УДК 338.2
DOI 10.26118/2782-4586.2025.74.25.068

Смирнов Сергей Андреевич
Владимирский государственный университет имени
Александра Григорьевича и Николая Григорьевича Столетовых

Меченая криптовалюта и риски её приёма: правовой анализ и проверка перед сделкой

Аннотация. В статье рассматривается феномен «меченой» криптовалюты – цифровых активов, ранее вовлечённых в противоправную деятельность и потому помеченных в блокчейне как **«грязные»**. Указаны риски принятия таких активов в качестве платежа, включая технические сложности и юридические последствия для получателя. Проанализированы современные инструменты мониторинга криптотранзакций (Chainalysis, TRM Labs, Elliptic и др.), с помощью которых регуляторы, биржи и пользователи выявляют *«испачканные»* монеты. Предложен практический алгоритм предварительной проверки криптовалюты на «чистоту» перед заключением сделки с использованием открытых данных блокчейна и AML-сервисов. Отдельное внимание уделено российским реалиям: отсутствию полноценного правового оборота криптовалют, усиливающемуся контролю за P2P-операциями и планируемым санкциям за криптоплатежи внутри страны. В заключении сформулированы выводы и рекомендации для бизнеса и частных лиц по минимизации рисков, связанных с **меченой криптовалютой**.

Ключевые слова: меченая криптовалюта, отмывание денег, комплаенс и AML, блокчейн-аналитика, криптовалютные риски, проверка криптоактивов.

Smirnov Sergey Andreevich
Vladimir State University named after Alexander Grigorievich and
Nikolay Grigorievich Stoletov

Labeled cryptocurrency and the risks of its acceptance: legal analysis and verification before the transaction

Annotation. The article examines the phenomenon of "labeled" cryptocurrencies – digital assets that were previously involved in illegal activities and therefore marked as "dirty" in the blockchain. The risks of accepting such assets as payment are indicated, including technical difficulties and legal consequences for the recipient. Modern cryptotransaction monitoring tools (Chainalysis, TRM Labs, Elliptic, etc.) are analyzed, with the help of which regulators, exchanges and users identify "dirty" coins. A practical algorithm is proposed for pre-checking cryptocurrencies for "purity" before concluding a transaction using open blockchain data and AML services. Special attention is paid to Russian realities: the lack of a full-fledged legal turnover of cryptocurrencies, increasing control over P2P transactions and planned sanctions for crypto payments within the country. In conclusion, conclusions and recommendations are formulated for businesses and individuals to minimize the risks associated with labeled cryptocurrencies.

Keywords: labeled cryptocurrency, money laundering, compliance and AML, blockchain analytics, cryptocurrency risks, verification of crypto assets.

Стремительный рост использования криптовалют сопровождается появлением феномена «меченых» либо «грязных» монет – цифровых активов, которые оказались связанными с незаконной деятельностью и были помечены как таковые в цепочке транзакций. По оценкам аналитиков, объём *«испачканных»* криптоактивов неуклонно увеличивается. Так, на российском рынке в первой половине 2024 г. из ~2,3 трлн ₽

операций около 112 млрд ₽ были прямо или косвенно связаны с незаконными источниками[1, с. 2]. Более того, сохраняется тенденция, при которой в ближайшие годы почти вся оборотная криптовалюта рискует получить статус «грязной», что сделает её использование крайне проблематичным[1, с. 2]. Подобные прогнозы подчёркивают актуальность темы: получение платежа в меченой криптовалюте может повлечь серьёзные последствия для добросовестного участника сделки, от финансовых потерь до правовой ответственности.

Особенно остро проблема стоит в условиях усиления регулирования. Международные организации (FATF и др.) требуют соблюдения принципов *AML/CFT* при обращении криптоактивов, включая т. н. правило «Travel Rule», обязывающее идентифицировать отправителей и получателей переводов[14, с. 3]. Банки и биржи внедряют системы *Know-Your-Transaction* (KYT) для автоматического выявления сомнительных поступлений. В результате даже отдельные монеты, прежде считавшиеся взаимозаменяемыми, начинают обладать *«репутацией»* – негативной меткой происхождения. Это приводит к размыванию базового свойства криптовалют – их полной fungibility (взаимозаменяемости): на практике «грязная» монета отличается от «чистой» тем, что первая может быть отклонена рынком или изъята регулятором[3, с. 2].

Правовой аспект также предельно важен. В Российской Федерации с 2021 г. законодательно запрещено использование криптовалют как средства платежа (ст. 14 Закона № 259-ФЗ)[11, с. 1]. В 2025 г. ожидается усиление ответственности: планируется ввести штрафы от 100 тыс. ₽ (для граждан) до 1 млн ₽ (для компаний) за расчёты в цифровой валюте, а сами незаконно использованные криптоактивы подлежат конфискации[6, с. 2]. Таким образом, любое лицо, принимающее криптовалюту в счёт оплаты, уже рискует столкнуться с санкциями государства. Если же принятые монеты окажутся ещё и *мечеными* – т.е. связанными с преступлением, – риск возрастает многократно. Данная работа сфокусирована на комплексном разборе этих рисков – технических и правовых – и на практических мерах их предотвращения.

Единого строгого определения *меченой (помеченной) криптовалюты* в нормативных актах пока не существует[1, с. 1]. На практике под этим термином понимаются криптомонеты, участвовавшие в противозаконных операциях либо имеющие иное сомнительное происхождение, вследствие чего их адреса или транзакции были занесены в специальные списки мониторинговых систем. Иначе говоря, меченая (она же *«грязная»* или *«запачканная»*) криптовалюта – это актив, ранее украденный у законных владельцев, полученный мошенническим путём, использованный для оплаты противозаконных товаров/услуг (например, на даркнет-маркетплейсах) либо прошедший через схемы отмывания денег[8, с. 1][9, с. 1]. Типичные примеры – биткоины, побывавшие в кошельках наркоторговцев или террористов, *«замешанные»* в выплате выкупа вымогателям, либо полученные из взломанных криптобирж. Попадая в поле зрения правоохранительных органов, такие средства отслеживаются и маркируются: известные подозрительные адреса заносятся в базы данных, что позволяет автоматически видеть движение этих монет по блокчейну[1, с. 1]. В результате любая новая транзакция с участием *меченых* монет будет помечена и может привлечь внимание как аналитических систем, так и субъектов финансового мониторинга.

Следует отметить, что степень «испорченности» криптовалюты не всегда оценивается однозначно. В целом под сомнительными (*risky*) понимаются активы, имеющие в своей истории хотя бы один переход через адрес, связанный с преступлением[8, с. 1]. Однако между *явно криминальными* монетами и относительно чистыми есть градации риска. Современные AML-системы присваивают транзакциям и кошелькам баллы риск-скоринга на основе ряда факторов: близость к известным «тёмным» сервисам (игорные сайты, криптомиксеры, даркнет-биржи), участие в схемах *peel chain* (многоступенчатого расщепления средств), а также попадание под финансовые санкции или в адреса-хранилища украденных средств[2, с. 1][3, с. 3]. Например, адрес, напрямую получивший платеж с

кошелька хакера, будет отмечен как High Risk с категорией «специализированная кража», если же сомнительный перевод находился тремя «ходами» ранее, риск может считаться умеренным. Единых стандартов оценки пока нет, хотя регуляторы некоторых стран издают рекомендации по «окрашиванию» подозрительных цепочек транзакций[1, с. 1–2]. По сути, глобальные аналитические компании сами формируют профессиональные стандарты разметки, присваивая «цветовую» категорию практически каждому адресу в блокчейне[1, с. 2]. Как метко замечено экспертами, к 2024 г. практически вся обращающаяся криптовалюта уже так или иначе размечена: какая-то – хорошо, какая-то – плохо[1, с. 2]. Поэтому для участников рынка всё более актуально понятие «криптогигиены» – умения отличать чистые монеты от потенциально грязных и избегать взаимодействия с последними[1, с. 3].

Технические риски и блокировка средств. Принятие платежа в меченой криптовалюте чревато, прежде всего, риском утраты доступа к этим средствам. Крупнейшие централизованные криптобиржи уже давно внедрили механизмы проверки на входящие транзакции и автоматически замораживают поступления, если их источник находится в *чёрных списках*[8, с. 1–2]. Получив на биржевой счёт *«испачканные»* монеты, пользователь рискует почти мгновенно попасть под блокировку со стороны службы комплаенса площадки[4, с. 3]. Разблокирование аккаунта возможно, но потребует длительной процедуры: пользователю придётся предоставлять бирже доказательства законности происхождения активов, вести переписку с поддержкой, и нет никакой гарантии успеха[9, с. 2]. В худшем же случае аккаунт и средства на нём будут заморожены навсегда, без права восстановления[9, с. 2]. Подобные инциденты – не редкость: специалисты отмечают случаи, когда счёт добропорядочного клиента блокировался сразу после пополнения, если в его кошельке обнаруживались подозрительные активы[9, с. 1]. Достаточно единственной сомнительной записи в истории операций, чтобы *«испачкать»* не только конкретный токен, но и все остальные, хранящиеся с ним на одном кошельке[9, с. 1–2]. То есть, если на ваш адрес пришла некоторая сумма от нелегального источника, всё остальное содержимое адреса также считается скомпрометированным.

Более того, «окраска» криптовалюты может распространяться ретроспективно. В отличие от фиатных денег, где «прошлое» купюры практически отследить невозможно, в блокчейне новая информация о противоправных действиях способна *задним числом* сделать ранее чистые монеты грязными[4, с. 4]. Например, если через несколько месяцев после сделки выяснится, что в её цепочке полугодовой давности фигурировал кошелёк, принадлежащий мошенникам, все звенья цепи, в том числе финальный получатель, получат соответствующую метку риска[4, с. 4]. Эксперты поясняют: в большинстве случаев аналитические системы распространяют риск вперед по хронологии (от свежего преступления к новым адресатам средств), но при запоздалом выявлении инцидента разметка производится и в обратном направлении[4, с. 4]. Таким образом, даже если на момент получения платеж был «чист», со временем он может оказаться меченым – если только это не совсем *«первичная»* монета, полученная напрямую от майнера[1, с. 3]. (Новые монеты, добытые майнингом, априори считаются чистыми, поэтому на них даже возник премиальный спрос: ряд покупателей готовы платить за свежедобытые биткоины чуть больше рыночной цены[1, с. 3].)

Правовые последствия и кейсы. Ещё более серьёзны юридические риски, сопряжённые с получением «грязных» криптоактивов. Хотя в российском законодательстве пока нет норм, прямо устанавливающих ответственность за владение криптовалютой преступного происхождения, применимы общие положения о соучастии в отмывании доходов, приобретении имущества, добытого преступным путём, и т. п. Так, Федеральный закон № 115-ФЗ «О противодействии легализации…» обязывает финансовые организации блокировать сомнительные операции и сообщать о них в Росфинмониторинг[10, с. 5]. Банки активно используют это право: если клиент массово проводит P2P-сделки по покупке/продаже криптовалюты, банк может заподозрить его в нарушении 115-ФЗ и

заморозить счёт, мотивируя это борьбой с отмыванием денег[13, с. 3]. За последние годы известны прецеденты, когда добросовестные на первый взгляд криптотрейдеры сталкивались не только с блокировками, но и с уголовными делами. Показателен первый в России приговор за P2P-сделку с криптой: в 2023 г. суд приговорил частного трейдера к 2 годам лишения свободы условно за пособничество в мошенничестве[7, с. 1]. В данной истории молодой человек продавал криптовалютные «коды» на неофициальной бирже и получил оплату на свой банковский счёт от третьих лиц, как оказалось – похищенные ими у жертвы телефонного мошенничества[7, с. 2]. Следствие квалифицировало такие действия как участие в преступной схеме (по сути, отмывание краденых денег), несмотря на заявления обвиняемого о незнании происхождения средств[7, с. 1–2]. Этот случай показал, что любые граждане, вовлечённые в неформальный обмен криптовалют, не застрахованы от уголовно-правовых последствий: правоохранительные органы уже научились собирать доказательства и по таким эпизодам[7, с. 2]. Юристы ожидают роста числа подобных дел, особенно в отсутствие специальных норм о регулировании криптообмена[7, с. 3].

Кроме уголовных рисков, имеются и административные. Как отмечалось, в России планируется прямое наказание за расчёты в криптовалюте – штраф и конфискация цифровых денег[6, с. 1–2]. Причём регулятор подчёркивает, что конфисковываться будет именно та криптовалюта, которая использовалась незаконно в качестве платёжного средства[6, с. 3]. Иными словами, если компания или гражданин примет оплату в биткоинах, такие биткоины могут быть изъяты властями как *«неправомерно используемые»*. Таким образом, сам по себе факт приёма криптоактива как оплаты уже закладывает конфискационный риск. А если при этом выяснится, что полученные монеты ранее участвовали в преступлении (например, это похищенные хакерами средства), их получатель теоретически может быть привлечён и как фигурант дела об отмывании денег. Даже за рубежом, где расчёты в криптовалюте легальны, законом предусмотрена ответственность за подобные действия. Например, в США лица, управляющие криптомиксерами или сознательно пытающиеся «очистить» монеты посредством смешивания транзакций, привлекаются к тяжким уголовным преступлениям и многомиллионным штрафам[9, с. 3]. В августе 2022 г. Минфин США внёс в санкционный список популярный сервис Tornado Cash, а ФБР добилось ареста его предполагаемого разработчика по обвинению в содействии отмыванию ~$7 млрд криптовалют[8, с. 2]. В итоге сотни пользователей, которые когда-либо взаимодействовали с Tornado (даже случайно, получив *«пыли»* на кошелёк), потеряли доступ к своим средствам – децентрализованные протоколы Aave и Uniswap блокировали такие адреса, а централизованные биржи замораживали аккаунты клиентов, имевших перевод через миксер[8, с. 2]. Этот случай продемонстрировал, что контакт с мечеными монетами может нанести ущерб даже постфактум: транзакция, совершённая в прошлом без злого умысла, способна позднее привести к санкциям против кошелька.

Репутационные и экономические риски. Наконец, не стоит упускать из виду и репутационную сторону. Если предприятие (например, криптообменник или торговая площадка) замечено в приёме нелегальных средств, оно рискует попасть в *«чёрные списки»* финансовых регуляторов. Так, в 2022 г. американский OFAC включил в санкционный список российскую биржу Garantex, обвинив её в обслуживании операций российского киберпреступного сообщества[2, с. 2][11, с. 3]. После этого любая криптовалюта, прошедшая через кошельки Garantex, стала маркироваться аналитиками как условно неблагонадёжная[11, с. 2]. Представители Garantex заявляли о необоснованности такого обобщения, указывая на ошибки разметки адресов, однако факт остаётся фактом: любые криптоактивы, связанные с подсанкционными сервисами, зачастую автоматически получают негативную окраску[11, с. 2–3]. Более того, крупные международные биржи и даже крипто-кошельки (например, встроенный кошелёк Wallet в мессенджере Telegram) внедрили правила, по которым автоматически блокируют пользователей, если те получили прямой перевод с адреса, фигурирующего в санкционных перечнях[11, с. 3]. То есть *даже*

однократная транзакция с *мечеными* средствами способна отсечь субъект от значимой части криптоинфраструктуры. С экономической точки зрения, владелец таких монет сталкивается с падением ликвидности актива: реализовать *«запятнанный»* биткоин или USDT по рыночной стоимости практически невозможно, его придётся либо продавать с дисконтом на сомнительных площадках, либо тратить вне официальной финансовой системы. Всё это означает прямые убытки и для бизнеса, и для частного инвестора.

Для выявления меченых криптовалют разработан целый класс AML-сервисов блокчейн-аналитики. К их числу относятся прежде всего американские компании *Chainalysis, Elliptic, TRM Labs*, а также ряд других (CipherTrace, Crystal Blockchain, Scorechain и т. д.)[2, с. 1][14, с. 1][14, с. 5]. Эти организации на постоянной основе мониторят блокчейн-сети (Bitcoin, Ethereum и многие другие) в поисках нелегальной активности и аккумулируют обширные базы метаданных по адресам. Каждому кошельку присваиваются метки (теги) и уровень риска. Например, адрес может быть помечен как Exchange (биржевой), Darknet Market (относящийся к площадке в теневой сети), Mixer (миксер-транзакция), Stolen Coins (адрес хранения похищенных средств), Scam (мошеннический проект) и т. п.[14, с. 1–2]. Одновременно системе присваивают числовой риск-балль – обычно по шкале 0–100 или низкий/средний/высокий риск – показывающий, насколько тесно данный объект связан с противоправными схемами. Как отмечалось, именно на данные таких аналитических компаний опираются почти все посредники, осуществляющие проверку криптовалют на «чистоту»[2, с. 1]. И крупные биржи, и специализированные AML-провайдеры интегрируют API Chainalysis, TRM и им подобных для сканирования входящих транзакций в режиме реального времени[2, с. 1]. Например, система Chainalysis KYT (*Know Your Transaction*) позволяет бирже отсеивать депозиты с нежелательных адресов и тем самым предотвращать пополнение счёта «грязными» монетами[1, с. 3]. Регуляторы также активно используют эти инструменты: по данным самой Chainalysis, около 65% её доходов приходится на госконтракты с правоохранительными органами по всему миру[2, с. 1].

Помимо крупных международных игроков, существуют и локальные сервисы для частных пользователей. В РФ известны платформы *AMLBot, GetBlock, Merkle Science*, биржа Matbea с функцией AML и др.[1, с. 3]. Они предоставляют услуги онлайн-проверки: достаточно указать интересующий адрес кошелька или хэш транзакции, после чего пользователь получит отчёт о их *«репутации»* – списке выявленных меток и общем рисковом статусе (как правило, в процентах или уровнях от Low до Critical). Многие такие сервисы доступны через удобных ботов в мессенджерах, базовая проверка может быть бесплатной или требовать небольшую плату, более глубокий анализ – по подписке. Алгоритмы у разных провайдеров могут различаться, однако все они опираются на упомянутые глобальные базы данных. В результате вероятность расхождения оценок невелика: если адрес был засвечен в криминальных схемах, об этом узнают сразу во всех системах.

Отдельно стоит упомянуть инструменты государственного контроля. В отсутствие доступа к иностранным API некоторые страны развивают собственные аналитические модули. Так, российский Росфинмониторинг с 2021 г. создает систему «Прозрачный блокчейн» для отслеживания криптотранзакций[5, с. 1]. Пилотные испытания уже проведены: к сервису подключены свыше 12 тыс. сотрудников правоохранительных органов РФ и ряда зарубежных стран СНГ[5, с. 2]. В 2023 г. началось тестирование «Прозрачного блокчейна» российскими банками, а к концу 2025 г. планируется полноценное внедрение модуля в их внутренних системах[5, с. 1]. Фактически банки получат возможность автоматически выявлять связи операций клиента с криптовалютой и присваивать таким клиентам повышенный риск-профиль[5, с. 3]. Ожидается, что это поможет эффективнее раскрывать случаи отмывания денег через криптообмен. Представители Росфинмониторинга отмечают значительный рост *выявленных* подозрительных операций, связанных с криптой: по сравнению с 2022 г. количество

соответствующих уголовных дел в 2023 г. увеличилось в разы[5, с. 4]. Это подтверждает, что механизмы маркировки «грязных» средств уже активно работают и в российских условиях.

На основе вышеизложенного можно предложить прикладной алгоритм действий для продавца или посредника, желающего убедиться в «чистоте» принимаемых криптоактивов до заключения сделки:

1. Запрос информации о платеже. Ещё на этапе переговоров с контрагентом следует выяснить, откуда именно он намерен перевести криптовалюту. Идеальный вариант – если средства хранятся на крупной бирже, соблюдающей KYC/AML (Binance, OKX и т. п.), либо если это новые монеты из майнинга. В таком случае риск минимален[4, с. 2][1, с. 3]. Если же контрагент собирается платить с личного кошелька, обязательно запросите адрес этого кошелька и (желательно) TXID будущей транзакции заранее[1, с. 3][4, с. 3]. Добросовестный участник не станет скрывать эти данные. Напротив, отказ предоставить адрес или внятно рассказать о происхождении криптовалюты – тревожный сигнал, при котором стоит серьезно задуматься о продолжении сделки[4, с. 3].

2. Первичная открытая проверка. Получив адрес отправителя, выполните самостоятельный поиск по открытым блокчейн-обозревателям и базам. Например, на сайте blockchain.com или Blockchair можно ввести адрес и проследить историю его транзакций. Обратите внимание на аномальные признаки: недавно созданный «пустой» кошелёк без истории (мог быть сгенерирован специально для разовой выплаты), либо наоборот – очень длинную цепочку микропереводов (возможно, результат работы миксера). Если видны переводы с известных бирж на адрес контрагента, это скорей плюс. Но если в истории засвечены сервисы с сомнительной репутацией (даркнет-площадки, азартные игры, Mixer-транзакции) – велик риск, что монеты меченые. В открытом доступе существуют списки известных преступных адресов (например, ресурсы Bitcoinabuse, Cryptoscamdb и др.), их тоже можно пробить вручную по предоставленному кошельку.

3. Использование специализированного AML-сервиса. Наиболее важный этап – формальная проверка через один из описанных сервисов блокчейн-аналитики. Многие из них (AMLBot, Crystal Blockchain и др.) имеют web-интерфейсы с интуитивно понятным отчётом. Достаточно вставить адрес – и система выдаст его риск-профиль: например, *“Risk Score: 5 (Low Risk)”* или *“45% риск (высокий), категории: Darknet Market 20%, Scam 10%…”* и тому подобное. Рекомендуется делать скриншот или выгружать PDF-отчёт – на случай возможных споров или для собственного архива. Если сервис показывает низкий риск (например, <= 5%) и не выявляет значимых тегов, можно считать проверку пройденной. Высокий же риск (от 50% и выше) – однозначный повод отказаться от приёма такого платежа[4, с. 3]. Промежуточные случаи потребуют анализа: некоторые системы считают рискованным, скажем, любой адрес, взаимодействовавший с незамеченным ранее миксером, хотя прямого криминала там может не быть. Поэтому, если отчёт неоднозначен, целесообразно *перепроверить через альтернативный сервис* или запросить у контрагента дополнительные подтверждения происхождения средств.

4. Принятие решения и оформление сделки. На основании собранной информации принимается решение о продолжении или отмене сделки. Если адрес числится в чёрных списках (санкционных или связанных с преступностью), сделку лучше отменить безусловно. Практикующие юристы советуют не рисковать: *«Время анонимных авантюристов, избегающих всяческой верификации, уходит в прошлое»*[4, с. 3]. Если же проверка не выявила ничего подозрительного, сделку можно проводить, однако с соблюдением общих мер осторожности. По возможности зафиксируйте факт проведения проверки (например, сохраните ID запроса в AML-сервисе или полученный отчёт). Стоит также убедиться, что итоговое получение средств происходит под вашим контролем. Желательно использовать новый адрес для каждой проверенной сделки, чтобы свести к нулю шанс смешения чистых и потенциально грязных монет на одном кошельке.

5. Дополнительные шаги для бизнеса. Если вы представляете организацию, регулярно принимающую криптоплатежи (например, онлайн-продавца), имеет смысл интегрировать автоматизированные решения. На рынке существуют API, позволяющие встраивать проверку транзакций в реальном времени в собственную инфраструктуру. Бизнесу, как говорится, самому *«диджитал-гигиену»* соблюдать мало – важно не подвергать риску своих клиентов[1, с. 3–4]. Поэтому рекомендуется выстроить систему комплаенса: регистрировать значимые криптооперации, проверять крупные поступления через несколько независимых источников, обучать сотрудников распознавать красные флаги. Эти меры помогут избежать не только прямых потерь от возможной блокировки средств, но и защитят деловую репутацию компании.

Приведённый алгоритм, конечно, не гарантирует абсолютной защиты – как уже отмечалось, даже самая тщательная проверка не исключает ситуаций, когда монета *«очерняется»* спустя время. Тем не менее соблюдение данных шагов существенно снижает вероятность столкновения с меченой криптовалютой и демонстрирует добросовестность участника оборота.

Ситуация с мечеными криптоактивами в России осложняется общими ограничениями на обращение криптовалют. Внутренний криптовалютный рынок де-юре находится вне закона: Закон № 259-ФЗ прямо запрещает приём цифровой валюты в оплату товаров, работ или услуг[11, с. 1]. Несмотря на это, в стране сформировался обширный серый сегмент P2P-торговли, особенно выросший после 2022 г., когда из-за санкций были ограничены операции россиян на иностранных биржах[13, с. 2]. Многие граждане переключились на неформальный обмен криптовалют *«с рук»*, используя телеграм-чаты, одноранговые платформы крупных бирж и услуги полулегальных обменников[13, с. 1][13, с. 3]. Такой формат позволяет обходить банковские запреты, но связан с повышенными рисками – в первую очередь, риском наткнуться на мошенников или «грязные» деньги.

Типичная схема мошенничества в P2P-обмене – когда злоумышленник под видом покупателя переводит продавцу криптовалюты деньги, похищенные у третьих лиц (например, со счета жертвы фишинга), а затем исчезает. В итоге на банковском счёте продавца оказываются украденные средства, и уже *он* становится фигурантом расследования[7, с. 2]. Как упоминалось, такой случай произошёл с трейдером, продававшим коды Garantex: банк заблокировал его карту, а позже суд признал его виновным в получении похищенных денег[7, с. 2]. Примечательно, что под ударом оказывается прежде всего продавец, принимающий оплату. Казалось бы, сам он никого не обманывал – но закон расценивает его как *«невольного соучастника»* отмывания[13, с. 4]. Эксперты подчёркивают: при продаже криптовалюты за фиат наиболее опасен именно риск стать таким невольным участником противоправной схемы[13, с. 4]. Ни один пользователь P2P не застрахован, поскольку до момента зачисления денег на счёт он не знает, от кого именно они поступят и легален ли их источник[13, с. 4].

Банковская система РФ реагирует на подобные угрозы жёстко. С июля 2024 г. российские банки обязаны на 2 дня приостанавливать переводы, если получатель фигурирует в базе данных подозрительных получателей ЦБ РФ[13, с. 1][13, с. 2]. Такая база пополняется, в частности, на основании заявлений в МВД о мошенничестве: достаточно, чтобы жертва указала реквизиты, куда злоумышленники вывели её деньги, – и эти реквизиты попадают в реестр[13, с. 2]. Банку затем предписано блокировать все операции по карточке и онлайн-банкингу данного клиента[13, с. 2]. В результате человек внезапно оказывается отрезан от собственных денег на всех счетах. И попасть в такую ситуацию может любой участник криптообмена, заключающий P2P-сделку с неизвестным контрагентом[13, с. 3]. Пока законодательство не урегулировало специальный порядок для криптовалютных обменов, банки и надзорные органы действуют в рамках общих норм о противодействии отмыванию средств – а они, как видим, весьма строгие.

Другой аспект – международные санкции, распространяющиеся на российский криптосектор. Западные аналитические компании фактически маркируют всё, что связано

с российскими адресами, как *High Risk*. Отмечено, что любая криптовалюта, прошедшая через российский сервис (особенно попавший под санкции), автоматически получает негативную метку в их системах[11, с. 2]. Даже средства, не имеющие отношения к криминалу, но просто связанные с РФ, могут быть помечены как *«подсанкционные»*. Представители российского парламента прямо заявляют: пока сохраняются геополитические ограничения, все цифровые активы, так или иначе связанные с Российской Федерацией, при выходе на глобальный рынок будут окрашены как подсанкционные[5, с. 4]. В условиях криптовалют это проявляется тем, что иностранные биржи вводят ограничения для россиян, блокируют переводы из российских обменников, а зарубежные контрагенты могут требовать подтверждений, что монеты не связаны с РФ. Таким образом, для российских пользователей и компаний проблема *«чистоты»* криптовалют осложняется политическими факторами.

В ответ на вызовы власти РФ разрабатывают особый правовой режим для ограниченного использования криптовалют во внешнеторговых расчетах (так называемый экспериментальный правовой режим, ЭПР)[6, с. 3]. Предполагается, что в рамках ЭПР отдельные уполномоченные участники смогут применять цифровые валюты для международных платежей, несмотря на внутренний запрет. Однако даже ЦБ РФ подчёркивает, что параллельно необходимо ужесточить ответственность за использование крипты *внутри страны*[6, с. 3–4]. Иными словами, курс регулятора ясен: недопущение свободного хождения криптовалют в экономике и максимальное пресечение их анонимного обмена. Это значит, что пространство для нелегитимного оборота будет и дальше сужаться, а контроль за «мечеными» монетами – усиливаться.

Выводы. Исследование показало, что *меченая криптовалюта* из абстрактного понятия постепенно превратилась в фактор реального правового и финансового риска. Монеты, связанные с преступностью или санкциями, выявляются всё более эффективно – как частными аналитическими компаниями, так и государственными органами. Приём в платёж таких активов может привести к блокировке средств, потере деловой репутации и даже привлечению к ответственности за вовлечение в отмывание доходов. В условиях, когда почти каждая десятая транзакция на рынке несёт в себе *«грязный»* след[1, с. 2], игнорировать проблему криптогигиены уже невозможно.

Для бизнеса и рядовых пользователей на первый план выходит необходимость выстроить превентивные меры. Практические рекомендации можно сформулировать следующим образом:

- Не принимать криптовалюту без проверки. Любой входящий криптоплатёж должен рассматриваться с точки зрения его истории. Желательно заранее знать, откуда придут средства – с биржевого ли аккаунта, нового ли адреса и т.д. От сомнительных сделок (анонимные обменники, неизвестные клиенты без репутации) разумнее воздержаться[4, с. 2–3].
- Пользоваться доступными AML-инструментами. В распоряжении участников рынка есть как минимум базовые сервисы для онлайн-проверки адресов. Затраты на такую проверку несоизмеримо малы по сравнению с потенциальными потерями от приема грязных монет. Если сделка крупная, имеет смысл воспользоваться несколькими сервисами параллельно.
- Фиксировать результаты и коммуникацию. Если вы всё же решили принять криптовалюту после проверки, сохраните отчёт AML-сервиса, переписку с контрагентом (где он, например, подтвердил легальность средств). В случае проблем эти данные могут послужить доказательством вашей добросовестности.
- Соблюдать закон. Российским компаниям не следует сейчас принимать криптовалюту в оплату напрямую – до появления соответствующего легального режима. Граждане, прибегающие к P2P-сделкам, должны помнить об угрозе банковской блокировки и стараться хотя бы ограничивать суммы операций, работать через проверенные площадки с эскроу-защитой, не пользоваться счетами третьих лиц и т.п.

- Следить за обновлениями правил. Сфера крипторегулирования динамична. Требования комплаенса (например, правило Travel Rule) могут быть вскоре имплементированы и в российскую юрисдикцию. Появление лицензируемых криптобирж в РФ (ожидаемое по заявлению законодателей) также повлияет на практики проверки средств[11, с. 4]. Поэтому политика обращения с криптоактивами должна регулярно пересматриваться с учётом актуальных норм.

Подводя итог, можно констатировать: «меченая» криптовалюта – не гипотетическая, а вполне осязаемая проблема, уже влияющая на экономический и правовой оборот. Борьба с отмыванием денег в цифровой среде неизбежно делает криптовалюты «прозрачными», устраняя их былую анонимность. В таких условиях все участники – от крупных бирж до частных владельцев кошельков – вынуждены внедрять принципы финансовой чистоты. Пренебрежение ими способно привести к серьёзным негативным последствиям. Напротив, внимательное отношение к происхождению криптомонет, использование современных аналитических средств и соблюдение законодательства позволит максимально снизить риски и безопасно пользоваться преимуществами криптовалют в легитимном поле.

Список источников

1. РБК-Крипто. «Это будет трендом. Почему так важно заниматься криптогигиеной» (14.08.2024) – Откуда берётся грязная криптовалюта и как избежать встречи с ней, с. 1–4.
2. РБК-Крипто. Как криптовалюты попадают под санкции. Кто определяет «чистоту» кошельков (24.08.2024) – интервью и обзор AML-сервисов, с. 1–4.
3. РБК-Крипто. Что такое криптомиксеры. Чем они опасны для пользователей криптовалют – автор: Г. Осипов (09.09.2024), с. 2–3.
4. РБК-Крипто. Не стать участником «отмыва» криптовалют. Эксперты о рисках P2P-обмена (26.02.2025) – аналитическая статья, с. 2–4.
5. РБК (Финансы). Финразведка назвала сроки запуска сервиса криптопроверки в банках (21.02.2025) – заявление А. Лисицына (Росфинмониторинг), с. 1–4.
6. CNews. Россиян будут штрафовать за криптоплатежи от 100 тысяч до 1 миллиона рублей. Криптоактивы могут конфисковать (22.05.2025) – разбор законопроекта ЦБ РФ, с. 1–3.
7. Право.ru. Первый приговор за P2P-торговлю на криптобирже: мнение экспертов (09.03.2023) – кейс А. Евдокимова (биржа Garantex), с. 1–3.
8. Dev.by / Bubble. Избавиться от грязных монет сложно: почему опасно покупать меченую крипту (08.11.2022) – обзор случаев (санкции Tornado Cash и др.), с. 1–2.
9. Bits.media (PR). AMLSafe: чем рискуют владельцы «грязных биткоинов» и как не попасть в их число (26.01.2021) – экспертиза, с. 1–3.
10. Федеральный закон № 115-ФЗ от 07.08.2001 (ред. от 14.07.2022) «О противодействии легализации (отмыванию) доходов…». – Собр. законодательства РФ, 2001, № 33 (ч. I), ст. 3418.
11. Федеральный закон № 259-ФЗ от 31.07.2020 «О цифровых финансовых активах, цифровой валюте…». – Собр. законодательства РФ, 2020, № 31, ст. 5003.
12. Федеральный закон № 161-ФЗ от 27.06.2011 (ред. от 24.07.2024) «О национальной платёжной системе». – Собр. законодательства РФ, 2011, № 27, ст. 3872.
13. РБК-Крипто. США выдвинули обвинения против трёх россиян – операторов криптомиксеров (10.01.2024) – новости Минюста США, с. 1–2.
14. CryptoCloud (vc.ru). Криптовалюты и отмывание денег: как работает AML и почему это важно (26.03.2023) – обзор AML-инструментов, с. 1–5.
15. FATF. Guidance for a Risk-Based Approach to Virtual Assets and VASPs – Paris, Oct 2021, p. 13–20 (рекомендации по Travel Rule).

Сведения об авторе

Смирнов Сергей Андреевич, аспирант, Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, г. Владимир, Россия

Information about the author

Smirnov Sergey Andreevich, Postgraduate, Vladimir State University named after Alexander Grigorievich and Nikolay Grigorievich Stoletov, Vladimir, Russia