

И. В. Коржова, Н. А. Хан

РАССЛЕДОВАНИЕ СОВЕРШАЕМЫХ В СФЕРЕ ОБОРОТА ЦИФРОВЫХ ФИНАНСОВЫХ АКТИВОВ УГОЛОВНЫХ ПРЕСТУПЛЕНИЙ

Освещаются последние тенденции в области правового регулирования криптовалюты в Российской Федерации, выявляются сложности, связанные с расследованием хищений криптоактивов. На примере практических ситуаций предлагается набор действий, которые необходимо провести органам, осуществляющим предварительное расследование или оперативно-розыскную деятельность, при расследовании хищений криптовалюты. Статья сосредоточена на доказательственном аспекте, связанным со сбором, анализом и фиксацией доказательств, полученных на досудебных стадиях уголовного судопроизводства. Основным результатом научного исследования является разработка методологии расследования преступлений, в которых криптоактивы выступают предметом преступного посягательства.

51

The authors highlight the latest trends in the legal regulation of cryptocurrencies in the Russian Federation, identify difficulties associated with the investigation of the theft of crypto assets. On the example of practical situations, the authors propose a set of possible actions that need to be carried out by the bodies conducting the preliminary investigation or by the body conducting operational-search activities in the investigation of the theft of cryptocurrency. Mainly, the article focuses on the evidence aspect related to the collection, analysis and fixing of evidence obtained at the pre-trial stages of criminal proceedings. The main result of scientific research is the development of a methodology for investigating crimes in which crypto assets are the subject of a criminal attack.

Ключевые слова: криптоактивы, криптовалюта, технология распределенного реестра, правонарушение, хищение, доказательства, расследование.

Keywords: crypto assets, cryptocurrency, distributed registry technology, offense, theft, evidence, investigation.

За последние несколько лет в имущественный оборот все прочнее включаются цифровые финансовые активы: криптовалюты и токены (инвестиционные, утилитарные, кредитные и т.п.) — активы, обладающие имущественной ценностью, в основе которых лежит технология распределенного реестра (технология Blockchain).

С одной стороны, новая цифровая технология предоставляет участникам преимущества с точки зрения безопасности за счет технологических принципов, лежащих в ее основе. Так, вся база Blockchain находится в публичном доступе, посмотреть данные того или иного блока и отследить изменение информации может любой желающий. Однако сведения о том, кто и кому перевел криптоактивы, могут быть доступны лишь непосредственным участникам обмена.



С другой стороны, обращение криптоактивов подвергает дополнительным угрозам их участников, общество в целом и государство. Согласно отчету компании Cipher Trace, с начала 2019 г. пользователи криптовалют потеряли свыше \$4,3 млрд из-за взломов криптобирж, мошенничества и вымогательства [9].

Рассмотрим обозначенный сектор криптопреступности – хищение криптоактивов, в котором последние выступают в качестве предмета преступного посяательства.

В первую очередь необходимо обратить внимание на существующие проблемы, связанные с расследованием и квалификацией преступлений, связанных с хищением криптоактивов, в том числе:

1) сложность в доказывании данного рода преступлений, отсутствие методических рекомендаций по организации раскрытия и расследования преступлений, связанных с хищением криптоактивов;

2) отсутствие у сотрудников правоохранительных органов специальных знаний, необходимых для расследования хищения криптоактивов;

3) отсутствие традиционных финансовых посредников и администраторов в криптовалютных платежных системах [13];

4) отсутствие требований по идентификации пользователей при совершении сделки и анонимность / псевдоанонимность некоторых транзакций, возможность сокрытия личностей отправителей и получателей криптовалюты [16];

5) трансграничность: владельцы криптоактивов и киберпреступники чаще всего находятся в различных юрисдикциях;

6) отсутствие полноценного правового регулирования криптоактивов в Российской Федерации.

В настоящее время (по состоянию на 15 ноября 2019 г.) Государственной Думой Российской Федерации приняты или находятся на рассмотрении три законопроекта, которые направлены на регулирование сферы цифровых финансовых активов:

1) принятый и вступивший в силу с 1 октября 2019 г. федеральный закон от 18.03.2019 №34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» [11] (далее – Закон о цифровых правах). В частности, Законом о цифровых правах в Гражданский кодекс Российской Федерации включена статья 1411, посвященная «цифровым правам», под которыми понимаются «названные в таком качестве в законе обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам» [4]. Из формулировки следует, что под нее попадают только те объекты, по которым обязательно какое-либо лицо, то есть токены, выпускаемые конкретными организациями, в то время как классические криптовалюты (такие, как Bitcoin) цифровыми правами не являются [8].

2) федеральный закон от 02.08.2019 № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» [12], который вступает в силу с 1 января 2020 г. Данным законом вво-

дится понятие утилитарных цифровых прав, которые, в сущности, являются бонусами, купонами или ваучерами на получение конкретных товаров и услуг в будущем;

3) проект федерального закона №419059-7 «О цифровых финансовых активах» (редакция, принятая ГД ФС РФ в I чтении 22.05.2018) [10], доработка и принятие которого ожидается в ближайшее время. В исходной редакции, принятой нижней палатой российского парламента, законопроект №419059-7 нормативно обозначал два вида цифровых финансовых актива: криптовалюту и токен, однако впоследствии все нормы о криптовалюте были исключены из текста законопроекта [15]. По информации ИА «Финмаркет» от 31 октября 2019 г., в процессе обсуждения проекта федерального закона №419059-7 выяснилось, что в России может быть легализован выпуск цифровых операционных знаков (криптовалют, в соответствии с терминологией законопроекта). Между тем, в отличие от классических криптовалют, основанных на permissionless-сетях, выпуск цифровых операционных знаков осуществляется на закрытых Blockchain-платформах [2].

Одним из последних наиболее интересных предложений со стороны правоохранительного сектора Российской Федерации стала планируемая разработка Министерством внутренних дел механизма ареста и конфискации криптовалют. Соответствующие предложения до 31 декабря 2021 г. должно подготовить МВД совместно с Росфинмониторингом, Генеральной прокуратурой, Следственным комитетом, Минюстом, ФСБ, ФТС и ФССП при участии Верховного суда. К виртуальным активам, которыми займется МВД, в первую очередь относятся криптовалюты [14]. Между тем, реализация данной идеи вызывает вопросы, обусловленные не только неопределенным статусом криптовалюты в Российской Федерации, но и техническими сложностями.

Анализ содержания названных законопроектов позволяет сделать вывод о том, что норм, посвященных непосредственно «охранительной тематике» в данных документах не содержится, однако с официальным появлением цифровых прав, а также связанных с ними феноменов в российском законодательстве появилась возможность включить в нормы уголовного и уголовно-процессуального кодекса соответствующие бланкетные нормы [6].

Поскольку в основе криптоактивов лежит технология Blockchain, можно говорить о наличии специфического слеодообразования при хищении криптоактивов [7], поскольку любая транзакция образует след в виде электронной записи (необходимо уточнение – происходит «журнализация изменений»), что облегчает задачу по установлению обстоятельств совершенного правонарушения [1].

Ввиду существующих проблем в области расследования преступлений, связанных с хищением криптоактивов, а также других обстоятельств нам представляется необходимой разработка специальной методики расследования преступлений, в которых криптоактивы являются предметом преступного посягательства.

К каким практическим ситуациям она применима? Попробуем рассмотреть на конкретных примерах: лицо А покупает за криптовалюту



несуществующий товар, у лица В похитили криптовалюту, создав фишинговый сайт, у лица С «выманили» инвестиции в мошеннический проект. Ситуации разные, однако механизмы, которые могут и должны использовать правоприменители, сходные.

Как расследовать подобные преступления? В первую очередь органам предварительного расследования необходимо проанализировать сопутствующие обстоятельства дела: баланс кошелька, стоимость и подробную историю операций (их регулярность, место, назначение), выделив адреса, связанные с адресом преступника, закономерности или подозрительные взаимодействия.

Для этого компетентные органы могут использовать специально разработанные для этих целей сервисы, анализирующие состояние криптокошелька [5]. Для демонстрации работы данных сервисов мы использовали приложение ORS CryptoHound, ввели в поисковую строку адрес биткоин-кошелька, сформированный случайной выборкой, и получили следующие результаты.

На рисунке 1 изображена частота совершения операций. Посмотрев на график, любой интернет-пользователь может сделать вывод о том, что пик совершенных владельцем кошелька операций пришелся на 18 февраля 2019 г. А к 19 августа 2019 г. активность владельца упала до нуля.

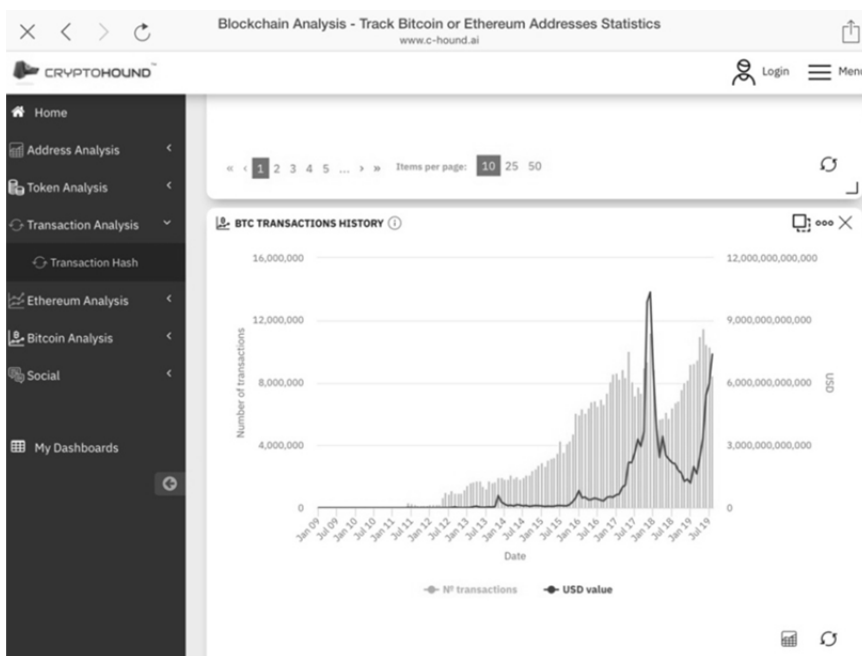
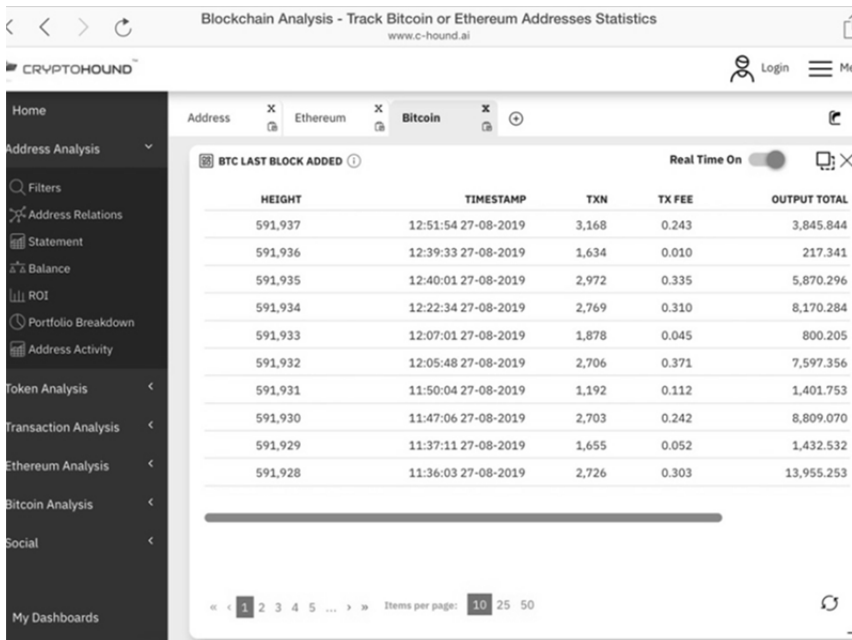


Рис. 1. Частота совершения операций

На рисунке 2 изображена таблица с подробным отчетом обо всех транзакциях, совершенных за выбранный промежуток времени

(с 9 июня по 19 июля 2019 г.). На диаграмме представлена информация о времени совершения той или иной транзакции, реквизитах электронных кошельков, на которые были переведена криптовалюта, а также суммы переводимых средств.



HEIGHT	TIMESTAMP	TXN	TX FEE	OUTPUT TOTAL
591,937	12:51:54 27-08-2019	3,168	0.243	3,845.844
591,936	12:39:33 27-08-2019	1,634	0.010	217.341
591,935	12:40:01 27-08-2019	2,972	0.335	5,870.296
591,934	12:22:34 27-08-2019	2,769	0.310	8,170.284
591,933	12:07:01 27-08-2019	1,878	0.045	800.205
591,932	12:05:48 27-08-2019	2,706	0.371	7,597.356
591,931	11:50:04 27-08-2019	1,192	0.112	1,401.753
591,930	11:47:06 27-08-2019	2,703	0.242	8,809.070
591,929	11:37:11 27-08-2019	1,655	0.052	1,432.532
591,928	11:36:03 27-08-2019	2,726	0.303	13,955.253

Рис. 2. Отчет о совершенных транзакциях

Таким образом, органы предварительного расследования могут получить большой массив информации, обладая всего лишь реквизитами криптокошелька пользователя. Для ознакомления с этой информацией достаточно обратиться к соответствующей записи в цепи блоков транзакций той альтернативной платежной системы, посредством которой осуществлен перевод [3, с. 91].

Следующим — наиболее сложным — этапом в процессе доказывания является установление конкретных лиц, осуществивших ту или иную транзакцию. Типичное поведение, которого придерживается криптопреступник, — использование кластера адресов, чтобы скрыть движение криптовалюты. Органы предварительного расследования, прослеживая всю цепочку переводов, смогут выйти на конечного бенефициара, которого необходимо при возможности идентифицировать. Но как это сделать? Посредством интерпретации ранее собранных доказательств, которая требует от «интерпретатора» не только опыта, но и интуиции, а также глубокой проработки открытых источников (пользовательский поиск в различных поисковых системах, новостные статьи от ведущих криптографических СМИ, социальные сети) [5].

Отдельно хотелось бы обратить внимание на Базу данных судебных исков Blockchain (BLD), запущенную нью-йоркской финансовой юри-



дической фирмой *Murphy & McGonigle*. Данный коммерческий проект (или аналогичные проекты, созданные по модели, которая будет описана ниже) могут быть использованы правоохранительными органами в целях расследования правонарушений, связанных с созданием мошеннических ICO, мошеннических криптофондов [17].

Данные, отслеживаемые BLD, включают общее количество случаев мошенничества в этой сфере, годовые тенденции, информацию, под сферу уголовного или гражданского права попадает дело, обобщенные обстоятельства одного или группы случаев, которые могут относиться к новым стартапам или проектам [17]. Подобные сервисы имеют большой потенциал и ресурсы, чтобы оказывать информационную поддержку компетентным властям. Также в будущем возможно создание аналогичных проектов, ориентированных в большей степени на правоохранительную составляющую.

При этом всю собранную информацию необходимо своевременно протоколировать, поскольку технология распределенного реестра, лежащая в основе похищенных криптоактивов, имеет специфический характер доказывания, хотя общие подходы в части исчерпывающего перечня видов доказательств и производства следственных действий применимы и к новым криптосущностям.

Факты, собранные посредством блокчейн-анализа, могут быть подведены к стандартным исчерпывающим видам доказательств, перечисленных в ст. 74 Уголовно-процессуального кодекса Российской Федерации. Например, в качестве протоколов следственных или судебных действий, заключений, показаний специалистов, других видов доказательств [18].

Таким образом, внедрение в оборот цифровых активов создает дополнительные угрозы информационной безопасности личности, общества и государства, что обуславливает необходимость разработки новых методики расследования правонарушений, совершаемых в этой сфере, а также совершенствования законодательства и разработки новых подходов регулирования правоотношений в области токенов и криптовалют, организации борьбы с киберпреступностью. Открытость информации о совершенных операциях является дополнительной возможностью в области эффективного расследования уголовного дела.

Список литературы

1. Борисов М.Б., Заводцев И.В. Проблемы совершенствования допуска и доступа субъектов в информационные системы в условиях цифровой экономики // Проблемы экономики и юридической практики. 2019. №2. С. 267 – 270.
2. Выпуск криптовалюты в РФ может быть легализован на закрытых блокчейнах // Финмаркет. URL: <http://www.finmarket.ru/news/5108559> (дата обращения: 10.11.2019).
3. Галушин П.В., Карлов А.Л. Сведения об операциях с криптовалютами (на примере биткойна) как доказательство по уголовному делу // Ученые записки Казанского юридического института МВД России. 2017. Т. 2, №4. С. 90 – 100.
4. Гражданский кодекс Российской Федерации (часть первая) от 30 нояб. 1994 г. №51-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

5. *How to Investigate a Crypto Crime: a Simple Step-by-Step Guide* // Crypto Digest. URL: <https://cryptodigestnews.com/how-to-investigate-a-crypto-crime-a-simple-step-by-step-guide-5a9baf5112ad> (дата обращения: 10.11.2019).

6. Коржова И. В., Хан Н. А. Рецензия на монографию А. А. Максурова «Криптовалюты и правовое регулирование их обращения» // Финансовая экономика. 2019. № 2. С. 267 – 269.

7. Кучеров И. И. К вопросу о методике расследования преступлений, совершенных с использованием криптовалюты // Российский следователь. 2018. № 12. С. 17 – 21.

8. Новоселова Л., Габов А., Савельев А. и др. Цифровые права как новый объект гражданского права // Закон. 2019. № 5. С. 31 – 56.

9. Преступники похитили 4,3 млрд долларов в криптовалюте в 2019 году // Bankir.ru. URL: <https://bankir.ru/novosti/20190813/prestupniki-pohitili-43-mlrd-dollarov-v-kriptovalute-v-2019-godu-10164368/> (дата обращения: 10.11.2019).

10. Проект федерального закона № 419059-7 «О цифровых финансовых активах» // Система обеспечения законодательной деятельности: [сайт]. URL: <http://sozd.parliament.gov.ru/bill/419059-7> (дата обращения: 11.11.2019).

11. О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации : федер. закон от 18 марта 2019 г. № 34-ФЗ // Российская газета. № 60 (7818).

12. О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации : федер. закон от 2 августа 2019 г. № 259-ФЗ // Российская газета. № 172 (7930).

13. Лейба А. Реальная жизнь виртуальных денег // ЭЖ-Юрист. 2014. № 23. С. 1.

14. МВД разработает механизм ареста и конфискации криптовалют // РБК. URL: <https://www.rbc.ru/finances/07/11/2019/5dc160019a7947c61a5119a3> (дата обращения: 10.11.2019).

15. Разбираем все минусы законопроекта о цифровых финансовых активах // Bit Journal Media. URL: <https://bitjournal.media/01-02-2018/razbiraem-vse-minusy-zakonoproekta-minfina-rf-o-tsifrovyyh-finansovyh-aktivah/> (дата обращения: 10.11.2019).

16. Рязузова Д. А. Понятие, гражданско-правовой статус и теоретическая модель уголовно-правовой охраны виртуальной валюты (криптовалюты) нормами главы 21 УК РФ // Международное уголовное право и международная юстиция. 2018. № 1. С. 29 – 32.

17. *The Blockchain Litigation Database (BLD) Opens Up a New Tech Focus for Law* // BeInCrypto. URL: <https://beincrypto.com/the-blockchain-litigation-data-base-bld-opens-up-a-new-tech-focus-for-law> (дата обращения: 10.11.2019).

18. Уголовно-процессуальный кодекс Российской Федерации от 18 дек. 2001 г. № 174-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

Об авторах

Ирина Вадимовна Коржова – магистрант, Московский государственный университет им. М. В. Ломоносова, Россия.

E-mail: irina140497@yandex.ru

Николай Александрович Хан – канд. ист. наук, ООО «Команда комплексных экспедиционных разработок», Россия.

E-mail: kh-niko@mail.ru



The authors

Inna V. Korzhova, Master's Student, Lomonosov Moscow State University, Russia.
E-mail: irina140497@yandex.ru

Dr Nikolay A. Khan, LLC «Team of Expeditionary Research and Development»,
Russia.
E-mail: kh-niko@mail.ru