ПРАКТИЧЕСКИЕ АСПЕКТЫ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С БИТКОИНОМ

Шандарович И.О., Кислицкая Н.А., студенты 4 курса юридического факультета БГУ, г. Минск, Республика Беларусь

В процессе расследования дел, связанных с биткоинами, перед следователем непосредственно стоит задача поиска следов релевантных программ. Некоторые предложили бы просмотреть носители данных с использованием ключевого слова-наименования криптовалюты, например, «биткоин» (bitcoin). Но эта проверка недостаточна, поскольку носители данных могут содержать следы использования биткоина без использования ключевого слова «биткоин» (bitcoin).

Те, кто ищет биткоин-адреса, могут часто сталкиваться со стандартной строкой-выражением, начинающейся с цифры 1 или 3, за которой следуют еще 25-34 символа.

На GitHub'е (библиотеке для разработчиков) можно найти программу BTCscan, которая представляет собой скрипт (алгоритм) для отслеживания строчек, написанных на кодировке base58. Base58 – это кодировка (алфавит), на котором написан блокчейн биткоина. Соответственно, если какая-либо программа найдёт файлы, использующие алфавит base58, то, вероятнее всего, на данном устройстве использовали программы, связанные с биткоином.

BTCscan – это программа с открытым исходным кодом, разработанная на Python, которая не требует какой-либо настройки. Последнюю версию BTCscan можно скачать с GitHub'а [1]. У программы есть интерфейс командной строки, но это не создает каких-либо препятствий.

В процессе работы программы единственным обязательным аспектом является «-i/--input» для указания диска, каталога или файла, где будет производиться поиск, поэтому команда может быть такой, как:

python BTCscan.py--input="C:\"

Соответственно, поиск будет проведён на диске С.

Как указали специалисты в области IT, BTCscan выполняет поиск по всем папкам и подкаталогам. Программа не ищет зашифрованные или сжатые элементы, поэтому перед запуском BTCscan придется распаковать файлы с сжатыми файлами. С другой стороны, она

может восстанавливать элементы из файлов, связанных с программным обеспечением биткоина и файлами кэша (файлами с сайтов, ранее посещённых с этого устройства) с сайтов, связанных с биткоинами.

Некоторые пользователи или службы владеют персонализированным биткоин-адресом. Эти адреса имеют неслучайный вид текста в начале или в конце, например, 1Ivan. Эти адреса называются персонализированными. Вероятно, самым известным примером является 1snowqQP5Vmzgu47i5Awwwz9fsgHQg94Fa, созданный Wikileaks для финансирования правовой защиты Эдварда Сноудена.

В случае, если следователь сталкивается с едва различимыми биткоин-адресами как в виде рукописных заметок, так и печатных заметок, где часть адреса отсутствует или неразборчива, то это может стать проблемой, потому что бесплатные блокчейн-поисковики обычно не ищут часть адреса биткоина. Здесь можно применить программу Chainalysis со встроенной функцией автозаполнения. [2]

Достаточно ввести только первые несколько символов, чтобы получить полный биткоин-адрес. Эта функция также может быть полезна в случае с биткоин-адресами, написанными на бумаге. В этом случае можно снова ввести первые несколько букв адреса и начнется автозаполнение. Это не только удобно, но также предотвращает ошибку, которая возможно произойдет при переписывании длинных строк.

Инструмент имеет расширенную кластеризацию (группировку) на месте и наибольшее количество идентифицированных объектов. Он четко определяет транзакции между различными кошельками и мгновенно предоставляет список всех транзакций между любыми выбранными объектами.

Данная программа - единственный продукт, который определяет воздействие количества биткоинов, которые прямо или косвенно поступают в и из исследуемого кошелька, на основе до 10 000 последних входящих и исходящих транзакций. Это быстрый способ оценить происхождение и назначение средств.

Как утверждают практики, Chainalysis также управляет алгоритмом, который собирает дополнительную информацию о биткоин-адресах в Интернете (Facebook, Reddit, Twitter и т. д.).

Elliptic - еще один коммерческий инструмент, который автоматически анализирует блокчейн. Подобно Chainalysis, его

ключевым преимуществом является способность идентифицировать ближайшую связь между адресом подозреваемого и организацией, которая может предоставить дополнительную информацию о подозреваемом [3].

Еще в 2011 году известный исследователь Дэн Каминский предположил, что можно обнаружить IP-адреса плательщика путем анализа интернет-трафика. Для проведения деанонимизации необходимо было открыть соединение со всеми биткоин-узлами, активными в сети, и для каждой транзакции найти IP-адрес клиента, который первым транслировал транзакцию в сеть.

Основываясь на том, как работает биткоин, первым, кто отправляет транзакцию в биткоин-сеть, будет плательщик. Поэтому обнаружение первого узла, который транслирует транзакцию, должно выявить IP-адрес владельца входных биткоин-адресов. Эта логика должна приводить к идентификации плательщика, если он или она не использует средства маскировки IP-адреса, например, прокси-сервер, VPN или Tor или использует виртуальный биткоин-кошелек.

Деанонимизация пользователей биткоинов посредством анализа сетевого трафика является предметом текущих исследований, проводимых как академическими кругами, так и частным сектором.

Что касается идентификация биткоин-адресов и подозреваемых, то можно отметить следующее. Как правило, при расследовании преступлений, связанных с биткоином, есть 2 основные цели: идентифицировать подозреваемого и конфисковать биткоины, приобретённые преступным путём.

Криптовалюта, если она используется в серых операциях, оставляет много следов в сети. Однако, идентификация не является чем-то, что может быть отсортировано самим блокчейном. Анонимный характер блокчейна поддерживает только биткоин-адреса без каких-либо ссылок на реальные личности. Поэтому для отслеживания транзакции в блокчейне необходимо объединить информацию, полученную из блокчейна, с данными, полученными из других источников.

Walletexplorer является оптимальным бесплатным инструментом, который связывает биткоин-адреса с известными субъектами включая обменники, майнинговый пул, игровые сайты, кошельки или даркнет. Он был разработан в 2014 году чешским программистом Алесом Яндой. [4]

Разработчик веб-сайта в настоящее время работает в Chainalysis и больше не обновляет Walletexplorer. Тем не менее, веб-сайт продолжает анализировать (обрабатывать) блокчейн, поэтому последние данные по-прежнему доступны, возможно, с небольшой задержкой, что позволяет обрабатывать самые последние входящие данные.

Он работает как поисковая система для биткоин-адресов; когда биткоин-адрес может быть связан с известным объектом, указывается имя объекта. Программа работает с кошельками, а не с адресами, и по этим причинам результаты более информативны и их легче интерпретировать.

Использовать Walletexplorer можно в качестве бесплатного блокчейн-обозревателя, но при просмотре транзакций следует учитывать ложные срабатывания. По этой причине лучше использовать Walletexplorer вместе с blockchain.info, который является источником более надежной информации, в то время как Walletexplorer дополняет информацию к тому, что обнаружено через blockchain.info.

14 ноября был активирован Taproot, новый метод транзакций в биткоине: pay to taproot. Прямо сейчас это не скажется на опыте почти никак, но в течении ближайших месяцев, когда кошельки, ноды и биржи добавят поддержку такого типа транзакций — это существенно увеличит конфиденциальность транзакций в сети, что может затруднить идентификацию подозреваемых.

Закон от 06.01.2021 № 85-З «Об изменении кодексов по вопросам уголовной ответственности» внёс изменения в Уголовно-процессуальный кодекс Республики Беларусь. Законодатель ввёл новый вид имущества, на которое можно наложить арест – криптовалюту. Ч. 15 ст. 132 УПК предполагает, что изъятие и хранение арестованных денежных средств осуществляется в электронных кошельках органа, ведущего уголовный процесс. [5, 6]

В отличии от тех преступлений, где злоумышленники хранят деньги в банках (на счетах или в ячейках) или наличными в тайниках, биткоины имеют свою специфику. Кто-то может предположить, что биткоины хранятся на компьютере подозреваемого, но в ддействительности биткоины хранятся в блокчейне, который находится на тысячах компьютеров по всему миру.

При этом, на компьютере подозреваемого располагается кошелёк, содержащий закрытый ключ, который позволит правоохранителям изъять биткоины с компьютера если на то будут основания.

Помимо компьютера, как описано выше, закрытый ключ может храниться на другом носителе, например, флешке, телефоне, записан на листке бумаги и т.д. Также он может храниться у третьей стороны, распоряжающаяся биткоинами, или на виртуальной бирже, которая позволяет совершать транзакции при помощи биткоина, не скачивая клиент, или у онлайн-провайдера кошелька.

Как уже указывалось выше, существует различное количество кошельков, которые позволяют проверять баланс на своих биткоин-адресах без скачивания всего блокчейна, так называемые «лёгкие кошельки». Самые популярные – BitcoinCore и Electrum. Данные кошельки скачивают лишь ту часть блокчейна, которая релевантна для пользователя.

Программное обеспечение биткоин-кошельков хранит файл bitcoin-wallet.1 на локальном диске. В этом файле закрытый ключ может быть как в незашифрованном виде, так и зашифрованном. В первом случае доступ к компьютеру подозреваемого – это все, что необходимо для обнаружения биткоина и его перемещения на биткоин-кошелек, подконтрольный правоохранительными органами. Однако, подавляющее большинство пользователей независимо от того, используют ли они биткоин в законных или незаконных целях, шифруют свои биткоин-кошельки.

«Лёгкие» кошельки не загружают блокчейн и, следовательно, не имеют возможности проверять транзакции для сети. Это экономит десятки гигабайт на жестких дисках и вычислительные мощности компьютера. Так, например, BitcoinCore на моём компьютере скачал лишь 2 Гб блокчейна из 450. По этой причине «легкие» кошельки особенно популярны на мобильных устройствах и смартфонах, которые ограничены дисковым пространством, вычислительными мощностями и батареей. Поскольку блокчейн постепенно увеличивается, всё большее число пользователей переходит от полных к «легким» клиентам (онлайн-кошелькам), или мобильным кошелькам, таким как Coinbase, Blockchain.info или Trust.

Легче всего понять различие между полной нодой и «лёгким» кошельком проведя аналогию с человеком в незнакомом месте. В первом случае у него есть телефон, на котором при помощи GPS можно отследить своё местоположение и проложить маршрут на

карте до нужного мета, а во втором случае – телефона нет и его действия зависят от того, у кого он есть.

Если следователь идентифицирует биткоин-адреса подозреваемого в блокчейне, то необходимо учитывать, что невозможно изъять биткоины удаленно (если только подозреваемый держит свои средства на онлайн-бирже). Чтобы изъять биткоины с компьютера подозреваемого, следователь должен найти:

1. биткоин-кошелек на жестком диске подозреваемого – в этом случае необходим пароль, чтобы осуществлять какие-либо действия с биткоинами, поскольку подавляющее большинство биткоин-кошельков в настоящее время зашифровано;

2. закрытый ключ подозреваемого – в этом случае необходимо импортировать его в биткоин-кошелек;

3. seed-пароль зашифрованного кошелька (Как указано в кошельке, это десять ли более случайных символов или восемь и более слов). Seed – специальная кодовая фраза, которая используется для доступа к кошельку.

Изъять биткоины – это не значит просто взять и скопировать файл bitcoin-wallet, импортировать закрытый ключ или ввести seedдля работы с программным обеспечением, используемым правоохранительными органами. Действуя так, следователь просто обнаружит соответствующие открытые ключи вместе с суммой неизрасходованных биткоинов. В этом случае, биткоины нельзя считать изъятыми, так как сам подозреваемый или другое лицо, у которого есть закрытый ключ, может переместить денежные средства на другой адрес. Чтобы действительно изъять биткоины требуется дополнительный шаг для завершения перевода средств. Таким образом, следователь должен переместить их на биткоин-адрес, созданный специально для этих целей правоохранительными органами.

Список литературы:

1. BTCScan // github.com [Электронный ресурс]. - Режим доступа: http://gist.github.com/chriswcohen/7e28c95ba7354a986c34.- Дата доступа: 29.04.2021.

2. Chainalysis // chainalysis.com [Электронный ресурс]. - Режим доступа: https://www.chainalysis.com/. - Дата доступа: 15.11.2021.

3. Elliptic // elliptic.com [Электронный ресурс]. - Режим доступа: https://www.elliptic.com/.- Дата доступа: 30.04.2021.
4. Walletexplorer // walletexplorer.com [Электронный ресурс]. - Режим доступа: walletexplorer.com. - Дата доступа: 30.04.2021.
5. Закон Республики Беларусь от 06.01.2021 N 85-З "Об изменении кодексов по вопросам уголовной ответственности" // Доступ из СПС «КонсультантПлюс».
6. Уголовно-процессуальный кодекс Республики Беларусь [Электронный ресурс] : Кодекс Республики Беларусь, 24 июня 1999 г. No 295-З : в ред.от 14.04.2021г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац.центр правовой информ. Республики Беларусь. – Минск, 2021.

CONSTITUTIONAL AND LEGAL FOUNDATIONS OF THE FORMATION OF THE INSTITUTION OF LOCAL SELF-GOVERNMENT IN THE REPUBLIC OF KAZAKHSTAN.

ShlyakhovayaYa.D., student of the Department of International and Constitutional Law of the E.A.Buketov Karaganda University, Karaganda, Republic of Kazakhstan
Scientific supervisor: Eremenko N.S., Senior Lecturer of the Department of International and Constitutional Law of the E.A.Buketov Karaganda University, Karaganda, Republic of Kazakhstan

The history of the formation and development of local representative bodies of the Republic of Kazakhstan began only with the proclamation of Kazakhstan's independence on December 16, 1991, however, without studying the historical roots of their origin, it is impossible to understand the essence and driving leitmotifs that led to the reform of local authorities and the creation of maslikhats in their modern version.[1]

Initially, in Kazakhstan, the ideas of self-government, not representation, receive the greatest embodiment. The roots of self-government among the Kazakhs were formed with the emergence of tribal and tribal communities, as the nomadic lifestyle emerged. Elders and tribal leaders were elected at kurultai. They were authorized to resolve disputes, train and command units of soldiers, and tribal communities enjoyed great