

Научная статья

УДК 340.1

ПРОЦЕССУАЛЬНАЯ СПЕЦИФИКА В РАССЛЕДОВАНИИ ПРЕ- СТУПЛЕНИЙ, СВЯЗАННЫХ С КРИПТОВАЛЮТОЙ

**Владислав Матвеевич ЧЕРЕПКОВ и Альбина Маратовна КАША-
ПОВА**

Московская Академия Следственного комитета Российской Федерации
им. А.Я. Сухарева, г. Москва, Россия

alcashapova@yandex.ru

Научный руководитель профессор кафедры уголовного процесса Мос-
ковской Академии Следственного комитета Российской Федерации им.
А.Я. Сухарева, доктор юридических наук, доцент, профессор **Игорь Бори-
сович ТУТЫНИН**, Tutig@rambler.ru

Аннотация. Статья посвящена актуальным проблемам процессуального обеспечения расследования преступлений, связанных с использованием криптовалют. Основное внимание уделяется процессуальной специфике сбора цифровых следов как ключевого этапа доказывания в условиях децентрализации и псевдоанонимности блокчейн-экосистем.

Авторами проводится анализ современных методик идентификации владельцев кошельков и отслеживания перемещения активов. Особое внимание уделяется корректному процессуальному оформлению результатов такой аналитики для придания им статуса допустимых доказательств.

В работе детально исследуются сложные процессуальные аспекты изъятия и ареста криптовалюты, взаимодействие с криптобиржами и провайдерами крипто-услуг для наложения обеспечительного ареста на цифровые активы.

Ключевые слова: криптовалюта, цифровые следы, доказывание, OSINT, блокчейн, деанонимизация, изъятие криптовалюты.

PROCEDURAL SPECIFICS IN THE INVESTIGATION OF CRYPTO- CURRENCY-RELATED CRIMES

Vladislav M. CHEREPKOV and Albina M. KASHAPOVA

A.Ya. Sukharev Moscow Academy of the Investigative Committee of the Russian Federation, Moscow, Russia

alcashapova@yandex.ru

Scientific adviser - Professor at the Department of Criminal Procedure, A.Ya. Sukharev Moscow Academy of the Investigative Committee of the Russian Fed-

eration; Doctor of Law, Associate Professor, Professor **I. B. Tutynin**,
Tutig@rambler.ru

Abstract. This article addresses current issues regarding the procedural aspects of investigating crimes involving the use of cryptocurrencies. The primary focus is on the procedural specifics of collecting digital traces—a key stage in the evidentiary process—amidst the decentralization and pseudo-anonymity characteristic of blockchain ecosystems.

The authors analyze modern methods for identifying wallet owners and tracking asset movements. Particular attention is paid to the proper procedural documentation of such analytical findings to ensure their status as admissible evidence.

The paper examines in detail the complex procedural aspects of cryptocurrency seizure and asset freezing, as well as interaction with crypto exchanges and service providers to secure digital assets through provisional measures.

Keywords: cryptocurrency, digital traces, evidentiary process, OSINT, blockchain, deanonymization, cryptocurrency seizure

Современный этап цифровой трансформации финансового оборота характеризуется активным внедрением криптоэкономических инструментов, основанных на технологии блокчейн. Криптовалюты как децентрализованные виртуальные активы, защищенные криптографическими методами, обеспечивают высокий уровень анонимности пользователей, что предопределяет не только их привлекательность для легитимного использования, но и растущую эксплуатацию в преступных целях.

Широкий спектр противоправных деяний, совершаемых с применением цифровых активов, - от легализации доходов и финансирования терроризма, до торговли запрещенными товарами и кибермошенничества - формирует новый вызов для системы уголовного судопроизводства. Универсальность криптовалют позволяет преступникам не только опосредовать расчеты в теневом секторе, но и эффективно маскировать происхождение и движение средств, существенно осложняя традиционные механизмы раскрытия преступлений.

Использование криптовалют позволяет преступникам минимизировать прямой контакт и оставлять цифровой след, крайне трудно поддающийся процессуальной фиксации и интерпретации в рамках уголовного дела [1, с. 167–173]. Эмпирические данные подтверждают масштаб проблемы, указывая на криптовалюты как на доминирующий инструмент в незаконном обороте наркотиков¹ и иных доходоприносящих преступлениях.

В этих условиях противодействие «криптопреступности» - кругу деяний, совершаемых с использованием цифровых активов или направленных на них, - упирается в системные процессуальные затруднения. Ключевым препятствием становится неадаптированность существующих процедур собирания, проверки и оценки доказательств к специфике технологии блокчейн, использованию обменных сервисов и кошельков, чья инфраструктура зачастую находится вне национальной юрисдикции.

В следственной практике выделяются две типовые ситуации:

1. когда известен криптовалютный адрес;
2. когда есть подозрения в отношении конкретного лица, которое может использовать криптовалюту. В первой ситуации стратегия строится на движении от адреса к личности через выявление его взаимодействия с регулируемым финансовым сектором, прежде всего с провайдерами услуг виртуальных активов (биржами, обменниками).

Современный этап развития информационного общества, характеризующийся экспоненциальным ростом больших данных (Big Data) в виртуальном пространстве, предопределяет особую роль информационно-телекоммуникационных сетей как ключевого источника криминалистически значимой информации. Это становится фундаментальной основой для установления обстоятельств преступлений, особенно совершаемых с использованием IT-технологий, и причастных к ним лиц. В этом контексте

¹ Рынок незаконного оборота наркотиков на 60% использует криптовалюту [Электронный ресурс] // РАПСИ. – URL: rapsinews.ru (дата обращения: 26.10.2023)

актуализируется необходимость применения в процессуальной и оперативно-розыскной деятельности специальной технологии - «Поиска и анализа информации из открытых источников» (OSINT - Open Source Intelligence). К ее основным преимуществам относится способность эффективно работать с большими объемами разрозненных (неструктурированных) данных. Сущность OSINT заключается в системном мониторинге открытых источников и элементов инфраструктуры информационно-телекоммуникационной среды с применением информационно-аналитических методов (Data Mining). Целью является поиск, обнаружение и фиксация информации, имеющей значение для раскрытия и расследования подготавливаемого, совершаемого или совершенного преступления. Таким образом, OSINT представляет собой техническое мероприятие, направленное на получение и анализ релевантной общедоступной информации из сети «Интернет» для нужд уголовного судопроизводства [2, с. 261].

Так, на этапе деанонимизации и выявления цифровых следов активно применяются методы OSINT (Open Source Intelligence), реализуемые в том числе через специализированный программный комплекс «Охотник»², который позволяет в автоматизированном режиме агрегировать и анализировать данные из открытого интернета, социальных сетей и даркнета для установления личности владельца аккаунта или его связей. Непосредственно анализ криптовалютных транзакций и реконструкция финансовых схем обеспечиваются государственными инструментами блокчейн-аналитики: государственной системой «Прозрачный блокчейн» (Росфинмониторинг), программой «КриптоФинМон» [3, с. 61], а также коммерческими платформами типа Tokenscope. Эти сервисы выполняют задачи отслеживания цепочек транзакций, кластеризации адресов, выявления точек

² Свидетельство о государственной регистрации программы для ЭВМ № 2021680077 от 07.12.2021.

«входа/выхода» на регулируемые биржи и оценки рисков, что в совокупности создает основу для формирования доказательственной базы и последующего изъятия цифровых активов.

В рамках типовой следственной ситуации, когда в материалах дела присутствует криптовалютный адрес, первоочередной задачей является установление его принадлежности к конкретному провайдеру услуг виртуальных активов - централизованной бирже или обменному сервису. После успешной идентификации такого провайдера следователь направляет ему адресованный запрос с истребованием комплекса идентификационных данных пользователя, включая реквизиты банковских карт или электронных кошельков, номера телефонов, IP-адреса сессий доступа и персональные данные, предоставленные при верификации. Если прямая принадлежность адреса не установлена, процессуальная деятельность переходит к углубленному анализу цепочек транзакций. Данный этап, как отмечается в методических рекомендациях, предполагает выявление всех связанных адресов (например, адресатов по транзакциям ввода-вывода) с последующей проверкой их на принадлежность известным операторам через специализированные сервисы блокчейн-аналитики. Такая проверка позволяет установить опосредованного оператора и направить ему аналогичный запрос на предоставление цифровых следов конечного владельца целевого адреса [3, с. 51–55].

Исполнение решения суда подтверждается не присутствием представителя, а записью в блокчейне.

Таким образом, эффективное доказывание по делам о преступлениях с использованием криптовалют требует синтеза специальных технических знаний и классических процессуальных процедур. Успех зависит от системного применения инструментов OSINT и блокчейн-аналитики, оперативного взаимодействия с провайдерами услуг и грамотной фиксации цифровых следов для последующего изъятия криптоактивов.

Во второй типовой ситуации, когда подозрение падает на конкретное лицо, процессуальный поиск строится в обратном направлении: от фигуранта к его криптоактивам [3, с. 63]. Эффективными мерами, согласно практическим рекомендациям, являются:

1. тщательный анализ операций по банковским счетам лица на предмет нетипичных поступлений или списаний некруглых сумм (например, 3912 руб. 62 коп.), что может свидетельствовать о конверсии криптовалюты в фиатные средства, с последующим установлением контрагентов;

2. направление адресных запросов как в известные следователю, так и в наиболее популярные криптобиржи (Binance, Bybit и др.) по имеющимся данным фигуранта (ФИО, телефон, email) для установления факта наличия учетной записи и получения истории операций;

3. производство обыска по месту жительства или работы с целенаправленным поиском цифровых следов. К ним относятся не только аппаратные кошельки (например, устройства Trezor, Ledger) и установленные криптовалютные приложения, но и материальные носители seed-фраз или приватных ключей (записи на бумаге, в записных книжках, файлы на электронных носителях), обнаружение которых является критически важным для последующего доступа к активам. Дополнительно, при изъятии компьютерной техники, может назначаться судебно-техническая экспертиза с целью извлечения приватных ключей с помощью специализированного программного обеспечения.

Кульминационной и наиболее специфичной процессуальной процедурой является изъятие и арест криптовалюты. В силу децентрализованной природы этих активов изъятие возможно только путем перевода средств с адреса подозреваемого на контролируемый следствием кошелек. Заблокировать сам адрес в блокчейне невозможно, за исключением блокировки аккаунта на централизованной бирже по решению суда.

В настоящее время механизм наложения ареста на криптовалюту и ее конфискации не отработан. Поскольку установление ключей к электронным кошелькам на практике проблематично, фактически конфискация криптовалюты, которая находится на них, возможна лишь в случае, если владелец кошелька сообщит шифр ключа правоохранительным органам либо его удастся установить иным способом. Так, иногда владельцы криптокошельков записывают ключи от них на бумажных / электронных носителях, которые сотрудники правоохранительных органов устанавливают при проведении обыска/выемки. Техническая возможность взлома криптокошелька при отказе подозреваемого/обвиняемого от сотрудничества в настоящее время лишь прорабатывается [4, с. 152–157].

К организационно-техническим аспектам изъятия следует отнести [3, с. 71–75]:

1. Создание кошелька следствия. Предпочтительнее использовать аппаратный кошелек (например, Tangem), как наиболее безопасный и изолированный вариант. Использование программных или бумажных кошельков нежелательно из-за рисков несанкционированного доступа.

2. Особенности перевода. Необходимо учитывать, что перевод возможен только в рамках одной сети и одного типа актива, за операцию взимается сетевой сбор, а время подтверждения зависит от загруженности сети.

3. Процессуальная фиксация. В протоколе осмотра детально отражаются: источник и способ доступа; данные об активах (адреса, вид, количество); стоимость (курс на момент изъятия); детали перевода (адрес получателя, комиссия); а после подтверждения - хэш транзакции и ее детали в обозревателе блокчейна.

4. Наложение ареста наиболее надежно осуществляется тем же переводом на подконтрольный адрес, что гарантирует сохранность актива. Альтернативой может служить запрет операций с уже изъятим адресом или блокировка аккаунта на бирже.

Таким образом, эффективное доказывание по делам о преступлениях с использованием криптовалют требует синтеза специальных технических знаний и классических процессуальных процедур. Успех зависит от системного применения инструментов OSINT и блокчейн-аналитики, оперативного взаимодействия с провайдерами услуг и грамотной фиксации цифровых следов для последующего изъятия криптоактивов.

Список источников

1. Поддубный И. В., Панферов Р. Г. Современные тенденции использования криптовалюты в противоправных целях // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. – 2024. – № 1(98). – С. 167–173.
2. Бессонов А. А. Информационные технологии в уголовно-правовой сфере / под ред. А. И. Бастрыкина, А. Н. Савенкова. – Москва: Юнити, Юнити-Дана, 2023. – 261 с.
3. Сбор и анализ цифровых следов преступления: практическое пособие / коллектив авторов (С. В. Петраков, Д. П. Бащук, А. А. Тимофеев и др.). – Москва: Проспект, 2023. – 75 с.
4. Тисен О. Н. Доказывание преступлений, совершенных с использованием криптовалют // Криминологический журнал. – 2023. – № 2. – С. 152–157. – URL: <https://doi.org/10.24412/2687-0185-2023-2-152-157> (дата обращения: 15.03.2024).

Информация об авторах

А.М. Кашапова - курсант 2 курса магистратуры

В.М. Черепков - курсант 2 курса магистратуры

Information about the authors:

A.M. Kashapova – 2nd-year master's student

V.M. Cherepkov – 2nd-year master's student