели

Банки, по сути, говорят нам следующее: «Мы провели тестирование на фокус-группах. Люди хотят, чтобы считывание карты при оплате проходило не путем „прокатывания“ карты в считывателе, а просто поднесением ее к устройству; при этом экономится пара секунд времени и минимум усилий». А я говорю, что мы можем работать с четырьмя миллиардами людей, у которых нет доступа к банкам и к чистой питьевой воде. Мы можем решить проблему, из-за которой у подавляющего большинства людей нет доступа к финансовым услугам. Либо мы можем экономить усилия покупателя, сделав контактную карту бесконтактной.

Необходимо признать факт: причина, по которой в банковскую систему не вовлечено более четырех миллиардов людей, заключается в том, что сегодня на каждом этапе транзакции требуется идентификация личности. Такой подход позволяет построить тотальную систему наблюдения (которой позавидовала бы даже «Штази») для мониторинга любой финансовой транзакции в любой точке мира. Всё это потому, что, исходя из буржуазной осмотрительности, мы сами себя убедили: нам необходима такая повышенная защита, – и мы решаем эту задачу не путем устранения бедности, не путем прекращения бомбардировок других стран, а путем организации постоянного наблюдения за каждым, кто покупает бургер, – просто так, на всякий случай.

Мы сами предоставили власть над собой этому механизму, который довел себя до совершенства, – и, подобно фабрике, штампующей одни лишь красные пожарные машинки, эта система позволяет оказывать привилегированные финансовые услуги лишь элитарной прослойке населения, а тотальное наблюдение прочно узаконено законодательством каждой страны, и пограничные барьеры мешают развитию международной торговли. Это финансовая система, в которой власти могут применять давление, чтобы вы не могли финансировать WikiLeaks, поскольку им эта организация не по душе, – зато любой может спокойно перечислять пожертвования для Ку-клукс-клана (и я вовсе не шучу). Именно так и обстоит дело. Банками была построена система, которая решает лишь одну задачу – задачу нашего порабощения. Эта система пригодна лишь для того, чтобы нас обеднять. Она забирает нашу свободу наиболее эффективным из возможных способов. Такая система порочна и не имеет потенциала к развитию.

По сравнению с ней безумная путаная система, которую мы создали с помощью Биткойна, полна ошибок и работает медленно. В качестве международной банковской системы она неэффективна, вообще несерьезна и не столь продвинута. Зато она дает свободу и простор для реализации наших креативных идей.

Спасибо за внимание!

Масштабирование Биткойна

Семинар по Биткойну в центре Paralelni Polis; Прага, Чехия; март 2016 года

Примеры масштабирования

Сегодня я расскажу о масштабировании. Многие из вас, наверное, отметили, что в биткойн-сообществе сегодня идет довольно интересное обсуждение проблемы масштабируемости Биткойна. Именно об этом я и хочу рассказать, но не с технической точки зрения, а в более широкой перспективе, чтобы попытаться понять, что же это такое – масштабируемость.

Юзнет уничтожит интернет

Подходите поближе; я расскажу о том, что было давным-давно. В 1989 году интернет работал по аналоговым коммутируемым линиям. Не только пользователям приходилось выходить в интернет по телефонной сети: в большинстве случаев подключение магистральных линий связи к интернету было аналоговым. Между университетами, между научными лабораториями существовало немного постоянных высокоскоростных каналов со скоростями в 256 килобит/сек или 512 килобит/сек. Но в основном интернет работал с помощью аналогового коммутируемого подключения. В те времена электронная почта еще не вошла в широкий обиход. Существовало особое место в интернете, называвшееся «юзнет». Это система дискуссионных групп, в которых можно было разместить текстовое сообщение, а другие пользователи имели возможность его прочитать и даже на него ответить.

Обмен сообщениями был медленным, поскольку юзнет работал так: все сообщения передавались по коммутируемым системам, а затем распространялись от узла к узлу в системе хранения и пересылки. Вы размещали сообщение, и все остальные пользователи получали его в срок от 24 до 48 часов. После этого пользователи отвечали на сообщение, и в срок от 24 до 48 часов вы могли увидеть ответы. Сегодня подобный метод общения можно сравнить с общением героя Мэтта Деймона из фильма «Марсианин», который посылал сообщения с Марса на Землю.

В то время шло оживленное обсуждение этой системы среди инженеров, занимавшиеся интернетом, поскольку юзнет набирал популярность и объем данных увеличивался. Необходимо было передавать килобайты, а затем и мегабайты текстовой информации. Сначала для получения всех юзнет-сообщений за день требовалось примерно 30 минут по коммутируемому каналу связи.

Затем, с ростом популярности системы, возросло количество сообщений, что означало рост объема данных и увеличение необходимого времени соединения. Вскоре скачивание сообщений стало занимать час, затем два часа, а потом и три. Эксперты предсказывали скорый конец системы. Они говорили: если провести линию от точки, в которой мы находимся сейчас, до точки, в которой мы были полгода назад, можно увидеть, что вскоре для скачивания сообщений за день понадобится уже 26 часов, а в сутках всего 24 часа, и это уже становится серьезной проблемой.

И что же нас ждет? Интернет обрушится! Очевидно же, что он не масштабируется. Возможности масштабирования нет!

Альтернативные группы уничтожат интернет

В те времена юзнет делился на две части. Существовала стандартная часть, где находились тщательно структурированные группы для научных дискуссий, и маленькая часть юзнета, где все имена начинались с префикса «alt», – так называемые «альтернативные» группы. Эти alt-группы были необязательными. Провайдеры юзнета могли поддерживать alt-группу, но никто не принуждал их это делать. Разумеется,

всё самое интересное было собрано именно в этих альтернативных группах: например, существовали интереснейшие группы alt.folklore. computers, alt.security и, само собой, главная движущая сила масштабирования всего интернета – alt.sex.
Эти alt-группы, будучи необязательными, находились в фокусе всех тогдашних оживленных дискуссий. Надо ли их поддерживать? Потому что именно в них появился и первый в мире спам. Я помню, как получил свой первый спам. Это было сообщение, отправленное парой адвокатов сразу во все конференции юзнета. Так делать нельзя! Это не круто! Тысячи пользователей ответили им, что так делать нельзя, и это стало первой бурной волной всеобщего возмущения в интернете.
Обсуждался вопрос: надо ли поддерживать alt-группы? Поскольку в случае, если мы сохраним эти группы, интернет совершенно точно рухнет, ведь масштабируемостью он пока не обладает. Если alt-группы наберут популярность, то люди начнут размещать еще больше сообщений и у нас не хватит пропускной способности для обработки этих данных. Подобные дискуссии продолжались более двух лет. Нашлось несколько храбрых провайдеров, которые поддерживали alt-группы; они использовали жёсткие диски внушительных размеров, огромные диски размером 5МБ. Затем вновь обсуждалась идея – вот «если взять точку, где мы сейчас, и точку, куда мы стремимся, то мы упремся в стену».
Вот с чего началась проблема масштабируемости интернета. Он не масштабируется и не будет масштабироваться – это же очевидно! Многие исследователи написали диссертации на эту тему, доказывая вышеприведенное утверждение. Со временем нам удалось решить проблему юзнета. Каналы связи были обновлены, всё большее количество систем стало подключаться к сети по выделенным каналам и напрямую. Постепенно коммутируемые каналы были заменены на выделенные. Люди принялись инвестировать в инфраструктуру, нам стало легко передавать трафик в юзнет. А затем в обиход вошла электронная почта, и проблема масштабируемости возникла вновь.

Электронная почта с вложениями уничтожит интернет

Популярность электронной почты росла, и этот сервис стал занимать место юзнета, даже заслоняя его. И возникла еще одна большая проблема: люди желали общаться напрямую. Сообщение теперь доставлялось не за 24 часа, а всего за пару часов, через весь интернет, – и это означало, что люди стали беседовать в режиме реального времени (ну почти что в реальном времени). Произошел взрывной рост количества пользователей электронной почты. И вновь интернет было невозможно масштабировать, поскольку, если провести линию от точки, где мы сейчас, до точки, где мы были полгода назад, станет очевидно, что вскоре будет достигнут предел. Интернет рухнет! Были написаны очередные диссертации о том, что интернет погибнет от перегрузки электронной почтой и его никогда не удастся масштабировать.
Постепенно мы приступили к оптимизации. Мы решили проблему электронной почты. Я в те времена являлся просто наблюдателем, мне было лишь 16 лет, и я не понимал, что происходит вокруг. Так что говоря «мы», я имею в виду нас – человечество; мы решили эту проблему, справились с масштабированием. Интернет не масштабировался под юзнет – и он же масштабировался под юзнет, и всё лишь для того, чтобы не иметь возможности масштабирования под электронную почту! Затем он смог масштабироваться под электронную почту – лишь для того, чтобы какой-то умник взял и придумал мультимедийные интернет-сообщения MIME, а это означало, что теперь к сообщению электронной почты можно было прикреплять файлы. Такие вложения были в десять раз больше по объему, чем текст, потому что люди принялись рассылать объемные файлы – например, рисунки и фотографии; разумеется, тема секса вновь была раскрыта полностью.
Итак, мы смогли провести масштабирование для электронных писем – но не для вложений. Поднялся крик: «Мы никогда не сможем масштабировать интернет для передачи вложений, интернет обязательно рухнет!» А затем мы решили и эту проблему. И всё было отлично до тех пор, пока один британец, сэр Тим Бернерс-Ли (тогда он был просто Тим), не изобрел WEB – Всемирную паутину. Теперь картинки стало можно вставлять в рамки.

Всемирная паутина уничтожит интернет

Примерно в 1992 году в университетской лаборатории я загрузил и запустил первый браузер – это был NCSA Mosaic. Я собрал друзей, нас было трое или четверо. Несколько часов мы работали, чтобы загрузить дистрибутив NCSA Mosaic, скомпилировать код и установить программу. Затем мы ее запустили и вышли во Всемирную паутину. Мы облазили ее всю! Я один из немногих, кто может похвастаться: в 1992 году я за день облазил весь интернет! Потому что тогда в интернете было всего два сайта. Я подумал тогда: боже мой, когда-нибудь это станет громадным пространством! И интернет не сможет масштабироваться. Подумать только, какой простор для порно в этой Всемирной паутине! И, само собой, именно данное применение, как все мы знаем, стало движущей силой масштабирования. Именно оно двигало развитие интернета с самого начала, хотя в приличном обществе об этом предпочитают не говорить.

«Я один из немногих, кто может похвастаться: в 1992 году я за день облазил весь интернет! Потому что тогда в интернете было всего два сайта. Я подумал тогда: боже мой, когда-нибудь это станет громадным пространством! И интернет не сможет масштабироваться».

Интернет не масштабировался под Всемирную паутину! Люди говорили: «Нам никогда не справиться со всеми этими картинками и гипертекстовыми документами. Интернет не масштабируется!» И вновь писались диссертации, и вновь пошли обсуждения. И интернет не масштабировался. На сегодняшний день он с удивительным достоинством отказывается масштабироваться уже более десяти лет – с достоинством и весьма успешно.

Передача голосовой информации уничтожит интернет

Затем кто-то изобрел сервис передачи голосовой информации по интернет-протоколу (VoIP). А еще кто-то подумал: а почему бы нам не заменить интернетом всю телефонную сеть? Идея была совершенно безумной. Телефонные компании проделали огромную работу, разъясняя, почему сети с пакетной передачей данных никогда не смогут качественно отправлять голосовую информацию. Телефонные компании говорили: «Настоящее качество передачи голоса может обеспечить только иерархическая коммутируемая сеть, которой владеют национальные монопольные телекоммуникационные компании; интернет никогда не сможет масштабироваться для передачи междугородной телефонии».
И именно эти телефонные компании (ну те, которые пока еще продолжают свою деятельность) теперь передают весь свой телефонный трафик через интернет. Сначала они не хотели передавать интернет-трафик по своим телефонным сетям. Потом они разрешили передавать его. А затем стали строить свои телефонные сети уже поверх интернет-сети.

Видео с котиками уничтожат интернет

Затем все принялись рассылать видео с котиками. И интернет опять не смог масштабироваться, потому что из-за YouTube интернет должен был рухнуть. Совершенно ясно: необходима фильтрация контента по качеству, потому что разве можно допустить, чтобы каждый идиот размещал в интернете видео со своим котом? Говорили так: «В интернете уже тысячи видео с котиками! Если построить график от точки со вчерашним количеством этих видео до точки с сегодняшним количеством и экстраполировать график на будущее, станет ясно, что уже к концу нынешнего десятилетия в интернете будет миллиард видео с котиками!» Что и случилось.
Но мы смогли масштабировать сеть. Теперь мы умеем делать и трехмерное видео (3D), и видео ультравысокой четкости (4K).

Netflix уничтожит интернет

Когда появился Netflix[65], повторилась та же ошибка. В 1992 году, когда я впервые зашел в интернет, то подумал: «Вот это да! Это же конец телевидению, потому что когда-нибудь можно будет моментально передавать фильмы». Но если бы вы сказали такое кому-нибудь в 1992 году, вас назвали бы идиотом. Потому что совершенно очевидно – если бы Netflix существовал в 1992 году, то один-единственный видеопоток, предназначенный одному-единственному пользователю, вывел бы из строя весь интернет. Но вот мы дожили до будущего. Интернет опять отказывается масштабироваться под Netflix и все остальные компании, которые транслируют видео в реальном времени. И интернет так и продолжит не поддаваться масштабированию. Вскоре станет возможной передача видео для шлемов виртуальной реальности Oculus Rift с поддержкой голографического видео 3D, 4K, VR. И тогда интернет опять невозможно будет масштабировать! И будут написаны новые диссертации о том, почему интернет вот-вот рухнет.

Масштабирование – это движущаяся цель

Масштабирование – это постоянно удаляющаяся от нас цель. Требования масштабируемости лежат на пределе сегодняшних возможностей. С ростом требований эти возможности расширяются. Причина проста: сама по себе масштабируемость не является целью, которой нужно достичь, – это просто определение того, что вы можете сделать с сегодняшней сетью. В тот самый момент, когда пропускная способность увеличивается, само определение того, что вы можете сделать с сегодняшней сетью, меняется, потому что кто-нибудь говорит: «Секундочку! Вы хотите сказать, что я теперь могу сделать X, что требует в десять раз больше ресурсов, чем всё, что можно было делать прежде? Так давайте этим и займемся!» И вам опять нужно масштабировать сеть. Так что масштабирование – постоянно удаляющаяся от нас мишень. Масштаб задает предел сегодняшних возможностей. Как только он укрупняется, возможности растут.

«Масштабирование – постоянно удаляющаяся от нас мишень. Требования масштабируемости лежат на пределе сегодняшних возможностей. И с ростом требований эти возможности расширяются».

Биткойн не способен масштабироваться. И если нам повезет, он еще 25 лет останется неспособным к масштабированию – прямо как интернет! Компании того же самого типа, которые когда-то заявляли, что интернету не справиться с электронной почтой, что в нем никогда не будет качественной телефонии, никогда не появится возможность смотреть качественное видео, теперь разводят всё те же дискуссии о том, почему Биткойн никогда не справится с платежами в розничной торговле, не достигнет масштаба системы Visa, а если достигнет, то попросту рухнет. Прямо сейчас пишется дюжина диссертаций о том, что Биткойн исчезнет, что он уже исчез, что он уже умер или умрет в скором времени еще раз.
Существует отличный сайт под названием bitcoinobituaries.com, где можно прочитать все написанные когда-либо заметки о смерти Биткойна начиная с 2009 года: регулярно, как часы, каждые три – шесть месяцев в крупных газетах, в научных изданиях появляются заголовки: «Свершилось! Биткойн мертв!» Эта тема стала на диво плодотворной для трудовой деятельности – требуется всего лишь дождаться, чтобы люди услышали, что Биткойн умер, что Путин запретил Биткойн; затем через четыре месяца кто-нибудь говорит: «Знаешь, в Биткойне есть несколько интересных приложений», – а они отвечают: «Что?! Этот Биткойн всё еще существует?»
«Биткойн всё еще существует?» – это слоган биткойн-сообщества. И если нам удается просто поддерживать его на уровне «Биткойн всё еще существует», это вызывает удивление и сбивает с толку. Никак невозможно, чтобы Биткойн всё еще существовал, поскольку весьма серьезные люди на весьма высоких постах в весьма небедных компаниях говорят о том, что Биткойну в их сфере никогда не бывать. Ну а Биткойн всё еще существует, потому что с присущим ему достоинством продолжает оставаться неспособным к масштабированию.

Оптимизация комиссий и масштабирование

Если во время проверки возрастающей нагрузкой или проверки производительности (когда сеть будет переполнена транзакциями) выяснится, что сети необходимо масштабирование, что произойдет? Некоторые пользователи окажутся в ужасной ситуации. Они, как всегда, запустят транзакцию с комиссией в 0,1 миллибита, а на ее подтверждение уйдет три дня! И всё это время они будут страшно волноваться, особенно если это новые пользователи. Поскольку они считают, будто деньги ушли с их счета (хотя в Биткойне нет счетов) и находятся в пути к счету получателя (повторяю: в Биткойне нет счетов), так что деньги «зависли» где-то в пути. На самом деле деньги по-прежнему находятся у них на счете: просто транзакция пока не подтверждена. Транзакция находится либо у отправителя, либо у получателя, в соответствии с атомарной природой транзакции. Промежуточное состояние у нее отсутствует. Транзакция не может нигде «зависнуть», потому что в Биткойне ничего не передается – узлами сети принимается общее согласованное решение.
Но вот в сети внезапно начались проблемы, и некоторые кошельки поведут себя «умно», увеличив комиссию за передачу транзакций (в особых случаях на 100 процентов). Ну и что с того? Вместо уплаты четырех центов за отправку международного перевода, который придет через несколько секунд в любую точку мира, полностью защищенный от какого-либо контроля, придется заплатить целых восемь центов! Очевидно, это свидетельствует о том, что Биткойн мертв! Некоторые из разработчиков скажут: «Нет, я больше этим не занимаюсь. Биткойн мертв!» В газетах напишут: «Биткойн мертв. Транзакции не выполняются!»
Но транзакции выполняются. Вот мои транзакции, они выполняются. Я пользуюсь «умным» кошельком, который рассчитывает тариф за транзакцию. И что же произойдет из-за такого провала производительности? Появятся улучшенные кошельки.
Вот в чем суть ответа динамической системы на давление: когда кошельки станут лучше, то они начнут корректнее рассчитывать комиссии за транзакции. Несложно забить целую сеть трафиком, если в ней работает множество «неумных» кошельков, работающих с комиссией 0,1 миллибита, но в таком случае вам надо просто увеличить ваш тариф до 0,11 миллибита – и вот вы уже на коне! Потому что глупцы не обновили свое программное обеспечение и забили всю сеть своими транзакциями. Но если они получают возможность установить тариф 0,12 миллибита, то вам нужно просто поставить 0,13. Начинается гонка, и вы даже не заметите, как начнете тратить целых 0,5 миллибита (о боже!) на транзакцию, которая, разумеется (если вы обычный пользователь), ничего не стоит. Ну а если вы таким образом пытаетесь «положить» сеть, то это мероприятие очень быстро станет для вас слишком затратным.

Спам-транзакции, допустимые транзакции, недопустимые транзакции

Здесь возникают интересные вопросы: что считать спам-транзакцией? Что такое допустимая транзакция и недопустимая? Существует два пути, чтобы найти ответы на эти вопросы. Первый – следовать административно-командному подходу, гласящему, что дозволено, а что не дозволено: путем составления соответствующего списка мы защитим сеть от перегрузок. Но такой подход нарушает фундаментальный принцип Биткойна, заключающийся в сетевом нейтралитете. Биткойну всё равно, кто отправитель, кто получатель, какое приложение при этом использовалось, какова ценность транзакции. Всё, что имеет значение для сети, – это факт существования комиссии за обработку транзакции. Если вы включили комиссию в транзакцию, тогда она по определению допустима, поскольку допустима в ваших глазах настолько, что вы заплатили за ее обработку. Сам факт указания комиссии в транзакции делает ее допустимой. Если мы начнем принимать решения, что является спамом, а что нет, то сведем Биткойн к набору приложений. Гений, который создает какое-либо уникальное приложение, не сможет распространить это приложение по сети, поскольку мы применили административно-командный подход, чтобы объявить эти транзакции недопустимыми.

«Сам факт указания комиссии в транзакции делает ее допустимой. Если мы начнем принимать решения, что является спамом, а что нет, то сведем Биткойн к набору приложений».

Другой способ решить эту проблему – использовать рыночный подход. У нас есть рынок и валюта. Так давайте воспользуемся рынком для решения проблемы. Позвольте ему установить минимальный тариф, соответствующий требованиям майнеров, который будет способствовать быстрому созданию блоков в сети, а также соответствующий требованиям пользователей приложений. Если вы платите по тарифу,

ваша транзакция допустима. Нет никаких спам-транзакций. Нет никаких недопустимых транзакций. Есть лишь транзакции, которые обрабатываются майнерами, и транзакции, за которые не указан достаточный размер комиссии (для их обработки майнерами).

Десятилетия неспособности к масштабированию

Вот так и будет развиваться Биткойн. Проблема масштабирования никогда не разрешится; я надеюсь, что у нас впереди еще десятки лет ежегодных дискуссий о масштабировании Биткойна. Каждый год мы будем успешно «проваливать» эту задачу для вновь появившихся приложений и так же успешно решать ее для уже существующих. Как только произойдут улучшения, люди придумают новые приложения – и мы вновь окажемся «неспособны» к масштабированию.
Интернет вот уже 25 лет не может «элегантно» масштабироваться. У Биткойна те же проблемы, и Биткойн всё еще не мертв.
Спасибо за внимание!

Спасибо за чтение!

Благодарю вас за то, что вы прочитали эту книгу! Надеюсь, читать вам было так же интересно, как мне было интересно проводить лекции. Если вам понравилось это издание, разрешите мне попросить вас об одном небольшом одолжении: зайдите, пожалуйста, на страницу этой книги в онлайн-магазине Amazon и напишите там о ней пару слов. Это поможет книге получить лучшую позицию в рейтингах поисковиков и позволит ей привлечь внимание большего количества людей, которые, быть может, еще не слышали о Биткойне. Если вы хотите со мной пообщаться или посмотреть видеозаписи приведенных здесь выступлений, приглашаю вас посетить сайт TheInternetOfMoney. info. И не забудьте подписаться на мой блог в Twitter – мой ник @aantonop.

Приложение А. Ссылки на видеозаписи

Каждая глава этой книги подготовлена по текстам выступлений Андреаса М. Антонопулоса на конференциях и семинарах по всему свету. Значительная часть выступлений была рассчитана на самую широкую аудиторию, хотя отдельные лекции состоялись перед специально отобранной публикой (студентами) по конкретным поводам.
Андреас замечательно общается со зрителями во время выступлений, но всё-таки большинство диалогов при подготовке текста книги пришлось удалить. Мы рекомендуем просмотреть оригинальные видеозаписи выступлений, чтобы почувствовать саму атмосферу событий. Все эти видеозаписи и другие материалы доступны на канале Андреаса в YouTube – он называется aantonop.
https://www.youtube.com/user/aantonop
Далее приведен список лекций, включенных в эту книгу, с указанием мест, дат и со ссылками на оригинальный контент.

Что такое Биткойн?

«Взрывай, создавай новое, расширяй масштаб»; Афины, Греция; ноябрь 2013 года
https://www.youtube.com/watch?v=LA9A1RyXv9s

Одноранговая денежная система

«Изобретаем заново деньги», лекция прочитана в Университете им. Эразма Роттердамского, Голландия; сентябрь 2015 года
https://www.youtube.com/watch?v=n-EpKQ6xIJs

Конфиденциальность, идентификация, надзор и деньги

Семинар по Биткойну в FabLab; Барселона, Испания; март 2016 года
https://www.youtube.com/watch?v=Vcvl5piGlYg

Инноваторы, разрушители, «белые вороны» и Биткойн

«Ярмарка изобретений»; музей им. Генри Форда; Детройт, штат Мичиган; июль 2014 года
https://www.youtube.com/watch?v=LeclUjKm408

«Упрощенные» сети, инновации и «процветание ресурсов общего пользования»

Лекция прочитана в рамках проекта O'Reilly Radar Summit; Сан-Франциско, штат Калифорния; январь 2015 года
https://www.youtube.com/watch?v=x8FCRZ0BUCw

Переворот в инфраструктуре

Цюрихский семинар по Биткойну; Цюрих, Швейцария; март 2016 года
https://www.youtube.com/watch?v=5ca70mCCf2M

Валюта как язык

«Биткойн-Экспо – 2014»; Торонто, провинция Онтарио, Канада; апрель 2014 года
https://www.youtube.com/watch?v=jw28y81s7Wo

Принципы работы Биткойна

Гарвардская лаборатория инноваций, проектный семинар IDEO Lab; Бостон, штат Массачусетс; июнь 2015 года
https://www.youtube.com/watch?v=Ur037LYsb8M

Деньги как один из видов контента

Южная конференция по Биткойну; Куинстаун, Новая Зеландия; ноябрь 2014 года
https://www.youtube.com/watch?v=6vFgBGdmDgs

Элементы доверия: свободная реализация креативных идей

Семинар по Блокчейну; Берлин, Германия; март 2016 года
https://www.youtube.com/watch?v=uLpSM3HWU6U

Масштабирование Биткойна

Семинар по Биткойну в центре Paralelni Polis; Прага, Чехия; март 2016 года
https://www.youtube.com/watch?v=bFOFqNKKns0

Примечания

1

Эта лицензия позволяет распространять, редактировать и брать за основу произведение (даже для коммерческих целей) с указанием автора. Такая лицензия рекомендована для максимального распространения и использования лицензированных материалов. –
Примеч. ред
.

2

Andreas M. Antonopoulos. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. – O’Reilly Media Inc., 2014. –
Примеч. ред.

3

Майкл Кейси, Пол Винья
. Эпоха криптовалют. Как биткойн и блокчейн меняют мировой экономический порядок. – М.: «Манн, Иванов и Фербер», 2017. –
Примеч. ред
.

4

Биткойн (
англ.
Bitcoin, от bit – «бит» и coin – «монета») – пиринговая платежная система, использующая одноименную единицу (биткойн) для учета операций и одноименный протокол передачи данных. В русскоязычном сообществе принято написание «Bitcoin» или «Биткойн/биткойн». –
Примеч. ред
.

5

Один сатоши, дробная часть 1/100 000 000 биткойна. –
Примеч. науч. ред.

6

В начале ноября 2013 года курс биткойна составлял 269 долларов. В декабре 2017 года курс превысил 19 000 долларов. На 1 мая 2018 года его курс составил 9119 долларов. –
Примеч. науч. ред.

7

Стоит отметить, что бурный рост популярности Биткойна, количества транзакций, стоимости криптовалюты в конце 2017 года привел к росту комиссии. –
Примеч. науч. ред.
.

8

CNN (Cable News Network) – американский кабельный и спутниковый новостной телеканал. –
Примеч. науч. ред.

9

На март 2018 года насчитывается более 900 криптовалют. –
Примеч. науч. ред.

10

От
англ.
demurrage – штраф за хранение денег. –
Примеч. ред.

11

По сути, денежные переводы с помощью (или внутри) одноранговой или пиринговой системы (
англ.
peer-to-peer, P2P) – это переводы средств (в любой валюте) напрямую между субъектами, например двумя физическими лицами. –
Примеч. науч. ред.

12

В 1902 году на территории современного Ирака была найдена двухметровая колонна из черно-зеленого диорита с многочисленными клинописными параграфами законов. Знаменитая находка хранится в Лувре. Этот древнейший свод законов, получивший название кодекса Хаммурапи, составлен примерно за 1700 лет до Рождества Христова. Он содержит два параграфа, посвященные производству и продаже пива, один из которых устанавливал предельные цены на пиво (в перерасчете на зерно) и был направлен против злоупотреблений торговцев. –
Примеч. ред
.

13

Здесь автор имеет в виду появление денег как таковых; оперируя понятием денег как технологии, он сообщает об их древнем происхождении. –
Примеч. науч. ред.
.

14

Плодородный полумесяц (
англ

. Fer tile Crescent) – историко-географический регион на Ближнем Востоке: от предгорий Эш-Шара через Палестину, предгорья Ливана и Антиливана, через Южный Тавр и Иракский Курдистан до Южного Загроса. –
Примеч. науч. ред.

15

Diners Club International – компания, выпускающая пластиковые карты. Основана 28 января 1950 года Фрэнком К. Макнамарой, Альфредом Блумингдейлом и Ральфом Снайдером. После своего образования стала первой в мире независимой кредитной компанией, которая начала работать с кредитными картами, ориентированными в первую очередь на оплату путешествий и развлечений. –
Примеч. ред
.

16

Application Programming Interface – интерфейс создания приложений; под интерфейсом подразумевается набор различных функций или структур, а также библиотек и сервисов, которые можно использовать в сторонних приложениях и сервисах. –
Примеч. ред.

17

Протокол TCP/IP – сетевая модель передачи данных, представленных в цифровом виде; она описывает способ передачи данных от источника информации к получателю. Модель TCP/IP происходит от двух важнейших взаимосвязанных протоколов: Transmission Control Protocol (TCP) и Internet Protocol (IP). –
Примеч. ред.

18

Цитата принадлежит британскому автору Джону Актону. В оригинале она звучит так: «Power tends to corrupt, and absolute power corrupts absolutely». –
Примеч. ред.

19

IP-адрес – уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP. –
Примеч. ред.

20

Пакет – упорядоченная совокупность данных и управляющей информации, передаваемая через сеть как часть сообщения. –
Примеч. ред.

21

Бит (
англ.
bit) – единица измерения количества информации. –
Примеч. ред.

22

Развитые страны – группа стран, занимающих ведущее положение в мировой экономике. В этих странах проживает 15–16 процентов мирового населения, но они при этом производят 3/4 валового мирового продукта и создают основную часть экономического и научно-технического потенциала мира. –
Примеч. ред.

23

WikiLeaks – международная некоммерческая организация, которая публикует секретную информацию, полученную из анонимных источников или при утечке данной информации. Главным редактором и директором WikiLeaks является австралийский интернет-журналист Джулиан Ассанж. –
Примеч. ред.

24

Блок генезиса – первый блок, созданный в Биткойне 3 января 2009 года. –
Примеч. науч. ред.

25

Адрес – здесь имеется в виду адрес биткойн-кошелька, на который осуществляется перевод средств. –
Примеч. науч. ред.

26

South by Southwest (SXSW) – ежегодное мероприятие, включающее в себя ряд музыкальных, кино- и медиафестивалей и конференций, проходящее в середине марта в США, в городе Остин, штат Техас. Фестиваль проводится с 1987 года. –
Примеч. науч. ред.

27

Seed – единственный пароль персонального доступа, состоящий из набора слов, к отдельному биткойн-кошельку. –
Примеч. науч. ред.

28

DoS-атака (от
англ.
Denial of Service) – атака на вычислительную систему с целью довести ее до отказа, то есть создание таких условий, при которых легальные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам (серверам) либо этот доступ затруднен. –
Примеч. ред.

29

Антихрупкость как свойство системы означает способность к извлечению выгоды из неудач, потерь, ошибок; умение развиваться и становиться устойчивее при столкновении с хаосом. Это понятие ввел экономист Нассим Талеб и подробно описал в своей книге «Антихрупкость». –
Примеч. ред.

30

Капитализация Биткойна составила более 151 миллиардов долларов по состоянию на 1 мая 2018 года. –
Примеч. науч. ред.

31

Как технология и платежная система. –
Примеч. науч. ред.

32

От результатов внедрения технологии. –
Примеч. науч. ред.

33

JPMorgan Chase (рус. «Джей Пи Морган Чейз») – американский финансовый холдинг. Образовался в результате слияния нескольких крупных банков США. –
Примеч. ред.

34

Wal-Mart Stores, Inc. – американская компания, управляющая крупнейшей в мире сетью оптовой и розничной торговли, действующей под торговой маркой Walmart. Основана в 1962 году. –
Примеч. ред.

35

Linux – семейство операционных систем на базе одноименного ядра Linux. Linux-системы распространяются в основном бесплатно в форме, готовой для установки и удобной для сопровождения и обновлений. –
Примеч. ред.

36

Линус Бенедикт Торвальдс (швед. Linus Benedict Torvalds, р. 28 декабря 1969, Хельсинки, Финляндия) – финно-американский программист, хакер. –
Примеч. ред.

37

Sun Microsystems – американская компания – производитель программного и аппаратного обеспечения, основана в 1982 году, в период с апреля 2009 года по январь 2010-го была поглощена корпорацией Oracle. –
Примеч. ред.

38

Имеются в виду несколько судебных дел (кражи данных из внутренних корпоративных сетей Dave & Busters, TJ Maxx, Heartland Payment System в 2008–2010 годах) в отношении Альберта Гонсалеса (
англ.
Albert Gonzalez). –
Примеч. науч. ред.

39

Обычно употребляется понятие СКУД – система контроля управления доступом. –
Примеч. науч. ред.

40

Майнер (от
англ.
miner – «шахтер») – человек, который занимается майнингом, или специализированное устройство для майнинга криптовалют. С технической точки зрения майнинг – это расчет хэша заголовка блока, который включает в себя, среди прочего, хэш заголовка предыдущего блока, хэш набора транзакций и случайное число. –
Примеч. науч. ред.

41

«Британская энциклопедия», или «Британника» (
англ.
The Encyclopedia Britannica) – старейшая англоязычная универсальная энциклопедия. Первое издание вышло в Эдинбурге в 1768–1771 годах. –
Примеч. ред.

42

O’Reilly (O’Reilly Media, ранее – O’Reilly & Associates) – американская издательская компания, основанная Тимом О’Райли в 1978 году. Издательство публикует в основном книги компьютерной тематики. O’Reilly Radar – интернет-блог, посвященный перспективным технологиям и новостям в сфере ИТ. В октябре 2015 года блог прекратил свое существование, но все архивные статьи доступны на сайте издательства. –
Примеч. ред.

43

Консенсус, или согласие участников сети. Консенсус – математический алгоритм, заложенный в самом программном коде (протоколе) сети. –

Примеч. науч. ред.

44

В данном контексте имеется в виду словосочетание «умная сеть» (от
англ
. smart network), и, соответственно, антонимы к нему – «простая сеть» или «упрощенная сеть». –
Примеч. науч. ред.

45

По своему функционалу. –
Примеч. науч. ред.

46

По сравнению с телефонной сетью. –
Примеч. науч. ред.

47

Смарт-контракт (
англ.
smart contract, дословно – «умный» контракт) – компьютерный алгоритм, предназначенный для заключения и поддержания коммерческих контрактов в технологии Блокчейн. –
Примеч. ред.

48

API (
англ.

application programming interface) – набор функций, предоставляемых приложением или операционной системой для использования во внешних программных продуктах и сервисах. –
Примеч. науч. ред.

49

Трагедия общин (
англ.
Tragedy of the Commons) – термин обязан своим происхождением притче Уильяма Форстера Ллойда из его книги 1833 года о населении. –
Примеч. науч. ред.

50

Эфириум (от
англ.
Ethereum) – открытая платформа блокчейн-приложений, созданная на основе технологии распределенного реестра и собственного языка программирования (Solidity), которая позволяет разработчикам создавать смарт-контракты. –
Примеч. науч. ред.

51

S&P 500 – список 500 акционерных компаний США, имеющих наибольшую капитализацию. Составляется аналитической компанией Standard & Poor’s (сокр. S&P), публикуется с 4 марта 1957 года. –
Примеч. ред.

52

LIBOR (Лондонская межбанковская ставка предложения;
англ.
London Interbank Offered Rate, сокр. LIBOR) – средневзвешенная процентная ставка по межбанковским кредитам. –
Примеч. науч. ред.

53

Чтобы избежать угрозы инфляционного обесценивания, создатели Биткойна изначально заложили принцип ограниченности виртуальных монет. Общее их число никогда не превысит 21 миллиона. –
Примеч. ред.

54

Блумберг-терминал – компьютерная система электронной торговли облигациями и другими ценными бумагами, предоставляемая компанией Bloomberg. Этот терминал позволяет пользоваться сервисом Bloomberg Professional. Через него пользователи могут в реальном времени контролировать и анализировать движение финансового рынка. –
Примеч. ред.

55

BTM – банкомат для биткойнов (от
англ.
Bitcoin Automatic Teller Machine). –
Примеч. науч. ред.

56

Например, информационной системы отдельного онлайн-банка. –
Примеч. науч. ред.

57

Craigslist («Крейгслист», дословно – каталог Крейга, по имени основателя, Крейга Ньюмарка) – сайт электронных объявлений, весьма популярный у американских пользователей интернета. –
Примеч. ред.

58

Эти слова принадлежат канадскому философу Маршаллу Маклюэну (
англ.
Herbert Marshall McLuhan, 21 июля 1911 – 31 декабря 1980). –
Примеч. науч. ред.

59

Существуют сервисы, которые позволяют отправлять пользователю Twitter небольшие пожертвования в биткойнах. Для такой транзакции нужно лишь знать имя получателя. –
Примеч. ред.

60

Уолтер Лиланд Кронкайт-младший (
англ.
Walter Leland Cronkite, Jr.; 4 ноября 1916 – 17 июля 2009) – американский тележурналист и телеведущий. Наибольшую известность получил как бессменный ведущий вечернего выпуска новостей CBS на протяжении 19 лет с 1962 по 1981 год. –
Примеч. ред.

61

Кривая Гартнера, или цикл зрелости технологии Гартнера (
англ.
Gartner Hype cycle) – кривая зрелости технологии, графически представляющая различные стадии, которые проходит технологическая инновация по мере своего становления. –
Примеч. науч. ред.

62

UTXO – информация с данными о размере непотраченных средств от исходящей транзакции в блокчейн-сети, которые можно использовать в качестве входных данных в новой транзакции. Модель UTXO, модель выполнения транзакций, применяется в блокчейн-сети Биткойна. –
Примеч. науч. ред.

63

Испанский густой овощной суп с мясными фрикадельками. –
Примеч. ред.

64

Hash time-locked contract – смарт-контракт, в котором получатель транзакции должен подтвердить платеж, создав криптографическое доказательство в течение определенного периода времени. –
Примеч. науч. ред.

65

Netflix – американская развлекательная компания, основанная Ридом Хастингсом и Марком Рэндольфом, поставщик фильмов и сериалов на основе потокового мультимедиа. Основана 29 августа 1997 года. С 2013 года Netflix производит собственные фильмы, сериалы и телепрограммы. –
Примеч. ред.