

Дата поступления рукописи в редакцию: 15.05.2026 г.
Дата принятия рукописи в печать: 25.06.2026 г.

DOI: 10.24412/2782-3849-2026-6-205-209

ПОСАШКОВ Антон Сергеевич,

заместитель командира взвода факультета подготовки дознавателей Бел ЮИ МВД России им. И.Д. Путилина,

e-mail: posashkov04@internet.ru

ВИНОКУРОВ Эдуард Александрович,

кандидат юридических наук, доцент, доцент кафедры уголовного процесса Бел ЮИ МВД России им. И.Д. Путилина,

e-mail: VinokurovEA@yandex.ru

ПРОЦЕССУАЛЬНЫЕ ОСОБЕННОСТИ ДОКАЗЫВАНИЯ ЭКОНОМИЧЕСКИХ ПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ КРИПТОАКТИВОВ

Аннотация. Эксперты в области обеспечения экономической безопасности и права обеспокоены растущим влиянием криптовалют на рынках. Основная проблема заключается в том, что нерегулируемый процесс майнинга создает каналы для неконтролируемого трансграничного движения денежных масс (капитала), что в определенный период может спровоцировать массовый отток средств из национальной экономики.

Поэтому, процесс расследования и доказывания данной категории преступлений осложняется особенностями: децентрализацией, анонимностью, отсутствием возможности отслеживания всех транзакций, трансграничным характером, сложностью возмещения причиненного вреда потерпевшим.

Для повышения эффективности процесса расследования авторы работы предлагают комплекс мер, в том числе и дополнения УПК РФ статьей 164.2, установив общий срок исполнения запросов органов предварительного расследования в 7 рабочих дней, а для уголовных дел с криптовалютой сократить до 48 часов. Инициатива поможет оперативнее собирать доказательства, формировать доказательственную базу и защищать права потерпевших.

Ключевые слова: цифровые следы, криптовалюты, майнинг, электронное доказательство, мошенничество, расследование преступлений, УПК РФ, носитель цифровых следов, компьютерная информация, информационно-телекоммуникационные технологии.

POSASHKOV Anton Sergeevich,

Deputy Platoon Commander, Investigator Training Department, Belgorod Law Institute of the Ministry of Internal Affairs of Russia Named After I.D. Putilin

VINOKUROV Eduard Aleksandrovich,

Candidate of Law, Associate Professor, Associate Professor of the Department of Criminal Procedure Belgorod Law Institute of the Ministry of Internal Affairs of Russia Named After I.D. Putilin

EVIDENCE-BASED CASES OF CRYPTOCURRENCY FRAUD: SUBSTITUTE ACCOUNT SCHEMES

Annotation. Experts in the field of economic security and law are concerned about the growing influence of cryptocurrencies on the markets. The main problem is that the unregulated mining process creates channels for the uncontrolled cross-border movement of money (capital), which in a certain period can provoke a massive outflow of funds from the national economy.

Therefore, the process of investigating and proving this category of crimes is complicated by the following features: decentralization, anonymity, lack of ability to track all transactions, cross-border nature, complexity of compensation for harm caused to victims.

To increase the effectiveness of the investigation process, the authors propose a set of measures, including supplementing the Criminal Procedure Code of the Russian Federation with Article 164.2, setting the total deadline for executing requests from preliminary investigation authorities at 7 working days, and reducing it to 48 hours for criminal cases involving cryptocurrencies. The initiative will help to collect evidence more quickly, form an evidence base and protect the rights of victims.

Key words: *digital traces, cryptocurrencies, mining, electronic evidence, fraud, crime investigation, Criminal Procedure Code of the Russian Federation, digital trace carrier, computer information, information and telecommunication technologies.*

Эксперты и ученые в области экономического права выражают серьезную озабоченность в связи с растущим влиянием криптовалют, особенно в странах с развивающимися рынками. Их внимание сосредоточено на явлении майнинга – процессе, при котором вычислительные мощности конвертируются в цифровые активы, потребляя при этом значительное количество электроэнергии. Нерегулируемая деятельность по добыче электронной валюты (криптовалюты) на международном уровне создает канал для трансграничного движения капитала, который сложно или практически невозможно отследить, а, следовательно, зачастую служит инструментом для совершения преступлений.

В период наступления кризиса или экономической нестабильности институт криптовалюты может привести к масштабному и неконтролируемому оттоку средств из национальной экономики, подрывая усилия властей по стабилизации ситуации. В ответ на данный вызов МВФ призывает уполномоченные органы уравнивать в правах мониторинга и контроля операции с криптовалютами и традиционные финансовые потоки.

В своем недавнем аналитическом отчете МВФ конкретизирует свои рекомендации. В них указывается, что существующие правовые рамки, регулирующие валютный контроль и движение капитала, требуют срочного пересмотра и модернизации. Официально признанные виды криптовалют должны быть законодательно включены в эти регуляторные системы, даже если их формальный статус (как финансового актива или иностранной валюты) остается предметом дискуссий.

Практическим следствием реализации такой политики может стать установление для граждан ограничений на покупку, владение и транзакции с биткоином, эфириумом и другими цифровыми валютами. Парадокс заключается в том, что ключевые признаки и технологическое преимущество криптовалют (децентрализация и высокий уровень анонимности транзакций) представляют главную правовую проблему. А.И. Савельев утверждает, что общественные отношения с криптовалютой усложняют

идентификацию виновных лиц и восстановление прав [1]. Отсутствие государственного регулирования и контроля значительно затрудняет процесс уголовного преследования, значительно осложняя доказывания и раскрытие преступлений данного вида.

В контексте уголовного процесса институт доказывания, составляющий основу и определяющий цель судопроизводства, представляет собой фундамент расследования. Доказывание – это сложная деятельность уполномоченных лиц, которая заключается в системном собирании, всесторонней проверке и объективной оценке доказательств на досудебных стадиях уголовного судопроизводства. Основные цели данного процесса: установление события преступления, изобличение виновных лиц, выявление сопутствующих обстоятельств и обстоятельств, подлежащих доказыванию. При расследовании преступлений, связанных с использованием криптовалют, органы предварительного расследования сталкиваются с уникальными проблемами правоприменительного характера. Первоочередной задачей, как и в иных видах преступлений, является фиксация самого события преступления. Однако специфика цифровых активов предопределяет необходимость глубокого изучения и установления конкретных способов их использования в противоправных целях.

В рамках проводимого анализа необходимо, и решения возникающих проблем необходимо раскрыть сущность процесса майнинга. Майнинг – это технологический процесс генерации новых единиц криптовалюты, осуществляемый мощными компьютерными системами (майнеры, ASIC) путем решения сложных криптографических задач (хеш-функций) [2].

Процесс физического обмена криптовалютой на наличные фиатные деньги представляет собой одно из наиболее уязвимых звеньев в системе транзакций и вывода цифровых активов и порождает широкий спектр преступлений. К ним относятся различные виды мошеннических схем (обман при курсовой разнице, продажа несуществующей

криптовалюты), вымогательство с требованием перевода средств в биткоинах, а также преступления против личности, совершаемые с целью завладения криптовалютными сбережениями. Чаще всего факт незаконной добычи криптовалют выявляют при проведении оперативно-розыскных мероприятий. Это связано с высокой латентностью экономических преступлений. Важно при этом отметить, что поводом к возбуждению уголовного дела служит, как правило рапорт, составленный должностным лицом, который осуществляет, как первоначальную проверку информации о совершенном преступлении, так и осуществляет сбор доказательств о механизме совершения преступления (способы хищения электроэнергии и т.д.). Решением ряда указанных задач, как правило выступают запросы в компанию по электроснабжению с целью выяснения динамики электропотребления по адресу, где было установлено оборудование, или по месту возможного расположения. При этом, следует учитывать технические характеристики устройств по добыче криптовалют, это обусловлено тем, что одна единица современного майнингового оборудования потребляет значительное количество энергии (от 2,5 кВт/ч и более), что при массовой установке приводит к заметным аномалиям в сетевой нагрузке

Ярким примером является приговор № 1-68/2025 от 27.04.2025[1]. Используя свое служебное положение, оператор энергокомпании обнаружил незаконную майнинг-ферму. Затем он ввел владельца в заблуждение, что штраф за незаконное потребление необходимо возместить ему, тем самым похитив денежную сумму размером 492 000 рублей путем злоупотребления доверием при оказании услуг. Данное преступление было выявлено сотрудниками оперативных подразделений при проверке сообщения о преступлении связанного с хищением электроэнергии. Отметим, что зачастую в рамках проверки сообщения о преступлении сотрудники правоохранительных органов, также выявляют и иные преступления.

Также поводом для возбуждения уголовных дел данной категории, являются заявления потерпевших (организации, выявившей факт незаконного подключения, сообщение от уполномоченной организации, обеспечивающее распределение электроэнергии между конечными потребителями). Сложность доказывания обуславливается анонимностью контрагентов, необходимостью отслеживания финансовых потоков, международным сотрудничеством и установлением ущерба от преступного деяния.

Основной процесс собирания доказательственной базы начинается на стадии

возбуждения уголовного дела в данной сфере и имеет свою специфику. Основными трудностями на данном этапе являются: определение ущерба и состава преступления, квалификация деяния проведения неотложных следственных действий.

Осмотр места происшествия в стадии возбуждения уголовного дела является одним из первоочередных и наиболее эффективных следственных действий с точки зрения формирования доказательственной базы. В ходе него уполномоченные лица правоохранительных органов и специалисты, как правило, обнаруживают и изымают специализированное оборудование для майнинга (криптофермы, ASIC), незаконно подключенное к электрической сети. Зачастую выявляются и силовые кабели, ведущие к распределительным подстанциям или сетям, которые были присоединены в обход приборов учета (электросчетчиков), что является фактом безучетного потребления.

Доказывание на стадии предварительного расследования сопряжено с рядом особенностей и сложностей:

Цифровые доказательства (переписки в сети интернет, скриншоты и доступ в личный кабинет криптовалютных бирж, транзакции на блокчейне);

Дефицит специалистов данного направления. При производстве следственных действий во избежание ошибок по фиксации доказательств необходима помощь специалиста;

Взаимодействие с криптобиржами и отделениями банков. Наиболее остро данная проблема проявляется при ответе на запрос следователя в рамках возбужденного уголовного дела и запрос уполномоченного лица в рамках проверки сообщения о преступлении. Срок исполнения в законодательстве запросов не ограничен, что ведет к злоупотреблениям со стороны финансовых организаций и нарушений сроков производства и принципа разумного срока;

Необходимость наличия специальных знаний у субъекта, осуществляющего предварительного расследования, с целью минимизации процессуальных ошибок и недопущению утраты доказательств.

Одним из наиболее распространенных и сложных для доказывания видов преступлений экономической направленности в цифровой среде является мошенничество, совершенное с использованием цифрового актива для инвестирования. Его специфика заключается в том, что подозреваемые используют высокий уровень общественного интереса и нередко недостаточную осведомленность потенциальных жертв о механизмах работы блокчейн-технологий.

Основной массив сообщений о преступлении в данной категории связан с привлечением инвестиций в рамках проекта ICO. Данная форма представляет собой выпуск цифровых активов, когда организаторы проекта привлекают средства граждан, предлагая им приобрести новые, специально выпущенные криптовалютные токены с потенциальным ростом в будущем. Инвесторам обещают исключительную доходность и рост стоимости токенов в будущем. Однако после сбора капитала проект внезапно прекращает свое существование, его сайты и каналы связи блокируются, а организаторы исчезают вместе с криптовалютными средствами вкладчиков.

К этому же виду относится и организация противоправной деятельности по систематическому привлечению денежных средств или иного имущества граждан под ложные обещания высокой прибыли от торговли на биржах криптовалют и иного цифрового актива, участия в якобы прибыльных майнинговых пулах или от так называемого облачного майнинга. Жертвам предлагают передать свои средства или криптоактивы в управление «профессионалам», гарантирующим регулярные выплаты, где доход первым вкладчикам выплачивается за счет средств последующих, до момента неизбежной остановки привлечения новых лиц.

Опасность и массовость данного вида мошенничества подчеркивается данными аналитиков. По информации международной компании в области кибербезопасности Group-IB, более половины привлеченных средств были похищены с использованием методов фишинга. Это означает, что помимо прямого обмана с несуществующего проекта, подозреваемые активно применяют технические средства, создавая копии официальных сайтов, рассылая поддельные письма от имени известных платформ и используя иные способы для получения доступа к приватным ключам и seed-фразам кошельков доверчивых инвесторов, что ведет к полной и безвозвратной утере их активов. Речь идет о дублировании официальных веб-сайтов криптобирж, обменных сервисов или кошельков, а также о публикации в официальных магазинах приложений, таких как GooglePlay и AppStore, мошеннических программ, маскирующихся под легитимные клиенты. В постановлении № 1-578/2025 группа лиц обвиняется в создании и управлении организованной преступной группой с целью хищения денежных средств граждан в особо крупном размере. Группа создала проект Yusra, позиционируя его как инновационную IT-компанию с высокодоходным продуктом, а на самом деле - финансовую пирамиду, не имеющую реальной экономической деятельности [2].

Несмотря на то, что модераторы данных площадок, в основном, оперативно удаляют подобный вредоносный контент, но в течение временного промежутка нахождения в доступе данного приложения оно скачивается значительным числом пользователей, доверяющих репутации магазина.

Эффективность данной схемы основана на эксплуатации типичных моделей поведения пользователей и невнимательности к деталям. Основными индикаторами мошеннического веб-ресурса являются отсутствие защищенного соединения: в адресной строке браузера не отображается значок замка и протокол «https», что свидетельствует о том, что передаваемые данные не шифруются. Другим распространенным методом является использование фишинговых ссылок, ведущих на сайты с адресами, почти идентичными настоящим. Зачастую пользователи попадают на такие страницы через автоматические редиректы с других сайтов или рекламных объявлений и ссылок, не утруждая себя ручной проверкой и вводом URL-адреса доверенного сервиса вручную. После ввода своих учетных данных в фальшивом приложении жертва напрямую передает злоумышленникам полный контроль над своими денежными средствами.

При этом схемы мошенничества постоянно эволюционируют, приобретая все более изощренные гибридные формы, сочетающие социальную инженерию с техническим манипулированием информационными потоками. Ученые также отмечают, что киберпреступники часто комбинируют различные каналы связи (социальные сети, мессенджеры, звонки) и зачастую используют многоканальные атаки. Ярким примером служит так называемая «челночная» афера, которая использует репутацию легальных офлайн-обменных пунктов для прикрытия мошеннических действий в цифровой среде[5].

Сущность указанного преступления, заключается в том, что подозреваемые создают фейковый аккаунт, имитирующий службу поддержки реального обменного сервиса, а жертва, желающая обменять наличные средства на криптовалюту, выходит на связь с мошенником, который назначает встречу в действующем офисе выбранной компании, персонал которой не осведомлен о готовящемся обмане. Во время следования жертвы к месту встречи и сделки, преступник, используя скопированный аватар и данные жертвы, от ее имени связывается с настоящим оператором обменника через официальный канал, дублируя условия и время встречи. В офисе сотрудник просит клиента для подтверждения сделки отправить в чат адрес своего криптокошелька для пробного перевода. Ввиду психологического восприятия ситуации как прямого контакта, жертва отправляет

не легальному сотруднику, а своему изначальному собеседнику пробный перевод, который преступник переводит оператору обменника. После клиент переводит всю сумму денежных средств, которые похищает преступник.

На основании проведенного исследования, мы приходим к выводу, что из-за сложности расследования и доказывания данного вида преступлений и ограниченных процессуальных сроков необходимо оптимизировать деятельность следователя.

Поэтому, необходимо организовывать и стимулировать к прохождению дополнительных курсов и повышению квалификации действующих сотрудников органов предварительного расследования

Также важной особенностью является частое привлечение специалистов к проведению следственных действий совместно со следователем или дознавателем. Мы предлагаем ввести процедуру обязательного привлечения специалиста при работе с компьютеризированной техникой.

Огромным препятствием при реализации принципа разумного срока уголовного судопроизводства является ответа на запрос сотрудников правоохранительных органов. Выходом из данной ситуации, является внесением соответствующих изменений в положение УПК РФ, в частности дополнения ст. 164.2 следующим содержанием «Сроки исполнения запросов следователя, руководителя следственного органа, дознавателя, органа дознания», где определить срок исполнения запроса до 7 рабочих дней с момента его получения. В рамках расследования преступлений, связанных с криптовалютой, данный запрос необходимо выполнить в течение 48 часов с момента его получения. Срочность выполнения данного процессуального действия необходима ввиду влияния на возможность возмещения ущерба потерпевшим.

В результате предложенные изменения определяют, что криптобиржи из пассивных наблюдателей или труднодоступных иностранных субъектов превращаются в активных и ответственных участников уголовного процесса. Данная новелла создает действенный инструмент для защиты прав потерпевших и повышает эффективность борьбы с преступлениями в сфере цифровых активов, переводя противодействие им с декларативного уровня на практический.

Предложенный комплекс мер направлен на улучшение процесса собирания доказательственной базы, обеспечения принципа разумного срока уголовного судопроизводства и минимизации ошибок при формировании доказательственной базы.

Список литературы:

[1] Янковский Р.М. Криптовалюты в российском праве: суррогаты, «иное имущество» и цифровые деньги

/ Р.М. Янковский // Российское право: состояние, перспективы, комментарии. — Москва, 2020. — С. 43–77.

[2] Зиняков К.Ю. Принципы работы технологии блокчейн и майнинга // КиберЛенинка: научная электронная библиотека. — URL: <https://cyberleninka.ru/article/n/mayning-kriptovalyuty-problemy-i-perspektivy/viewer> (дата обращения: 20.04.2026).

[3] Приговор Левашинского районного суда Республики Дагестан от 27 апреля 2025 г. по делу № 1-68/2025 // Судебные и нормативные акты РФ : сайт. — URL: <https://sudact.ru/regular/doc/JEDdRGDW0uojtxt> (дата обращения: 20.04.2026).

[4] Постановление Ленинского районного суда г. Махачкалы от 11 марта 2025 г. по делу № 1-158/2025 // Судебные и нормативные акты РФ : сайт. — URL: <https://sudact.ru/regular/doc/JEDdRGDW0uojtxt> (дата обращения: 20.04.2026).

[5] Зотина, Е. В. Претекстинг как приём социальной инженерии, используемый телефонными мошенниками: криминологический взгляд на проблему / Е. В. Зотина // Вестник Казанского юридического института МВД России. сайт. — URL: <https://vestnikkui.ru/ru/nauka/author/654816/view> — 2022. — Т. 13, № 4. — С. 1-7

References:

[1] Yankovsky R.M. Cryptocurrencies in Russian law: surrogates, “other property” and digital money / R.M. Yankovsky//Russian law: state, prospects, comments. - Moscow, 2020. - S. 43-77.

[2] Zinyakov K.Yu. Principles of blockchain and mining technology//CyberLeninka: scientific electronic library. — URL: <https://cyberleninka.ru/article/n/mayning-kriptovalyuty-problemy-i-perspektivy/viewer> (дата обращения: 20.04.2026).

[3] Verdict of the Levashinsky District Court of the Republic of Dagestan dated April 27, 2025 in case No. 1-68/2025//Judicial and regulatory acts of the Russian Federation: website. - URL: <https://sudact.ru/regular/doc/JEDdRGDW0uojtxt> (access date: 20.04.2026).

[4] Resolution of the Leninsky District Court of Makhachkala dated March 11, 2025 in case No. 1-158/2025//Judicial and regulatory acts of the Russian Federation: website. - URL: <https://sudact.ru/regular/doc/JEDdRGDW0uojtxt> (access date: 20.04.2026).

[5] Zotina, E.V. Pretexting as a social engineering technique used by telephone scammers: criminological view of the problem/E.V. Zotina//Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. site. — URL: <https://vestnikkui.ru/ru/nauka/author/654816/view> — 2022. - T. 13, NO. 4. - S. 1-7