ОСОБЕННОСТИ СЛЕДОВОЙ КАРТИНЫ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ХИЩЕНИЕМ БИТКОИНОВ

И. О. Шандарович, Н. А. Кислицкая

Белорусский государственный университет, г .Минск;
Igor.shandarovich@yandex.by, n.kislickaya@gmail.com;
науч. рук. – А. М. Хлус, канд. юрид. наук, доц.

В статье наглядно демонстрируются программы, приёмы и особенности следовой картины при расследовании преступлений, связанных с биткоином. Объясняется технология блокчейна для понимания особенностей расследования вышеупомянутых преступлений. Установлено, что при расследовании дел, связанных с биткоинами, следы транзакций можно найти в виде использования подозреваемым биткоин-кошельков или биткоин-бирж. Определено, что блокчейн не является сверхприватной системой, развитие технологий облегчает процесс установления личности преступников, пользующихся преимуществами блокчейна, а невозможность удалить запись об осуществлённых транзакциях может сыграть против них.

Ключевые слова: биткоин, преступление, хищение биткоинов, криптовалюта.

Полагаем, что для начала необходимо рассказать о том, как устроен биткоин, блокчейн и биткоин-кошелёк. Биткоин основан на сочетании нескольких технологий, одной из которых является криптография с открытым ключом, которая требует два разных ключа для отправки и получения транзакций. Открытый ключ может быть распространен среди всех, чтобы получить платеж, в то время как закрытый ключ, который должен быть известен только его владельцу, потому как используется для создания подписи для транзакции, которая не может быть подделана.

Криптография с открытым ключом решает две основные проблемы, с которыми сталкиваются все цифровые валюты:

· позволяет пользователям однозначно идентифицировать свои адреса в системе;

· запрещает пользователям тратить биткоины, которыми они не владеют.

Один пользователь может использовать любое количество биткоин-кошельков, содержащих любое количество биткоин-адресов, которые могут генерировать любое количествозакрытых ключей. Закрытый ключ, в свою очередь, генерирует открытые ключи. При этом, один закрытый ключ генерирует один открытый ключ, который хэшируется лишь в один биткоин-адрес.

Под хэшированием следует понимать функцию преобразования. Иными словами, данный процесс позволяет получить из закрытого клю-

ча, хранящегося в блокчейн-кошельке, открытый ключ. В официальном документе биткоина рекомендуется создавать новый биткоин-адрес для каждой новой транзакции [1].

Зачем нужны 2 вида ключей? Закрытый ключ предоставляет пользователю кошелька полноценный доступ и распоряжение средствами на счёте, а открытый ключ необходим для того, чтобы узнать биткоин-адрес, на который необходимо перевести средства, т.к. при хэшировании открытый ключ превращается в биткоин-адрес. При этом, из открытого ключа нельзя получить закрытый ключ.

Биткоин-адрес можно сравнить с адресом электронной почты: он тоже может быть открыто показан кому-либо для того, чтобы на этот конкретный адрес пришло письмо. Но, в отличие от адреса почты, знание биткоин-адреса позволяет посмотреть баланс и весь перечень транзакций, отправленные на или с этого адреса.

Во время транзакции кошелёк обращается с запросом в блокчейн, где проверяет список адресов в кошельке, объединяя сами кошельки до тех пор, пока не наберётся нужная сумма и, наконец, подписывает транзакцию закрытым ключом и передаёт её в блокчейн. Такая операция обусловлена тем, что средства хранятся не на компьютере пользователя, а в самом блокчейне.

Биткоин-адреса состоят из 30-35 символов и начинаются с цифр 1 или 3. Те адреса, что начинаются с цифры 3 являют собой pay-to-scriptP2SH хэш-адресами. Они управляются скриптами, а не владельцами, т.е. сценарий по которому будет проходить транзакция, направленная на этот адрес, прописан заранее и его остаётся лишь запустить. Хэш-функция необходима для обеспечения проверки неизменности данных, преобразования данных (ввода) любой длины в битовую строку определённой длины и менять данные таким образом, чтобы ввод не мог быть получен из вывода.

При расследовании дел, связанных с биткоинами,следы транзакций можно найти в виде использования подозреваемым биткоин-кошельков или биткоин-бирж: BlockchainWallet,CoinBase, Trezor, Currency.com, Bitstamp, Crypto.com, BitBay, Kuna и т.д. [2]

Во время проверки носителей данных недостаточно просмотреть лишь те файлы, которые появились при фильтре по слову «bitcoin»,в связи с тем, чтоданные могут содержать следы транзакций и без этого слова. Можно использовать скрипт «BTCscan.py», который позволяет искать в информации с носителя строки base58[3]. Наличие таких строк в информации с носителей данных доказывает то, что пользователь применял программы, написанные на алфавите из 58 символов. А самой распространённой программой, написанной на таком алфавите, является

блокчейн. При этом, наличие таких строк не является прямым доказательством использования блокчейна, т.к. на этой кодировке могут быть написаны и другие программы.

Также можно использовать программу «Chainalysis», которая позволяет восстановить полный биткоин-адрес, используемый злоумышленниками, имея лишь его часть, которая, например, написана на бумаге или понятна из неразборчивой фотографии всего биткоин-адреса. Далее требуется лишь сопоставить восстановленный биткоин-адрес с адресами, используемыми для транзакций кошелька. Таким образом, эта программа помогает доказать, что владелец просматриваемого носителя информации взаимодействовал с интересующим нас восстановленным биткоин-адресом [4].

При просмотре данных с носителей подозреваемого можно узнать биткоин-адреса, включённые в биткоин-кошелёк, список транзакций, а также баланс кошелька.Дэн Каминский, инженер в области компьютерной безопасности, консультирующий корпорации из списка Fortune 500, предположил, что обнаружить IP-адрес, с которого сделана транзакция, можно путём анализа интернет-трафика: необходимо синхронизироваться с подключёнными узлами (как правило, один кошелёк одновременно подключается к 8 узлам) и для каждой транзакции найти IP-адрес, с которого первым транзакция транслировалась в сеть.Узел представляет собой подключённый к сети компьютер, на котором помимо биткоин-кошелька хранится ещё и весь блокчейн. Также узлы проверяют транзакции и распространяют данные о проверенных транзакциях дальше в сеть. При запуске узел устанавливает соединение с другими узлами, становясь частью сети. Учитывая специфику работы блокчейн-кошелька, которая описана нами выше, во время транзакции, первым, кто отправляет транзакцию в сеть будет плательщик.

Более того, любая транзакция, попавшая в блокчейн остаётся в нём навсегда и не может быть удалена оттуда в принципе: технология попросту не позволит сделать это. Этим фактом могут пользоваться сотрудники правоохранительных органов, уличившие лицо в незаконных действиях, связанных с биткоином.

Для идентификации биткоин-адресов и подозреваемых также можно использовать Walletexplorer.com [5]. Это оптимальный бесплатный инструмент, который связывает биткоин-адреса с известными субъектами включая обменники, майнинговый пул, игровые сайты, кошельки или даркнет.

Проводник Walletexplorer прост в использовании и результаты легко интерпретировать. 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 [6].

В результате расследования следователю может понадобиться изъять биткоины, нажитые преступным путём, с кошелька подозреваемого. 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.

Безопасный кошелек, как правило, должен иметь загруженный блокчейн и быть проверен сообществом, поэтому биткоин-кошелек Bitcoin-Core – крайне предпочтительный вариант. Очевидно, официальный биткоин-адрес правоохранительного органа должен быть заранее известен сотрудникам, проводящим обыск или изъятие, чтобы они могли перемещать биткоины без каких-либо задержек.

Таким образом, блокчейн не является сверхприватной системой, как о том писалось с момента его запуска. Улучшение технологий облегчает процесс деанонизации (установления личности) злоумышленников, пользующихся преимуществами блокчейна, а невозможность удалить запись об осуществлённых транзакциях может сыграть против злоумышленников, если они захотят замести следы.

Библиографические ссылки:

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System [Электронный ресурс] / Режимдоступа: https://bitcoin.org/bitcoin.pdf. – Дата доступа: 01.04.2021
2. Обменники Биткоин. Места для покупки Биткоин в обмен на другие валюты. [Электронный ресурс] / Режим доступа: https://bitcoin.org/ru/exchanges. – Дата доступа: 01.04.2021

3. BTCscan.py // github.com [Электронный ресурс] / Режим доступа: https://gist.github.com/chriswcohen/7e28c95ba7354a986c34. – Дата доступа: 01.04.2021
4. Chainanalysis // chainalysis.com [Электронный ресурс]. - Режим доступа: https://go.chainalysis.com/2021-Crypto-Crime-Report.html. - Дата доступа: 29.04.2021.
5. Bitcoin block explorer with address grouping and wallet labeling// walletexplorer.com [Электронный ресурс]. – Режим доступа: https://www.walletexplorer.com/. – Дата доступа: 29.04.2021.
6. Bitcoin //blockchain.com [Электронный ресурс]. - Режим доступа: https://www.blockchain.com/explorer. - Дата доступа: 29.04.2021.