Дата поступления рукописи в редакцию: 02.10.2026 г. DOI: 10.24412/2224-9133-2026-10-601-608
Дата принятия рукописи в печать: 10.11.2026 г.

ОЛЬМЕЗОВ Якуб Тахирович,
ассистент, Кабардино-Балкарский государственный университет им. Х.М. Бербекова, Российская Федерация, г. Нальчик, ассистент кафедры гражданского права и процесса Института права, экономики и финансов, ORCID: 0009-0007-0613-6960, e-mail: yakub.bayzik@mail.ru

ЗУМАКУЛОВА Зарема Ахматовна,
кандидат юридических наук, доцент, Кабардино-Балкарский государственный университет им. Х.М. Бербекова, Российская Федерация, г. Нальчик, заведующая кафедрой гражданского права и процесса Института права, экономики и финансов, ORCID: 0009-0000-8480-6527, e-mail: zarema.zum@mail.ru

ЖУГОВ Азамат Аскерович,
кандидат юридических наук, доцент, Кабардино-Балкарский государственный университет им. Х.М. Бербекова, Российская Федерация, г. Нальчик, доцент кафедры гражданского права и процесса Института права, экономики и финансов, ORCID: 0000-0003-3333-3963, e-mail: zhugov@mail.ru

КРИПТОВАЛЮТА В ЦИФРОВЫХ ФИНАНСОВЫХ ПИРАМИДАХ: КРИТЕРИИ КВАЛИФИКАЦИИ

Аннотация. *Введение. Использование цифровой валюты в схемах привлечения средств ставит перед правоприменителем сложную задачу: необходимо разграничить финансовую пирамиду, мошенничество, манипулятивную торговлю и обычный инвестиционный риск. Сама технологическая форма актива ответа не дает — она не раскрывает ни экономического источника выплат, ни направленности умысла организаторов. Методы. В ходе исследования нами применены формально-юридический, системный, функциональный и экономико-правовой методы. Нормативный материал изучен по состоянию на 18 сентября 2026 г.; для аналитической апробации использованы российский уголовно-правовой материал, позиция Конституционного Суда Российской Федерации, материалы уголовного преследования Forsage и результаты эмпирических исследований криптовалютных злоупотреблений. Результаты. Нами предложен трехэтапный функциональный тест, предусматривающий последовательную проверку экономической модели движения стоимости, коммуникационной модели привлечения участников и доказательственного контура, связывающего цифровые адреса с конкретными лицами. Установлено, что применение статьи 172.2 УК РФ требует доказать выплаты прежним участникам за счет последующих при отсутствии сопоставимой законной деятельности. Rug pull, напротив, предполагает самостоятельную проверку признаков мошенничества, тогда как pump-and-dump не может автоматически квалифицироваться как финансовая пирамида. Обоснована необходимость раздельной оценки on-chain и off-chain данных, а также уточнения антиманипуляционного регулирования применительно к цифровым валютам.*

Ключевые слова: *цифровая валюта; финансовая пирамида; мошенничество; квалификация преступлений; блокчейн; цифровые доказательства; манипулирование рынком.*

Для цитирования: *Ольмезов Я. Т., Зумакулова З. А., Жугов А. А. Криптовалюта в цифровых финансовых пирамидах: критерии квалификации // Право и управление. 2026. № 10. С. 601–608.*

OLMEZOV Yakub T.,
Assistant, Kabardino-Balkarian State University named after H.M. Berbekov, Nalchik, Russian Federation Assistant Lecturer, Department of Civil Law and Procedure, Institute of Law, Economics and Finance

ZUMAKULOVA Zarema A.,
Candidate of Law, Associate Professor, Kabardino-Balkarian State University named after H.M. Berbekov, Nalchik, Russian Federation Head, Department of Civil Law and Procedure, Institute of Law, Economics and Finance

ZHUGOV Azamat A.,
Candidate of Law, Associate Professor, Kabardino-Balkarian State University named after H.M. Berbekov, Nalchik, Russian Federation Associate Professor, Department of Civil Law and Procedure, Institute of Law, Economics and Finance

CRYPTOCURRENCY IN DIGITAL FINANCIAL PYRAMIDS: CRITERIA FOR LEGAL CLASSIFICATION

Annotation. *Introduction. The use of digital currency in fundraising schemes creates a difficult classification problem: financial pyramids, fraud, manipulative trading, and ordinary investment risk must be distinguished without treating the technological form of the asset as determinative. Technology alone reveals neither the economic source of returns nor the organisers' intent. Methods. We employ formal legal, systemic, functional, and law-and-economics methods. Russian legislation was analysed as in force on 18 September 2026. The analytical pilot application draws on a Russian criminal-law case, a Constitutional Court position, Forsage prosecution materials, and empirical studies of cryptocurrency abuse. Results. We propose a three-stage functional test that sequentially examines the economic model of value flows, the communication model used to attract participants, and the evidentiary framework linking digital addresses to specific persons. Our analysis shows that Article 172.2 of the Russian Criminal Code requires proof that benefits to earlier participants are funded by later participants in the absence of comparable lawful activity. A rug pull requires a separate fraud analysis, whereas a pump-and-dump scheme should not automatically be treated as a financial pyramid. We also substantiate the need to distinguish on-chain from off-chain evidence and to clarify market-manipulation rules as applied to digital currencies.*

Key words: *digital currency; financial pyramid; fraud; criminal-law classification; blockchain; digital evidence; market manipulation.*

For citation: *Olmezov Ya. T., Zumakulova Z. A., Zhugov A. A. Cryptocurrency in digital financial pyramids: criteria for legal classification. Law and administration. 2026;(10):601–608. (In Russ.).*

Введение

Криптовалюта сама по себе финансовой пирамидой не является. Мы исходим из иной посылки: цифровая валюта — это технологический, особый имущественный инструмент, который может обслуживать как правомерный оборот, так и преступное привлечение денежных средств. Отождествление этих явлений методологически неверно. В одном случае обычный рыночный риск, присущий привычному рынку ценных бумаг, начинает восприниматься как преступление; в другом — организатор противоправной схемы получает удобную возможность скрыть ее экономическую сущность за терминологией токеномии, майнинга, стейкинга или децентрализованных финансов.

Практический масштаб проблемы подтверждается данными Банка России: в 2025 г. регулятор выявил 3 562 субъекта с признаками финан-

совых пирамид, причем значительная часть таких проектов действовала в сети Интернет и принимала цифровую валюту. Эти сведения приведены Банком России в материалах «Противодействие нелегальной деятельности на финансовом рынке. Результаты за 2025 год». Показатели характеризуют превентивно выявленные признаки, а не число вступивших в силу обвинительных приговоров. Для уголовно-правового исследования принципиально иное: цифровая среда делает привычные пирамидальные механизмы быстрее, трансграничнее и технически сложнее для атрибуции, но не изменяет нормативные признаки составов преступлений.

Российские научные труды раскрывают как экономические основания устойчивости финансовых пирамид [1, с. 22–38], так и уголовно-правовые проблемы криптовалютных схем. М.М. Долгиева рассматривает ответственность за криптовалютные пирамиды [2, с. 63–68], А.Ю. Сердюк — признаки состава статьи 172.2 УК РФ [3, с. 17–20], З.Г. Алиев, В.А. Швырёва и А.В. Разин — криптовалюту как предмет мошенничества и проблемы доказывания [4, с. 2–7]. Правовую природу криптовалюты и меры противодействия соответствующим пирамидам исследуют Р.М. Янковский [5, с. 43–77] и С.В. Мурадян [6, с. 93–104].

Зарубежные работы преимущественно сосредоточены на технической архитектуре злоупотреблений. Исследованы понци-механизмы в Ethereum [7, p. 259–277], экосистема Bitcoin Ponzi [8, p. 101–112] и типология криптовалютных мошеннических практик [9, p. 148353–148373]. Pump-and-dump анализируется в работах A. Dhawan и T.J. Putniņš [10, p. 935–975], J.T. Hamrick и соавторов [11], J. Kamps и B. Kleinberg [12], а технические признаки scam-токенов и rug pull — в исследованиях P. Xia и соавторов [13], B. Mazorra, V. Adan и V. Daza [14], M.H. Nguyen и соавторов [15]. Однако технический индикатор сам по себе не определяет уголовно-правовую квалификацию.

Цель и задачи исследования

Цель работы — объединить анализ движения стоимости, содержания публичных обещаний и цифровых доказательств в последовательный алгоритм разграничения финансовой пирамиды, мошенничества, манипулятивной торговли и законного высокорискового проекта. Для достижения цели поставлены задачи: определить юридически значимые признаки экономической и коммуникационной моделей цифровой схемы; соотнести их с признаками статей 159, 172.2 и 185.3 УК РФ; сформировать доказательственный контур, связывающий цифровые действия с конкретным лицом и умыслом; апробировать предложенный алгоритм на контрастных материалах российской и зарубежной практики. Рабочая гипотеза состоит в том, что квалификация должна определяться фактической моделью движения стоимости, способом формирования ожиданий участников и доказанным содержанием умысла, а не названием цифрового продукта.

Методы

Нормативный массив исследован по состоянию на 18 сентября 2026 г. В него включены Федеральный закон от 4 августа 2026 г. № 282-ФЗ «О цифровых валютах и цифровых правах», Федеральный закон от 4 августа 2026 г. № 283-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу законодательных актов (отдельных положений законодательных актов) Российской Федерации», уголовное и административное законодательство, законодательство о противодействии манипулированию рынком, рекламе и легализации преступных доходов, а также Федеральный закон от 20 февраля 2026 г. № 38-ФЗ, изменивший уголовное и уголовно-процессуальное регулирование цифровой валюты. Учтены Постановление Конституционного Суда Российской Федерации от 20 января 2026 г. № 2-П, Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» и материалы Банка России.

Формально-юридический метод мы использовали для сопоставления признаков статей 159, 172.2 и 185.3 УК РФ и смежных административных составов. Системный анализ позволил соотнести эти нормы с новым режимом цифровой валюты. Функциональный подход мы использовали для установления фактического назначения операции, не ограничиваясь ее техническим наименованием, также экономико-правовой анализ был сосредоточен на источнике дохода участника и устойчивости самой модели.

Постановка исследовательской проблемы, анализ нормативного материала, интерпретация источников, научные выводы и ответственность за содержание статьи принадлежат авторам.

Результаты

С 1 сентября 2026 г. базовый специальный режим цифровой валюты задает Федеральный закон № 282-ФЗ. Законодатель отделяет цифровую валюту от цифровых финансовых активов и допускает ее обращение в установленных законом пределах. Для уголовно-правовой квалификации это имеет прямое практическое значение: наличие криптовалютного адреса, факт обмена или высокая волатильность не свидетельствуют сами по себе о пирамидальной природе проекта. Мы полагаем, что отправной точкой должен оставаться способ привлечения и последующего перерас-

пределения имущественной стоимости.

Статья 172.2 УК РФ связывает финансовую пирамиду с привлечением денежных средств или иного имущества, когда выгода ранее привлеченным лицам предоставляется за счет последующих участников при отсутствии сопоставимой законной деятельности. Цифровая валюта может выступать «иным имуществом», вкладом и средством выплаты. Смарт-контракт меняет технику исполнения, но не источник дохода: программное перераспределение новых поступлений между прежними участниками не выводит схему за пределы статьи 172.2 УК РФ.

Rug pull имеет иную конструкцию: создатель токена может контролировать выпуск, функции контракта или ликвидность, а затем вывести ликвидность, увеличить эмиссию либо ограничить продажу. Технические признаки таких практик описаны в исследованиях [13–15], однако для уголовно-правового вывода необходимы данные о моменте возникновения умысла, сообщениях участникам, фактическом контроле и направлении полученной стоимости. Если намерение обратить имущество в пользу виновного существовало при привлечении средств и реализовывалось посредством обмана или злоупотребления доверием, проверке подлежит статья 159 УК РФ. Падение цены или неудача проекта сами по себе такого умысла не доказывают.

Pump-and-dump также не тождествен финансовой пирамиде. Организатор обычно заранее приобретает низколиквидный актив, создает искусственный ажиотаж координированными сообщениями и сделками, а затем продает позицию вошедшим на пике покупателям; повторяемость таких аномалий подтверждается эмпирическими исследованиями [10–12]. При отсутствии выплат прежним участникам за счет последующих не возникает ключевой признак статьи 172.2 УК РФ. Возможность применения статьи 185.3 УК РФ требует отдельной проверки предмета и способа манипулирования по Федеральному закону № 224-ФЗ, особенно для операций вне российского организованного рынка.

Научная новизна нашего исследования состоит в объединении известных признаков в единую последовательность проверки, не подменяющую действующие составы. Сначала устанавливается экономика схемы, затем содержание коммуникации с участниками и, наконец, доказательственная связь цифровых действий с конкретным лицом и умыслом.

Таблица 1. Трехэтапный функциональный тест квалификации

Этап	Ключевой вопрос	Наблюдаемые данные	Юридическое значение
1.Экономическая модель	Откуда возникает доход? Есть ли деятельность, сопоставимая с привлечением? Кто контролирует предложение и ликвидность?	Потоки между адресами; эмиссия; разблокировка токенов; выручка и расходы; пул ликвидности.	Выявляет перераспределение вкладов и реальный источник дохода; отделяет пирамиду от рыночного риска.
2.Коммуникационная модель	Что было обещано участнику? Раскрыты ли риски, контроль и конфликт интересов?	Сайт; white paper; реклама; переписка; записи трансляций; реферальные условия.	Позволяет установить содержание обмана, способ привлечения и публичность продвижения.
3.Доказательственный контур	Кто контролировал адреса, ключи, код и ликвидность? Можно ли персонализировать роль и умысел?	On-chain транзакции в сочетании с KYC, устройствами, журналами доступа, договорами и перепиской.	Не допускает отождествления технического риска с доказанной виновностью конкретного лица.

Источник: составлено авторами.

Первый этап предполагает реконструкцию входящих и исходящих потоков и отделение внешнего экономического дохода от поступлений новых участников. Второй восстанавливает информационную среду: гарантии доходности, сведения о продукте, раскрытие контроля и оплачиваемого продвижения. Третий персонализирует цифровой след. Кластер адресов, сходство кода или включение проекта в риск-список не указывают на конкретного обвиняемого без доказательств контроля, осведомленности, совершенных действий и полученной выгоды.

Этапы образуют цепочку взаимной проверки. Экономическая модель выявляет источник выплат, коммуникационная — способ его представления участникам, доказательственная — связь цифровых действий с конкретным лицом. Если движение стоимости допускает несколько интерпретаций, окончательная квалификация преждевременна до установления контроля над адресами, содержания договоренностей и роли участника: наблюдаемость операции в реестре не раскрывает ее юридического основания.

Проверка на контрастных материалах показала, что последовательность этапов меняет не саму норму, а качество постановки квалификационного вопроса. В российском уголовном материале сообщение Прокуратуры Республики Дагестан от 15 апреля 2026 г. описывает виртуальную финансовую пирамиду, выплаты по которой производились исключительно за счет новых вкладчиков; одновременно сообщается об осуждении по мошенничеству и организации финансовой пирамиды. В материалах Министерства юстиции США по делу United States v. Vladimir Okhotnikov et al. (Court Docket No. 23-cr-57) по версии обвинения смарт-контракты Forsage автоматически перераспределяли поступления новых участников, а публичное продвижение не соответствовало фактическому устройству схемы. Постановление Конституционного Суда Российской Федерации от 20 января 2026 г. № 2-П о споре, связанном с передачей 1000 USDT, напротив, демонстрирует

границу: невозврат цифрового актива и проблема судебной защиты не заменяют установления источника выплат и первоначального обмана.

Таблица 2. Пилотное применение функционального теста

Материал	Экономическая модель	Коммуникационная модель	Квалификационная граница
Российское дело о криптовалютной пирамиде; сообщение прокуратуры о приговоре	Выплаты, по официальному сообщению, осуществлялись за счет средств новых вкладчиков.	Участникам предлагалось инвестирование в криптопроект с обещанием доходности.	Наличие перераспределительного механизма поддерживает проверку ст. 172.2 УК РФ; мошеннические эпизоды требуют самостоятельной индивидуализации.
Forsage; обвинительные материалы США	По версии обвинения, смарт-контракты направляли средства новых участников прежним.	Проект продвигался как децентрализованная доходная возможность при несоответствии заявлений механике схемы.	Материал совместим с пирамидальной моделью, но не является российским приговором и требует самостоятельной квалификации по российскому праву.
Спор, рассмотренный Конституционным Судом РФ № 2-П	Передача и последующий невозврат 1000 USDT; данные о перераспределении между новыми и прежними участниками отсутствуют.	Спор возник из договорной передачи цифровой валюты.	Невозврат имущества не позволяет автоматически заключить о пирамиде или мошенничестве; нужны дополнительные данные об умысле и способе завладения.

Источник: составлено авторами.

Технические исследования подтверждают необходимость такого разграничения и одновременно пределы своей доказательственной силы. При pump-and-dump ценовые и объемные аномалии указывают на необычную активность [12], а при rug pull концентрация ликвидности и функции контракта позволяют выявить риск [14; 15]. Однако эти признаки не устанавливают личность, содержание сообщений и умысел. Поэтому алгоритмический сигнал может служить основанием для углубленной проверки, приобретая юридическое значение лишь в совокупности с данными об источнике стоимости, коммуникациях и контроле над активами.

Предлагаемый тест не подменяет квалификацию и не превращает риск-индикаторы в презумпцию виновности. Его результатом может быть и вывод о недостаточности данных: отсутствие сведений об источнике выплат, обещаниях или принадлежности ключей препятствует обоснованному разграничению финансовой пирамиды, мошенничества, рыночной манипуляции и гражданско-правового спора. Тест задает порядок проверки обстоятельств, а не дополнительное основание ответственности.

Обсуждение

Полученные результаты позволяют разграничить три уровня анализа: экономический — источник выплат и наличие сопоставимой законной деятельности; коммуникативный — сведения и ожидания, сформированные у участника; персональный — контроль адресов, ключей, ликвидности и публичных сообщений. Подмена этих уровней создает риск квалификационной ошибки. Высокая доходность, концентрация токенов или резкое падение цены могут быть риск-индикаторами, но не заменяют признаки статей 159 и 172.2 УК РФ.

Практическое значение предложенного алгоритма особенно проявляется в ситуациях, когда цифровой проект сочетает признаки нескольких моделей. Например, наличие реферального вознаграждения еще не свидетельствует о финансовой пирамиде, если выплаты обеспечиваются самостоятельной хозяйственной деятельностью, сопоставимой с объемом привлечения. Аналогично централизованный контроль над смарт-контрактом или пулом ликвидности повышает риск злоупотребления, но сам по себе не доказывает первоначальный обман. Для квалификации требуется сопоставить хронологию привлечения средств, момент возникновения и изменения публичных обещаний, фактическое направление активов и действия лиц, контролировавших ключи и код. Такое сопоставление позволяет исключить две симметричные ошибки: криминализацию обычного инвестиционного риска и, напротив, маскировку перераспределительной либо мошеннической модели технической терминологией. В процессуальном плане это означает, что вывод о составе преступления должен опираться не на отдельный on-chain индикатор, а на согласованную совокупность цифровых, документальных и коммуникативных данных. При противоречии между ними приоритет не может заранее отдаваться ни одному виду доказательств: требуется установить происхождение каждого сведения, способ его получения и связь с конкретным лицом.

Соотношение статей 159 и 172.2 УК РФ определяется механизмом посягательства. Для финансовой пирамиды ключевым является перераспределение имущества последующих участников в пользу ранее привлеченных при отсутствии сопоставимой деятельности; для мошенничества — завладение имуществом посредством обмана или злоупотребления доверием. При пересечении механизмов необходимо индивидуализировать потерпевших, эпизоды, содержание обмана и направление активов, а затем решать вопрос о конкуренции или совокупности норм. Само использование криптовалюты основанием для механического совмещения составов не является.

Административные составы также нельзя смешивать. Часть 1 статьи 14.62 КоАП РФ охватывает организацию либо осуществление соответствующей перераспределительной деятельности при отсутствии уголовно наказуемого деяния; часть 2 — ее публичное продвижение. Статья 14.56.1 КоАП РФ имеет иной предмет и связана с незаконным привлечением инвестиций, включая требования Федерального закона от 5 марта

1999 г. № 46-ФЗ «О защите прав и законных интересов инвесторов на рынке ценных бумаг». Поэтому публичная реклама, само привлечение имущества и пирамидальный механизм должны проверяться раздельно.

Особое значение имеет доказательственный контур. On-chain данные позволяют установить хэш транзакции, номер блока, адреса, параметры вызова смарт-контракта, состояние пула ликвидности, эмиссию и перемещение токенов. Они надежно фиксируют цифровое событие, но не раскрывают его правовое основание и не тождественны личности. Off-chain слой — договоры, white paper, рекламные кабинеты, переписка, записи трансляций, сведения KYC, журналы входа, устройства, банковские и бухгалтерские документы — чаще раскрывает содержание обещаний, контроль над ключами и распределение ролей. Риск-индикаторы FATF, сформулированные в докладе Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (2020), могут направлять проверку, но не заменяют установления состава конкретного деяния.

Процессуальная реформа 2026 г. требует точного разграничения процедур. Особенности наложения ареста на цифровую валюту закреплены в частях 7.1 и 7.2 статьи 115 УПК РФ, тогда как статья 164.2 УПК РФ регулирует ее изъятие при производстве следственных действий и предусматривает участие специалиста. Сохранность актива при этом не равна сохранности доказательственной информации: отдельно должны фиксироваться состояние устройства, идентификаторы кошельков, исходные транзакционные данные, примененная методика и действия должностного лица после получения доступа.

Предупредительный список Банка России выполняет профилактическую, а не обвинительную функцию. Попадание проекта в список компаний с выявленными признаками нелегальной деятельности на финансовом рынке способно обосновать углубленную проверку и предусмотренные законом превентивные меры, однако в уголовном процессе оно должно оцениваться вместе с первичными данными. Тот же принцип действует для коммерческой блокчейн-аналитики: кластеризация адресов является вероятностным выводом и требует подтверждения KYC, устройствами, журналами доступа, подписанными транзакциями либо иными источниками.

Антиманипуляционный режим требует согласования Федерального закона № 224-ФЗ и статьи 185.3 УК РФ с новым режимом цифровых валют. При этом следует различать манипулирование финансовым инструментом, связанным с цифровой валютой, и воздействие на спотовую цену самой цифровой валюты. Для операций вне российского организованного рынка необходимы четкие критерии охватываемого рынка, искусственного характера воздействия и уголовно значимого результата, чтобы не распространить запрет на обычную волатильную торговлю.

Второе направление касается раскрытия информации в регулируемом контуре. Нам представляется обоснованным закрепление проверяемых сведений о бенефициарном контроле, распределении и графике разблокировки токенов, административных полномочиях в смарт-контракте, условиях блокировки и вывода ликвидности, связанных адресах, оплачиваемом продвижении и конфликте интересов. При этом предел обязанности должен быть очерчен законом: она допустима лишь там, где соответствующее публичное сообщение разрешено действующим регулированием, и не может превращаться в способ обхода запрета рекламы конкретной цифровой валюты.

Для органов расследования, специалистов и экспертов целесообразна единая методика исследования цифровых схем: идентификация актива, сохранение исходных данных, реконструкция потоков, атрибуция адресов, анализ кода и коммуникаций, после чего — юридическая квалификация. Исследование должно раскрывать исходные данные, допущения, степень неопределенности и воспроизводимость результата. Технические обозначения «scam», «Ponzi» или «risk address» остаются аналитическими характеристиками, а не юридическими выводами.

Создание самостоятельного общего состава «криптовалютного мошенничества» нам представляется преждевременным. Статьи 159 и 172.2 УК РФ технологически нейтральны и при корректном установлении фактических обстоятельств охватывают значительную часть рассматриваемых деяний. Мы видим более обоснованный путь в точной настройке отраслевого регулирования, доказательственных процедур и антиманипуляционных правил. Специальная криминализация оправданна лишь в том случае, если выявлен конкретный нормативный пробел, который нельзя устранить толкованием действующей нормы либо средствами регуляторного законодательства.

Заключение

Исследование подтверждает, что цифровая валюта не образует самостоятельной разновидности финансовой пирамиды: квалификацию определяют источник выплат и способ привлечения имущественной стоимости, а не технологическая форма актива. Статья 172.2 УК РФ требует установить перераспределение имущества последующих участников в пользу ранее привлеченных при отсутствии сопоставимой законной деятельности; токен и смарт-контракт лишь обеспечивают технику исполнения. Rug pull требует самостоятельной проверки признаков мошенни-

чества и момента возникновения умысла, а pump-and-dump — отдельной оценки условий применимости антиманипуляционного регулирования. Пилотная апробация показала методическую пригодность трехэтапного теста: последовательная проверка экономической модели, коммуникаций и доказательственного контура препятствует подмене юридического вывода отдельным техническим признаком. Дальнейшее развитие регулирования целесообразно связывать с уточнением правил манипулирования рынком, раскрытием контроля в регулируемом контуре и воспроизводимыми процедурами фиксации цифровых доказательств; перспективным направлением остается апробация теста на расширенном массиве вступивших в силу судебных актов.

Список литературы:

[1] Рыжкова М.В., Кашапова Э.Р. Устойчивость феномена финансовой пирамиды // Terra Economicus. 2022. Т. 20. № 3. С. 22–38. DOI: 10.18522/2073-6606-2022-20-3-22-38..

[2] Долгиева М.М. Криптовалютные финансовые пирамиды в России: вопросы уголовной ответственности // Вестник Дальневосточного юридического института МВД России. 2018. № 4 (45). С. 63–68.

[3] Сердюк А.Ю. Привлечение организатора «финансовой пирамиды» к уголовной ответственности по статье 172.2 УК РФ: разбор признаков состава конкретного преступления // Мировой судья. 2026. № 7. С. 17–20. DOI: 10.18572/2072-4152-2026-7-17-20..

[4] Алиев З.Г., Швырёва В.А., Разин А.В. Криптовалюта как предмет мошенничества: правовая природа и теоретические проблемы доказывания состава преступления, предусмотренного ст. 159 УК РФ // Российский следователь. 2026. № 8. С. 2–7. DOI: 10.18572/1812-3783-2026-8-2-7..

[5] Янковский Р.М. Криптовалюты в российском праве: суррогаты, «иное имущество» и цифровые деньги // Право. Журнал Высшей школы экономики. 2020. № 4. С. 43–77. DOI: 10.17323/2072-8166.2020.4.43.77..

[6] Мурадян С.В. Актуальные проблемы противодействия деятельности криптовалютных пирамид // Имущественные отношения в Российской Федерации. 2024. № 2 (269). С. 93–104.

[7] Bartoletti M., Carta S., Cimoli T., Saia R. Dissecting Ponzi schemes on Ethereum: Identification, analysis, and impact // Future Generation Computer Systems. 2020. Vol. 102. P. 259–277. DOI: 10.1016/j.future.2019.08.014..

[8] Vasek M., Moore T. Analyzing the Bitcoin Ponzi Scheme Ecosystem // Financial Cryptography and Data Security. FC 2018 International Workshops. Berlin, Heidelberg: Springer, 2019. P. 101–112. DOI: 10.1007/978-3-662-58820-8_8..

[9] Bartoletti M., Lande S., Loddo A., Pompianu L., Serusi S. Cryptocurrency Scams: Analysis and Perspectives // IEEE Access. 2021. Vol. 9. P. 148353–148373. DOI: 10.1109/ACCESS.2021.3123894..

[10] Dhawan A., Putniņš T.J. A New Wolf in Town? Pump-and-Dump Manipulation in Cryptocurrency Markets // Review of Finance. 2023. Vol. 27. No. 3. P. 935–975. DOI: 10.1093/rof/rfac051.

[11] Hamrick J.T., Rouhi F., Mukherjee A., Feder A., Gandal N., Moore T., Vasek M. An examination of the cryptocurrency pump-and-dump ecosystem // Information Processing & Management. 2021. Vol. 58. No. 4. Article 102506. DOI: 10.1016/j.ipm.2021.102506..

[12] Kamps J., Kleinberg B. To the moon: defining and detecting cryptocurrency pump-and-dumps // Crime Science. 2018. Vol. 7. Article 18. DOI: 10.1186/s40163-018-0093-5..

[13] Xia P., Wang H., Gao B. et al. Trade or Trick? Detecting and Characterizing Scam Tokens on Uniswap Decentralized Exchange // Proceedings of the ACM on Measurement and Analysis of Computing Systems. 2021. Vol. 5. No. 3. Article 39. P. 1–26. DOI: 10.1145/3491051.

[14] Mazorra B., Adan V., Daza V. Do Not Rug on Me: Leveraging Machine Learning Techniques for Automated Scam Detection // Mathematics. 2022. Vol. 10. No. 6. Article 949. DOI: 10.3390/math10060949.

[15] Nguyen M.H., Huynh P.D., Dau S.H., Li X. Rug-pull malicious token detection on blockchain using supervised learning with feature engineering // Proceedings of the 2023 Australasian Computer Science Week. 2023. P. 72–81. DOI: 10.1145/3579375.3579385.

References:

[1] Ryzhkova M.V., Kashapova E.R. Sustainability of the phenomenon of the financial pyramid // Terra Economicus. 2022. T. 20. № 3. S. 22-38. DOI: 10.18522/2073-6606-2022-20-3-22-38..

[2] Dolgieva M.M. Cryptocurrency financial pyramids in Russia: issues of criminal liability // Bulletin of the Far Eastern Law Institute of the Ministry of Internal Affairs of Russia. 2018. № 4 (45). S. 63-68.

[3] Serdyuk A.Yu. Bringing the organizer of the "financial pyramid" to criminal responsibility under Article 172.2 of the Criminal Code of the Russian Federation: analysis of signs of a specific crime // Magistrate. 2026. № 7. S. 17-20. DOI: 10.18572/2072-4152-2026-7-17-20..

[4] Aliyev Z.G., Shvyreva V.A., Razin A.V. Cryptocurrency as a subject of fraud: legal nature and theoretical problems of proving corpus delicti under Art. 159 of the Criminal Code of the Russian Federation // Russian investigator. 2026. № 8. S. 2-7. DOI: 10.18572/1812-3783-2026-8-2-7..

[5] Yankovsky R.M. Cryptocurrencies in Russian law: surrogates, "other property" and digital money // Law. Journal of the Higher School of Economics. 2020. № 4. S. 43-77. DOI: 10.17323/2072-8166.2020.4.43.77..

[6] Muradyan S.V. Actual problems of counteracting the activities of cryptocurrency pyramids // Property relations in the Russian Federation. 2024. № 2 (269). S. 93-104.

[7] Bartoletti M., Carta S., Cimoli T., Saia R. Dissecting Ponzi schemes on Ethereum: Identification, analysis, and impact // Future Generation Computer Systems. 2020. Vol. 102. P. 259–277. DOI: 10.1016/j.future.2019.08.014..

[8] Vasek M., Moore T. Analyzing the Bitcoin Ponzi Scheme Ecosystem // Financial Cryptography and Data Security. FC 2018 International Workshops. Berlin, Heidelberg: Springer, 2019. P. 101–112. DOI: 10.1007/978-3-662-58820-8_8..

[9] Bartoletti M., Lande S., Loddo A., Pompianu L., Serusi S. Cryptocurrency Scams: Analysis and Perspectives // IEEE Access. 2021. Vol. 9. P. 148353–148373. DOI: 10.1109/ACCESS.2021.3123894..

[10] Dhawan A., Putniņš T.J. A New Wolf in Town? Pump-and-Dump Manipulation in Cryptocurrency Markets // Review of Finance. 2023. Vol. 27. No. 3. P. 935–975. DOI: 10.1093/rof/rfac051.

[11] Hamrick J.T., Rouhi F., Mukherjee A., Feder A., Gandal N., Moore T., Vasek M. An examination of the cryptocurrency pump-and-dump ecosystem // Information Processing & Management. 2021. Vol. 58. No. 4. Article 102506. DOI: 10.1016/j.ipm.2021.102506..

[12] Kamps J., Kleinberg B. To the moon: defining and detecting cryptocurrency pump-and-dumps // Crime Science. 2018. Vol. 7. Article 18. DOI: 10.1186/s40163-018-0093-5..

[13] Xia P., Wang H., Gao B. et al. Trade or Trick? Detecting and Characterizing Scam Tokens on Uniswap Decentralized Exchange // Proceedings of the ACM on Measurement and Analysis of Computing Systems. 2021. Vol. 5. No. 3. Article 39. P. 1–26. DOI: 10.1145/3491051.

[14] Mazorra B., Adan V., Daza V. Do Not Rug on Me: Leveraging Machine Learning Techniques for Automated Scam Detection // Mathematics. 2022. Vol. 10. No. 6. Article 949. DOI: 10.3390/math10060949.

[15] Nguyen M.H., Huynh P.D., Dau S.H., Li X. Rug-pull malicious token detection on blockchain using supervised learning with feature engineering // Proceedings of the 2023 Australasian Computer Science Week. 2023. P. 72–81. DOI: 10.1145/3579375.3579385.

