Глава

6

Гонка вооружений

Время — деньги.

Бенджамин Франклин

Майнинг биткоинов, некогда бывший вотчиной гиков от криптографии, сегодня становится крупным бизнесом.

По приблизительной оценке исследователя из Великобритании, за 12 месяцев до апреля 2014 года майнеры в совокупности инвестировали ни много ни мало 1 миллиард долларов в новое, суперпроизводительное специализированное компьютерное оборудование для майнинга. Любой участник этой увлекательной игры должен сделать выбор — или отстегнуть немалые деньги на оборудование, или смириться с постоянно снижающейся отдачей от майнинга. В этом бизнесе все еще можно сделать неплохие деньги, но его рентабельность существенно снизилась, а рентабельность инвестиций сильно колеблется в зависимости от курса биткоина.

Как мы уже говорили, «гонка вооружений» началась с того, что Ласло Ханеч понял: его графическая карта (или графический процессор) обеспечивает в 800 раз более высокую производительность майнинга биткоинов, чем центральный процессор. По мере того как рос его биткоиновый счет, другие майнеры следовали его примеру и переключали майнинг на графическую карту, стремясь возместить упущенную выгоду. На форумах технических специалистов вспыхивали дискуссии об этом новом подходе, как и о пицце, на которую потратил свои первые биткоины один из основателей этой денежной системы; а тем временем толпы новичков со всех уголков земного шара пускались в погоню за биткоинами.

Одним из таких новичков был студент колледжа в Беллвилле (штат Онтарио) Джейсон Уэлан, фанатично увлекавшийся двумя вещами: компьютерными играми и компьютерными сетями [1]. Интерес к последним привел его на онлайн-форумы криптографов, и осенью 2010 года он обнаружил, что среди их обитателей нарастает большое возбуждение в связи с биткоином. Он выяснил, что незадолго до этого в интернете появилась новая валютно-биткоиновая биржа под названием Mt. Gox. Это означало, что множество людей не только занимаются майнингом биткоинов, но и покупают их, причем курс постоянно растет. Например, в октябре курс утроился по сравнению с первоначальным — с шести до двадцати с лишним центов. Понадеявшись получить быструю прибыль, Уэлан внес некоторые изменения в домашний компьютер: он переключил две супермощные графические карты Nvidia, которыми раньше пользовался для игр, на майнинг, превратив таким образом свой ПК в мощный майнинговый узел.

И с этого момента у студента начались трудности. В первый же месяц его отец поинтересовался, какого черта счет за электроэнергию оказался просто космическим. Уэлан работал в мощной хеш-программе 24/7, предназначенной для интенсивного майнинга. В процессе работы компьютер так нагревался, что его владелец, всерьез опасавшийся за безопасность предмета своей гордости, переставил его в прохладный угол полуподвального помещения, заодно и подальше от глаз отца. Но тут возникла другая проблема: его нежно любимый игровой компьютер теперь был полностью загружен этой рутинной работой. И не похоже, чтобы можно было быстро разбогатеть таким путем.

«Меня больше интересовали компьютерные игры на моем новом игровом компьютере, чем сидение перед ним и наблюдение за процессом добычи каких-то сказочных денег, который я не очень-то понимал», — вспоминал Уэлан. Поэтому он выключил майнинговую программу, когда на счетчике монет в его электронном кошельке красовалась цифра 30. На тот момент они стоили 6 долларов, а на момент нашего разговора в конце мая 2014-го — уже 18 тысяч долларов. Как ни грустно, он много раз переформатировал жесткий диск компьютера, не позаботившись сохранить пароли и ключи к своему электронному кошельку. А без личного ключа, и даже без открытого ключа, прикрепленного к самому кошельку, эти деньги казались навсегда потерянными. «Уверен, таких, как я, очень много, и мы часто сожалеем о том, что

упустили возможность разбогатеть, бросив заниматься майнингом», — говорит он.

Тремя годами позже, уже будучи студентом второго курса Технологического института в Университете Онтарио (г. Ошава, штат Онтарио), Уэлан с изумлением узнал, что курс биткоина вырос до 120 долларов. Он начал читать литературу по цифровым валютам и, опираясь на свой опыт в области сетевых технологий, быстро понял их социальную и технологическую значимость, то есть то, что ускользнуло от него в юности. Он принял решение вернуться к майнингу.

Но это легче сказать, чем сделать. За три года перерыва в майнинге графические карты сами по себе устарели. Вслед за технологическим прорывом в январе 2013 года, когда компания Avalon из Китая оснастила первые компьютеры майнеров новыми специализированными интегральными микросхемами (чипами) ASIC, рынок биткоинов перешел под контроль специализированных майнинговых узлов, оснащенных этими супербыстрыми чипами, которые предназначены исключительно для обработки хешей. Курс биткоина рос по экспоненте, а в «гонку вооружений» вступали все более быстрые чипы и все более производительные майнинговые узлы. На момент выхода этой книги новейшие суперкомпьютеры, стоившие в рознице около 6000 долларов, выполняли три терахеша операций в секунду — три триллиона хеш-расчетов в секунду или 1800 триллионов за те 10 минут, которые требуются для создания и подтверждения блока. Это примерно в три миллиона раз быстрее, чем мог бы выполнить эту работу самый быстрый центральный процессор в 2009 году, когда Накамото добывал свои первые биткоины.

В то время как виртуальный мир майнинга развивался со скоростью света, традиционный мир заводов и каналов поставок тоже старался не отставать. К сентябрю 2013 года пишущая о биткоине пресса была переполнена историями о долгих задержках в доставке новейших майнинговых узлов даже от ведущих производителей. Можете себе представить разочарование людей, выложивших 4000 долларов авансом, чтобы заказать майнинговый комплекс Imperial Monarch от компании Butterfly Labs, и вынужденных ждать доставки шесть месяцев, зная при этом, что с каждой неделей добывать биткоины становится все труднее, а более мощные суперкомпьютеры уже на подходе. Федеральная торговая комиссия приостановила операции

производителя майнинговых компьютеров из штата Миссури. И это далеко не единственная компания, испортившая отношения со своими покупателями: KnC Miner из Стокгольма, CoinTerra из Остина, Alydian с острова Бейнбридж (штат Вашингтон) и Hashfast из Сан-Франциско — у них у всех были проблемы с доставкой, причем две последние компании обанкротились. В судах разбиралось множество исков с обвинениями в обмане покупателей: компании брали с них предоплату и тратили эти деньги на собственные майнинговые операции. Со своей стороны компании пытались переложить вину на своих поставщиков, обвиняя их в поставке бракованных комплектующих. Соучредитель компании Avalon Нг Чзан говорит, что тайваньские производители чипов ASIC сначала не принимали всерьез заказчиков, закупавших комплектующие для майнинговых комплексов. Однако по состоянию на середину 2014 года проблемы с поставками так и не были решены.

Уэлан преодолел это препятствие, купив подержанный майнинговый узел Jalapeno производства Butterfly Labs за 500 долларов, который нашел в разделе объявлений местной газеты. Это было все равно что купить подержанный мерседес со 100 тысячами километров пробега на спидометре. Его хешрейт составлял всего пять гигахешей в секунду, что намного меньше, чем у самых скоростных машин на рынке, зато его можно было получить немедленно — а это большое преимущество. Курс биткоина стабильно рос, и Уэлану не терпелось начать майнинг как можно скорее.

Затем Уэлан поступил так же, как поступал тогда практически каждый мелкий и средний майнер: он присоединился к майнинговому пулу. В этом случае он получал гарантии устойчивого притока биткоинов, хотя и в очень незначительных суммах, вместо того чтобы годами ждать счастливого случая, когда его компьютер выиграет целый блок биткоинов из 25 монет. Тем более что величина дохода его не слишком интересовала. В отличие от первого знакомства с майнингом в свои школьные годы, в этот раз он преследовал более серьезные цели. «В 2010 году я видел, что зарабатываю всего лишь *x* долларов, — говорит он. — Но сейчас у меня другой подход: даже если я потеряю деньги в долларах, перспективы биткоина настолько радужные, что можно смело ставить на будущий рост его курса».

К тому же на этот раз Уэлану выпал козырный туз: университет оплачивал его расходы на электроэнергию. Это объяснялось

достаточно просто: университеты еще не осознали необходимости бороться с майнингом в студенческих общежитиях. Но он ничего не мог поделать с постоянным шумом и жарой, создаваемыми майнинговым узлом в его маленькой комнатушке. Поэтому осенью он постоянно держал окно открытым и наслаждался потоком прохладного воздуха с улицы. Зимой окно приходилось закрывать и включать вентилятор, который вместе с компьютером производил адский шум. Тем временем в начале декабря курс биткоина достиг максимума в 1150 долларов, что в 10 раз превышало его значение в тот день, когда Уэлан возобновил занятия майнингом. Его вера в будущее биткоина блестяще подтвердилась, и он решил реинвестировать часть добытых биткоинов в расширение парка майнинговых узлов. Для их охлаждения пришлось купить еще один вентилятор. «Я себя чувствовал каким-то виртуальным наркоторговцем, — рассказывает он. — Приходилось постоянно присматривать за своими “посевами”, следить за бесперебойной работой и одновременно уклоняться от встреч с сотрудниками общежития, которым наверняка бы не понравилась постоянная работа мощных компьютеров, пожирающих электроэнергию».

Этот тайный и шумный бизнес приносил неплохую прибыль, но создавал многочисленные неудобства в быту. Очень быстро Уэлан столкнулся с неопровержимыми математическими доказательствами того, что поскольку хешрейт узла постоянен, удельный вес его вычислительного ресурса в неуклонно расширяющейся майнинговой сети постепенно снижается. Общий вычислительный ресурс сети к тому времени почти удваивался каждый месяц. В результате его и без того очень малая доля в общем объеме добычи с течением времени систематически уменьшалась. В начале весны 2014 года Уэлан подумывал о покупке еще одного подержанного майнингового узла AntMinter S1 от компании Bitmain с солидным хешрейтом 180 гигахешей в секунду. Но тут курс биткоина начал падать: за первые четыре месяца он снизился в три раза по сравнению со значением на начало года. В то же время хешрейт сети постоянно рос. Оба эти фактора в совокупности быстро сократили в два раза стоимость этого узла: на фоне узлов с хешрейтом более терахеша в секунду он морально устарел. В декабре новый майнинговый узел AntMinter продавался в рознице за 3000 долларов, но Уэлан искал подержанную модель примерно за 800 долларов. Осознавая, что оборудование и в будущем будет быстро устаревать, он изменил планы.

Уэлан знал, что существует альтернатива в виде облачного хеширования. Компании, предоставлявшие эти услуги, выкупали майнинговые узлы, объединяли их в больших дата-центрах с невысокими эксплуатационными расходами, а затем сдавали в аренду лоты вычислительного ресурса. Клиенты получали долю общей добычи биткоинов, пропорциональную доле вычислительного ресурса, которую они оплачивали. В частности, Уэлан подписал контракт на пять лет с компанией Pbcmining.com, выплатил полную стоимость аренды ресурса, равную 1,1 биткоина, или 600 долларам. Зато «...треклятые машины больше не терзают мои уши, и не надо беспокоиться об их моральном устаревании», — заявил он.

Уэлан, конечно, не надеялся, что этот бизнес сделает его миллионером, но небольшую прибыль дело приносило. К началу лета он зарабатывал ежемесячно около 200 долларов в биткоинах, из которых 50 долларов реинвестировал в дополнительный вычислительный ресурс в фирме Pbcmining.com. Это было просто необходимо, раз он не хотел отстать от постоянно растущей сложности математических задач и не собирался полагаться на все более редкие выигрыши биткоина в системе по мере адаптации последней к постоянно растущему вычислительному ресурсу сети. По мнению некоторых, из этого уравнения следует то, что цена многих контрактов на использование облачного хеширования установлена таким образом, чтобы доходы клиентов никогда ее не перекрыли. Уэлан же уверен в том, что поступает правильно: «Вряд ли я когда-нибудь сумею купить дата-центр, набитый майнинговым оборудованием, но генерировать достаточно биткоинов, чтобы оставаться частью биткоиновой революции, я смогу».

Облачное хеширование стало возможным благодаря другому собирательному тренду, развивающемуся параллельно с майнинговыми пулами: созданию гигантских центров обработки данных, где сотни или даже тысячи майнинговых узлов размещаются в огромных цехах, спроектированных так, чтобы максимизировать вычислительный ресурс и эффективно использовать электроэнергию. Часто такие цеха размещаются в странах с холодным климатом, чтобы снизить затраты на кондиционирование помещений и электроэнергию. Оптимальными местами их размещения признаны Исландия с ее геотермальной энергией, окрестности Вашингтона с их гидроэлектростанциями, богатая углем Юта, а также Швеция, где активно строятся

гидростанции, атомные электростанции и ветряки, что обеспечивает низкую стоимость электроэнергии и низкий уровень вредных выбросов в атмосферу. Не все дата-центры могут работать с облачным хешированием. Одни эксплуатируют майнинговые узлы самостоятельно. Другие приглашают владельцев размещать узлы на их производственных площадях и взимают с них плату за аренду и электроэнергию. Но все они — лишь часть феномена, благодаря которому за пять лет биткоиновый майнинг превратился в крупномасштабное промышленное производство.

В дата-центре, расположенном в окрестностях Солт-Лейк-Сити, посетители сначала проходят через автоматизированную цилиндрическую камеру, открывающуюся с помощью электронного пропуска и оборудованную сенсорными датчиками веса, роста и объема человека, чтобы предотвратить хищение неучтенного сервера [2]. Пройдя на территорию центра, они попадают на пост службы безопасности, сотрудники которого непрерывно наблюдают за изображением с камер видеонаблюдения, расположенных в наиболее уязвимых местах комплекса, или компьютерными моделями технического этажа, где расположены подстанция и установки кондиционирования воздуха. Вторая дверь расположена дальше по коридору и ведет в основной зал.

Основной зал напоминает пещеру: на высоте девяти метров на потолке смонтированы огромные вентиляторы с диаметром лопастей шесть метров, они медленно вращаются, перемешивая закачиваемый извне воздух. Под ними расположены стеллажи с серверами и прочим офисным оборудованием, которое принадлежит финансовым компаниям и сайтам электронной коммерции, продающим онлайн все что угодно — от цветов до книг. Цель суперэффективного, экономичного решения по охлаждению помещения состоит и в том, чтобы обеспечить им надлежащие условия хранения. Поодаль, в отдельной секции, оборудованы стеллажи для установки дополнительного оборудования клиента, решившего расширяться, — компании CoinTerra, производящей оборудование для майнинговых узлов, а в 2014 году занявшейся непосредственно майнингом. В то время как дата-серверы обычных клиентов тихо гудят и подмигивают красными, желтыми и зелеными огоньками, тщательно обрабатывая базы данных и обновляя записи на счетах клиентов, машины CoinTerra производят

невероятный шум. На каждом из 50 поставленных в ряд стеллажей размещено по 10 майнинговых узлов TerraMiner ASIC. Их хешрейт составляет 1,6 терахеша в секунду, что в 320 раз больше, чем у уэлановского Jalapeno. Под потолком безостановочно работают на предельной скорости три мощных встроенных вентилятора, охлаждая узлы. Их специализированные интегральные микросхемы непрерывно производят вычисления, причем каждый узел потребляет 2 кВт·час. Этого достаточно, чтобы обычный ноутбук проработал целый месяц. Таким образом, узлы, размещенные на одном таком стеллаже, потребляют 20 кВт·час, что в 10 раз превышает потребление электроэнергии стоящими рядом и занимающими примерно такую же площадь серверами менее продвинутых компаний из сферы электронной коммерции.

«Только в этом помещении находится вычислительный ресурс на 800 терахешей в секунду», — говорит CEO CoinTerra Рави Айенгар. Он вынужден почти кричать, чтобы перекрыть грохот, а поток воздуха от работающих вентиляторов треплет его уже начинающую редеть черную шевелюру. При прослушивании аудиозаписи нашей беседы создается впечатление, что мы разговаривали в эпицентре бушующего урагана. «Через две недели наш парк машин увеличится до 2400 единиц, а их суммарный хешрейт составит немногим менее четырех петахешей в секунду. Мы ставим цель нарастить хешрейт наших подразделений в Северной Америке до 10 петахешей».

Десять петахешей, или 10 тысяч триллионов хешей, в секунду — это примерно десятая часть совокупной мощности биткоиновой сети по состоянию на июнь 2014 года. Такой вычислительный ресурс требовался CoinTerra для диверсификации своих рисков. Айенгар объясняет, что спрос на их оборудование будет снижаться по мере падения курса биткоина, поэтому им требуется стратегия хеджирования. Они решили, что лучшим вариантом для компании станет выход на рынок майнинга и самостоятельное получение прибыли от него. Некоторой частью имеющегося вычислительного ресурса компания может распоряжаться самостоятельно, а остальное собирается арендовать через контракты на облачный хешинг со своими клиентами, которые представляют собой довольно пеструю компанию — от мелких частных любителей до оставшегося неизвестным человека, согласившегося арендовать весь петахешинговый вычислительный ресурс сроком на год за плату в 1 миллион долларов.

Айенгар, работавший инженером завода компании Samsung по производству микросхем в Остине, говорит, что он не просто готов поставить на дальнейшее расширение сферы применения биткоина как средства платежа, но и считает, что сеть блокчейнов ляжет в основу целого ряда сервисов обмена добавленной стоимостью (мы обсудим концепцию «Биткоин 2.0» в главе 9). «Хотя бы по этой причине майнинговая сеть в будущем будет расширяться», — утверждает он. И объясняет, каким образом собирается зарабатывать: сначала установит комиссионные для клиентов облачного майнинга на уровне себестоимости, а затем будет поднимать их по мере неизбежного роста производительности хеширования, а значит, и прибыльности бизнеса.

Ключевой фактор рентабельности майнинга, с точки зрения Айенгара, — это стоимость электроэнергии. В Солт-Лейк-Сити киловатт-час стоит дороже, чем в штате Вашингтон (где у его компании также есть производственные мощности), поскольку в последнем гидроэлектростанции вырабатывают более дешевую электроэнергию. Но и у Солт-Лейк-Сити имеются свои преимущества: международный аэропорт, развитая инфраструктура, продвинутое сообщество технических специалистов. Благодаря этим обстоятельствам город более или менее доступен из таких центров, как Лос-Анджелес или Сан-Франциско, что облегчает привлечение квалифицированного персонала для установки новых майнинговых узлов и наращивания объемов майнинга. Айенгар считает, что «гонка вооружений» вскоре заставит его пойти по этому пути. Поскольку его производственные помещения расположены в пустынной местности, окруженной горами с заснеженными вершинами, на высоте 1300 метров над уровнем моря, то воздух здесь сухой и прохладный, с низким уровнем статического электричества, отсутствует разъедающая металл влажность. Штат Юта также богат электроэнергией, вырабатываемой частично на низкоуглеродистом угле, частично на атомных электростанциях и гелиоустановках. В крупномасштабном и низкорентабельном бизнесе, каковым стал майнинг биткоинов, именно эти факторы способны определить финансовый результат — прибыль или убыток. Этот бизнес определенно прошел долгий путь со времен комнаты Джейсона Уэлана в студенческом общежитии.

«Гонка вооружений» в майнинге, заставившая компанию CoinTerra обосноваться в Солт-Лейк-Сити, полностью опровергла закон Мура, гласящий, что вычислительный ресурс микропроцессов удваивается каждые 18 месяцев. За 12 месяцев, предшествующих июню 2013 года, хешрейт биткоиновой сети увеличился в восемь раз. В следующие 12 месяцев этот показатель возрос в 845 раз. К этому моменту сеть, производившая 88 триллионов хешей в секунду, имела вычислительный ресурс, в 6000 раз превышающий совокупный ресурс 500 наиболее мощных суперкомпьютеров мира [3]. А всего 2,5 месяца спустя он почти утроился, достигнув 252 тысяч триллионов хешей. Мир никогда не знал таких темпов компьютерной экспансии. Способов расчета суммарной электроэнергии, потребляемой всей биткоиновой майнинговой сетью, не существует, но это не мешает заинтересованным лицам пытаться их отыскать. В апреле 2013 года в прессе появлялись статьи, где утверждалось, что биткоиновая сеть потребляет 131 тысячу мегаватт-часов в день, что обходится в 19,7 миллиона долларов [4]. Несколькими месяцами позже эколог из Австралии Гай Лейн предложил метод под названием BitCarbon, позволяющий количественно оценить экологические последствия биткоинового майнинга [5]. Если исходить из предположения о том, что 90% затрат на майнинг одного биткоина приходится на электроэнергию, то, по подсчетам Лейна, при курсе биткоина 1000 долларов за единицу его углеродный след составляет 8,2 миллиона тонн в год. Примерно такой же объем выбросов углекислого газа обеспечивает экономика Кипра. Если же курс биткоина достигнет 100 тысяч долларов за единицу, то его углеродный след составит 825 миллионов тонн выбросов в год, что равно углеродному следу, производимому экономикой Германии. Если же обменный курс биткоина когда-нибудь достигнет 1 миллиона долларов за единицу (в реальность этой цифры некоторые верят — конечно, при условии, что биткоин станет ведущей платежной системой мира), то его углеродный след составит 8,2 гигатонны, или 20% от общего объема выбросов углекислого газа в мире.

Однако у всех этих тревожных прогнозов есть один большой недостаток: все они основаны на непроверенных данных от Blockchain.info, которая до сих пор использует устаревшую информацию о расходе электроэнергии различными типами процессоров. В начале лета 2014 года новые майнинговые узлы на базе ASIC расходовали гораздо меньше электроэнергии — всего лишь 1 ватт при хешрейте гигахеш

в секунду. Это в 650 раз меньше, чем у графической карты. Если все майнеры перейдут на такие узлы, то сеть в целом будет потреблять столько же электроэнергии, сколько 7000 типичных американских домохозяйств: вполне умеренное количество, если учесть, что речь идет обо всем мире [6]. Конечно, майнеры используют как энергоэффективные, так и устаревшие майнинговые узлы. Пока еще это достаточно прибыльно. Поэтому несмотря на то, что суммарное потребление электроэнергии в биткоиновой сети существенно превышает потребление 7000 домохозяйств, речь уже не идет о том, что биткоиновая сеть увеличит расход электроэнергии в США вдвое.

Появляются и другие инновационные идеи по поводу того, как уменьшить затраты на электроэнергию. Одна из них состоит в том, чтобы использовать основной продукт повышенного энергопотребления — тепло — для отопления домов зимой и удовлетворения других энергетических потребностей. Но в настоящее время рассредоточенный характер сети не позволяет эффективно использовать этот ресурс. В идеале было бы хорошо организовать работу биткоиновой сети на сезонной основе: например, производственные мощности в Южном Гэмпшире могли бы взять на себя львиную долю нагрузки с июня по сентябрь, а Северный Гэмпшир принимал бы эстафету в зимние месяцы. Но при нынешнем принципе свободного рынка «победитель получает все» это невозможно. Поэтому летом 2014 года, когда биткоиновая сеть задействовала в 845 раз больший вычислительный ресурс, чем 12 месяцами ранее, и была плохо подготовлена к смене сезона, консультанты дата-центра рекомендовали майнерам обеспечить водонепроницаемость своих узлов и хранить их в специальной охлаждающей жидкости [7].

Насколько оправдан такой расход ресурсов и затраты? В XIX столетии по аналогичному поводу высказал свое мнение Адам Смит, заявив, что трата сил и ресурсов на добычу золота для чеканки монет не имеет смысла, если деньги представляют собой лишь символ [8]. Однако когда лауреат Нобелевской премии по экономике и колумнист газеты New York Times Пол Кругман пытается сослаться на эти слова Смита, чтобы высмеять сторонников биткоина, следует признать, что он упускает из виду несколько весьма важных факторов. Во-первых, стоимость потребленной электроэнергии необходимо сопоставлять с выгодой от верификации транзакций в платежной системе, а золото

никогда не выполняло эту функцию. Во-вторых, затраты на функционирование биткоиновой платежной системы нужно сравнивать с достаточно высокими затратами на функционирование традиционной денежной системы, включая содержание отделений банков, бронированных автомобилей и службы безопасности. И наконец, в-третьих, у новаторов есть важнейший стимул борьбы за эффективность — погоня за прибылью. Именно благодаря ей мы наблюдали такое колоссальное сокращение потребления электроэнергии новыми майнинговыми узлами. Если расходы на электроэнергию сделают майнинг неэффективным, люди прекратят им заниматься.

Таким образом, вряд ли можно ожидать скорого наступления экологического Судного дня для биткоина. Но даже если так, было бы безответственно игнорировать проблему расхода электроэнергии. Как подчеркивает Лейн из BitCarbon, возросшая экономичность новых майнинговых узлов прямо влияет на рост прибыльности, что вкупе с растущим курсом биткоина вовлекает все новых майнеров в гонку, а это, в свою очередь, приводит к дальнейшему росту потребления электроэнергии. И это один из многих факторов, которые делают биткоин уязвимым перед будущими угрозами и заставляют изобретателей рассматривать два варианта: либо совершенствование биткоина, либо разработку нового проекта криптовалюты.

Об одной такой уязвимости общественность внезапно узнала 11 марта 2013 года в 22 часа 27 минут по гринвичскому времени [9]. Непосредственно перед этим моментом, когда глобальная сеть майнеров напряженно трудилась, подтверждая транзакции и охотясь на биткоины, какой-то бдительный майнер заметил нечто странное. Один из майнинговых узлов в сети обрабатывал блок с более высоким номером, чем тот, который только что был зарегистрирован на сайте blockexplorer.com — примитивной версии Blockchain.info, где в режиме реального времени размещается информация о последних занесенных в книгу учета транзакциях. Это заставило майнера задуматься о том, какой же блок присоединился последним. Правильно ли его компьютер определил, к какому блоку следует присоединять сформированный им блок?

Программное обеспечение биткоина периодически обновляется небольшой группой программистов, которые по всеобщему согласию

и за небольшой гонорар от неприбыльной организации Bitcoin Foundation администрируют сервисную программу с открытым кодом. Вышеупомянутый майнер решил, что сбой случился из-за того, что он пытался заменить свою версию 0.7 биткоинового программного обеспечения более новой версией 0.8, совсем недавно выпущенной группой администраторов и уже установленной многими участниками сети. Поэтому он зашел на ветку разработчиков биткоина в сообществе пользователей системы групповых дискуссий в интернете на форуме Bitcoin. Появившись в чате под ником thermoman, позаимствованным у супергероя с планеты Ультрон из британского комедийного сериала, он отправил сообщение одному из пяти ведущих разработчиков, Питеру Вуилле (ник sipa), работающему под руководством ведущего специалиста Bitcoin Foundation Гэвина Андресена. Именно он отвечал за работоспособность базового программного обеспечения для биткоина. Thermoman сообщил sipa о несоответствии в номерах блоков в блокчейне. Завязалась дискуссия, в которую втянулись эксперты из группы разработчиков базовых программ с открытым кодом для биткоина.

Джоук Хофман (ник Jouke) из Нидерландов вклинился в разговор, заявив, что тоже сталкивался с расхождениями в номерах блоков. Тогда sipa предложил несколько вариантов разрешения проблемы, но ни один не сработал. В ходе беседы участники продолжали проверять номера блоков в блокчейне на разных сайтах. Расхождения продолжали появляться. В конце концов в 23:06 по гринвичскому времени разработчик программного обеспечения для майнинга Люк Дашжр (ник luke-jr) понял, что случилось.

23:06. Luke-jr: Итак??? Увы, случайное раздвоение блокчейна? :x

23:06. Jouke: Вот тебе и на!

Теоретически блокчейн должен быть только один. По идее, он последовательно формируется на основе хеш-связей, создающих неразрывную, монолитную запись всех подтвержденных транзакций. Время от времени в блокчейне появляются раздвоения: возникает брошенный блок — незавершенный или содержащий неподтвержденные транзакции. Другие майнеры стремятся верифицировать его, но иногда бывают не уверены в его легитимности и возможности присоединять к нему свои блоки. Но гениальность построенной на общем согласии биткоиновой системы состоит в том, что такие раздвоения не могут существовать долго. Ведь сообщество майнеров действует,

исходя из предположения о том, что легитимной считается самая длинная ветвь блокчейна. Большинство майнеров, работая совместно над конкретной ветвью блокчейна, подтверждают ее легитимность, поскольку в совокупности обладают бóльшим вычислительным ресурсом, чем меньшая часть их коллег, ошибочно (или даже из мошеннических соображений) продолжающая короткое ответвление цепи, не признаваемое большинством майнеров. Больший вычислительный ресурс означает, что обладающее им большинство майнеров будет выигрывать большее количество блоков монет и с течением времени построит более длинную цепь блокчейна (с более высокими номерами блоков). Этот факт сразу же заметят компьютеры, присоединяющие свои блоки к более короткой ветви цепи с более низкими номерами блоков. Эти «заблудившиеся» майнеры затем переключатся на более длинную ветвь цепи. Ведь блоки и транзакции считаются легитимными, только если их признает таковыми большинство майнеров. Но этот принцип может породить проблему, если один отдельно взятый майнер сосредоточит в своих руках более 50% вычислительного ресурса сети.

В данном случае эта стандартная процедура устранения расхождений не сработала. Обе ветви блокчейна продолжали расти. Это означало, что единого списка подтвержденных транзакций больше не существует. Представьте себе, что половина обитателей нашего воображаемого села на острове Яп вдруг решила пересмотреть балансы камней фэй, принадлежащих односельчанам, и внедрить свой вариант списка. Такой ситуацией могут воспользоваться мошенники, чтобы платить одними и теми же биткоинами дважды — например, если администратор майнингового пула, который отвечал, скажем, за верификацию 30% объединенного блокчейна, получал полный контроль над одной из двух ветвей и мог заставить электронные кошельки отправлять уже израсходованные биткоины друг другу.

Расчет делается на то, что другие майнеры признают эту транзакцию легитимной, равно как и баланс в кошельках, с которых эти биткоины уже давно списаны в результате предшествующих транзакций. Обычно большинство майнеров замечают эти манипуляции и переходят на более длинную легитимную ветвь блокчейна, но при неустраненном раздвоении блокчейна крупный пул майнеров, обладающий более чем 50% вычислительного ресурса, использует его для поддержания ошибочной ветви блокчейна, верифицируя мошеннические

транзакции. Если пустить ситуацию на самотек, можно разрушить целостность всей биткоиновой системы.

[196] Вуилле быстро понял, что конкретно это раздвоение вызвано отнюдь не действиями алчного хакера, а программным глюком, случившимся в результате внедрения его коллегами из группы администрирования новой версии 0.8 биткоиновой программы. Предполагалось, что ее реорганизованная база данных объединится с базой данных 0.7, но этого не произошло. Вскоре в дело вмешался ведущий разработчик Андресен. Проконсультировавшись с Вуилле и еще двумя базовыми разработчиками, Джеффом Гарзиком и Грегори Максвеллом, а также переговорив с владельцем биткоиновой биржи Mt. Gox, которая на тот момент была наиболее крупным финансовым учреждением биткоиновой сети, Марком Карпелесом (ник MagicalTux), Андресен решил отказаться от новой версии программного обеспечения 0.8 и вернуться к старой версии 0.7.

Был выявлен один случай «двойной траты» на сумму около 10 тысяч долларов, и это заставляет предположить, что нашелся по меньшей мере один негодяй, сумевший извлечь выгоду из общего хаоса [10]. Однако некоторые майнеры оказались перед необходимостью отказаться от биткоинов, которые они уже считали честно заработанными в результате эксплуатации версии 0.8. Общая сумма потерь достигала 600 монет и в пересчете на доллары составила около 26 тысяч. Вся эта суматоха привела к быстрому падению курса биткоина на 24%. Напугавший всех майнеров компьютерный глюк освещался в некоторых средствах массовой информации, интересующихся криптовалютной проблематикой, но в целом не привлек большого внимания — отчасти потому, что был очень оперативно устранен. Курс биткоина также достаточно быстро вернулся на прежний уровень.

Раздвоение блокчейна в 2013 году было случайным, но оно оживило опасения некоторых членов биткоинового сообщества относительно того, что перевод майнинга биткоинов на промышленные рельсы в один прекрасный день приведет к появлению возможности преднамеренного раздвоения блокчейна каким-нибудь бесчестным майнером. Для этого ему достаточно захватить контроль над совокупным вычислительным ресурсом. Такая ситуация получила название «атаки 51%». В своей знаменитой статье Накамото утверждал, что

биткоиновая майнинговая сеть способна гарантировать справедливую и честную обработку транзакций до тех пор, пока ни один из майнеров или майнинговых пулов не сосредоточил в своих руках более 50% совокупного вычислительного ресурса. Если злонамеренные игроки тайно создадут альтернативную ветвь блокчейна из мошеннических транзакций, чтобы тратить биткоины, которые им не принадлежат, их усилия по получению одобрения этих транзакций не увенчаются успехом, если в их распоряжении не будет большей части совокупного вычислительного ресурса. Вероятность того, что нечистоплотные майнеры будут решать достаточно много математических задач, чтобы суметь построить более длинную ветвь блокчейна и тем самым легитимизировать свои мошеннические транзакции, быстро устремится к нулю. Следовательно, им никогда не удастся потратить полученные таким образом биткоины. Плохим парням никогда не победить — по крайней мере теоретически.

Но что случится, если мощный конгломерат майнинговых пулов сосредоточит-таки в своих руках достаточный вычислительный ресурс? Он сможет сформировать блок мошеннических транзакций, а затем не менее мошенническим путем верифицировать его. А поскольку они будут выигрывать больше половины блоков, то смогут удлинять незаконную ветвь блокчейна, которую другие майнеры сочтут легитимной только потому, что она окажется наиболее длинной.

Сайт coinometrics.com утверждает, что летом 2014 года стоимость майнингового оборудования и электроэнергии, необходимой для организации «атаки 51%», достигла 913 миллионов долларов [11]. Это очень дорогостоящая затея, но существует способ сократить затраты: объединение в майнинговые пулы. По сути дела, майнинговые пулы вплотную подошли к отметке в 50% вычислительного ресурса — в июне 2014 года пул GHash.IO обнаружил, что его доля в совокупном вычислительном ресурсе в течение месяца колеблется между 40 и 50% [12]. Поскольку каждый пул использует свои хешинговые возможности консолидированно, то и подтверждать транзакции он может как единая группа. В результате вся его вычислительная мощь оказывается в руках администраторов программного обеспечения пула, и это вызывает понятное беспокойство в среде биткойнеров. Такие лидеры биткоинового сообщества, как тот же Андресен, пытаются побудить людей присоединяться к новым одноранговым пулам, которые

через децентрализованную сеть передают полномочия подтверждения достоверности транзакций отдельным майнерам, отобрав их у администраторов пулов. Но в крупнейших пулах, как правило, существует авторитетный лидер-основатель, и лишить его полномочий очень сложно. Более того, менеджер пула GHash.IO под ником CEX.IO предлагает весьма привлекательные условия с нулевыми комиссионными, пытаясь сохранить и развить оба направления бизнеса своей компании: обмен криптовалют и услуги облачного майнинга.

Но и это еще не все плохие новости: ученые-компьютерщики из Корнеллского университета Иттай Эйал и Эмин Гюн Сирер недавно продемонстрировали, что минимальная доля вычислительного ресурса, достаточная для такой атаки, составляет даже менее 51%. В дискуссионной по характеру статье они показали, как меньшинство действующих заодно майнеров могут с успехом заниматься майнингом для личной выгоды, формируя секретную альтернативную ветвь блокчейна, неизвестную большинству участников [13]. При этом она растет быстрее, чем легальная ветвь добросовестных майнеров. Таким способом они заставляют остальных майнеров впустую тратить компьютерный ресурс на фальшивую ветвь, выигрывая больше биткоиновых монет, чем по справедливости приходилось бы на их долю, исходя из объема их вычислительного ресурса. Эта статья обескуражила многих в биткоиновом сообществе и в первую очередь, как сказал Сирер, «...наиболее горячих энтузиастов, которые и слышать не хотели ничего плохого о биткоине» [14]. Однако затем один энтузиаст биткоина, стремясь доказать ошибочность этой концепции, смоделировал ситуацию и выяснил, что Эйал и Сирер правы. После этого шум начал стихать. «Люди успокоились, а наиболее заинтересованные (вроде нас), видя, что биткоин выдержал испытание, пришли к выводу, что это был очень полезный опыт. Теперь люди понимают, что в условиях децентрализованной системы необходимо иметь встроенный в нее механизм поддержания равновесия, — говорит Сирер. — В протоколе не должно быть таких уязвимостей».

Таким образом, сообщество программистов, работающее с программами с открытым кодом, в настоящее время занято поисками дополнительных мер защиты от «эгоистичного майнинга» и «атаки 51%». Честно говоря, никаких мошеннических проделок с тех пор не было, и не похоже, чтобы они случились — по вполне убедительной причине.

Как писал Накамото, «...если какой-нибудь энергичный мошенник сумеет аккумулировать больше вычислительного ресурса, чем все добропорядочные майнеры, перед ним встанет выбор: использовать его в мошеннических целях, повторно тратя свои биткоины, или генерировать с его помощью новые монеты. Вполне возможно, он решит, что играть по правилам гораздо выгоднее: это принесет ему больше монет, чем всякие трюки, не говоря уже о том, что трюки могут подорвать всю систему и обрушить его благосостояние» [15].

Иными словами, здоровый эгоизм не позволит кому-то, кто задействован в биткоиновой системе, уничтожить ее. По сути, пока еще короткая история биткоина показывает, что аналогичными мотивами руководствуются маломощные майнеры: им тоже выгодно поддерживать равновесие в сети. Некоторые члены майнинговых пулов, вычислительный ресурс которых приближался к показателю 50%, выходили из их состава и присоединялись к конкурирующим пулам только ради поддержания принципов справедливости. Чтобы успокоить опасения относительно слишком большой концентрации вычислительного ресурса, CEX.IO периодически заявлял о том, что его майнинговый пул GHash.IO ограничит прием новых членов [16].

Но что, если плохие парни не заинтересованы в развитии и процветании биткоина? Что, если вся их мотивация сводится к обрушению устоявшейся системы, а не к получению прибылей от инвестиций в биткоиновый бизнес? Биткойнеры иногда называют это «атакой Доктора Зло», но отвергают наиболее часто встречающиеся примеры таких атак: террористическая организация, решившая ввергнуть западный мир в хаос; суверенная нация, возможно, Россия или Китай, чьей денежной системе угрожает биткоин; консорциум мультинациональных банков, стремящихся защитить свою монополию на платежную систему. При внимательном рассмотрении все эти угрозы выглядят как маловероятные. В итоге реализация всех этих сценариев возможна только в случае глубокой интеграции биткоина в традиционную систему, когда его катастрофа отразится и на ней. Но к тому времени расходы потенциальных злоумышленников будут намного превышать 1 миллиард долларов на каждый заказ на специализированные микросхемы ASIC и майнинговое оборудование, что, несомненно, привлечет к ним внимание. Тем не менее такая уязвимость существует. Фактически биткоин не имеет абсолютной защиты, и этот факт мог бы

обеспокоить сверхосторожного корпоративного юриста, решающего, стоит ли компании связываться с этой криптовалютой.

Однако не только эти экстремальные сценарии вызывают опасения, что концентрация технической и финансовой мощи окажет неблагоприятное влияние на биткоин. По данным сайта bitcoinrichlist.com, на конец августа 2014 года 44% биткоинов, находящихся в обращении, числились всего лишь за 1528 электронными адресами, причем на каждом из них находилось более 1000 биткоинов (или 507 тысяч долларов) [17]. Это менее 0,01% от общего количества в 40,7 миллиона электронных адресов в биткоиновой сети на тот момент. Отсюда вывод: мы имеем дело с очень высокой и потенциально опасной неравномерностью распределения активов.

Давайте подробнее рассмотрим этот факт. Для характеристики неравномерности распределения активов этот показатель не подходит. Во-первых, следует отметить, что электронный адрес и электронный кошелек — это не одно и то же. Общее количество кошельков неизвестно, но их по определению должно быть меньше, чем адресов, несмотря на то что многие имеют более одного кошелька. Их владельцам в произвольном порядке выделяются электронные адреса для различных транзакций, поэтому их оказывается больше одного. Баланс значительной части из 39 миллионов адресов, находящихся в 96 нижних процентилях списка сайта bitcoinrichlist.com, составляет менее 0,001 биткоина. Эти адреса не что иное, как «мелкая сдача», то есть адреса, которые биткоиновый протокол присваивает плательщикам при каждой транзакции как часть своей уникальной трехсторонней процедуры согласования балансов. Даже если многие мелкие суммы на адресах переводятся в кошельки с небольшой суммой, все равно вряд ли это основное хранилище активов биткойнеров. Большинство из них хранят основную часть своего состояния в традиционных бумажных деньгах. Эту группу владельцев адресов в нижних 96 процентилях списка bitcoinrichlist.com ни в коем случае нельзя считать люмпен-пролетариями.

Тем не менее эти цифры дают представление о том, как быстрый рост курса биткоина создал немногочисленную группу богатых «биткоиновых баронов» чуть ли не за одну ночь. Ее влияние на биткоиновую экономику несоразмерно велико. Эта группа очень заинтересована в успехе биткоина, а также имеет возможность и желание проводить недоступные другим платежи просто ради популяризации

идеи криптовалюты в обществе. Отсюда проистекают сообщения о демонстративных покупках за биткоины вилл на Бали, автомобилей Lamborghini в Калифорнии и билетов на полеты в космос от компании Virgin Galactica [18]. Возможно, они руководствуются благими намерениями, но если деньги для них не имеют никакого значения и они готовы швырять их направо и налево, то как они смогут соблюдать платежную дисциплину, необходимую для того, чтобы снизить курс биткоина в целях оздоровления биткоиновой экономики?

Большой разрыв в уровне благосостояния негативно сказывается на имидже криптовалют как «народных денег» и способа выхода из-под контроля «жирных котов» с Уолл-стрит. Власть и материальное благополучие, зависящие от узкого круга избранных, отнюдь не вызывают доверия у общественности. Конечно, экономика доллара, евро и иены тоже отличается большой концентрацией власти и финансов, а разрыв между бедными и богатыми в ней достиг уровня 1920-х годов. Но эти традиционные валюты не нуждаются в привлечении общественности на свою сторону. А криптовалютам следует предложить решение этих задач, иначе у них не будет будущего.

Однако есть и хорошие новости: многие разработчики и бизнесмены реализуют проекты, ориентированные на устранение этих опасений. Некоторые опираются на уже существующую инфраструктуру и ищут способы обеспечить доступ к ней для более широких групп населения. Они продвигают биткоин в качестве средства расширения возможностей самых обездоленных слоев населения. Предлагаются решения, позволяющие лишенным доступа к банковскому обслуживанию людям найти свое место в глобальной экономике (более подробно мы рассмотрим эти решения в главе 8). Но не менее важно, чтобы многие продвинутые энтузиасты криптовалют осознали тот факт, что в своем нынешнем виде биткоин далек от идеала и его можно усовершенствовать, устранив некоторые из описанных выше проблем и угроз.

Угроза «атаки 51%» привлекает внимание множества интеллектуалов в области биткоина. Почему? Потому что она представляет собой единственную неопровержимую структурную уязвимость в биткоиновой системе. Все остальные угрозы, о которых вы слышали — взломанные кошельки, преступления и волатильность курса, — это проблемы, связанные не с самим по себе биткоином, а, скорее, со сложившейся

вокруг него экосистемой. Многие из этих проблем уже решены: электронные кошельки с мультиподписью, предлагаемые инновационными фирмами вроде BitGo, обеспечивают практически абсолютную защиту от хакеров; высокотехнологичные, регулируемые биткоиновые биржи наподобие Atlas ATS, вероятно, уже не повторят ошибок, совершенных Mt. Gox; более жесткое государственное регулирование предотвратит (или как минимум ограничит) появление на бирже торговцев наркотиками [19]. Но трудно найти какой-то способ противодействия «атаке 51%». Даже если проблемы организации и затраты, связанные с проведением такой атаки, делают ее маловероятной, все равно специалисты, изучавшие биткоиновую систему, беспокоятся по поводу того, что элегантный, блестящий проект Накамото по объединению интересов и стимулов индивидуумов с интересами и стимулами общества в целом подвержен этой угрозе.

Один из ключевых разработчиков биткоинового программного обеспечения Джефф Гарзик — один из тех пяти человек, которые работали непосредственно с Гэвином Андресеном, — предложил частичное решение, основанное на неизменном преимуществе низкозатратных приватных стартапов [20]. Он старается мобилизовать 2 миллиона долларов на запуск в космос целого флота миниатюрных низкозатратных спутников, чтобы сделать майнинговую сеть менее централизованной. Эти «бит-спутники» объемом всего лишь в 10 кубических сантиметров предоставят недорогую спутниковую интернет-связь майнинговым узлам, а также будут постоянно сохранять полную запись блокчейна на своих внутренних жестких дисках. Теоретически это может обеспечить двойные преимущества. Во-первых, майнинг станет более доступным широкому кругу биткойнеров благодаря снижению затрат на создание так называемого полного узла, играющего в сети очень важную роль. Он должен сохранять огромный объем данных, и эта функция в настоящее время выполняется мощными и дорогими чипами ASIC. Во-вторых, поскольку спутники не поддаются контролю индивидуумов, государств или компаний, они могут обеспечить критически важное резервирование информации в случае отключения крупного провайдера интернет-услуг или их кластера. Такой форс-мажор, возможно, спровоцированный решением правительства одной страны или ряда стран, приведет к отключению множества майнеров от сети, а значит, возрастет риск того, что мощный майнинговый пул,

находящийся вне отключенной территории, сможет сосредоточить в своих руках более 50% вычислительной мощности. Альтернативный, расположенный в космосе источник интернета с большой пропускной способностью может снизить риск этих нежелательных последствий.

Однако концентрация вычислительного ресурса имеет гораздо менее капиталоемкую альтернативу — пересмотреть правила, которым следуют майнеры, зарабатывая биткоины, и устранить мотивы к аккумулированию вычислительного ресурса. Инженеры по вычислительной технике в сфере криптовалют, рассматривающие возможность реализации подобных проектов, скорее всего, будут играть ведущую роль в определении будущего биткоиновой технологии. Возможно, именно их идеи в один прекрасный день дадут такой импульс развитию биткоиновой денежной системы, что она станет главным драйвером будущего биткоиновой технологии в целом.

Недостатки биткоина стараются преодолеть путем развития альтернативных криптовалют, например альткоина. Как упоминалось в главе 3, в настоящее время существует уже несколько сотен этих имитаторов биткоина. Многие из них не имеют будущего, поскольку внедрялись ради быстрого обогащения или просто ради шутки. Однако есть и такие, которые предлагают прогрессивные пути изменения правил игры в области распределения криптовалюты в сообществах пользователей. Их основатели рекламируют свои проекты как более справедливые и устойчивые. Они заявляют о необходимости позаимствовать у биткоина все лучшие свойства децентрализованной структуры, но при этом избавиться от его недостатков, в том числе «гонки вооружений», избыточного потребления электроэнергии, стремления к промышленной концентрации вычислительного ресурса. Биткоин имеет большое преимущество первопроходца по сравнению с новыми игроками на этом поле, поэтому многие разработчики считают, что лучше устранить его недостатки, чем заниматься разработкой совершенно новых платежных систем. Тем не менее лучшие образцы альтернативных криптовалют создают острую и потенциально конструктивную конкуренцию биткоину, что способствует развитию криптовалют в целом.

Наиболее успешной из всех альтернативных криптовалют на сегодня следует признать лайткоин, изобретенный Чарли Ли [21]. Секрет успеха лайткоина заключается в другом алгоритме процесса хеширования, используемом майнерами для монтирования транзакций

в блокчейн. Кроме того, система Ли предусматривает конкуренцию среди майнеров, но ее методика хеширования, известная как алгоритм, облегчает майнерам достижение хешинговых целей по сравнению с биткоиновой функцией SHA-256. Не углубляясь в сложные проблемы функционирования системы лайткоина, отметим, что алгоритм существенно видоизменяет цели, не позволяя майнерам получать преимущество исключительно за счет постоянного наращивания вычислительного ресурса. В результате вычислительный ресурс лайткоина распределяется более или менее произвольно и более демократично. У майнеров остаются стимулы стремиться получить вознаграждение в монетах, но «гонка вооружений» и расход электричества не настолько интенсивны, как в случае с биткоином. Ускоряется процесс формирования и верификации блоков: на это уходит примерно 2,5 минуты, в то время как формирование блока биткоинов занимает около 10 минут. Это означает, что продавцы и покупатели тратят меньше времени на ожидание окончательного подтверждения транзакции. Главную уязвимость лайткоина рассматривают как продолжение его сильных сторон: поскольку майнинг лайткоинов обходится дешевле, а функционирующие на основе алгоритма майнинговые узлы могут добывать и другие криптовалюты, основанные на том же принципе, например догкойны, майнеры не так сильно заняты постоянной работой по формированию блокчейна. Это может повышать риск «атаки 51%», если в сети одновременно не будет находиться достаточно майнеров. Некоторых специалистов беспокоит, что майнинг валюты на основе алгоритма менее защищен, «доказательства работы» менее надежны, и теоретически это допускает проникновение в блокчейн фальшивых транзакций с некорректным подтверждением. Однако до настоящего момента лайткоину удавалось избегать крупных провалов. Со временем он сможет стать более безопасным в экологическом плане и демократичным конкурентом биткоина.

Майнинг на основе алгоритма — это не единственное решение для децентрализации майнинга биткоина и предотвращения «атаки 51%». Некоторые альтернативные криптовалюты, в том числе некстоины и пиркоины, используют «доказательство доли» вместо «доказательства работы», требующего ресурсоемкого и затратного вычислительного процесса. Таким образом, право вашего компьютера на получение вознаграждения тем больше, чем больше вы инвестируете в предложение

денег. Если говорить о некстkоине, который полностью основан на «доказательстве доли», то там монеты не добываются, а «зарабатываются» на комиссиях [22]. В некстkоиновой экономике обращается лимитированное количество монет, ежедневно используемых в транзакциях. Они генерируют комиссионные за совершение транзакций, перечисляемые узлу, который выпустил последний блок. Как и в случае с биткоином, корректный хеш для «запечатывания» блока транзакций выявляется в результате случайного перебора, но, в отличие от биткоина, ваши шансы выиграть в эту лотерею зависят не от вычислительного ресурса, а от количества подтвержденных монет на вашем счету. Идея состоит в том, что это устраняет стимулы к наращиванию экологически небезопасного и экономически затратного вычислительного ресурса.

Существование альтернативных криптовалют помогает осознать недостатки биткоина. Но у творения Накамото есть и другие проблемы. В частности, одна биткоиновая сеть одномоментно может обрабатывать около семи транзакций в секунду — ничтожно мало по сравнению с 10 тысячами транзакций в секунду у компании Visa. Если биткоин собирается выходить на новый уровень, то его придется модифицировать таким образом, чтобы майнинговые узлы, ныне лимитированные одним мегабайтом данных на десятиминутный блок, могли обрабатывать гораздо больший объем информации. Технически этого несложно добиться, майнерам придется хешировать более крупные блоки транзакций, не получая существенного прироста вознаграждения. Разработчики сейчас анализируют модель вознаграждения, основанную исключительно на комиссионных за транзакции, поскольку она обеспечивает более справедливое распределение вознаграждений, если объем информации становится слишком большим.

Основанный на открытом коде биткоин конструктивно взаимодействует с альтернативными криптовалютами, и в этом его большое преимущество. До настоящего времени все возникавшие проблемы — от мошенничества на крупнейших биржах до раздвоения блокчейна или багов в программном обеспечении — решались на основе консенсуса биткоинового сообщества, то есть наиболее справедливым образом из всех возможных. Тем не менее эти проблемы *остаются* весьма серьезными. Разработчики криптовалютных проектов трудятся на стыке экономики (подчеркивается стимулирование такого поведения

индивидуума, которое приносило бы пользу сообществу в целом) и технологии. Создатели компьютерных систем в таких компаниях, как SAP и IBM, концентрируются на похожих проблемах поиска баланса между поведением и технологиями, но они работают в контролируемых и централизованных средах своих корпоративных клиентов. В противоположность этому лаборатория, которой пользуются разработчики криптовалют, представляет собой весь мир и включает все человечество, на благо которого они действуют. Никакие корпоративные правила или сборник инструкций, обязательный на всех уровнях управления, не увязывают выбор отдельных индивидуумов с общими целями корпорации. Стимулирование оптимального поведения людей полностью зависит от того, насколько дизайн программы влияет на их образ мышления и насколько удачная система стимулов в него заложена.

Уязвимости и недостатки, описанные в этой главе, неизбежно мешают формированию у обычных людей доверия к криптовалютам — по иронии судьбы, мы говорим это о криптовалюте, которая сама была создана для того, чтобы избежать необходимости в таком доверии. Однако при этом не следует забывать, что уязвимости и недостатки свойственны и традиционным денежным системам. Вспомните, сколько преступлений и мошеннических сделок связано, например, с долларами. А если задуматься над уязвимостями финансовой системы, то следует вспомнить о глобальном рынке финансовых деривативов, которым продолжают управлять банки, невзирая на кризис, спровоцированный в 2008 году этим «финансовым оружием массового разрушения», как называл их Уоррен Баффетт [23]. Номинальная, или учетная, стоимость ценных бумаг, обращающихся на этом рынке, составляет 710 триллионов долларов.

Очень важно помнить, что над решением проблем, связанных с биткоином и прочими криптовалютами, трудится коллективный интеллект невиданной мощи. Имея открытый код и децентрализованную модель, эти технологии не подвержены ограничениям, с которыми сталкиваются бюрократические организации и неповоротливые гигантские корпорации. В сфере криптовалют появляется невероятное количество инноваций, причем касающихся не только обеспечения их безопасности, но и поиска путей того, как сделать их более полезными для общества. В следующей главе мы поговорим о молодых изобретателях, создающих эти инновации.

Глава

7

Мельница Сатоши

Человек проверяет пробу золота, а золото — пробу человека.

Томас Фуллер

издательство
МАНН, ИВАНОВ И ФЕРБЕР
Максимально полезные книги