

ЭЛЕКТРОННЫЕ ИНФОРМАЦИОННЫЕ РЕСУРСЫ

УДК 004.65:[336.743-021.131]-047.44

<https://doi.org/10.33186/1027-3689-2022-10-85-100>

Блокчейн-анализ рынка биткоинов. (Часть 2)

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 проведён на трёх основных этапах. 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 языка¹ на русский было весьма затруднительным в связи с новизной финансовой тематики и широким использованием его авторами распространённого на За-

¹ Оригинальный текст:

https://www.nber.org/system/files/working_papers/w29396/w29396.pdf.

паде, 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 2) / И. Макаров, А. Шоар // Научные и технические библиотеки. 2022. № 10. С. 85–100. <https://doi.org/10.33186/1027-3689-2022-10-85-100>

3.2. Реальный объём

Теперь рассмотрим экономически значимую, не ложную часть объёма транзакций биткоинов. Чтобы понять, для каких целей используется биткоин, мы отслеживаем его потоки между различными типами объектов в блокчейне. В список организаций входят биржи, онлайн-кошельки, платёжные системы, сайты азартных игр, сервисы микширования, нелегальные сервисы и пулы для майнинга. Мы идентифицируем эти организации из большого количества общедоступных и коммерческих источников, как описано в разделе 2. Данные.

Такие криптовалютные биржи, как Coinbase, Binance или Kraken, и онлайн-кошельки Blockchain.info и BixIn являются представителями основных типов организаций, в которых биткоин можно хранить, а также торговать им. Теоретически биржи должны предоставлять платформы для торговли биткоинами за фиатные валюты и другие монеты, а онлайн-кошельки – специализироваться на сервисах хранения. Однако на практике разница между ними зачастую невелика. В большинстве случаев оба типа объектов предлагают и ту, и иную функции. Поэтому в обзоре об использовании биткоинов мы сгруппировали эти объекты вместе. Платёжные системы, такие как BitPay или CoinPayments, облегчают оплату онлайн-магазинам, продавцам азартных игр и другим организациям, принимающим криптовалюту как средство оплаты товаров и услуг. В список организаций, оказывающих незаконные услуги, входят торговые площадки в «тёмной» сети, такие как Hydra Market, многочисленные кошельки с программами-

вымогателями и компании, занимающиеся мошенничеством. Сервисы смешивания или тумблеры, такие как Bitcoin Fog и кошелёк Wasabi, – это сайты, которые позволяют своим клиентам объединять средства, чтобы скрыть адрес их отправки.

Другой список учреждений и лиц из числа основных компонентов системы Биткоин – это майнинг-пулы и майнеры. Мы идентифицируем индивидуальных майнеров, отслеживая их вознаграждение в крупнейших майнинговых пулах (процедура отслеживания майнеров описана в разделе 4 и в приложении). Всего идентифицировано 248 тыс. майнеров.

Как обсуждалось ранее, псевдонимный характер биткоина затрудняет возможность связать адрес с реальным объектом, стоящим за ним. Таким образом, идентификация сущностей является неполной по смыслу, поскольку полагается на то, что субъект либо добровольно раскрывает свой адрес, либо информация об адресе юридического лица обнаруживается в ходе взаимодействия с ним.

Чтобы решить проблему неполной идентификации юридических лиц и организаций и убедиться, что мы не упустили из виду крупных игроков блокчейна, нами было проанализировано 10 тыс. крупнейших неизвестных кластеров с наибольшим объёмом неидентифицированных биткоинов. Из этого множества кластеров мы выбрали те, которые либо получают регулярные потоки от майнеров, либо получают более 50% своих поступлений от известных бирж (или отправляют более 40% на известные биржи). Эти пороговые уровни определены по шаблонам транзакций известных нам организаций. Для типичной биржи 53% оттока биткоинов (отправлений) идёт на другие биржи, а 52% притока биткоинов поступает от других бирж. По всем остальным организациям эти цифры значительно ниже. Например, типичный игорный сайт отправляет на биржи 21%, а получает от них 29% от общего потока. Мы обнаружили, что 4 507 кластеров удовлетворяют указанным выше условиям. Вместе они поставляют 63% биткоинов, поступающих в крупнейшие 10 тыс. кластеров. В дальнейшем мы будем ссылаться на такие кластеры, как биржи типа LEOTD (Likely Exchanges, OTC brokers, or Trading Desks – вероятные биржи, внебиржевые брокеры или торговые столы).

Основываясь на этой классификации участников, мы показываем среднемесячный объём транзакций, который создан этими учреждениями в цепочке блоков с начала 2015 г. по май 2021 г. (рис. 3, оригинал рисунка здесь: https://www.nber.org/system/files/working_papers/w29396/w29396.pdf). Объём рассчитывается как сумма биткоинов, отправленных организациям различных типов в определённый месяц. На рис. А объём биткоинов показан в миллионах (BTC), а на рис. В – в процентах от общего ежемесячного объёма.

Мы видим, что большая часть объёма генерируется транзакциями с участием бирж и кластеров типа LEOTD. Объём, поступающий на известные биржи, составляет около 40% от общего объёма, ещё 20% приходится на объём, поступающий от 11 организаций типа LEOTD. Чтобы подчеркнуть доминирующую роль бирж и LEOTD, мы разделили объём, попадающий в категорию Other (все неизвестные кластеры, не являющиеся LEOTD), на две части: поступающий с бирж, LEOTD и остальной. Это распределение показывает, что объём от бирж и LEOTD до Other занимает ещё 20% объёма. Таким образом, объём, связанный с биржей и торговыми системами, составляет около 80% от общего. Другим известным организациям по данным за 2020 г. принадлежит только незначительная часть от общего объёма. Например, на незаконные операции, мошенничество и азартные игры приходится менее 3% от общего объёма. Доля, связанная с майнерами, ещё меньше.

Этот анализ объёма отличает доминирование транзакций, связанных с торговлей и со спекуляциями в блокчейне. На первый взгляд кажется, что он расходится с более ранними версиями, результаты которых указывали на преобладание незаконных транзакций в блокчейне. В частности, в работе Foley et al. (2019) более 46% транзакций связаны с незаконными операциями. Разница между расчётами происходит по двум причинам: во-первых, Foley et al. (2019) намеренно исключает из своих расчётов все связанные с биржей объёмы, чтобы сосредоточиться только на оплате товаров и услуг. Мы показали выше, что торговля является основным видом деятельности в блокчейне, поэтому этот выбор сильно меняет знаменатель дроби. Во-вторых, оценка объёмов в Foley et al. (2019) основана на надуманной сети незаконных кластеров, в которой любой кластер рекурсивно считается незаконным, если

большинство его транзакций совершается с ранее идентифицированными незаконными кластерами. Несмотря на то, что этот метод вменения интуитивно привлекателен, он не делает различий между реальными пользователями и недолговечными транзитными кластерами, которые существуют исключительно для пресечения отслеживаний. В разделе 3.5 мы покажем, что этот тип паразитных потоков обычно составляет очень большую часть незаконных сделок. В результате объём, рассчитанный этим методом, вероятно, завышает экономическую ценность незаконных сделок².

Наш результат, конечно, не означает, что незаконная деятельность в блокчейне Биткоин не является проблемой с точки зрения социального обеспечения. Мы солидарны с общей обеспокоенностью тем, что псевдонимный характер Биткоина способствует злоупотреблениям, таким как незаконная деятельность, уклонение от уплаты налогов или даже взятки. Несмотря на то, что объёмы незаконных торгов BTC оставались относительно стабильными в последние несколько лет, сумма за незаконную деятельность в долларах увеличилась, так как выросла долларовая стоимость BTC. Мы вычислили чистый поток биткоинов по незаконным организациям в период с 2020 г. с разбивкой по типам. Мы считаем, что на адреса, идентифицированные как мошеннические, поступает около 550 млн долларов. Около 16 млн долларов поступает в виде установленных выкупов и более 1,6 млрд долларов в виде «тёмных» платежей и даркнет-сервисов. Около 1,7 млрд долларов поступает на адреса, связанные с азартными играми, ещё 1,4 млрд долларов тратится на оплату за микширование.

Мы считаем важным оценить масштабы транзакционной активности, чтобы понять, каковы основные движущие силы, влияющие на стоимость биткоинов. Наши результаты не подтверждают идею о том, что высокая оценка криптовалют основана на незаконных сделках. Мы предполагаем, что большинство биткоин-транзакций связаны со спекуляциями.

² Точное сравнение наших результатов с предыдущей работой затруднительно, потому что мы используем существенно больший набор идентифицированных сущностей.

3.3. Центральность сети

В предыдущем разделе мы показали, что биржи криптовалют несут ответственность за большую часть объёма транзакций в сети Биткоин и, вероятно, будут играть в ней доминирующую роль. Чтобы уточнить наше понимание роли бирж, мы проанализировали структуру сети Биткоин. Мы рассматривали наиболее релевантные кластеры, то есть кластеры, идентичность которых известна и которые входят в 10 тыс. кластеров с наибольшим объёмом. С учётом этих ограничений рассмотрим 11 043 учреждения, выполняющих более 55% от общего объёма транзакций. Из-за быстро меняющейся эволюции экосистемы Биткоин мы фокусируемся на периоде с 2018 г. до конца 2020 г. У нас осталось 6 248 сущностей. Для представления этой сети мы используем ориентированный взвешенный сетевой граф, где узел i соответствует кластеру i , а ребро от узла i до j соответствует общему потоку биткоинов за период 2018–2020 гг. из кластера i в кластер j . Полученная сеть состоит из 6 248 узлов и 622 тыс. рёбер. Каждая сущность получает и отправляет в среднем биткоины другим ста объектам (см. график). График 4 показывает подмножество этого сетевого графа Биткоин. Для простоты иллюстрации мы оставляем только узлы, получившие не менее 500 тыс. биткоинов за выбранный период (рис. 4, оригинал рисунка здесь: https://www.nber.org/system/files/working_papers/w29396/w29396.pdf).

Сеть самых крупных объектов состоит из 23 объектов и 492 рёбер³.

Узел и размер ребра пропорциональны объёму, полученному объектом, и объёму транзакций между двумя разными объектами. В случае, когда два кластера отправляют потоки друг другу, направление края между этими кластерами соответствует наибольшему потоку, а ребро отмечено красным сегментом.

В статье для построения этой и других сетей мы используем пакет программного обеспечения Graphia, доступный по адресу <https://graphia.app/> (Freeman et al., 2020).

³ В направленной сети рёбра от узла i до j и от узла j до i считаются отдельными.

Из 23 объектов три (BitGo, Харо и BixIn) – это онлайн-кошельки, 18 – идентифицированные биржи, два – неизвестные организации (скорее всего, это неидентифицированные биржи или крупные внебиржевые кассы). Они активно взаимодействуют с известными биржами и получают солидную сумму майнерских вознаграждений: 1 252 биткоина и 4 795 биткоинов соответственно.

На рис. 4 проиллюстрирована высокая степень взаимосвязанности между основными биржами. Мы видим, что они образуют почти полный граф, в котором каждый узел соединяется со всеми остальными. И это при том, что биржи работают в разных регионах. Например, Bithumb и Upbit – корейские биржи; bitFlyer – японская; Bitstamp, Coinbase, Gemini и Kraken ориентируются на пользователей из США и Европы, а Huobi, BixIn, OKEx и OceanEx – из Китая. Высокая степень взаимосвязанности важна для регулирования требований KYC, о которых мы скажем в разделе 3.5.

Binance, Huobi и Coinbase являются крупнейшими и самыми активными участниками сети Биткоин (рис. 4). Для формальной количественной оценки важности различных сущностей мы вычисляем центральность собственных значений каждой из них в полной сети. Центральность собственных значений для объекта i – это i -й компонент вектор x , который является решением уравнения на собственный вектор:

$$Ax = \lambda x \quad (1)$$

где матричные элементы A_{ij} задаются полными потоками биткоинов от объекта i к j в течение 2018–2020 гг., а λ – наибольшее собственное значение, связанное с вектором матрицы A . Центральность собственного вектора учитывает не только полный объём, полученный сущностью, но также структуру сети Биткоин и даёт больший вес кластерам, которые получают большой объём от других кластеров, получающих большой объём⁴.

⁴ Для более подробной информации см. Newman (2010), 7.1.2. Центральность собственного вектора, основанная на измерениях других сетей, например на общем количестве транзакций, даёт аналогичные результаты.

Список 25 крупнейших организаций с наибольшей центральностью в сети Биткоин приведён на рис. 5 (оригинал рисунка здесь: https://www.nber.org/system/files/working_papers/w29396/w29396.pdf). Подтверждая наши предыдущие наблюдения (рис. 4), Binance, Coinbase и Huobi демонстрируют высшую меру центральности. Другие биржи (рис. 4) также входят в число 25 наиболее центральных субъектов. Это не должно вызывать удивления, поскольку все эти биржи часть очень плотной сети.

Центральность собственных значений (уравнение 1) подтверждает доминирующую роль бирж в сети Биткоин. В заключение отметим, что потенциально центральность собственных значений может стать новым и полезным показателем значимости биржи.

Другими популярными критериями, которыми ранее пользовались многие агрегаторы данных (например, CoinMarketCap), являются объём торгов вне сети, трафик веб-сайта или количество подписчиков в Twitter. Желательным качеством любого рейтингового показателя должна быть устойчивость к манипуляциям. К сожалению, ни один из существующих критериев не защищён от манипуляций полностью⁵.

Из-за того, что центральность собственных значений основана на потоках биткоинов между биржами на блокчейне, для улучшения своего положения в рейтинге биржа должна иметь возможность отправлять большое количество биткоинов на другие биржи. Это может оказаться значительно дороже, чем заниматься демоторговлей (посылать куда-либо средства и тут же получать их обратно) или покупать трафик веб-сайта. Поэтому разумно полагать, что центральность собственных значений может быть более устойчива к манипуляциям, чем другие критерии.

3.4. Межбиржевые потоки

Наш анализ в разделах 3.2 и 3.3 показывает, что большую часть объёма биткоинов составляют потоки между биржами. Чем обусловлены эти потоки? Чтобы ответить на этот вопрос, необходимо признать, что рынки криптовалюты состоят из многих неинтегрированных бирж,

⁵ См., например, отчёт компании по надзору за рынком криптовалюты BTI Verified: <https://btiverified.com/crypto-market-data-report-2020/>.

которые имеют независимых владельцев, существуют параллельно и находятся в разных странах. Большинство этих бирж самостоятельно функционирует как традиционные фондовые рынки, где трейдеры подают заказы на покупку и продажу, а биржа завершает сделки на основе централизованной книги заявок. Однако на рынке криптовалют, в отличие от традиционных регулируемых фондовых рынков, нет гарантии того, что инвесторы получат лучшую цену при совершении сделок⁶.

Отсутствие таких механизмов повышает роль арбитров, торгующих на разных биржах и обеспечивающих согласованные цены. Предположим, обменный курс между биткоинами и какой-либо другой валютой, скажем С, различается на двух биржах. Идеальной арбитражной сделкой будет обмен биткоинов на С на бирже, где курс обмена высок, и обмен С на биткоины на бирже с невысоким курсом обмена. Затем биткоины и С перенесутся между биржами, реализуется безрисковая прибыль.

Вышеописанная сделка сталкивается с небольшими препятствиями, если С является криптовалютой, так как псевдонимный характер криптовалют делает их невосприимчивыми к любому контролю за движением капитала. В случае, если С является фиатной валютой, возможность репатриировать средства из одной страны в другую может быть затруднена из-за трансграничного контроля за капиталом. Рынок может стать потенциально сегментированным.

В работе Игоря Макарова и Антуанетты Шоар (2020) показано, что в период 2017–2018 гг. отклонения цен на криптовалюту на разных биржах были существенными и повторяющимися, что указывает на значительную сегментацию рынка. А арбитражные спреды для обменов в разных странах были намного больше, чем в пределах одной страны. Они определённо связаны с трансграничным контролем за движением капитала⁷.

⁶ Регулирование со стороны Комиссии по ценным бумагам и биржам США (SEC) в рамках положения о Национальной лучшей ставке и предложении (NBBO) в Соединённых Штатах требует от брокеров исполнения клиентских сделок по наилучшим доступным на нескольких биржах ценам.

⁷ Сам по себе контроль за трансграничным капиталом может быть мотивом для трансграничных потоков. Поскольку биткоины не подлежат контролю, их можно использовать как средство его обхода. Однако одно это не объясняет потоки между криптовалютными биржами и между биржами одной страны.

Приведённое выше обсуждение предполагает, что:

Биржи внутри страны с сильным контролем за капиталом могут быть более взаимосвязаны друг с другом, чем с другими биржами.

Биржи, торгующие схожими валютными парами, могут демонстрировать более высокие межбиржевые потоки.

Чтобы проверить эти предположения, мы вычисляем два критерия сходства пары бирж. Один основан на схожести криптовалютных пар, торгуемых на каждой бирже. А другой – на сходстве взаимодействия двух бирж с другими биржами в блокчейне Биткоин. Чтобы вычислить схожесть валютных пар, мы используем данные частной фирмы Kaiko, собирающей торговую информацию о криптовалютах с 2014 г. Данные Kaiko охватывают только подмножество бирж, которые мы можем идентифицировать в блокчейне Биткоин, но это крупнейшие биржи. Полученный набор состоит из 57 бирж.

Для каждой биржи мы рассматриваем все торгуемые валютные пары, в которых одной из валют является биткоин. Другой валютой может быть фиатная валюта, стабильные монеты или другие криптовалюты. В общей сложности у нас 4 360 валютных пар на 57 биржах, причём среднее количество валютных пар на бирже составляет 13. Для каждой биржи i и криптовалютной пары j рассчитываем общий объём торгов за период 2018–2020 гг., деноминированный в биткоинах (v_{ij}). Затем мы нормализуем объём на каждой бирже по евклидовой норме:

$$\hat{v}_{ij} = \frac{v_{ij}}{\sqrt{\sum_j v_{ij}^2}},$$

и используем евклидово расстояние между векторами

$$\mathbf{v}_i = \{\hat{v}_{ij}\}_{j=1}^N \text{ and } \mathbf{v}_k = \{\hat{v}_{kj}\}_{j=1}^N$$

как меру сходства бирж i и k .

Чтобы вычислить сходство бирж на основе потоков биткоинов, сначала мы вычислим матрицу перекрёстных потоков A . Каждый элемент a_{ij} матрицы A является средним биткоин-потоком с биржи i на биржу j и наоборот.

Как и раньше, нормализуем объём на каждой бирже по евклидовой норме:

$$\hat{a}_{ij} = \frac{a_{ij}}{\sqrt{\sum_j a_{ij}^2}},$$

и используем евклидово расстояние между векторами

$$\mathbf{a}_i = \{\hat{a}_{ij}\}_{j=1}^N \text{ and } \mathbf{a}_k = \{\hat{a}_{kj}\}_{j=1}^N,$$

где j = от 1, чтобы получить меру сходства бирж i и k на блокчейне Биткоин.

Чтобы увидеть, выделяют ли две построенные меры сходства одну и ту же группу бирж, мы применяем алгоритмы кластеризации K-medoids к каждой из мер сходства. Алгоритмы K-medoids пытаются сгруппировать похожие биржи вместе, чтобы минимизировать внутри-кластерную сумму расстояний между биржами. Это популярный метод кластеризации во многих случаях⁸.

На рис. 6 (оригинал рисунка здесь: https://www.nber.org/system/files/working_papers/w29396/w29396.pdf) показан результат применения алгоритмов кластеризации K-medoids на основе меры сходства валютных пар. Мы видим, что есть четыре заметные группы обменов. Это американско-европейские (группа 5), корейские (3), биржи японской группы (4) и Tether (2). Резкая кластеризация корейских и японских бирж объясняется тем, что в качестве базовых на этих биржах используются национальные фиатные валюты, торговля осуществляется небольшим количеством валютных пар. Аналогичная ситуация наблюдается на американско-европейских биржах, где в качестве базовой валюты обслуживаются доллар, и евро, причём доллар обычно более популярен. Большинство бирж 2-й группы – это только криптовалютные

⁸ В нашем анализе мы используем процедуру K-medoids из модуля Python sklearn extra (см. Hastie et al. (2001), 14.3.10 для более подробной информации). Алгоритмы кластеризации K-medoids принимают в качестве параметра количество кластеров. Поскольку для его определения нет строгих правил, мы по умолчанию используем значение 8.

биржи, которые не предлагают торговлю против фиатной валюты. Обычно эти биржи в качестве базовой валюты используют Tether и размещают большое количество различных криптовалют для торговли. Также есть несколько разрозненных бирж с менее популярными базовыми валютами. Например, Coinflood использует британский фунт стерлингов, BitBay – польский злотый, а ACX – австралийский доллар.

Затем мы применили алгоритмы кластеризации K-medoids к измерению сходства цепочки биткоинов (рис. 7, оригинал рисунка здесь: https://www.nber.org/system/files/working_papers/w29396/w29396.pdf). Сравнивая рис. 6 и 7, можно увидеть, что разница в расстоянии между биржами внутри кластера и биржами из разных кластеров не так ярко выражена, как в случае кластеризации на основе криптовалютных пар. Это не должно удивлять, так как интеграция биржи зависит не только от торгуемых криптовалют, но и от средств контроля за капиталом, действующих в данной стране. Две биржи в разных странах могут быть разделены значительным расстоянием между криптовалютами парами, если они используют разные фиатные валюты, но могут быть очень похожими на расстоянии блокчейна Биткоин, если они работают в странах без контроля за движением капитала.

Тем не менее метод кластеризации основных групп бирж, основанный на двух показателях сходства, в целом даёт аналогичные результаты (рис. 6, 7). Особенно отчётливо в обоих случаях сгруппированы вместе корейские и японские биржи. Американские, европейские и Tether разделены менее чётко. Например, Poloniex, которая является только криптовалютной биржей, теперь сгруппирована вместе с Coinbase, Bitstamp, «Близнецы», Kraken и Bitfinex. Это согласуется с результатами работы Игоря Макарова и Антуанетты Шоар (2020), в которой показано, что американо-европейские биржи и биржи Tether интегрированы лучше, чем биржи в Корее и Японии.

3.5. Обеспечение соблюдения норм KYC для биткоин-транзакций

Мы завершаем наше исследование объёма потоков биткоинов анализом, связанным с теневой экономикой. Нежесткое (лёгкое) регулирование и анонимность сделали криптовалюты популярными у всех, кто хочет избежать юридической или нормативной проверки, укло-

ниться от уплаты налогов. Сторонники криптовалюты часто указывают на то, что она по-прежнему превосходит наличные из-за своего цифрового следа. Цифровой след действительно накладывает некоторые ограничения на анонимность транзакций и в некоторых случаях помогает найти правонарушителей, однако есть и существенные ограничения.

Чтобы понять проблемы, связанные с соблюдением норм «Знай своего клиента» (KYC), полезно и поучительно рассмотреть сеть, сосредоточенную на Рынке Гидры (Hydra Market), который является одной из крупнейших торговых площадок в «тёмной» сети⁹.

Hydra Market начал работу в 2015 г. и с тех пор быстро растёт. Мы ориентируемся на период 2020 г. – июнь 2021 г. За этот период на Hydra Market поступило 147 620 биткоинов из 514 855 кластеров. Биткоины отправлены в 315 359 кластеров. Эти 514 855 отправляющих в Hydra Market кластеров, в свою очередь, получили свои потоки из 3 291 180 кластеров, а вышеупомянутые 315 359 кластеров-получателей отправили потоки в 500 544 кластера, из них 116 131 новые кластеры.

На рис. 8 (оригинал рисунка здесь: https://www.nber.org/system/files/working_papers/w29396/w29396.pdf) изображена получившаяся сеть, где для простоты иллюстрации мы сохраняем только узлы, которые отправляют не менее тысячи биткоинов в этой сети. При вычислении объёма мы намеренно исключаем объём между любыми кластерами, которые принадлежат к списку известных или крупных объектов, который мы изучали в разделах 3.3 и 3.4.

Размер узла отражает общее количество биткоинов, отправленных с Hydra Market соответствующему лицу или организации. Размер связующей линии пропорционален объёму потоков между двумя разными объектами. В случае, когда два кластера отправляют потоки друг другу, длина линии между этими кластерами соответствует наибольшему потоку, а линия изображена в красном сегменте. Оранжевый цвет показывает идентифицированные кластеры, зелёный отмечает неизвестные кластеры большого объёма, бирюзовый – короткоживущие кластеры

⁹ <https://www.bloomberg.com/news/articles/2021-02-01/darknet-market-had-a-record-2020-ledby-russian-bazaar-hydra>.

с продолжительностью жизни менее одного месяца. Оставшиеся кластеры отмечены фиолетовым цветом.

На рис. 8 продемонстрировано, что объектами с наибольшим объемом, напрямую взаимодействующими с Hydra Market, являются биржи, не поддерживающие KYC, такие как LocalBitcoins, Bitzlatо, Binance, Huobi и Totalcoin¹⁰.

Поступая на биржи, потоки смешиваются и становятся практически неотслеживаемыми, поэтому впоследствии могут быть отправлены куда угодно.

Рисунок также демонстрирует, что прямое взаимодействие Hydra Market с теми биржами, которые пытаются обеспечить соблюдение норм KYC, такими как Coinbase и Gemini, скромны, но их взаимодействие с соседними кластерами значительно шире. Например, Coinbase напрямую отправила и получила 196 и 126 биткоинов с Hydra Market соответственно. Но она отправила 530 тыс. и получила 218 тыс. биткоинов через соседние кластеры.

Мы видим (рис. 8), что большинство потоков на Coinbase и обратно происходят через короткоживущие кластеры, которые в большинстве случаев создаются с единственной целью сокрытия происхождения средств. Типичная транзакция включает смешивание испорченных средств (те, которые можно отследить до Hydra Market) с «чистыми» (не связанными с незаконными сделками). Каждое смешивание снижает долю испорченных потоков. Процесс повторяется несколько раз, пока полученные потоки не станут достаточно чистыми, чтобы отправить их в KYC-биржи.

Каковы последствия? Во-первых, учреждения, не участвующие в KYC, служат для отмывания денег и другой серой деятельности. Децентрализованный характер протокола Биткоин упрощает работу этих организаций – им нужно только иметь свои серверы в стране, где власти готовы мириться с их существованием. Если организациям KYC разрешено принимать потоки от организаций, которые не соблюдают строгие нормы KYC (текущее состояние дел), то цифровой след очень ограниченно предотвращает попадание загрязнённых потоков в широкое распространение. Возможность торговать «монетами конфиденциаль-

¹⁰ <https://bitshills.com/best-non-kyc-crypto-exchanges/>.

ности», такими как Monero, и растущая популярность платформ DeFi способствуют реализации этих стратегий отмывания денег.

Во-вторых, даже если бы учреждениям, соблюдающим KYC, разрешить иметь дело исключительно с другими KYC-организациями, предотвратить приток испорченных средств по-прежнему будет почти невозможно, разве что кто-нибудь наложит строгие ограничения на то, кто с кем может совершать сделки, и сделает все транзакции подлежащими одобрению аналитическими компаниями типа блокчейн, такими как Bitfury Crystal Blockchain и Chainalysis. Если бы такой режим был реализован, эти фирмы стали бы фактически доверенными сторонами, необходимыми для функционирования сети Биткоин. Но протокол Биткоин предназначен именно для того, чтобы обойти ограничения.

Операции с наличными деньгами и их хранение требуют значительных затрат и создают операционные риски, а операции с криптовалютами и их хранение практически бесплатны (за исключением колебаний стоимости биткоинов). Чем более широкое распространение получит биткоин, тем проще будет использовать его для транзакций без участия регулируемых юридических лиц, и тем более привлекательным он станет для должностных преступлений и теневой экономики.

*Перевод А. И. Земскова, ГПНТБ России
(Продолжение в следующем номере журнала.)*

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

DIGITAL INFORMATION RESOURCES

UDC 004.65:[336.743-021.131]-047.44
<https://doi.org/10.33186/1027-3689-2022-10-100-114>

Blockchain analysis of the Bitcoin market. (Part 2)

Igor Makarov¹, Antoinette Schoar²

¹*London School of Economics Houghton Street London WC2A 2AE UK,
i.makarov@lse.ac*

²*MIT Sloan School of Management 100 Main Street, E62-638 Cambridge, MA 02142
and NBER, aschoar@mit.edu*

Abstract. The detailed analysis of the Bitcoin network and its main participants. The expert authors (Igor Makarov, London School of Economics, Antoinette Schoar, MIT Sloan School of Management) completed the study authorized by the National Bureau of Economic Research (NBER), the US-based private agency.