

Олена Анатоліївна ПЕТРИК

д.е.н., професор, зав. кафедри, Київський національний економічний університет імені Вадима Гетьмана

ORCID: <https://orcid.org/0000-0003-1881-9412>

e-mail: auditlena@ukr.net

Олег Вікторович ДЯК

аспірант, Київський національний економічний університет імені Вадима Гетьмана

ORCID: <https://orcid.org/0000-0003-0249-924X>

e-mail: olegd1997@gmail.com

ПРОЦЕДУРИ АУДИТУ ФІНАНСОВОЇ ЗВІТНОСТІ КРИПТОВАЛЮТНОЇ БІРЖИ ТА ЇХ ТЕХНОЛОГІЧНА ПОСЛІДОВНІСТЬ

Статтю присвячено вдосконаленню аудиту фінансової звітності централізованих криптовалютних бірж з урахуванням специфіки цифрового середовища. Визначено, що блокчейн-природа активів, їх висока волатильність, кіберризик і регуляторна фрагментація створюють загрози викривлення звітності, які не охоплюються чинними МСА. Метою дослідження є розроблення технологічної послідовності аудиторських процедур, що поєднує класичні стандарти з інструментами блокчейн-верифікації. У результаті запропоновано ризик-орієнтований алгоритм, що включає тестування контролів доступу, підтвердження резервів через криптографічні докази і вибірково перевірку транзакцій. У висновках обґрунтовано переваги інтегрованої моделі аудиту для підвищення прозорості, достовірності та стійкості криптовалютної екосистеми.

Ключові слова: аудит криптовалют, підтвердження активів, блокчейн-аналітика, аудиторські ризики, суттєвість, тестування контролів, верифікація транзакцій, фінансова звітність

ВСТУП

Зростаюче поширення криптовалют як фінансових інструментів та поява численних централізованих бірж обумовлюють потребу у розробленні надійних аудиторських процедур, що здатні забезпечити достовірність фінансової звітності таких суб'єктів. Однак чинні міжнародні стандарти аудиту (МСА) не враховують повністю специфіку цифрових активів, криптографічних механізмів верифікації та розподіленої природи блокчейн-інфраструктур. Аудит криптовалютних бірж ускладнюється численними викликами: безперервністю торгів, кібератаками, мультиюрисдикційним регулюванням, зберіганням активів у криптогаманцях, нестабільністю цін та ризиком шахрайства.

Проблема ускладнюється відсутністю уніфікованих процедур перевірки даних з блокчейну, інтеграції підтвердження резервів, а також інтерпретації нормативних актів різних країн. Тоді як цифрові активи набирають ваги у глобальних фінансах, наукова та практична спільнота стикається з викликом: як забезпечити прозорість і достовірність звітності криптовалютних платформ. Це питання набуває особливої актуальності у світлі частих зловживань на ринку, що підривають довіру інвесторів і регуляторів. У цьому контексті дослідження процедур аудиту криптовалютної біржі набуває стратегічного значення як для наукових завдань, так і для вирішення прикладних проблем у сфері цифрових фінансів.

Концептуальні засади цифрових активів закладено у працях S. Nakamoto [1], які визначили децентралізовану природу блокчейна та викликали хвилю досліджень з бухгалтерського обліку й аудиту. Подальші зусилля PwC [2] та FATF [3] окреслили ризики кібербезпеки й регуляторні вимоги AML/KYC, що лягли в основу сучасних підходів до ідентифікації ризиків бірж. EY [4], ISACA [6] і KPMG [7] розробили перші методики оцінювання внутрішніх контролів, однак їхня практична апробація обмежена кейс-стаді окремих бірж.

Питання облікової класифікації та оцінювання крипто-

активів висвітлено у документах Міжнародних стандартів фінансової звітності (МСФЗ) [5] та Ради зі стандартів фінансового обліку (FASB) [10], де запропоновано трактувати їх як нематеріальні активи, проте конкретні алгоритми переоцінки й тестування на знецінення залишаються дискусійними. Рада з нагляду за бухгалтерським обліком публічних компаній (PCAOB) [8] і Deloitte [9] акцентували на необхідності ончейн-підтвердження резервів, але не надали інтегрованого фреймворку з вибірковими процедурами перевірки транзакцій.

Дослідження ICAEW [23] вказує на потребу перегляду процедур перевірки транзакцій в межах юрисдикцій з різними регуляторними режимами. В академічному дискурсі Dai & Vasarhelyi [14] аргументували доцільність безперервного аудиту блокчейнів, а Oosthoek & Doerg [15] та Cong & He [16] зосередилися на юридичних та смарт-контрактних ризиках, проте питання узгодження таких підходів з МСА залишилося відкритим. Емпіричні дослідження Messari [17] та Bayes Business School [24] довели високий рівень розбіжностей в даних про обсяги торгів і ціни, що посилює виклики у верифікації доходів. The CPA Journal [19] розглядає відповідність МСА. Chainalysis [11] і Elliptic [12] висвітлюють новітні аналітичні інструменти для виявлення підозрілих транзакцій, що застосовуються в аудиті високоризикових криптовалютних платформ.

Водночас значна частина наявних напрацювань залишається на рівні концептуального осмислення проблем, не пропонуючи структурованих методик впровадження ризик-орієнтованого аудиту у практику бірж. Обмеженням багатьох досліджень є відсутність комплексної інтеграції процедур підтвердження резервів, мультипідпису, верифікації на блокчейні та традиційних контрольних механізмів. Також практично не висвітлені аспекти адаптації процедур до особливостей нових криптовалютних продуктів – NFT, стейкінгу, DeFi-протоколів.

Істотною проблемою є відсутність єдиних критеріїв визначення суттєвості та матеріальності для волатильних

криптоактивів; чинні рекомендації МСФЗ і FASB містять лише загальні рамки, що не враховують 24/7-торгівлю та фрагментовану ліквідність. Другим невирішеним аспектом залишається стандартизація процедур «proof-of-reserves»: різні біржі застосовують несумісні криптографічні схеми, унеможливаючи порівнянність результатів аудиту [16]. Ще одну проблему становить брак інтеграції безперервного аудиту з аналітикою в реальному часі: наявні моделі зосереджено на ретроспективних тестах вибірки й ігнорують можливість автоматизованого моніторингу потоків транзакцій [14]. Також недостатню увагу приділено оцінюванню ризиків нових продуктів DeFi та NFT, що швидко інтегруються у бізнес-модель бірж, але залишаються поза фокусом традиційних визначених МСА процедур [25].

Причини таких прогалин полягають у швидкості технологічних змін, фрагментарному регуляторному полі та відсутності консолідованої міждисциплінарної методики, що об'єднала б знання з бухгалтерського обліку, криптографії та регуляторики. Усунення цих недоліків необхідно для забезпечення достовірності фінансової звітності, зміцнення довіри інвесторів і запобігання системним ризикам на ринку цифрових активів. Так, проведене авторами дослідження заповнює прогалину, пропонуючи практичну модель аудиту криптовалютної біржі, що ґрунтується на комбінванні процедур підтвердження активів у ланцюжку, тестування контролів та аналітичної перевірки операцій за допомогою інструментів блокчейн-моніторингу.

МАТЕРІАЛИ ТА МЕТОДИ

У дослідженні застосовано методологію ризик-орієнтованого аудиту, адаптовану до цифрового середовища. Аналіз виконано на прикладі централізованих бірж, що оперують на ринках з підвищеним регуляторним навантаженням. Методи дослідження: аналіз нормативних документів (МСА, IFRS, FASB), компаративний аналіз публікацій професійних організацій (FATF, PCAOB, EY), а також експертне моделювання технологічної послідовності аудиту. Обрано змішану стратегію: тестування контролів, автоматизоване підтвердження транзакцій, статистична вибірка через API-інтерфейси та аналітичні процедури, засновані на агрегаторах даних (Chainalysis, Elliptic, CoinMarketCap). Особливу увагу приділено комбінованим методам підтвердження резервів (криптографічна верифікація та сторонні підтвердження).

МЕТА статті – розроблення структурованої моделі аудиту централізованої криптовалютної біржі, яка враховує специфіку цифрових активів, блокчейн-інфраструктури та динамічного регуляторного середовища. Для досягнення цієї мети поставлено такі завдання: визначити основні ризики аудиту криптобірж, включаючи волатильність активів, технологічні загрози, правові вимоги та шахрайство; запропонувати процедури оцінювання внутрішнього контролю, адаптовані до цифрового середовища, включаючи контроль доступу, мультипідпис, авторизацію транзакцій; розробити алгоритм підтвердження активів в блокчейні, включаючи методи on-chain верифікації та третестороннього депозитарного підтвердження; обґрунтувати доцільність застосування безперервного аудиту із застосуванням аналітичних інструментів для моніторингу високоризикових транзакцій; запропонувати методіку оцінювання справедливої вар-

тості цифрових активів у контексті міжнародних стандартів фінансової звітності; надати практичні рекомендації із вдосконалення аудиторських протоколів у сфері цифрових активів.

Реалізація цих цілей дає змогу сформувати уніфіковану рамку для проведення ефективного й достовірного аудиту у криптовалютній індустрії, забезпечуючи дотримання принципів прозорості, надійності та відповідності глобальним стандартам.

РЕЗУЛЬТАТИ

Проведення аудиту криптовалютної біржі пов'язане з низкою складних проблем, які виходять за рамки традиційних методів аудиту, що застосовуються у звичайних фінансових установах. Ці труднощі виникають під впливом кількох взаємопов'язаних факторів: глобальний і безперервний характер торгівлі цифровими активами, криптографічна основа транзакцій, надзвичайна волатильність цін на криптовалюту та регуляторне середовище, що швидко розвивається і регулює діяльність таких платформ.

Етап планування аудиту є фундаментом, на якому будується решта його завдань. Аудитори повинні розробити чіткий, структурований план, який включає глибоке розуміння бізнес-моделі біржі, ландшафту ризиків, системи внутрішнього контролю та відповідних зовнішніх нормативних актів. Цей план встановлює обсяг завдання, визначає ключовий персонал і ресурси, а також визначає критичні сфери, які потребують підвищеної уваги.

Перед початком виконання завдань з аудиту аудитори повинні мати глибоке розуміння бізнес-моделі криптовалютної біржі, зокрема характеру її активів, операційних юрисдикцій та конкретних продуктів і послуг, які вона пропонує. Це особливо важливо в криптовалютному секторі через високу варіативність біржових структур, моделей зберігання та користувацьких інтерфейсів. Таке розуміння має бути задокументоване за допомогою попередніх зустрічей з керівництвом, аналізу системної документації та процедур, які відстежують життєвий цикл транзакцій від депозиту користувача до виведення коштів.

Ретельне оцінювання ризиків є наріжним каменем ефективного планування аудиту. У сфері криптовалютних бірж ризик, притаманний біржам, часто перевищує ризики багатьох традиційних галузей через низку відмінних рис:

1. *Волатильність ринку.* Криптовалюти, такі як Bitcoin або Ethereum, можуть зазнавати швидких цінових коливань, іноді протягом декількох годин або навіть хвилин. Ці швидкі зміни створюють значні ризики вимірювання та оцінювання, які можуть призвести до суттєвих викривлень у фінансовій звітності, якщо їх ретельно не враховувати. Наприклад, коли біржа володіє значними обсягами певної монети, рух ціни в бік зниження поблизу звітної дати може кардинально змінити оцінювання активів, потенційно залишаючи керівництву недостатньо часу для точного відображення знецінення або переоцінки.

2. *Кібербезпека та технологічні ризики.* Криптовалютні біржі є частою мішенню для хакерів, зважаючи на можливість отримання великих прибутків від доступу до гаманців користувачів або приватних ключів [2]. Однак кібератака може призвести до значних фінансових

та репутаційних втрат. Оцінювання надійності IT-систем та оцінювання того, наскільки ефективно біржа захищає свої гарячі та холодні гаманці, є життєво важливими кроками у визначенні того, чи можна довіряти звітним балансам біржі.

3. *Питання регуляторного та правового характеру.* Криптовалютні біржі часто працюють у декількох юрисдикціях, кожна з яких має власні правові норми з протидії відмиванню грошей (AML) та вимог «Знай свого клієнта» (KYC) [3]. Невиконання цих вимог може призвести до великих штрафів, примусового призупинення діяльності або інших регуляторних втручань, які суттєво впливають на фінансовий стан біржі. Тому на етапі планування аудитор повинні визначити, які нормативно-правові акти застосовуються, та оцінити стратегії керівництва з їх дотримання.

4. *Зберігання активів.* Фундаментальним питанням аудиту криптовалютних бірж є те, чи належно платформа відокремлює депозити клієнтів від власних активів [4]. Змішані активи можуть спотворювати фінансову звітність, особливо якщо біржа неавтоматично розглядає активи клієнтів як частину власного капіталу. Така неправильна класифікація створює не лише проблеми з оцінюванням, але й юридичну невизначеність стосовно права власності та контролю над цими активами.

5. *Ризик шахрайства.* Як і в будь-якому суб'єкті аудиту цей ризик наявний, але має свою специфіку. Криптовалютні біржі можуть брати участь у «відмиванні» коштів або надавати неправдиві дані про свої активи, що може призвести до загрози банкрутства або судових справ з можливістю закриття.

Перераховуючи ці ризики та оцінюючи їх ймовірність настання і вплив, аудитор зосереджує свою увагу на певних об'єктах та операціях, застосовуючи принцип аудиту, що базується на оцінці ризиків. Цей принцип гарантує, що більше часу та ресурсів виділяється на сфери, де ймовірність суттєвих викривлень є найвищою.

У рамках аудиту необхідно оцінити ризик засобів контролю, який у криптографічному контексті включає: доступ до приватних ключів та гарячих гаманців; механізми авторизації для переказу коштів; розподіл обов'язків у системному адмініструванні; застосування гаманців з мультипідписом та протоколів резервного копіювання ключів. Недоліки контролю в будь-якій з цих сфер можуть вимагати проведення масштабної перевірки у суті.

Після визначення ризиків та засобів їх контролю наступним етапом є розроблення індивідуальної стратегії аудиту, що визначає загальний підхід до збору достатніх та належних доказів. На перший план виходять кілька стратегічних міркувань:

Поріг суттєвості. У контексті нестабільних криптовалютних ринків встановлення чітких порогів суттєвості часто є більш складним завданням, ніж у більш стабільних галузях [5]. Визначення суттєвості для аудиту криптовалютних бірж вимагає ретельного врахування як кількісних, так і якісних факторів. Хоча традиційні показники, що базуються на відсотках від загальних активів або доходів, можуть слугувати відправною точкою, аудитор повинні враховувати інші фактори: відносну значущість різних криптовалют, чи зберігаються, важливість тверджень про зберігання для користувачів фінансової звітності, регуляторні пороги, які можуть спри-

чинити додаткові вимоги, міркування суспільного інтересу з огляду на високу видимість сектору криптовалют [6].

Суттєвість повинна бути встановлена як на рівні фінансової звітності, так і для конкретних тверджень, пов'язаних з криптовалютами, з особливою увагою до активів, що зберігаються в «гарячих гаманцях», через їх підвищений профіль ризику.

Обсяг аудиторських процедур. Криптовалютні біржі можуть здійснювати різноманітні операції – від спотової торгівлі до ф'ючерсів, маржинального кредитування, стейкінгових послуг та інші. Кожну з цих сфер пов'язано з певними ризиками. Ретельне визначення обсягу аудиту гарантує, що всі основні потоки доходів, зобов'язання та операційні сегменти буде включено у сферу аудиту [7]. Виключення будь-якого сегмента з високим рівнем ризику може залишити аудитора вразливим до помилок.

Часові рамки та ресурси. Ринки криптовалют працюють безперервно. Торгівля відбувається цілодобово, а це означає, що тестування на відсікання ускладнюється, і журнали транзакцій значно зростають з кожним днем [8]. Щоб вирішити ці питання, аудиторська група повинна визначити, коли відбуватиметься проміжне тестування, як проводитимуться процедури наприкінці року та чи потрібні спеціалізовані IT-аудитори або зовнішні експерти з блокчейну.

Координація з експертами з правових та регуляторних питань. Оскільки багато правових режимів ще не завершили розроблення чітких, єдиних правил для цифрових активів, співпраця з юрисконсультами або фахівцями з комплаєнсу може гарантувати, що стратегія аудиту враховує динамічний регуляторний ландшафт [9]. Така координація часто допомагає в інтерпретації нещодавно виданих керівних принципів, які може бути ще не кодифіковано у стандартну практику бухгалтерського обліку.

Такий структурований підхід до стратегії аудиту діє як дорожня карта, що спрямовує групу з виконання завдання через складну екосистему криптовалютних бірж. Завдяки ретельному стратегічному плануванню аудиторі можуть систематично перевіряти сфери підвищеного ризику, не занурюючись у хитросплетіння операцій з цифровими активами.

Наступним елементом аудиторської перевірки є оцінювання системи внутрішнього контролю криптовалютної біржі, яка є сполучною ланкою між визначеною стратегією аудиту та реальним виконанням аудиторських тестів. Надійна система внутрішнього контролю, якщо вона функціонує ефективно, може зменшити обсяг тестування у суті, необхідний для перевірки певних тверджень. Ефективний внутрішній контроль є наріжним каменем фінансової доброчесності, особливо для криптовалютних бірж, де ризик незаконного привласнення активів, кібератак та маніпулювання системою значно підвищений. Однак слабкі або погано розроблені системи контролю, особливо в технологічно складних умовах, таких як криптовалютна біржа, завжди вимагають більш глибокої перевірки статей фінансової звітності. Узагальнену схему оцінювання та тестування системи внутрішнього контролю зображено на рис. 1.

Розглянемо детальніше ключові аспекти тестування контролів криптовалютної біржі.

Управління приватними ключами та контроль доступу. Можливо, найбільш важливим елементом внутрішнього



Рис. 1. Елементи оцінювання та тестування внутрішніх контролів криптовалютної біржі (узагальнено авторами на основі аналізу [2, 8])

контролю для криптовалютної біржі є захист приватних ключів, які дають змогу здійснювати транзакції з певних адрес гаманців [10]. Надійні засоби контролю часто включають гаманці з декількома підписами – коли для переказу коштів потрібні два або більше різних дозволів, і розмежування прав доступу, гарантуючи, що жодна особа не володіє необмеженим контролем над великими запасами цифрових активів.

Авторизація та реєстрація транзакцій. Враховуючи величезний обсяг торгів, автоматизовані торгові системи та потенціал мікротранзакцій, дуже важливо, щоб біржа вела вичерпні журнали, які деталізують кожну транзакцію. Аудитори повинні оцінити, чи захищені ці журнали від несанкціонованого втручання, чи активно відстежують їх внутрішні команди управління ризиками біржі на предмет виявлення незвичайних торгових схем, а також чи ретельно відстежуються зміни в журналах і чи підлягають вони наглядовому контролю [11].

Заходи з дотримання вимог AML та KYC. Оскільки регуляторні штрафи можуть суттєво вплинути на фінанси біржі, аудитори повинні перевірити, наскільки ретельно біржа впроваджує перевірки AML та KYC [12]. Це включає перевірку того, що ідентифікаційні дані користувачів підтверджуються, що підозріла діяльність оперативно фіксується і повідомляється, і що є адекватні протоколи для заморожування або розслідування проблемних рахунків. Недоліки в цих сферах можуть свідчити про загальний брак організаційної дисципліни, що може поставити під загрозу надійність фінансової звітності.

Плани реагування на інциденти та відновлення. Навіть найнадійніші системи можуть стати жертвами непередбачуваних збоїв або складних кібератак. Аудитори повинні проаналізувати протоколи реагування на інциденти на біржі, щоб переконатися, що вони належно забезпечують безперервність роботи та захист активів [6]. Елементами такої перевірки є наявність резервних копій, чітко визначені процедури ескалації, а також політики, що детально описують, як керівництво повідомляє про порушення безпеки регуляторам і зацікавленим сторонам.

Добре задокументоване, ретельно перевірене середовище контролю надає впевненість аудитору в тому,

що фінансові дані біржі менш схильні до маніпуляцій або випадкових викривлень. Якщо аудитори виявляють недоліки контролю, їм необхідно провести розширені процедури у суті, щоб підтвердити повноту і точність звітних балансів і операцій біржі.

Найбільш вагомому частину аудиту складають процедури у суті. Паралельно з тестуванням засобів контролю або після нього аудитори виконують процедури по суті, призначені для отримання прямих доказів достовірності конкретних залишків на рахунках, розкриття інформації та класів транзакцій. В аудиті криптовалютних бірж ці процедури повинні бути адаптовані до унікальних атрибутів цифрових активів, але водночас відповідати встановленим нормам аудиту, таким як MSA або рекомендації PCAOB у США [13].

Верифікація балансів активів у ланцюжку є одним з найбільш характерних аспектів аудиту криптовалютних бірж. У своїй суті блокчейн є децентралізованою бухгалтерською книгою, доступною для будь-кого, хто має відповідні інструменти:

➤ *Підтвердження в ланцюжку.* Застосовуючи загальнодоступні дослідження блокчейнів, аудитори можуть незалежно підтвердити цифрові активи, пов'язані з конкретною адресою гаманця, станом на певну дату [14]. Так, вони отримують рівень прозорості, який рідко можливий у традиційних банківських системах, де залежність від зовнішніх підтверджень має першорядне значення. Така прозорість також знижує ризик змови між суб'єктом, що підлягає аудиту, та зовнішніми третіми сторонами.

➤ *Підтвердження депозитарного зберігання від третіх осіб.* Деякі біржі вирішують передати зберігання своїх цифрових активів на аутсорсинг спеціалізованим зберігачам, які пропонують безпеку інституційного рівня. У таких випадках аудитор отримує підтвердження безпосередньо від зберігачів, аналогічно до отримання банківських виписок під час звичайного аудиту. Однак аудитори повинні бути уважними до специфіки депозитарних угод і перевіряти, чи дійсно активи зареєстровані на ім'я біржі або чи існують адекватні трастові угоди.

➤ *Протоколи підтвердження резервів.* У просторі цифрових активів з'являється нова практика – публікація протоколів підтвердження резервів, де біржа застосовує криптографічні методи, щоб продемонструвати, що баланси в ланцюжку відповідають сукупним зобов'язанням користувачів, записаним у її внутрішній книзі [16]. Аудитори, які перевіряють підтвердження резервів, повинні оцінити криптографічну методологію на предмет цілісності та повноти, переконавшись, що жоден гаманець не пропущено і що не включено фальшивих залишків на гаманцях.

Враховуючи колосальний обсяг транзакцій, що здійснюються на біржах з високим трафіком, перевірка точності цих транзакцій створює як *логістичні, так і технічні перешкоди*:

1. *Вибірка транзакцій та аналіз даних:* Збалансоване поєднання статистичної та експертної вибірки допомагає визначити репрезентативну підгрупу транзакцій для більш ретельного вивчення [17]. Автоматизований аналіз даних може виявити аномалії, такі як незвично великі транзакції, численні швидкі транзакції з однієї IP-адреси або транзакції, здійснені за неринковими цінами. Ці транзакції з високим ризиком вимагають більш

глибокого розслідування для визначення їхньої легітимності та правильного обліку.

2. *Процедури відключення*: На відміну від традиційних ринків цінних паперів, які зазвичай закриваються у визначений час, торгівля криптовалютою відбувається безперервно. Тому аудиторі повинні переконатися, що транзакції, здійснені напередодні звітної дати, зареєстровані у відповідному періоді [18]. Це часто передбачає порівняння часових міток транзакцій у блокчейні із записами в бухгалтерському обліку суб'єкта господарювання для підтвердження відповідності.

3. *Перевірка розрахунків*. Оскільки між виконанням угоди й остаточним розрахунком у мережі може бути часовий лаг, особливо якщо біржа застосовує внутрішні книги замовлень для позамережових транзакцій, узгодження розрахункових записів з фактичними підтвердженнями в блокчейні має вирішальне значення [19]. Будь-які розбіжності можуть свідчити про операційні помилки або потенційні шахрайські дії.

Важливо довести, що біржа законно контролює гаманці, на які вона претендує. Адреси в блокчейні є псевдонімами, тому знання публічної адреси не є достатнім доказом права власності. Найпоширеніший метод полягає в тому, що суб'єкта просять підписати повідомлення з викликом: наприклад, випадковий рядок, за допомогою приватного ключа, пов'язаного з гаманцем. Перевіряючи цей підпис за допомогою відкритого ключа, аудиторі отримують значну впевненість у тому, що гаманець дійсно знаходиться під контролем суб'єкта господарювання [20]. У деяких випадках аудитор може попросити клієнта виконати мінімальну тестову транзакцію на певну адресу, яку контролює аудитор, що додає ще один рівень перевірки.

Оцінювання справедливої вартості є постійною проблемою, враховуючи фрагментовану природу криптовалютних ринків:

Методології оцінювання. Біржі можуть оцінювати свої власні активи на основі середньозваженої ціни (VWAP) на декількох торгових платформах або покладатися на єдине довідкове джерело [21]. Роль аудитора полягає в тому, щоб оцінити відповідність обраного методу, переконавшись, що він точно відображає ринкові умови і не призводить до штучного завищення або заниження вартості активів.

Зовнішні агрегатори цін. Щоб підтвердити вартість активів, аудиторі можуть провести перехресну перевірку біржових оцінок за допомогою зовнішніх агрегаторів, таких як CoinMarketCap або Coingecko. Однак ці агрегатори самі собою можуть відрізнятися за рівнем надійності, що спонукає аудитора ретельно вивчати механізми збору та коригування даних кожного агрегатора [22]. Наприклад, деякі агрегатори виключають або зменшують вагу даних з менших, неліквідних бірж, що може спотворювати середні ціни на монети, які рідше торгуються.

Згідно зі стандартами бухгалтерського обліку криптовалюти, утримувані як нематеріальні активи, повинні тестуватися на знецінення, якщо їхня справедлива вартість знижується нижче собівартості. Аудиторі повинні перевірити аналіз зменшення корисності, проведений управлінським персоналом, щоб переконатися, що будь-які коригування оцінки в бік зменшення визнаються вчасно, а подальше зростання ціни враховується відповідно

до застосованих керівних принципів [23].

Оскільки процес тестування мільярдів транзакцій є неможливим, важливу роль у підтвердженні доходів відіграють саме *аналітичні процедури*. Вони надають цінні докази та вказують напрямок для подальшого тестування. До них можна віднести, наприклад, такі: порівняння звітних обсягів з даними блокчейну та ринковими даними третіх сторін; оцінювання взаємозв'язку між обсягами торгів і доходами від комісійних; аналіз змін у складі криптовалютних активів з плином часу; оцінювання ключових показників ефективності порівняно з галузевими бенчмарками.

Також невід'ємною частиною аудиту є застосування інструментів блокчейн-аналітики, які можуть допомогти аудиторам у моніторингу та перевірці транзакцій. Експоненціальне зростання щоденних обсягів торгівлі зумовило потребу в передових цифрових інструментах, які можуть допомогти аудиторам у моніторингу та перевірці транзакцій. До них можна віднести такі платформи, як Chainalysis та Elliptic, набули популярності завдяки своїм можливостям. Відстежуючи рух коштів між адресами блокчейну, ці інструменти можуть виявляти підозрілі схеми, які можуть свідчити про відмивання грошей, фінансування тероризму або маніпулювання ринком [24]. Аудиторі можуть застосовувати цю інформацію для визначення пріоритетності транзакцій з високим рівнем ризику для детальної перевірки. Дані платформи пропонують сповіщення про великі або незвичайні транзакції, забезпечуючи оцінювання ризиків у режимі, близькому до реального часу. Така можливість безперервного аудиту може бути особливо корисною в середовищах, де транзакції відбуваються постійно, оскільки вона дає змогу раніше виявляти порушення та застосовувати більш проактивний підхід до управління ризиками шахрайства [25]. Інструменти блокчейн-аналітики можуть інтегруватися з системами аналізу даних аудитора, щоб допомогти вибрати конкретні блоки транзакцій з високим рівнем ризику. Така інтеграція спрощує процес аудиту та підвищує надійність висновків стосовно точності транзакцій.

У підсумку результатом аудиту має стати те, що криптовалютна біржа повинна подати фінансову інформацію так, щоб вона достовірно відображала здійснені операції:

Класифікація статей балансу. Оцінювання належного відображення активів, що належать компанії, та відокремлення активів, що перебувають на зберіганні.

Адекватність розкриття інформації. Оцінювання того, чи надає розкриття інформації прозорі дані про ризики, депозитарні угоди та методології оцінювання.

Відповідність галузевій практиці. Порівняння підходів до подання та розкриття інформації з новими галузевими стандартами.

Зважаючи на те, що криптовалютні бізнеси перебувають на стадії становлення, аудиторі повинні враховувати суттєві невизначеності, спеціалізований характер та міркування стосовно безперервності діяльності.

Проведене дослідження та узагальнення опрацьованих джерел надає можливість визначити шляхи вдосконалення аудиту криптовалютних бірж.

Складне поєднання технологій, глобального регулювання та волатильності ринку у криптовалютному просторі вимагає постійної адаптації підходів до аудиту. На основі вищезазначених процедур можна розробити

рекомендації, які підсилюють науково-теоретичну значимість та практичну ефективність аудиту криптовалютних бірж:

Стандартизація протоколів верифікації блокчейну. Індустрія та регуляторні органи повинні співпрацювати, щоб розробити єдині правила для підтвердження гаманців, формування резервів та узгодження транзакцій. Такі стандартизовані протоколи зменшать неузгодженість між аудитами та сприятимуть порівняльності між різними біржами [26].

Інтеграція безперервного аудиту та аналітики в режимі реального часу. Враховуючи безперервний характер криптовалютних ринків, моніторинг транзакцій в режимі реального часу може значно знизити ризик невиявленого шахрайства або накопичення помилок. Впровадження моделей безперервного аудиту, в яких аналітика блокчейну забезпечує автоматичне сповіщення про порушення, дасть змогу йти в ногу з великими обсягами транзакцій [27].

Цілеспрямований професійний розвиток. Успішний аудит криптовалют вимагає поєднання традиційних бухгалтерських знань та передових технологічних компетенцій. Тому аудиторські групи повинні інвестувати в спеціалізоване навчання, що охоплює такі сфери, як криптографічні принципи, смарт-контракти та архітектура децентралізованих фінансів (DeFi). Таке розширення набору навичок дасть аудиторам змогу краще виявляти прогалини в контролі та викривлення, характерні для цифрових активів [8].

Тісніша співпраця з регуляторами. Оскільки регулятори в усьому світі уточнюють свої позиції стосовно криптовалют, відкриті канали комунікації з фахівцями з аудиту можуть сприяти формуванню політики, яка буде ефективною з погляду нагляду та здійсненою на практиці. Зі свого боку, аудиторі можуть краще передбачати законодавчі зміни, зменшуючи ризик недотримання вимог і даючи можливість пропонувати клієнтам проактивні рекомендації [29].

Підвищення прозорості для нових криптовалют. Стрімка еволюція протоколів DeFi, токенів, що майнінують, та не взаємозамінних токенів (NFT) призводить до нових проблем класифікації активів та оцінювання ризиків. Біржі, що пропонують такі інструменти, повинні запровадити прозору систему розкриття інформації, яка б пояснювала, як оцінюються ці активи, як вони приносять дохід і як зменшуються пов'язані з ними ризики. Аудиторі, зі свого боку, повинні бути в курсі нових ха-

рактеристик продуктів, щоб адекватно оцінювати фінансові та регуляторні наслідки.

Важливим аспектом є вдосконалення керівних принципів оцінювання активів.

Враховуючи високу волатильність цін та обмежену ліквідність багатьох криптовалют, аудиторські фірми повинні вести внутрішні бази даних цін на криптовалюту з часовими позначками; застосовувати середньозважене ціноутворення з декількох майданчиків; позначати токени з <5% щоденного обсягу торгів для класифікації на рівні 3 за стандартами справедливої вартості [30].

За необхідності аудиторі можуть проконсультуватися з незалежними фахівцями з оцінювання або експертами з токеноміки для перевірки токенів, забезпечених емітентом, або управлінських активів.

Також належну увагу має бути приділено розробленню системи оцінювання криптографічних ризиків. Планування аудиту повинно виходити за рамки загальних матриць ризиків. Необхідно враховувати специфічні для криптовалют ризики: ризики сумісності смарт-контрактів та їх оновлення; управління гаманцями та фрагментацію сховищ; вразливість DeFi, торгівлі із застосуванням кредитного плеча; географічну та юрисдикційну фрагментацію. Ці висновки можна кодифікувати в моделі оцінювання ризиків, що уможливило масштабовані, повторювані стратегії аудиту.

ВИСНОВКИ

Проведене дослідження дало можливість розробити комплексне уявлення про особливості, ризики та ефективні підходи до аудиту фінансової звітності централізованих криптовалютних бірж. Обґрунтовано модель аудиту, що інтегрує традиційні аудиторські стандарти з новітніми технологічними інструментами перевірки цифрових активів, враховуючи високий рівень волатильності, складну структуру операцій та юридичну фрагментацію цього сектору.

Водночас потребують подальшого дослідження питання розроблення уніфікованих стандартів підтвердження резервів криптобірж, інституційна стандартизація аудиту DeFi-платформ і NFT-продуктів, а також адаптація МСА до особливостей безперервного моніторингу в блокчейні. Лише комплексний підхід до вирішення визначеної проблеми дасть змогу створити стійку рамку для незалежного контролю цифрових фінансових екосистем у глобальному масштабі.

References

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. URL: <https://bitcoin.org/bitcoin.pdf>
2. PwC. Crypto assets guide. 2023. URL: https://viewpoint.pwc.com/dt/us/en/pwc/accounting_guides/crypto-assets-guide/assets/pwccryptoassetsguide1223.pdf
3. Financial Action Task Force (FATF). Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs. 2021. URL: <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf>
4. EY. Applying IFRS: Accounting by holders of crypto assets. 2021. URL: <https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/technical/financial-services/documents/ey-apply-ifrs-crypto-assets-update-october2021.pdf>
5. IFRS Foundation. Accounting for and Disclosure of Crypto Assets. 2023. URL: <https://www.ifrs.org/content/dam/ifrs/meetings/2023/september/fasb-iasb/ap38-crypto-fasb-iasb-education-meeting-september-2023.pdf>
6. ISACA. Methods and Techniques of Blockchain Security for IT Auditors. 2021. URL: <https://engage.isaca.org/muscatchapter/viewdocument/virtual-webinar-7-2021-methods?CommunityKey=572c27d0-2218-42ec-9260-d7574b3be1e1&tab=librarydocuments>
7. KPMG. Investing in Digital Assets. 2022. URL: <https://assets.kpmg.com/content/dam/kpmg/sg/pdf/2022/11/investing-in-digital-assets.pdf>
8. PCAOB. Audits Involving Cryptoassets. 2020 URL: <https://pcaobus.org/Documents/Audits-Involving-Cryptoassets-Spotlight.pdf>
9. Deloitte. Global Blockchain Survey. 2021. URL: https://www2.deloitte.com/content/dam/insights/articles/US144337_Blockchain-survey/DI_Blockchain-survey.pdf
10. FASB. Accounting for and Disclosure of Crypto Assets. 2023. URL: <https://www.fasb.org/page/PageContent?pageId=/projects/recentlycompleted/accounting-for-and-disclosure-of-crypto-assets.html>

11. Chainalysis. Blockchain Analytics Tools for Improved Audit. URL: <https://www.chainalysis.com/services/>
12. Elliptic. Crypto Compliance for Centralized Exchanges URL: <https://www.elliptic.co/industries/centralized-exchanges>
13. AICPA. Accounting for and auditing of Digital Assets practice aid. 2025. URL: <https://www.aicpa-cima.com/resources/download/accounting-for-and-auditing-of-digital-assets-practice-aid-pdf>
14. Dai J., Vasarhelyi M.A. Toward Blockchain-Based Accounting and Assurance. *Journal of Information Systems*. 2017. № 31(3). pp. 5–21. URL: <https://doi.org/10.2308/isys-51804>
15. Oosthoek K., Doerr C. Cyber Security Threats to Bitcoin Exchanges: Adversary Exploitation and Laundering Techniques. 2020. URL: <https://ieeexplore.ieee.org/document/9300238>
16. Cong L., He Z. Blockchain Disruption and Smart Contracts. *The Review of Financial Studies*. 2019. № 32(5). pp. 1754-1797. URL: <https://academic.oup.com/rfs/article-abstract/32/5/1754/5427778?redirectedFrom=fulltext>
17. Messari. Messari Market Data Service. URL: <https://docs.messari.io/docs/market-data-methodology>
18. CoinMarketCap. CoinMarketCap's Crypto Playbook. 2023. URL: <https://s3.coinmarketcap.com/uploads/2023-cmc-crypto-playbook-en.pdf>
19. The CPA Journal. Auditing Cryptocurrency Companies. 2025. URL: <https://www.cpajournal.com/2025/03/24/auditing-cryptocurrency-companies/>
20. Thomson Reuters. Crypto Auditing: A Guide to Reporting and Compliance. 2025. URL: <https://tax.thomsonreuters.com/blog/crypto-auditing-a-guide-to-reporting-and-compliance/>
21. ISACA Journal. Assertion-Based Financial Audit Procedures Related to Crypto Assets. 2024 URL: <https://www.isaca.org/resources/isaca-journal/issues/2024/volume-2/assertion-based-financial-audit-procedures-related-to-crypto-assets>
22. ICAEW. Considerations for Auditing Cryptocurrencies. 2024. URL: <https://www.icaew.com/-/media/corporate/files/technical/technology/know-how/considerations-for-auditing-cryptocurrencies.ashx>
23. ScienceDirect. Issues, Risks, and Challenges for Auditing Crypto Asset Transactions. 2023. URL: <https://www.sciencedirect.com/science/article/abs/pii/S1467089522000215>
24. Bayes Business School. Client-level Exposure to Cryptocurrency and Auditor Responses. 2023 URL: https://www.bayes.city.ac.uk/_data/assets/pdf_file/0006/756177/cryptocurrency_and_auditor_responses.pdf
25. Review of Accounting Studies. Financial Reporting for Cryptocurrency. 2023. URL: <https://link.springer.com/article/10.1007/s11142-022-09741-w>
26. PwC Switzerland. Crypto Custody: Risks and Controls from an Auditor's Perspective. 2023. URL: <https://www.pwc.ch/en/insights/digital/crypto-custody-risks-and-controls-from-an-auditors-perspective.html>
27. Sage Journals. Enterprise Audits and Blockchain Technology. 2023. URL: <https://journals.sagepub.com/doi/full/10.1177/21582440231218839>
28. SEC. Staff Accounting Bulletin No. 121: Accounting for Obligations to Safeguard Crypto-Assets. 2022. URL: <https://www.sec.gov/oca/staff-accounting-bulletin-121>
29. Financial Accounting Standards Board (FASB). Accounting for and Disclosure of Crypto Assets. Proposed Accounting Standards Update. 2023. URL: <https://www.fasb.org/document/blob?fileName=ASU2023-CryptoAssets.pdf>
30. Pinsker R., Wheeler P. Auditing Smart Contracts: Challenges and Research Opportunities. *Current Issues in Auditing*. 2020. 14(1), A13–A21. URL: <https://doi.org/10.2308/ciia-52579>
31. Yermack, D. Corporate Governance and Blockchains. *Review of Finance*. 2017. № 21(1). pp. 7–31. URL: <https://doi.org/10.1093/rof/rfw074>
32. Chainalysis. Crypto Crime Report: Trends and Compliance Solutions. 2023. URL: <https://go.chainalysis.com/2023-Crypto-Crime-Report.html>
33. International Financial Reporting Standards (IFRS). (2019). Holding of cryptocurrencies. IFRS Interpretations Committee. URL: <https://www.ifrs.org/news-and-events/2019/06/agenda-decision-cryptocurrencies-june-2019/>
34. Kanu, David Hope. Digital Currencies Financial Reporting and Auditing: A New Concern for Accounting Professionals in the Accounting Industry. 2025. URL: <https://papers.ssrn.com/sol3/Delivery.cfm/5138691.pdf?abstractid=5138691&mirid=1>

Olena PETRYK

Doctor of Economics, Professor, Head of the Department, Kyiv National Economic University named after Vadym Hetman
ORCID: <https://orcid.org/0000-0003-1881-9412>
e-mail: auditlena@ukr.net

Oleh DIAK

postgraduate student, Kyiv National Economic University named after Vadym Hetman
ORCID: <https://orcid.org/0000-0003-0249-924X>
e-mail: olegd1997@gmail.com

PROCEDURES FOR AUDITING FINANCIAL STATEMENTS OF A CRYPTOCURRENCY EXCHANGE AND THEIR TECHNOLOGICAL SEQUENCE

Introduction. The paper is devoted to the scientific and practical substantiation of the basic procedures for auditing the financial statements of a centralized cryptocurrency exchange. Traditional International Standards on Auditing (ISA) are not fully equipped to handle issues such as cryptographic custody, 24/7 market activity, pseudonymous blockchain identifiers, and fragmented regulatory regimes. As a result, audit procedures must evolve to address valuation risks, custody verification, transaction traceability, and reserve confirmation.

The purpose of the paper is to develop a technological audit sequence tailored to the operations of centralized exchanges, combining classical audit planning, control evaluation, and substantive testing with blockchain-native techniques like on-chain verification and cryptographic proofs.

Results. The paper systematizes the features of audit planning in the digital asset environment, which combines continuous global trade, cryptographic verification mechanisms and a dynamic regulatory landscape. A risk-based approach is proposed, which includes an assessment of market volatility, cybersecurity threats, regulatory and jurisdictional requirements for AML/KYC, as well as the risks of storing assets in hot and cold wallets. The algorithm for integrating continuous audit and blockchain analytics is substantiated for operational tracking of high-risk transactions and confirmation of reserves is revealed. A methodology for the combined use of on-chain verification and external depository confirmations is proposed, which increases the reliability of the evidence base and reduces the risk of collusion between the entity and third parties. The procedures essentially describe in detail the random verification of transactions using automated data analysis, confirmation of control over wallets by cryptographic signature of an arbitrary string and a test minimum transaction, as well as the procedure for reconciling internal order books with blockchain records to ensure that transactions are correctly attributed to the reporting period.

Conclusion. By integrating ISA-compliant procedures with cryptographic tools and real-time analytics, the model enhances the credibility of audit conclusions and provides a roadmap for standardizing assurance practices in digital asset markets, contributing to investor trust and regulatory compliance in an evolving financial ecosystem.

Keywords: cryptocurrency audit, asset confirmation, blockchain analytics, audit risks, materiality, control testing, transaction verification, financial statements