

ВОПРОСЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ОБОРОТА КРИПТО-АКТИВОВ И ПУТИ ИХ РЕШЕНИЯ (ПРАКТИКА РЕСПУБЛИКИ УЗБЕКИСТАН)

КАЮМОВ БАХТИЁР ЭРКИНЖОНОВИЧ

Начальник факультета бакалавриата Правоохранительной Академии.

Советник юстиции, д.ф.ю.н. (PhD)

КАМАЛХОДЖАЕВ АМАР ЗАУРОВИЧ

Студент 3 курса по направлению подготовки «Следственная деятельность»

Правоохранительной Академии

Аннотация В статье рассматриваются уголовно-правовые проблемы, связанные с преступлениями в сфере крипто-активов в условиях развития цифровой экономики. Анализируются особенности правовой природы крипто-активов, отсутствие единообразного понятийного аппарата и его влияние на квалификацию преступлений и судебную практику. Исследуются основные формы преступного использования крипто-активов, а также практические сложности их расследования, включая установление субъектов, определение юрисдикции и работу с цифровыми доказательствами. На основе анализа законодательства и судебной практики Республики Узбекистан выявлены ключевые проблемы правоприменения. Обосновывается необходимость совершенствования уголовного и уголовно-процессуального законодательства, развития международного сотрудничества и внедрения новых подходов, включая принцип «цифрового эффекта», для повышения эффективности противодействия преступлениям в данной сфере.

Ключевые слова: *крипто-активы, криптовалюта, цифровые активы, уголовное право, квалификация преступлений, цифровые доказательства, блокчейн.*

Введение. Развитие цифровой экономики, технологий распределенного реестра (блокчейн) и виртуальных финансовых инструментов обусловило появление новых объектов гражданского оборота, среди которых особое место занимают крипто-активы. Их стремительное распространение привело к возникновению новых форм преступной деятельности и поставило перед

уголовно-правовой наукой ряд сложных теоретических и практических вопросов.

Актуальность темы статьи обусловлена тем, что несмотря на активное развитие законодательства в сфере цифровых технологий, единый подход к определению правовой природы крипто-активов до настоящего времени отсутствует. Данное обстоятельство оказывает существенное влияние на квалификацию преступлений, связанных с их незаконным оборотом, хищением, использованием в целях легализации преступных доходов и финансирования противоправной деятельности.

В настоящее время наблюдается стремительный рост преступлений в сфере крипто-активов, что свидетельствует об усилении криминогенных рисков в цифровой финансовой среде. Согласно данным аналитического отчёта компании Chainalysis, в период с января по начало декабря 2025 года общий объём похищенных крипто-активов превысил 3,4 млрд долларов США. Одним из наиболее значительных инцидентов стал взлом криптовалютной биржи Bybit, произошедший в феврале 2025 года, в результате которого злоумышленниками было похищено около 1,5 млрд долларов США.¹

Исследователь из Республики Узбекистан Гуломов Ш.² отмечает, что в различных нормативных актах и научных публикациях крипто-активы определяются по-разному: как цифровое имущество, средство обмена, цифровой код либо разновидность виртуального актива. По мнению автора, подобная терминологическая неопределенность приводит к проблемам квалификации преступлений, поскольку правоохранительные органы и суды фактически применяют различные правовые режимы к одному и тому же объекту.

¹ North Korea Drives Record \$2 Billion Crypto Theft Year, Pushing All-Time Total to \$6.75 Billion. URL: <https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/> (дата обращения: 24.12.2025).

² Гуломов Ш. Анализ правовых основ преступлений в сфере оборота крипто-активов // Общество и инновации. 2025. URL: <https://inscience.uz/index.php/socinov/article/view/6150?> (дата обращения: 25.03.2025).

Схожей позиции придерживается российский ученый Роман Янковский, который указывает, что в российской доктрине крипто-актив одновременно рассматривается как денежный суррогат, цифровые деньги, иное имущество либо особый вид имущественных прав³. Исследователь подчеркивает, что отсутствие единого понятийного аппарата негативно влияет на судебную практику и создает неопределенность при решении вопроса о возможности применения норм уголовного законодательства к крипто-активам.

Поддерживая данную позицию, Аристархов А.Л. указывает, что даже специальное законодательство о цифровых финансовых активах не содержит четкого и универсального определения крипто-активов. Автор приходит к выводу, что неопределенность законодательных дефиниций препятствует единообразному пониманию крипто-активов в уголовном процессе и усложняет разграничение предмета преступления и средства совершения преступления⁴.

В доктрине дальнего зарубежья также отсутствует единообразный подход к определению правовой природы крипто-активов. Так, европейский исследователь Wyczik J. отмечает, что крипто-активы обладают смешанной правовой природой, поскольку одновременно включают признаки цифрового имущества, информации и имущественных прав⁵. Автор полагает, что традиционные правовые конструкции вещного права не способны в полной мере охватить специфику Web3-активов⁶.

Таким образом, большинство современных исследователей сходятся во мнении, что отсутствие унифицированной терминологии является

³ Янковский Р. Криптовалюты в российском праве: суррогаты, «иное имущество» и цифровые деньги // Право. Журнал высшей школы экономики. 2020. URL: <https://law-journal.hse.ru/article/view/19949?> (дата обращения: 15.03.2020).

⁴ Аристархов А. Л. Значение вопросов регламентации криптовалюты для уголовного судопроизводства // Право. 2024. URL: <https://cyberleninka.ru/article/n/znachenie-voprosov-reglamentatsii-kriptovalyuty-dlya-ugolovnogo-sudoproizvodstva> (дата обращения: 2024).

⁵ Jakub Wyczik. The Property Law of Crypto Tokens // Computer Science. Cryptography and Security. 2024. URL: <https://arxiv.org/abs/2311.01461?> (дата обращения: 02.11.2023).

⁶ Jiajing W, Kaixin L, Dan L, Ziyi Z, Huawei H, Zibin Z.. Financial Crimes in Web3-empowered Metaverse: Taxonomy, Countermeasures, and Opportunities. // Help | Advanced Search All fields Search Computer Science. Cryptography and Security. 2022. URL: <https://ralj.ru/article/view/%282021%293.1?> (дата обращения: 27.12.2022).

фундаментальной проблемой уголовно-правовой квалификации преступлений в сфере крипто-активов. Однако между учеными сохраняются разногласия относительно правовой природы крипто-активов и ее соотношения с традиционными объектами гражданских прав.

Объектом исследования являются общественные отношения, возникающие в сфере уголовно-правовой охраны крипто-активов, а также отношения, складывающиеся в процессе предупреждения, выявления, расследования и судебного рассмотрения преступлений, связанных с незаконным оборотом и использованием крипто-активов.

Предметом исследования являются нормы уголовного и уголовно-процессуального законодательства, а также иные ведомственные нормативно-правовые акты Национального агентства перспективных проектов Республики Узбекистан, регулирующие вопросы ответственности за преступления, связанные с криптоактивами, практика их применения, порядок оборота, хранения и передачи криптоактивов, а также научные подходы к определению их правовой природы и уголовно-правового статуса.

Целью настоящего исследования является анализ существующих научных подходов к квалификации преступлений, связанных с крипто-активами, выявление практических проблем их расследования и разработка предложений по совершенствованию уголовного законодательства Республики Узбекистан.

Основная часть. Одной из наиболее дискуссионных проблем современной уголовно-правовой науки является отсутствие единых дефиниций понятий «крипто-актив», «криптовалюта», «цифровой актив», «виртуальная валюта» и «цифровая валюта». В научной литературе отсутствует единое мнение относительно соотношения указанных категорий и их места в системе объектов права.

Исследователи отмечают, что крипто-активы рассматриваются как цифровое имущество, средство обмена, разновидность имущественных прав либо самостоятельный объект гражданских правоотношений. Отсутствие

единообразного понятийного аппарата приводит к неодинаковому толкованию правовой природы крипто-активов судами и правоохранительными органами.

Другой важной научной дискуссией является вопрос о признании крипто-активов предметом преступления. Традиционная теория уголовного права исходит из материального характера предмета преступления, тогда как крипто-активы существуют исключительно в цифровой форме и представляют собой записи в распределённом реестре.

Сторонники признания крипто-активов предметом преступлений против собственности указывают на наличие у них экономической ценности, оборотоспособности и возможности выступать объектом владения, распоряжения и обмена. Противники данной позиции считают необходимым формирование самостоятельной уголовно-правовой конструкции для цифровых активов ввиду их особой правовой природы.

Особое значение имеет вопрос о признании крипто-активов имуществом. Решение данной проблемы непосредственно влияет на возможность квалификации их хищения как преступлений против собственности, применения института конфискации имущества, признания предметом легализации преступных доходов и обеспечения возмещения ущерба потерпевшим.

Анализ научной литературы показывает, что большинство современных исследователей признают имущественную природу крипто-активов. Вместе с тем продолжается дискуссия относительно необходимости выделения специального правового режима для цифровых активов.

Практические сложности расследования преступлений, связанных с крипто-активами, обусловлены техническими особенностями блокчейн-технологий, высокой степенью анонимности участников транзакций и транснациональным характером цифровых активов.

Одной из ключевых проблем является установление субъекта преступления. Несмотря на открытый характер блокчейна, адрес криптовалютного кошелька не содержит сведений о личности владельца. Для идентификации правонарушителей правоохранительные органы вынуждены

использовать методы цифровой криминалистики, включающие анализ IP-адресов, данных криптовалютных бирж, информации KYC, цифровых устройств и социальных сетей.

Серьёзные трудности вызывает определение места совершения преступления. Транзакции в блокчейне одновременно обрабатываются множеством узлов сети, расположенных в различных государствах. Это создаёт коллизию юрисдикций и усложняет определение компетентного органа расследования.

На сегодняшний день одной из правовых коллизий в правоприменительной практике Республики Узбекистан является то, что в соответствии с национальным уголовным законодательством приобретение, сбыт или обмен крипто-активов может влечь административную и (или) уголовную ответственность. Вместе с тем на практике наблюдаются случаи, когда граждане Республики Узбекистан выезжают в зарубежные государства, где совершают операции по приобретению, сбыту или обмену крипто-активов, после чего возвращаются на территорию страны. В подобных ситуациях они остаются без наказания, поскольку на момент совершения соответствующих действий находились в юрисдикции государства, в котором данные деяния не признаются противоправными. Причиной невозможности привлечения указанных лиц к уголовной ответственности выступает принцип двойной наказуемости (*double criminality*), являющийся одним из основополагающих принципов международного уголовного сотрудничества. Согласно данному принципу, деяние, в связи с которым запрашивается выдача лица, должно быть признано уголовно наказуемым как в государстве, инициирующем запрос об экстрадиции, так и в государстве, рассматривающем вопрос о его исполнении.

К тому же в Республике Узбекистан особую актуальность приобретают проблемы изъятия и ареста (замораживания) крипто-активов. В отличие от традиционного имущества цифровые активы контролируются посредством криптографических ключей, а не физического владения. Отсутствие доступа к приватному ключу делает фактическое изъятие актива невозможным даже при наличии судебного решения.

Дополнительные сложности возникают при работе с цифровыми доказательствами. К ним относятся адреса криптовалютных кошельков, хэши транзакций, журналы криптовалютных бирж, данные облачных сервисов, переписка в мессенджерах и иные цифровые следы. Их высокая изменчивость требует оперативного проведения следственных действий и применения специальных методов цифровой криминалистики.

В мировой практике для расследования подобных преступлений активно используются инструменты blockchain forensics, включая Chainalysis, CipherTrace и Elliptic. Данные технологии позволяют устанавливать связи между кошельками, отслеживать перемещение активов и выявлять подозрительные транзакции.

Особую проблему для Республики Узбекистан представляет недостаточное количество специалистов в области цифровой криминалистики. Рост преступлений в сфере информационно-коммуникационных технологий значительно опережает возможности правоохранительных органов по обеспечению расследований квалифицированными экспертами.

Анализ судебной практики по преступлениям в сфере крипто-активов в Республике Узбекистан за 2024–2026 годы показал, что более 95 % уголовных дел связаны непосредственно с нарушением законодательства, регулирующего оборот, хранение, передачу крипто-активов. К тому же значительная часть данных деяний совершается в совокупности с преступлениями, связанными с легализацией преступных доходов, мошенничеством, кражами, а также незаконным оборотом наркотических средств. Полученные данные свидетельствуют о том, что крипто-активы всё чаще используются не в качестве самостоятельного предмета преступления, а как инструмент совершения иных противоправных деяний. Это обусловлено тем, что особенности обращения крипто-активов позволяют злоумышленникам существенно затруднять выявление источника происхождения средств, маршрутов их перемещения и

лиц, причастных к совершению преступления, что осложняет процесс раскрытия и расследования преступных деяний⁷.

Тем самым, показательным примером квалификации является судебное дело, рассмотренное судами Республики Узбекистан в 2024 году⁸. В рассматриваемом судебном деле исследовалась деятельность организованной группы лиц, связанная с совершением мошенничества с использованием информационно-коммуникационных технологий и незаконным оборотом крипто-активов. Со стороны следственных органов установлено, что преступная схема строилась на привлечении потерпевших через социальные сети (Instagram, Facebook) посредством размещения фиктивных инвестиционных предложений с использованием вымышленных историй о высокой доходности и ссылок на псевдоинвестиционные платформы. Потерпевшие, введенные в заблуждение, осуществляли переводы денежных средств на банковские карты подставных лиц, после чего денежные средства последовательно конвертировались в крипто-активы (в основном USDT) и выводились через P2P-платформы и криптовалютные сервисы, включая «Only Finance» и «Pay2Play». Совокупный размер причинённого ущерба по установленным эпизодам превысил один миллиард сумов. Дополнительно установлены операции с крипто-активами в объёме более 169 000 USDT, что эквивалентно более 1,6 миллиард сумов. Суд квалифицировал действия участников по ст. 168 ч.3 п.«б,г» УК Республики Узбекистан (мошенничество, совершённое группой лиц по предварительному сговору с использованием информационных технологий), ст. 168 ч.4 п.«а» УК (мошенничество в особо крупном размере), а также ст. 278⁸ ч.3 п.«а» УК (незаконный оборот крипто-активов).

Таким образом, данная практика наглядно демонстрирует, что крипто-активы используются как средство (инструмент) совершения преступления,

⁷ Жиноят ишлари бўйича судлар томонидан интернет тармоғида эълон қилинган суд қарорлари. URL: <https://public.sud.uz/report/CRIMINAL>

⁸ Жиноят ишлари бўйича судлар томонидан интернет тармоғида эълон қилинган суд қарорлари. URL: <https://public.sud.uz/report/CRIMINAL>

поскольку основная преступная цель заключалась в хищении денежных средств граждан, а крипто-активы (USDT) использовались как инструмент их конвертации, сокрытия и последующего вывода. Одновременно он частично охватывает и первую группу (крипто-активы как предмет преступления), так как установлены крупные операции с незаконным оборотом криптовалюты, и третью группу (нарушение порядка оборота крипто-активов), поскольку использовались нелицензированные и анонимные криптосервисы.

Другим примером является уголовное дело, рассмотренное судом города Ташкента в 2026 году. С октября 2024 года по август 2025 года лицо, действуя из корыстных побуждений и без получения лицензии в установленном порядке, организовало преступную группу для незаконного оборота крипто-активов. Участники группы арендовали квартиру под офис, где круглосуточно осуществляли операции по покупке и продаже стейблкоина USDT через иностранную анонимную платформу Desend. Для этого использовались около 975 банковских «дроп-карт», оформленных на третьих лиц, SIM-карты, мобильные телефоны, ноутбуки и иная техника. Один из участников группы лично подбирал и обучал операторов, распределял роли и смены, обеспечивал техническими средствами и выплачивал вознаграждение в размере 150–200 долларов США в неделю каждому. В результате преступной деятельности группой было проведено транзакций на общую сумму 12 472 360,88 USDT, что эквивалентно 165 185 317 589 сумов.

Таким образом, рассматриваемая практика представляет собой пример правонарушений, связанных с нарушением установленного порядка оборота крипто-активов, поскольку их объективная сторона выражается в незаконном обмене и обращении крипто-активов без соответствующей лицензии либо разрешения, предусмотренного национальным законодательством.

Таким образом, результаты проведённого исследования свидетельствуют о необходимости дальнейшего совершенствования уголовного и уголовно-процессуального законодательства Республики Узбекистан, а также ведомственного нормативно-правового регулирования общественных отношений, связанных с оборотом, хранением и передачей

крипто-активов, в целях обеспечения надлежащей уголовно-правовой охраны данных отношений и повышения эффективности противодействия преступлениям в рассматриваемой сфере.

Следовательно, выявленные в ходе исследования проблемы и существующие пробелы в правовом регулировании обуславливают необходимость разработки и внедрения комплекса мер, направленных на повышение эффективности расследования преступлений, связанных с использованием крипто-активов. В связи с этим автором предлагаются следующие рекомендации.

Первое. Прежде всего представляется целесообразным внесение изменений в статью 95¹ УПК Республики Узбекистан, предусматривающих возможность самостоятельного производства следователем выемки и осмотра электронных данных в случаях, не терпящих отлагательства, с последующим проведением обязательной технической экспертизы.

Второе. Особое внимание следует уделить формированию единообразной судебной практики. Представляется необходимым принятие Пленумом Верховного суда Республики Узбекистан специального постановления, посвящённого вопросам квалификации преступлений, совершаемых с использованием цифровых финансовых технологий.

Третье. Дополнительным направлением совершенствования правоприменительной практики должно стать создание специализированных судебных составов по рассмотрению уголовных дел в сфере цифровых технологий и развитие международного сотрудничества в области обмена цифровыми доказательствами.

Четвёртое. С практической точки зрения правоохранительные органы в настоящее время сталкиваются с проблемой изъятия и замораживания крипто-активов. В связи с этим представляется важным создание в ведомствах, осуществляющих противодействие преступлениям в сфере крипто-активов, холодных криптокошельков для хранения изъятых крипто-активов. Кроме того, автор считает целесообразным расширение взаимодействия правоохранительных органов с централизованными криптовалютными

биржами и эмитентами стейблкоинов, что будет способствовать повышению эффективности расследования преступлений в сфере крипто-активов.

Пятое. По результатам проведённого исследования автор обосновывает необходимость совершенствования уголовного законодательства Республики Узбекистан в части регулирования ответственности за деяния, связанные с незаконным оборотом крипто-активов.

В связи с этим предлагается закрепить в национальном законодательстве и международно-правовых актах новый правовой принцип — принцип цифрового эффекта, предусматривающий возможность осуществления уголовной юрисдикции государства в отношении деяний, совершённых в цифровой среде, если их последствия затрагивают охраняемые законом интересы данного государства независимо от места совершения таких деяний.

Под принципом цифрового эффекта следует понимать основание реализации уголовной юрисдикции государства в отношении деяний, совершаемых в цифровом пространстве, включая операции с крипто-активами, когда такие деяния, независимо от места их фактического осуществления, причиняют вред либо создают реальную угрозу причинения вреда охраняемым законом общественным отношениям соответствующего государства.

Необходимость разработки данного принципа обусловлена трансформацией общественных отношений под воздействием цифровизации экономики и широким распространением технологий распределённого реестра. В отличие от традиционных объектов правового регулирования, крипто-активы не обладают устойчивой территориальной привязкой. Субъект противоправного деяния может находиться в одном государстве, используемая цифровая платформа — в другом, серверная инфраструктура — в третьем, тогда как негативные последствия такого деяния способны одновременно проявляться на территории нескольких государств. В этих условиях применение традиционных критериев определения уголовной юрисдикции, основанных преимущественно на территориальном принципе, существенно затрудняется.

Дополнительной проблемой является ограниченная эффективность принципа двойной преступности применительно к деяниям, связанным с крипто-активами. Это обусловлено значительными различиями в подходах государств к регулированию цифровых активов. Одни государства устанавливают строгие ограничения или запреты на осуществление операций с крипто-активами, другие допускают их свободное обращение либо не предусматривают специального регулирования. В результате возникает возможность использования различий между национальными правовыми порядками для обхода требований законодательства того государства, интересам которого фактически причиняется ущерб.

В связи с этим представляется обоснованным исходить из того, что определяющим критерием уголовной юрисдикции в отношении деяний, совершаемых с использованием цифровых технологий, должно выступать не место нахождения лица либо технической инфраструктуры, а место наступления или потенциального наступления общественно опасных последствий. Данный подход предлагается обозначить как принцип цифрового эффекта.

Согласно указанному принципу государство вправе распространять действие своего уголовного закона на деяния, совершённые за пределами его территории посредством цифровых технологий, если такие деяния направлены против его финансовой системы, рынка цифровых активов, прав и законных интересов граждан либо иных охраняемых законом интересов государства и способны причинить им существенный вред.

При этом принцип цифрового эффекта не заменяет существующие принципы уголовной юрисдикции, а дополняет их с учётом особенностей цифровой среды. Его ключевая особенность заключается в смещении акцента с физического места совершения деяния на место проявления его общественно опасных последствий. Соответственно, основным объектом правовой оценки становится не территория совершения действия, а территория, на которой возникает или может возникнуть вредоносный результат.

Внедрение принципа цифрового эффекта позволит устранить существующие пробелы в регулировании трансграничных преступлений, связанных с крипто-активами, повысить уровень защиты экономической безопасности государства и ограничить возможности использования цифровых технологий для обхода национального законодательства посредством выбора наиболее благоприятной иностранной юрисдикции.

Заключение. Проведённое исследование показывает, что современная уголовно-правовая доктрина находится на этапе формирования единых подходов к пониманию правовой природы крипто-активов и особенностей квалификации преступлений, связанных с их использованием.

Основными проблемами остаются отсутствие единообразного понятийного аппарата, дискуссионность вопроса о признании крипто-активов имуществом, сложности определения предмета преступления, транснациональный характер цифровых активов и недостаточная урегулированность процессуального статуса цифровых доказательств.

Практика расследования преступлений в сфере крипто-активов свидетельствует о необходимости совершенствования механизмов идентификации субъектов преступлений, изъятия и хранения цифровых активов, использования методов цифровой криминалистики и международного сотрудничества.

Реализация предложенных законодательных изменений позволит повысить эффективность уголовно-правовой охраны общественных отношений в сфере цифровых финансовых технологий, обеспечить единообразие правоприменительной практики и создать необходимые условия для противодействия современным формам цифровой преступности.

Список использованной литературы:

1. North Korea Drives Record \$2 Billion Crypto Theft Year, Pushing All-Time Total to \$6.75 Billion. URL: <https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/> (дата обращения: 24.12.2025).

2. Статистика МВД // Kun.uz. URL: <https://kun.uz/ru/news/2025/12/24/uzbekistansam-za-11-mesyatsev-nanesen-ushcherb-kiberprestupleniyami-na-1-trln-890-mlrd-sumov> (дата обращения: 24.12.2025).
3. Гуломов Ш. Анализ правовых основ преступлений в сфере оборота крипто-активов // Общество и инновации. 2025. URL: <https://inscience.uz/index.php/socinov/article/view/6150?> (дата обращения: 25.03.2025).
4. Янковский Р. Криптовалюты в российском праве: суррогаты, «иное имущество» и цифровые деньги // Право. Журнал высшей школы экономики. 2020. URL: <https://law-journal.hse.ru/article/view/19949?> (дата обращения: 15.03.2020).
5. Аристархов А. Л. Значение вопросов регламентации криптовалюты для уголовного судопроизводства // Право. 2024. URL: <https://cyberleninka.ru/article/n/znachenie-voprosov-reglamentatsii-kriptovalyuty-dlya-ugolovnogo-sudoproizvodstva> (дата обращения: 2024).
6. Jakub Wyczik. The Property Law of Crypto Tokens // Computer Science. Cryptography and Security. 2024. URL: <https://arxiv.org/abs/2311.01461?> (дата обращения: 02.11.2023).
7. Jiajing W, Kaixin L, Dan L, Ziye Z, Huawei H, Zibin Z.. Financial Crimes in Web3-empowered Metaverse: Taxonomy, Countermeasures, and Opportunities. // Help | Advanced Search All fields Search Computer Science. Cryptography and Security. 2022. URL: <https://ralj.ru/article/view/%282021%293.1?> (дата обращения: 27.12.2022).
8. Жиноят ишлари бўйича судлар томонидан интернет тармоғида эълон қилинган суд қарорлари. URL: <https://public.sud.uz/report/CRIMINAL>