

DOI: <http://dx.doi.org/10.21686/2411-118X-2026-1-88-93>

Криминалистический анализ цифровых следов в блокчейне: методология верификации для уголовного процесса

А. Г. Соломатина

кандидат юридических наук, доцент,
доцент кафедры противодействия преступлениям
в сфере информационно-телекоммуникационных технологий
Московского университета МВД России им. В. Я. Кикотя;
доцент кафедры международного и публичного права
Финансового университета при Правительстве Российской Федерации.
Адрес: ФГКОУ ВО «Московский университет
Министерства внутренних дел Российской Федерации имени В. Я. Кикотя»,
117437, Москва, Академика Волгина ул., д. 12;
ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации»,
125167, Москва, ул. Ленинградский проспект, д. 49/2.
E-mail: a.smorodina@mail.ru

Forensic Analysis of Digital Traces in Blockchain: Verification Methodology for Criminal Proceedings

A. G. Solomatina

PhD in Law, Associate Professor, Associate Professor of the Department
of Combating Crimes in the Field of Information and Telecommunication Technologies
of Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikot;
Associate Professor of the Department of International and Public Law
of Financial University under the Government of the Russian Federation.
Address: Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikot,
12 Academic Volgin Str., Moscow, 117437, Russian Federation;
Federal State-Funded Educational Institution of Higher Education
“Financial University under the Government of the Russian Federation”,
49/2 Leningradskiy Ave., Moscow, 125167, Russian Federation.
E-mail: a.smorodina@mail.ru

Поступила 25.12.2025 Принята к печати 10.01.2026

Аннотация

Статья посвящена разработке комплексной методологии криминалистического анализа цифровых следов в блокчейне для их использования в уголовном процессе. Авторы предлагают многоуровневую модель, которая интегрирует этапы верификации блокчейн-данных, поведенческой кластеризации адресов, графового анализа потоков активов, сигнатурного выявления аномалий и деанонимизации псевдонимных идентификаторов. Практическая значимость подхода подтверждена на примерах реальных уголовных дел, расследуемых ГУЭБиПК МВД России, включая схемы вишинга и отмыwania средств через криптообменники вроде Suex и BTC-e. Сформулированы строгие критерии допустимости таких следов как доказательств в соответствии со статьями 75, 80, 86 Уголовно-процессуального кодекса Российской Федерации. Особое внимание уделено первичной экстракции данных через полные узлы или API-эксплореры с перекрестной верификацией, преодолению псевдонимности отечественных платформ («Прозрачный блокчейн», «ШАРД») и конвергенции с внешними источниками (VASP по Travel Rule FATF). Результаты формируют научно-методическую основу для органов предварительного расследования и финансового мониторинга.

Ключевые слова: блокчейн-криминалистика, цифровые следы, доказывание, криминалистическая идентификация, кластеризация блокчейн-адресов, графовый анализ транзакций, деанонимизация, электронные доказательства, допустимость доказательств, верификация данных.

Abstract

The article is devoted to the development of a comprehensive methodology for forensic analysis of digital traces in the blockchain for their use in criminal proceedings. The authors propose a multi-level model that integrates the stages of blockchain data verification, behavioral clustering of addresses, graph analysis of asset flows, signature detection of anomalies, and de-anonymization of pseudonymous identifiers. The practical significance of the approach is confirmed by examples of real criminal cases investigated by the Main Directorate for Economic Security and Anti-Money Laundering of the Ministry of Internal Affairs of the Russian Federation, including schemes of vishing and money laundering through crypto exchanges such as Suex and BTC-e. Strict criteria for the admissibility of such traces as evidence have been formulated in accordance with Articles 75, 80, and 86 of the Code of Criminal Procedure of the Russian Federation. Special attention has been paid to the primary extraction of data through full nodes or API explorers with cross-verification, overcoming pseudonymity via domestic platforms (Transparent Blockchain, SHARD), and convergence with external sources (VASP according to the FATF Travel Rule). The results form a scientific and methodological basis for preliminary investigation and financial monitoring bodies.

Keywords: blockchain forensics, digital traces, proof, forensic identification, blockchain address clustering, transaction graph analysis, deanonymization, electronic evidence, admissibility of evidence, data verification.

Стремительная цифровизация экономических отношений, сопровождающаяся внедрением децентрализованных реестров, детерминировала возникновение качественно нового класса цифровых следов. Их правовая природа и доказательственное значение остаются дискуссионными как в рамках теории доказывания, так и в правоприменительной практике. Блокчейн-транзакции, представляя собой криптографически защищенные записи, объективно совмещают атрибуты публичной доступности с псевдонимностью участвующих субъектов [7]. Данное обстоятельство ставит под вопрос прямую применимость традиционных криминалистических методов, ориентированных на централизованные системы хранения информации и материальные носители. Высокая степень стандартизации протоколов ведущих публичных блокчейн-сетей (Bitcoin, Ethereum и их форков) создает предпосылки для формализации строгой, научно обоснованной методологии анализа и процессуальной верификации соответствующих цифровых следов [6].

Отечественное уголовно-процессуальное законодательство не содержит специальных норм, регламентирующих порядок собирания, проверки и оценки данных распределенных реестров в качестве источников доказательств. Существующие научные подходы [1] зачастую либо ограничиваются общими положениями цифровой криминалистики, либо фокусируются на частных технико-криптографических особенностях вне системной связи с критериями допустимости доказательств, установленными нормами Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ). Вместе с тем правопримени-

тельная практика требует разработки четких оснований для признания легитимными таких цифровых данных, как записи криптовалютных кошельков, отчеты блок-эксплореров, кластерные модели владения адресами и графовые схемы движения средств. Актуальность разработки методологии подчеркивается ростом числа преступлений, связанных с криптоактивами, в России начиная от крупных международных дел, таких как расследование деятельности биржи BTC-e/WEX и Александра Винника, до внутренних расследований вишинга и кибермошенничеств, где криптовалюты используются для финального обналичивания средств [3]. Таким образом, формируется ключевая научная проблема: каковы методологические и процессуальные основания, позволяющие рассматривать результаты блокчейн-анализа в качестве достоверных, верифицируемых, воспроизводимых и соответствующих фундаментальным принципам доказательственного права?

Под цифровым следом в блокчейн-среде понимается формализованная совокупность структурированных данных, отражающих факт, условия и результат совершения юридически значимых действий в распределенном реестре. Эта совокупность может быть объективно выявлена, зафиксирована, исследована и интерпретирована с применением специальных криминалистических и технических познаний. Блокчейн-транзакция, содержащая детерминированные поля (хеши предыдущих выходов, публичные ключи получателей, суммы, временные метки, цифровые подписи), полностью соответствует указанным критериям. Однако имманентные свойства распределенного реестра – децентра-

лизация, неизменяемость и криптографическая целостность – формируют новые квалифицирующие признаки: отсутствие единого администратора данных и техническая невозможность уничтожения или модификации записи без получения контроля над большинством хешрейта сети [6]. В этой связи классические следственные действия по изъятию материальных носителей (ст. 164, 176 УПК РФ) подлежат трансформации в процедуры «логико-криптографической фиксации», фокусирующиеся на доказательном закреплении конкретных криптографических хешей, временных интервалов доступа и состояния реестра.

Методологический каркас блокчейн-криминалистики как прикладного направления криминалистической техники образует синтез следующих методов: криптографическое восстановление – проверка подлинности цепочек транзакций путем верификации цифровых подписей и хеш-связей (доказательства по Мерклу, упрощенная верификация платежей); поведенческая кластеризация – группировка адресов по признакам вероятного единого владельца на основании закономерностей использования (общие входы, адреса сдачи, цепочки последовательных переводов) с применением методов машинного обучения; сетевое моделирование – реконструкция и анализ направленного мультиграфа движения активов для выявления ключевых узлов и маршрутов; сигнатурно-статистический анализ – выявление аномалий и криминалистически значимых закономерностей (сервисы смешивания, атаки пылевыми транзакциями, круговые переводы) на основе эталонных моделей; внешняя корреляция – установление вероятной связи псевдонимных идентификаторов с реальными субъектами путем сопоставления с данными из регулируемых внеблочных источников (криптовалютные биржи, фиатные платежные шлюзы, интернет-сервисы).

Реализация указанных методов предполагает наличие надлежащей эмпирической базы, что обуславливает первостепенное значение процедуры первичного извлечения данных.

Первый этап следует обозначить как экстракцию ончейн-данных (on-chain data) и обеспечение криптографической цепочки сохранности. Этот этап является исходной точкой и эквивалентен первоначальному изъятию и фиксации вещественных доказательств в уголовном судопроизводстве. Его целью является получение из блокчейн-сети точной, неизменной и верифицируе-

мой копии цифровых данных (транзакций), пригодной для последующего экспертного исследования и приобщения к материалам уголовного дела, а главной задачей – технически и процессуально гарантировать, что полученные данные подлинны, не подвергались манипуляциям, поскольку любое нарушение целостности исходного массива делает последующую верификацию транзакций, построение поведенческих паттернов и корреляционный анализ юридически недопустимыми.

Процедура включает два ключевых компонента: получение данных и обеспечение их достоверности. Данные извлекаются из публичного распределенного реестра двумя способами, выбор которых определяется требуемой степенью автономности и доказательственной значимостью. Первый способ – через программный интерфейс (API) публичных обозревателей блоков (Blockchair, Etherscan), что оперативно, но создает зависимость от потенциально уязвимого стороннего сервиса. Второй способ – запуск и синхронизация полного узла сети (например, Bitcoin Core, Geth), являющегося «золотым стандартом», поскольку обеспечивает независимую полную копию блокчейна и исключает риски, связанные с доверием третьим лицам. Для подтверждения подлинности извлеченной информации, учитывая возможность технических сбоев или целенаправленных воздействий даже на авторитетные источники, применяется принцип перекрестной верификации.

Следующим этапом следует установление единства контроля и идентификация владельцев, направленный на преодоление ключевого свойства блокчейна – псевдонимности. Цель этапа – установить вероятную принадлежность множества разрозненных адресов (публичных ключей) единому контролирующему субъекту (кошельку, сервису, преступной группе), преобразуя тем самым анонимные идентификаторы в значимые для расследования сущности. Практическое значение данного этапа ярко иллюстрируется в расследовании деятельности криптообменной платформы Suex (OTCbro). Аналитики, используя методы кластеризации, смогли сформировать устойчивые кластеры адресов, связанных с платформой, и впоследствии доказать, что более 40% ее транзакций были связаны с незаконными операциями, и это послужило основанием для

введения против нее санкций Министерством финансов США¹. Блокчейн-аналитики компании Chainalysis, чьи данные использовались в этом расследовании, отмечали, что именно кластеризация позволила выявить масштаб и паттерны взаимодействия Suex с хакерскими группами².

Аналогичный подход применяется в России с использованием отечественных сервисов. Сервис Росфинмониторинга «Прозрачный блокчейн» позволяет кластеризовать адреса по более чем 30 криптоактивам, выявляя подозрительные кластеры, связанные с отмытием средств от наркоторговли и других преступлений. В 2025 г. завершен пилотный проект с пятью банками для интеграции в антиотмывочную систему³. Платформа «ШАРД» реализует кластеризацию через графы связей для деанонимизации адресов мошенников, определения путей вывода средств на биржи и холодные кошельки, что упрощает подготовку запросов в полицию и сервисы для заморозки активов⁴.

Третьим этапом служит графовый анализ потоков активов и идентификация аномальных структур. Он необходим для системного исследования взаимодействий между установленными на предыдущем шаге субъектами (адресами и кластерами). Его цель – выявление структуры финансовых потоков, обнаружение ключевых точек концентрации и распределения активов, а также распознавание паттернов, характерных для легальных экономических операций и противоправной деятельности. В расследовании дела вишинг-банды, действующей в России, сотрудники ГУЭБиПК МВД России и эксперты Росфинмониторинга построили детальную схему движения средств (граф), которая позволила выявить аккаунты на P2P-площадках, через которые проходил основной объем конвертации украденных фиатных средств в криптовалюту и обратно. Этот графовый

анализ стал ключом к пониманию архитектуры всей преступной схемы. Ниже наглядно представлены входящие в него процессы.

Построение и формализация модели потоков моделирует всю транзакционную активность в виде ориентированного взвешенного мультиграфа $G=(V, E)$, где:

- V (вершины) – множество адресов или кластеров адресов, представляющих единых контролируемых субъектов;

- E (ребра) – множество транзакций между вершинами. Каждое ребро обладает направлением (от отправителя к получателю) и весом, соответствующим сумме перевода. Визуализация такого графа создает интуитивно понятную карту движения средств, на которой явно видны основные пути, источники и стоки активов.

Далее следует количественный анализ топологии графа на основе аппарата сетевого анализа для объективной идентификации наиболее значимых узлов в целях расчета ключевых метрик, позволяющих количественно охарактеризовать структурную роль вершин. Завершает процесс сигнатурный анализ, который фокусируется на обнаружении аномальных и подозрительных паттернов, служащих маркерами попыток маскировки следов или иной нелегальной активности. Это дополняет структурный анализ графа, усиливая способность выявлять скрытые стратегии противодействия.

Таким образом, графовый анализ трансформирует линейную последовательность транзакций в структурную модель, поддающуюся как количественному измерению, так и качественному анализу. Он позволяет перейти от наблюдения за отдельными операциями к пониманию логики и архитектуры всей финансовой схемы, будь то легальный бизнес-процесс или многоуровневая система отмыкания средств.

Четвертый этап – сигнатурный и статистический анализ транзакционных паттернов – направлен на переход от структурного анализа связей к семантическому анализу поведения. Его цель – выявить не просто связи между субъектами, а характерные поведенческие шаблоны (сигнатуры), которые статистически коррелируют с противоправной деятельностью, что достигается за счет синтеза экспертного (сигнатурного) и машинного (статистического) подходов. Библиотека сигнатур формируется в том числе на основе анализа реальных дел, рассматриваемых Росфинмониторингом, что обеспечивает ее практическую релевантность для российских правоохранительных органов.

¹ U.S. Department of the Treasury. Treasury Sanctions Russia-Based Cryptocurrency Exchange Suex for Facilitating Financial Transactions for Ransomware Actors. 2021, Sent. 21. – URL: <https://home.treasury.gov/news/press-releases/jy0426>

² Chainalysis. Suex (OTCbro) Investigation Summary. 2021, Sent. 16. – URL: <https://go.chainalysis.com/suex-otcbro-investigation-summary.html>

³ Росфинмониторинг завершил апробацию сервиса по отслеживанию криптовалют для банков // Федеральная служба по финансовому мониторингу. 2025, 28 дек. – URL: <https://www.fedsfm.ru/news/9441>

⁴ Практические аспекты криптовалютных расследований // Платформа Shard. 2022, 31 окт. – URL: https://shard.ru/article/practical_aspects_of_cryptocurrency_investigations

Кульминацией аналитического процесса выступает этап деанонимизации – финальная стадия, нацеленная на установление реальной личности, стоящей за псевдонимом блокчейн-адреса или кластера. Эта процедура, основанная на вероятностях и доказательствах, объединяет данные из блокчейна со сведениями из внешних источников, получая надежную доказательственную основу в рамках российского и международного законодательства. Среди признанных легитимных методов деанонимизации первостепенное место занимает запрос сведений у регулируемых провайдеров виртуальных активов (VASP). В соответствии с рекомендациями Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ) – в частности, Рекомендацией 16 «Электронные переводы средств» (также известной как «Правило поездки», или *Travel Rule*) – операторы криптовалютных бирж и аналогичных сервисов обязаны внедрять процедуры идентификации клиентов («Знай своего клиента») и сохранять идентификационные данные клиентов¹. Правоохранительные органы, в свою очередь, инициируют официальные запросы через механизмы международного сотрудничества и в соответствии с нормами УПК РФ, требуя раскрытия владельца адреса, временных меток операций, IP-адресов и связанных банковских счетов.

Дополнительно применяется корреляционный анализ цифровых следов и временных сигнатур, позволяющий сопоставить таймстампы блокчейн-транзакций с параллельными следами активности подозреваемого – логами входов в онлайн-аккаунты (форумы, мессенджеры, электронный адрес), IP-адресами и сессионными идентификаторами (cookies) при управлении кошельком через веб-интерфейсы, а также публикациями под устойчивыми псевдонимами, эхом отзывающимися на обсуждаемые операции. Точная синхронизация временных окон порождает косвенные, но убедительные доказательства идентичности субъекта.

Сопоставление с традиционными финансовыми потоками приобретает решающее значение

в уголовно-процессуальном доказывании в точке конвертации между фиатом и криптоактивами. Здесь тщательно изучаются банковские выписки, фиксирующие переводы на счета известных криптобирж или ОТС-платформ. Установив по материалам биржи конкретный криптоадрес, на который зачислены приобретенные средства, и соотнеся его с данными о владельце фиатного счета из банка, следователь обретает прямое доказательство цепочки «физическое лицо → блокчейн-адрес».

Критерий доказанности связи опирается на принцип конвергенции доказательств. Для минимизации ошибок и формирования убедительной доказательственной базы установление личности считается достоверным при выполнении принципа трех независимых источников. Личность считается установленной, когда одна и та же связь (например, «адрес 1ABC... принадлежит гражданину И.») подтверждается из трех или более независимых каналов, не вытекающих один из другого, например: сведения идентификационной проверки с биржи, журналы регистрации операторов связи, показания свидетеля или данные изъятой переписки. Это исключает случайные совпадения и формирует устойчивую систему доказательств [1].

Заключительным этапом является фиксация и процессуальное оформление доказательств блокчейн-анализа. В структуру процедурного протокола входят две ключевые операции: 1) криптографическая фиксация и 2) временное анкерование (в порядке, установленном приказом Минцифры России от 06.11.2020 № 580²), завершающиеся оформлением финального отчета (рекомендуемый формат – PDF/A-2u в соответствии с ГОСТ Р ИСО 19005-2-2013³). Криптографическая фиксация – вычисление уникального цифрового отпечатка для всего массива данных и отчета посредством стойких алгоритмов хеширования, обнаруживающего любое вмешательство в содержимое и делающего подлог технически невозможным.

¹ Рекомендации Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ) по борьбе с отмыванием денег и финансированием терроризма (с изменениями 2023 г.). Рекомендация 16 «Переводы средств» («Правило поездки»). Париж, FATF, 2019 (обновлено 2023). – URL: <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>

² Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 6 ноября 2020 г. № 580 «Об утверждении порядка создания и проверки метки доверенного времени» // Собрание законодательства Российской Федерации. – 2020. – № 46. – Ст. 7266.

³ ГОСТ Р ИСО 19005-2-2013. Системы управления документацией. Формат файлов электронных документов для долгосрочного хранения. Часть 2. Применение ИСО 32000-1 (PDF 1.7). – М., Стандартинформ, 2015.

можным. Результат криптографической фиксации обязательно документируется в протоколе. Временное анкерование – направление цифрового отпечатка в аккредитованную службу доверенных меток времени (согласно рекомендациям упомянутого приказа Минцифры), которая возвращает криптографический сертификат, удостоверяющий момент предъявления отпечатка по всемирному координированному времени. Финальный отчет составляется в формате, обеспечивающем долговременное сохранение и неизменность представления электронного документа (рекомендуется применение упомянутого формата PDF/A-2u). Документ заверяется усиленной квалифицированной электронной подписью ответственного исполнителя (следователя, эксперта), что в соответствии с частью 1 статьи 6 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» [1] придает ему юридическую силу, равнозначную документу на бумажном носителе, подписанному собственноручной подписью и скрепленному печатью.

Результаты анализа обретают силу уголовно-процессуального доказательства только при неукоснительном соблюдении уголовно-процессуальной формы и протокола, гарантиру-

ющем их целостность, аутентичность, неизменность и юридическую значимость.

Наконец, все материалы – отчеты, сырые данные, хеши, сертификаты – переносятся на новый чистый носитель информации (флеш-накопитель или диск), снабжаются этикеткой по ГОСТ Р 7.0.8-2013 и приобщаются к материалам уголовного дела в соответствии со статьями 81, 84, 166 УПК РФ, обретая статус вещественного доказательства.

Подводя итог, следует сделать вывод, что предложенная многоуровневая криминалистическая методология решает фундаментальную задачу процессуального освоения блокчейн-данных, обеспечивая научную обоснованность, воспроизводимость и юридическую неуязвимость результата. Каждый этап формализован для идентичной репликации результатов; система перекрестных верификаций, криптографической защиты и конвергенции источников создает монолитную доказательственную цепь. Все процедуры – от извлечения данных до оформления протокола – разработаны с учетом критериев допустимости доказательств, установленных статьями 75, 80, 86 УПК РФ.

Список литературы

1. Борисов А. С. Совершенствование уголовно-процессуального режима обращения информации в досудебном производстве // Вестник Пермского университета. Юридические науки. – 2023. – № 2. – С. 195–215.
2. Крылов Г. О., Токолов А. В. Разработки ФАТФ для провайдеров услуг виртуальных активов // Вестник Московского университета МВД России. – 2020. – № 8. – С. 197–200.
3. Лемайкина С. В. Актуальные вопросы установления личности, использующей криптовалюту в преступных целях // Юрист — Правоведъ. – 2021. – № 3 (98). – С. 213–218.
4. Любый И. А., Сидоренко Р. В. Расследование преступлений, связанных с криптовалютой: правовые инструменты и эффективность их применения // Российский следователь. – 2025. – № 10. – С. 9–13.
5. Пушкарев В. В., Токолов А. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют // Вестник экономической безопасности. – 2023. – № 4. – С. 88–92.
6. Токолов А. В. Блокчейн как инструмент в борьбе за искоренение коррупции // Вестник Академии Следственного комитета Российской Федерации. – 2020. – № 3 (25). – С. 155–157.
7. Токолов А. В., Морозов А. В. Особенности правового регулирования технологии блокчейн // Вестник Московского университета МВД России. – 2020. – № 1. – С. 149–151.