

Д. И. Шнейдерова

*преподаватель кафедры уголовного процесса и криминалистики
Могилевского института МВД (Беларусь)*

КРИПТОВАЛЮТА В МЕХАНИЗМЕ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ

Стремительное развитие информационных технологий способствовало появлению новых способов осуществления расчетов как между физическими, так и юридическими лицами. На смену расчету наличными денежными средствами постепенно пришел безналичный, контролируемый и осуществляемый обслуживающими банками, затем стали популярны расчеты, совершаемые посредством интернет-банкингов и электронных денег. Усовершенствование системы обмена денежных средств на товары и услуги, обмена валют, денежных переводов привело к появлению достаточно востребованных на сегодняшний день цифровых валют, именуемых в быту криптовалютой. Привлекательность криптовалют заключалась в ее основополагающих принципах работы: анонимности, децентрализации регулирования и независимой от человеческого фактора безопасности. Однако простота использования и отсутствие контроля со стороны государства обеспечили повышенный интерес к криптовалютам не только со стороны обычных граждан, но и субъектов преступного мира. Представляется целесообразным рассмотреть вопрос использования криптовалюты в механизме совершения противоправных деяний, а также определить меры предупреждения и пресечения указанных преступлений.

Республика Беларусь — одна из немногих стран, которая предприняла попытку легализовать цифровую валюту и даже создать свою собственную монету, именуемую «талер». Декрет № 8 от 21 декабря 2017 г. «О развитии цифровой экономики» (далее — Декрет) закрепил право физических и юридических лиц покупать, продавать и обменивать токены через официальных операторов криптоплатформ, зарегистрированных в Парке высокой технологий, и даже получать доход от таких сделок, не облагаемый до 2023 года налогом. Кроме того, законодатель устанавливает определения терминов «криптовалюта» и «токен», что дает основанием считать эти инструменты в качестве универсального средства обмена, являющегося одновременно и собственностью их владельца.

Следует отметить, что вопрос правовой природы криптовалюты решается в различных странах неоднозначно. Например, Япония признает

цифровую валюту в качестве средства платежа, Китай наделяет ее качествами товара, США представляет криптовалюту и как аналог денежных средств, и как товар, облагаемый налогом, Россия включила данный инструмент в категорию «денежный суррогат». Однако однозначного значения на мировом рынке криптовалюта не имеет, что лишает ее признака универсальности.

Так как цифровая валюта признается в Республике Беларусь собственностью, соответственно, она охраняется нормами уголовно-правового закона. Однако в данном случае необходимо указать, что только законно приобретенная цифровая валюта попадает под охрану правовых норм, установленных государством. Исходя из положений Декрета, законно приобретенной считается только та криптовалюта, которая была получена при совершении сделок купли, продажи или обмена указанного инструмента через официально зарегистрированные в Парке высоких технологий криптовалютные биржи и обменники. Следовательно, если лицо приобретает криптовалюты через какую-либо иную криптобиржу, которых зарегистрировано в сети Интернет бесчисленное множество, то его права на такую валюту не будут защищены государством. Кроме того, подобные сделки никак не контролируются со стороны правоохранительных органов и в большинстве случаев носят анонимный характер, что и привлекает преступников.

Сегодня участились случаи использования криптовалюты в процессе легализации доходов, полученных преступным путем, финансирования терроризма, получения вознаграждения при сбыте наркотических средств, психотропных веществ и оружия, проявления коррупции, незаконного оборота различных товаров и услуг.

Рассмотрим механизм совершения такого преступления на примере торговли наркотиками. Актуальным и самым популярным на сегодня способом сбыта наркотических средств является размещение объявлений в социальных сетях или иных интернет-ресурсах, носящих однодневный характер. Кроме основной информации о товаре, такие объявления содержат сведения и о способе оплаты, в рамках которого потенциальному покупателю предлагается произвести оплату не денежными средствами, которые ранее передавались из рук в руки, закладывались в определенных местах или перечислялись на счет, а путем покупки и перевода на адрес виртуального кошелька цифровой валюты определенного вида, а их в мире насчитывается более 1500.

Исходя из вышеизложенного, появляется вопрос, почему же преступник не боится быть обнаруженным и изобличенным в своем деянии при наличии доступной информации о нем. Суть безопасности личных данных заключается в принципах совершения сделок с криптовалютой. Для того чтобы любое лицо могло приобретать, хранить, продавать или обменивать криптовалюту ему необходимо завести электронный кошелек, скачав в Интернете специальную программу или же зарегистрировавшись в онлайн-сервисе. Далее начинает действовать принцип анонимности, заложенный при создании криптовалют. При регистрации программа может запрашивать у пользователя его личные данные, однако актуальность и действительность этих данных никем и ничем не проверяется, а принимается как должное. Некоторые сервисы и вовсе не требуют ввода анкетных данных при регистрации, а пользователи идентифицируются по присваиваемому личному номеру — адресу кошелька. Таким образом, установить подлинную личность владельца электронного хранилища не представляется возможным, за исключением, конечно, сложных и длительных операций по определению IP-адреса компьютера, с которого осуществлялась регистрация. Однако даже при данном способе существует риск использования злоумышленником программы, маскирующей подлинный IP, или же осуществление действий через свободно доступный Интернет в общественных местах, или при незащищенности роутера.

Далее следует раскрыть принцип децентрализованного регулирования. Сам процесс осуществления транзакций базируется на применении распределительной технологии блокчейн. Все пользователи, зарегистрированные в одной системе, обладают одинаковым пакетом записей об осуществленных внутри системы сделках. При этом каждая транзакция перед ее завершением должна быть одобрена пользователями. Определенное количество транзакций формируют закрытый блок, защищаемый криптокодом. Все блоки объединены в одну последовательную цепочку, убрать звено из которой невозможно, а следовательно, и изменить или аннулировать сохраненную в нем транзакцию. Таким образом, проявляется принцип безопасности совершения сделок и хранения данных о них. Децентрализация же заключается в отсутствии координирующего и контролирующего процесс субъекта. Все члены системы равны между собой, обладают одинаковым набором блоков на своих компьютерах и сообща контролируют совершаемые друг с другом сделки.

Таким образом, такой способ получения денежного вознаграждения для любого преступника является наиболее приемлемым, так как просле-

дуть движение денежных средств от отправителя получателю, а равно как и установить их личности, опираясь только на данные распределительной системы, не представляется возможным. Кроме того, так как в таких сервисах отсутствует управляющее звено, то и пытаться получить информацию о владельце электронного кошелька и его сделках не у кого.

И даже если правоохранительным органам все же удастся определить злоумышленника, то установить его реальный доход, а в первую очередь его существование, они смогут только при наличии логина и ключа доступа к электронному кошельку, а также информации о конкретной распределительной системе (или программе на компьютере). При таких обстоятельствах может складываться несколько различных ситуаций. Маловероятно, что преступник сам добровольно выдаст необходимую информацию, поэтому необходимо надеяться на его небрежность. Ключ-доступ в большинстве случаев представляет собой буквенно-цифровую запись, состоящую из 64 и более символов. Запомнить такие комбинации очень тяжело, поэтому они, как правило, фиксируются на различных материальных носителях, файлах, записях в социальных сетях, заметках и так далее. Также информация о ключе может быть известна соучастникам или просто свидетелям, сожителям. В противном же случае, получить доступ к электронному кошельку будет практически невозможно. Конечно, не следует исключать возможность подбора необходимой комбинации, но на это может уйти достаточно много времени.

Таким образом, если при передаче денег из рук в руки, или переводе с одного счета на другой определенное количество раз, или при придании деньгам иной природы их возникновения все же можно установить источники их отправления и получения, то при использовании сервисов, работающих по технологии блокчейн, обнаружить «денежный след» затруднительно ввиду налаженного механизма действия принципов децентрализации и анонимности, к которым можно также добавить и закрытость от несанкционированного доступа.

При этом современные возможности предоставляют сегодня владельцам криптовалют услуги по обеспечению дополнительной анонимности и увеличению степени скрытости участников транзакций. Это стало возможно благодаря программам-миксерам, позволяющих смешивать транзакции без участия владельцев цифровых валют. Механизм работы заключается в автоматическом смешивании криптовалют различных пользователей, которые потом делятся между ними и поступают на уже новые, созданные

программой, электронные кошельки, гарантируя, таким образом, полную анонимность участников [1].

Кроме того, не следует оставлять без внимания и определение размера полученного преступным путем дохода. Так как любая криптовалюта может быть продана за реальные денежные средства через криптобиржи, то, соответственно, единица цифровой валюты должна обладать определенным денежным эквивалентом. Однако в данном вопросе также присутствуют проблемные аспекты, заключающиеся в нестабильности своего рода курса (уставной цены). На практике стоимость цифровых монет определяется в зависимости от спроса на них, то есть чем больше спрос на покупку криптовалют, тем выше их номинальная цена. При этом характерной чертой является нестабильность курса и его различие в зависимости от вида криптовалюты. Резкие и частые скачки уставной цены не позволят адекватно оценить полученную преступником выгоду.

Резюмируя вышеизложенное, представляется необходимой разработка мер, направленных на предупреждение и пресечение преступлений, средством совершения которых являются криптовалюты. Так, целесообразно на законодательном уровне установить контроль над деятельностью обменных сервисов и криптобирж, не зарегистрированных в Парке высоких технологий. В рамках контроля необходимо осуществлять мониторинг совершения сделок с криптовалютой на предмет выявления преступной активности отдельных пользователей, который может быть возможен при обеспечении доступа контролирующего органа к таким системам. При этом необходимо возложить на обменные сервисы и биржи обязанность по введению обязательной регистрации пользователей с подтверждением личности посредством смс-оповещений, что позволит в последующем идентифицировать участников сделки. Однако следует отметить, что данные меры не могут быть применены в отношении сервисов и программ, обеспечивающих хранение электронных кошельков, так как последние строятся на принципе децентрализации и обязать всех их участников предоставлять анкетные данные невозможно.

Таким образом, активное распространение цифровых валют в качестве средства обмена или платежа приводит к неизбежному появлению таких отрицательных тенденций со стороны криминогенных лиц и структур, как использование рассматриваемого инструмента в качестве средства совершения преступлений. Востребованность криптовалют определяется ее основополагающими принципами, которые позволяют злоумышленникам оставаться не обнаруженными. Ввиду повышенного риска проявления пре-

ступной активности представляется необходимым принятие государством на законодательном уровне мер по контролю над оборотом криптовалюты и сделок с ней.

Библиографический список

1. Батоев, В. Б. Использование криптовалюты в преступной деятельности: проблемы противодействия [Электронный ресурс] / В. Б. Батоев // Труды Академии управления МВД России. — 2017. — № 2. — Режим доступа: <https://cyberleninka.ru/article/v/ispolzovanie-kriptoalyuty-v-prestupnoy-deyatelnosti-problemy-protivodeystviya>. — Дата доступа: 21.03.2019. [Вернуться к статье](#)