Секция «Криминалистика»

Способы выявления легализации (отмывания) денежных средств с использованием криптовалюты

Храпач Дмитрий Сергеевич
Студент (бакалавр)
Московский государственный университет имени М.В.Ломоносова, Юридический факультет, Кафедра криминалистики, Москва, Россия
E-mail: hrapachd@gmail.com

За последние годы криптовалюта стала все чаще стала упомянаться как один из инструментов придания правомерного владения денежным средствам, полученным преступным путем. Об этом свидетельствует статистка, так, объем сделок с использованием криптовалют в Российской Федерации, по некоторым оценкам, достигает 5 млрд долл. США в год, однако, при таких активных темпах роста, законодатель только с 1 января 2022 г. признал криптовалюту имуществом [1] [4].

Криптовалюта - цифровой актив и в то же время платежная система, которая использует криптографическую функцию для шифрования записей. Практически все нынешние криптовалюты основаны на технологии блокчейн (blockchain technology), суть которой заключается в использовании распределительной сети. В такой системе отсутствуют посредники и централизованные агенты, а также иерархия, все контрагенты становятся равными, что и обеспечивает анонимность [5].

Анонимность, простота в трансграничных переводах, а также отсутствие единого механизма урегулирования этого института с каждым годом привлекает все большее количество преступников [2]. Поэтому правоохранительные органы столкнулись не только с проблемой выявления данных преступлений, но и в некоторых случаях не могут доказать незаконное происхождение денежных средств, так, Верховный суд Республики Мордовия отменил приговор районного суда ввиду отсутствия в деянии лица состава преступления, предусмотренного ч. 1 ст. 174.1 УК РФ, так как сторона обвинения не смогла опровергнуть доводы осужденного о расходовании денежных средств, полученных с крипто-кошелька, для собственных нужд [3].

Непосредственно крипто-адреса, которые выглядят как случайный набор латинских букв и цифр не могут содержать информацию о сторонах сделки. Однако, злоумышленников, которые будут использовать систему блокчейн в незаконных целях, в том числе для отмывания доходов, полученных преступным путем, можно вычислить по совокупности косвенных признаков.

В первую очередь, что должны искать сотрудники правоохранительных органов - это адрес электронного кошелька, который может выглядеть как совокупность цифр и латинских букв или qr-код. Преступник может оставить, его в переписке с контрагентом или подельником, а также он может храниться в файлах принадлежащего ему электронного устройства.

Более опытные преступники будут использовать анонимную сеть «TOR» для выхода в интернет,и проводить зачисление криптовалюты с майнингового пула. Майниговый пул - это совместный майнинг криптовалюты, когда майнеры объединяют свои усилия, при этом определить субъектный состав пула практически невозможно, так как некоторые площадки позволяют заниматься добычей криптовалюты даже без регистрации. Пул используется чаще всего для bitcoin, однако такая система подходит для всех криптовалют на протоколе Proof-of-Work (PoW).

Также злоумышленники могут воспользоваться технологией «CoinJoin», с помощью которой несколько переводов от разных пользователей объединяются в одну транзакцию

с большим количеством выходов, что затрудняет идентификацию конкретного пользователя, но не исключает ее, так как сотрудники правоохранительных органов смогут применить инстумент «coinjoinsudoku», просмотреть все входы и выходы, тем самым, идентифицируя транзакцию.

Похожие инструменты для деанонимизации транзакций использует Федеральная налоговая служба США (IRS), а именно, продукцией компании «Chainalysis». Программа «Chainalysis Reactor» позволяет автоматически определить адрес кошелька при наличии хотя бы небольшой зацепки с криптоданными. Сотрудники правоохранительных органов с помощью API в режиме реального времени мониторят огромные объемы информации и выявляют подозрительные транзакции, которые выявляются алгоритмами программы автономно.

Chainalysis Reactor анализирует практически всю финансовую активность, в том числе, поток украденных средств, транзакции NFT и экспресс-кредиты, сканируя интернет-трафик через социальные сети, медиа-форумы и даже сайты даркнета [6].

Таким образом, на данный момент уже существуют механизмы, позволяющие не только выявить подозрительные финансовые операции, используемые для легализации (отмывания) денежных средств, но и установить причастность конкретного лица к совершению данного деяния, однако правоохранительные органы пока еще не выявили единой, наиболее оптимальной и универсальной методики.

Источники и литература

1) Федеральный закон от 31 июля 2020 г. N 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // СПС "КонсультантПлюс".
2) Информационное сообщение Росфинмониторинга "Об использовании криптовалют". [Электронный ресурс] URL: http://www.fedsfm.ru/news/957 Дата обращения 13.02.2023.
3) Определение Верховного суда Республики Мордовия от 21 января 2021 г. N 22-117 "Обзор судебной практики Верховного суда Республики Мордовия по уголовным делам за 1-е полугодие 2021 года" (утв. 22.07.2021). [Электронный ресурс] URL: http://vs.mor.sudrf.ru/modules.php?name=docum_sud&id=741. Дата обращения 12.02.2023.
4) Банк России: криптовалюты: тренды, риски, меры. Доклад для общественных консультаций [Электронный ресурс] URL: http://www.cbr.ru/content/document/file/132241/consultation_paper_20012022.pdf Дата обращения 13.02.2023.
5) Криптовалюты: новая экономика или новая пирамида?: Лекция Фонда Егора Гайдара. [Электронный ресурс] URL: https://www.kommersant.ru/doc/3474129 Дата обращения 13.02.2023.
6) Chainalysis – инструмент крипто-мониторинга и анализа блокчейна. [Электронный ресурс] URL: https://cryptonews.net/ru/news/analytics/3767065/ Дата обращения 12.02.2023.