

ОРИГИНАЛЬНАЯ СТАТЬЯ



DOI: 10.26794/2408-9303-2023-10-3-86-93
УДК 657.631(045)
JEL M41, M42

Идентификация криптокошельков хозяйствующих субъектов для целей аудита

А.В. Тетюшин

Финансовый университет, Москва, Россия

АННОТАЦИЯ

Статья посвящена проблеме идентификации криптокошелька аудируемой организации, становящейся все более актуальной по мере развития криптоэкономики. В качестве объектов анализа выбраны компании, осуществляющие транзакции с криптоактивами, причем количество таких организаций постоянно растет. Более того, их акции обращаются на мировых финансовых рынках, а проблема аудита криптоактивов этих компаний становится одной из наиболее сложных среди традиционных аудиторских процедур. **Целью** исследования явилась разработка методики проведения аудиторских проверок для идентификации криптокошельков хозяйствующих субъектов. Автором работы приведены случаи опровержения признания криптоактивов вместе с необходимым перечнем действий аудитора; поднят вопрос «токсичных» криптоактивов, который в ближайшее время может стать большой проблемой для использующих их компаний – в рамках абсолютно легальной деятельности организации могут получить активы нелегального происхождения, которые впоследствии окажутся не признанными в рамках аудита и не войдут в суммарный объем их активов. На основе подобных случаев отвержения (опровержения принадлежности) были выработаны критерии признания криптоактивов. В статье предложена методика проведения необходимых аудиторских процедур, основанная на аудите активов посредством технологии блокчейн, позволяющей идентифицировать криптоактивы, работающие в блокчейнах как с наличием смарт-контрактов, так и без них. На данный момент она является достаточной для проведения процедуры признания любых криптоактивов аудируемой организации. В ходе исследования использовались **методы** синтеза, анализа, индукции и абдукции.

Ключевые слова: цифровые финансовые активы; цифровые валюты; криптовалюты; токен; аудит; блокчейн; токсичные криптоактивы; смарт-контракты; биткоин

Для цитирования: Тетюшин А.В. Идентификация криптокошельков хозяйствующих субъектов для целей аудита. Учет. Анализ. Аудит = *Accounting. Analysis. Auditing*. 2023;10(3):86-93. DOI: 10.26794/2408-9303-2023-10-3-86-93

ORIGINAL PAPER

Companies' Crypto wallets Identification for Auditing Purposes

A.V. Tetyushin

Financial University, Moscow, Russia

ABSTRACT

The article examines the problem of identifying the crypto wallet of an audited organization, which is becoming increasingly important and relevant as crypto economy develops. Companies that conduct transactions with crypto assets are chosen as the objects of the analysis. The number of these companies is constantly growing due to the promotion of a completely new sector of the economy – crypto economy. In addition, the shares of these companies are traded on global financial markets, and the problem of auditing their crypto assets is becoming one of the most difficult within traditional auditing procedures. The aim of the study was to develop an audit methodology for the identification of business entities' cryptocurrencies. The author of the paper presents the cases of refutation and rejection of the recognition of crypto assets along with the required list of auditor's actions. The article raises the issue of «toxic» crypto assets, which in the near future may become a big problem for companies using them. Companies within the framework of absolutely legal activities may receive assets of illegal origin, which may subsequently not be recognized as part of the audit and not be included in the total amount of the assets of the organization. Based on such cases of rejection (denial of ownership and affiliation), criteria for the recognition of crypto assets have been developed. As a result of the study, a methodology for conducting the necessary auditing procedures is proposed, based on the auditing of assets using

© Тетюшин А.В., 2023

blockchain technology, which makes it possible to identify crypto assets operating in blockchains both with and without the presence of smart contracts. The methodology at this point in time is sufficient to carry out the procedure for the recognition of any crypto assets of the audited organization. In the course of the study, methods of synthesis, analysis, induction and abduction were used.

Keywords: Digital financial assets; digital currencies; cryptocurrencies; token; auditing; blockchain; toxic crypto assets; smart contracts; bitcoin

For citation: Tetyushin A.V. Companies' crypto wallets identification for auditing purposes. *Uchet. Analiz. Audit = Accounting. Analysis. Auditing*. 2023;10(3):86-93. (In Russ.). DOI: 10.26794/2408-9303-2023-10-3-86-93

ВВЕДЕНИЕ

Представленное в статье исследование посвящено разработке методики проведения аудиторских процедур для идентификации криптокошельков¹ хозяйствующих субъектов, для чего прежде всего необходимо определиться с понятием «криптокошелек» и критериями его идентификации. Ускоряющаяся цифровизация современного мира оказывает положительное влияние на разные сферы человеческой деятельности, облегчая многие ее процессы: от взаимодействия с банками и до получения государственных услуг. Такое быстрое развитие технологий оказывает влияние и на достаточно консервативные области, например бухгалтерский учет, аудит, юриспруденция и другие — применяющаяся в них технология блокчейн позволяет значительно увеличить уровень информационной прозрачности организации [1–3].

В рамках данной статьи исследуется важная проблема, и, хотя ее нельзя отнести к глобальным (она, скорее всего, точечная), она актуальна и важна с позиции методологии и методики учета, поскольку, как и развитие цифровизации и криптоэкономики, создает новые риски для сферы учета и аудита. Отметим, что внедрение персональных компьютеров не создавало такого количества «серых зон», для которых отсутствовали методические указания, а всего лишь упростило и ускорило работу аудиторов [4, 5]. Однако развитие криптоэкономики, в том числе, криптоактивов, требует от сообщества бухгалтеров и аудиторов решения серьезных задач, начиная от теоретико-концептуальных и заканчивая организационно-техническими.

Еще 5–7 лет назад организаций, заинтересованных в отражении в своей отчетности криптоактивов

и, соответственно, в аудите их учета и раскрытия в ней, практически не было. В настоящее время на Американской фондовой бирже торгуется множество акций, связанных с криптоэкономикой, в результате чего ее развитие, а также совершенствование финансовых технологий все больше стирает границы между компетенциями специалистов в сфере финансов и в области информационных технологий (ИТ). Для успешной работы в этих секторах профессионалам следует разбираться сразу в обеих сферах, а поскольку финансово-технологические компании все чаще становятся клиентами аудиторов, последним необходимо хорошо ориентироваться в технологической составляющей операций с криптоактивами, чтобы провести успешную проверку и подготовить заключение. Развитие технологии блокчейн требует существенной трансформации методологии аудита, а потому эти проблемы активно исследуются целым рядом ученых в России и странах СНГ, причем не только с экономико-финансовой, но и с учетной позиции [6–8].

Определения цифровых финансовых активов и цифровой валюты, приведенные в Федеральном законе «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»², не охватывают все виды существующих криптоактивов, поэтому в данной статье будет использоваться именно всеобъемлющее понятие «криптоактив» [9, 10].

Необходимость изучения и применения технологии блокчейн для финансового учета и аудита отмечает Ю.Н. Гузов [8]. По его утверждению, отсутствие должной методики как раз и является причиной, с одной стороны, потенциальных трудностей

¹ Криптокошелек — это специальная программа, которая позволяет учитывать, хранить и совершать иные действия с криптоактивами. При регистрации кошелька пользователь получает к нему доступ в виде открытого (публично) и закрытого (приватного) ключа — криптографического кода.

² Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (последняя редакция). URL: https://www.consultant.ru/document/cons_doc_LAW_358753/?ysclid=ld00pmltof995139300

и рисков, связанных с цифровизацией, а с другой — возможности применения цифровых технологий для верификации. Чем сложнее становятся объекты и операции компаний в условиях цифровизации, тем больше появляется технологий, позволяющих их осуществлять. Чем тяжелее проводить их аудит, тем лучше должны быть методические инструменты, адаптированные к новым явлениям, вызванным цифровизацией. И все это требует от аудиторов знаний в области ИТ для перехода к следующей стадии развития аудиторского дела.

ПРОБЛЕМА ИДЕНТИФИКАЦИИ КРИПТОКОШЕЛЬКА КОМПАНИИ

Другая проблема, с которой предстоит столкнуться аудиторам, — идентификация криптокошелька хозяйствующего субъекта. В случае традиционных банковских счетов этот вопрос не стоит так остро и может быть закрыт банковской выпиской. В условиях новой технологии появляется понятие «криптоадрес», который является парой ключей — закрытого и открытого. Первый используется для подписи транзакции с целью ее совершения; второй — для получения криптоактивов. Но в большинстве случаев для взаимодействия с криптоактивами применяются криптокошельки, значительно упрощающие взаимодействие с открытым и закрытым ключами. Криптокошелек — это информационная система, позволяющая просматривать состояние криптосчета и осуществлять с ним различные операции, в том числе и отправлять транзакции [11, 12].

Открытый адрес и закрытый ключ — это определенный набор символов, но он не позволяет однозначно идентифицировать владельца криптоадреса без дополнительных верификационных мероприятий. Именно поэтому аудитор может столкнуться со значительным количеством частных проблем, включая сложность методики подтверждения и выявления подлога со стороны аудируемой организации для получения немодифицированного аудиторского заключения. Конечной целью подлога, как правило, является обман инвесторов или сокрытие от них реального положения дел в компании. Соответственно, перед аудитором стоит задача (и это — промежуточный шаг к более важному этапу по идентификации криптоактивов, находящихся на данном криптокошельке) осуществления необходимых и достаточных проверок в целях доказательства либо опровержения принадлежности криптокошельков аудируемой организации.

В результате проведенного ситуационного анализа нами были определены следующие случаи опровержения такой принадлежности (см. таблицу):

- признание организацией криптокошелька, который не должен признаваться, так как она им не владеет (т.е. не контролирует его). Как правило, подобная ситуация вызвана введением аудиторов в заблуждение для намеренного вуалирования неоправданного увеличения суммы активов организации. Аудитор обязан обнаружить это нарушение на основе методики идентификации принадлежности активов криптокошелька к определенным видам и исключить из активов организации те криптоактивы, которые не удовлетворяют критериям признания (т.е. уменьшить сумму активов);
- признание организацией криптокошелька при поступлении криптоактивов на счет незадолго до окончания аудируемого периода. Аудитор обязан детально изучить эту ситуацию для подтверждения наличия у организации контроля над данными криптоактивами (т.е. то, что они действительно ей принадлежат, используются по ее усмотрению и способны принести выгоды именно ей) и удостовериться в их зачислении на счет для неискажения финансовой отчетности;
- выявление на криптокошельке организации «токсичных» криптоактивов, т.е. помеченных в блокчейне как полученные вследствие нелегальной или противозаконной деятельности, которые нельзя признать активами. В большинстве случаев аудируемая компания не является вовлеченной в данную деятельность, а получает такие активы в качестве оплаты за свои абсолютно легальные услуги. Но в дальнейшем она не сможет распоряжаться этими активами и получить от них выгоду, так как ни одна крупная биржа не будет зачислять их на счет для дальнейшей конвертации в национальные валюты — рубль, доллар, евро и др. В данном случае признание криптокошелька может быть подтверждено, но криптоактивы не будут учитываться в сумме активов с представлением необходимых раскрытий-пояснений;
- признание криптокошелька при наличии недостаточной степени достоверности. В таком случае аудитор признает криптоактивы либо целиком, либо — не в полном объеме, либо вообще не признает. Недостаточная степень достоверности может касаться только части активов на криптокошельке. Например, аудитор, получив необходимые и достаточные подтверждения количества биткоинов на криптокошельке, не уверен в отношении

Таблица / Table

Случаи опровержения признания активов криптокошельков и обязанности аудитора / Cases of refutation of the recognition of assets of crypto-wallets and the obligations of the auditor

№	Случай опровержения / Case of refutation	Обязанности аудитора / Obligations of the auditor
1	Предоставление «чужого» криптокошелька	Исключение криптоактивов из активов
2	Поступление криптоактивов перед окончанием аудируемого периода	Детальный анализ транзакций для окончательного решения о признании или исключения криптоактивов, как непризнанных
3	«Токсичные криптоактивы»	Исключение криптоактивов из активов с необходимыми пояснениями
4	Недостаточная степень достоверности признания криптокошелька	Частичное признание криптоактивов, идентифицируемость и выполнение критериев признания которых однозначно установлены

Источник / Source: разработано автором / developed by the author.

эфириума³ и других криптоактивов; в таком случае он должен признать только часть активов.

В данной статье исследуются лишь первые два случая, когда признание криптокошелька может быть опровергнуто, поскольку другие в меньшей степени касаются вопросов идентификации криптоактивов, а больше относятся к вопросу методики учета тех из них, которые являются спорными.

В ходе исследования автором были выявлены необходимые и достаточные критерии признания криптокошелька аудируемой организации:

- признание активом каждого из криптоактивов. Для аудиторского подтверждения полного или частичного признания криптокошелька аудитором должно быть проведено индивидуальное признание составляющих его активов, неопровержимыми доказательствами чего являются факты индивидуального признания каждого криптоактива, т.е. получение доказательств возможности его применения аудируемой организацией в целях получения выгод;

- соответствие криптотранзакций основной деятельности компании, т.е. соответствующее ей использование криптоактивов на криптокошельке. Транзакции могут совершаться ежедневно или очень редко, но их частота должна быть обоснована

³ Эфириум (от англ. Ethereum, от англ. Ether — эфир) — криптовалюта и платформа для создания децентрализованных онлайн-сервисов на базе блокчейна (децентрализованных приложений), работающих на основе умных контрактов. Реализована как единая децентрализованная виртуальная машина. Концепт был предложен в конце 2013 г., сеть запущена 30 июля 2015 г. Ethereum изначально создавался не столько как платежная система, сколько как база для доступного внедрения технологии блокчейна в сторонние проекты.

на деятельностью экономического субъекта. Например, для предприятий, специализирующихся на продаже продуктов питания, характерны ежедневные транзакции, а для тех, что занимаются продажей недвижимости, может быть достаточно одной в течение нескольких месяцев. Таким образом, вид деятельности организации позволяет аудитору понять, не использует ли она разовые транзакции в конце аудируемого периода для намеренного искажения финансовой отчетности;

- доступ как к публичному, так и к закрытому ключу. Он необходим только компаниям, владеющим некастодиальными криптокошельками⁴, передающими информацию о ключах владельцу и не хранящими ее на своей стороне. Безусловно, организации могут держать определенный объем криптоактивов на криптобиржах, но период хранения должен быть минимальным — только для целей обмена криптоактивов. Этот критерий необходим для увеличения безопасности хранения криптоактивов.

Аудитор может выразить немодифицированное заключение относительно признания активов криптокошелька и учесть их в общей сумме активов организации только в случае одновременного выполнения требований всех трех критериев:

- а) признание активом каждого из криптоактивов;
- б) соответствие криптотранзакций основной деятельности;

⁴ Некастодиальным обычно считается криптокошелек, сохраняющий за пользователем возможность полностью контролировать ключи и свои средства. К данной категории можно отнести аппаратные, мобильные, бумажные, десктоп- и веб-кошельки.

в) хранение криптоактивов на некастодиальных криптокошельках.

В случае, если, по мнению аудитора, не выполнен хотя бы один из критериев, он обязан все еще раз детально перепроверить и, при сохранении своего мнения сделать заключение о невозможности включения данных криптоактивов в суммарный объем активов.

Для подтверждения признания криптокошельков используются онлайн- и офлайн-методы. Второй относительно прост и надежен: аудитор лично присутствует при открытии кошелька и совершении какой-либо транзакции. Но такой вариант имеет недостатки в виде необходимости физического присутствия и возможности компрометации секретной информации. Онлайн-методы различаются в зависимости от конкретного криптоактива, признание которого и принадлежность к определенному виду необходимо подтвердить. Если блокчейн криптоактива позволяет работать со смарт-контрактами⁵, то целесообразно использовать маркерный токен⁶. В случае отсутствия смарт-контрактов как, например, в сети блокчейна, может быть применен метод минимальной транзакции.

ОПИСАНИЕ МЕТОДИКИ

Автором разработана методика аудита процедуры идентификации и признания криптокошелька аудируемой организации, которая заключается в использовании механизмов блокчейна. Это позволяет более просто, не прибегая к стороннему программному обеспечению, осуществлять признание принадлежности криптокошелька организации и в кратчайшие сроки удаленно получить результат с максимальным уровнем достоверности. Кроме того, методика предполагает работу со всеми блокчейнами: имеющими смарт-контракты и не обладающими им.

Блокчейн обеспечивает полную прозрачность транзакций, давая возможность не только признать или опровергнуть принадлежность криптокошелька, но и осуществить (в том числе и для подтверждения выводов, сделанных аудиторами) повторную проверку независимой стороной при помощи общедоступной копии блокчейна.

⁵ Смарт-контракт (от англ. smart contract — умный контракт) — договор, записанный в виде компьютерной программы.

⁶ Специально созданный аудиторской организацией токен (запись в блокчейне) для подтверждения, что аудируемая организация владеет криптокошельком.

Обоснованием ценности методики служит проведенный и представленный ранее ситуационный анализ рисков, связанных с признанием организацией активов на криптокошельке; кроме того, на ее применении требуется минимум затрат при полной автоматизации процесса проверки посредством маркерных токенов или минимальной транзакции.

Методика предполагает индивидуальный подход к криптоактивам и криптокошелькам. При использовании последовательного подхода сначала необходимо идентифицировать криптокошелек, а уже затем произвести признания каждого криптоактива в отдельности.

Принципы, положенные в основу методики:

- объективность, т.е. представление в отчетности информации, как можно более точно соответствующей реальности;
- прозрачность, гарантируемая технологией блокчейн;
- проверяемость, так как результат может быть перепроверен в будущем независимой стороной;
- универсальность, т.е. возможность применения для всех блокчейнов;
- сохранение тайны контрольного времени (т.е. принцип внезапности) и параметров контроля.

Используемые методы — офлайн-метод (физическое присутствие аудитора и подтверждение принадлежности криптокошелька), создание смарт-контракта с маркерными токенами и применение минимальной транзакции для идентификации криптокошелька.

Этапы проведения аудиторской процедуры идентификации активов криптокошелька, позволяющие произвести полное или частичное его признание (т.е. полное или частичное включение его криптоактивов в суммарные активы организации):

- создание аудиторской компанией контрольных маркерных токенов, например в блокчейне эфириум, для подтверждения идентификации и признания активов криптокошелька;
- сохранение в тайне от аудируемой организации адреса смарт-контракта данного токена и криптоадреса, на которые будут переведены маркерные токены для подтверждения владения счетами;
- отправка в конкретное время на все публичные счета, заявленные аудируемой компанией, контрольных маркерных токенов; обязательная для сотрудников компании пересылка данных токенов на определенные аудиторами контрольные

счета в течение получаса (не более) после их получения.

Данная методика позволит однозначно идентифицировать счета организации и верифицировать наличие у нее криптоактивов. Безусловно, вместе с этой проверкой необходимо подтвердить характер расходных операций, как было описано ранее.

Этапы метода минимальной транзакции схожи с приведенными, но при его применении аудируемая организация должна отправить на определенные счета не маркерные токены, а минимально возможную транзакцию, например один сатоши⁷, для подтверждения владения криптокошельком. Затраты при использовании обеих методик верификации минимальны, особенно в сравнении со средней стоимостью аудиторских услуг.

ОБСУЖДЕНИЕ

Предложенная методика имеет определенные проблемные точки. Она еще не была апробирована и требует от аудиторских компаний дополнительных технических ресурсов для создания маркерных токенов и идентификации при помощи них криптоактивов. Кроме того, критерий соответствия криптотранзакций основной деятельности компании требует экспертной оценки, которая в сложных ситуациях, скорее всего, будет значительно варьироваться. Затраты на реализацию данной методики обусловлены необходимостью наличия у аудиторских компаний минимальных криптоактивов для создания и использования маркерных токенов. Некастодиальные кошельки в большинстве случаев не требуют идентификации владельца в отличие от криптобирж, которые ее подразумевают. Поэтому вопрос о том, кто именно в компании может распоряжаться криптокошельком, требует отдельного рассмотрения и приведения дополнительных рекомендаций в части внутренних нормативных актов. Тем не менее методика позволяет производить идентификацию внутри блокчейна, что увеличивает достоверность результатов и дает возможность аудиторским компаниям, взаимодействующим с криптоактивами, относительно просто и с высокой степенью надежности их идентифицировать, несмотря на отмеченные проблемные

точки. Кроме того, важен вопрос передачи доступа к криптоактивам в случае антикризисного управления, что небезопасно: секретная информация может быть скомпрометирована. Поэтому единственным способом является перемещение всех криптоактивов на новый криптокошелек, доступ к которому имеет антикризисный управляющий; иные варианты излишне рискованны.

Отдельно необходимо рассмотрение вопроса идентификации криптокошельков и криптоактивов в коммерческих банках, поскольку предмет данной статьи — проведение аудита в коммерческих организациях. Базельский комитет по банковскому надзору⁸ в 2021 г. выпустил рекомендации по обеспечению резерва капитала, достаточного для полного покрытия любых убытков, связанных с криптоактивами. Соответственно, это увеличивает сложность аудиторских процедур, так как необходимо не только провести идентификацию криптокошельков и криптоактивов, но и подтвердить достаточность резерва капитала под последние. В 2022 г. были выпущены рекомендации по разделению криптоактивов на две группы по степени их рискованности и установлены максимальные доли этих групп в капиталах банков, что еще больше затрудняет аудиторские процедуры.

ВЫВОДЫ

Аудитор в условиях активного развития криптоэкономики обязан не только разбираться в сущности криптоактивов, но и глубоко проникнуть в концепцию технологии блокчейн. Без детального ее изучения он не сможет понимать направления и способы использования этой технологии для проведения аудиторских процедур. В настоящее время индустрия аудиторских услуг уже никоим образом не может игнорировать развитие криптоэкономики и должна как можно быстрее и менее затратно адаптироваться к ней через повышение компетенций сотрудников в данной области и разработку соответствующего методического инструментария. Предложенная методика может рассматриваться как начальная точка его создания. Данные рекомендации адресованы как практикующим аудиторам, так и всему научному сообществу для дальнейшего обсуждения.

⁷ Сатоши (satoshi) — единица измерения, дробная часть биткойна (первой криптовалюты, созданной на основе технологии Blockchain), равная 0,00000001 BTC. Таким образом, 1 Bitcoin = 100 000 000 Сатоши.

⁸ Базельский комитет (официальный сайт). URL: <https://www.bis.org/bcbs/publ/d545.htm> (дата обращения: 05.01.2023).

Сложность идентификации криптокошельков и признание криптоактивов — лишь малая часть проблем, с которыми могут столкнуться аудиторы по мере интенсификации использования криптоактивов экономическими субъектами. В статье был исследован лишь один из аспектов идентификации криптоактивов, однако в дальнейшем более важным станет аспект выявления их «токсичности», когда сложность и риски будут состоять в том, что, хотя принадлежность криптоактивов будет подтверждена, от аудитора (ввиду их «токсичности»)

потребуется проведение дополнительных процедур для определения возможности включения данных активов в суммарные активы организации, каждая из которых может стать причиной ошибки. С распространением криптоактивов увеличиваются и риски подлога; соответственно, аудиторским компаниям для нивелирования последних придется усложнять процедуры идентификации. Но на текущий момент предложенная методика имеет должную обоснованность и является достаточной для вынесения немодифицированного аудиторского заключения.

СПИСОК ИСТОЧНИКОВ

1. Булыга Р.П., Сафонова И.В. Технология блокчейн как инструмент повышения информационной прозрачности экосистемы бизнеса. *Учет. Анализ. Аудит*. 2021; 8(4):6–17.
2. Супрунова Е.А. Цифровые финансовые активы как объект бухгалтерского учета: дискуссионные вопросы. *Международный бухгалтерский учет*. 2020;(3):297–313.
3. Журавлев А., Брисов Ю., Янковский Р., Левашенко А. Эволюция криптоэкономики и последние тренды децентрализованных финансов. *Банковское обозрение*. 2020;(10):32–35.
4. Долганин А.А. Соотношение невзаимозаменяемых токенов (NFT) и интеллектуальной собственности: триумф проприетарного подхода? *Цифровое право*. 2021;2(3):46–54.
5. Рожнова О.В. Архитектура учетной сферы в контексте цифровизации. *Аудиторские ведомости*. 2019;(4):22–24.
6. Антипенко Н.А. Аудит цифровых знаков (токенов) в условиях цифровизации экономики Республики Беларусь. Сборник научных трудов IV национальной (с международным участием) научно-практической конференции. СПб.: СПбГЭУ; 2020:182–185.
7. Булыга Р.П., Сафонова И.В. Трансформация методологии аудита в связи с использованием технологий блокчейн и DLT. *Учет. Анализ. Аудит*. 2021;8(5):6–13.
8. Вейнер И.Н., Генералова Н.В., Гузов Ю.Н., Дюкина Т.О., Зуга Е.И., Карельская С.Н. и др. Бухгалтерский учет в XXI веке. Монография. Гузов Ю.Н., Ковалев В.В., Маргания О.Л., ред. СПб.: Скифия-принт, 2021:7–19.
9. Рябинин В.В. Правовое регулирование цифровой валюты и цифровых финансовых активов. *Актуальные вопросы бухгалтерского учета и налогообложения*. 2021;(3):67–74.
10. Цинделиани И.А., Нигматулина Л.Б. Криптовалюта как объект гражданско-правового и финансово-правового регулирования. *Финансовое право*. 2018;(7):11–18.
11. Добролюбов Н.А. Проблемы учета, отражения и аудита операций с криптовалютой в России. Сборник трудов конференции «Бухгалтерский учет: достижения и научные перспективы XXI в.». М.: Канцлер; 2019:79–83.
12. Рожнова О.В. Гармонизация учета, аудита и анализа в условиях цифровой экономики. *Учет. Анализ. Аудит*. 2018;5(3):16–23.

REFERENCES

1. Bulyga R.P., Safonova I.V. Blockchain technology as a tool for increasing the information transparency of the business ecosystem. *Uchet. Analiz. Audit = Accounting. Analysis. Auditing*. 2021;8(4):6–17. (In Russ.).
2. Suprunova E.A. Digital Financial Assets as an Object of Accounting: Discussion Issues. *Mezhdunarodnyi bukhgalterskii uchet = International Accounting*. 2020;(3):297–313. (In Russ.).
3. Zhuravlev A., Brisov Yu., Yankovsky R., Levashenko A. Evolution of crypto economics and recent trends in decentralized finance. *Bankovskoe obozrenie = Banking review*. 2020;(10):32–35. (In Russ.).
4. Dolganin A.A. Value of non-fungible tokens (NFT) and intellectual property: the triumph of proprietary approach? *Tsifrovoe pravo = Digital Law Journal*. 2021;2(3):46–54. (In Russ.).

5. Rozhnova O.V. Accounting architecture in the context of digitalization. *Auditorskie Vedomosti = Audit statements*. 2019;(4):22–24. (In Russ.).
6. Antipenko N.A. Audit of digital signs (tokens) in the context of digitalization of the economy of the Republic of Belarus. Collection of scientific papers of the IV national (with international participation) scientific and practical conference. Saint Petersburg: St. Petersburg State University of Economics; 2020:182–185. (In Russ.).
7. Bulyga R.P., Safonova I.V. Transformation of the audit methodology in connection with the use of blockchain and DLT technologies. *Uchet. Analiz. Audit = Accounting. Analysis. Auditing*. 2021;8(5):6–13. (In Russ.).
8. Veiner I.N., Generalova N.V., Guzov Yu.N., Dyukina T.O., Zuga E.I., Karelskaya S.N. and others. Accounting in the XXI century. A Monograph. Guzov Yu.N., Kovalev V.V., Marganiya O.L., eds. St. Petersburg: Scythia-print; 2021:7–19. (In Russ.).
9. Ryabinin V.V. Legal regulation of digital currency and digital financial assets. *Aktual'nye voprosy bukhgalterskogo ucheta i nalogooblozheniya = Topical issues of accounting and taxation*. 2021;(3):67–74. (In Russ.).
10. Tsindeliani I.A., Nigmatulina L.B. Cryptocurrency as an object of civil and financial and legal regulation. *Finansovoe pravo = Financial law*. 2018;(7):11–18. (In Russ.).
11. Dobrolyubov N.A. Problems of accounting, reflection and audit of cryptocurrency transactions in Russia. Collection of proceedings of the conference “Accounting: achievements and scientific prospects of the XXI century”. Moscow: Chancellor; 2019:79–83. (In Russ.).
12. Rozhnova O.V. Harmonization of accounting, auditing and analysis in the digital economy. *Uchet. Analiz. Audit = Accounting. Analysis. Auditing*. 2018;5(3):16–23. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ / ABOUT THE AUTHOR

Алексей Викторович Тетюшин — аспирант департамента аудита и корпоративной отчетности факультета налогов, аудита и бизнес-анализа, Финансовый университет, Москва, Россия

Alexey V. Tetyushin — postgraduate student of the Department of Audit and Corporate Reporting of the Department of Taxes, Audit and Business Analysis, Financial University, Moscow, Russia

<https://orcid.org/0000-0001-6512-3536>

altet97@gmail.com

Конфликт интересов: автор заявляет об отсутствии конфликта интересов.

Conflicts of Interest Statement: The author has no conflicts of interest to declare.

Статья поступила в редакцию 21.12.2022; после рецензирования 11.01.2023; принята к публикации 26.06.2023.

The article was submitted on 21.12.2022; revised on 11.01.2023 and accepted for publication on 26.06.2023.

Автор прочитал и одобрил окончательный вариант рукописи.

The author read and approved the final version of the manuscript