УДК 343.9

КРИПТОКРЕДИТЫ: КРИМИНАЛИСТИЧЕСКИЙ АНАЛИЗ СПОСОБОВ СОВЕРШЕНИЯ ХИЩЕНИЙ

Д. И. Шнейдерова
Могилевский институт МВД Республики Беларусь,
преподаватель кафедры правовых дисциплин
e-mail: galuzodi@mail.ru

Аннотация. *В статье автором определяется сущность и виды криптокредитов, приводится анализ способов реализации мошеннических действий, направленных на хищение криптовалют как посредством обмана пользователей, так и децентрализованных криптоплатформ, использующих ценовые оракулы.*

Ключевые слова: *криптовалюта, криптокредит, флеш-кредит, ценовой оракул, мошенничество, хищение, децентрализованная биржа.*

Annotation. *In the article, the author defines the essence and types of cryptocredits, provides an analysis of ways to implement fraudulent actions aimed at stealing cryptocurrencies both by deceiving users and decentralized crypto platforms using price oracles.*

Keywords: *cryptocurrency, cryptocredit, flash credit, price oracle, fraud, theft, decentralized exchange.*

Криптокредитование как относительно новый и малоисследованный с точки зрения криминалистического анализа институт криптосферы в последнее время активно используется кибермошенниками с целью хищения различных видов криптовалют. Сущность криптокредитования заключается в предоставлении виртуальными сервисами под низкие процентные ставки пользователям займов в криптовалюте или фиатных денежных средствах под залоговое обеспечение в виде отличных от кредитных криптовалют или фиата. Такой вид кредитования обладает рядом преимуществ перед стандартным банковским кредитом. В первую очередь, это связано с отсутствием проверки кредитной истории пользователя, что позволяет любому заемщику взять криптокредит, даже имея задолженности по иным договорам, поскольку такая информация никем не проверяется. Еще одним преимуществом является скорость получения кредита, поскольку процедура кредитования упрощена и может занять несколько минут: от момента регистрации на сервисе до получения на онлайн-кошелек средств. Для инвесторов кредитование — возможность получения пассивного дохода за счет процентов по кредитам.

Среди целей обращения к криптокредитованию можно выделить следующие: желание заработать на волатильности курсов криптовалют при отсутствии своих криптосредств; получение криптовалют в кредит под небольшой

процент для последующей их реализации на другой платформе в качестве инвестора под более высокий процент; обмен кредитных криптовалют на фиатные денежные средства в случаях невозможности обращения в банки и др. Однако, несмотря на положительную тенденцию в сфере виртуальных криптокредитов, отмечаются и некоторые недостатки, которые связаны с нестабильностью курсов криптовалют, отсутствием правового регулирования и страхования активов, а также возможностью потери средств ввиду мошеннических действий киберпреступников.

Криптокредиты по функциональности можно разделить на обеспеченные залогом и необеспеченные, к которым относятся флеш-кредиты («мгновенный займ») и кредитное плечо. Обеспеченные кредиты предоставляются пользователям в криптовалюте под залог иного вида криптовалюты или денежных средств, по своему количеству превышающий большую часть займа или равный ему (в случае невозврата залог переходит в собственность сервиса или инвестора). Флеш-кредиты выдаются без обеспечения, но под условием возврата полученных средств в рамках одного блока транзакций, что свидетельствует о максимальной скорости возврата полученных активов, так как в противном случае при невыполнении данного условия все транзакции считаются аннулированными и займ возвращается в пул сервиса. Кредитное плечо дает возможность в несколько раз увеличить вносимый задаток для дальнейшего осуществления обменных операций и получения дохода, исходя из разницы курсов криптовалют на различных платформах.

В зависимости от профессиональных навыков кибермошенников и механизмов криптокредитования способы осуществления хищений криптовалют подразделяются на две группы: бытовые и профессиональные. К бытовому хищению относятся мошеннические действия заемщиков средств, пользующихся отсутствием должной верификации пользователей со стороны криптокредитных сервисов. Так, незначительная часть криптоплатформ готовы предоставлять пользователям займы, не удостоверившись в личности будущего клиента, что и позволяет заемщикам, получив средства на специально созданный онлайн-кошелек, пропустить их через криптомиксер и вывести на другой кошелек или в фиат через обменник. Те сервисы, которые используют усиленную систему KYC (знай своего клиента), также подвержены мошенническим действиям заемщиков, поскольку последние представляют поддельные документы и фотографии. Частота подобных случаев привела к созданию всеобщего клиентского черного списка, куда администрации сервисов заносят недобропорядочных клиентов. Однако даже такая мера вскоре была предусмотрена мошенниками, которые на протяжении определенного промежутка времени брали и действительно возвращали кредиты, создавая себе образ добросовестного заемщика,

после чего возвращались к первоначальным схемам обмана. Стоит отметить, что сумма похищенных при данных обстоятельствах криптовалют небольшая, поскольку такими методами хищение можно реализовать только с залоговыми кредитами. Таким образом, мошенник похищает лишь разницу между суммой кредита и его обеспечением.

Хищения профессионального уровня, то есть осуществляемые лицами, обладающими знаниями в сфере программирования и IT-технологий, осуществляются посредством трех способов, различающихся требуемыми навыками для их реализации: простой — хищение средств инвесторов, усложненный — использование фишинговых и фарминговых сайтов, сложный — хищение посредством хакерских атак, сопряженных с манипулированием ценовыми оракулами. В основе простого способа лежит создание проекта сервиса по криптовалютному кредитованию, цель которого — аккумулирование средств инвесторов, привлекаемых обещаниями о высоких процентных ставках, для последующего их хищения. Так, мошенники разрабатывают ICO-проект и его оболочку, активно рекламируют сервис в социальных сетях и иных интернет-ресурсах. Когда инвесторы своими вкладами сформировали пул проекта, мошенники выводят активы с платформы на сторонний кошелек, для сокрытия цифровых следов используют криптомиксеры, анонимные криптокошельки, VPN-сервисы, после чего нейтрализуют проект. Описанный механизм требует от преступников базовых знаний в сфере программирования и веб-дизайна для создания оболочки и рекламы, а также определенного промежутка времени для сбора достаточного инвестиционного фонда.

Усложненный механизм базируется на создании фишинговых или фарминговых страниц, копирующих дизайн реальных действующих проектов, имеющих положительную репутацию. Переход к «дублирующим» сайтам криптокредитных сервисов осуществляется через рекламные объявления, электронные письма или вирусные программы (свойственны для фарминга, при котором программный код в фоновом режиме изменяет в браузере адрес искомого ресурса на поддельный, куда и попадает пользователь). Фишинговые схемы направлены на хищения криптовалют как у инвесторов, так и у заемщиков, вносящих обеспечение. Так хакеры либо обманным путем получают на свои кошельки криптовалюту, либо путем использования конфиденциальных данных пользователей, введенных на сайте, несанкционированно попадают в их криптокошельки и переводят средства самостоятельно. Далее механизм действует по уже описанной схеме сокрытия и реализации похищенного.

В отличие от двух вышеописанных способов сложная хакерская атака базируется на манипуляции с протоколами блокчейна ценового оракула и содержит в своем механизме операции со всеми тремя видами криптокредитования.

Для того чтобы на примере разобрать преступный механизм, необходимо выяснить сущность и функциональное назначение смарт-контрактов и оракулов.

Смарт-контракты являются основой криптокредитования, организуют взаимоотношения между инвесторами, образующими пул сервиса кредитования, и заемщиками. Смарт-контракт — протокол, который содержит алгоритм последовательных действий, выполняемых автоматически по заданным параметрам сделки без привлечения третьих лиц. Особенностью смарт-контракта является отсутствие возможности внести изменения в алгоритм или остановить выполняемые программой действия, если они уже были инициированы. Так как смарт-контракт действует внутри блокчейна, не имеющего связи с процессами, происходящими в онлайн-сети, то ему необходимо некоторое связующее звено, которое могло бы предоставлять необходимую информацию и перерабатывать ее на формат, усваиваемый блокчейном платформы. В роли такого ассистента в криптокредитовании выступает блокчейн-оракул. Для работы блокчейн-оракулу необходимы три составляющие: источник данных, запрос и оракул (консенсус оракулов) [1]. В роли источника данных ценового оракула выступают сервисы, отслеживающие волатильность курса необходимых блокчейну пар криптовалют. Для обращения к источнику данных блокчейн-оракул использует запрос — код, устанавливающий потоки данных. И центральным звеном блокчейн-оракула является сам оракул (или их группа) — алгоритм, который отвечает за связь с источником и форматирование полученной информации для основного блокчейна.

С целью установления причины, по которой стала возможна манипуляция с блокчейн-оракулами, рассмотрим два примера мошеннических действий с криптокредитами.

Пример 1. Шаг 1: заемщик (хакер) берет на децентрализованной платформе A флеш-кредит на 10 000 ETH (криптовалюта — эфир). Из них 5 500 ETH (остаток — 4 500 ETH) вносит на платформу B в качестве залога под кредит в 112 WBTC. Шаг 2: из оставшихся 4 500 ETH переводит 1 300 ETH на платформу C (остаток 3 200 ETH) под кредитное плечо 5x, т. е. получает на выходе уже 6 500 ETH. Шаг 3: из 6 500 ETH вносит 5 600 ETH (остаток 900 ETH) на платформу D, которая, используя ценовой оракул, через резерв криптообменника E производит обмен 5 600 ETH на 51 WBTC, что позволило увеличить курс WBTC на платформе E. Шаг 4: 112 WBTC, взятые на платформе B, заемщик продает через обменник E, только теперь уже по завышенной цене, и получает 6 900 ETH. Шаг 5: из оставшихся во 2-м шаге 3 200 ETH и полученных из 4-го шага 6 900 ETH заемщик погашает флеш-кредит на платформе A, после чего у него остается 100 ETH и 900 ETH от кредитного плеча, которое покрыли 51 WBTC, увеличенные в цене. Таким образом, можно заметить, что платфор-

ма E является единым источником для оракулов платформ B, C и D, т. е. при изменении курса пары валют на платформе E курсы автоматически меняются и на платформах B, C и D, что и позволяет хакеру вывести криптовалюты из пулов платформы C. Предусмотреть и предупредить такие ситуации практически невозможно, так как все операции по флеш-кредитам производятся за несколько минут, а выведенные активы миксуются через криптомиксеры и выводятся в фиат.

Пример 2. Шаг 1: заемщик (хакер) берет на децентрализованной платформе A флеш-кредит на 7 500 ETH (криптовалюта — эфир). Из них 3 500 ETH (остаток — 4 000 ETH) продает в криптообменнике B за 940 000 SUSD (стейблкоин, который имеет денежное обеспечение, его стартовая цена равна 1 доллару). Полученные 940 000 SUSD переводит в качестве обеспечения флеш-кредита на платформу A. Шаг 2: из оставшихся 4 000 ETH заемщик 900 ETH (осталось 3 100 ETH) вносит на платформу C и обменивает через источник — платформу D на SUSD, в результате чего курс SUSD увеличивается до 2,30 долларов, а значит, увеличивается и залог в 940 000 SUSD на платформе A в два раза. Шаг 3: увеличенный залог позволяет заемщику взять на платформе A теперь уже залоговый кредит в 6 800 ETH, который он переводит в качестве погашения первоначального флеш-кредита, дополняя остатком 3 100 ETH из шага 2. Таким образом, у заемщика остались 2 400 ETH, выведенные из пула платформы A. Причина удачи данной схемы та же, что и в первом примере: D — общий источник курса для A и C.

С точки зрения криминалистической методики расследования хищений криптовалют, совершаемых описанными выше способами, основной проблемой для следствия и дознания является отсутствие цифровых данных, позволяющих отследить дальнейший переход похищенных криптовалют, а также невозможность выявления пользователя, совершившего такие действия, по IP-адресу ввиду использования VPN, анонимайзеров или сети Tor. Несмотря на то, что указанные сервисы централизованы и каждый имеет сервер, хранящий данные о пользователях и их деятельности, получить эти сведения не представляется возможным по следующим причинам: во-первых, сервисы, используемые мошенниками, зарегистрированы в различных государствах, преимущественно с низкой степенью развития инфраструктуры и отсутствием налаженных контактов по оказанию международной помощи в рамках расследования уголовных дел или сбора оперативных данных по материалам проверки; во-вторых, даже если поручение исполняется и запрос доходит до адресата, то ответом является отказ в предоставлении информации, обосновываемый политикой конфиденциальности или иными причинами. Следовательно, единственная легитимная возможность по цифровым следам разыскать мошенников и хакеров для при-

влечения к уголовной ответственности и возмещения ущерба остается недоступной, ввиду чего более 90 % уголовных дел, возбужденных по факту хищения криптовалют, приостанавливаются.

Таким образом, криптовалютное кредитование стало еще одним средством для реализации преступных схем хищения криптовалют как путем обмана пользователей, так и путем несанкционированного доступа к онлайн-кошелькам. Криминалистический анализ хищений в сфере криптокредитования позволил определить способы и механизмы совершения преступных операций, а также выявить ключевую проблему в работе с цифровыми следами, устранение которой требует дальнейшей совместной работы криминалистов, правоохранительных органов и специалистов в сфере IT-индустрии и оборота криптовалют с целью разработки путей и способов получения криминалистически значимой информации, применимой в процессе доказывания по материалам и уголовным делам.

---

1. Блокчейн-оракулы как связь между цифровым и реальным миром [Электронный ресурс] // Интернет-журнал «DeCenter». URL: https://decenter.org/ru/blokcheyn-orakuly-kak-svyaz-mezhdu-tsifrovym-i-realnym-mirom (дата обращения: 12.02.2021). Перейти к источнику Вернуться к статье