

## Блокчейн-анализ рынка биткоинов. (Часть 1)

Игорь Макаров<sup>1</sup>, Антуанетта Шоар<sup>2</sup>

<sup>1</sup>Лондонская школа экономики Houghton Street Лондон WC2A 2AE  
Соединённое Королевство, [i.makarov@lse.ac.uk](mailto:i.makarov@lse.ac.uk)

<sup>2</sup>Школа менеджмента MIT Sloan School of management 100 Main Street, E62-638  
Кембридж, Массачусетс 02142 и NBER, [aschoar@mit.edu](mailto: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<sup>1</sup> 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 бит-

---

<sup>1</sup> Оригинальный текст:  
[https://www.nber.org/system/files/working\\_papers/w29396/w29396.pdf](https://www.nber.org/system/files/working_papers/w29396/w29396.pdf).

коинов, 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 1) / И. Макаров, А. Шоар // Научные и технические библиотеки. 2022. № 9. С. 84–97. <https://doi.org/10.33186/1027-3689-2022-9-84-97>

## **Введение**

Созданная более десяти лет назад криптовалюта буквально совершила революцию в денежно-кредитной политике. Значительно поднявшись в цене, сегодня она находится в центре внимания широкой общественности и вызывает противоречивые мнения. Отличительной чертой криптовалюты является децентрализованная система платежей или средств сбережения вне традиционного государственного контроля. Технология блокчейн в основе криптовалюты заменяет зависимость от нескольких организаций, ведущих централизованные учётные записи, таких как банки или сети кредитных карт, на сеть с большим набором децентрализованных и анонимных участников – агентов. Отсутствие централизованной подотчётности и анонимность пользователей часто рассматриваются как основные преимущества, однако в то же время мешают своевременной диагностике состояния здоровья системы, создают множество проблем для регулирующих органов и вводят новые источники систематических рисков.

Биткоин, оригинальная криптовалюта, по-прежнему остаётся самой крупной и популярной монетой, причём её рыночная капитализация выше, чем у всех остальных монет, вместе взятых. Она часто рассматривается как шаблон или эталон для других новых монет. Сегодня многие призывают к ещё более широкому внедрению биткоинов – в качестве инструмента государственных инвестиций либо законного платёжного средства. Это давление ставит в сложное положение регулирующие органы, которые хотят найти правильный баланс между защитой общественных интересов и поддержкой инноваций. Несмотря на то, что биткоины существуют более десяти лет, по-прежнему имеет-

ся много открытых вопросов об их использовании, концентрации собственности, а также структуре основных элементов, которые составляют основу одноимённой экосистемы. Представляется необходимым проведение анализа сети Биткоин и её участников для принятия решения о том, как и каким образом интегрировать эту валюту в традиционную финансовую систему.

В данной статье нами была предпринята попытка дать ответы на эти вопросы с помощью моделирования новой базы данных, которая позволила нам задокументировать эволюцию рынка биткоинов и его различных участников. Для создания этой базы мы использовали большое количество общедоступных и проприетарных источников, которые связывают биткоин-адреса с реальными объектами, и разработали набор алгоритмов, имеющих коммерческий характер блокчейна Биткоин для извлечения информации о поведении основных участников рынка. Созданная нами база данных Биткоин на сегодняшний день считается наиболее полной из тех, которые используются в академических исследованиях.

Мы провели три базовых этапа анализа, в которых основное внимание было уделено наиболее крупным участникам экосистемы Биткоин. Во-первых, проанализировали объём транзакций и структуру сети основных участников блокчейна. Во-вторых, задокументировали концентрацию и региональный состав майнеров, обеспечивающих целостность реестра блокчейн (гроссбуха, леджера). И, наконец, рассмотрели концентрацию собственности крупнейших держателей биткоинов.

**Объём транзакций и структура сети Биткоин.** Для начала мы установили, что 90% объёма транзакций в блокчейне Биткоин не привязано к экономически значимой деятельности, но является побочным продуктом конструкции биткоин-протокола, а также анонимностью участников. Поскольку блокчейн Биткоин – это публичный реестр (гроссбух), все потоки оплаты между адресами прекрасно наблюдаются. Следовательно, многие биткоин-пользователи применяют стратегии, предназначенные для предотвращения их отслеживания, перемещая средства по длинным цепочкам из нескольких адресов и разделяя платежи между ними; в результате чего в большом количестве генерируются ложные объёмы транзакций. Мы разработали алгоритмы для их филь-

трации и фиксации экономически значимых платежей, проводимых между реальными организациями.

Мы доказали, что подавляющее большинство биткоин-транзакций между реальными объектами предназначено для торговых и спекулятивных целей. Начиная с 2015 г. 75% реального объёма транзакций биткоинов было связано с биржами или подобными биржам объектами, такими как онлайн-кошельки, внебиржевые столы, крупные институциональные трейдеры. Другие известные организации несут ответственность только за незначительную часть от общего объёма. Например, незаконные транзакции, мошенничество и азартные игры вместе составляют менее 3%. Доля объёма, связанная с майнерами, ещё меньше.

Биржи не только генерируют наибольший объём, но и являются наиболее активно связанными узлами в сети Биткоин. В частности, у них самый высокий показатель сконцентрированности собственных значений. Кроме того, большая часть объёма транзакций состоит из перекрёстного (межбиржевого) обмена. Высокий кросс-обмен потоков является следствием современной структуры рынка. В отличие от традиционных регулируемых бирж, рынки криптовалют состоят из множества неинтегрированных и независимых бирж без каких-либо гарантий того, что инвесторы получают самые крупные суммы при совершении сделок. В результате согласованность цены биткоинов на биржах оказывается зависима от арбитражёров и спекулянтов, которые через них осуществляют торговлю. В поддержку этой идеи мы наглядно продемонстрировали, что торговля схожими валютными парами имеет более высокий кросс-обмен.

Наши оценки незаконных транзакций намного меньше, чем указывается в других источниках (например, [1]). Одна из причин такого различия заключается в том, что мы располагаем гораздо более подробным и исчерпывающе полным документом идентификации участников блокчейна. В указанной же работе авторы опираются на условно вычисляемую сеть, в которой любой биткоин-адрес рекурсивно классифицируется как принадлежащий незаконному объекту, если большинство его транзакций осуществляется с адресами, ранее признанными незаконными. Однако этот метод приводит к значительному завышению незаконных объёмов, поскольку не идентифицирует различия между реальными пользователями и ложными.

Мы доказали, что сконцентрированность собственных значений может служить новым и полезным показателем для ранжирования объёма и важности обменов, поскольку он основан на кросс-бирже потоков биткоинов в блокчейне и поэтому, вероятно, будет более устойчивым к манипуляции, чем другие меры.

Сильная взаимосвязанность бирж имеет важные последствия для обеспечения прозрачности и отслеживаемости транзакций, а в особенности для обеспечения соблюдения норм «знай своего клиента» (KnowYour-Customer, KYC) во всей сети. В настоящее время акцент в регуляторных усилиях по обеспечению большей прозрачности достигается посредством соблюдения этих норм и налоговой отчётности о приросте капитала на уровне отдельных учреждений, таких как биржи или платёжные системы. Однако, если пользователи биткоинов смогут свободно торговать регулируруемыми и нерегулируемыми биржами даже со странами с разными уровнями правоприменения, эффективное регулирование системой KYC может оказаться невозможным на уровне отдельных институтов.

Для изучения потоков на рынке биткоинов мы использовали в качестве примера Hydra Market, которая является одной из крупнейших торговых площадок в даркнете. Наш анализ показал, что наибольшее количество организаций, напрямую взаимодействующих с пользователями Hydra Market, в том числе Binance и Huobi – две крупнейшие биржи в мире, не являются биржами, соблюдающими KYC. Как только финансовые потоки поступают на эти биржи, они смешиваются с другими и становятся виртуально не отслеживаемыми, а потому могут быть отправлены впоследствии куда угодно, даже на биржи, которые применяют нормы KYC. Напротив, прямое взаимодействие бирж, соблюдающих KYC, таких как Coinbase или Gemini, с пользователями Hydra Market весьма скромно. Но их косвенное взаимодействие с потоками рынка Hydra Market значительно больше, так как эти потоки направляются через сеть недолговечных кластеров, созданных исключительно с целью запутывания происхождения этих средств.

Эти результаты показывают, что организации, не поддерживающие KYC, служат шлюзом для «отмывания» денег и других «серых» действий. Децентрализованный характер протокола Биткоин упрощает работу этих учреждений – им нужно только иметь свои серверы в стране, в которой власти готовы мириться с их существованием. Если компаниям, выполняющим нормы KYC, разрешено принимать потоки от организаций, которые не соблюдают строгие нормы KYC (а это именно так на текущий момент), то цифровой след имеет очень ограниченное влияние на предотвращение поступления в широкое обращение сомнительных потоков.

Даже если организациям, выполняющим нормы KYC, будет разрешено иметь дело исключительно с организациями, также выполняющими нормы KYC, предотвратить приток испорченных средств будет почти невозможно в случае, если вы не готовы к строгим ограничениям на совершение сделок и установлению контроля над совершениями всех транзакций (похожие схемы работы предоставляют такие компании, как Bitfury Crystal Blockchain или Chainalysis). Потенциальная реализация такого режима предполагает, что объектом мониторинга блокчейна станут де-факто доверенные стороны, необходимые для функционирования сети Биткоин.

**Состав биткоин-майнеров.** На втором этапе анализа мы исследовали концентрацию и региональный состав биткоин-майнеров, которые несут ответственность за обработку и проверку транзакций сети Биткоин и поддерживают её целостность, за что получают оплату в виде вновь созданных биткоинов.

Проверка протокола сети Биткоин позволила установить, что её функционирование требует честности работы децентрализованных майнеров и безупречности ведения учёта бухгалтерской книги биткоинов. В случае нарушения механизма управления системой финансовая стабильность и безопасность сбережений могут оказаться под угрозой.

Поэтому важно понимать, насколько сконцентрированы майнинговые мощности. В ранее опубликованных работах основное внимание уделялось концентрации майнинговых пулов. По дизайну системы вероятность получения блока и получения вознаграждения за блок в цепочке биткоинов пропорциональна мощности хеширования, затрачиваемого на добычу. Это даёт майнерам возможность объединения своих вычис-

лительных мощностей и совместного страхования друг друга. Как следствие, в майнинге блокчейна Биткоин преобладают майнинговые пулы.

Но в то время как пулы функционируют как агрегаторы хеш-мощности и, следовательно, могут оказывать существенное влияние на протокол Биткоин, они не обязательно контролируют своих майнеров. Как сообщает [2], власть оператора пула по отношению к майнеру зависит от лёгкости, с которой майнеры могут перемещать мощность между пулами, что, в свою очередь, зависит от основного распределения майнеров по размеру.

В отличие от общедоступности информации о пулах для майнинга, информации об отдельных майнерах пока нет. Их идентификация осуществляется путём отслеживания распределения вознаграждений за майнинг от 20 крупнейших майнинговых пулов до майнеров, которые на них работают. Поскольку каждый пул использует свой алгоритм для распределения вознаграждений, мы создали отдельные алгоритмы для каждого пула. Насколько нам известно, это первое исследование, в котором установлена точная связь майнеров с их пулами для майнинга.

Наиболее крупные 10% майнеров контролируют 90% майнинговых мощностей и всего 0,1% (около 50 майнеров) – примерно 50% майнинговых мощностей. Кроме того, эта концентрация мощности майнинга является контрциклической и зависит от цены биткоинов. Она уменьшается после резкого роста цены биткоинов и увеличивается в периоды ценопадения. Таким образом, риски атаки на блокчейн (атаки 51%) увеличиваются при резком падении цены биткоина.

Кроме того, мы доказали, что существует значительная географическая кластеризация майнеров. Как показал наш анализ, подавляющее большинство майнинговых пулов зарегистрировано в Китае (от 60% до 80% по данным на 2015 г. – апрель 2020 г.). Однако это совершенно не означает, что майнеры должны находиться там же. Основные данные об их местонахождении получены путём анализа IP-адресов из нескольких избранных пулов. В тот момент, когда майнер подключается к серверу пула, оператор может видеть IP-адрес майнера (если майнер не использует VPN-адрес). Оператор пула может использовать этот IP-адрес для определения географического положения. Имея возможность отслеживания адресов майнеров и транзакции биткоинов, мы можем видеть, на каких биржах они обналичивают свои вознаграждения. Как правило,

майнеры, находящиеся в определённом регионе, отправляют свои сбережения на биржу, также расположенную в этом регионе.

Чтобы проверить правильность нашего подхода к определению местоположения майнеров с помощью отслеживания того места, где они обналичивают свои биткоин-вознаграждения, мы использовали статистику за апрель 2021 г. по китайской провинции Синьцзян. После разрушительной аварии на угольной шахте правительство остановило добычу угля и отключило электроснабжение всего района почти на двое суток. Отключение электричества повлекло за собой массовое обналичивание биткоинов в регионе. Это помогло нам установить, что многие китайские майнеры располагались именно здесь, вероятно, из-за дешёвых поставок угля, за счёт которых работают электростанции.

**Концентрация собственности.** Наконец, мы изучили владельцев биткоинов. С момента появления сети Биткоин наблюдается большой интерес к личности крупнейших владельцев биткоинов и размеру их капитала. Существуют веб-сайты, посвящённые отслеживанию их адресов, на которых публикуется так называемый «богатый список», один из самых известных и популярных списков в криптосообществе. Но вопрос концентрации собственности – это не только любопытство. С точки зрения государственной политики, важно, кто получит наибольшую выгоду от повышения цен, которое произойдёт, если регулирующие органы разрешат более широкое внедрение биткоинов, – несколько избранных инвесторов или широкая публика?

Определение концентрации собственности сложнее, чем просто отслеживание авуаров самых богатых адресов, поскольку многие из них принадлежат «холодным кошелькам» бирж и онлайн-кошелькам, в которых хранятся биткоины инвесторов. На основе анализа граф мы разработали набор алгоритмов для классификации адресов, принадлежащих индивидуальным инвесторам или посредникам.

Полученные нами данные свидетельствуют о том, что остаток на счетах у посредников с 2014 г. неуклонно растёт. К концу 2020 г. он составил 5,5 млн биткоинов, примерно треть из них находится в обращении; 8,5 млн биткоинов контролируется индивидуальными инвесторами; высока концентрация биткоинов в холдингах: 1 тыс. крупнейших инвесторов контролируют около 3 млн, а 10 тыс. – около 5 млн.



Следующий этап анализа имел своей целью документирование эволюции объёма вложений различных участников блокчейна. В частности, мы разработали алгоритмы для отделения ложного объёма биткоинов от реального, а затем отобразили сетевую структуру участников. Далее мы осуществили анализ майнеров, их состав и географическую концентрацию, а также зафиксировали концентрацию собственности участников биткоинов.

**Данные сети Биткоин.** Все транзакции с биткоинами регистрируются в распределённой публичной книге (гроссбухе). Организованные в блоки, они добавляются в реестр в среднем каждые 10 минут. Один блок содержит несколько тысяч биткоин-транзакций, включающих в себя список отправителей и получателей, представленных адресами – псевдонимами, количество отправленных и полученных биткоинов, а также отметку о времени сделки.

Мы осуществили загрузку данных блокчейна, используя программное обеспечение с открытым исходным кодом Bitcoin Core [3] и программу BlockSci [4] для разбиения необработанных данных на отдельные транзакции. По статистике на 28 июня 2021 г. было создано 689 тыс. блоков из 652 млн транзакций биткоинов и 896 млн адресов, организованных в базе данных блокчейна объёмом более 379 Гб.

Адрес в блокчейне можно рассматривать как банковский счёт. Любой человек может отправлять биткоины на любой адрес. Но чтобы отправить биткоины с заданного адреса, нужно знать пароль, связанный с этим адресом. В отличие от банковских счетов биткоин-адреса могут быть сгенерированы свободно, поэтому обычно один и тот же владелец управляет несколькими адресами, а в некоторых случаях даже десятками миллионов различных адресов. Сообщество Биткоин разработало несколько эвристических алгоритмов для назначения адресов одним и тем же организациям. В качестве отправной точки мы используем наиболее консервативный метод кластеризации адресов, при этом все адреса, которые отправляют биткоины в любой отдельной транзакции, считаются принадлежащими к одному и тому же учреждению либо лицу. Эти алгоритмы оправданы протоколом Биткоин, который требует, чтобы подписывающая транзакцию сторона имела контроль над всеми выходными адресами.

Отметим, что некоторые сервисы, например CoinJoin, позволяют пользователям смешивать биткоины с монетами других пользователей, по этой причине программа BlockSci избегает транзакций CoinJoin в своём алгоритме кластеризации.

На практике пользователю обычно достаточно указать адрес назначения перевода и его сумму. Специальная программа, называемая кошельком, сама решает, с каких адресов отправлять биткоины, эквивалентные той сумме, которую пользователь хочет перевести. Затем этот процесс позволяет алгоритму кластеризации успешно сгруппировать все адреса пользователей вместе. Однако следует подчеркнуть, что пользователь может намеренно скрыть связи между своими адресами; в этом случае кластеризация определяет только нижнюю границу количества отдельных сущностей (людей, организаций).

Чтобы связать кластеры адресов с реальными объектами, мы использовали блоги и веб-сайты с криптовалютой, такие как Reddit, Blockchain.info, bitinfocharts.com, bitcointalk.org, walletexplorer.com, Matbea.com, для всех общедоступных адресов известных компаний Биткоин (бирж, платёжных систем, сайтов азартных игр и др.). Мы дополнили эту информацию современной базой данных криптосущностей от Bitfury Crystal Blockchain – одного из ведущих поставщиков инструментов для борьбы с отмыванием денег и аналитических решений в криптопространстве. Материалом для нашего исследования послужили 1 043 сущности, из них 393 биржи, 86 игорных сайтов, 39 онлайн-кошельков, 33 платёжных процессора, 63 пула для майнинга, 35 мошенников, 227 злоумышленников, 151 нелегальный рынок или сервис.

**Объём транзакций блокчейна. Ложный объём.** Дизайн блокчейна Биткоин и анонимность многих его пользователей создают массу ложного объёма транзакций, который не привязан к экономически значимым сделкам. В этом разделе мы постарались описать, как мы идентифицируем и отделяем этот объём от реального, то есть платежей за товары и услуги и другие финансовые переводы между двумя сторонами.

Поучительно и полезно начать с рассмотрения конкретного примера транзакции<sup>2</sup>, изображённой на рис. 1 «Транзакции

---

<sup>2</sup> Вторую транзакцию в блоке 600000 можно увидеть, например, по адресу <https://explorer.btc.com/btc/block/600000>.

биткоинов и ложный объём» (оригинал рисунка здесь: [https://www.nber.org/system/files/working\\_papers/w29396/w29396.pdf](https://www.nber.org/system/files/working_papers/w29396/w29396.pdf)). Это типичная транзакция блокчейна биткоинов с большим ложным объёмом. С адреса отправителя «17A16Q...» в левой части гроссбуха отправлены средства по трём адресам. Адрес последнего из трёх получателей, которому отправляется наибольшая сумма, совпадает с адресом отправителя.

В приведённой в пример транзакции участник с адресом «17A16Q...» отправляет валюту со своего баланса по следующим трём адресам: «3QKAn2...», «1F8fDp...» и «17A16Q...». Сумма полученных средств равна отправленной сумме за вычетом небольшой комиссии в размере 0,001 биткоина, которая составляет вознаграждение за блок.

Стоит отметить, что последний из трёх адресов совпадает с адресом отправителя, то есть адрес «17A16Q...» отправляет большую часть своего баланса сам себе. Это означает, что общий объём данной транзакции в блокчейне достаточно большой, однако экономически значимый (реальный) объём, генерируемый в результате транзакции, то есть обмен между разными объектами, невелик.

Вышеупомянутая ситуация, когда участник отправляет свою сумму самому себе или на другой адрес, контролируемый одним и тем же лицом, очень распространён. Отчасти это следствие конструкции протокола Биткоин. Непогашенный остаток по адресу не сохраняется, но рассчитывается из всей истории транзакций, связанных с этим адресом, и будет виден при просмотре реестра биткоинов. Для вычислительной эффективности биткоин-протокол позволяет отправлять только те суммы, которые были ранее получены данным адресом. Например, предположим, что на адрес ранее были получены 5, 7 и 10 биткоинов, поэтому непогашенный остаток составляет 22 биткоина. Чтобы отправить 8 биткоинов с этого адреса, можно либо отправить 10 биткоинов, либо любую из следующих линейных комбинаций: 5 + 7, 5 + 10, 7 + 10, 5 + 7 + 10. Так как в любом случае сумма превышает 8 биткоинов, отправителю необходимо собрать разницу, используя один из своих адресов. Этот процесс создаёт большое количество ложного объёма, который скрывает истинный объём транзакций в цепочке блоков.

Ещё одна распространённая причина возникновения ложного объёма – это анонимность участников блокчейна. Поскольку блокчейн

биткоинов является публичной книгой, все потоки платежей между адресами прекрасно наблюдаются. Поэтому многие пользователи выбирают стратегии, предназначенные для предотвращения отслеживания потоков биткоинов.

Рассмотрим, например, ситуацию, когда хакер требует, чтобы платёж от компании был отправлен на адрес биткоинов, который он контролирует. Поскольку адрес выкупа является общедоступной информацией, если хакер позже отправит биткоины с этого адреса третьему лицу, сторона может легко заявить, что средства поступают в результате незаконной деятельности. Чтобы этого не произошло, хакеры часто пытаются скрыть трассировку, создавая несколько адресов и разделяя первоначальный взнос между ними. Этот процесс обычно повторяется много раз, в результате чего возникают так называемые «цепочки отслаивания», когда средства перемещаются на большое расстояние от одного адреса к другому, что приводит к появлению большого количества записей фиктивных адресов в бухгалтерской книге.

Цепочки отслаивания также широко используются многими биржами, такими как Coinbase и Kraken, и многими пулами майнинга. Эти учреждения каждый раз, когда им нужно создать изменения (как в транзакции на рис. 1), генерируют новый адрес вместо повторного использования старого адреса. Затем этот новый адрес применяется для отправки средств другому лицу, и изменения собираются по другому новому адресу. Процесс обычно повторяется много раз, пока не будет израсходован весь первоначальный баланс. Адреса в цепочках отслаивания обычно используются только для мгновенного получения и немедленной отправки биткоинов с типичным сроком службы 10 часов.

Существует два способа учёта транзакций цепочки отслаивания. Первый способ предполагает возможность изменения алгоритма кластеризации, чтобы добавить адреса в цепочках отслаивания к соответствующим кластерам. Другой подход, которому мы следуем в этой статье, – это возврат переходов в цепочках отслаивания до исходных кластеров и отбрасывание всех любых промежуточных адресов из дальнейшего анализа. Для этого мы разработали эффективный рекурсивный алгоритм, подробно описанный ниже.

Выделение цепочек отслаивания снижает вычислительную нагрузку и приводит к значительному сокращению адресов и кластеров.

Исходная база данных насчитывает 896 млн адресов, однако если удалить адреса в цепочках отслаивания, получится 640 млн. Эти адреса принадлежат 189 млн кластеров, из которых 116 млн являются одноадресными.

На рис. 2 «Разделение объёма на компоненты: внутренний, сквозной и реальный объём» (оригинал рисунка здесь: [https://www.nber.org/system/files/working\\_papers/w29396/w29396.pdf](https://www.nber.org/system/files/working_papers/w29396/w29396.pdf)) показано разложение общего объёма блокчейна Биткоин на то, что мы называем внутренним/сквозным/реальным объёмом. Внутренний объём – это объём, который создаётся, когда кластер отправляет биткоины самому себе. Сквозной объём – это переходный объём, связанный с отслаивающимися цепями. Наконец, реальный объём – это оставшийся объём, который представляет собой переводы между кластерами. Он составляет только 10% от общего объёма биткоинов на блокчейне; 90% объёма не привязаны к экономически значимым сделкам.

Верхняя (оранжевая) часть на рисунке показывает сквозной объём, который создаётся, когда пользователи перемещают свои средства по длинным цепочкам из нескольких адресов (так называемым отшелушивающим цепочкам) и делят между ними платежи, чтобы препятствовать отслеживанию потоков. Следующая часть (жёлтая) показывает внутренний объём, который генерируется, когда пользователь (кластер) отправляет сам себе биткоины. Наконец, оставшаяся часть (зеленая) – настоящий (истинный) объём, который представляет собой переводы между кластерами, контролируемые разными пользователями.

Публикация результатов масштабного анализа сети Биткоин будет продолжена в следующих номерах журнала.

*Перевод А. И. Земскова, ГПНТБ России  
(Продолжение в следующих номерах 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/> (дата обращения: 05.08.2022).
4. **BlockSci.** URL: <https://github.com/citp/BlockSci> (дата обращения: 05.08.2022).
5. **Ron D., Shamir A.** Quantitative Analysis of the Full Bitcoin Transaction Graph. URL: <https://eprint.iacr.org/2012/584.pdf> (дата обращения: 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](mailto: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](mailto:aschoar@mit.edu)