

Дата поступления рукописи в редакцию: 15.07.2026 г.

DOI: 10.24412/2076-1503-2026-8-762-765

Дата принятия рукописи в печать: 04.08.2026 г.

ШИКУЛА Ильмира Рифкатьевна,
доктор юридических наук, доцент, профессор Департамента
методики преподавания социальных и гуманитарных наук
Института гуманитарных наук ГАОУ ВО «Московский
городской педагогический университет»; профессор
кафедры Гражданского и Уголовного права и процесса
АНО ВО «Московский международный университет», член
экспертного совета комитета Государственной Думы РФ
по защите семьи, вопросам отцовства, материнства и
детства, академик РАЕН,
e-mail: ila.vnii@mail.ru

КУЗЬМИН Кирилл Евгеньевич,
заместитель начальника линейного отдела полиции в порту
"Северный" ЛО МВД России на ВТ,
e-mail: kirill_kuzmin03@mail.ru

ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ БЛОКЧЕЙН

Аннотация. В данной работе авторами рассматривается понятие и сущность технологии блокчейн с целью рассмотрения проблематики вопроса о квалификации преступлений с ее использованием, анализируется актуальная статистика совершаемых преступлений на примере правоприменительной практики, рассматривается нормативно-правовое регулирование в сфере использования цифровых активов, а также рассматриваются проблемные вопросы квалификации преступлений, вносятся обоснованные предложения по совершенствованию действующего законодательства.

Ключевые слова: блокчейн, цифровой актив, криптовалюта, компьютерные технологии, хищение.

SHIKULA Ilmira Rifkatyevna,
Doctor of Law, Associate Professor, Professor, Department of
Teaching Methods of Social Sciences and Humanities, Institute
of Humanities, Moscow City Pedagogical University; Professor,
Department of Civil and Criminal Law and Procedure, Moscow
International University, Member of the Expert Council of
the State Duma Committee on Family Protection, Fatherhood,
Motherhood, and Childhood, Academician of the Russian Academy
of Natural Sciences

KUZMIN Kirill Evgenievich,
Deputy Chief of the Linear Police Department at the Severny Port,
Leningrad Region, Ministry of Internal Affairs of Russia, on VT

PROBLEMS WITH THE CLASSIFICATION OF CRIMES COMMITTED USING BLOCKCHAIN TECHNOLOGY

Annotation. In this work, the authors consider the concept and essence of blockchain technology in order to address the issue of criminal liability for crimes committed using this technology. The authors analyze current statistics on crimes committed using blockchain technology, examine the legal regulation of digital assets, and discuss the challenges of criminal liability. The authors also make suggestions for improving current legislation.

Key words: blockchain, digital asset, cryptocurrency, computer technology, theft.

Развитие информационных технологий в современном мире способствует появлению новых способов совершения преступлений, среди которых особое место занимают преступные деяния, сопряженные с использованием технологии блокчейн. Для того, чтобы подробно разобраться с поставленной темой, в первую очередь необходимо дать определение и рассмотреть сущность вышеуказанной технологии блокчейн. Сам термин «блокчейн» в переводе с английского означает цепочку блоков, что довольно точно отражает устройство данной технологии. Иными словами, это технология распределенного хранения данных, в которой информация записывается в виде последовательной цепочки блоков. Каждый блок содержит набор тех или иных записей (например, транзакций) и криптографическую ссылку на предыдущий блок. Благодаря подобному устройству этой системы, незаметно изменить данные в одном блоке невозможно. На сегодняшний день указанная технология широко применяется во многих сферах жизни общества. Самое распространенное применение она находит в использовании криптовалюты. Кроме того, стоит отметить, что блокчейн используют в логистике для отслеживания поставок, в финансовой сфере, а также при оформлении цифровых прав собственности. Многие отечественные и зарубежные ученые-юристы, рассматривая технологию блокчейн в своих работах отмечали её ключевые особенности, к таким, на наш взгляд следует отнести децентрализацию, неизменяемость, а также ее прозрачность. Если говорить подробно о вышеназванных особенностях, то стоит отметить, что принцип работы этой технологии выстроен на принципе последовательности, таким образом, если изменить одну запись, криптографический отпечаток перестанет совпадать и все участники сети обнаружат попытку подмены данных. Благодаря такому устройству участники сети могут доверять записям, даже если совершенно не знают друг друга. Исходя из этого следует выделить еще одну особенность – отсутствие посредников в использовании технологии.

Продолжая рассмотрение данной темы, стоит отметить, что распределенные реестры и построенные на их основе виды криптовалют, первоначально создавались как инструменты повышения прозрачности и надежности финансовых операций, однако, свойственный им децентрализованный характер и отсутствие единого контролирующего органа привлекли внимание лиц, стремящихся скрыть следы преступления. Правоприменительная практика последних лет демонстрирует нам устойчивый рост числа хищений криптовалютных активов, случаев легализации доходов, полученных преступным путем, а также фактов

финансирования запрещенной деятельности с использованием цифровых активов, что в свою очередь требует от науки уголовного права осмысления возникающих проблем и выработки согласованных подходов к их разрешению. Так, например, по данным Верховного суда РФ на май 2025 года, за последние годы рассмотрено свыше 20 уголовных дел, связанных с посягательством на криптовалюту или её использованием для легализации доходов.

В 2023–2024 годах московские суды рассмотрели семь таких дел, суды Московской области – 4 [4]. Правоохранительные органы и Росфинмониторинг фиксируют увеличение числа дел по статьям 174 и 174.1 УК РФ (легализация преступных доходов), где в качестве инструмента использовались обменные сервисы и миксеры. Суды всё активнее признают: последовательная конвертация криптовалюты, полученной от преступления (например, от наркобизнеса), через обменники в фиат и вывод на карты третьих лиц может свидетельствовать о цели придать правомерный вид криминальным доходам.

Сложность квалификации подобных деяний обусловлена прежде всего неопределенностью правовой природы самих цифровых активов, поскольку вопрос о том, следует ли рассматривать криптовалюту в качестве имущества, имущественного права или иного объекта гражданских прав, до настоящего времени не получил однозначного ответа. От ответа на данный вопрос напрямую зависит вопрос квалификации преступных деяний и возможность применения к хищениям криптовалюты традиционных составов преступлений против собственности, а также разграничение деяний с преступлениями в сфере компьютерной информации. Правоприменители отмечают, что, несмотря на ежегодный рост преступлений в сфере IT-технологий, их раскрываемость не превышает 25%. Подобное соотношение показателей зарегистрированных и раскрытых преступлений, а также реально привлечённых к уголовной ответственности лиц наводит на мысли о том, что, с одной стороны, положения главы 28 УК РФ практически не играют значимой роли в процессе предупреждения распространения преступлений, совершаемых в сфере компьютерной информации, а с другой стороны, у правоприменителей в целом возникают проблемы в процессе квалификации соответствующих преступных деяний.

Названные проблемы, как представляется, будут лишь углубляться по мере развития информационных технологий и увеличения сфер их применения. Исследователи отмечают, что с течением времени некоторые разновидности преступной активности в сфере компьютерной информации

будут направлены не только на информационную безопасность, но и на иные социально значимые сферы – жизнь, здоровье, честь и достоинство личности и т.д. [5]. Указанное особенно актуально для уголовно-правового регулирования сферы функционирования технологий блокчейна, которые, с одной стороны, весьма охотно применяются добросовестными субъектами хозяйствования для обеспечения прозрачности деятельности в различных сферах, в том числе, в здравоохранении, при организации голосования, в финансовом секторе, при обработке персональных данных, а также в процессе лицензирования, выдачи патентов и т.п., а с другой стороны, характеризуются применением особых способов шифрования данных, позволяют обеспечивать анонимность пользователей теневых виртуальных площадок Darknet, связаны с получением незаконной прибыли в особо крупных размерах (с учётом курса криптовалют) и затрудняют возврат незаконно изъятых цифровых активов или данных (невозможность возврата транзакций).

Переходя к более детальному анализу обозначенных проблем, необходимо отметить нормативно-правовое регулирование в сфере цифровых активов. Первостепенным нормативно-правовым актом выступает Федеральный закон "О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации" от 31.07.2020 N 259-ФЗ, который ввел в правовое поле понятие цифровой валюты, однако не признал ее законным средством платежа [2]. Уголовный закон, в свою очередь, апеллирует понятием имущество, применительно к ст. 158 УК РФ, где под хищением понимается совершенное с корыстной целью противоправное безвозмездное изъятие и обращение чужого имущества в пользу виновного или других лиц. Возникает закономерный вопрос о том, может ли криптовалюта, не имеющая материальной формы и существующая исключительно в виде записей в распределенном реестре, выступать предметом хищения в его традиционном понимании. Судебная практика последних лет показывает нам, что уголовное судопроизводство все чаще признает криптовалюту имуществом для квалификации хищений, что в свою очередь нашло отражение в позициях Верховного Суда РФ.

Особую сложность в квалификации представляет разграничение хищений криптовалюты, совершаемые путем неправомерного доступа к компьютерной информации, предусмотренного ст. 159.6 УК РФ. Когда виновный получает доступ к закрытому ключу потерпевшего посредством вредоносного программного обеспечения либо фишинговых ресурсов и переводит цифровые активы

на подконтрольные ему адреса, правоприменители сталкиваются с необходимостью выбора между квалификацией содеянного как кражи, как компьютерного мошенничества либо как совокупности указанных деяний с преступлениями, предусмотренными главой 28 УК РФ.

Постановление Пленума Верховного Суда РФ от 30.11.2017 N 48 (ред. от 15.12.2022) "О судебной практике по делам о мошенничестве, присвоении и растрате" разъяснил, что вмешательство в функционирование средств хранения, обработки и передачи компьютерной информации образует признак объективной стороны мошенничества в сфере компьютерной информации. Однако, применяя данное положение к криптовалюте, подобное разъяснение не всегда позволяет решить вопрос однозначно, так как сама природа транзакций в распределенном реестре предполагает, что виновный не вмешивается в работу системы, а использует ее штатный функционал, неправомерно завладевая средством доступа [3].

На наш взгляд, отдельного внимания заслуживает проблема определения места и времени совершения преступления, сопряженных с технологией блокчейн, что в свою очередь имеет принципиальное значение для установления территориальной подследственности и подсудности уголовных дел. Составляющие распределительного реестра могут размещаться в различных государствах, потерпевший и виновный могут находиться в различных зонах оперативного обслуживания, а транзакция может проходить через звенья цепи, разбросанных по всему миру, по этой причине определение территориальности преступления значительно затрудняется. Изучая правоприменительную практику, можно отметить, что в данный момент, зачастую складывается подход, согласно которому, местом совершения преступления признается местонахождение потерпевшего в момент утраты контроля над цифровыми активами, однако точного закрепления данный подход в настоящее время не получил, что порождает множество процессуальных споров. Дополнительной сложностью на наш взгляд выступает оценка размера ущерба. Это связано с тем, что курс криптовалют отличается высокой финансовой изменчивостью и стоимость активов на момент хищения и возбуждения уголовного дела может в существенной мере различаться. Исходя из этого, представляется обоснованной позиция, в соответствии с которой стоимость криптовалюты должна определяться на момент совершения преступления исходя из рыночных корректировок на крупных мировых площадках.

Подводя итог проведенному исследованию, необходимо обратить внимание, что проблемы

квалификации преступлений, связанные с технологией блокчейн имеют множество проблемных вопросов, связанных с объективной сложностью самой технологии и несовершенством действующего законодательства в данной области. Для решения поставленных проблем, считаем целесообразным предложить внести изменения в уголовный кодекс Российской Федерации, путем признания цифровой валюты имуществом для квалификации преступлений против собственности. Помимо этого, необходимо повышать уровень технической подготовки правоохранительных органов, а также внедрять специализированные программные средства анализа технологий блокчейн в деятельность органов предварительного следствия.

Список литературы:

[1] Уголовный кодекс Российской Федерации // Собрание законодательства Российской Федерации, 1996, № 25, ст. 2954.

[2] Федеральный закон от 31.07.2020 № 259-ФЗ (в ред. от 15.12.2025) «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства Российской Федерации. — 2020. — № 31 (часть I). — Ст. 5018.

[3] Постановление Пленума Верховного Суда РФ от 30.11.2017 N 48 (ред. от 15.12.2022) "О судебной практике по делам о мошенничестве, присвоении и растрате" // СПС КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_283918/ (дата обращения: 18.07.2026).

[4] Верховный Суд: криптовалюта все чаще становится объектом преступных посягательств // Верховный Суд Российской Федерации. URL: https://www.vsrp.ru/press_center/mass_media/34394/ (дата обращения: 18.07.2026).

[5] Рускевич Е.А., Мельников А.С. Об

отдельных проблемах квалификации создания, использования и распространения вредоносных компьютерных программ // Российский следователь. 2018. № 8. С. 60-64.

[6] Глушков В. А. Криптовалюта как предмет преступления по законодательству Российской Федерации // Цифровое право. 2025. № 1. С. 56-64.

References:

[1] Criminal Code of the Russian Federation // Collection of Legislation of the Russian Federation, 1996, No. 25, Art. 2954.

[2] Federal Law No. 259-FZ of July 31, 2020 (as amended on December 15, 2025) "On digital financial assets, digital currency and amendments to certain legislative acts of the Russian Federation" // Collection of Legislation of the Russian Federation. — 2020. — No. 31 (part I). — St. 5018.

[3] Resolution of the Plenum of the Supreme Court of the Russian Federation dated November 30, 2017 N 48 (as amended on December 15, 2022) "On judicial practice in cases of fraud, misappropriation and embezzlement" // SPS ConsultantPlus. URL: https://www.consultant.ru/document/cons_doc_LAW_283918/ (date of access: 07.18.2026).

[4] Supreme Court: cryptocurrency is increasingly becoming the target of criminal attacks // Supreme Court of the Russian Federation. URL: https://www.vsrp.ru/press_center/mass_media/34394/ (access date: 07/18/2026).

[5] Ruskevich E.A., Melnikov A.S. On certain problems of qualifying the creation, use and distribution of malicious computer programs // Russian investigator. 2018. No. 8. P. 60-64.

[6] Glushkov V. A. Cryptocurrency as a subject of crime under the legislation of the Russian Federation // Digital Law. 2025. No. 1. P. 56-64.

