

Блокчейн-анализ рынка биткоинов. (Часть 3)

Игорь Макаров¹, Антуанетта Шоар²

¹Лондонская школа экономики Houghton Street Лондон WC2A 2AE
Соединённое Королевство, i.makarov@lse.ac.uk

²Школа менеджмента MIT Sloan School of management 100 Main Street,
E62-638 Кембридж, Массачусетс 02142 и NBER, aschoar@mit.edu

Аннотация. В настоящей статье представлен подробный анализ сети Биткоин (Bitcoin) и её основных участников, проведённый авторитетными специалистами – Игорем Макаровым из Лондонской школы экономики и Антуанеттой Шоар из Массачусетского технологического института по поручению Национального бюро экономических исследований (NBER) – частной организации в США. Сеть Биткоин детерминируется как новая база данных, включающая большое количество общедоступных и проприетарных источников для связывания адресов биткоинов с реальными объектами и обширный набор алгоритмов для извлечения информации о поведении основных участников рынка. Анализ экосистемы Биткоин состоял из трёх основных этапов. Во-первых, проанализированы объём транзакций и сетевая структура основных участников блокчейна. Во-вторых, задокументированы концентрация и региональный состав майнеров, которые осуществляют проверку (верификацию) и обеспечивают целостность реестра блокчейна (гроссбуха, леджера). В-третьих, рассмотрена концентрация собственности крупнейших держателей биткоинов. Установлено, что владельцами трети всех выпущенных биткоинов являются 10 тыс. индивидуальных инвесторов. Делается вывод, что высокая концентрация делает рынок первой в мире криптовалюты уязвимым перед гипотетической атакой хакеров.

Переводчик статьи отмечает, что переложение текста с английского языка [1] на русский было весьма затруднительным в связи с новизной финансовой тематики и широким использованием его авторами распространённого на Западе, однако нового для нас термина entity (сущность). Несмотря на данный факт, представляется необходимым ознакомить читателей с технологией биткоинов, что будет иметь практическую пользу для библиотечно-информационного сообщества.

Ключевые слова: криптовалюта, биткоин, блокчейн, транзакции, майнеры, концентрация собственности

Для цитирования: Макаров И., Шоар А. Блокчейн-анализ рынка биткоинов. (Часть 3) / И. Макаров, А. Шоар // Научные и технические библиотеки. 2022. № 11. С. 135–152. <https://doi.org/10.33186/1027-3689-2022-11-135-152>

4. Майнеры

Майнеры являются основой процесса проверки блокчейна Биткоин. Их роль заключается в осуществлении, обработке и проверке транзакций биткоинов, при этом решаются трудные вычислительные проблемы. За эту услугу майнеры получают вознаграждение в виде вновь созданных биткоинов и комиссий за транзакции.

Протокол доказательства работы, такой как Биткоин, требует честности и ведения учёта от децентрализованных майнеров. Если один или группа сговорившихся майнеров станут управлять большей частью майнинговых мощностей в сети, бухгалтерская книга может оказаться под их контролем, что может привести к печально известной «атаке 51%», когда группа изменила ранее проверенные записи.

Важно понимать, насколько распределены или, наоборот, сконцентрированы майнинговые мощности. Обсуждение этого вопроса в существующей литературе сосредоточено вокруг концентрации майнинговых пулов. По замыслу, вероятность добычи блока и получение вознаграждения за блок в цепочке блоков Биткоин пропорциональны мощности хеширования, затрачиваемой на майнинг. Это создаёт мощные стимулы для майнеров, которые объединяют свои вычислительные мощности и страхуют друг друга. Как следствие, в блокчейне Биткоин доминируют пулы для майнинга.

На рис. 9 (оригинал рисунка здесь: https://www.nber.org/system/files/working_papers/w29396/w29396.pdf) показано, как с течением времени изменяются доли майнингового пула. В майнинге доминирует несколько пулов. Шесть крупнейших зарегистрированы в Китае. Они имеют прочные связи с влиятельной компанией Bitmain Techno-

logies, производителем оборудования для майнинга биткоинов (Ferreira et al. (2019)). Единственным крупным, не китайским пулом является SlushPool (Чехия).

Пулы функционируют как агрегаторы хеш-ёмкости и, следовательно, могут существенно влиять на протокол Биткоин. При этом они не обязательно контролируют своих майнеров. Как подчёркивают Cong et al. (2020a), власть оператора пула над майнерами зависит от лёгкости, с которой они перемещают мощность между пулами, что, в свою очередь, зависит от распределения майнеров по размеру. Последнее влияет и на системный риск биткоинов. Чем выше концентрация майнинга, тем легче разрушить или захватить его мощность путём атаки нескольких майнеров.

Информация о пулах для майнинга общедоступна, информация об отдельных майнерах недоступна¹.

Поскольку каждый пул распределяет вознаграждения по своему алгоритму, мы воссоздали различные алгоритмы, отражающие динамику распределения. Это сложный процесс, так как пулы по-разному организуют свои протоколы распределения и часто накапливают вознаграждения перед отправкой майнерам на адреса нескольких уровней. В табл. 1 указано количество блоков и количество биткоинов, добытых каждым пулом за период 2015–2021 гг. Мы отслеживаем самые крупные пулы, выделенные жирным шрифтом. Частные пулы выделены курсивом.

Мы отслеживаем 20 крупнейших пулов, кроме четырёх китайских, тесно интегрированных с соответствующими биржами – BTCC Pool, VixIn, Huobi Pool и OKExPool. В частности, их адреса распространения хранятся на этих биржах, что затрудняет отслеживание отдельных майнеров. Из отслеживаемых пулов Bitfury и Lubican относятся к частным, которые мы рассматриваем как отдельные объекты. Это первое исследование, которое точно связывает майнеров с их пулами для майнинга.

¹ Майнеры часто используют файл scriptSig, чтобы включить имя своего пула для майнинга в базу, которая позволяет распределять вознаграждения по пулам. Мы используем данные транзакций из блокчейна Биткоин для отслеживания вознаграждений за майнинг из разных пулов к майнерам, которые с ними работают.

Сводная статистика майнинговых пулов

Pool name	bitcoins mined	blocks mined
AntPool	876,845	53,535
F2Pool	840,083	51,701
BTC.com	425,200	35,095
BTCC	353,253	17,719
<i>BitFury</i>	351,880	18,185
SlushPool	320,982	21,657
ViaBTC	258,443	21,302
BWPool	250,044	12,733
BTC.TOP	222,190	17,039
Poolin	209,018	19,833
KnCMiner	109,923	4,466
Huobi Pool	86,571	9,044
Bixin	80,682	5,778
GHash.IO	47,644	1,912
1THash	42,711	4,780
Eligius	41,002	1,650
OKExPool	40,241	3,957
Binance Pool	32,395	4,683
BTC Guild	24,731	985
WAYI.CN	17,486	1,465
<i>Lubian.com</i>	13,279	1,783
BytePool	12,712	1,002
BATPOOL	6,266	441
SpiderPool	4,367	493
tigerpool.net	3,629	285
Sigmapool.com	2,204	217

Некоторые майнеры предпочитают получать вознаграждения, используя личные (частные) кошельки, а некоторые – отправляют свои вознаграждения непосредственно на учётные записи с помощью биржевых служб или онлайн-кошелька.

Первый тип мы называем майнером частного кошелька, а второй – майнером биржевого кошелька. Мы различаем майнеров с частным и обменным кошельками. Мы можем более точно определить размер деятельности майнера с частным кошельком, так как можем назначать одному майнеру разные адреса майнинга, принадлежащие одному и тому же кластеру. При этом мы не можем сгруппировать разные адреса майнера биржевого кошелька, поэтому относимся к каждому биржевому адресу майнинга как к отдельному майнеру. В результате мы можем предоставить только более низкую привязку к размеру этих майнеров биржевых кошельков, поскольку данная организация может контролировать несколько адресов.

Чтобы отделить майнеров с частным кошельком от майнеров с биржевым кошельком, в первую очередь проверяем, принадлежит ли адрес майнера известной бирже или учреждению. Поскольку в наших данных могут отсутствовать некоторые биржи или внебиржевые торговые площадки, мы учитываем все адреса майнеров, которым принадлежат подозрительно большие кластеры, как кластеры биржевого кошелька. Это кластеры, которые состоят из множества адресов, получают большое количество неотслеживаемых до майнинга биткоинов, имеют в качестве членов много адресов для майнинга. Это означает, что мы консервативны в оценках при определении размера майнера.

На следующем этапе мы отсеиваем те объекты, которые получают нерегулярные вознаграждения, получили менее тысячи долларов или менее 25-кратного вознаграждения за время своего существования. Мы вручную проверили 150 крупнейших майнеров независимых кошельков на вознаграждение в долларах США, чтобы убедиться, что мы не принимаем адреса перераспределения за майнеров. После применения этих фильтров получено 105 494 адреса кластеров частных кошельков и 137 656 адресов биржевых кошельков. Адреса биржевых кошельков принадлежат 305 известным биржам и онлайн-кошелькам и 284 неизвестным кластерам. Поскольку вознаграждение майнера пропорционально его майнинговым возможностям, мы измеряем мощ-

ность каждого майнера как количество биткоинов, которые отправляются пулами через транзакции распределения вознаграждений².

Наш алгоритм фиксирует мощность майнинга в биткоинах блокчейн с января 2015 г. до начала 2021 г. как часть всей Coinbase-награды, доступной на данной неделе (рис. 10, оригинал рисунка здесь: https://www.nber.org/system/files/working_papers/w29396/w29396.pdf).

Синяя линия обозначает вознаграждения пулов, которые можно отследить. Эти данные получены из публичной информации от майнинговых пулов на агрегированном уровне. В начале выборки наши пулы получают около 60% вознаграждений за майнинг, а в конце это число близко к 90%. Красная линия – это распределённые вознаграждения за майнинг, которые можно отследить в блокчейне от адреса распределения пула до базовых майнеров (около 90% вознаграждений). Зелёная линия демонстрирует вознаграждения, собранные майнерами биржевого кошелька. В целом, майнеры с биржевым кошельком и частным кошельком курируют почти половину общей мощности.

4.1. Концентрация майнинговых мощностей

Мы анализируем концентрацию майнинговых мощностей у отдельных майнеров. Каждый месяц активные майнеры сортируются по размеру и подсчитывается, какой процент от общей мощности майнинга контролируется разными квантилями. Результаты для лучших 50%, 10%, 5%, 0,5% и 0,1% майнеров представлены на левой панели рис. 11 (оригинал рисунка здесь: https://www.nber.org/system/files/working_papers/w29396/w29396.pdf).

Заметно, что майнинг биткоинов сконцентрирован, а концентрация майнинговых мощностей относительно стабильна во времени. Половина лучших майнеров контролирует почти все майнинговые мощности, лучшие 10% контролируют 90% мощности и всего 0,1% – около половины мощности.

² Пулы различаются по сумме, которую они взимают с майнеров, и схемам выплат, см. Cong et al. (2020a). Поскольку пулы конкурируют друг с другом, мы ожидаем, что эти различия несущественно повлияют на измерение мощности майнеров.

Затем мы рассчитали количество майнеров, необходимое для покрытия 10, 20%, 30%, 40% или 50% от общей мощности майнинга. На правой панели рис. 11 показано, что для порога в 50%, представляющего особый интерес из-за опасности «атаки 51%», в период с 2015 г. по 2017 г. обычно требовалось менее 50 майнеров. В начале 2018 г. количество майнеров увеличилось до 250, а к концу 2020 г. их снова стало менее 50. Можно предположить, что остальные пулы имеют аналогичную концентрацию. К концу 2020 г. мы отслеживали около 90% мощности майнингового пула. Согласно нашим наблюдениям в конце 2020 г. 55–60 майнеров из числа крупнейших контролировали как минимум половину всех мощностей по добыче биткоинов. На рис. 11 справа также показано, что концентрация майнинговых мощностей антициклическая. Она уменьшается после резкого роста цены биткоинов и увеличивается в периоды, когда цена падает, например, в 2018 г.

Кроме того, концентрация увеличивается после «уполовинивания» биткоинов – даты, когда вознаграждение за блок уменьшается вдвое (в нашей выборке это июль 2016 г. и май 2020 г.). Эти результаты говорят о том, что набор крупных майнеров относительно стабилен, а в ответ на ценовые шоки приходят и уходят мелкие майнеры. Таким образом, риск «атаки 51%» увеличивается в несколько раз, когда цена биткоина резко падает или «уполовинивается».

4.2. Географическая концентрация майнеров

Другая область интересов – географическое распределение майнеров. Фактически контроль над большей частью майнинговых мощностей означает контроль над криптовалютой. Географическая концентрация увеличивает риск того, что частный или государственный субъект в одной части мира может получить контроль над сетью и нанести большие убытки общественности и финансовым учреждениям, если они держат биткоины.

Определить географическое распределение майнеров – непростая задача. Пока что основные данные извлекаются из анализа IP-адресов майнеров.

При подключении майнера к серверу пула оператор пула может видеть IP-адрес майнера. Если майнер не использует VPN-адрес,

оператор может использовать этот IP-адрес для определения географического положения³.

В этой статье мы используем новый подход, с учётом наших возможностей для отслеживания майнеров на блокчейне. Поскольку мы можем наблюдать адреса майнеров на блокчейне, мы видим, на каких биржах они обналичивают свои вознаграждения. Можно предположить, майнеры из определённого региона, скорее всего, отправят свои вознаграждения на биржу, которая преобладает в этом регионе. Изучая, на какие биржи отправляют майнеры свои вознаграждения, мы можем сделать вывод об их местонахождении.

У нашего метода есть несколько преимуществ перед существующими. Во-первых, мы можем охватить большинство из множества майнеров, а не только несколько избранных пулов. Во-вторых, наш метод может дать более точную картину, чем использование IP-адресов, особенно для майнеров, работающих в тех странах, где майнинг запрещён. В таких странах майнеры могут намеренно скрывать своё местоположение или дать указание пулам не раскрывать их местоположение из-за боязни раскрытия информации местным властям или регулирующим органам.

Одним из недостатков нашего подхода является то, что некоторые биржи не привязаны к региону, а работают во многих юрисдикциях. Поскольку майнеры могут отправлять биткоины на общедоступные биржи вне зависимости от своего местоположения, отслеживание потоков не обязательно сообщает, где находится майнер. Чтобы зафиксировать эти биржи, мы создали отдельную категорию – «международная». В результате мы делим биржи на четыре большие группы: китайские, американско-европейские, международные и другие. Категория «международные» включает биржи, которые работают во многих юрисдикциях и полагаются на стабильные монеты, привязаны к ним. Это такие биржи, как Binance и Gate.io. Категория «другие» включает все идентифицированные биржи за пределами вышеописанных. Карта различий между биржами и регионами отражена в табл. 2 (пере-

³ Один из самых известных поставщиков данных, использующий этот подход, – Кембриджский центр альтернативных исследований Finance. Он собирает агрегированные данные из трёх пулов: BTC.com, Poolin, ViaBTC, а в последнее время из Foundry USA.

числены географические регионы, к которым мы относим каждую из бирж для классификации майнеров по биржам, на которых они обналичивают вознаграждения: 1. США/Европа; 2. Китай; 3. Международные). Используя этот прокси-метод для определения местоположения майнера, можно показать, как мощность майнинга распределена по регионам (рис. 12, панели А и В, оригинал рисунка здесь: https://www.nber.org/system/files/working_papers/w29396/w29396.pdf). Панель А – месячная стоимость биткоинов вознаграждения, которые обналичиваются майнерами в разных регионах, панель В – проценты в разных регионах⁴.

С 2015 г. до середины 2017 г. большая часть майнинговых мощностей находилась в Китае (от 60% до 80%). Во второй половине 2017 г. наблюдается небольшое снижение майнинговых мощностей у майнеров, обналичивающих на китайских биржах (доля падает до 50%). В то же время отмечается значительный рост майнеров, которые обналичивают деньги на международных биржах, в частности на Binance. Эта биржа была основана в 2017 г. и быстро стала одной из крупнейших и ликвидных, что сделало её привлекательной торговой площадкой для майнеров. Среди китайских майнеров это второе по популярности место после Huobi. С 2017 г. китайские компании доминируют в майнинге, на их долю приходится около 70% общей мощности, что соответствует предыдущим оценкам.

4.3. Инцидент в Синьцзяне

Чтобы проверить, правомерно ли определять местоположение майнеров, отслеживая места, в которых они обналичивают свои биткоин-вознаграждения, мы воспользуемся недавним случаем в китайской провинции Синьцзян. В апреле 2021 г. на крупной угольной шахте погибли несколько горняков. Правительство закрыло шахту на два дня

⁴ На этом графике мы сосредоточены на вознаграждениях, выплачиваемых майнерам биржевыми кошельками и частными пулами. Многие крупные майнеры с частными кошельками со временем накапливают свои вознаграждения, а некоторые не обналичивают их вовсе. Региональное распределение майнеров с частными кошельками, которые обналичивают свои вознаграждения, соответствует майнерам биржевых кошельков.

Месторасположение бирж

Exchange name	Region
Binance US	US/Europe
Bitstamp	US/Europe
Coinbase	US/Europe
Coinsquare	US/Europe
Gemini	US/Europe
Kraken	US/Europe
Liquid	US/Europe
LocalBitcoins	US/Europe
Paxful	US/Europe
Uphold	US/Europe
BTCChina	China
Bitkan	China
BixIn	China
Bkex	China
EXX	China
Huobi	China
MXC.com	China
OkCoin	China
Allcoin	International
BCEX	International
Bibox	International
BigONE	International
Binance	International
Bit-Z	International
BitForex	International
Bitfinex	International
Bittrex	International
Cobinhood	International
CoinEgg	International
CoinEx	International
Gate.io	International
HitBTC	International
Kucoin	International
OKEx	International
Poloniex	International
Tidex	International
ZB.com	International

(17–18 апреля), прекратилось снабжение электричеством всего региона. Обилие электроэнергии, вырабатываемой угольными электростанциями, привлекло в Синьцзян множество майнеров. Во время аварии мировые мощности по добыче биткоинов снизились более чем на 35%. Поскольку только майнеры, физически находящиеся в провинции Синьцзян, были напрямую затронуты остановкой электростанций, то выявление майнеров, у которых значительно упала мощность хеширования 17–18 апреля 2021 г., помогает точно определить майнеров, которые физически локализованы в этом регионе Китая. Большинство крупных майнеров в Китае работают в нескольких регионах страны, и мы не ожидаем, что многие из них будут иметь 100% падение.

Чтобы с высокой степенью точности идентифицировать пострадавших майнеров, мы ориентировались на тех, кто в период до 8 апреля получал вознаграждение каждый день. Их оказалось 5 012. Мы измерили присутствие в данном месте на основе полученных вознаграждений. На рис. 13 (оригинал рисунка здесь: https://www.nber.org/system/files/working_papers/w29396/w29396.pdf) показан временной ряд майнеров, потерявших более 20% с 8 апреля по 8 мая. Мы видим, что 1 158 майнеров потеряли 20% мощности, 804 майнера – более 50%, 460 – 100%. После открытия угольной шахты и восстановления доступа к электроснабжению уровень мощности быстро вернулся, и мы видим быстрое возвращение почти к тому же уровню мощности, что и до инцидента. Но некоторые из самых мелких майнеров, похоже, перестали работать.

Из 804 майнеров, потерявших более 50% своей хеш-мощности из-за инцидента, 608 вернулись в сеть до 23 апреля. Из них 403 майнера – биржевые. Этот набор майнеров использует следующие биржи для торговли биткоинами в период до аварии на майнинге: Huobi (42%), Binance (10%), OKEx (9%), BixIn 25 (6%), EXX (4%), Bit.com (4%) и 15% обналичиваются на неизвестных биржах. Мы учитываем период до аварии на шахте, чтобы избежать любых помех, которые могли произойти из-за аварии. Из 205 независимых майнеров 140 отправили биткоины вышеназванным учреждениям. Биржи, используемые большинством этих независимых майнеров, всё те же: Huobi (40%), Binance (26%), OKEx (8%) и BixIn (4%). Результаты подтвердили наше предположение об использовании китайских бирж. Мы видим, что майнеры,

которые, как мы знаем, находятся в Китае, используют преимущественно китайские биржи и Binance. В общем виде результаты подтверждают верность нашего подхода: определять географическое положение майнеров по региону, в котором они обналичивают свои биткоин-вознаграждения.

5. Право собственности на биткоин

С момента появления биткоина в 2009 г. интерес к тому, кто является его крупнейшим владельцем и сколько ему (им) принадлежит, не ослабевает. Существуют сайты, формирующие адреса крупнейших биткоин-холдингов, так называемый «богатый список» – один из самых известных и широко используемых в криптографическом сообществе. Но вопрос концентрации собственности – это не только вопрос любопытства и интриги. Обществу и государству важно понимать, кто получит наибольшую выгоду от повышения цен. Это несколько избранных инвесторов? Или широкая публика? Чтобы пролить свет на эти вопросы, мы изучаем права собственности на биткоин-холдинги и их концентрацию по состоянию на конец 2020 г.

Определить концентрацию собственности сложнее, чем просто отследить авуары самых богатых адресов, так как не все крупные адреса принадлежат отдельным лицам. Многие государственные организации, например, биржи и онлайн-кошельки, хранят биткоины от имени других инвесторов. Следовательно, первым шагом в нашем анализе является разграничение адресов частных инвесторов и посредников.

Когда участники рынка депонируют свои биткоины на биржах или в интернете в кошельках хранения, они передают свои биткоины бирже. Обычно биржи смешивают все депозиты и хранят их в так называемых холодных кошельках – биткоин-адресах на специальных устройствах, не подключённых к интернету из соображений безопасности.

У такого посредника обычно только несколько биткоин-адресов, составляющих его холодный кошелёк, но на них хранятся очень большие остатки. Например, Binance – один из крупнейших холодных кошельков – хранил 300 тыс. биткоинов по состоянию на конец июня 2021 г.⁵

⁵ <https://bitinfocharts.com/bitcoin/wallet/Binance-coldwallet>.

Однако не на всех биржах есть холодный кошелёк, столь же заметный, как Binance. Холодный кошелёк обычно состоит из нескольких адресов, по которым нечасто отправляют и получают средства, и во многих случаях алгоритм кластеризации по умолчанию не привязывает их к соответствующим горячим кошелькам бирж. Поэтому выявление холодных кошельков представляет серьёзную проблему.

Чтобы решить её, мы внимательно изучили адреса в расширенном «богатом» списке организаций, у которых на 31 декабря 2020 г. на балансе находилось не менее тысячи биткоинов. Таких адресов учреждений было 2 258. Они контролировали 7,9 млн биткоинов – почти половину всех биткоинов в обращении. Поскольку холодные кошельки содержат большие остатки, их адреса, скорее всего, находятся среди этих «богатых» адресов. Тот факт, что так мало адресов контролирует почти половину биткоинов в обращении, часто воспринимается как очевидное свидетельство высокой концентрации холдингов биткоинов. Однако эта точка зрения не учитывает, что некоторые из этих адресов принадлежат холодным кошелькам и, следовательно, представляют собой холдинги большого количества людей. Мы устраняем недостатки алгоритма кластеризации по умолчанию, разрабатывая набор алгоритмов, основанный на анализе графов, для классификации адресов на две группы: принадлежащих индивидуальным инвесторам либо посредникам. Мы проверяем каждый расширенный адрес: принадлежит ли он кластеру, указанному в нашей базе данных. Если адрес не принадлежит какому-либо известному объекту, мы строим сеть из кластеров, которые отправляют биткоины на этот адрес (или кластер, содержащий этот исходный адрес). Это рекурсивный процесс. Сначала мы находим кластеры, которые отправляют свои балансы прямо по адресу. Во многих случаях такой кластер бывает уникальным. Например, 1GR9qNz7zgtaW5HwwVpEJWMnGWhsbsieCG получил 17 мая 2018 г. весь свой баланс с другого адреса 1MzG9Gx5G3ZTXtEQT4FJg23Cb3gS6UF982, который, в свою очередь, получил весь баланс от крупного неизвестного кластера, датированного 2014 г.

Случаи, когда на каждом шаге есть уникальный родительский кластер, просты. Мы останавливаем процесс, если, во-первых, достигаем кластера, принадлежащего известной организации или лицу, во-вторых, достигаем большого неизвестного кластера, в-третьих, достигаем достаточно старого кластера, про который известно, что это не холодный кошелёк биржи или онлайн-кошелёк. В первом случае, когда известный субъект является активным посредником (биржа или онлайн-кошелёк), мы отмечаем богатый адрес как связанный с посредником. Если известная сущность является индивидуальной (майнер или несуществующий посредник), мы отмечаем её как физическое лицо. Во втором случае, если большой неизвестный кластер активен, мы классифицируем начальный богатый адрес, связанный с посредником или, в противном случае, с индивидуальным инвестором. Наконец, в последнем случае мы классифицируем исходный расширенный адрес как принадлежащий отдельному инвестору.

В случае, когда богатый адрес пополняет свой баланс от нескольких кластеров, мы продолжаем отслеживать потоки до каждого родительского кластера. Обычно достигаются следующие результаты. Во-первых, процесс может связать адрес с сетью, в которой доминирует один большой кластер, и в этом случае мы следуем тем же правилам классификации, что и в случае уникального родительского кластера. Например, сеть на рис. 20 (оригинал рисунка здесь: https://www.nber.org/system/files/working_papers/w29396/w29396.pdf) реализована путём отслеживания потоков до 1P5ZEDWTKTFGxQjZphgWPQUpe554WKDfHQ (сокращённо 1P5ZE), который был третьим по величине адресом на момент написания этой статьи. Картина показывает, что все его потоки исходят из одного кластера, содержащего адрес 1FzWLkAahHooV3kzTgyx6qsswXJ6sCXkSR (сокращённо 1FzWL). Последний кластер является активным большим неопознанным кластером, который взаимодействует в основном с крупными биржами. Поэтому мы классифицируем 1FzWL как посредника. Поскольку 1P5ZE не только принимает потоки от 1FzWL, но и отправляет их обратно, мы заключаем, что 1P5ZE – это холодный кошелёк 1FzWL.

Второй распространённый результат – когда баланс адреса отслеживается как минимум до двух известных сущностей. Если адрес не принадлежит большому активному кластеру, мы отмечаем его как ин-

дивидуальный. В случаях, когда нет уверенности в том, принадлежит адрес посреднику или физическому лицу, мы отмечаем его как двусмысленный (неоднозначный). В целом из 2 258 расширенных адресов 1 013 мы классифицируем как индивидуальные, 1 154 как связанные с посредниками, а 47 – неоднозначные.

На рис. 21 (оригинал рисунка здесь: https://www.nber.org/system/files/working_papers/w29396/w29396.pdf) показана динамика количества биткоинов, хранящихся в кошельке посредников. Сальдо на счетах посредников стало ускоряться в 2014 г., оно стабильно увеличивается с течением времени. К концу 2020 г. насчитывалось 5,5 млн биткоинов (примерно одна треть биткоинов, находящихся в обращении).

Сопоставим холдинги посредников с холдингами частных лиц, которые мы аппроксимируем двумя способами: включим расширенные адреса, классифицированные как индивидуальные, в анализ «богатых» адресов, а также включим все неизвестные кластеры, не активные в течение всего 2020 г. и имеющие на балансе к концу года от одного до тысячи биткоинов. Мы накладываем ограничение бездействия, чтобы отделить отдельные индивидуальные кошельки от кошельков, которые могут принадлежать посредникам. Некоторые из этих кластеров могут быть старыми или даже забытыми адресами, а другие, вероятно, принадлежат долгосрочным инвесторам. Таких кластеров 400 тыс., вместе они контролировали 8,5 млн биткоинов на конец 2020 г. Это на 3 млн биткоинов больше, чем хранится в биржевых кошельках.

На рис. 22 (оригинал рисунка здесь: https://www.nber.org/system/files/working_papers/w29396/w29396.pdf) показано изменение баланса отдельных биткоинов во времени. На панели А мы вычисляем дату первой транзакции для каждого отдельного кластера и считаем это как прокси (приближение) для возраста этого кластера. Затем мы фиксируем баланс кластера с конца 2020 г. до даты его создания. Это позволяет нам разложить холдинги индивидуальных инвесторов по состоянию на 2020 г. по времени его владения собственником. На панели В показано, как остатки накапливались с течением времени.

Результаты показывают, что было несколько периодов, когда создавались значительные остатки биткоинов. Во-первых, на заре блокчейна Биткоин более 1 млн биткоинов добывал инвестор Сатоши Накамото, истинная личность которого до сих пор не установлена, как и право собственности на эти ранние биткоины. Остальные периоды накопления значительных остатков совпадают со временем очень быстрого роста цен на биткоины и последующих спадов, таких как в 2014 г., в конце 2017 г. и в начале 2018 г.

В заключение рассмотрим концентрацию индивидуального владения биткоинами. Мы сортируем отдельные кластеры по величине их баланса на конец 2020 г. и сопоставляем совокупный баланс с количеством отдельных кластеров, которые держат эти биткоины (рис. 23, оригинал рисунка здесь: https://www.nber.org/system/files/working_papers/w29396/w29396.pdf). Заметно, что даже в конце 2020 г. участие в биткоинах всё ещё сильно смещено в сторону нескольких топовых игроков. Мы видим, что только тысяча кластеров контролирует 3 млн биткоинов, а 10 тыс. лучших владеют более чем 5 млн биткоинов (примерно четверть всех, введённых в обращение).

Важно отметить, что это, скорее всего, преуменьшение в измерении концентрации, поскольку мы не можем исключить, что некоторые крупнейшие адреса контролируется одним и тем же лицом. В частности, в приведённых выше расчётах мы не определили владение ранними биткоинами, хранящимися примерно по 20 тыс. адресов, одному человеку (Сатоши Накамото), но считаем, что они принадлежат 20 тыс. разных людей (рис. 23).

Рис. 14 демонстрирует типы краткосрочных кластеров, рис. 15 – краткосрочный кластерный цикл, рис. 16 – транзакцию Coinbase блока 684887, рис. 17, 18 и 19 соответственно – адреса отправлений, дерево распределения вознаграждений и пример распределения базы AntPool (оригиналы рисунков здесь: https://www.nber.org/system/files/working_papers/w29396/w29396.pdf).

6. Выводы

Мы изучили транзакционное поведение и формы собственности на основном рынке участников экосистемы Биткоин, используя данные из блокчейна Биткоин. Выявлено, что, во-первых, биржи играют главную роль в этой экосистеме. Они обеспечивают 75% реального объёма потоков биткоинов, тогда как другие типы транзакций (незаконные или вознаграждения за майнинг), объясняют только небольшую часть от общего объёма. Биржи являются наиболее подключёнными узлами на блокчейн. Сильная взаимосвязь бирж и лёгкость, с которой испорченные биткоины могут смешиваться с чистыми, влияют на прозрачность и отслеживаемость транзакций, а также соблюдение норм Know-YourCustomer (KYC) в сети.

Во-вторых, мы задокументировали концентрацию и региональный состав биткоин-майнеров – лиц, обеспечивающих проверку транзакций на платформе Биткоин. В отличие от информации о пулах для майнинга, информация об отдельных майнерах ранее была недоступна. Мы не только показываем высокую концентрацию мощностей по добыче биткоинов, но отмечаем, что она меняется противочиклически в зависимости от вознаграждения за майнинг. В результате риск «атаки 51%» увеличивается, когда цена биткоина резко падает или «уполовинивается».

В-третьих, мы изучили владение и концентрацию биткоин-холдингов. В то время как остаток на счетах у посредников стабильно увеличивался с 2014 г., даже к концу 2020 г. он составлял всего 5,5 млн биткоинов – примерно треть всех биткоинов в обращении. Индивидуальные инвесторы, напротив, коллективно контролируют 8,5 млн биткоинов – почти половину из находящихся в обращении к концу 2020 г. Внутри индивидуальных холдингов существует значительная асимметрия владения.

Несмотря на значительное внимание к биткоину, в последние несколько лет в его экосистеме по-прежнему доминируют крупные и концентрированные игроки, будь то майнеры, держатели биткоинов или биржи. Эта врождённая концентрация делает Биткоин подверженным системному риску и предполагает, что большая часть прибыли от дальнейшего внедрения, вероятно, достанется непропорционально небольшому числу участников.

Дополнительную информацию по теме исследования, включая развёрнутый список источников, можно найти в Приложении (Appendix), представленном в англоязычном варианте части 3.

Список источников

1. **Foley S., Karlsen J., Putniņš T.** Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies? // *The Review of Financial Studies*. 2019. № 32 (5). P. 1798–1853. <https://doi:10.1093/rfs/hhz015>
2. **Cong Y., Ulasli M., Schepers H. et al.** Nucleocapsid Protein Recruitment to Replication-Transcription Complexes Plays a Crucial Role in Coronaviral Life Cycle // *J Virol*. P. 169–176. 2020. № 94 (4). doi: 10.1128/JVI.01925-19
3. **Bitcoin Core.** URL: <https://bitcoin.org/en/bitcoin-core/> (accessed: 05.08.2022).
4. **BlockSci.** URL: <https://github.com/citp/BlockSci> (accessed: 05.08.2022).
5. **Ron D., Shamir A.** Quantitative Analysis of the Full Bitcoin Transaction Graph. URL: <https://eprint.iacr.org/2012/584.pdf> (accessed: 05.08.2022).
6. **Meiklejohn C., Holmbeck M., Siddiq M. et al.** An Incompatibility between a Mitochondrial tRNA and Its Nuclear-Encoded tRNA Synthetase Compromises Development and Fitness in *Drosophila* // *PLOS Genetics*. № 9 (1). doi: 10.1371/journal.pgen.1003238

Информация об авторах

Игорь Макаров – Лондонская школа экономики Houghton Street Лондон WC2A 2AE Соединённое Королевство
i.makarov@lse.ac.uk

Антуанетта Шоар – Школа менеджмента MIT Sloan School of management
100 Main Street, E62-638 Кембридж, Массачусетс 02142 и NBER
aschoar@mit.edu