Эвристические методы кластеризации адресов в распределенных реестрах

Д. А. Зенюк

Институт прикладной математики им. М. В. Келдыша РАН, Москва

eldrich@yandex.ru

Аннотация

В работе дан обзор эвристических методов кластеризации адресного пространства публичных распределенных реестров. Упомянутые техники опираются на достаточно простые наблюдения за поведением типичных пользователей и здравый смысл. Формально эвристики представляют собой вырожденные решающие правила, которые не предполагают подбора параметров в ходе обучения по заранее отобранным данным. Можно также считать, что эвристикам соответствуют устойчивые мотивы в графовых представлениях истории транзакций. Несмотря на кажущуюся простоту и отсутствие возможности проверить правильность результатов их работы, эти подходы демонстрируют достаточно хорошую эффективность и зачастую их применение предваряет использование гораздо более сложного инструментария на основе современного машинного обучения и искусственного интеллекта. Приведены эвристики для Bitcoin, Ethereum, Ripple, Monero и Zcash. Кратко рассмотрен пример эвристической кластеризации по данным о cross-chain транзакциях. Отмечены случаи, когда эвристики дают некорректные результаты. Насколько можно судить, обзор такого рода публикуется на русском языке впервые.

Ключевые слова: блокчейн, миксеры, анализ транзакций, криптоактивы, анонимность, эвристики, кластеризация.

Классификация JEL: E42, G18, K24.

Address Clustering Heuristics for Distributed Ledgers

Dmitry A. Zenyuk

Keldysh Institute of Applied Mathematics, the Russian Academy of Sciences, Moscow

Abstract

The paper surveys heuristic methods of clusterization in address space of public distributed ledgers. The techniques mentioned rely on collecting behavioral patterns of typical actors and some common sense. Formally heuristics are degenerate clusterization rule-based algorithms, which do not tune their parameters via learning on curated datasets. They can be treated also as persistent motifs in transaction networks. Despite its seeming simplicity and inability to assess correctness of the results such approach demonstrates a reasonable effectiveness and often is used as a preliminary step before applying much more sophisticated tools based on machine learning algorithms and AI. Heuristics for Bitcoin, Ethereum, Ripple, Monero and

Zcash are discussed. Heuristic clusterization in cross-chain setting is briefly mentioned. Cases when heuristic approach leads to incorrect results are discussed.

Keywords: blockchain, tumblers, transaction analysis, cryptoassets, anonymity, heuristics, clusterization.

JEL codes: E42, G18, K24.

Введение

Настоящий текст представляет собой обзор публикаций по тематике трассировки транзакций и идентификации принадлежности адресов в распределенных реестрах, таких как Bitcoin или Ethereum. Поскольку во всем мире сейчас предъявляются все более высокие требования к регуляции этих систем, связанные с соблюдением национальных законов о борьбе с отмыванием денег, развитие соответствующих алгоритмических методов становится необходимым условием выживания крупных институциональных игроков на этом рынке.

Bitcoin является, пожалуй, самым известным примером распределенной транзакционной сети. Экосистема Bitcoin была полностью описана в 2008 г. (Nakamoto 2008) и представляла собой попытку создать жизнеспособную платежную инфраструктуру, в которой доверие основано не на участии авторизованных посредников (брокеров, банков, клиринговых агентств), а только на алгоритмических принципах. Широкий интерес к ней пришел лишь в первой половине 2011 г. после публикации в журнале Forbes и достижения рыночной стоимости в 1 доллар США, а начиная с 2013 г. Bitcoin и подобные ему системы стали одной из центральных тем в дискуссии о будущем мировой финансовой индустрии.

Bitcoin изначально был спроектирован как система, где не требуется никакого априорного доверия между участниками, т. е. как потенциально небезопасная среда. Это обстоятельство является одной из причин использования псевдонимов, скрывающих реальные личности участников. Этим Bitcoin и другие подобные системы существенно отличаются от привычных платежных систем, где все участники движения средств достоверно известны с самого начала. Однако именно из-за этой особенности Bitcoin стал весьма популярен на сером и черном рынках. С его помощью оформляли сделки по продаже товаров с ограниченным оборотом, уходили от налогов и спонсировали террористические группировки по всему миру, см., например, (Foley 2019). Там же годовой оборот Bitcoin за 2019 г., связанный со всей нелегальной торговлей, оценен в 76 млрд. долларов США, что составило 46% от совокупного объема транзакций.

После непродолжительной «растерянности» фискальные и монетарные власти по всему миру начали процесс постепенного ужесточения регуляции рынка децентрализованных цифровых активов. Сейчас все легальные участники рынка, осуществляющие операции с этими активами, обязаны проводить процедуры *anti-money laundering/know-your-customer* (AML/KYC), аналогичные тем, что выполняют обычные банки. Одним из элементов этого процесса является уточнение источников средств транзакции. Таким образом, весьма актуальным становится поиск алгоритмических инструментов для трассировки транзакций, позволяющих с высокой степенью уверенности устанавливать, были ли средства на конкретном адресе (см. определение ниже) когда-либо ранее замечены в противоправной или даже просто подозрительной активности. С одной стороны, эта задача сильно осложнена тем, что в этих системах не требуется никакой идентификации пользователей, кроме обладания приватным ключом (см. далее), который необходим для электронной подписи. Более того, после триумфа Bictoin были специально разработаны системы (к примеру, Zcash и Monero), в которых обеспечение анонимности стало основной целью. В то же самое время, особенности функционирования распределенных систем, такие как наличие гарантии неизменности истории транзакций и использование протоколов поиска консенсуса, основанных на криптографии с открытым ключом, напротив, несколько облегчают анализ — если только удастся надежно связать адреса-псевдонимы с конкретными людьми.

Ужесточению регуляции сопутствует поощрение исследовательской работы в этой области. Так, с 2017 по 2020 гг. в Европейском союзе действовал проект TITANIUM, выполняемый консорциумом европейский технических институтов и министерств внутренних дел при участии Интерпола. Некоторые статьи, цитируемые далее, были выполнены в рамках этого проекта. Методы

трассировки транзакций, которые сейчас объединяют под названием *know-your-transactions* (KYT), примыкают к другим методам цифровой криминалистики (*digital forensics*), которые сейчас активно развиваются в ответ на прогресс в областях искусственного интеллекта и Интернета вещей. Появились частные компании, специализирующиеся на проведении расследований подобного рода с использованием новейших разработок в области машинного обучения и анализа данных, такие как Chainalysis, CipherTrace, Elliptic, Bitfury (проект Crystal), IdentityMind, Scorechain, Traceer, Blockseer.

Говоря о задаче кластеризации адресов, необходимо подчеркнуть, что это более слабая постановка по сравнению с задачей атрибуции или деанонимизации. Действительно, в первом случае нам достаточно лишь с высокой уверенностью указать наборы псевдонимов, принадлежащих одному и тому же актору (см. определение ниже). При этом не нужно знать, кем именно является этот актор. Решение второй задачи — деанонимизации — является гораздо более трудным и по всей видимости не может быть полностью автоматизировано, поскольку для этого почти наверняка придется вручную собирать информацию помимо той, что хранится в распределенном реестре. Дать конкретный перечень такой информации, которая позволит связать сетевые псевдонимы с конкретными акторами, весьма трудно. Это могут быть IP-адреса, метки времени и геолокации, данные веб-трекеров, записи на форумах и их стилистика, привычки и даже хобби и т. д. Более подробное обсуждение аспектов анонимности и проблемы деанонимизации в блокчейнах см. в (Amarasinghe 2019).

Терминология и понятийный аппарат

В самом общем случае транзакцией называется набор инструкций, исполнение которых обязательно должно привести к изменению текущего состояния реестра, с электронной подписью отправителя. Обычно под инструкциями понимается перевод активов с одного адреса на один или несколько других. Возможны и более сложные наборы инструкций, которые вызывают функции, определенные в смарт-контрактах (*smart-contracts*), но в настоящем тексте они рассматриваться не будут. Больше о смарт-контрактах см. в (Zheng 2020).

Формально транзакция представляет собой стандартизованную запись с числовыми и текстовыми полями. Формат зависит от конкретной сети, но по крайней мере пять полей есть всюду: это уникальный идентификатор транзакции, набор адресов отправителей, набор адресов получателей, объем переводимых средств (который далее для удобства также будет называться суммой) и отметка времени. В различных реестрах существуют специальные типы транзакций, необходимые для поддержания заявленного функционала, но эти различия несущественны для дальнейшего изложения. Информация о транзакциях в открытых реестрах не шифруется и публично доступна для любого узла в сети.

Адреса — это уникальные псевдонимы, используемые для идентификации участников транзакций. Каждая транзакция должны иметь электронную подпись отправителя, а для этого нужна асимметричная пара ключей. Приватный (закрытый) ключ используется для создания подписи, а публичный (открытый) ключ позволяет быстро проверить правильность этой подписи. Таким образом, для стороннего наблюдателя публичный ключ становится идентификатором отправителя, гарантированно уникальным. Хеши публичных ключей называются адресами. Обладание приватным ключом является единственным допустимым подтверждением владения активами на балансе соответствующего адреса. В реестре можно встретить только те адреса, баланс которых хотя бы один раз был ненулевым. В наиболее популярных реестрах любой актор может создавать сколь угодно много пар ключей, а значит, и адресов. Адреса обычно не дают никакой информации о тех акторах, которым они принадлежат, хотя иногда можно встретить адреса, содержащие определенный намек — в большинстве случаев это делается намеренно самим владельцем адреса.

На физическом уровне любой распределенный реестр (*distributed ledger*) представляет собой одноранговую (*peer-to-peer*, P2P) сеть, узлы которой могут одновременно и выступать в качестве клиентов, и брать на себя функции серверов. Как и любая другая P2P сеть, распределенные реестры являются оверлейными сетями, т. е. они созданы «поверх» уже существующих коммуникационных сетей, и обмен сообщениями между узлами выполняется по стандартным транспортным протоколам (обычно это стек TCP/IP). Узлы хранят информацию об уже подтвержденных транзакциях — либо всю историю, либо какую-то ее часть. За счет такого многократного дублирования информации достигается устойчивость всей системы: даже если часть узлов выйдет из строя, вся история

транзакций может быть восстановлена по тем фрагментам, что хранятся на оставшихся узлах. Хорошее общее представление о технологии распределенных реестров можно найти, к примеру, в (Natarajan 2017).

Блокчейн (калька с англ. *blockchain*) — это одна из форм реализации распределенного реестра. Нестрого, основная идея заключается в том, что информация в таком типе реестров хранится отдельными блоками, которые сцеплены между собой за счет того, что последний блок хранит внутри хеш предыдущего. Поскольку надежные хеш-функции являются вычислительно необратимыми, информация, хранимая в такой структуре, с высокой долей уверенности может считаться неизменной. Действительно, если бы потенциальный злоумышленник захотел бы изменить даже всего один символ в конкретном блоке, то хеш этого блока сразу бы изменился и пришлось бы менять соответствующим образом и все последующие блоки. Воплощение этой идеи требует решения множества сопутствующих проблем, описание которых выходит далеко за рамки настоящего текста. Заинтересованный читатель может найти дополнительную информацию в (Tschorsch 2016; Narayanan 2016).

Важным условием функционирования распределенных реестров является гарантия того, что представления о текущем состоянии реестра, хранящиеся на разных узлах, являются непротиворечивыми. Для этого в современных распределенных реестрах используются различные протоколы консенсуса. К примеру, в Bitcoin консенсус основан на схеме подтверждения выполнением вычислительной работы (*proof-of-work,* PoW) по поиску решения задачи отыскания хеша с заданным количеством нулей. Основная идея в том, что задача должна быть достаточно сложной — в случае Bitcoin она решается только полным перебором. Изучение протоколов консенсуса представляет собой отдельную и весьма интересную проблему, которая отсылает к т. н. задаче о византийских генералах (см. классическую работу (Lamport 1982)): можно ли создать такой алгоритм обмена сообщениями, который позволяет установить истинность любого высказывания в системе, где априорно никому нельзя доверять? Дополнительные сведения о протоколах консенсуса см., например, в (Nguyen 2018).

Как уже было отмечено выше, на сегодняшний день существует большое количество разных реализаций идеи распределенного реестра и даже самого блокчейна, которые отличаются друг от друга алгоритмическими и инженерными решениями. Для дальнейшего изложениями нам, однако, понадобится представление лишь о двух основных моделях транзакций, которые получили наибольшее распространение. Хронологически первой появилась модель *unspent transaction output* (UTXO), апробированная в сети Bitcoin. Здесь у каждой транзакции есть один или несколько выходов, которые описываются кортежем из уникального номера, суммы и адреса. Эти выходы становятся входами для последующих транзакций, которые как бы «тратят» эти выходы. При этом использовать еще не потраченный выход можно только целиком, а неиспользованные средства затем появятся в качестве нового выхода на том же или другом адресе. Такая особенность, как вскоре будет видно, используется для кластеризации, поскольку у акторов возникает потребность регулярно направлять «сдачу» на другие принадлежащие им адреса. Балансы адресов явно нигде не хранятся — их можно вычислить, но только просмотрев всю историю транзакций вплоть до текущего момента. Другая популярная модель, которая была предложена создателями Ethereum, выглядит более привычно. Состоянием реестра в ней является список записей уникальных адресов и балансов на них. Существенная разница заключается в формате самих транзакций: в модели UTXO каждая транзакция может иметь множество входов и выходов, а в модели балансов у транзакций один вход и один выход.

Криптоактивы (*cryptoassets*), криптовалюты (*cryptocurrencies*) и токены — все это цифровые активы, для создания и использования которых используются криптографические алгоритмы и распределенные реестры. Подробная таксономия не имеет здесь большого значения. Отметим лишь, что криптоактивы можно разделить на нативные криптовалюты, такие как BTC, ETH или XMR, которые непосредственно «хранятся» в реестре и являются неотъемлемым условием функционирования этих сетей (поскольку именно в них выплачивается награда за поддержание работоспособности протокола консенсуса), и токены, такие как CRV, UNI, USDT, которые «выпускаются» с помощью смарт-контрактов. Особую популярность получили токены стандарта ERC20, использующие богатые возможности блокчейна Ethereum.

Под сущностями (*entities*) и акторами (*actors*) будут пониматься частные лица, коллективы или организации, владеющие одним или несколькими адресами (что означает — владеющие соответствующими приватными ключами). С позиций AML/KYC различение адресов и сущностей важно, поскольку операции с «грязными» активами характеризуют именно сущности, а не адреса по-отдельности. В настоящем тексте будет использоваться также термин «актор» в качестве синонима для «сущность».

Миксеры (*mixers*, *tumblers*) — это специальные сервисы для усложнения трассировки транзакций. Они возникли как ответ на первые работы по трассировке и эмпирическому анализу графов транзакций, которые показали, что распределенные реестры вовсе не гарантируют полной анонимности. Миксеры используют различные алгоритмические схемы, которые приводят к созданию длинных цепей из множества фиктивных транзакций, где активы разных акторов сначала объединяются на адресах, созданных самим сервисом, а затем снова расщепляются, направляясь на указанные пользователями адреса. Более подробное описание таких схем см., например, в (Möser 2013; Amarasinghe 2019) и цитированной там литературе.

Сама структура транзакций, в которой обязательно должна быть отражена информация об отправителях и получателях средств, делает одним из наиболее естественных подходов к их исследованию аппарат теории графов. Наиболее полное описание истории транзакций в UTXO-блокчейнах дает граф адресов и транзакций (AT-граф). Он представляет собой двудольный ориентированный граф, в котором различаются вершины-адреса и вершины-транзакции. Ребра могут идти только от адресов отправителей к транзакции, а от нее — к адресам получателей.

AT-граф заключает в себе всю доступную информацию о совокупности рассматриваемых транзакций, но в силу своей огромной размерности он обычно непригоден для непосредственного анализа и визуализации. Поэтому на его основе можно создать несколько редуцированных графов, которые дают более компактное представление. Так, граф транзакций (T-граф) представляет собой направленный ациклический граф, в котором каждая вершина соответствует транзакции. Если выход транзакции был использован как вход в другой транзакции, то соответствующие вершины в графе соединяются ребром, направление которого совпадает с движением средств. Для не потраченных выходов используются специальные фиктивные вершины. Такое представление, очевидно, будет иметь смысл только для UTXO-блокчейнов.

Другой, гораздо более популярный способ редукции — это граф адресов (A-граф). Его вершины отождествляются с адресами, а направленные ребра — с транзакциями. Вершина, из которой ребро исходит, соответствует отправителю, а та, в которою оно входит — получателю. В строгом смысле, эти конструкции являются мультиграфами, поскольку одни и те же адреса могут участвовать в нескольких различных транзакциях, что порождает кратные ребра. A-графы могут быть построены для любого блокчейна, а не только для тех, которые используют модель UTXO. Следующий уровень редукции дает граф сущностей (E-граф), который можно получить из A-графа, применив ко множеству его вершин какие-либо алгоритмы, позволяющие «конденсировать» все адреса, принадлежащие одному и тому же актору, в одну вершину. Собственно, именно такое представление будет наиболее полезным для выполнения AML-расследований. Хорошее изложение подходов к построению различных графовых структур для современных блокчейнов дано в (Akcora 2022). Отметим здесь в заключение, что пока терминология для графовых представлений не стала общепризнанной, и поэтому, к примеру, то, что здесь называется A-графом, в других публикациях может называться сетью транзакций (*transaction network*) или как-нибудь еще.

Достаточно подробный реферативный обзор работ по анализу графов, представляющих транзакции в различных блокчейнах, дан в (Wu 2021). Из этого обзора следует, что так или иначе исследовались все структурные свойства графов: распределения степеней вершин, индексы центральности, клики и компоненты связности в слабом или сильном смыслах, типичные мотивы, ассортативность, свойства кратчайших путей.

Эвристики кластеризации

Для перехода от A-графа к более компактному E-графу необходимо выполнить кластеризацию адресного пространства. Здесь под кластерами понимается максимальный по включению набор уникальных адресов, которые принадлежат одному и тому же актору. Точного решения для этой

задачи не существует, поскольку соответствующей информации о принадлежности адресов нет, и скорее всего, никогда не будет в наличии. Для приближенного же решения предложено множество эвристических методов. Само название подчеркивает, что эти техники не дают никаких гарантий того, что результат будет правильным.

Обоснование эвристик может быть разным. Оно может следовать из особенностей протокола, по которому функционирует сеть — характерным примером является эвристика множественных входов, основанная на том, как подписываются транзакции в сети Bitcoin и похожих на нее. Существуют эвристики, основанные на часто повторяющихся поведенческих паттернах пользователей. Предваряя обзор эвристик, заметим, что их результативность может существенно меняться со временем, вслед за меняющими привычками пользователей сети или эволюцией самих протоколов. Более того, самый факт публикации описания эвристики в открытом доступе может привести к тому, что заинтересованные в сохранении анонимности акторы начнут специально создавать транзакции, нарушающие логику работы этих эвристик, возможно даже за счет некоторого убытка (например, чтобы обмануть эвристику, им придется заплатить бóльшую комиссию). Тем не менее эвристики кластеризации, даже те, что были предложены еще до 2017 г., остаются весьма популярным и, что более важно, эффективным инструментом.

Больше всего эвристик было предложено для Bitcoin и подобных ему UTXO-блокчейнов. Хронологически первым методом кластеризации адресов стала эвристика множественных входов (*multiple input*), иногда также используется название *common spending*. Считается, что впервые она была апробирована в (Reid 2013), хотя сами авторы там отмечают, что еще в (Nakamoto 2008, раздел 8) упоминалась подобная схема идентификации пользователей.

Эвристика заключается в следующем: если несколько адресов используются в качестве входов транзакции, то они скорее всего принадлежат одному актору. Причина такого вывода в том, что для формирования и отправки в сеть транзакции необходимо обладать приватными ключами к каждому из входов. Хотя транзакции с несколькими независимыми подписями допустимы, они требуют некоторого дополнительного администрирования, а некоторые приложения вообще их не поддерживают, поэтому обычные пользователи задействуют этот функционал крайне редко. А значит, самое простое объяснение заключается в том, что адреса использованных входов принадлежали одному и тому же актору.

Эта эвристика подчиняется правилу транзитивного замыкания: если множества адресов входов к двум транзакциям имеют непустое пересечение, то тогда следует считать, что объединения этих множеств принадлежат одному и тому же кластеру. К примеру, если в одной транзакции участвуют входы с адресов A1 и A1, а в другой — с адресов A2 и A3, то тогда все три адреса объединяются в одну сущность.

Некоторые возможные причины эффективности этой эвристики были предложены в (Harrigan 2016). По мнению авторов, она связана с удобством повторного использования адресов и структурными характеристиками A-графа. Там же отмечена одна характерная особенность кластеризации с помощью этой эвристики: обычно уже существующий крупный кластер сливается с одним или несколькими небольшими, но слияние двух крупных адресных кластеров почти невозможно. На основе этого наблюдения предлагалось ввести дополнительное правило, запрещающее такие слияния и предотвращающее некоторые ложноположительные срабатывания.

Одной из главных проблем для эвристики множественных входов являются ложноположительные результаты для транзакций, осуществляемых миксерами. Собственно, само появление миксеров было отчасти связано с потребностью обмануть эту эвристику. До некоторой степени бороться с этим можно с помощью отмеченного выше правила, поскольку обычно у таких транзакций очень много входов, что будет приводить к спонтанному объединению множества сравнимых по размеру кластеров, которое в обычных условиях крайне маловероятно. Трудность заключается лишь в том, как выделить конкретные числовые параметры, управляющие этим правилом, к примеру, какие кластеру считать слишком большими для объединения.

Следующая по популярность эвристика связана с еще одной характерной особенностью модели UTXO: все использованные входы должны быть потрачены полностью. Из-за этого у актора, инициировавшего транзакцию, часто возникает необходимость перевести неиспользованную

«сдачу» на какой-нибудь адрес, также принадлежащий ему. Впервые этот подход был систематически рассмотрен в (Meiklejohn 2013).

Оказалось, что весьма часто акторы в сети для перевода сдачи использовали адрес одного из входов — такое поведение (соответствующие адреса были названы *self-change*) было отмечено в 23% случаев. В остальных случаях адрес для сдачи выделялся по следующим характеристикам: он не появлялся в предыдущих транзакциях, а все остальные выходы транзакции уже когда-либо участвовали в других транзакциях. Заметим, что такой анализ может быть только ретроспективным. Одноразовый адрес для сдачи должен быть единственным, который удовлетворяет всем этим условиям. Если такой адрес действительно есть, то эвристика относит его к тому же самому кластеру, что и адреса входов.

Эта эвристика также имеет модификацию, призванную уменьшить число ложноположительных результатов. Авторы специально проверили, чтобы одноразовый адрес для сдачи не использовался потом в последующих транзакциях как обычный — если это все-таки произошло, то такой адрес исключался из списка. С помощью этого дополнительного правила им удалось отбросить 13% адресов из тех, что изначально были опознаны как адреса для сдачи. Тщательный анализ ошибок выявил несколько слабых мест эвристики, в результате чего к своду правил добавили еще одно условие: если среди выходов уже есть адрес, который раньше был self-change, то никакой другой адрес в этой транзакции уже не может быть считаться адресом для сдачи. Независимое, но во многом похожее исследование было выполнено в (Androulaki 2013): там адреса для сдачи получили название *shadow addresses*.

В (Ermilov 2017) эвристика сдачи была расширена дополнительным правилом, согласно которому адрес для сдачи должен получать сумму с бóльшим количеством цифр в дробной части. Объяснение выглядело так: плата за услуги и товары обычно номинирована в «удобных и круглых» числах (см., например, (Fraser-Mackenzie 2015)), а входы, из которых компонуются транзакции, могут иметь почти случайные десятичные части, поэтому и сдача тоже должна отличаться тем же свойством. Возможно, что на первых этапах существования Bitcoin это правило было достаточно эффективно. Но сейчас, когда 1 BTC стоит десятки тысяч долларов США (весьма много по сравнению со стоимостью базовых товаров и услуг) и демонстрирует весьма большую волатильность котировок, применимость такой модификации базовой эвристики уже спорна.

Еще один интересный взгляд на эвристику сдачи был предложен в (Nick 2015): выход для сдачи должен быть меньше, чем любой из входов транзакции. Эвристика опирается на простой здравый смысл. Действительно, если бы существовал вход, который меньше чем сдача, то этот вход был использован в транзакции без всякой цели. К примеру, пусть в транзакции два входа, с 10 и 1 BTC, и два выхода, с 8 и 3 BTC, причем первый выход был потрачен на приобретение чего-либо, а второй был для сдачи. Очевидно, что можно было бы убрать вход с 1 BTC и достичь точно того же результата (разумеется, выходы при этом изменятся на 8 и 2). Если акторы хотя бы до некоторой степени рациональны, то они не стали бы так делать.

Даже одна только сумма транзакции может стать основанием для эвристики, если удастся каким-либо образом выделить конкретное значение среди всех прочих. Другими словами, если известно, что частные пользователи платят за некоторый сервис, например, 1 BTC, то это тоже дает достаточно много информации, особенно если адрес самого сервиса известен. Эта идея была использована в (Liao 2016) для исследования шифровальщика CryptoLocker. Авторы помимо стандартных эвристик множественных входов и сдачи использовали информацию о ценовой политике вымогателей: вначале те требовали 2 BTC, потом снизили плату до 1 BTC, через два дня — до 0.5 BTC, и, наконец, плата была установлена в размере 0.3 BTC. В качестве отправной точки авторы рассматривали два конкретных адреса, которые были обнародованы в посвященной шифровальщику дискуссии на Reddit. Сочетание этих методов позволило авторам достаточно подробно изучить потоки украденных средств. Тем не менее, такие эвристики создаются всегда *ad hoc* и их трудно обобщать. Более того, как отмечено в той же работе, даже сами злоумышленники быстро поняли, что по строго фиксированным суммам переводов их легко отследить и ввели некоторую рандомизацию.

Интересный пример совместного использования эвристик и информации сетевого уровня, более близкий к цифровой криминалистике, был приведен в (Neudecker 2017). В качестве базовых

эвристик авторы использовали правило множественных входов и эвристику сдачи с упоминавшимися выше дополнениями. Помимо этого был учтен запрет на спонтанное слияние крупных адресных кластеров. Другим элементом их анализа было использование особенностей рассылки сообщений в сети Bitcoin, а именно, тот факт, что узел, от которого сообщение с транзакцией пришло первым, скорее всего и был создателем этой транзакции. Это, в своюочередь, используется для уточнения первичной эвристической кластеризации. Предложенный метод технически сложнее, чем здесь написано, и использует свой свод правил отбора подходящих транзакций. Вывод из их эксперимента таков: правдоподобная связь с IP-адресами может быть установлена лишь для небольшого количества кластеров. Тем не менее, эту информацию можно использовать конструктивно, например, можно запретить слияние кластеров с адресами, к которым приписаны разные IP, или использовать IP-адреса для поиска истинного адреса сдачи, если есть несколько кандидатов. Весьма похожий подход был использован в (Juhász 2018), с той лишь разницей, что немного отличалась процедура определения IP-адресов и использовалась техника наивного байесовского анализа.

Для сети Ethereum также возможны эвристические подходы к кластеризации адресов, хотя она и не использует UTXO-модель, особенности которой лежат в основе обсуждавшихся выше техник. Подробное их исследование приведено в (Victor 2020). Все адреса в сети Ethereum подразделяются на внешние (*externally owned adress*, EOA) и адреса смарт-контрактов. Помимо этого, в отдельную группу в статье были выведены EOA, которые доподлинно принадлежат биржам — они были выявлены с помощью уже имевшейся на тот момент базы Etherscan, ручного анализа форумов и экспериментов с собственными аккаунтами автора на этих биржах.

Предложенные эвристики были основаны на типичных поведенческих паттернах. Остановимся на двух наиболее полезных на практике. Первая из них связана с использованием депозитарных адресов. Чтобы продать ETH, обычно сначала нужно послать их на специальный депозитарный счет, а уже оттуда они будут переведены на основной операционный счет биржи. Депозитарные счета создаются для каждого клиента биржи при регистрации, т. е. их нельзя создавать сколь угодно много, как обычные адреса. Отсюда следует само эвристическое правило: все адреса, с которых средства переводятся на конкретный депозитарный счет, считаются принадлежащими одному актору.

Для использования эвристики, однако, необходимо каким-то образом найти сами депозитарные счета, поскольку обычно эта информация не раскрывается. Отличительным свойством этих счетов является то, что они переводят средства только одному получателю — основному операционному счету биржи. Кроме того, сумма транзакции почти не меняется, за исключением известной комиссии. Наконец, перевод с депозитарного счета на операционный обычно выполняется очень быстро, что служит дополнительным характеристическим признаком.

Вторая эвристика использует особенность поведения участников кампаний по розыгрышу ERC20-токенов (т. н. *airdrop*). Многие проекты используют такой ход для привлечения внимания. Стало обычной практикой заводить множество адресов как якобы независимые и участвовать в льготном распределении, чтобы увеличить свои шансы на успех. По условиям все эти адреса получат одну и ту же фиксированную награду. Но поскольку хранить приобретенные таким образом токены на счетах по-отдельности не имеет особого смысла, то по завершении раздачи их обычно консолидируют на одном адресе. Именно этот паттерн и предлагается использовать для кластеризации.

Сначала нужно выявить все адреса, получившие одну и ту же фиксированную награду от адреса-дистрибьютора. Затем следует найти все счета, на которые эта награда была полностью переправлена. Счета «второго слоя» должны быть активными EOA, которые не принадлежат биржам. В кластеры попадают все адреса, которые консолидировали выплаты на одном и том же счете, и сам этот финальный адрес.

Иногда адреса-дистрибьюторы известны заранее. Во всех остальных случаях их необходимо найти с помощью некоторых дополнительных правил и предположений. Во-первых, это можно сделать по специальным меткам событий, которые хранятся в блокчейне, а также по факту отправки большого количества транзакций строго фиксированной суммы. Во-вторых, поскольку aidrop обычно

автоматизирован и токены переводятся почти одновременно, можно использовать метки времени (*timestamps*) транзакций.

Заключение

Как уже отмечалось выше, возможность использования простых эвристических методов для кластеризации в адресном пространстве была быстро осознана как злоумышленниками, так и законопослушными приверженцами полной анонимности. Одним из ответов сообщества стало создание специальных блокчейнов, где обеспечение максимальной приватности было объявлено главной целью. Среди наиболее известных к настоящему моменту можно отметить Monero и Zcash. Тем не менее, как выяснилось, и для этих блокчейнов удается создать, в свою очередь, эвристики кластеризации.

В (Kumar 2017) подробно исследована сеть Monero. Важным элементом механизма обфускации в этой сети является использование *mix-in* адресов (подробности см. в оригинальной статье), причем чем их больше, тем надежнее обеспечивается анонимность акторов. Но оказалось, что в истории транзакций доминировали небольшие количества mix-in адресов, 65.9% транзакций их вообще не использовали. Более того, выяснилось, что пользователи в известной степени сами игнорировали этот механизм: 85.9% транзакций, где mix-in адреса вообще не использовались, могли бы их использовать; если же говорить о всех транзакция в целом, то уже 99% всех входов могли бы использоваться с бóльшим количеством mix-in адресов. Авторы делают вывод о том, что аномалия объясняется желанием сэкономить на комиссиях. Но, по всей видимости, объяснение еще проще — большинству пользователей Monero приватность вообще не важна. Эвристики, предложенные в (Kumar 2017) не всегда выявляют принадлежность адресов акторам, а скорее позволяют с высокой вероятностью найти истинного отправителя среди нескольких mix-in адресов — но это именно то, чего создатели протокола хотели избежать.

Исследование кластеризации адресов для блокчейна Zcash было выполнено в (Kappos 2018). В основе Zcash лежит использование современных криптографических методов, в частности, доказательств с нулевым разглашением (*zero-knowledge proofs*, см. недавний обзор (Sun 2021)). Этот блокчейн позиционируется как по-настоящему анонимная платежная система, поскольку существует возможность удостовериться в совершении транзакции, не узнавая при этом сумму, отправителя или получателя.

Оказалось, что как и в случае с Monero, возможности Zcash по обеспечению анонимности оказались по большей части невостребованными — лишь 14.96% от общего числа транзакций использовали их. Поскольку Zcash использует модель UTXO, то здесь применимы все эвристики, обсуждавшиеся в прошлом разделе. Авторы сообщают и о более интересных хотя и несколько ситуативных подходах, используют особенности функционирования протокола Zcash.

Другой сложный для эвристик сценарий — движение средств между несколькими блокченами. Протоколы, реализующие эту возможность, сейчас уже достаточно распространены. К примеру, сеть Ripple с самого начала была создана для обращения в ней разных активов. Оказалось, однако, что можно проследить связь между адресами в блокчейне Ripple и сопряженными адресами, например, в Bitcoin. Затем, используя эвристики для Bitcoin, можно индуцировать соответствующую кластеризацию и в адресном пространстве Ripple. Подробности см. в оригинальной статье (Moreno-Sanchez 2016).

В (Yousaf 2019) был дан еще один подход к проблеме перекрестных (*cross-chain*) транзакций. Там авторы изучали эвристики для двух популярных на тот момент сервисов — Changelly и ShapeShift — которые использовались для создания своеобразных шлюзов между блокченами, даже если они изначально не поддерживали такой функциональности. Далее для удобства будем обозначать сеть, из которой средства выводятся, как X, а сеть, куда они попадают, как Y.

Здесь вновь удалось выявить несколько характерных поведенческих паттернов, которые позволяют указывать группы адресов в обоих блокчейнах X и Y, которые с большой вероятностью принадлежат одному и тому же актору. Для борьбы с ложноположительными срабатываниями авторы использовали метки времени и сумму транзакций (последние могут отклоняться друг от

друга не более чем на 1%). Обсуждение эффективности всех предложенных эвристик рассматривалось на целом ряде примеров, подробнее см. текст оригинальной работы.

По-видимому, самыми трудными для эвристик на сегодняшний день остаются миксеры. Несмотря на определенные усилия, создать простые эвристики для их выявления пока не удалось. Экспериментальное исследование этого вопроса было предпринято в (Möser 2013). Авторы направляли небольшие суммы в эти сервисы, указывая в качестве желаемого назначения контролируемые ими адреса. Используя тот факт, что и адреса, с которых средства отправляли, и на которые в итоге средства пришли, были заранее известны, удалось показать логику работы миксеров. Выявить какой-то типичный паттерн не удалось — используя в несколько этапов рандомизацию, миксерам действительно удалось сделать эвристический анализ бесполезным.

Но здесь нужно заметить, что миксеры сами по себе остаются достаточно маргинальным инструментом, а их использование зачастую несет репутационные риски. Большинство таких сервисов просуществовали непродолжительное время и были либо закрыты правоохранительными органами, либо попали под санкции, либо просто оказались нерентабельными для своих владельцев. Так что они вряд ли пока могут стать действительно серьезной и непреодолимой проблемой для KYT-анализа.

В заключение стоит подчеркнуть, что эффективность большинства описанных в настоящей статье эвристик опиралась именно на характерные поведенческие паттерны. Где-то они были продиктованы техническими особенностями протоколов, а где-то — очень простым и понятным человеческим желанием сделать что-либо побыстрее и подешевле. И поскольку человеческое поведение меняется гораздо медленнее технологий, подобные эвристические приемы, по всей видимости, еще долго не утратят своей актуальности. Как было показано, создание специальных протоколов и сервисов для обфускации действительно снижает эффективность эвристик и привносит дополнительные технические трудности, но тем не менее не делает соотнесение адресов с акторами невозможным. Разумеется, не обязательно останавливаться на применении только лишь одних эвристик — первичная грубая кластеризация, которую они дают, может стать основой для использования более сложных современных методов машинного обучения. Работ, посвященных такому комплексному анализу, достаточно много, и их обзор представляет собой отдельную задачу, требующую отдельной статьи.

Список литературы

[1] Akcora C. G., Gel Y. R., Kantarcioglu M. Blockchain networks: Data structures of Bitcoin, Monero, Zcash, Ethereum, Ripple, and IOTA // Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. – 2022. – Т. 12. – №. 1. – С. e1436.

[2] Amarasinghe N., Boyen X., McKague M. A survey of anonymity of cryptocurrencies // Proceedings of the Australasian Computer Science Week Multiconference. – 2019. – С. 1-10.

[3] Androulaki E. et al. Evaluating user privacy in Bitcoin // Financial Cryptography and Data Security: 17th International Conference, FC 2013, Okinawa, Japan, Revised Selected Papers 17. – Springer Berlin Heidelberg, 2013. – С. 34-51.

[4] Ermilov D., Panov M., Yanovich Y. Automatic Bitcoin address clustering // 16th IEEE International Conference on Machine Learning and Applications (ICMLA). – 2017. – С. 461-466.

[5] Foley S., Karlsen J. R., Putniņš T. J. Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? // The Review of Financial Studies. – 2019. – Т. 32. – №. 5. – С. 1798-1853.

[6] Fraser-Mackenzie P., Sung M., Johnson J. E. V. The prospect of a perfect ending: Loss aversion and the round-number bias // Organizational Behavior and Human Decision Processes. – 2015. – Т. 131. – С. 67-80.

[7] Harrigan M., Fretter C. The unreasonable effectiveness of address clustering // 2016 Intl IEEE conferences on ubiquitous intelligence & computing, advanced and trusted computing, scalable computing and communications, cloud and big data computing, internet of people, and smart world congress. – 2016. – С. 368-373.

[8] Juhász P. L. et al. A Bayesian approach to identify Bitcoin users // PloS one. – 2018. – Т. 13. – №. 12. – С. e0207000.

[9] Kappos G. et al. An empirical analysis of anonymity in Zcash // 27th USENIX Security Symposium (USENIX Security 18). – 2018. – С. 463-477.
[10] Kumar A. et al. A traceability analysis of Monero's blockchain // Computer Security–ESORICS 2017: 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part II 22. – Springer International Publishing, 2017. – С. 153-173.
[11] Lamport L., Shostak R., Pease M. The Byzantine generals problem // Concurrency: the works of Leslie Lamport. – 2019. – С. 203-226.
[12] Liao K. et al. Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin // 2016 APWG symposium on electronic crime research (eCrime). – 2016. – С. 1-13.
[13] Meiklejohn S. et al. A fistful of bitcoins: characterizing payments among men with no names // Proceedings of the 2013 conference on Internet measurement conference. – 2013. – С. 127-140.
[14] Moreno-Sanchez P., Zafar M. B., Kate A. Listening to whispers of ripple: Linking wallets and deanonymizing transactions in the Ripple network // Proc. Priv. Enhancing Technol. – 2016. – Т. 2016. – №. 4. – С. 436-453.
[15] Möser M., Böhme R., Breuker D. An inquiry into money laundering tools in the Bitcoin ecosystem // 2013 APWG eCrime researchers summit. – 2013. – С. 1-14.
[16] Nakamoto S. Bitcoin whitepaper. URL: https://bitcoin.org/bitcoin.pdf [свободный доступ] (February 2024).
[17] Narayanan A. et al. Bitcoin and cryptocurrency technologies: a comprehensive introduction. – Princeton University Press, 2016.
[18] Natarajan H., Krause S., Gradstein H. Distributed ledger technology and blockchain. FinTech Note No. 1. – Washington, DC: World Bank, 2017.
[19] Neudecker T., Hartenstein H. Could network information facilitate address clustering in Bitcoin? // Financial Cryptography and Data Security: FC 2017, Sliema, Malta, 2017, Revised Selected Papers 21. – Springer International Publishing, 2017. – С. 155-169.
[20] Nguyen G. T., Kim K. A survey about consensus algorithms used in blockchain //Journal of Information processing systems. – 2018. – Т. 14. – №. 1.
[21] Nick J. D. Data-driven de-anonymization in Bitcoin : дисс. – ETH-Zürich, 2015.
[22] Reid F., Harrigan M. An analysis of anonymity in the Bitcoin system. – Springer New York, 2013. – С. 197-223.
[23] Sun X. et al. A survey on zero-knowledge proof in blockchain // IEEE network. – 2021. – Т. 35. – №. 4. – С. 198-205.
[24] Tschorsch F., Scheuermann B. Bitcoin and beyond: A technical survey on decentralized digital currencies // IEEE Communications Surveys & Tutorials. – 2016. – Т. 18. – №. 3. – С. 2084-2123.
[25] Victor F. Address clustering heuristics for Ethereum // Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, Revised Selected Papers 24. – Springer International Publishing, 2020. – С. 617-633.
[26] Wu J. et al. Analysis of cryptocurrency transactions from a network perspective: an overview // Journal of Network and Computer Applications. – 2021. – Т. 190. – С. 103139.
[27] Yousaf H., Kappos G., Meiklejohn S. Tracing transactions across cryptocurrency ledgers // 28th USENIX Security Symposium (USENIX Security 19). – 2019. – С. 837-850.
[28] Zheng Z. et al. An overview on smart contracts: Challenges, advances and platforms // Future Generation Computer Systems. – 2020. – Т. 105. – С. 475-491.