КОНЦЕПЦІЯ БУХГАЛТЕРСЬКОГО ОБЛІКУ В УМОВАХ ЦИФРОВОЇ ДЕЦЕНТРАЛІЗАЦІЇ

(НА ЗАСАДАХ БЛОКЧЕЙН-ТЕХНОЛОГІЙ)



ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

КОНЦЕПЦІЯ БУХГАЛТЕРСЬКОГО ОБЛІКУ В УМОВАХ ЦИФРОВОЇ ДЕЦЕНТРАЛІЗАЦІЇ (НА ЗАСАДАХ БЛОКЧЕЙН-ТЕХНОЛОГІЙ)

Монографія

ЕЛЕКТРОННЕ ВИДАННЯ

Ірпінь
2026

УДК 657.1:004
ББК 65.052.2
К 65

Рекомендовано до друку Вченою радою
Державного податкового університету
(протокол № 9 від 19 лютого 2026 року)

Рецензенти:

Малюга Н. М., доктор економічних наук, професор, завідувач кафедри бухгалтерського обліку, оподаткування та аудиту Поліського національного університету;

Ізмайлов Я. О., доктор економічних наук, професор, професор кафедри адміністрування податків Державного податкового університету.

Автори:

Мискін Ю. І., доктор економічних наук, професор, професор кафедри економічної політики, маркетингу та бізнес-аналітики; **Краєвський В. М.,** доктор економічних наук, професор, декан факультету податкової справи, обліку та аудиту; **Мискіна О. О.,** кандидат економічних наук, доцент кафедри адміністрування податків; **Іщенко В. В.,** кандидат економічних наук, доцент кафедри економічної політики, маркетингу та бізнес-аналітики.

К 65 **Концепція бухгалтерського обліку в умовах цифрової децентралізації (на засадах блокчейн-технологій)** : монографія [Електронне видання] / Ю. І. Мискін, В. М. Краєвський, О. О. Мискіна, В. В. Іщенко. – Ірпінь : Державний податковий університет, 2026. – 174 с. – PDF-формат ; мережеве видання ; інституційний репозитарій.
ISBN 978-966-337-803-9

У монографії розкрито напрями трансформації бухгалтерського обліку в умовах цифрової децентралізації через призму блокчейн-технологій. Для науковців, бухгалтерів, аудиторів, викладачів і студентів ця книга стане основою для нового розуміння обліку як цифрової інфраструктури економічної довіри. Вона не просто описує технології, а розкриває їхній вплив на методологію, організацію й професійну роль бухгалтера, окреслюючи перехід від централізованого контролю до самоверифікованої та інтелектуально керованої системи обліку.

УДК 657.1:004
ББК 65.052.2

© Мискін Ю. І., Краєвський В. М.,
Мискіна О. О., Іщенко В. В., 2026
© Державний податковий університет, 2026

ISBN 978-966-337-803-9

ЗМІСТ

ВСТУП 5

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ БУХГАЛТЕРСЬКОГО ОБЛІКУ В УМОВАХ ЦИФРОВОЇ ДЕЦЕНТРАЛІЗАЦІЇ 8
1.1. Еволюція наукових підходів до розуміння сутності бухгалтерського обліку в цифровій економіці 8
1.2. Концепт цифрової децентралізації: економічний зміст і вплив на інститути обліку 14
1.3. Теоретичні основи цифровізації бухгалтерського обліку на основі блокчейн-технологій 22
1.4. Методологічні принципи формування нової облікової парадигми на засадах децентралізації та прозорості інформації 22
Висновки до розділу 1 39

РОЗДІЛ 2. КОНЦЕПТУАЛЬНІ ЗАСАДИ ІНТЕГРАЦІЇ ТЕХНОЛОГІЇ БЛОКЧЕЙН У БУХГАЛТЕРСЬКИЙ ОБЛІК 42
2.1. Архітектура децентралізованого облікового середовища: суб'єкти, об'єкти, інформаційні потоки 42
2.2. Механізм функціонування блокчейн-реєстру у відображенні господарських операцій 53
2.3. Смартконтракти як інструмент автоматизації облікових процедур і контролю достовірності даних 67
2.4. Методика облікової оцінки, визнання та верифікації фактів господарської діяльності у блокчейн-системах 79
2.5. Стандартизація та уніфікація облікових процедур у контексті використання децентралізованих технологій 90
Висновки до розділу 2 104

РОЗДІЛ 3. ОРГАНІЗАЦІЙНО-ПРИКЛАДНІ АСПЕКТИ БУХГАЛТЕРСЬКОГО ОБЛІКУ В УМОВАХ ЗАСТОСУВАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ 107
3.1. Модель організації облікового процесу в середовищі цифрової децентралізації 107
3.2. Ризики та етичні виклики блокчейн-орієнтованого обліку 117
3.3. Перспективи розвитку нормативно-правового забезпечення та професійних стандартів у сфері децентралізованого обліку 133
3.4. Напрями подальшої еволюції облікової науки під впливом цифрової децентралізації 149
Висновки до розділу 3 158

ВИСНОВКИ 161

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 165

ВСТУП

Сучасна економіка зазнає стрімкої цифрової трансформації, яка докорінно змінює природу фінансових та управлінських процесів. Однією з найглибших трансформацій стає переосмислення бухгалтерського обліку – традиційно централізованої системи документального контролю – у напрямі формування децентралізованої обліково-аналітичної системи даних. Умови цифрової децентралізації, що ґрунтуються на використанні блокчейн-технологій, створюють нову парадигму облікового мислення, у якій достовірність, прозорість та інваріантність інформації забезпечуються не інституційними структурами, а технологічними механізмами консенсусу й криптографічної верифікації. Саме тому формування наукової концепції бухгалтерського обліку на засадах цифрової децентралізації виступає одним із ключових викликів сучасної економічної науки.

Цифровізація господарських процесів, зростання обсягів транзакцій у реальному часі та поява децентралізованих реєстрів (блокчейн) зумовлюють необхідність перегляду теоретико-методологічних основ бухгалтерського обліку.

Цифровізація облікової системи була і є об’єктом досліджень значної кількості вітчизняних вчених [1–21; 26–35; 61; 83]. Так, В. О. Осмятченко, С. В. Шевчук і Я. О. Ізмайлов обґрунтували напрями адаптації обліку до цифрового середовища [5]. В. В. Муравський розробив концепцію комп’ютерно-комунікаційної форми обліку [16]. У праці Р. Ф. Бруханського і П. Р. Пуцентейла [27] цифровізація розглядається як інструмент підвищення ефективності управління підприємствами. С. Ф. Легенчук, М. П. Городиський та Н. М. Майстренко акцентують на безпеці бухгалтерських даних в умовах Інтернету речей [11]. А в монографії «Accounting and Cybersecurity» В. В. Муравський та З. М. Задорожний розкривають взаємозв’язок між цифровізацією обліку та новими формами управління кіберризиками [61].

Міжнародна наукова думка також активно концентрується на дослідженні потенціалу блокчейн-технологій у бухгалтерському обліку [37–40; 43–50; 52–60; 63–82; 84; 85]. Так, М. Беллуччі, Д. Чеза Б’янкі та Г. Манетті систематизували наукові підходи до використання блокчейну в обліковій практиці [39], а В. Гросу, Д. Ботез, А. Мелега, Р. Кічі, С. Міхайла і А. Маковей показали його антикорупційний ефект [49]. А. Сута і А. Тот виокремили напрями розвитку бухгалтерського обліку

на блокчейні як передумови забезпечення сталого розвитку [77], а Х. Хан, Р. Шівакоті, Р. Джарвіс, К. Морді та Д. Ботчі розглянули взаємодію блокчейну й штучного інтелекту в обліку [50].

Окремий пласт наукових розвідок присвячено впливу блокчейн-технологій на трансформацію облікової парадигми [42; 51; 69; 73; 75; 79; 81; 83].

Дослідження науковців заклали методологічний фундамент для осмислення цифрової природи облікової інформації, проте на сьогодні залишається відсутньою цілісна концепція бухгалтерського обліку, що функціонує на принципах децентралізації, прозорості та самоверифікації даних. Це зумовлює необхідність розробки теоретико-методологічної моделі, яка б поєднувала класичні принципи бухгалтерського обліку з новими технологічними механізмами формування довіри в цифрових мережах.

Сучасні тенденції розвитку обліку свідчать, що блокчейн-технології здатні забезпечити радикально новий рівень достовірності та аналітичності даних. Бухгалтерський облік у цьому контексті перестає бути лише засобом реєстрації господарських фактів і трансформується в систему децентралізованої економічної довіри. Його функціонування в межах блокчейн-архітектури дає змогу інтегрувати процеси фіксації, верифікації, оцінки й звітності в єдиний цифровий цикл, де помилки, маніпуляції чи дублювання інформації усуваються алгоритмічно.

Актуальність дослідження зумовлюється також потребою переосмислення професійної ролі бухгалтера в умовах автоматизації, штучного інтелекту та смартконтрактів. Фахівець нового покоління має бути координатором цифрових потоків, куратором алгоритмів і гарантом етичної легітимності облікових процесів. Так, у центрі нової облікової парадигми перебуває людина як носій професійного судження, яка поєднує економічну інтерпретацію з технологічною компетентністю.

Метою монографії є розробка концепції бухгалтерського обліку в умовах цифрової децентралізації на засадах блокчейн-технологій, обґрунтування її теоретико-методологічних основ та визначення організаційно-прикладних механізмів її реалізації.

Об’єктом дослідження є процес формування та функціонування бухгалтерського обліку в умовах цифрової децентралізації.

Предметом дослідження є теоретико-методологічні, організаційні та практичні засади трансформації бухгалтерського обліку на основі блокчейн-технологій, спрямовані на підвищення достовірності, прозорості та автономності облікової інформації.

Теоретико-методологічну основу дослідження становлять філософські та загальнонаукові методи пізнання економічних і технологічних процесів децентралізації бухгалтерського обліку. Для досягнення поставленої мети та вирішення дослідницьких завдань застосовано такі наукові методи: абстрактно-логічний – для визначення мети, завдань і логіки побудови концепції цифрової трансформації бухгалтерського обліку; історичний – для дослідження еволюції бухгалтерського обліку та етапів його цифровізації; системно-комплексний – для обґрунтування архітектури блокчейн-орієнтованої системи бухгалтерського обліку; спостереження, порівняння, узагальнення та формалізації – для оцінювання ефективності використання децентралізованих технологій у бухгалтерському процесі; логічного узагальнення – для формулювання висновків.

Наукова новизна дослідження полягає у формуванні концепції бухгалтерського обліку в умовах цифрової децентралізації, яка відображає перехід від документально-централізованої моделі фіксації фактів до алгоритмічно верифікованої системи цифрової довіри, у межах якої істинність облікової інформації забезпечується технологічно, а контроль, звітність та аналітика інтегруються в єдиний саморегульований механізм управління економічною реальністю.

Практичне значення одержаних результатів полягає у створенні теоретико-методологічної бази для розроблення нових моделей бухгалтерського обліку, систем внутрішнього контролю, формування облікових стандартів у сфері цифрової економіки, а також у визначенні перспектив розвитку професії бухгалтера в умовах технологічної автономізації та етичної відповідальності за достовірність даних.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ БУХГАЛТЕРСЬКОГО ОБЛІКУ В УМОВАХ ЦИФРОВОЇ ДЕЦЕНТРАЛІЗАЦІЇ

«Коли зникає потреба в посереднику,
з'являється простір для справжньої відповідальності»
Сатоші Накамото (псевдонім автора Bitcoin)

1.1. Еволюція наукових підходів до розуміння сутності бухгалтерського обліку в цифровій економіці

Еволюція наукових підходів до розуміння сутності бухгалтерського обліку в цифровій економіці є складним і багатовимірним процесом, що відображає поступову трансформацію фундаментальних парадигм бухгалтерської науки та практики. На ранніх етапах формування облікової науки у класичному розумінні бухгалтерський облік позиціонувався як механізм суворого контролю за господарськими операціями, основна функція якого полягала в достовірному документальному відображенні фінансових фактів діяльності підприємства. Такий підхід формувався під впливом принципів бухгалтерської точності, юридичної відповідальності та обов'язковості дотримання національних стандартів обліку, що забезпечувало стабільність та передбачуваність інформаційного середовища бізнесу.

Центральним елементом класичної концепції був принцип лінійності та централізованості облікового процесу. Вона передбачала формування єдиного центра обробки облікових даних, де всі господарські операції підлягали документальному підтвердженню, систематизації та відображенню у фінансових звітах. У такій моделі ключовою була роль бухгалтера як незалежного та об'єктивного суб'єкта, що гарантував точність і повноту інформації для зовнішніх користувачів, зокрема інвесторів, податкових органів, державних регуляторів, а також для внутрішніх управлінських структур підприємства. З точки зору теорії інформації, така модель обліку забезпечувала формалізацію і стандартизацію даних, створюючи умови для їхньої порівнянності, достовірності та юридичної значущості, що знайшло пізніше своє теоретичне осмислення в рамках інформаційної теорії обліку в постіндустріальному суспільстві [28].

Водночас класичний підхід був досить обмеженим у здатності оперативно реагувати на зміни ринкового середовища, оскільки обліковий процес був орієнтований на ретроспективну фіксацію подій, а не на прогнозування або інтеграцію нефінансових показників у стратегічне управління. Наукові дослідження того періоду акцентували увагу на методах коректного обчислення, ведення подвійного запису та забезпечення відповідності нормативним вимогам, що забезпечувало стабільність фінансової звітності, проте не враховувало швидкозмінність економічних умов та потребу в більш динамічному управлінні ресурсами.

Класична концепція бухгалтерського обліку сформувала міцну методологічну основу для систематизації господарських операцій та забезпечення їхньої достовірності, водночас вона заклала передумови для подальшого розвитку науки в напрямі інтеграції інформаційних технологій, цифрової аналітики та, згодом, децентралізованих систем управління даними. Ця еволюція підкреслює необхідність переосмислення ролі обліку в сучасних умовах, де критичною стає не лише точність і контроль, а й швидкість, прозорість та інтегрованість облікової інформації в цифрові економічні процеси.

З розвитком інформаційних технологій та посиленням глобалізаційних процесів наукові підходи до бухгалтерського обліку зазнали суттєвої трансформації, що відображало нові вимоги економічного середовища та динаміку бізнес-процесів. У другій половині XX століття наукова думка у сфері обліку поступово відійшла від вузькоформалізованого розуміння обліку як механізму контролю і документальної фіксації господарських операцій. На зміну класичній моделі прийшли концепції інтегрованого та системного обліку, які акцентували увагу на взаємозв'язку фінансових і нефінансових показників діяльності підприємства. Зокрема, розвинулася концепція креативного обліку як створення інформації для менеджерів [22], що свідчило про зміщення акцентів у бік управлінської корисності. Такий підхід давав змогу враховувати не лише фінансові результати, а й ефективність використання ресурсів, якість виробничих та управлінських процесів, рівень інноваційної активності та інші нефінансові детермінанти економічного розвитку.

Ключовою особливістю інтегрованого підходу стало усвідомлення обліку як системи, що забезпечує комплексний та узгоджений аналіз даних, де фінансова інформація взаємопов'язана з оперативними і стратегічними показниками підприємства. Це сприяло формуванню нової методологічної парадигми, яка підкреслює не лише

достовірність, а й своєчасність та релевантність облікової інформації. Наукові дослідження того періоду відзначають потребу в розробці моделей оперативного доступу до даних для забезпечення ефективного управління, що стало важливим чинником підвищення конкурентоспроможності підприємств у глобальному економічному середовищі, що знайшло відображення в дослідженнях перспектив розвитку бухгалтерського обліку, аналізу та аудиту в умовах інноваційних інформаційних технологій [18].

Одночасно значної уваги набули питання автоматизації облікових процесів та застосування аналітичних методів для підтримки управлінських рішень. Бухгалтерський облік перестав бути пасивним інструментом контролю й трансформувався в активний компонент управлінської діяльності, інтегрованої у внутрішні інформаційні системи підприємства. З'явилася можливість моделювання фінансових потоків, прогнозування економічних результатів та оцінювання ризиків на основі накопичених даних, що формувало наукову базу для подальшого розвитку цифрових облікових технологій та інтеграції їх у стратегічне планування. Цей перехід до комп'ютерно-комунікаційної форми обліку та прагнення до створення інтелектуальної системи обліку стали логічним продовженням еволюції облікової думки [16, 23].

Другий етап еволюції наукових підходів до обліку характеризується зміщенням акценту від ретроспективного контролю до інтегрованого, системного підходу, який забезпечує комплексне відображення діяльності підприємства, оперативність інформаційного забезпечення та активну участь обліку в процесі прийняття управлінських рішень. Ця трансформація, яка розглядається в контексті розвитку цифровізації обліку, оподаткування, аналізу й контролю [5; 27] та формування інформаційних ресурсів для бізнесу [25], заклала основу для подальшої цифровізації та децентралізації облікових систем, що є актуальною передумовою для впровадження блокчейн-технологій у бухгалтерську практику.

Сучасна цифрова економіка створює умови для радикальної трансформації бухгалтерської науки та практики, актуалізуючи ідеї децентралізованих технологій, зокрема блокчейн, які формують принципово нові підходи до організації обліку та контролю фінансової інформації. В умовах цифрової децентралізації бухгалтерські системи перестають бути централізованими реєстрами даних, а функціонують як розподілені мережі, де кожна господарська операція відображається

одночасно у всіх вузлах системи. Така архітектура забезпечує незмінність та оперативність обробки облікової інформації, що кардинально змінює традиційні уявлення про функції бухгалтерського обліку як інструменту виключно ретроспективного контролю, що відповідає останнім тенденціям цифровізації обліку [41].

Блокчейн-технології надають бухгалтерському обліку нові методологічні можливості, пов'язані з автоматизацією ведення записів, верифікацією транзакцій у режимі реального часу та забезпеченням високого рівня достовірності даних без участі централізованих посередників. Це створює передумови для формування обліку, у якому інформація про господарські операції стає доступною для аналізу та перевірки в будь-який момент, що значно підвищує ефективність внутрішнього і зовнішнього контролю. Прозорість цифрових реєстрів дає змогу знизити ризики помилок і шахрайства, а незмінність записів гарантує юридичну та фінансову бездоганність даних, що відкриває нові горизонти для розвитку аудиторських процедур та аналітики на основі блокчейн-реєстрів.

Наукові дискусії останніх років акцентують увагу на потенціалі інтеграції цифрових реєстрів у корпоративний та міжкорпоративний облік, де блокчейн є технологічною основою для створення єдиної інформаційної екосистеми підприємств. Така інтеграція дає змогу забезпечити безперервний моніторинг господарських операцій, автоматичну синхронізацію даних між контрагентами та підвищує ефективність аудиторського контролю за рахунок доступу до достовірної та повної інформації без необхідності централізованого підтвердження. Це зі свого боку сприяє підвищенню довіри між економічними суб'єктами, оптимізації управлінських рішень та формуванню умов для широкомасштабної цифровізації бухгалтерських і фінансових процесів, реалізуючи ідеї, висунуті ще в концепції ідеальної системи обліку [24].

Впровадження децентралізованих технологій у сучасну бухгалтерську практику не лише змінює функціональні параметри облікових систем, а й трансформує саму сутність облікового процесу, створюючи умови для формування якісно нового наукового підходу до облікової інформації. У традиційній системі бухгалтерського обліку центральні інститути є гарантом достовірності та цілісності даних, тоді як у децентралізованому середовищі ці функції покладаються на технологічний механізм розподіленого реєстру. Такий підхід зумовлює перехід від централізованих моделей облікової довіри до технологічно

забезпеченого механізму колективної верифікації, який унеможливлює маніпулювання інформацією та забезпечує її непідробність.

В умовах цифрової децентралізації відбувається докорінна зміна принципів організації бухгалтерських процесів. Інформація перестає бути лише відображенням господарських операцій – вона стає активом, який функціонує у глобальному цифровому середовищі, взаємодіє з іншими економічними системами.

Узагальнюючи викладений матеріал, представимо еволюцію наукових підходів до розуміння сутності бухгалтерського обліку у формі таблиці 1.1.

Таблиця 1.1 – Еволюція наукових підходів до розуміння сутності обліку

№	Назва етапу розвитку	Часовий інтервал	Коротка характеристика
1	2	3	4
1.	Класичний етап розвитку бухгалтерського обліку	кінець XIX – перша половина XX століття	На цьому етапі бухгалтерський облік формувався як механізм контролю та документального підтвердження господарських операцій. Основна увага приділялася точності, юридичній відповідальності та відповідності нормативним вимогам. Система обліку мала централізований, лінійний характер і виконувала переважно ретроспективну функцію. Облік розглядався як самодостатня дисципліна, спрямована на формування достовірної фінансової звітності, орієнтованої на зовнішніх користувачів (інвесторів, державу, контролювальні органи)
2.	Етап інтегрованого та системного підходу до обліку	друга половина XX століття	Облік почали розглядати як елемент єдиної інформаційної системи управління підприємством. З’явилися концепції інтегрованого обліку, що поєднує фінансові та нефінансові показники. Акцент змістився на оперативність та аналітичність облікової інформації, яку почали використовувати для підтримки управлінських рішень. Важливого значення набули процеси автоматизації, моделювання фінансових потоків і прогнозування, що підготувало базис для подальшої цифровізації

Продовження таблиці 1.1

1	2	3	4
3.	Етап цифрової трансформації бухгалтерського обліку	кінець XX – початок XXI століття	Цей етап характеризується активною інтеграцією інформаційних технологій у бухгалтерський процес. З'являються комп'ютеризовані системи обліку, ERP-рішення та електронна звітність. Облік поступово стає частиною цифрового управлінського циклу, орієнтованого на реальний час. Наукові дослідження цього періоду фокусуються на інформаційній функції обліку, аналітичних технологіях, швидкості обробки даних і релевантності інформації, що формує підґрунтя для подальшої цифрової децентралізації
4.	Етап становлення обліку в умовах цифрової децентралізації	початок XXI століття – сучасність	Сучасна парадигма бухгалтерського обліку формується під впливом блокчейн-технологій. Облік перестає бути централізованим реєстром і трансформується в розподілену мережу взаємодії учасників економічних процесів. Ключовими принципами стають прозорість, незмінність та алгоритмічна верифікація. Така модель забезпечує автоматичну верифікацію транзакцій, зниження ризиків фальсифікації та формує основу для нової облікової парадигми – обліку як інтегрованої частини цифрової економіки, заснованої на довірі без посередників

Джерело: складено авторами.

Так, еволюція наукових підходів до бухгалтерського обліку відображає поступовий перехід від централізованих і документально орієнтованих моделей до цифрово-орієнтованих, децентралізованих систем, які поєднують функції контролю, аналітики та управління в умовах глобальної інформаційної економіки. Цей процес формує нову парадигму обліку, у якій ключовими стають не лише точність і повнота даних, а й їхня оперативність, прозорість та інтеграція в екосистеми цифрового бізнесу.

1.2. Концепт цифрової децентралізації: економічний зміст і вплив на інститути обліку

Цифрова децентралізація як новітній економіко-організаційний феномен відображає процес перерозподілу владних, управлінських і контрольних повноважень від централізованих суб'єктів до розподілених цифрових мереж. Її сутність полягає у відмові від традиційної ієрархічної моделі обміну даними та прийняття рішень на користь горизонтальних систем, де учасники володіють рівними правами доступу, перевірки та верифікації інформації. У своїй основі цифрова децентралізація ґрунтується на технологічних механізмах, серед яких провідне місце належить блокчейн-технологіям, що забезпечують достовірність, незмінність і відкритість даних без потреби в посередницьких структурах, про що свідчать дослідження суті та сфер використання цих технологій [2; 3].

З економічної точки зору перехід довіри з інституційної в технологічну площину означає не просту технічну зміну носія інформації, а фундаментальну трансформацію механізмів формування, розподілу й забезпечення ресурсів довіри в господарських відносинах. У традиційній моделі довіра була продуктом інституційних гарантій – правового порядку, ліцензованих посередників, банківських та аудиторських процедур, репутаційних санкцій і державного примусу. Ці інститути оперували як зовнішні гаранти верифікації фактичних господарських подій, надавали економічним агентам сигнали про достовірність інформації і несли транзакційні витрати, пов'язані з ухиленням від ризику та асиметрією інформації. В умовах цифрової децентралізації частина цих функцій поступається алгоритмічним механізмам: криптографічні протоколи, розподілені реєстри та смартконтракти забезпечують властивості записів – автентичність, цілісність, незмінність і підзвітність у часі – без необхідності централізованого довірчого посередника, що розглядається в контексті організації, управління та довіри до «блокчейн-обліку» [68].

Економічний зміст такої заміни довіри полягає у перерозподілі транзакційних витрат і ризиків. По-перше, знижується інформаційна асиметрія між партнерами завдяки відкритому або контрольовано відкритому доступу до первинних записів у розподіленому реєстрі, що зменшує витрати на перевірку та скорочує потребу в повторних

верифікаціях. По-друге, зникає або скорочується рента, яку традиційно отримували посередники за надання гарантій достовірності; натомість виникають нові механізми винагороди – токенізовані стимули, механізми стейкінгу або винагороди за участь у консенсусі, які перерозподіляють економічні вигоди між учасниками мережі. По-третє, трансформуються мотиваційні структури: контроль довіри більше покладається на криптоекономічні стимули й протидії атакам (наприклад, відсікання зловмисників через економічні штрафи), натомість соціальні санкції і регуляторний тиск зберігають роль, але в новому, комплементарному форматі.

Ця технологічна трансформація довіри змінює базові інструменти економічного контролю та звітності. У розподілених системах верифікація операцій може відбуватися в режимі реального часу або з мінімальною затримкою: консенсусні алгоритми гарантують порядок і долучення транзакцій, а криптографічні підписи дають змогу встановити виявлення джерела даних. Смартконтракти забезпечують автоматичне виконання узгоджених правил обліку та розрахунків, що знижує потребу в ручних узгодженнях і корегуваннях. У результаті звітність може набувати статусу постійно оновлюваної цифрової істини, доступної різним зацікавленим сторонам із різними рівнями доступу, що створює передумови для переходу від періодичного фінансового звіту до безперервного аналітичного моніторингу, як це передбачають принципи проєктування облікових систем на основі розподілених реєстрів [37].

Водночас алгоритмічна довіра не є ідеальною заміною інституційної. По-перше, технологічні протоколи забезпечують технічні гарантії лише щодо цілісності та послідовності даних у межах реєстру; вони не можуть самі по собі гарантувати правдивість зовнішніх фактів або коректність введення первинних даних, що постачають дані у блокчейн. По-друге, алгоритми вразливі до технічних ризиків: помилки в коді смартконтрактів, дефекти у протоколах консенсусу або атаки на мережу створюють нові джерела ризику, які мають економічні наслідки (наприклад, крадіжки, подвійні витрати, збої у виконанні зобов'язань). По-третє, частина економічних атрибутів довіри – юридична відповідальність, право на відшкодування, податкові наслідки – залишається предметом правової системи і вимагає інтеграції технологічних рішень із нормативно-правовим полем.

Перехід довіри в технологічну площину породжує складну взаємодію між ринковими інститутами та цифровими протоколами: інститути перестають повністю витіснятися, натомість вони реінтерпретуються й реорієнтуються. Регулятори, аудиторські організації та стандарт-сетери отримують нові ролі – не лише як верифікатори фактів, а як сертифікатори протоколів, оцінювачі криптографічної належності, аудитори смартконтрактів та наглядачі за системами оракулів і механізмами управління мережею. Для економіки це означає, що витрати на забезпечення довіри не зникають, але змінюють свою структуру: вони переміщуються від витрат на підтримку великих централізованих апаратів до витрат на розробку, аудит і супровід розподілених протоколів та на створення правового середовища, здатного визнавати цифрові докази.

Нарешті, важливо відзначити, що технологічна довіра породжує як позитивні зовнішні ефекти (підвищення прозорості, зниження транзакційних бар'єрів, стимулювання інновацій), так і негативні – концентрацію технічної влади в руках розробників протоколів, ризики стандартизації помилок, можливість регуляторного арбітражу та проблеми приватності й контролю доступу до даних. Для бухгалтерського обліку як науки і практики це означає необхідність розробки методологій, що інтегрують криптографічні гарантії у традиційні критерії достовірності, забезпечують адекватну інтерпретацію цифрових доказів у правовому полі та формують нові підходи до аудиту, контролю та професійної етики в умовах цифрової де централізованості облікових процесів.

У парадигмі цифрової децентралізації інститути бухгалтерського обліку втрачають статус виключного посередника у формуванні інформаційної бази для прийняття управлінських рішень і одночасно набувають низку нових, більш комплексних функцій. Замість монополії на реєстрацію й консолідацію первинних записів бухгалтерські служби стають архітекторами та інтеграторами розподілених інформаційних систем: вони беруть участь у визначенні логіки облікових подій, структурі метаданих, правилах токенізації активів і механізмах консенсусу, що забезпечують автоматичну верифікацію транзакцій. Така еволюція передбачає переклад частини операційних функцій на алгоритмічні механізми (смартконтракти, автоматизовані верифікатори), але зберігає за обліковою професією роль гаранта семантичної коректності бізнес-логіки та адекватності облікових правил до економічної

сутності операцій, що розглядається як ключовий засіб трансформації обліку [8].

Функціональна трансформація охоплює кілька взаємопов'язаних напрямів. По-перше, зростає значення проєктування і контролю джерел даних – бухгалтер має формулювати вимоги до сенсорних систем та інтерфейсів, через які зовнішні факти потрапляють у розподілений реєстр, забезпечуючи тим самим інваріантність облікових категорій і зменшуючи ризик маніпуляцій на етапі первинного введення. По-друге, виникає потреба в управлінні правами доступу та політиками приватності: бухгалтерські системи повинні поєднувати принцип прозорості розподіленого реєстру з регуляторними і контрактними вимогами щодо конфіденційності та селективного розкриття інформації. По-третє, роль внутрішнього контролю трансформується в постійну валідацію алгоритмічних правил і процедур – не лише перевірку виконання транзакцій, але й аудит смартконтрактів, конфігурацій консенсусу та механізмів оновлення протоколів.

Перехід обліку в режим реального часу змінює підходи до оцінювання і представлення інформації. Оцінка активів і зобов'язань дедалі більше базується на потоках подій і автоматичних тригерах, що вимагає адаптації методик вимірювання – від фіксованих періодичних переоцінок до безперервних процедур облікової оцінки з використанням алгоритмічних правил і статистичних моделей. Це породжує потребу в нових підходах до документування припущень і конфігурації смартконтрактів у формі криптографічно підписаних доказів, які можуть бути юридично значущою підставою для звітності. Водночас з'являються вимоги до стандартизації метаданих та уніфікації схем токенізації, щоб забезпечити інтероперабельність різних реєстрів та адекватне зіставлення облікових показників у мультисистемних середовищах.

Професійний портрет бухгалтера змінюється: традиційні навички реєстрації та калькуляції доповнюються компетенціями в інформаційних технологіях, криптографії, аналізі даних і менеджменті цифрових ризиків. Бухгалтер стає аналітиком і координатором інформаційних потоків, відповідальним за формування, інтерпретацію та представлення цифрових доказів економічної діяльності. Це означає, що кадрова політика підприємств, освітні програми і професійні стандарти мають інтегрувати курси з розробки смартконтрактів, принципів консенсусу та етичних аспектів автоматизованих рішень.

Інституційні наслідки стосуються перерозподілу ролей між внутрішніми службами, регуляторами, аудиторами та розробниками протоколів. Аудитори поступово втрачають монопольну роль з підтвердження достовірності звітності, але набувають нової – надання впевненості у працездатності та безпеці автоматизованих облікових механізмів, перевірці коду смартконтрактів і процедур управління ключами. Регулятори вимушені переосмислити критерії прийнятності цифрових доказів, механізми ліцензування і сертифікації технологічних рішень, а підприємства – вбудувати відповідні процеси корпоративного управління та управління ризиками в цифрову інфраструктуру.

Разом із перетвореннями виникають і значні виклики. Залежність від складності верифікації зовнішніх фактів, ризиків помилок у коді й уразливості протоколів формують нові джерела операційного і репутаційного ризику. Перехід від традиційних систем і практик обліку та звітності до обліку на основі цифрової децентралізації потребує розробки проміжних інструментів і стандартизованих перехідних процедур. Крім того, постає проблема розмежування відповідальності й правової підзвітності за автоматичне виконання облікових правил, що вимагає кооперації між фахівцями бухгалтерії, IT-експертами та юристами для розробки адекватних моделей відповідальності та страхових механізмів.

Перетворення бухгалтерського обліку з адміністративного інструменту в інтегровану частину цифрової інфраструктури є не лише технічною модернізацією, а глибокою інституційною трансформацією. Воно вимагає синергії нових методологій обліку, оновлених професійних компетенцій і адаптивних правових режимів, що разом забезпечать надійну, зрозумілу й контрольовану роботу розподілених облікових систем за децентралізованого підходу.

Цифрова децентралізація на структурному рівні спричиняє радикальну переорієнтацію архітектури облікових систем: централізовані бази даних замінюються на розподілені реєстри, у яких кожен уповноважений учасник має власну консистентну копію бухгалтерської інформації. Така архітектоніка змінює моделі збереження й реплікації даних – від простого клієнт-серверного зберігання до консенсусно-орієнтованих протоколів, що гарантують послідовність записів і стійкість до окремих відмов. У практичному вимірі це означає, що класичні «єдині джерела істини» еволюціонують у множинні, криптографічно пов’язані джерела, де автентичність записів забезпечується

не довірою до центру, а криптографічними доказами (підписи, хеші, Merkle-дерева) та механізмами консенсусу (PoW, PoS, BFT-варіанти тощо). Технічно така модель знижує можливість локальних маніпуляцій і спотворень, оскільки будь-яка спроба змінити історію транзакцій потребує компрометації значної частини учасників мережі або контролю над консенсусним механізмом.

Перехід до розподілених реєстрів має істотні наслідки для управління даними та корпоративної IT-інфраструктури. По-перше, зростає значення інтероперабельності й стандартизації метаданих: для зіставлення записів між різними реєстрами та системами потрібні уніфіковані семантичні словники і схеми токенізації активів. По-друге, змінюється модель зберігання конфіденційної інформації – замість централізованого контролю дані можуть розподілятись за моделлю «повний реєстр – зашифровані поля – селективне розкриття», що ставить вимогу до впровадження криптографічних протоколів приватності. По-третє, архітектонічні зміни породжують нові вимоги до масштабованості та продуктивності: розподілені системи повинні забезпечувати високопродуктивну обробку транзакцій зі збереженням консенсусної безпечності, що стимулює розвиток шарів агрегування транзакцій і гібридних підходів із частковою централізацією для критичних навантажень.

Функціонально цифрова децентралізація трансформує сутність облікових процедур. Автоматизація верифікації операцій, реалізована через смартконтракти та оркестрацію автоматичних тригерів, спрямовує систему від реактивного постфактумного обліку до проактивного, безперервного моніторингу. Смартконтракти дають змогу закласти облікові правила й бізнес-логіку в код, що призводить до автоматичного визнання економічних подій, розрахунку нарахувань, блокування ресурсів або виконання платежів за настання умов. Це зменшує людський чинник у рутинних облікових операціях та скорочує час узгоджень, але водночас переносить частину відповідальності на коректність алгоритмічної імплементації правил.

Для аудиту і внутрішнього контролю такий функціональний зсув означає зміну парадигми підтвердження достовірності: класичний вибірковий постаудит має доповнюватись аудитом протоколів, кодів смартконтрактів і механізмів управління ключами. Безперервний аудит у режимі реального часу стає можливим завдяки доступу

до реплік реєстру та криптографічних доказів; натомість з'являються нові завдання – верифікація джерел зовнішніх даних, тестування сценаріїв атаки на консенсус та оцінювання ризику поведінкових стимулів у криптоекономіці. Такі зміни змушують аудиторські стандарти розширити охоплення, долучивши критерії оцінювання технічної безпеки, процедур оновлення протоколів та відновлення після інцидентів.

Наслідки для корпоративного управління і відповідальності також є фундаментальними. Розподілена архітектура потребує нових механізмів управління версіями смартконтрактів та процедур внесення змін до логіки обліку. Виникає потреба у створенні ролей, що відповідають за аудиторський супровід протоколів, управління ключовими інфраструктурними елементами та координацію між розробниками, бухгалтерами і юристами. Паралельно з тим змінюється модель розподілу витрат: зменшується потреба в централізованих людських ресурсах для рутинних перевірок, але зростають витрати на розробку, кібербезпеку та відповідність регуляторним вимогам.

Водночас структурні й функціональні переваги децентралізації не є універсальною панацеєю: підвищена прозорість реєстрів може вступати в конфлікт із вимогами конфіденційності, а забезпечення одночасної цілісності й масштабованості залишається технічно складною задачею. Ризики помилок у смартконтрактах, неналежної конфігурації консенсусу або компрометації зовнішніх даних створюють нові вектори операційного і юридичного ризику, які потрібно врегулювати через комбіновані техніко-організаційні заходи: багатоступеневе тестування, формалізовані процедури верифікації, страхові механізми та адаптивне регулювання.

Отже, вплив цифрової децентралізації на інститути обліку виявляється у глибокому переосмисленні як технічних, так і методологічних засад обліку: структурна реорганізація інформаційних архітектур і функціональна автоматизація контрольних процедур взаємодіють, створюючи середовище, де достовірність даних забезпечується поєднанням криптографічних доказів, алгоритмічних правил і нових форм інституційного нагляду. Це формує високі вимоги до оновлення професійних стандартів, технологічної компетенції та нормативного супроводу, але й відкриває значні можливості для підвищення ефективності, прозорості та швидкості прийняття економічних рішень.

Порівняльна характеристика традиційної моделі бухгалтерського обліку та моделі бухгалтерського обліку в умовах цифрової децентралізації наведена в таблиці 1.2.

Таблиця 1.2 – Порівняльна характеристика традиційної моделі бухгалтерського обліку та моделі бухгалтерського обліку в умовах цифрової децентралізації

Критерій порівняння	Порівняльна характеристика моделей бухгалтерського обліку	
	Традиційна модель бухгалтерського обліку	Модель бухгалтерського обліку в умовах цифрової децентралізації
Коротка характеристика	Базується на централізованій організації облікових даних, де їх формування, оброблення й контроль здійснюються в межах підприємства або регулятора. Надійність інформації забезпечується нормативними процедурами, аудитом і людським контролем	Спирається на блокчейн-технології, що забезпечують фіксацію й підтвердження операцій без централізованого посередника. Дані зберігаються в розподіленому реєстрі, а достовірність гарантується криптографічними механізмами
Основні особливості	Наявність єдиного центру зберігання даних, періодичність облікових процедур, залежність від людського чинника та часові затримки між подією і її відображенням. Достовірність інформації визначається інституційною довірою, а не технологічними гарантіями	Прозорість, незмінність записів, автоматична верифікація через смартконтракти та моніторинг у реальному часі. Роль бухгалтера трансформується від реєстратора до аналітика та координатора інформаційних потоків
Умови для практичного провадження	Потребує централізованої інфраструктури, стандартів обліку, аудиторської системи та кваліфікованих кадрів	Потребує цифрової інфраструктури, правового визнання електронних транзакцій, кіберзахисту та фахівців із міждисциплінарними компетенціями
Ризики	Можливість маніпуляцій, втрати або спотворення даних, обмежена прозорість і неефективність у середовищі великих обсягів транзакцій	Технологічні збої, уразливість смартконтрактів, регуляторна невизначеність і складність інтеграції з традиційними системами

Джерело: складено авторами.

Отже, концепт цифрової децентралізації формує нову методологічну базу бухгалтерського обліку, в якій об'єктом аналізу стає не лише економічна діяльність суб'єктів, а й цифрова взаємодія між ними в межах розподілених мереж. Цей процес вимагає переосмислення традиційних принципів достовірності, повноти та нейтральності облікової інформації, які набувають технологічного наповнення. Відтак цифрова децентралізація не просто змінює технічні засоби обліку – вона трансформує його інституційну сутність, переводячи бухгалтерський облік у нову фазу розвитку як інструмент довіри в цифровій економіці.

1.3. Теоретичні основи цифровізації бухгалтерського обліку на основі блокчейн-технологій

Цифровізація бухгалтерського обліку на основі блокчейн-технологій є новітнім етапом еволюції облікової теорії, що передбачає перехід від централізованих інформаційних систем до децентралізованих цифрових платформ, у межах яких забезпечується повна прозорість, достовірність і безперервність облікових процесів. Теоретично ця трансформація ґрунтується на синтезі концепцій інституціональної економіки, теорії інформації та кібернетичного підходу до управління, де бухгалтерський облік розглядається як інтегрована частина цифрового середовища, а не як автономна підсистема господарського механізму. Блокчейн є технологічним ядром цієї концепції, адже забезпечує новий формат довіри – алгоритмічний, який замінює соціально-інституційні гарантії верифікації даних технологічними, що знаходить підтвердження в дослідженнях впливу блокчейн-технології на бухгалтерський облік та аудит [40].

У межах блокчейн-орієнтованої цифровізації бухгалтерського обліку відбувається фундаментальне переосмислення сутності облікової інформації: вона перестає бути пасивним відображенням минулих господарських фактів і набуває статусу самопідтверджуваного цифрового запису. Кожна транзакція, зафіксована в розподіленому реєстрі, супроводжується криптографічними доказами автентичності (цифровими підписами, хешами, Merkle-посиланнями) та проходить процедуру підтвердження консенсусом мережі, що робить одноособову

модифікацію історії технічно складною або неможливою без широкої співучасті учасників. У такому контексті первинний запис перестає бути настільки вразливим до суб'єктивних корегувань чи адміністративних впливів, оскільки його статус підтверджується не лише внутрішньою процедурою підприємства, а криптографічною непротирічністю відтворюваності в усіх вузлах мережі, що підтверджує можливість використання блокчейну для цілей обліку [45].

Така трансформація має прямі наслідки для концепції довіри й стандартів достовірності: замість зовнішніх гарантій, що походять від інституційних посередників, роль гаранта інформації переходить до технологічних механізмів – консенсусних алгоритмів, механізмів управління ключами та процедур управління доступом. Це створює передумови для переходу від періодичного (професійного) підтвердження звітності до моделі «аудиту в реальному часі», коли підтвердження фактів та автоматичний моніторинг виконання облікових правил можуть здійснюватися безпосередньо за допомогою вбудованих алгоритмів та інструментів аналітики. Внаслідок цього змінюється і часовий характер інформації: облікові дані починають функціонувати як синхронізовані потоки подій, які забезпечують оперативність управлінських рішень і знижують інформаційні лаги між подією та її відображенням, що є прямим ефектом від впровадження сучасних інформаційних технологій в облік [1].

Однак технічна незмінність записів не автоматично означає істинність змісту: виникає класичне питання «гарантії походження даних». Якщо зовнішні факти потрапляють у блокчейн через проміжні джерела або прилади збору даних, то можливі помилки, зумисні викривлення або технічні збої на етапі введення залишаються значущими. Отже, статус самопідтверджуваного запису підлягає доповненню процедурою гарантії якості джерел даних: багатоканальною верифікацією, застосуванням методів криптографічного шифрування і механізмів доказової цілісності на кордоні між фізичними подіями й їх цифровими репрезентаціями. Така інтеграція технічних та організаційних гарантій стає ключовим напрямом методології обліку в децентралізованих системах, що відповідає аналізу основних можливостей та ризиків цифрових технологій в обліку [4].

Поява можливості «аудиту в реальному часі» вимагає перегляду аудиторських процедур і стандартів надання впевненості. Традиційні

вибіркові підходи мають бути доповнені інструментарієм аудиту протоколів, перевірки механізмів консенсусу, тестування сценаріїв виходу з непередбачуваних станів та оцінювання кіберризиків. Аудиторське оцінювання повинно поєднувати аналіз безперервних цифрових слідів у реєстрі з верифікацією джерел зовнішніх даних і контролем над процедурами управління ключами та доступом. Нова методологія аудиту повинна також акумулювати підходи формального верифікування коду та тестування інтеграційних сценаріїв, що дасть змогу адекватно інтерпретувати цифрові докази облікових фактів.

Трансформація облікових даних у динамічні потоки також ставить нові вимоги до методик оцінювання, документування припущень і відображення невизначеності. Базові принципи обліку – відповідність економічній суті, повнота та нейтральність – потребують технологічного втілення у вигляді уніфікованих метаданих, стандартів токенізації активів і процедур верифікації облікових правил у кодованому вигляді. Водночас для практичного застосування потрібні правові рамки, які визнають криптографічні докази як допустимі джерела облікової інформації та врегулюють питання відповідальності під час автоматичного виконання смартконтрактів. Лише поєднання технологічних гарантій, методологічних стандартів і нормативно-правового визнання дасть змогу перетворити самопідтверджувані записи блокчейну на надійну основу для повноцінної бухгалтерської звітності та управлінської аналітики, що є центральним питанням для сучасних наукових досліджень обліково-аналітиченого спрямування [48].

Теоретичні основи цифровізації бухгалтерського обліку на базі блокчейн-технологій вимагають формалізації нової логіки побудови облікових систем, у якій центральними координатами є принципи децентралізації, прозорості, незмінності та автоматичної верифікації даних. Децентралізація перестає бути лише технічною характеристикою мережі – вона стає організаційно-методологічним принципом, що змінює уявлення про джерела істини: замість одного централізованого реєстру існують множинні, криптографічно зв’язані репліки, доступ до яких регламентується ролями, правами і політиками селективного розкриття. Прозорість у такій системі має подвійний характер – вона підвищує зворотну видимість господарських фактів для зацікавлених сторін одночасно з вимогою реалізувати механізми захисту конфіденційності; незмінність записів підвищує показники відтворюваності

й довіри, але зумовлює необхідність нових процедур корегування у випадку встановлення помилок або юридично обґрунтованих змін у записах.

Інтеграція обліку в цифровий управлінський цикл означає, що облікова інформація перестає бути виключно ретроспективним звітом і стає оперативним елементом планування, прогнозування та аналітики. Потоки транзакцій у реальному часі дають змогу моделювати ліквідність, ризики і фінансові показники на основі безперервно оновлюваних даних, що змінює часову динаміку прийняття рішень і знижує латентність інформації. Методологічно це вимагає переходу до процедур, які комбінують облікові стандарти з техніками безперервної обробка даних у реальному часі та інструментами аналітики для забезпечення коректного інтерпретування подій як облікових фактів у режимі реального часу, що відповідає сучасним тенденціям використання інформаційних технологій у бухгалтерському обліку [9].

Смартконтракти є ключовим інструментом технологічного детермінізму: вони кодують правила визнання, оцінювання та розкриття економічних подій і забезпечують автоматичне виконання договірних умов із одночасним відображенням у реєстрі. Така автоматизація підсилює предиктивний аспект обліку – наприклад, автоматичне нарахування відсотків, тригерне визнання доходу або умовне блокування активів, яке виконуються без людського втручання згідно з формалізованими умовами. З методологічної точки зору це вимагає формалізації облікових правил у формі, яку розпізнає і розуміє техніка, стандартизації метаданих та розробки процедур верифікації коректності коду як самостійного артефакту облікового процесу, що є ключовим аспектом упровадження блокчейну в облік [53].

Наслідком зазначеного детермінізму є переформатування ролей професійних агентів: бухгалтер перестає бути лише реєстратором і перетворюється на аналітика, системного дизайнера та контролера алгоритмічних правил. Нова парадигма вимагає гібридних компетенцій – від розуміння облікових принципів до навичок формального опису бізнес-логіки, оцінювання ризиків смартконтрактів та управління цифровими ключами й правами доступу. Це зі свого боку пред'являє вимоги до навчальних програм, професійних стандартів і внутрішніх процедур корпоративного управління, що підтверджує суттєвий вплив технології блокчейн на бухгалтерський облік [64].

Водночас технологічний детермінізм не є абсолютом: він ставить виклик забезпеченню походження і якості даних, сумісності стандартів токенізації активів та інтероперабельності реєстрів. Теоретичною відповіддю на ці виклики має стати розробка концепції гібридної валідності, що поєднує криптографічні гарантії реєстру з процедурними гарантіями походження даних (сертифікація джерел, багатоканальна верифікація, ланцюжкова відповідальність). Це також потребує формалізації метаданих, правил токенізації та схем відображення економічних прав у цифровому середовищі для забезпечення коректності облікового вимірювання і звірки.

Нарешті, впровадження концепції вимагає узгодженого нормативно-правового середовища: визнання цифрових записів як доказової бази, регламентації відповідальності за автоматичного виконання смартконтрактів, стандартів аудиту протоколів і механізмів управління оновленнями правил у мережі. Лише синтез технологічних рішень, методологічних підходів і правового визнання дасть змогу перетворити принципи децентралізації, прозорості, незмінності й автоматичної верифікації на стійку, аналітично значущу основу сучасного бухгалтерського обліку, що є основним змістом впровадження блокчейн-технології в облік [57].

У методологічному вимірі цифровізація бухгалтерського обліку на засадах блокчейн-технологій зумовлює необхідність глибокого переосмислення фундаментальних категорій облікової науки – активів, зобов’язань, доходів і витрат – через призму їхньої цифрової природи та форм репрезентації у децентралізованому інформаційному середовищі. У традиційній парадигмі ці категорії фіксують економічні ресурси та зобов’язання у формі документально підтверджених фактів, що зберігаються в централізованих облікових системах. Натомість у блокчейн-орієнтованому середовищі об’єкти обліку набувають цифрового формату існування, у якому їхня автентичність, обсяг прав власності та вартісне вираження забезпечуються не актом реєстрації людиною, а алгоритмічним протоколом, який фіксує, підтверджує і захищає дані в розподіленому реєстрі.

Цифрові активи в такій системі постають не лише як цифрові відображення реальних ресурсів, але й як самостійні об’єкти економічних відносин, що мають власну вартість, ліквідність і правовий статус у межах блокчейн-екосистеми. Токенізація матеріальних і нематеріальних

ресурсів створює умови для їх уніфікованої облікової ідентифікації та обігу, оскільки кожен токен є криптографічно унікальним і невід'ємно пов'язаним із власником. У цьому контексті поняття активу набуває подвійного змісту: як економічного ресурсу в традиційному розумінні та як цифрового запису в децентралізованій базі даних, що гарантує право власності без посередників. Зобов'язання зі свого боку можуть існувати у формі смартконтрактів – алгоритмів, які автоматично виконують умови господарських договорів і тим самим трансформують концепцію зобов'язань із декларативної у виконавчу площину.

Автоматизовані потоки платежів і смартзобов'язання змінюють методику відображення господарських подій у часі, сприяючи переходу до концепції обліку в режимі реального часу. Оцінювання об'єктів господарського обліку більше не може базуватися виключно на історичній вартості або експертних судженнях – воно стає функцією алгоритмічних процедур, що враховують поточні ринкові параметри, коди ризиків, а також автоматичну зміну вартості активів у результаті подій, зафіксованих у блокчейні. Це означає, що облікові оцінки стають не лише аналітичними, а й інтерактивними – їх формування забезпечується безперервною взаємодією з цифровим середовищем, у якому кожна транзакція має власну верифіковану історію, що є прямим наслідком впровадження інформаційних технологій і систем в облік [12].

Перехід від документального підтвердження до протокольної верифікації є одним із найглибших методологічних зрушень, яке трансформує основу облікової достовірності. У традиційному підході первинний документ був матеріальним або електронним носієм доказу господарської події, що потребував підписів, печаток і зовнішнього контролю. У блокчейн-орієнтованій системі сам факт транзакції, підтверджений консенсусом і криптографічним алгоритмом, набуває статусу документа – тобто юридично та методологічно достовірного запису, який не потребує подальшої верифікації. Так, бухгалтерський запис перестає бути похідним від документа – він і є документом у чистому вигляді: незмінним, прозорим і самодостатнім джерелом облікової інформації.

Цей процес формує нову парадигму достовірності в обліковій теорії, де істинність даних забезпечується не соціальним контролем чи адміністративними процедурами, а технологічною надійністю механізмів консенсусу, криптографічним захистом та незмінністю записів.

У результаті формується інституційно-технологічна модель бухгалтерського обліку, у якій поняття «первинного документа» і «облікового запису» зливаються в єдиний інформаційний об'єкт – транзакцію, що є водночас фактом господарського життя, його підтвердженням і доказом достовірності.

У перспективі це відкриває напрям до створення саморегульованих облікових систем, де облік функціонує як автономна частина економічної інфраструктури, а його достовірність забезпечується технологічно, а не процедурно. Так, блокчейн-орієнтована цифровізація бухгалтерського обліку не лише змінює методику ведення облікових процесів, а й трансформує саму епістемологію бухгалтерської науки, переводячи її в площину алгоритмічної раціональності, де дані стають носіями істини незалежно від людського втручання, що дає відповідь на питання, чи чекає бухгалтерів революція обліку під впливом блокчейну [71; 72].

Отже, теоретичні основи цифровізації бухгалтерського обліку на базі блокчейн-технологій формують нову парадигму достовірності, де облік функціонує як саморегульована система, що поєднує елементи технологічного контролю, алгоритмічної логіки та інституційної довіри. Це не лише трансформує класичну облікову методологію, але й закладає підґрунтя для побудови глобальних децентралізованих облікових систем, у яких економічна інформація стає універсальною, синхронізованою та незалежною від людського втручання.

1.4. Методологічні принципи формування нової облікової парадигми на засадах децентралізації та прозорості інформації

Формування нової облікової парадигми на засадах децентралізації та прозорості інформації є результатом глибинної трансформації економічного середовища, у якому цифрові технології поступово набувають статусу системоутворювального чинника соціально-економічного розвитку. Цей процес характеризується не лише технічними інноваціями, а й переосмисленням фундаментальних принципів організації облікової діяльності, де цифрові інструменти є не допоміжними засобами, а повноцінними елементами управлінської інфраструктури.

В умовах переходу до цифрової економіки відбувається злиття облікових, аналітичних та управлінських процесів у єдину інтегровану систему, яка забезпечує оперативний моніторинг, контроль і прогнозування фінансово-господарської діяльності суб'єктів господарювання.

У межах цієї трансформації методологія бухгалтерського обліку перестає бути лише сукупністю процедур фіксації господарських фактів, а набуває рис комплексної інформаційно-аналітичної системи, що функціонує у режимі реального часу та забезпечує безперервність облікових процесів. Вона спрямована не тільки на документування економічних подій, а й на забезпечення довіри між усіма учасниками економічних відносин – від внутрішніх структур підприємства до зовнішніх стейкхолдерів, включно з інвесторами, аудиторами та регуляторами. Така система гарантує достовірність і незмінність даних завдяки технологічним механізмам підтвердження, які замінюють традиційні форми зовнішнього контролю. Внаслідок цього облік еволюціонує від формальної процедури звітності до механізму забезпечення корпоративної прозорості та цифрової довіри.

Децентралізація в цьому контексті постає як нова форма інституційної організації обліку, що базується на відсутності єдиного центру зберігання, перевірки чи підтвердження інформації. Замість цього формується мережеве середовище, де кожен учасник є одночасно користувачем і носієм облікових даних, а прозорість стає наслідком відкритого доступу до транзакцій, підтверджених механізмом консенсусу.

Методологічні принципи нової облікової парадигми, що спирається на децентралізацію та прозорість інформації, потребують ґрунтовного теоретичного й практичного обґрунтування кожної з чотирьох базових засад – децентралізованої довіри, незмінності даних, алгоритмічної верифікації та інтеграції обліку в цифровий управлінський цикл – і розгляду їхніх взаємодій як єдиної системи гарантування достовірності облікової інформації (табл. 1.3).

З позицій бухгалтерської науки це означає зміщення центру уваги від контролю достовірності окремих документів до оцінки надійності системи, у межах якої ці документи створюються, узгоджуються і зберігаються. Принцип децентралізованої довіри передбачає, що підтвердження господарських фактів здійснюється не засобом подальшої аудиторської перевірки, а через механізм спільного узгодження, де всі учасники мережі беруть участь у перевірці правильності записів

відповідно до наперед визначених правил. Так, контроль і підтвердження достовірності стають постійними і невід'ємними складовими самого процесу обліку, що підвищує його надійність і знижує ризик помилок чи фальсифікацій.

Таблиця 1.3 – Характеристика методологічних принципів формування нової облікової парадигми на засадах децентралізації та прозорості інформації

Назва принципу	Характеристика принципу
Принцип децентралізованої довіри	Сутність цього принципу полягає в перенесенні функції довіри від централізованих інституцій (державних чи корпоративних) до розподіленої мережі учасників, що взаємодіють на основі консенсусних алгоритмів. Це забезпечує незалежну автентифікацію облікових даних без потреби в посередниках
Принцип незмінності даних	Усі облікові записи, внесені до розподіленого реєстру, стають незмінними, що вилучає можливість їхньої фальсифікації або несанкціонованого корегування. Така властивість гарантує сталість, відтворюваність та доказовість бухгалтерської інформації в часі
Принцип алгоритмічної верифікації	Перевірка достовірності облікових даних відбувається автоматизовано за допомогою криптографічних і смарт-контрактних механізмів. Це мінімізує людський чинник, підвищує точність облікових процедур і забезпечує об'єктивність контролю
Принцип інтеграції обліку в цифровий управлінський цикл	Бухгалтерський облік трансформується з ретроспективної системи фіксації фактів у динамічний елемент управлінської аналітики, що функціонує в режимі реального часу. Така інтеграція забезпечує безперервний обмін даними між обліковими, аналітичними та управлінськими контурами цифрової організації

Джерело: складено авторами.

Реалізація цього принципу потребує розроблення чітких критеріїв оцінки облікової інфраструктури. Потрібно визначити стандарти для вузлових операцій – тобто дії, які виконують окремі елементи мережі з прийому, перевірки і фіксації транзакцій. Такі стандарти мають встановлювати вимоги до технічної стійкості вузлів, їх здатності до

автономного функціонування, а також до захисту від несанкціонованих втручань. Критично важливим є також запровадження процедур сертифікації постачальників послуг, які забезпечують роботу облікових мереж, що буде охоплювати перевірку їх відповідності встановленим технічним і методичним вимогам, рівню безпеки та відкритості алгоритмів.

Формування системи децентралізованої довіри вимагає також створення формалізованих процедур управління змінами в мережі. Будь-яке оновлення або корегування правил має відбуватися відповідно до чітко визначених процедур, які забезпечують збереження історії змін, відкритість процесів прийняття рішень та узгодженість дій усіх учасників. Це створює умови для стабільності облікової системи і водночас забезпечує її адаптивність до нових вимог середовища, не порушуючи принципу незмінності даних.

Методологічно децентралізована довіра передбачає переосмислення ролей інституцій у системі обліку. Якщо в традиційній моделі аудитор, контролер або регулятор був зовнішнім гарантом достовірності, то в умовах цифрової децентралізації ці функції розподіляються між усіма учасниками мережі через механізми колективного підтвердження. Такий підхід створює умови для появи нових професійних напрямів – розроблення стандартів для протоколів узгодження, сертифікації вузлів, формування механізмів відповідальності за модифікації системи та її технічне супроводження. У підсумку принцип децентралізованої довіри стає не лише технологічною основою нового типу бухгалтерського обліку, а й методологічним орієнтиром для його наукового осмислення, оскільки змінює саму природу довіри – із персональної вона стає системною, із зовнішньої – внутрішньо вбудованою у структуру облікових процесів.

Принцип незмінності даних становить один із наріжних каменів нової методології бухгалтерського обліку в умовах цифрової децентралізації. Його зміст полягає в тому, що будь-яка інформація, один раз зафіксована в розподіленому реєстрі, не може бути змінена або вилучена без збереження історичного сліду цієї дії. Такий підхід докорінно трансформує уявлення про динаміку облікових записів, відмовляючись від традиційної можливості їх ретроспективного редагування. Це зі свого боку усуває потенційну можливість фальсифікації даних і забезпечує максимальну прозорість усіх господарських подій,

що відображаються в системі обліку. У контексті облікової науки це означає переосмислення самої природи облікової інформації – вона набуває рис юридично значущого цифрового свідчення, достовірність якого забезпечується не зовнішнім контролем, а властивостями самої системи.

Методологічно принцип незмінності даних змінює традиційну процедуру виправлення помилок, яка раніше передбачала можливість редагування або вилучення помилкового запису. У децентралізованій системі такі дії замінюються механізмами компенсації, коли замість зміни первинного запису створюється новий – корегувальний. Цей підхід дає змогу зберегти повну історію змін, оскільки кожне уточнення має власне цифрове відображення в реєстрі, із зазначенням підстав, часу та ініціатора корекції. Внаслідок цього формується безперервний і прозорий обліковий ланцюг, який забезпечує логічну послідовність та доказову силу даних, не порушуючи їх історичної цілісності.

У межах такої системи важливо створити чітко регламентовані механізми управління змінами, що реалізуються через процедури узгодження – так званий змінний консенсус. Йдеться про випадки, коли корекція запису є юридично обґрунтованою і потребує підтвердження більшістю учасників мережі або спеціально визначеними органами. Такі процедури мають бути формалізовані та забезпечені прозорими правилами ініціювання, верифікації й документування змін. Так, навіть у разі виправлення даних сама суть принципу незмінності не порушується – адже зміни не затирають минулого, а доповнюють його новим рівнем облікової інформації, забезпечуючи логічну і правову спадкоємність усіх записів.

Особливого значення в цьому контексті набуває методика формалізації облікового сліду, тобто системи метаданих, що супроводжують кожну дію в обліковій системі. Такі метадані фіксують джерело ініціації змін, підстави для їх здійснення, коло осіб, що здійснювали перевірку та підтвердження, а також юридичні обґрунтування прийнятих рішень. Це забезпечує не лише збереження історичної достовірності, але й створює доказову базу, здатну витримати перевірку як у внутрішньому аудиті, так і в зовнішньому контролі або судовому процесі. Відповідно, кожна зміна в системі не просто відображається технічно, а документально закріплюється як подія з власною історією, контекстом і юридичними наслідками.

Так, принцип незмінності даних стає гарантією не лише технічної цілісності облікової інформації, але й її правової захищеності. Він формує новий рівень дисципліни у веденні бухгалтерського обліку, де будь-яка зміна є підзвітною і невід'ємною частиною єдиного цифрового реєстру. Це створює основу для якісно нового типу довіри до облікових даних – довіри, що ґрунтується на відтворюваності, непідробності та відкритості інформації, і водночас забезпечує найвищий рівень відповідності між технологічними можливостями та методологічними принципами сучасної бухгалтерської науки.

Принцип алгоритмічної верифікації становить одну з фундаментальних засад нової методології бухгалтерського обліку, що формується в умовах цифрової децентралізації. Його сутність полягає в переході від традиційних форм контролю, які базуються на людському судженні, професійному досвіді та суб'єктивній інтерпретації фактів господарського життя, до автоматизованих, математично вивірених механізмів перевірки правильності та достовірності облікових записів. У межах цієї концепції облік перетворюється на систему, де перевірка достовірності даних відбувається не постфактум, а безпосередньо під час здійснення операції – через алгоритми, що закладені в програмні протоколи блокчейн-мережі.

У методологічному вимірі алгоритмічна верифікація означає створення формальних специфікацій облікових правил у вигляді структур, які є зрозумілими для технічного опрацювання, здатних до автоматичного виконання. Це передбачає перехід від описових нормативних положень до чітко визначених логічних умов, які однозначно інтерпретуються системою. Такі умови реалізуються у вигляді смартконтрактів – програмних модулів, що автоматично контролюють дотримання умов господарських угод, здійснюючи запис операцій лише після виконання всіх визначених критеріїв. Так, процес перевірки стає частиною самої транзакції, а не окремим етапом облікового циклу, що мінімізує ризики людської помилки і забезпечує повну узгодженість між фактом події та її обліковим відображенням, що реалізує теоретико-прикладні засади використання блокчейн-технології в бухгалтерському обліку [19].

Важливою складовою реалізації цього принципу є формалізація схем токенізації, метаданих і структур записів. Кожен обліковий об'єкт у децентралізованій системі має бути описаний у формі цифрового

представлення, що містить усю необхідну інформацію для автоматичної перевірки його достовірності, походження та правомірності. Це потребує розробки методичних стандартів щодо створення токенів, структури метаданих і процедур їх верифікації. У цьому контексті алгоритмічна верифікація не лише забезпечує технічну надійність даних, але й формує основу для уніфікації цифрових форматів бухгалтерської інформації на міжорганізаційному рівні.

Не менш важливою методологічною вимогою є перевірка правильності алгоритмів, що реалізують облікову логіку. Для цього потрібно впроваджувати формальні методи контролю – такі як математичне верифікування коду, модульне тестування, моделювання сценаріїв і симуляційні перевірки. Кожен алгоритм, який використовується для фіксації чи перевірки облікових даних, має проходити процедуру сертифікації, що охоплює незалежний аудит коду, перевірку його стійкості до збоїв, коректності логічних зв'язків і відповідності встановленим стандартам. Для забезпечення системності цих процесів потрібно створювати централізовані репозитарії перевірених шаблонів облікової логіки, доступних для спільного використання в межах економічних мереж.

Водночас алгоритмічна верифікація не може бути абсолютно статичною – вона має зберігати здатність до адаптації у відповідь на зміни економічних умов, нормативного середовища та управлінських потреб. Тому в межах методології цього принципу особливого значення набувають механізми управління оновленнями алгоритмів – процеси версіювання, погодження змін і формалізоване управління розвитком системи. Такі механізми забезпечують баланс між незмінністю історичних даних, які залишаються недоторканними, і гнучкістю облікової логіки, яка може змінюватися відповідно до нових реалій без втрати цілісності облікової системи.

Загалом принцип алгоритмічної верифікації в бухгалтерському обліку формує новий рівень наукової раціональності, коли достовірність інформації гарантується не суб'єктивними судженнями, а об'єктивними алгоритмічними процедурами. Це відкриває перспективу переходу від періодичного контролю до безперервної автоматичної перевірки, від людського нагляду – до системної самоперевірки, а від довіри до фахівця – до довіри до технології, що працює за чітко визначеними, перевіреними й документованими правилами. У результаті

бухгалтерський облік набуває властивостей науково формалізованої системи, де контроль і верифікація інтегровані в саму структуру даних, утворюючи нову форму технологічної достовірності, яка поєднує точність, надійність і прозорість у єдиному цифровому середовищі.

Інтеграція обліку в цифровий управлінський цикл підводить облік із рівня ретроспективної реєстрації до ролі оперативного джерела управлінських рішень, постачаючи показники на основі постійно оновлюваного потоку верифікованих транзакцій. Методологічно це означає поєднання традиційних облікових стандартів із подієво-орієнтованою архітектурою, підходами обробки потоків і сучасними методами аналітики, зокрема методами автоматичного навчання. Верифікований потік транзакцій має стати першопричиною формування управлінської інформації: кожна подія в реєстрі містить необхідні для агрегування метадані, відомості про походження та криптографічні докази цілісності, що дає змогу перетворювати транзакційні дані в оперативні показники без проміжних ручних перетворень.

Ключовим методичним елементом є визначення правил агрегування і часових інтервалів, які забезпечують коректність перетворення потоку транзакцій в узагальнені показники. Це вимагає формалізації правил: визначення типів подій, рівнів деталізації, методів обчислення агрегатів (сума, середнє, кумулятивні значення), а також вибору інтервалів узагальнення (фіксовані інтервали, ковзні вікна, тригерні агрегації). Методика має містити правила синхронізації даних із різних реєстрів, алгоритми погодження часового маркування та процедури узгодження часткових транзакцій під час відкладеної остаточності записів, щоб уникнути помилкових управлінських сигналів через латентність або різний ступінь остаточності даних.

Збереження гарантій достовірності за трансформації потокових даних досягається через вимоги до доказової бази джерел: кожна агрегована величина повинна мати вбудовані посилання на криптографічні докази походження і на метадані, що фіксують ланцюг подій. Методика повинна визначати формат таких посилань, процедуру збереження і відтворення, а також критерії прийнятності джерел (сертифіковані канали надходження, багатоканальна перевірка, маркування якості даних). Для забезпечення відтворюваності й перевірки розрахунків потрібно передбачити механізми версіонування правил агрегування та зберігання конфігурацій аналітичних процесів.

Особлива методична увага приділяється межам автономії автоматизованих рішень. Потрібно визначити категорії рішень, які можуть виконуватися повністю автоматично (наприклад, розрахунок рутинних нарахувань, блокування платежів за чітко визначених умов), та ті, що вимагають попередньої або постфактумної участі людини (складні оцінки, правові спори, нетипові події). Для цього вводяться порогові значення ризику і критерії аномалій, за досягнення яких система автоматично ініціює ескалацію до людини – надання контекстної інформації, опису сценарію та рекомендованих дій. Методика має також охоплюаати вимоги до пояснюваності автоматичних рішень та збереження логів, що дають змогу відтворити ланцюг прийняття рішення.

Практична реалізація інтеграції обліку в управлінський цикл потребує окремих процедур для забезпечення сумісності з існуючими системами: правила погодження даних у міжсистемній інтеграції, процедури періодичної звірки, механізми компенсації розбіжностей та алгоритми злиття агрегатів. Пртрібно також установити вимоги до показників якості облікових сигналів (точність, повнота, своєчасність, надійність) і вбудувати процедури контролю цих показників у щоденний операційний цикл. Важливим елементом є визначення сервісних рівнів і планів відновлення після інцидентів, що гарантуватиме стабільність управлінської інформації в критичних ситуаціях.

Нарешті, методологія інтеграції має охоплювати правові та етичні аспекти: правила збереження конфіденційності, обмеження доступу до чутливих полів за агрегації, дотримання вимог щодо зберігання первинних доказів і відповідність нормативним вимогам щодо звітності. Поєднання технічних правил, формалізованих процедур агрегування, критеріїв контролю якості та механізмів ескалації забезпечить, з одного боку, оперативність і аналітичну корисність облікових даних, а з іншого – збереження принципів достовірності, підзвітності та правової захищеності інформації в умовах цифрової децентралізації.

Інституційні та процедурні наслідки реалізації принципів нової облікової парадигми зумовлюють необхідність створення цілісної нормативно-методичної системи, яка забезпечуватиме узгодженість облікових процесів у цифровому середовищі. Центральне місце в цій системі посідає стандартизація метаданих, токенізації облікових одиниць та форматів сліду аудиту, що мають забезпечити взаємну сумісність

облікових даних між різними технологічними платформами, інформаційними системами та правовими юрисдикціями. Формування таких стандартів повинно спиратися на принципи прозорості, універсальності та розширюваності, оскільки від них залежить можливість інтеграції облікової інформації у глобальні цифрові ланцюги створення вартості. Важливо не лише визначити єдину структуру метаданих, а й запровадити уніфіковані правила опису джерел даних, посилань на первинні документи, методів токенізації та маркування операцій, що надає змогу відстежувати походження кожної облікової події та забезпечує достовірність її відтворення.

Методологічна побудова децентралізованого облікового середовища вимагає також багаторівневої моделі контролю, у якій поєднуються автоматизовані алгоритмічні перевірки, незалежна верифікація даних і правові гарантії. На першому рівні контроль здійснюється безпосередньо технологічними засобами – механізмами консенсусу, алгоритмами перевірки цілісності блоків, системами автоматичного співставлення показників. На другому рівні передбачається незалежна перевірка достовірності джерел інформації – через сертифікованих посередників, механізми багатоканальної верифікації або процедури взаємного підтвердження між незалежними вузлами. Третій рівень становлять правові й організаційні інструменти – системи арбітражу, механізми страхування технічних та операційних ризиків, а також регламентовані процедури компенсації збитків у разі збоїв. Така структурована модель контролю забезпечує стійкість облікової системи навіть у ситуаціях часткової відмови вузлів, спотворення даних або некоректної поведінки окремих учасників мережі.

Важливою складовою методології є розробка системи управління ризиками, що притаманні цифровим і децентралізованим середовищам. Йдеться насамперед про три ключові групи ризиків: кіберризики, пов’язані з можливістю зовнішніх втручань або вразливостей програмного коду; ризики консенсусу, що виникають унаслідок можливих збоїв у механізмах узгодження записів між вузлами; та ризики помилкового моделювання облікових правил, які можуть призвести до систематичних викривлень даних.

Для мінімізації цих загроз методологічна база повинна передбачати диверсифікацію джерел інформації, регулярне оновлення алгоритмів перевірки, страхування відповідальності ключових учасників,

а також створення аварійних планів відновлення даних і функцій системи у випадку надзвичайних подій. Збалансоване поєднання цих заходів дозволить зберегти цілісність облікових процесів і забезпечити їх безперервність навіть за умов зовнішніх або внутрішніх криз.

Окрему увагу потрібно приділити підготовці професійних кадрів, здатних працювати в умовах цифрової децентралізації. Професійна спільнота бухгалтерів, аудиторів та аналітиків потребує нової системи компетенцій, яка поєднує глибокі знання облікової теорії з технічними навичками роботи в розподілених інформаційних середовищах. Методологічні засади повинні передбачати формування нових професійних ролей, таких як розробник облікових протоколів, аудитор смартконтрактів, аналітик токенізованих активів, менеджер управління протоколами та корпоративного консенсусу. Для кожної з цих ролей мають бути визначені компетенційні профілі, програми підготовки й підвищення кваліфікації, а також етичні кодекси, що регламентують поведінку фахівців у середовищі, де довіра ґрунтується на технічних механізмах, а не на централізованому контролі.

Комплексна реалізація вказаних методологічних принципів – від стандартизації даних і процедур контролю до формування нової професійної культури – створює цілісний фундамент для практичного втілення децентралізованої облікової системи. Саме поєднання технологічних, організаційних і правових інструментів забезпечує перехід від теоретичних моделей до дієвої практики, де принципи децентралізованої довіри, незмінності даних, алгоритмічної верифікації та інтегрованості обліку в управлінський цикл реалізуються як взаємопов’язані складові сучасного облікового процесу. Такий підхід формує основу нового типу бухгалтерського обліку – прозорого, безперервного та самоорганізованого, здатного забезпечити достовірність інформації у цифровій економіці децентралізованих взаємодій.

Отже, методологічні принципи формування нової облікової парадигми базуються на переході від централізованої, документально орієнтованої системи до децентралізованої, протокольно перевіреної інформаційної структури. Це перетворює бухгалтерський облік із засобу відображення минулих подій на інтегрований елемент цифрової економіки, який забезпечує реальний, прозорий і безперервний облік економічної діяльності. У результаті бухгалтерська методологія входить у нову фазу розвитку, де технологія стає носієм методологічної істини, а децентралізація і прозорість – фундаментальними принципами облікової достовірності.

Висновки до розділу 1

Еволюція наукових підходів до розуміння сутності бухгалтерського обліку в цифровій економіці засвідчує глибинну трансформацію його теоретико-методологічних засад – від класичної централізованої парадигми контролю та документального підтвердження господарських операцій до сучасної децентралізованої моделі цифрового обліку, інтегрованої в глобальні інформаційні мережі. Якщо на початкових етапах розвитку бухгалтерський облік виконував переважно ретроспективну функцію формування достовірної звітності, то подальша еволюція наукової думки спрямувала його в бік системності, аналітичності й управлінської релевантності. У контексті цифрової економіки облік перетворюється на динамічну, інтегровану інформаційну систему, що функціонує в режимі реального часу, забезпечуючи прозорість, автоматичну верифікацію та незмінність даних. Впровадження блокчейн-технологій формує якісно нову наукову концепцію бухгалтерського обліку, в основі якої лежить децентралізована довіра, алгоритмізація контролю та синергетична взаємодія між усіма учасниками економічного процесу без потреби в централізованому посереднику. Так, сучасний бухгалтерський облік еволюціонує від інструменту обліково-контрольного характеру до інтелектуальної, самоверифікованої підсистеми цифрової економіки, що поєднує принципи достовірності, оперативності та прозорості в єдину методологічну конструкцію нового типу.

Цифрова децентралізація є не лише технологічним трендом, а фундаментальною інституційною трансформацією, що вимагає переосмислення економічної природи довіри, механізмів контролю та організації облікових процесів у цифровій економіці. Її вплив проявляється в переході від централізованих систем обробки даних до розподілених мереж, де достовірність і цілісність інформації забезпечуються алгоритмічними, а не інституційними гарантіями. У межах цієї парадигми бухгалтерський облік еволюціонує від ролі адміністративного реєстратора до функції інтегратора цифрової інфраструктури, відповідального за проєктування, валідацію та інтерпретацію даних, що циркулюють у блокчейн-екосистемах. Такий підхід формує передумови для становлення нового типу облікової архітектури – відкритої, прозорої та самоверифікованої, у якій контроль і звітність здійснюються в

режимі реального часу, а аудиторська перевірка набуває алгоритмічного характеру. Водночас цифрова децентралізація актуалізує потребу в синтезі бухгалтерської, правової та технологічної методологій, що дає змогу забезпечити збалансованість між технічною достовірністю даних, нормативною відповідальністю та етичними засадами професії. Так, цифрова децентралізація стає методологічним ядром нової парадигми бухгалтерського обліку, де довіра, прозорість і контроль реалізуються через технологічно опосередковані, але економічно обґрунтовані механізми взаємодії між суб'єктами цифрової економіки.

Цифровізація бухгалтерського обліку на основі блокчейн-технологій репрезентує перехід від централізованої моделі фіксації господарських фактів до децентралізованої системи алгоритмічно підтверджуваної достовірності, у якій істинність даних забезпечується технологічними механізмами консенсусу та криптографічного захисту, а не соціально-інституційними гарантіями. У межах цієї парадигми бухгалтерський облік трансформується з інструменту ретроспективного контролю в саморегульовану цифрову інфраструктуру, що функціонує в режимі реального часу, забезпечуючи прозорість, незмінність та автоматичну верифікацію облікових записів. Блокчейн є не лише технологічною основою, а й методологічним детермінантом нової епістемології обліку, де кожна транзакція є одночасно фактом, доказом і документом господарської діяльності. Така архітектура зумовлює появу якісно нової системи довіри – алгоритмічної, у межах якої облікові дані стають самопідтверджуваними та автономними від людського втручання. Теоретично це означає формування нового типу облікової реальності – децентралізованої, інтерактивної та технологічно самоверифікованої, у якій бухгалтерський облік еволюціонує як компонент глобальної цифрової інфраструктури, що забезпечує не лише достовірність, а й безперервність, прозорість і синхронність економічної інформації.

Методологічні принципи формування нової облікової парадигми на засадах децентралізації та прозорості інформації відображають глибинну трансформацію сутності бухгалтерського обліку – від централізованої системи ретроспективного контролю до децентралізованої, алгоритмізованої та самоверифікованої інформаційної інфраструктури, у якій достовірність і довіра забезпечуються не інституційними, а технологічними механізмами. Реалізація принципів децентралізованої

довіри, незмінності даних, алгоритмічної верифікації та інтеграції обліку в цифровий управлінський цикл створює методологічну основу нового типу бухгалтерського мислення, що ґрунтується на відкритості, доказовості та відтворюваності облікових фактів у режимі реального часу. Така парадигма формує цілісну систему гарантування достовірності економічної інформації, де контроль і звітність є не зовнішніми етапами, а внутрішньо вбудованими властивостями облікових процесів. Унаслідок цього бухгалтерський облік перетворюється на інтелектуальну складову цифрової економіки, здатну забезпечувати прозорість, підзвітність і стійкість фінансової інформації в умовах децентралізованих технологічних екосистем.

РОЗДІЛ 2
КОНЦЕПТУАЛЬНІ ЗАСАДИ ІНТЕГРАЦІЇ ТЕХНОЛОГІЇ БЛОКЧЕЙН У БУХГАЛТЕРСЬКИЙ ОБЛІК

«Цифрова епоха не змінює істину –
вона змінює спосіб її відображення»
Ювал Ной Харарі

2.1. Архітектура децентралізованого облікового середовища: суб'єкти, об'єкти, інформаційні потоки

Архітектура децентралізованого облікового середовища в контексті цифрової економіки постає як складна багаторівнева система, що поєднує технологічні, організаційні та методологічні компоненти, спрямовані на забезпечення достовірності, безперервності та прозорості бухгалтерської інформації. В основі такої архітектури лежить розподілений реєстр, який є інфраструктурною основою для реєстрації, збереження та перевірки облікових операцій без необхідності централізованого контролю з боку традиційних інституцій [32]. Цифрова децентралізація обліку трансформує уявлення про роль бухгалтера, підприємства та користувача інформації, формуючи нову парадигму взаємодії між суб'єктами господарювання та середовищем облікових даних [46].

Суб'єктний вимір децентралізованого облікового середовища суттєво трансформує традиційну інституційну картину бухгалтерського процесу: замість чітко вираженої ієрархії з централізованим оператором реєстру виникає мережа автономних і напівавтономних агентів, кожен із яких одночасно виконує ролі генератора, власника та верифікатора інформації. У такому середовищі економічний агент перестає бути пасивним постачальником даних і набуває статусу активного вузла бухгалтерської екосистеми – він ініціює транзакції, підписує їх цифровими ключами, зберігає локальні копії реєстру та бере участь у механізмах підтвердження. Така поліцентрична модель змінює нормативні уявлення про відповідальність: відповідальність за автентичність записів розподіляється між усіма учасниками мережі і технічно підкріплюється криптографічними доказами походження і цілісності даних.

Роль учасників можна розглядати як багаторівневу: на операційному рівні це господарюючі суб'єкти, які формують первинні цифрові сліди господарських фактів; на рівні забезпечення достовірності – верифікатори та валідатори, які виконують функції перевірки й долучення транзакцій до блоків; на рівні контролю та нагляду – аудитори, регулятори та кредитори, які отримують доступ до агрегованих або селективно розкритих даних для здійснення незалежного оцінювання. Такий розподіл ролей вимагає чіткого визначення прав доступу, процедур цифрової ідентифікації та механізмів делегування повноважень, що реалізуються через криптографічні протоколи і смартконтракти як носії ролей і політик.

Відсутність централізованого адміністратора створює закономірну потребу в формалізації правил участі та механізмів управління змінами. У практиці блокчейн-мереж це вирішується через моделі децентралізованого управління, які визначають процедури оновлення протоколу, політики доступу та санкційні механізми [66]. Для бухгалтерського середовища такі моделі мають долучати норми щодо оприлюднення облікових політик, процедур корегування помилок, обмежень на редагування метаданих і умов виходу / входу учасників, забезпечуючи поєднання технічної стійкості та юридичної відповідальності.

Алгоритмами консенсусу реалізуються функції контролю, підтвердження та збереження даних, тому їхній вибір має безпосередній вплив на облікові характеристики мережі. Консенсуси на основі витрат обчислювальної потужності забезпечують високий рівень стійкості до цензури і переписування історії, але створюють затримки й істотні витрати; алгоритми, що покладаються на узгодження учасників, зменшують енергетичні витрати й забезпечують швидшу фіналізацію, проте накладають ризики концентрації впливу та необхідність додаткових механізмів економічних стимулів та протидії зловживанням [58]. Для бухгалтерського застосування критично важливі такі характеристики консенсусу, як швидкість підтвердження транзакцій, рівень гарантії фіналізації, можливість відтворення історії та стійкість до маніпуляцій.

Економічні стимули та економіка токенів, інтегровані в механізми консенсусу, створюють додатковий шар відповідальності й мотивації для суб'єктів обліку. Учасники, які діють як валідатори, зацікавлені в дотриманні правил мережі та коректності облікових записів, оскільки

їхні винагороди або ризики санкцій прямо залежать від довіри та технічної репутації. Це породжує нові форми корпоративної поведінки і може сприяти підвищенню якості первинної інформації, якщо модель стимулів синхронізована з принципами достовірності та повноти облікових даних. Водночас токен-економіка вимагає ретельного проєктування, аби уникнути конфлікту інтересів між комерційними вигодами та роллю незалежного контролера.

Криптографічні механізми управління ідентичністю й доступом стають фундаментом відповідальності в децентралізованому середовищі. Надійне зберігання приватних ключів, протоколи відновлення доступу, використання мультипідписних схем і розподілених систем збереження паролей визначають, хто й коли може ініціювати облікові записи або змінювати стан активів. Для бухгалтерії це означає, що традиційні принципи розподілу обов'язків і внутрішнього контролю мають трансформуватися в криптографічно захищені процедури, які фіксують делегування прав, слідування політикам і надають доказову базу у випадку спорів.

Взаємодія між ончейн- та офчейн-складовими набуває ключового значення для забезпечення повноти обліку. Не всі первинні документи чи дані про події є сенс зберігати повністю в розподіленому реєстрі; часто застосовується модель гібридного зберігання, коли в реєстр заносяться хеш-відбитки, метадані й посилання на зовнішні сховища, забезпечуючи невід'ємність і трасованість, але зберігаючи приватність та ефективність [78]. У цьому контексті суб'єкти повинні погоджувати формати доказів, стандарти метаданих і процедури взаємної верифікації між ончейн- і офчейн-джерелами, щоб гарантувати, що облікові регістри мають повну доказову силу для аудиту та регуляторного нагляду.

Аудитори та контролювальні органи в децентралізованому середовищі отримують нові інструменти й одночасно нові завдання: з одного боку, наявність розподіленого, криптографічно захищеного журналу робить можливим реалізацію безперервного аудиту з високим ступенем автоматизації; з іншого – аудитори повинні володіти компетенціями у сфері криптографії, протоколів консенсусу та специфіки смартконтрактів для оцінювання достовірності й трактування on-chain даних. Навіть за умов широкої прозорості залишаються питання інтерпретації економічних сутностей, оцінювання контрагентного ризику та

застосування облікових політик, що вимагає поєднання технічної перевірки доказів із професійним судженням.

Нарешті, суб'єктний аспект децентралізованого обліку містить у собі юридично-регуляторну складову: юрисдикційна визначеність прав на цифрові активи, вимоги щодо збереження первинних документів, правила ідентифікації клієнтів та AML-нормативи, процедури надання доступу регуляторам повинні бути інтегровані в технічну архітектуру мережі. Така інтеграція правових механізмів у технічну інфраструктуру децентралізованого обліку покликана забезпечити баланс між прозорістю даних і захистом приватності користувачів. Для цього потрібно впровадити багаторівневі системи автентифікації, управління доступом і криптографічного захисту, що дадуть змогу узгодити технологічну автономність із вимогами фінансового моніторингу, аудиту та податкового контролю. Це зумовлює потребу в створенні механізмів прозорої співпраці між мережевими стейкхолдерами та державними інституціями, які зможуть визнавати ончейн-докази як юридично значущі, не втрачаючи водночас принципів приватності та децентралізації.

Узагальнюючи викладений вище матеріал, структуруємо його у вигляді характеристики суб'єктного компонента децентралізованого бухгалтерського середовища (табл. 2.1).

Таблиця 2.1 – Характеристика суб'єктного компонента децентралізованого бухгалтерського середовища

Назва елементу	Змістовна характеристика	Ключові наслідки для бухгалтерського обліку
1	2	3
Трансформація інституційної структури	Замість централізованого реєстратора формується мережа автономних агентів, які є одночасно генераторами, власниками й верифікаторами даних	Перехід від ієрархічної до поліцентричної моделі обліку; суб'єкт є активним вузлом екосистеми, ініціює та підтверджує транзакції
Розподіл відповідальності	Відповідальність за автентичність та цілісність записів децентралізується, підтверджується криптографічними доказами	Формується колективна відповідальність мережевих учасників; відмова від концепції єдиного адміністратора даних

Продовження таблиці 2.1

1	2	3
Рівнева структура ролей	Операційний рівень – господарюючі суб'єкти генерують первинні цифрові сліди. Рівень достовірності – верифікатори й валідатори перевіряють транзакції. Рівень контролю – аудитори, регулятори, кредитори аналізують агреговані дані	Формалізація прав доступу, цифрової ідентифікації, делегування повноважень через смартконтракти
Механізми управління без адміністратора	У децентралізованих мережах правила участі та зміни протоколів визначаються спільнотою через моделі децентралізованої автономної організації	Необхідність регламентації облікових політик, процедур корегування, правил редагування метаданих, умов входу / виходу учасників
Алгоритми консенсусу	Реалізують функції контролю, підтвердження й збереження даних. Види: 1) Proof of Work (висока безпека, низька швидкість); 2) Proof of Stake / Byzantine Fault Tolerance (швидше узгодження, менші витрати, але ризик концентрації впливу)	Вибір алгоритму визначає облікові характеристики: швидкість підтвердження, фіналізацію транзакцій, відтворюваність історії, стійкість до маніпуляцій
Економічні стимули та токен-економіка	Валідатори отримують винагороди або санкції залежно від дотримання правил мережі	Формується новий рівень мотивації і відповідальності; стимулюється достовірність первинних даних; можливий конфлікт інтересів між прибутковістю та об'єктивністю
Управління ідентичністю та доступом	Криптографічні ключі, мультипідпис, протоколи відновлення доступу та розподілене збереження паролів	Трансформація принципів внутрішнього контролю: делегування прав і процедур фіксується у криптографічній формі, створюючи доказову базу

Продовження таблиці 2.1

1	2	3
Ончейн- та офчейн-взаємодія	Частина даних зберігається в блокчейні (хеші, метадані), а решта – у зовнішніх сховищах	Гарантується трасованість та цілісність без надмірного навантаження мережі; потреба у стандартизації форматів доказів і процедур взаємної верифікації
Роль аудиторів та контролерів	Безперервний аудит на основі розподіленого журналу; необхідність нових компетенцій у сфері криптографії й консенсусів	Можливість автоматизованого контролю; зростає значення професійного судження при інтерпретації ончейн-даних
Юридично-регуляторна інтеграція	Потреба в узгодженні цифрових активів із правовими нормами: збереження документів, протидія відмиванню грошей, доступ регуляторів, юрисдикційна визначеність	Формування правових механізмів визнання ончейн-доказів як юридично значущих; баланс між приватністю та відповідальністю
Системна узагальнювальна характеристика	Децентралізоване облікове середовище – це сукупність ролей, повноважень, стимулів і технічних протоколів, що забезпечують довіру без централізованого контролера	Потреба в проєктуванні архітектур, що поєднують криптографічну безпеку, формалізоване управління правами, адаптивні механізми консенсусу й юридичну придатність облікових записів

Джерело: складено авторами.

Так, суб'єктна структура децентралізованого облікового середовища є не просто набором учасників; це цілісна система ролей, повноважень, стимулів і відповідальності, що реалізуються через технічні протоколи та економічні механізми. Для практичної імплементації концепції бухгалтерського обліку в умовах цифрової децентралізації потрібно проєктувати архітектури, які поєднують криптографічну безпеку, формалізоване управління правами та адаптовані механізми консенсусу, що разом забезпечать коректність, відтворюваність і юридичну придатність облікових записів у розподіленому реєстрі.

Об'єктний аспект децентралізованого бухгалтерського обліку формує нову парадигму осмислення економічних фактів діяльності, які переходять із площини документально-фіксованих подій у сферу

цифрових репрезентацій, підтверджених технологічно, а не адміністративно. У контексті блокчейн-технологій об'єкти обліку набувають вигляду токенізованих активів, смартконтрактів та транзакційних записів, що відображають господарські процеси у формі невід'ємних цифрових сутностей. Кожна така сутність є не просто носієм інформації про факт господарського життя, а елементом цифрової структури, який існує в розподіленому реєстрі та забезпечує безперервність облікового ланцюга. Саме тому блокчейн є не лише технічною платформою збереження, а середовищем формування об'єктів обліку, де економічна подія і її облікове відображення зливаються в єдину транзакційну сутність.

Токенізація активів, як базовий механізм репрезентації об'єктів у блокчейн-середовищі, означає перетворення матеріальних або нематеріальних ресурсів у цифрові токени, що мають однозначне відображення в реєстрі та підтверджуються криптографічним підписом їхнього власника. Токен може уособлювати власність на актив, право користування, зобов'язання, частку в капіталі чи навіть конкретну облікову позицію (наприклад, дебіторську заборгованість або запас). Завдяки цьому формується концепція «цифрового двійника» об'єкта обліку, коли його цифрова форма не є просто копією або записом у базі даних, а функціонує як юридично значущий артефакт господарської реальності. Така природа токенізованих об'єктів створює передумови для синхронізації бухгалтерських даних із процесами управління активами, ризиками та фінансовими потоками, оскільки кожна зміна стану токена автоматично фіксується в розподіленому реєстрі, формуючи хронологічно впорядковану історію подій.

Смартконтракти в цій системі виконують роль динамічних об'єктів обліку, що одночасно поєднують інформаційну та функціональну компоненти. Вони не лише фіксують факт господарської операції, а й забезпечують її автоматичне виконання за визначених умов, що програмно кодуються в їхній структурі. Наприклад, смартконтракт може ініціювати обліковий запис лише після підтвердження поставки товару або отримання оплати, забезпечуючи таким способом самоверифікацію факту здійснення операції. Це переводить об'єкт обліку в нову категорію – «самообліковний» об'єкт, здатний автоматично генерувати обліковий запис у момент виникнення економічної події без участі бухгалтера як посередника. Звідси виникає нова методологічна риса

децентралізованого обліку – об'єкти не лише відображають економічну діяльність, а й беруть участь у її регулюванні.

Транзакційні записи, що утворюють основу блокчейн-реєстру, є найменшими структурними одиницями об'єктного рівня обліку. Кожна транзакція містить унікальний криптографічний хеш, який визначає її автентичність і позицію у хронологічному ланцюгу блоків. Цей хеш є результатом криптографічного алгоритму, що унеможливлює зміну або видалення даних без порушення цілісності всієї системи. Так, об'єкт бухгалтерського обліку в децентралізованій системі не може бути корегований або знищений традиційними методами, а лише може бути компенсований новим записом, що відображає виправну дію. Така незворотність формує принцип «облікової інваріантності», коли кожна зміна стану активу є публічною, верифікованою і невід'ємною частиною загальної історії господарської діяльності.

Криптографічна ідентифікація кожного об'єкта створює новий рівень достовірності облікової інформації. Ідентифікаційний код (хеш) є не лише технічним засобом верифікації, а й економіко-правовим маркером власності, що підтверджує приналежність активу певному суб'єкту. Це відкриває можливості для побудови системи обліку, де автентичність даних не потребує зовнішньої перевірки, адже вона забезпечується самим алгоритмом функціонування блокчейну. Такий підхід радикально змінює зміст принципу доказовості в бухгалтерському обліку: первинний документ у його традиційному вигляді трансформується в цифровий запис, чия достовірність підтверджується математичними методами, а не інституційною довірою.

Об'єкти децентралізованого обліку стають ядром інтегрованої інформаційної інфраструктури підприємства. Завдяки стандартизованим інтерфейсам та API-з'єднанням вони можуть бути автоматично синхронізовані з управлінськими, фінансовими, аналітичними та логістичними системами. У результаті створюється єдиний інформаційний простір, у якому бухгалтерський облік перестає бути автономною функцією і стає частиною наскрізного цифрового процесу управління підприємством. Це сприяє переходу від ретроспективного відображення фактів діяльності до режиму реального часу, де всі зміни в активах, зобов'язаннях чи власному капіталі фіксуються негайно, а інформація оновлюється синхронно у всіх вузлах системи.

Юридична природа об'єктів децентралізованого обліку проявляється в їхній функції як елементів цифрової доказової бази господарської діяльності. Кожна транзакція у блокчейні містить криптографічно підтверджену інформацію про ініціатора, зміст операції та час її здійснення, що забезпечує непідробність і юридичну валідність даних. Відповідно, такі записи можуть бути доказами в процесах аудиту, контролю, розслідувань чи судового розгляду. Так, блокчейн-об'єкт поєднує інформаційно-економічний і правовий статус, виконуючи одночасно функції елемента облікового процесу та юридичного артефакту, що засвідчує достовірність господарських подій.

Узагальнюючи викладений вище матеріал, структуруємо його у вигляді характеристики об'єктного компоненту децентралізованого бухгалтерського середовища (табл. 2.2).

Таблиця 2.2 – Характеристика об'єктного компонента децентралізованого бухгалтерського середовища

Назва елементу	Змістовна характеристика	Ключові наслідки для бухгалтерського обліку
1	2	3
Нова парадигма об'єкта обліку	Економічні факти діяльності переходять із площини документально фіксованих подій у цифрові репрезентації, підтверджені технологічно, а не адміністративно	Об'єкт обліку стає частиною цифрової структури блокчейну; бухгалтерський запис та економічна подія зливаються в єдину транзакційну сутність
Токенізація активів	Матеріальні й нематеріальні ресурси перетворюються в токени з унікальним криптографічним підписом, що засвідчує їхню власність і права користування	Формується «цифровий двійник» об'єкта обліку – юридично значущий артефакт господарської реальності; забезпечується автоматична фіксація змін стану активів
Смартконтракти як динамічні об'єкти обліку	Смартконтракт поєднує інформаційну та функціональну складові: не лише фіксує подію, а й забезпечує її виконання через алгоритм	Виникає категорія «самообліковного» об'єкта, який самостійно генерує бухгалтерський запис; автоматизація первинного обліку без участі бухгалтера

Продовження таблиці 2.2

1	2	3
Транзакційний запис як мінімальна одиниця обліку	Кожна транзакція має унікальний хеш, що забезпечує автентичність, незмінність і позицію в ланцюзі блоків	Встановлюється принцип облікової інваріантності: зміни стану активу є незворотними; корегування можливе лише засобом нової транзакції
Криптографічна ідентифікація об'єктів	Хеш-ідентифікатор є доказом власності та засобом підтвердження автентичності даних	Змінюється природа принципу доказовості: достовірність підтверджується математично, без адміністративного затвердження
Інтеграція об'єктів у цифрову інфраструктуру підприємства	Об'єкти обліку синхронізуються з управлінськими, фінансовими та аналітичними системами через API та стандартизовані інтерфейси	Облік перетворюється на елемент наскрізного цифрового управління; переходить у режим реального часу з миттєвим оновленням інформації
Юридичний статус об'єктів	Кожна транзакція містить криптографічно підтверджені дані про ініціатора, зміст і час операції; є юридичним доказом господарських фактів	Об'єкт обліку набуває правового статусу доказу в аудиті, контролі чи судовому процесі; зростає доказова сила ончейн-даних
Інтегральна характеристика децентралізованих об'єктів обліку	Об'єкти є інтегрованими конструкціями, що поєднують економічну сутність, юридичну силу та алгоритмічну автономність	Формується новий тип облікової реальності – децентралізоване цифрове середовище, у якому довіра ґрунтується на математично підтвердженій достовірності даних

Джерело: складено авторами.

Отже, об'єкти децентралізованого бухгалтерського обліку не зводяться лише до цифрових копій традиційних облікових одиниць. Вони являють собою інтегровані інформаційно-технологічні конструкції, у яких поєднуються економічна сутність, юридична сила та алгоритмічна автономність. Їхня незмінність, трасованість та самоверифікаційна природа формують основу нового типу облікової реальності – децентралізованого цифрового середовища, у якому довіра ґрунтується не на суб'єктивних оцінках, а на математично підтвердженій достовірності кожного об'єкта обліку.

Інформаційні потоки в децентралізованому обліковому середовищі становлять одну з ключових архітектонічних основ цифрової бухгалтерської системи нового покоління, у якій інформація набуває властивостей автономності, самовідтворюваності та стійкості до спотворення. На відміну від традиційних централізованих облікових систем, де рух даних відбувається за ієрархічною схемою – від джерела первинного документа до центрального облікового реєстру через проміжні етапи обробки та верифікації, – у децентралізованій системі інформаційні потоки циркулюють у горизонтально структурованій мережі вузлів, що взаємодіють між собою на засадах рівноправності. Кожен вузол, який бере участь у системі, отримує, перевіряє, фіксує і зберігає дані одночасно з іншими, що унеможливлює появу «центру контролю» або єдиного джерела істини. Такий принцип архітектурного розподілу створює передумови для формування нової парадигми облікової інформаційної рівноваги – коли всі користувачі системи мають доступ до єдиного, синхронізованого й підтвердженого набору даних.

Динаміка інформаційних потоків у блокчейн-орієнтованій системі визначається принципом розподіленого реєстру, де кожна транзакція є водночас інформаційною одиницею, об'єктом контролю та елементом формування облікових даних. Процес руху інформації розпочинається з ініціації транзакції економічним агентом – це може бути операція купівлі-продажу, зміна стану активу, формування зобов'язання або виконання умови смартконтракту. Така транзакція кодується в цифровій формі, підписується приватним криптографічним ключем суб'єкта та передається в мережу для перевірки. Інші вузли системи здійснюють верифікацію транзакції за визначеним алгоритмом консенсусу, що гарантує її достовірність, відсутність дублювання або конфлікту з попередніми записами. Лише після підтвердження більшістю учасників транзакція долучається до нового блоку, який приєднується до ланцюга реєстру, утворюючи безперервну, хронологічно впорядковану структуру даних.

Саме завдяки механізмам консенсусу інформаційні потоки в децентралізованому обліковому середовищі набувають ознак саморегульованої системи. Розподілена перевірка даних вилучає необхідність централізованого контролю або зовнішньої аудиторської фільтрації – верифікаційна функція інтегрована безпосередньо в архітектуру облікового

процесу. Водночас різні типи консенсусу (Proof of Work, Proof of Stake, Delegated Proof of Stake, Practical Byzantine Fault Tolerance тощо) забезпечують баланс між швидкістю, безпекою та енергетичною ефективністю передавання інформації. Такий алгоритмічний контроль формує принцип «криптографічної довіри», за якого істинність даних підтверджується не авторитетом суб'єкта, а математичною перевіркою їх відповідності мережевим правилам.

Важливою характеристикою інформаційних потоків у децентралізованому обліку є їхня повна трасованість. Кожен запис у розподіленому реєстрі зберігає криптографічне посилання (хеш) на попередній блок, що створює безперервний ланцюг взаємопов'язаних даних. Унаслідок цього будь-яку транзакцію можна відстежити до її першоджерела, а будь-яка спроба змінити чи видалити інформацію автоматично порушує цілісність усього ланцюга і виявляється системою. Така архітектурна властивість формує технологічний аналог принципу «аудиторського сліду», який у традиційній системі забезпечується документальними доказами, а в блокчейн-середовищі – криптографічною незмінністю даних. Це відкриває можливості для формування концепції безперервного аудиту, у межах якого перевірка облікових даних відбувається в режимі реального часу, а не постфактум.

Синхронність інформаційних потоків у блокчейн-системі має фундаментальне значення для забезпечення узгодженості облікових даних. Оскільки кожен вузол володіє копією розподіленого реєстру, усі зміни в системі відображаються миттєво в усіх точках мережі після їх підтвердження. Так, усі учасники облікового процесу мають доступ до однаково актуальної інформації, що ліквідує часові лаги, інформаційні розриви та асиметрію даних між різними сторонами економічної взаємодії. З огляду на це блокчейн створює умови для переходу від дискретного фіксування операцій (у межах звітних періодів) до безперервного потоку даних, у якому бухгалтерський облік трансформується у процес безперервного моніторингу фінансово-господарської діяльності.

Однією з ключових рис інформаційних потоків у децентралізованому середовищі є їхня автономність. Дані після потрапляння до мережі існують незалежно від джерела їх створення і не потребують централізованого адміністрування або підтримки. Це забезпечується за рахунок криптографічної валідації, механізмів консенсусу та розподіленого збереження. Втрата одного або кількох вузлів не впливає

на доступність і цілісність інформації, оскільки інші учасники мережі зберігають її повні копії. Такий підхід радикально підвищує надійність облікової системи та усуває ризики маніпулювання або знищення даних унаслідок технічних чи людських помилок.

Інформаційні потоки в децентралізованому обліковому середовищі також відзначаються інтероперабельністю – здатністю взаємодіяти з іншими цифровими системами. Завдяки використанню відкритих протоколів, смартконтрактів і стандартизованих інтерфейсів (API) вони можуть бути інтегровані з фінансовими, управлінськими, логістичними та аналітичними платформами [82]. У результаті формується єдина цифрова екосистема, у межах якої бухгалтерська інформація перестає бути ізольованою функцією і стає системним елементом наскрізного управління ресурсами підприємства. Це сприяє реалізації концепції «єдиного джерела правди», коли всі користувачі системи оперують ідентичними даними, незалежно від функціонального контексту чи рівня доступу.

Узагальнюючи викладений вище матеріал, структуруємо його у вигляді характеристики інформаційних потоків децентралізованого бухгалтерського середовища (табл. 2.3).

Таблиця 2.3 – Характеристика інформаційних потоків децентралізованого бухгалтерського середовища

Назва елементу	Змістовна характеристика	Ключові наслідки для бухгалтерського обліку
1	2	3
Архітектоніка інформаційних потоків	Інформація циркулює в горизонтально структурованій мережі рівноправних вузлів, без централізованого контролера чи єдиного джерела істини	Формується нова парадигма інформаційної рівноваги – усі користувачі мають доступ до єдиного, синхронізованого набору даних
Принцип розподіленого реєстру	Кожна транзакція є одночасно інформаційною одиницею, об’єктом контролю та елементом облікових даних; її ініціює економічний агент, після чого відбувається мережна перевірка й долучення до блоку	Забезпечується безперервність, цілісність і хронологічна впорядкованість облікових даних; усувається потреба в централізованій обробці первинної інформації

Продовження таблиці 2.3

1	2	3
Механізми консенсусу як система контролю	Алгоритми (Proof of Work, Proof of Stake, DPoS, PBFT тощо) виконують функцію колективної верифікації достовірності транзакцій	Реалізується принцип «криптографічної довіри» – істинність даних визначається математичними доказами, а не авторитетом суб'єкта чи аудитора
Трасованість інформаційних потоків	Кожен блок містить хеш-посилання на попередній, що формує неперервний ланцюг даних; будь-яка зміна виявляється системою автоматично	Формується технологічний аналог принципу аудиторського сліду; створюються передумови для безперервного аудиту в режимі реального часу
Синхронність інформаційних оновлень	Копії розподіленого реєстру зберігаються в кожному вузлі; підтверджені зміни відображаються миттєво в усіх точках системи	Ліквідується інформаційна асиметрія; облік переходить від періодичного фіксування до безперервного моніторингу фінансово-господарської діяльності
Автономність інформаційних потоків	Дані після потрапляння до мережі існують незалежно від джерела, зберігаються у множині вузлів і не потребують адміністративної підтримки	Підвищується надійність облікової системи, усуваються ризики маніпулювання або втрати даних через людський чинник чи технічні збої
Інтер-операбельність та інтеграція	Використання відкритих протоколів, API та смартконтрактів забезпечує взаємодію з іншими цифровими системами (фінансовими, управлінськими, логістичними)	Формується єдина цифрова екосистема обліку; реалізується концепція «єдиного джерела правди»
Концепція довіри через технологію	Технологічна інфраструктура блокує можливості спотворення даних; верифікація та контроль вбудовані у саму систему	Перехід від моделі «довіри через перевірку» до «довіри через технологію»; формування самодостатньої, безперервно оновлюваної цифрової облікової системи
Інтегральна характеристика інформаційних потоків	Інформаційні потоки є основою нового типу цифрової облікової реальності, у якій дані мають властивості автономності, стійкості та самовідтворюваності	Бухгалтерський облік трансформується у саморегульовану інформаційно-аналітичну систему, що забезпечує достовірність й актуальність облікових даних у режимі реального часу

Джерело: складено авторами.

Можна стверджувати, що інформаційні потоки в децентралізованому обліковому середовищі формують якісно нову модель інформаційного обміну, де технологічна інфраструктура блокує можливості викривлення даних, а економічні процеси відображаються в реальному часі з гарантованим рівнем достовірності. Це забезпечує перехід від концепції «довіри через перевірку» до концепції «довіри через технологію», де верифікація і контроль стають невід'ємними властивостями самої інформаційної системи, а не зовнішніми інструментами регулювання. Так, блокчейн-технологія створює підґрунтя для формування самодостатньої, інтегрованої та безперервно оновлюваної системи бухгалтерського обліку, у якій інформаційні потоки є не лише каналами передавання даних, а структурною основою нового цифрового типу облікової реальності.

Отже, архітектура децентралізованого облікового середовища формує нову логіку бухгалтерського обліку, у якій традиційні функції оброблення, зберігання та перевіряння даних набувають алгоритмічного характеру. Вона створює підґрунтя для побудови довірчої цифрової екосистеми, де достовірність інформації забезпечується не суб'єктивними судженнями, а об'єктивними властивостями блокчейн-технологій. Це відкриває перспективи для розвитку концепції безперервного аудиту, автоматизованої аналітики та інтегрованої системи управління обліковими ризиками в умовах цифрової децентралізації.

2.2. Механізм функціонування блокчейн-реєстру у відображенні господарських операцій

Механізм функціонування блокчейн-реєстру у відображенні господарських операцій становить техніко-методологічне підґрунтя децентралізованої облікової системи, у якій бухгалтерська інформація формується, перевіряється та зберігається на основі розподіленого консенсусу учасників мережі [20]. На відміну від централізованих інформаційних систем, де оброблення облікових даних здійснюється в межах локальної бази даних під контролем адміністратора, блокчейн забезпечує одночасне функціонування множини взаємопов'язаних вузлів, кожен з яких зберігає ідентичну копію облікового реєстру [33]. Ключовою характеристикою такої архітектури є незмінність і безперервність даних, що гарантується криптографічними алгоритмами

хешування та механізмами узгодження (консенсусу) [84]. У результаті господарська операція не просто реєструється в системі, а стає частиною ланцюга блоків, де кожен новий запис підтверджує достовірність попередніх і водночас фіксує новий факт господарського життя.

Формування запису про господарську операцію в блокчейн-реєстрі є складним багаторівневим процесом, що поєднує технічні, методологічні та правові аспекти відображення економічних фактів у цифровому середовищі [56]. Його логіка ґрунтується на принципах достовірності, незмінності та відтворюваності даних, що досягаються через взаємодію криптографічних алгоритмів, мережевих протоколів та облікових стандартів, інтегрованих у єдину систему довіри. На відміну від традиційних бухгалтерських записів, які фіксуються в централізованих базах даних, блокчейн-технологія забезпечує децентралізовану верифікацію фактів господарської діяльності, що усуває потребу в посередницькому контролі та створює підґрунтя для формування саморегульованого інформаційного середовища бухгалтерського обліку [38].

Перший етап формування запису полягає у створенні цифрової транзакції ініціатором операції, яким є суб'єкт господарювання, контрагент або інший учасник мережі. У межах цієї транзакції формуються всі потрібні атрибути господарського факту – зміст операції, її економічна сутність, вартісна оцінка, дата здійснення, сторони взаємодії та посилання на активи або зобов'язання, яких вона стосується. Кожна транзакція супроводжується цифровим підписом, створеним за допомогою криптографічного ключа користувача, що забезпечує автентичність джерела інформації та вилучає можливість підроблення. На цьому етапі відбувається первинна ідентифікація суб'єкта, перевірка його повноважень щодо розпорядження активами, а також тестування транзакції на відсутність логічних суперечностей або дублювання попередніх записів у реєстрі. Так, перша фаза функціонування блокчейн-реєстру реалізує принципи верифікації, автентифікації та відповідності господарської операції внутрішнім правилам цифрової облікової системи.

На другому етапі розпочинається процес колективної перевірки інформації – досягнення консенсусу між вузлами мережі. Консенсус – це децентралізований алгоритмічний механізм, який забезпечує узгодженість усіх копій розподіленого реєстру. Його суть полягає в тому, що кожна нова транзакція має бути підтверджена більшістю учасників,

які незалежно один від одного перевіряють її достовірність і відповідність попередньому стану системи. Залежно від архітектури блокчейну, консенсус може досягатися різними методами –на основі обчислювальної складності (Proof of Work), через володіння часткою активів (Proof of Stake), через взаємне підтвердження повідомлень між вузлами (Practical Byzantine Fault Tolerance) тощо. Незалежно від алгоритму, спільним є те, що перевірка не залежить від людського чинника, а базується на обчислюваній довірі, що унеможливлює маніпуляції з даними. У такий спосіб система створює автоматизований аналог бухгалтерського контролю – кожна господарська операція проходить технокриптографічний аудит перед тим, як стати частиною постійного облікового запису.

Після досягнення консенсусу транзакції групуються в блок, який утворює новий елемент ланцюга облікового реєстру. Кожен блок містить набір підтверджених транзакцій, службову інформацію (метадані), часову позначку, хеш попереднього блоку та власний криптографічний ідентифікатор. Механізм хешування забезпечує унікальний зв'язок між блоками, утворюючи послідовний ланцюг, у якому будь-яке втручання в історичний запис автоматично призводить до порушення всієї структури. Це означає, що внесення змін у господарські дані без згоди мережі є технічно неможливим. Після успішної валідації новий блок додається до ланцюга, а його копія миттєво синхронізується на всіх вузлах мережі. Така одночасна дистрибуція гарантує єдність облікового простору та ліквідує ризик інформаційної асиметрії між користувачами. Усі учасники мають доступ до ідентичної, підтвердженої версії облікового реєстру, що підвищує рівень прозорості та взаємної довіри в господарському середовищі.

Особливу роль у механізмі функціонування блокчейн-реєстру відіграють смартконтракти, які перетворюють блокчейн із пасивного засобу зберігання інформації на активний інструмент виконання господарських дій. Смартконтракт – це програмний код, що автоматично виконує заздалегідь визначені умови, зафіксовані сторонами угоди. У системі бухгалтерського обліку він може забезпечувати автоматичне формування записів за настання подій, що мають облікове значення, наприклад – відображення доходу після виконання зобов'язання, нарахування відсотків або амортизації, проведення взаємозаліку чи корегування балансової вартості активів. Усі ці дії здійснюються без

участі людини, виключно за логікою алгоритму, що мінімізує ризики суб'єктивного впливу, затримок і помилок у відображенні господарських операцій.

Використання смартконтрактів у межах облікової системи створює умови для формування так званого «самообліковогo середовища», де господарські операції не лише реєструються, а й автоматично відображаються у звітності та аналітичних системах підприємства. Це означає, що обліковий процес трансформується з реактивного у проактивний: система не очікує на ручне введення даних, а генерує облікові записи в момент фактичного здійснення операції. Така логіка дає змогу інтегрувати бухгалтерський облік із суміжними підсистемами управління – фінансовими, логістичними, виробничими, маркетинговими – на основі єдиного інформаційного простору, де кожна подія має цифровий слід і юридичну значущість.

Процес формування запису в блокчейн-реєстрі є не лише технічною операцією, а й фундаментальним елементом нової методології бухгалтерського обліку, де кожен господарський факт проходить через багаторівневу верифікацію, автоматичне підтвердження та незмінне збереження. Це створює безпрецедентний рівень прозорості, достовірності та довіри до бухгалтерської інформації, що дає змогу говорити про перехід до нової парадигми –обліку на основі децентралізованого консенсусу, у якому істинність господарських операцій підтверджується не владними структурами чи аудиторами, а математичною логікою самої системи.

Криптографічний захист інформації в межах блокчейн-реєстру є ключовим техніко-методологічним інструментом забезпечення достовірності, цілісності та конфіденційності облікових даних, що обробляються в децентралізованому середовищі. У традиційних облікових системах безпека інформації покладається переважно на організаційні заходи контролю – паролі, політику доступу, внутрішній аудит, – тоді як у блокчейні захист реалізується на рівні самої архітектури системи. Це означає, що кожен обліковий запис, транзакція чи документ мають власний криптографічний ідентифікатор, створений за допомогою хеш-функцій, який гарантує незмінність та автентичність інформації від моменту її фіксації. У результаті будь-яке спотворення чи несанкціоноване редагування даних призводить до розриву логічного ланцюга блоків, що миттєво виявляється усіма вузлами мережі. Так, безпека

бухгалтерських записів у блокчейн-реєстрі не є результатом зовнішнього контролю, а є наслідком самоорганізованої криптографічної структури системи.

Двокомпонентна природа криптографічного захисту полягає в одночасному забезпеченні конфіденційності та достовірності даних. Конфіденційність досягається через використання асиметричного шифрування, де кожен учасник системи володіє парою ключів – приватним і публічним. Приватний ключ використовується для підписання транзакцій, а публічний – для перевірки їх достовірності іншими вузлами. Це означає, що лише власник приватного ключа може створити дійсний обліковий запис, а будь-яка спроба підробити цифровий підпис буде відхилена мережею. Водночас зміст транзакції залишається зашифрованим і доступний лише тим суб'єктам, які мають відповідні права доступу, що особливо важливо в бухгалтерському середовищі, де зберігаються фінансові, комерційні та персональні дані.

Зі свого боку підтвердження достовірності транзакцій забезпечується механізмом цифрового підпису, який є аналогом власноручного підпису бухгалтера, керівника або аудитора, але у значно більш надійному вигляді. Цифровий підпис створюється за допомогою математичної функції, що поєднує зміст транзакції з приватним ключем користувача, у результаті чого формується унікальний хеш-код. Цей код не може бути повторно використаний або підроблений, оскільки навіть мінімальна зміна в змісті операції створює новий, принципово інший хеш. Такий підхід забезпечує абсолютну доказовість кожної облікової події та формує нову якість бухгалтерської інформації – її математичну достовірність. У перспективі це дає змогу розглядати криптографічний підпис як цифровий аналог первинного документа, який має юридичну силу в системах електронного обліку та звітності.

Особливу роль у структурі криптографічного захисту відіграє принцип селективної прозорості, що визначає рівень доступу користувачів до інформації. У межах бухгалтерського обліку це означає, що різні групи стейкголдерів – власники, інвестори, аудитори, контролювальні органи, контрагенти – можуть мати різний обсяг прав щодо перегляду чи обробки облікових записів. Наприклад, внутрішні користувачі мають повний доступ до змісту господарських операцій, тоді як зовнішні учасники бачать лише факт здійснення операції та її цифровий слід (хеш). Така модель дає змогу поєднати принципи прозорості

бізнесу з вимогами збереження комерційної таємниці, створюючи гнучку систему інформаційної взаємодії між усіма сторонами економічного процесу. Водночас вона забезпечує контрольовану відкритість, що є однією з ключових вимог сучасного корпоративного управління та аудиту.

Криптографічні алгоритми в блокчейн-реєстрі також відіграють роль механізму колективного підтвердження прав власності та відповідальності за господарські рішення. Оскільки кожен обліковий запис має власного автора, засвідченого цифровим підписом, стає можливим простежити повний ланцюг відповідальності – від ініціатора транзакції до всіх учасників, що підтвердили її достовірність. Це створює передумови для підвищення рівня прозорості управлінських процесів і зменшення ризику маніпуляцій або шахрайських дій. Фактично, блокчейн перетворюється на самодостатню систему довіри, де достовірність даних гарантується не соціальними чи адміністративними механізмами, а суто математичними принципами.

Збереження всіх записів у розподіленому середовищі забезпечує унікальну властивість – незнищуваність облікової інформації. Кожен вузол мережі містить повну копію реєстру, що робить неможливим його фізичне видалення або фальсифікацію навіть у разі втрати частини вузлів. Такий підхід формує основу для створення надійного бухгалтерського архіву, у якому всі дані зберігаються безстроково й у незмінному вигляді. Це зі свого боку створює нові можливості для аудиту, судово-економічної експертизи та державного фінансового контролю, адже кожен факт господарського життя має цифровий слід, який можна верифікувати незалежно від часу його виникнення. Так, блокчейн є не лише інструментом оперативного обліку, а й фундаментом для створення історично достовірної бази фінансових даних підприємства.

Криптографічний захист у блокчейн-реєстрі є не просто технічним засобом безпеки, а системоутворювальним елементом децентралізованої облікової моделі. Він забезпечує баланс між відкритістю інформаційного простору та збереженням комерційної конфіденційності, гарантує повну доказовість кожної господарської операції, а також створює технологічну основу для формування обліку нового покоління – обліку, в якому довіра ґрунтується не на людському контролі, а на математично доведеній істинності даних.

Механізми функціонування блокчейн-реєстру принципово трансформують класичну логіку бухгалтерського обліку, змінюючи його природу від послідовної обробки документів до безперервного процесу верифікації економічних фактів. У традиційній системі обліковий процес передбачає часовий розрив між здійсненням господарської операції, її документальним підтвердженням і відображенням у регістрах, що неминуче знижує оперативність і підвищує ризик інформаційних втрат або викривлень. Натомість у блокчейн-середовищі кожна операція набуває форми транзакції – цифрового запису, який створюється й підтверджується в момент її здійснення. Завдяки цьому бухгалтерський облік перетворюється на систему, що діє в реальному часі, де господарська подія одночасно є і фактом діяльності, і записом у реєстрі, і доказом її легітимності.

Фундаментальною особливістю такої архітектури є безперервність облікового ланцюга, у якому кожен запис (транзакція) пов'язаний із попередніми через криптографічні хеші, що створює хронологічно впорядковану, незмінну послідовність подій. Це усуває потребу в постійній реконсиляції даних між підсистемами чи контрагентами, адже кожна зміна автоматично фіксується й підтверджується мережею. Такий підхід означає перехід від моделі періодичного обліку, орієнтованого на звітні цикли, до моделі безперервного реєстру, у якому кожна господарська дія набуває статусу завершеної облікової одиниці в момент її підтвердження. Унаслідок цього формується нова парадигма бухгалтерського процесу – «облік як потік даних», а не «облік як етапна процедура документування».

Математичне підтвердження істинності кожної транзакції забезпечується алгоритмами консенсусу, які замінюють традиційні механізми бухгалтерського контролю. Рішення про достовірність господарського запису приймається не окремим фахівцем чи інституцією, а децентралізованою мережею вузлів, що перевіряють його відповідність визначеним правилам. Завдяки цьому відбувається автоматична перевірка наявності активів, відповідності суми операції, правильності підписів і відсутності подвійного відображення. Така колективна перевірка виконує роль математично вивіреного аудиту, який здійснюється постійно та унеможливлює спотворення даних навіть у разі збоїв або спроб маніпуляції.

Ключовим наслідком впровадження блокчейн-механізмів у бухгалтерський облік є перехід від постфактумного до проактивного підходу до фіксації господарських подій. Якщо в традиційній системі бухгалтер відображає операцію після її здійснення й підтвердження документом, то у блокчейн-середовищі сам факт виконання дії – передача активу, виконання зобов'язання, настання умов контракту – автоматично ініціює створення облікового запису. Смартконтракти є тригерами такого процесу, забезпечуючи синхронізацію між подією в реальному секторі та її цифровим відображенням у системі. Це не лише підвищує швидкість облікових процедур, а й формує основу для побудови «самообліковихх» підприємств, де облік відбувається без участі людини.

Високий рівень деталізації й безперервна валідація даних у блокчейн-реєстрі створюють унікальні умови для повної простежуваності господарських процесів. Кожна операція має точну часову позначку, ідентифікатор учасників, опис сутності операції й цифрове підтвердження її правомірності. Завдяки цьому формується так звана «цифрова історія активу», яка дає змогу простежити весь його життєвий цикл – від моменту створення або придбання до вибуття чи ліквідації. Для аудиту це означає можливість здійснення перевірки без запитів чи відбору вибірки – аудитор має доступ до повного, хронологічно впорядкованого масиву достовірних даних[6]. Така технологічна основа забезпечує появу нової концепції – «аудиту в режимі реального часу», який не лише виявляє відхилення, а й запобігає їх виникненню.

Вилучення ризику дублювання або спотворення інформації в блокчейн-реєстрі досягається за рахунок властивостей розподіленого зберігання та «єдиної версії істини». Кожен вузол мережі має ідентичну копію облікових записів, тому будь-які зміни одразу відображаються в усіх екземплярах системи. Це унеможливлює існування паралельних, конфліктних версій облікових даних, що є характерною проблемою централізованих систем. Так, облікова інформація набуває не лише технологічної, а й епістемологічної стабільності: її істинність підтверджується самою структурою системи, а не довірою до суб'єкта, який її формує.

Механізми функціонування блокчейн-реєстру не просто вдосконалюють окремі етапи облікового процесу, а створюють нову модель бухгалтерської реальності – відкриту, самоорганізовану, достовірну й

математично верифіковану. Вона забезпечує не лише фіксацію економічних подій, а й постійний моніторинг їх істинності, синхронізує бухгалтерський облік із бізнес-процесами в реальному часі та формує основу для еволюції облікової науки в напрямі цифрової автономії й технологічно підтвердженої довіри.

Узагальнюючи викладений вище матеріал, структуруємо його у вигляді характеристики механізму функціонування блокчейн-реєстру у відображенні господарських операцій (табл. 2.4).

Таблиця 2.4 – Характеристика механізму функціонування блокчейн-реєстру у відображенні господарських операцій

Назва елементу механізму	Змістовна характеристика	Методологічне значення для бухгалтерського обліку
1	2	3
Архітектура блокчейн-реєстру	Децентралізована мережа взаємопов'язаних вузлів, кожен з яких зберігає ідентичну копію облікового реєстру; відсутність центрального адміністратора	Формується техніко-методологічна основа децентралізованого бухгалтерського обліку, що вилучає єдину точку контролю та підвищує достовірність даних
Незмінність і безперервність даних	Гарантується криптографічним хешуванням і механізмами консенсусу; кожен новий запис підтверджує попередні	Створюється ланцюг достовірності – безперервна історія господарських подій, що унеможливлює фальсифікацію облікових записів
Формування цифрової транзакції	Ініціатор операції створює транзакцію, яка містить атрибути господарського факту (сутність, вартість, дата, сторони, активи / зобов'язання); підписується криптографічним ключем	Реалізуються принципи верифікації, автентифікації та відповідності господарської операції правилам облікової системи
Досягнення консенсусу	Колективна верифікація транзакцій усіма вузлами мережі за алгоритмами PoW, PoS, DPoS, PBFT тощо	Виникає автоматизований аналог бухгалтерського контролю – математична перевірка достовірності господарських фактів без людського втручання

Продовження таблиці 2.4

1	2	3
Формування блоку	Підтверджені транзакції групуються у блок; блок містить хеш попереднього блоку, часову позначку, метадані та унікальний криптографічний ідентифікатор	Забезпечується єдність облікового простору; будь-яке втручання в історію даних виявляється системою автоматично
Синхронізація реєстру	Новий блок миттєво розповсюджується по всіх вузлах; усі копії реєстру узгоджені та ідентичні	Усунення інформаційної асиметрії між користувачами; усі сторони мають доступ до однаково підтверджених даних
Смарт-контракти	Програмні коди, що автоматично виконують умови угод (нарахування відсотків, визнання доходів, амортизація тощо)	Формується самообліковесередовище, де господарські операції автоматично відображаються у звітності без участі бухгалтера
Крипто-графічний захист	Вбудовані механізми хешування, цифрових підписів і шифрування забезпечують цілісність, конфіденційність і автентичність даних	Перехід від організаційного контролюдо структурно-технологічної безпеки; кожен запис має власний криптографічний ідентифікатор
Асиметричне шифрування	Використання приватного та публічного ключів: підписання транзакцій і перевірка достовірності іншими вузлами	Забезпечується математична доказовістьоблікових записів; цифровий підпис стає аналогом первинного документа
Селективна прозорість	Різні групи стейкголдерів мають різний рівень доступу до даних: від повного перегляду до часткової видимості хешів	Поєднання прозорості та конфіденційності: контрольована відкритість інформації для різних користувачів
Колективне підтвердження відповідальності	Кожен запис має автора, підтвердженого цифровим підписом; створюється ланцюг відповідальності за господарські рішення	Підвищення прозорості корпоративного управління; усунення можливостей для маніпуляцій і шахрайства
Розподілене збереження	Копії реєстру зберігаються на всіх вузлах, що гарантує незнищуваність і довготривале збереження облікової інформації	Формується надійний цифровий архів – база для аудиту, судово-економічної експертизи й фінансового контролю

Продовження таблиці 2.4

1	2	3
Безперервність облікового ланцюга	Кожна транзакція пов'язана з попередньою; створюється хронологічна, незмінна послідовність облікових подій	Перехід від періодичного до безперервного обліку; ліквідується потреба в реконсиляції даних
Математична верифікація даних	Консенсусні алгоритми перевіряють коректність, наявність активів, відсутність подвійного відображення	Формується математично вивірений аудит, що здійснюється постійно і не залежить від людського чинника
Простежуваність і цифрова історія активів	Кожна операція має часову позначку, ідентифікатор і опис сутності; створюється цифровий ланцюг життєвого циклу активу	Можливість здійснення аудиту в реальному часі; забезпечення повної доказовості фінансових даних
Єдина версія істини	Ідентичність усіх копій реєстру унеможливлює паралельні чи конфліктні версії облікової інформації	Дані набувають епістемологічної стабільності – істинність забезпечується структурою системи, а не суб'єктивною оцінкою
Загальна методологічна трансформація	Облік стає процесом безперервної верифікації економічних фактів у момент їх виникнення	Перехід до парадигми обліку на основі децентралізованого консенсусу – «довіра через технологію»

Джерело: складено авторами.

Отже, блокчейн-реєстр у системі бухгалтерського обліку виконує роль не лише бази даних, а й механізму формування довіри, який гарантує автентичність, цілісність і хронологічну впорядкованість господарських фактів. Його функціонування забезпечує самодостатній, прозорий і технологічно контрольований процес відображення економічних операцій, де достовірність даних ґрунтується не на зовнішньому контролі, а на вбудованих алгоритмах консенсусу та криптографічного підтвердження. У перспективі така модель стає фундаментом для побудови нової парадигми бухгалтерського обліку – децентралізованої, автоматизованої та невразливої до маніпуляцій інформаційної системи, у якій кожен запис є незаперечним цифровим доказом реальної господарської діяльності.

2.3. Смартконтракти як інструмент автоматизації облікових процедур і контролю достовірності даних

Смартконтракти в системі децентралізованого обліку є фундаментальним інструментом автоматизації бухгалтерських процесів і забезпечення достовірності фінансових даних. Вони являють собою програмні алгоритми, що зберігаються в блокчейн-мережі й автоматично виконують заздалегідь визначені дії після настання конкретних умов. На відміну від традиційних договірних механізмів, які потребують участі посередників або ручного контролю, смартконтракти функціонують у межах коду, що гарантує їх безумовне виконання. У контексті бухгалтерського обліку це означає, що визнання, оцінювання, відображення та узгодження господарських операцій можуть здійснюватися безпосередньо системою – без участі людини, з дотриманням усіх методологічних принципів і часових параметрів.

Інтеграція смартконтрактів у бухгалтерське середовище створює принципово новий спосіб організації облікових процесів, який трансформує традиційно реактивну модель фіксації подій у проактивну модель їхнього автоматичного відображення. Замість того, щоб очікувати на завершення зовнішніх процедур і ручне введення інформації до облікових систем, смартконтракти дають змогу формалізувати договірні умови, тригери господарських подій і алгоритми їхнього оброблення у вигляді машинно-зчитуваних правил, що виконуються безпосередньо на рівні технологічної платформи [74]. Така формалізація означає, що юридично значуща подія або її цифрове підтвердження (наприклад, електронний транспортний лист, цифровий підпис поставки або подія від IoT-датчика) автоматично активує набір бухгалтерських алгоритмів: визнання доходу, нарахування дебіторської заборгованості, корекцію запасів, формування ПДВ-зобов’язань та інші записи в регістри.

На операційному рівні це реалізується через кодування кожного договору або господарської операції як набору умов, за виконання яких система генерує відповідні бухгалтерські записи за заздалегідь визначеними шаблонами відображення в плані рахунків. Прикладом є угода купівлі-продажу: отримання електронного підтвердження доставки товару від постачальника (подія, що надходить від зовнішнього джерела через оракул) є тригером для смартконтракту, який одночасно

виконує три взаємопов'язані дії – визнання доходу продавцем згідно з критеріями визнання, створення запису про дебіторську заборгованість покупця та зменшення кількості запасів у системі. Аналогічно, настання строку сплати податку може ініціювати автоматичне нарахування зобов'язання з податку і формування відповідного запису в реєстрі грошових зобов'язань, що забезпечує своєчасність податкових зобов'язань і зменшує ризик прострочень.

У такій моделі облікові операції набувають властивостей «самоініціації» й «самоузгодження»: смартконтракти не лише ініціюють записи, але й перевіряють взаємну консистентність даних між контрагентами та підсистемами (наприклад, відповідність даних логістики і виставлених рахунків), а також автоматично корелюють інформацію про оплату, період звітності та податкові правила. Це забезпечує безперервність і своєчасність відображення господарської діяльності, що сприяє переходу до режиму безперервної фінансової звітності та постійного контролю. Важливим ефектом є підвищення якості доказової бази: криптографічно підписані транзакції, часові мітки та незмінні ланцюги подій створюють надійний слід аудиту, який доступний для аудиторських процедур у режимі близькому до реального часу.

Водночас для забезпечення адекватності такої автоматизації потрібна чітка архітектура інтеграції, що містить узгодження семантики облікових категорій із кодом смартконтрактів, інтерфейси між блокчейн-реєстром і ERP / платіжними системами, механізми подачі зовнішніх даних (оракулів) та служби розв'язання винятків [21; 63]. Формалізація правил вимагає приведення договорів до машинно-сприйнятного вигляду, стандартизованих шаблонів проводок та однозначного відображення економічної суті операцій у плані рахунків. Для забезпечення цілісності й контролю важливим є впровадження багаторівневої логіки перевірок у смартконтрактах: валідація підписів, перевірка балансу, обмеження лімітів, умови подвійного затвердження для суттєвих операцій та механізми відкату або корекції в разі виявлення помилки.

Юридичні та регуляторні аспекти автоматичного бухгалтерського відображення вимагають узгодження з існуючими стандартами фінансової звітності та податкового законодавства. Потрібно гарантувати, що алгоритмічне визнання й оцінка операцій відповідають критеріям МСФЗ / НП(С)БО, зокрема в частині визначення моменту

визнання доходів, оцінки корисності та відображення зобов'язань. Оскільки смартконтракти виконуються автоматично, потрібна прозора документація версій контрактів, процедур тестування та аудитів коду (охоплюючи формальну верифікацію бізнес-логіки), щоб забезпечити відповідальність та відтворюваність рішень, що призвели до бухгалтерських записів.

Технічною та операційною проблемою є питання достовірності зовнішніх даних – ораклів, які передають підтвердження подій у блокчейн. Надійність автоматичного обліку напряму залежить від безпеки, доступності й чесності цих джерел; тому архітектура повинна передбачати децентралізовані або перевірені оракли, механізми репутації постачальників даних, мультисигнальні джерела даних та логіку вирішення розбіжностей. Крім того, у разі використання публічних ланцюгів потрібно враховувати питання масштабованості й вартості транзакцій (латентність, комісії), що впливають на оперативність та економічну доцільність автоматичних проводок; у деяких сценаріях доречніше застосовувати дозволені блокчейн-мережі з контрольованою пропускною здатністю і політиками доступу.

Інтеграція смартконтрактів також змінює підходи до внутрішнього контролю та розподілу обов'язків: автоматизація рутинних операцій знижує ризик помилок ручного введення й шахрайства, але одночасно вимагає нових контрольних точок – контроль за змінами коду контрактів, управління ключами, моніторинг аномалій у виконанні контрактів і процеси реагування на комп'ютерні інциденти. Впровадження повинно супроводжуватися адаптацією внутрішніх процедур верифікації, змінами в політиках доступу до системи, а також навчанням бухгалтерського персоналу й аудиторів у сфері цифрових доказів та інтерпретації криптографічних слідів.

Для практичного впровадження рекомендовано життєвий цикл смартконтракту, що охоплює: аналітичну стадію формалізації бізнес-правил; розробку й формалізацію бухгалтерської логіки (відповідність плану рахунків та обліковим політикам); тестування (охоплюючи тестування на тестових мережах та формальну верифікацію критичних алгоритмів); розгортання у контрольованому середовищі; моніторинг виконання та аудит; механізми версійності й процедур оновлення або відкликання контрактів [52]. Такий підхід дає змогу поєднати гнучкість автоматизації із суворими вимогами до обліку та аудиторської відтворюваності.

Переваги використання смартконтрактів у бухгалтерії очевидні: скорочення часу на обробку господарських операцій, зниження витрат на рутинні операції, підвищення точності й оперативності фінансових даних, посилення антиманіпуляційних бар'єрів і покращення доступності доказової бази для аудиту [7].

Використання смартконтрактів у бухгалтерському обліку відкриває новий вимір у реалізації принципів облікової політики підприємства, оскільки дає змогу інтегрувати її положення безпосередньо в алгоритмічну структуру цифрових процедур. На відміну від традиційного підходу, де облікова політика існує у вигляді нормативного документа, що регламентує порядок оброблення господарських операцій, алгоритмічне втілення цих правил у смартконтрактах перетворює їх на безпосередньо діючі інструкції, які виконуються в автоматичному режимі. У цьому контексті смартконтракти постають як своєрідний «операційний код» облікової політики, що забезпечує не лише її формальне дотримання, а й унеможливлює відхилення від установлених правил без відповідної авторизації або зміни коду.

Така інтеграція дає змогу створити середовище, у якому контроль за відповідністю облікових дій внутрішнім та зовнішнім стандартам здійснюється не постфактум, а в момент здійснення операції. Алгоритм, закладений у смартконтракт, здатний автоматично перевіряти, чи відповідає конкретна транзакція прийнятій обліковій політиці підприємства, чинним нормативним вимогам та принципам міжнародних стандартів фінансової звітності. Наприклад, система може бути запрограмована на перевірку коректності застосування методу оцінювання вибуття запасів відповідно до затвердженої облікової політики підприємства. Якщо господарська операція відображена з порушенням цих правил, смартконтракт може або заблокувати її виконання, або ініціювати процес автоматичного повідомлення відповідальної особи для прийняття рішення щодо корекції дій.

Аналогічний підхід може бути застосований до процедур визнання доходів і витрат. Смартконтракт здатний аналізувати умови договору, визначати момент переходу ризиків і вигод власності та, виходячи з цього, встановлювати момент визнання доходу або витрат згідно з вимогами МСФЗ / НП(С)БО. У такий спосіб алгоритм функціонує як вбудований контрольний механізм, що гарантує дотримання концептуальних засад бухгалтерського обліку – принципу нарахування,

суттєвості, превалювання сутності над формою тощо. Завдяки цьому облікові дані формуються із забезпеченням як своєчасності, так і відповідності економічній суті операцій, мінімізуючи ризики маніпуляцій або помилкового відображення фінансових результатів.

Фактична реалізація таких алгоритмів створює цифровий аналог внутрішнього контролю, який функціонує безперервно й не потребує постійного втручання бухгалтера чи аудитора. Якщо у традиційній системі контроль здійснюється за рахунок вибіркових перевірок, внутрішнього аудиту чи тестування процедур, то в умовах блокчейн-інтегрованих облікових систем смартконтракт виконує роль автоматизованого «вбудованого контролера». Його логіка забезпечує не лише перевірку правильності даних на етапі введення, але й постійний моніторинг змін, зв'язків між об'єктами обліку, наявності узгодженості між первинними даними, аналітичними регістрами та підсумковими звітами.

Крім того, автоматичний контроль, реалізований за допомогою смартконтрактів, підвищує рівень прозорості та відтворюваності облікових процедур. Усі операції, перевірки та результати їхньої валідації фіксуються в блокчейні, що унеможливлює несанкціоноване втручання в історію змін і створює незмінний цифровий слід для цілей аудиту. Так, кожна господарська подія супроводжується автоматичною верифікацією її відповідності правилам облікової політики, що дає змогу аудитору не лише перевіряти підсумкові результати, але й оцінювати сам процес облікового відображення як об'єкт контролю.

З методологічної точки зору, впровадження алгоритмізованої облікової політики на основі смартконтрактів сприяє переходу до парадигми «вбудованого контролю» в бухгалтерському обліку, де забезпечення достовірності даних здійснюється не через перевірки після здійснення операцій, а через їхню автоматичну валідацію в момент формування. Такий підхід відповідає сучасним концепціям безперервного аудиту та безперервного моніторингу, що набувають особливої актуальності в умовах цифрової децентралізації.

Смартконтракти є не лише технічним інструментом автоматизації бухгалтерських процедур, але й концептуальною основою побудови нової системи забезпечення достовірності облікових даних. Вони трансформують функцію контролю з періодичної та вибіркової у постійну й всеохопну, забезпечуючи високий рівень довіри до фінансової

інформації. У перспективі це може призвести до формування автономних облікових систем, де достовірність і відповідність даних забезпечуються не зовнішнім контролем, а внутрішньою алгоритмічною логікою, вбудованою у структуру кожної операції.

Застосування смартконтрактів у бухгалтерському обліку має глибокі наслідки для усунення інформаційної асиметрії, яка традиційно притаманна економічним відносинам між суб'єктами господарювання, контролювальними органами, аудиторами та іншими стейкхолдерами. Інформаційна асиметрія, що виникає внаслідок різного рівня доступу до даних, часу їхнього отримання та ступеня достовірності, є однією з основних причин зниження ефективності ринкових взаємодій і контролю. Смартконтракти, як елемент блокчейн-екосистеми, створюють принципово нове середовище, у якому всі учасники господарського процесу отримують одночасний, синхронізований і незмінний доступ до релевантної інформації, що забезпечує рівність інформаційних прав і можливостей.

Завдяки децентралізованій природі блокчейн-мережі всі сторони контракту – постачальник, покупець, фінансова установа, аудитор або контролювальний орган – мають доступ до єдиного джерела правди, у якому відображені умови договору, статус його виконання, підтверджені факти здійснення господарських операцій і результати взаєморозрахунків. Кожна дія, пов'язана з виконанням умов контракту, автоматично реєструється в блокчейні та верифікується мережею, що вилучає можливість односторонньої зміни даних або маніпуляцій із хронологією подій. Це створює об'єктивне цифрове середовище довіри, у якому дані не залежать від волі окремих сторін і не потребують постійного узгодження чи звірки між ними.

Смартконтракти усувають необхідність додаткового підтвердження фактів здійснення операцій, оскільки сама логіка їхнього виконання забезпечує автоматичну генерацію цифрового підтвердження в момент настання події. Наприклад, отримання товару покупцем, зафіксоване системою постачання або підтверджене електронним підписом, автоматично активує виконання умов смартконтракту: визнається дохід продавця, нараховується зобов'язання покупця, здійснюється запис у відповідних облікових реєстрах, а інформація про транзакцію одночасно стає доступною всім учасникам. У результаті усуваються часові лаги між здійсненням операції та її відображенням у

системах різних суб'єктів, а також мінімізуються ризики виникнення розбіжностей через різночитання або затримку інформації.

Ключовим аспектом є те, що всі записи у блокчейні мають ознаки незмінності, криптографічного захисту та підтвердження часової послідовності. Це означає, що інформація про факт здійснення операції, її суму, контрагентів, дату та умови є одночасно підтвердженою й доступною всім уповноваженим сторонам. У такий спосіб забезпечується тотальна прозорість і повна синхронізація даних.

Для зовнішніх користувачів інформації, насамперед контролювальних органів і аудиторів, такі властивості блокчейн-інфраструктури відкривають якісно нові можливості. Аудитор, отримуючи доступ до розподіленого реєстру, може в режимі реального часу перевіряти фактичність і повноту облікових даних, простежувати логіку формування записів, аналізувати послідовність операцій і відсутність спотворень. Контролювальні органи зі свого боку можуть здійснювати дистанційний моніторинг дотримання податкового та фінансового законодавства, отримуючи дані безпосередньо з децентралізованої системи, а не через проміжні звіти або декларації. Це дає змогу суттєво скоротити часові витрати на перевірки, зменшити ризики корупційного впливу та підвищити об'єктивність оцінки діяльності суб'єктів господарювання.

З методологічної точки зору, усунення інформаційної асиметрії завдяки смартконтрактам сприяє еволюції бухгалтерського обліку від моделі постфактум-реєстрації до моделі обліку в реальному часі, у якій усі облікові події фіксуються й підтверджуються безпосередньо в момент їх виникнення [63]. Це створює передумови для становлення концепції «прозорої економіки», де довіра між учасниками господарських процесів ґрунтується не на зовнішніх перевірках, а на технічній достовірності й незмінності даних, закладеній у блокчейн-протокол.

У перспективі така технологічна трансформація може призвести до зниження ролі посередницьких інституцій, відповідальних за підтвердження достовірності даних, оскільки їхні функції частково перейдуть до алгоритмічно контрольованого середовища. Проте це не означає зникнення потреби в професійних бухгалтерах і аудиторах – навпаки, змінюється характер їхньої діяльності: замість ручного збору й перевірки інформації акцент переноситься на аналітичну, інтерпретаційну та стратегічну роботу з даними, отриманими з високим рівнем достовірності.

Смартконтракти, інтегровані в систему бухгалтерського обліку на базі блокчейн-технологій, є не лише засобом автоматизації операцій, але й потужним інструментом гармонізації інформаційного простору між усіма учасниками економічної діяльності. Вони забезпечують рівність доступу до даних, усувають можливості інформаційних маніпуляцій, підвищують якість контролю й сприяють формуванню нового рівня довіри до фінансової інформації як основи економічного розвитку в умовах цифрової децентралізації.

З технічного погляду, смартконтракти функціонують як автономні програмні модулі, інтегровані у блокчейн-інфраструктуру, що взаємодіють із розподіленим реєстром через криптографічні механізми підтвердження подій. Кожен елемент такого контракту – умова, дія, результат – має чітко визначену логіку виконання, яка реалізується лише після досягнення консенсусу в мережі щодо істинності події, що її ініціює. Цей процес охоплює перевірку цифрових підписів, хешів транзакцій, часових міток і підтвердження валідності даних незалежними вузлами (нодами). Так, будь-яка дія, передбачена контрактом, може бути виконана виключно за умови криптографічної верифікації відповідних даних, що унеможливлює фальсифікацію, несанкціоноване втручання або передчасне виконання зобов'язань.

Така технічна архітектура створює унікальні передумови для формування абсолютно достовірної облікової інформації. Оскільки смартконтракт діє лише після підтвердження настання події з боку мережі, кожен бухгалтерський запис, сформований на його основі, має подвійний рівень верифікації: алгоритмічний (технологічний) та економічний (змістовний). Алгоритмічний рівень гарантує, що подія справді існувала в цифровому середовищі, а економічний забезпечує, що вона відповідає сутності господарської операції. Це забезпечує надзвичайно високий ступінь довіри до облікових даних, оскільки вони формуються не суб'єктивним рішенням бухгалтера, а на підставі об'єктивно підтверджених фактів, визнаних усією мережею.

У цьому контексті виникає концепція «самоперевірного обліку», за якої перевірка достовірності операції є невіддільною частиною процесу її фіксації. Іншими словами, сам акт запису господарської операції в блокчейн одночасно виконує функцію аудиторського підтвердження її істинності. Завдяки криптографічній цілісності записів, кожна операція стає елементом незмінного ланцюга, де будь-яка

спроба змінити інформацію в минулих блоках призводить до порушення структури всього реєстру, що виявляється автоматично. Так, сам блокчейн є універсальним механізмом внутрішнього контролю, а смартконтракт – його активним виконавчим компонентом, який ініціює лише ті події, достовірність яких безумовно підтверджена.

На концептуальному рівні смартконтракти забезпечують перехід бухгалтерського обліку до моделі цифрової автономії [63]. У межах цієї моделі облікова система набуває властивостей інтелектуального середовища, здатного не лише фіксувати, але й інтерпретувати економічні події згідно із заданими логічними правилами та принципами бухгалтерської політики. Смартконтракт може аналізувати умови договору, визначати настання моменту визнання доходу або витрат, автоматично виконувати оцінювання активів відповідно до визначеного методу, а також ініціювати нарахування податкових зобов'язань або резервів. У результаті бухгалтерський процес стає не просто автоматизованим, а концептуально переосмисленим – із наголосом на алгоритмізацію управлінських і контрольних функцій.

Інтеграція смартконтрактів у бухгалтерські системи створює передумови для побудови нового типу облікового циклу – безперервного, інтегрованого й самооновлюваного. Безперервність забезпечується тим, що кожна операція обробляється в реальному часі, а результати її виконання миттєво фіксуються у спільному реєстрі. Інтегрованість означає злиття етапів визнання, оцінки, класифікації та контролю в єдиний алгоритмічний процес, де відсутні часові або інформаційні розриви між подією та її бухгалтерським відображенням. Самооновлюваність виявляється у здатності системи адаптуватися до змін нормативних вимог або внутрішніх політик через оновлення логіки смартконтрактів, що дає змогу підтримувати актуальність облікової інформації без ручного втручання.

Таке переосмислення методології бухгалтерського обліку означає перехід від традиційної ролі бухгалтера як реєстратора господарських подій до функції аналітика та дизайнера алгоритмів, який визначає логіку їхнього відображення в цифровому середовищі. Смартконтракти в цьому контексті стають ядром нової методологічної парадигми, у якій достовірність фінансових даних має не лише документальне, а й математично доведене підтвердження. Криптографічна природа блокчейна, поєднана з логічною структурою смартконтрактів,

забезпечує таку рівновагу між точністю, прозорістю та ефективністю, яка раніше була недосяжною в централізованих облікових системах.

Узагальнюючи викладений вище матеріал, структуруємо його у вигляді характеристики смартконтрактів у системі децентралізованого бухгалтерського обліку (табл. 2.5).

Таблиця 2.5 – Характеристика смартконтрактів у системі децентралізованого бухгалтерського обліку

Аспект характеристики смартконтрактів	Змістовна характеристика	Ключові наслідки для бухгалтерського обліку
1	2	3
Сутність смартконтрактів у децентралізованому обліку	Смартконтракти – це програмні алгоритми, що зберігаються у блокчейн-мережі та автоматично виконують заздалегідь визначені дії за настання певних умов	Автоматизація бухгалтерських процесів, вилучення людського чинника, підвищення достовірності фінансових даних
Функціональна роль у системі обліку	Виконують роль автоматизованих виконавців господарських операцій: визнання, оцінювання, відображення, узгодження	Перехід від реактивної моделі фіксації подій до проактивної моделі автоматичного відображення операцій
Принцип дії	Виконання умов договору кодується як набір логічних правил; за настання події (через оракул) автоматично генеруються бухгалтерські записи	Формування проводок за заздалегідь визначеними шаблонами; забезпечення своєчасності відображення операцій
Властивості операцій	Самоініціація та самоузгодження: контракти самостійно перевіряють коректність і консистентність даних між підсистемами	Формування безперервного обліку й постійного контролю достовірності операцій
Архітектура інтеграції	Необхідне узгодження семантики облікових категорій із кодом контрактів, взаємодія з ERP/платіжними системами, використання оракулів	Потреба в стандартизації форматів даних, інтерфейсів і механізмів перевірки достовірності зовнішніх подій

Продовження таблиці 2.5

1	2	3
Система контролю та валідації	Передбачає валідацію підписів, балансів, лімітів, подвійне затвердження операцій, можливість повернення на крок назад у разі помилки	Формування багаторівневої структури контролю в автоматизованому режимі
Юридична та регуляторна відповідність	Необхідність узгодження алгоритмічного визнання операцій із МСФЗ / НП(С)БО	Забезпечення відповідності автоматичного обліку вимогам законодавства та стандартів звітності
Проблема достовірності оракулів	Оракули – джерела зовнішніх даних для блокчейна; ризики фальсифікації чи збоїв	Потреба в децентралізованих або перевірених оракулах, репутаційних механізмах, мультисигнальних джерелах даних
Вплив на внутрішній контроль	Автоматизація рутинних процедур знижує людський ризик, але потребує нових контрольних точок – управління ключами, моніторинг коду	Перехід від контролю документів до контролю алгоритмів; формування культури кіберконтролю
Переваги впровадження	Скорочення часу й витрат, підвищення точності, достовірності, прозорості та антикорупційної стійкості	Зростання ефективності облікової системи й довіри до фінансової інформації
Смартконтракт як «операційний код» облікової політики	Алгоритмічне втілення облікової політики у програмному коді, що виконує її положення автоматично	Гарантоване дотримання принципів облікової політики без відхилень
Механізм автоматичного контролю відповідності	Контракт перевіряє відповідність операцій політиці підприємства, МСФЗ / НП(С)БО, блокує або корегує порушення	Формування вбудованого механізму внутрішнього контролю в реальному часі
Безперервний аудит і моніторинг	Усі перевірки й транзакції фіксуються в блокчейні; аудитор має доступ до незмінного сліду подій	Перехід до моделі безперервного аудиту; забезпечення тотальної прозорості
Усунення інформаційної асиметрії	Всі учасники мають синхронізований доступ до єдиного джерела правди (розподілений реєстр)	Рівність інформаційних прав, скорочення часу на перевірки, мінімізація конфліктів даних

Продовження таблиці 2.5

1	2	3
Значення для зовнішнього контролю	Аудитори та регулятори можуть перевіряти достовірність операцій безпосередньо в блокчейні	Підвищення об'єктивності контролю, зменшення корупційних ризиків, розвиток дистанційного аудиту
Еволюція моделі обліку	Перехід від постфактум-реєстрації до реального часу; інтеграція фіксації, оцінки та контролю в єдиний процес	Формування концепції «самоперевірного обліку» та «прозорої економіки»
Технічна архітектура	Смартконтракти функціонують через криптографічну верифікацію подій (підписи, хеші, часові мітки, консенсус вузлів)	Забезпечення подвійної верифікації бухгалтерських записів: технологічної та економічної
Концепція «самоперевірного обліку»	Акт фіксації операції одночасно є її перевіркою; блокчейн гарантує незмінність та цілісність записів	Блокчейн виконує функцію внутрішнього контролю; смартконтракт – його виконавчий агент
Перехід до цифрової автономії обліку	Облікова система набуває здатності самостійно аналізувати та контролювати господарські операції	Формування інтелектуального середовища бухгалтерського обліку нового покоління
Зміна ролі бухгалтера й аудитора	Від реєстратора операцій – до аналітика, дизайнера алгоритмів й інтерпретатора даних	Трансформація професії: від обробки даних до стратегічного управління інформацією

Джерело: складено авторами.

Отже, смартконтракти є не лише інструментом технічної оптимізації облікових процедур, але й фундаментом нової парадигми цифрового бухгалтерського обліку – системи, що поєднує самоконтроль, самоперевірку та алгоритмічну інтерпретацію господарських подій. Така система формує середовище повної довіри до даних, де кожна транзакція є не лише зафіксованим фактом, але й математично підтвердженою істиною, що відповідає принципам достовірності, безперервності та адаптивності бухгалтерського обліку в умовах цифрової децентралізації.

2.4. Методика облікової оцінки, визнання та верифікації фактів господарської діяльності у блокчейн-системах

Методика облікової оцінки, визнання та верифікації фактів господарської діяльності в блокчейн-системах формується на перетині традиційних принципів бухгалтерського обліку й технологічних можливостей децентралізованих реєстрів. Її сутність полягає у трансформації способів фіксації, оцінювання та підтвердження господарських операцій у цифровому середовищі, де достовірність інформації забезпечується не лише професійним судженням бухгалтера, а й алгоритмічними механізмами консенсусу. Блокчейн-технологія є своєрідним «цифровим аудитором», який гарантує незмінність записів і прозорість взаємодії між суб'єктами економічних відносин [10; 47].

У блокчейн-системах облікова оцінка господарських фактів розгортається на двох взаємопов'язаних площинах – економічній і цифровій – кожна з яких вимагає власного методологічного опрацювання та одночасно впливає на кінцевий бухгалтерський запис. Економічна оцінка залишається традиційною за своєю сутністю: вона має визначати вартісний вимір активів, зобов'язань, доходів і витрат згідно з прийнятими обліковими принципами та нормативними вимогами. Проте вона повинна враховувати специфіку цифрового середовища: вартісні показники повинні бути представлені в такій формі, щоб їх можна було однозначно зіставити з даними, зафіксованими в розподіленому реєстрі, і щоб умови їх оновлення могли бути автоматизовані або документально відстежені.

Цифрова оцінка стосується форми й змісту інформаційного об'єкта в блокчейні: це характеристика структури запису, форматів метаданих, наявності криптографічних підписів, часових штампів та посилань на зовнішні джерела даних. Вона визначає, які атрибути операції вважаються достатніми для її визнання з погляду обліку (наприклад, ідентифікаційні реквізити контрагента, сума, дата виконання, доказ постачання товарів / надання послуг) і в якій формі ці атрибути зберігаються в ланцюзі блоків. Методично важливо встановити мінімальний набір цифрових реквізитів, який гарантує розуміння економічного змісту без додаткових тлумачень; цей набір стає частиною внутрішньої облікової політики підприємства та технічного протоколу мережі.

Процес формування вартісних показників у блокчейн-реальності повинен укладатися у дві послідовні операції: внутрішньооблікова оцінка (визначення первісної і подальшої оцінки згідно з обліковими стандартами) і цифрова фіксація цієї оцінки у вигляді машинозчитуваних записів. Первісна оцінка може здійснюватися на основі собівартості, справедливої вартості або дисконтованих майбутніх грошових потоків – залежно від економічної сутності операції. Після прийняття рішення про величину оцінки вона має бути перетворена в цифровий запис так, щоб не тільки цифра була відтворювана, але й були зафіксовані методика її обчислення, вхідні припущення і джерела даних; це дозволяє наступну верифікацію й аудит в ончейн-середовищі.

Механізм визнання і підтвердження вартості в блокчейні часто реалізується через розумні контракти (смартконтракти), які автоматично виконують умовні логіки фіксації господарського факту за настання визначених умов. З методичної точки зору це означає, що облікове визнання може відбуватися не за формальною датою події, а в момент виконання програмного сценарію, що фіксує виконання економічних умов (наприклад, фактичне постачання товару, отримання платежу чи завершення послуги). Отже, момент визнання вартісного показника співпадає з моментом досягнення консенсусу в мережі щодо того, що умова була виконана, і відповідний запис пройшов процедуру підтвердження вузлами реєстру.

Сам факт того, що момент визнання прив’язаний до досягнення консенсусу, посилює об’єктивність облікового запису: консенсусні алгоритми забезпечують колективну перевірку валідності події й унеможливлюють односторонню зміну вже зафіксованих даних [34; 85]. Методично це накладає на бухгалтерію обов’язок інтегрувати правила консенсусу в політику визнання – тобто визначити, які типи консенсусних повідомлень або криптографічних доказів є достатніми для визнання операції, а які потребують додаткового зовнішнього підтвердження. Така політика повинна враховувати різні варіанти технічних реалізацій мережі, можливість розгалужень реєстру (форків) і процедури вирішення розбіжностей.

Важливий практичний елемент методики – питання щодо джерел зовнішніх даних, на які опираються смартконтракти під час встановлення економічних умов. Оракли (зовнішні постачальники даних) перетворюють інформацію з реального світу у формат, зрозумілий

для блокчейну; отже, методично потрібно оцінювати надійність цих джерел, встановлювати механізми верифікації отриманих даних і враховувати ризик їхньої неточності під час формування облікових оцінок. Політика обліку має регламентувати алгоритми агрегування даних від кількох ораклів, часові межі прийнятності даних та процедури корегування вже зафіксованих значень у разі виявлення помилок.

З огляду на незмінність записів у ланцюзі блоків, виникає питання щодо можливості та методів корегування помилкових чи неточних облікових записів. Методика повинна передбачати концепції «коректуючих записів» та «виправних транзакцій», які створюються як нові записи, що явно посилаються на первісний запис і містять економічне обґрунтування зміни; такий підхід зберігає аудиторський слід і відповідає принципу прозорості. Водночас потрібно визначити порядок відображення впливу таких корегувань на звітні періоди, враховуючи часову невідкладність їхньої цифрової публікації та вимоги стандартів фінансової звітності.

Стосовно верифікації, блокчейн надає набір нових доказових елементів: криптографічні геші, підписи, часові штампи, структури дерев Меркла й інші математично обґрунтовані свідчення цілісності та послідовності записів. Методично аудит і внутрішня перевірка повинні адаптуватися до цих інструментів: аудитори повинні мати процедури верифікації криптографічних доказів, зіставлення цифрових записів з економічними підставами операцій і перевірки цілісності ключів та конфігурацій мережі. Важливо також визначити пріоритети доказової бази – коли ончейн-докази є достатніми, а коли потрібно додаткове офчейн-підтвердження (наприклад, фізичні акти приймання-передачі, контракти у традиційному вигляді).

Нарешті, методика має врахувати регуляторні та етичні аспекти: повноваження осіб, відповідальних за виставлення цифрових оцінок; правила збереження конфіденційності й захисту персональних даних; вимоги щодо зберігання оригіналів документообігу. У внутрішніх процедурах обліку потрібно закріпити, хто несе відповідальність за підготовку вхідних даних для смартконтрактів, хто контролює їх публікацію в мережі і які процедури застосовуються у випадку технічних збоїв або суперечностей даних. Такий комплексний підхід дає змогу зберегти економічну змістовність оцінок, одночасно використовуючи переваги цифрової достовірності, і забезпечує відтворюваність, підзвітність та захищеність облікових записів у середовищі цифрової децентралізації.

Процес верифікації у блокчейн-орієнтованих системах є не просто технічним механізмом, а фундаментальною процедурою формування доказової бази обліку, яка замінює і доповнює традиційні форми підтвердження первинних документів. У центрі цього процесу стоїть криптографічний геш – компактне числове подання вмісту кожного запису, яке одночасно фіксує його унікальність і встановлює криптографічний зв'язок із попередніми записами. Наявність гешу дає змогу в наступні моменти часу перевірити: чи не змінювалася операція після запису; чи належить вона саме тій послідовності подій, у якій була зафіксована; та чи вписується її відбиток у загальну структуру записів реєстру. Така властивість покладає основу для нефальсифікованого аудиторського сліду, що має математичну обґрунтованість замість виключно процедурного підтвердження.

Методично важливо розрізняти рівні верифікації: технічний, смисловий та юридичний. Технічна верифікація охоплює криптографічну перевірку гешів, підписів і структури реєстру (включно з перевіркою корінних значень у деревах цілісності), а також перевірку коректності виконання алгоритмів консенсусу. Смислова верифікація передбачає зіставлення ончейн-запису з економічною реальністю операції – наприклад, чи відповідає зафіксована кількість і якість товарів фактичному постачанню, чи відбувся розрахунок у договореному обсязі. Юридична верифікація визначає, чи має ончейн-доказ правову силу в конкретній юрисдикції і які додаткові документи потрібні для задоволення регулятивних вимог. Методика повинна чітко прописати процедури для кожного рівня та критерії адекватності доказів.

Децентралізована перевірка запису всіма або більшістю вузлів мережі є ключовим елементом: вона перетворює суб'єктивне судження окремої сторони на колективне підтвердження, сформоване згідно з заданими правилами консенсусу. З методологічної точки зору це вимагає визначення, які саме повідомлення від вузлів і в якій кількості вважаються достатніми для визнання запису як валідного. У системах з відкритим доступом (безперешкодний доступ вузлів) критерієм зазвичай є досягнення визначеної частки голосів або довжини ланцюга, у приватних або консорціумних мережах – наявність підписів певного переліку верифікованих учасників. Облікова політика організації має охоплювати ці технічні критерії як складову правил визнання факту господарської діяльності.

Наявність додаткових криптографічних конструкцій посилює силу верифікації. Використання структур, які дають змогу підпорядкувати велику кількість записів до єдиного контрольного значення (наприклад, деревах цілісності), прискорює процедури вибіркової перевірки та зменшує обсяг даних, необхідних для доведення цілісності великого масиву записів. Біометричні або апаратні засоби для зберігання ключів та цифрових підписів створюють додатковий рівень довіри до того, що підпис реально належить уповноваженій особі, а не зловмиснику. Методика верифікації має передбачати стандарти зберігання, ротації та анулювання ключів, а також впроцедури реагування в разі їх компрометації.

Практичний процес верифікації повинен також охоплювати процедури зіставлення ончейн-доказів із офчейн-документами і розподіляти відповідальність між підрозділами. Наприклад, операційний персонал може бути відповідальним за надання первинних даних і їх завантаження в мережу, внутрішній контроль – за перевірку коректності метаданих і відповідності політикам, а служба аудиту – за незалежну перевірку криптографічних доказів та економічного обґрунтування. Таке розподілення обов'язків забезпечує систему стримувань і противаг та відповідає базовим принципам внутрішнього контролю.

Питання джерел даних є критичним для забезпечення достовірності верифікації: якщо смартлогіка покладається на зовнішні сигнали, то потрібно оцінювати довіру до цих джерел, механізми їхнього підключення та способи агрегування інформації. Методика має регламентувати використання декількох незалежних постачальників даних, часові вікна прийнятності показників, критерії відхилення аномальних значень і процедури відкату у разі встановлення помилкових вхідних даних. Такі правила зменшують ризик «перенесення» помилок з реального світу в незмінну ончейн-історію.

У випадку виявлення помилкового або шахрайського запису методика верифікації повинна передбачати прозору процедуру виправлення, що зберігає цілісність аудиту. Оскільки базова властивість реєстру – незмінність вже записаних блоків – безпосередня модифікація первісного запису неможлива; натомість застосовуються механізми рефлективних записів, які створюють нові операції з посиланням на початкові, пояснюють причини корекції і документують її економічний ефект. Облікова політика має визначати, як такі корекції відображаються у звітних періодах і які підтвердження потрібні для їхнього прийняття.

Аудитори та контролери повинні володіти спеціальними методами перевірки цифрових доказів: процедурою перевірки відповідності гешів, підтвердженням цілісності ключів, аналізом журналів вузлів і реєстраційних даних про консенсусні події. Методично доцільно розробити перелік стандартних процедур перевірки, що охоплює вибіркову перевірку ончейн-записів, зіставлення їх із офчейн-джерелами, аналіз логіки виконання смартскриптів і тестування механізмів ораклів. Такий набір процедур дає змогу переконатися, що цифрові докази не лише технічно коректні, а й мають належну економічну основу.

Нарешті, методика верифікації повинна бути інтегрована в систему корпоративного управління та юридичної взаємодії з регуляторами: потрібно визначити, які ончейн-докази визнаються для податкових, цивільних та адміністративних процедур, які процедури нотаріального або інституційного визнання потрібні, та як зберігаються офіційні копії первинної інформації. Це забезпечує, що верифікація у блокчейні не залишиться лише технічним актом, а набуде практичної сили як частина доказової та звітної дисципліни суб'єкта господарювання.

Інтеграція процедур блокчейн-фіксації в облікову практику радикально змінює логіку документування господарських фактів: традиційний паперовий або електронний первинний документ як автономний доказ трансформується в єдину машинозчитувану одиницю – смартзапис, що поєднує в собі економічний зміст операції й формальні метадані, потрібні для її автоматичної обробки та верифікації. Смартзапис містить повний набір реквізитів операції – ідентифікатори сторін, умови договору, кількісні та вартісні показники, часові мітки, посилання на зовнішні джерела даних та відомості про методику оцінки – а також криптографічний підпис уповноваженої особи і контрольні значення, що забезпечують цілісність та автентичність інформації. Така структура дає змогу не лише зафіксувати факт, а й унеможливити його непомітну зміну, оскільки будь-яка модифікація змінює контрольні значення і робить спробу підміни відразу очевидною.

Автоматизована перевірка умов здійснення операції, закодована у смартлогіці, переводить значну частину процедур контролю в режим машинної валідації: виконання передбачених договором подій (поставка товару, оплата, надання послуги) підтверджується за рахунок

подачі вхідних даних у визначеному форматі й автоматичного запуску верифікаційних алгоритмів, після чого відповідний запис отримує статус визнаного і розповсюджується в облікових реєстрах. Це означає, що ідентифікація господарського факту відбувається миттєво від моменту досягнення умов, а бухгалтерський запис формується в режимі, близькому до реального часу; у подальшому такий запис стає компонентом цифрового аудиторського сліду, послідовність і цілісність якого підтверджуються математичними доказами, а не лише процедурними актами перевірки.

Перехід до смартзаписів вимагає від підприємства розробки єдиної схеми даних і метаданих, яка гарантує однозначність тлумачення економічного змісту незалежно від технічної платформи. Методика має визначати структуру реквізитів, формати кодування, правила часових міток, механізми посилання на зовнішні джерела та стандарти документування методики оцінки (включно з вихідними припущеннями і використовуваними алгоритмами). Така приведена до стандарту семантика дає змогу забезпечити інтероперабельність між корпоративними інформаційними системами, мережевими реєстрами партнерів та засобами аудиту, а також спрощує автоматизовану консолідацію даних для внутрішньої та зовнішньої звітності.

З погляду внутрішнього контролю формування смартзаписів диктує перегляд функцій розподілу повноважень і процедур доступу: хто готує вхідні дані для смартлогіки, хто уповноважений підписувати їх криптографічно, як відбувається ротація ключів та реагування на компрометацію підписів. Потрібно закріпити письмові процедури для виняткових випадків, коли автоматичне виконання неможливе або дані потребують додаткового підтвердження – наприклад, через суперечності офчейн-документів або сумнівну якість сигналів ораклів. Важливо, щоб механізми виправлення помилкових записів були прозорими: оскільки пряме видалення запису неможливе, корекції фіксуються як нові смартзаписи з посиланням на первісний і з явним поясненням підстав та впливу на звітні показники.

Ефект від переходу до режиму реального часу не зводиться лише до пришвидшення облікових операцій; він створює нові можливості для управлінського контролю та прийняття рішень, оскільки керівництво отримує оперативні, верифіковані дані про стан розрахунків,

запаси, зобов'язання та доходи. Водночас це підвищує вимоги до якості вхідних даних і до організації процесів їхньої генерації: помилка, допущена на початковому етапі, швидко поширюється по облікових реєстрах та вимагає відпрацьованих процедур виявлення і корекції. Тому впровадження смартзаписів має супроводжуватися навчанням персоналу, аудитом бізнес-процесів і тестуванням систем у реальних сценаріях.

Юридичні та регуляторні аспекти також набувають особливої ваги: для забезпечення визнання смартзаписів як первинних документів потрібно, щоб внутрішні процедури і застосовані криптографічні методи відповідали вимогам чинного законодавства щодо електронних документів, збереження архівів і захисту персональних даних. Це передбачає встановлення правил архівації офчейн-копій, процедур нотаріального або інституційного визнання ключових подій, а також механізмів співпраці з податковими та судовими органами в разі суперечок. Без належного правового оформлення переваги технології можуть залишатися технічно привабливими, але практично обмеженими.

Трансформація системи документування в бік смартзаписів означає перехід від постфактумного підтвердження до оновленої парадигми обліку, де визнання факту, його фіксація та первинна верифікація відбуваються в єдиному автоматизованому циклі. Це створює підґрунтя для підвищення оперативності управління, зміцнення доказової бази і зниження ризиків маніпуляцій, але одночасно висуває підвищені вимоги до стандартів даних, внутрішнього контролю, правового оформлення та професійної компетентності учасників облікового процесу.

Узагальнюючи викладений вище матеріал, структуруємо його у вигляді характеристики методики облікової оцінки, визнання та верифікації фактів господарської діяльності у блокчейн-системах (табл. 2.6).

Таблиця 2.6 – Характеристика методики облікової оцінки, визнання та верифікації фактів господарської діяльності у блокчейн-системах

Методологічний аспект	Змістовна характеристика	Наслідки для бухгалтерського обліку в умовах цифрової децентралізації
1	2	3
Концептуальна основа методики	Формується на стику традиційних принципів обліку (достовірність, об'єктивність, документальність) та технологічних можливостей децентралізованих реєстрів. Блокчейн є «цифровим аудитором», що гарантує незмінність записів	Підвищення достовірності, усунення маніпуляцій, заміна процедурного підтвердження математичною перевіркою
Двоєдиність оцінки	Оцінка має економічний (вартісний вимір активів, зобов'язань, доходів, витрат) та цифровий (структура даних, криптографічні атрибути, формат метаданих) виміри	Необхідність інтеграції економічного змісту з цифровими атрибутами для забезпечення автоматизованого відображення операцій
Економічна оцінка	Визначається за традиційними принципами (собівартість, справедлива вартість, дисконтовані потоки), але в цифровій формі, придатній до автоматизованої фіксації	Формування цифрової вартості як машинозчитуваного об'єкта; документування методики розрахунку
Цифрова оцінка	Визначає, які реквізити операції (ідентифікатор, сума, дата, підпис, джерело) є мінімально достатніми для її облікового визнання	Встановлення стандартизованого набору цифрових реквізитів у складі облікової політики підприємства
Визнання фактів через смартконтракти	Визнання операції здійснюється у момент виконання програмної логіки (фактична подія), що збігається з досягненням консенсусу вузлів	Об'єктивізація моменту визнання; усунення суб'єктивного людського судження
Консенсус як критерій достовірності	Колективна перевірка вузлів підтверджує валідність операції; алгоритми консенсусу стають частиною облікової політики	Формування принципу колективного підтвердження облікових фактів

Продовження таблиці 2.6

1	2	3
Корегування помилкових записів	Пряме редагування записів неможливе; застосовуються коректуючі смартзаписи, що посилаються на первісний факт	Збереження аудиторського сліду; забезпечення прозорості виправлень
Нові докази достовірності	Криптографічні геші, підписи, часові мітки, дерева Меркла; вони замінюють традиційні первинні документи як доказ цілісності	Формування цифрової доказової бази бухгалтерського обліку
Колективна перевірка записів	Визнання запису здійснюється в разі досягнення консенсусу більшістю вузлів (у публічних чи приватних мережах)	Усунення одноосібного контролю; підвищення довіри до системи обліку
Криптографічні структури контролю	Використання дерев Меркла, хеш-ланцюгів, апаратних ключів для підтвердження автентичності	Математичне гарантування незмінності й послідовності облікових фактів
Організація процесу верифікації	Визначення ролей: операційний персонал – введення даних; контроль – перевірка метаданих; аудит – перевірка гешів і консенсусу	Розподіл відповідальності, відповідність принципам внутрішнього контролю
Надійність джерел даних	Використання кількох незалежних постачальників, часові вікна прийнятності, процедури відкату в разі помилок	Зниження ризику системних викривлень, формування стійкої системи облікової довіри
Аудиторські процедури в ончейн-середовищі	Перевірка відповідності гешів, цілісності ключів, аналіз журналів вузлів, тестування логіки смартконтрактів	Формування нової галузі – блокчейн-аудиту з цифровими методами перевірки
Правова та регуляторна інтеграція	Визначення статусу ончейн-доказів у податкових, цивільних і судових процесах; збереження офіційних копій	Легітимація цифрових записів як первинних документів
Смартзапис як нова форма документа	Машинозчитувана одиниця, що містить економічний зміст і метадані: сума, дата, підпис, посилання на джерела, методику оцінки	Заміна первинного документа цифровим записом; формування безпаперової моделі обліку

Продовження таблиці 2.6

1	2	3
Автоматизована верифікація умов операцій	Смартлогіка перевіряє виконання договору й автоматично визнає операцію в момент настання події	Перехід до обліку в режимі реального часу; усунення часових лагів
Стандартизація структури смартзапису	Єдина схема реквізитів, метаданих, форматів часових міток, алгоритмів оцінки	Забезпечення інтероперабельності систем і автоматизованої консолідації звітності
Внутрішній контроль і розподіл повноважень	Визначення ролей щодо підготовки, підписання, публікації та виправлення даних; правила ротації ключів	Підвищення інформаційної безпеки та відповідальності учасників облікового процесу
Навчання та тестування систем	Вимагається підготовка персоналу, аудит бізнес-процесів, перевірка систем у реальних сценаріях	Гарантоване функціонування блокчейн-обліку в умовах практичного застосування
Юридичне визнання смартзаписів	Необхідна відповідність електронному документообігу, архівації, захисту даних та нотаріальному визнанню	Набуття смартзаписами правового статусу первинних документів
Нова парадигма документування	Визнання, фіксація та первинна верифікація відбуваються в єдиному автоматизованому циклі	Перехід до самоверифікованого обліку – системи, де доказовість вбудована у сам процес фіксації фактів

Джерело: складено авторами.

Отже, методика облікової оцінки, визнання та верифікації фактів господарської діяльності у блокчейн-середовищі формує нову парадигму достовірності облікової інформації. Її основна цінність полягає в забезпеченні синергетичного поєднання професійного судження бухгалтера з алгоритмічною довірою технологічних систем. Такий підхід створює передумови для побудови глобальної інфраструктури бухгалтерського обліку, у якій прозорість, незмінність та автоматизація процесів стають фундаментальними характеристиками економічної інформації в епоху цифрової децентралізації.

2.5. Стандартизація та уніфікація облікових процедур у контексті використання децентралізованих технологій

Стандартизація та уніфікація облікових процедур у контексті використання децентралізованих технологій є необхідною умовою формування узгодженого, відтворюваного та порівнянного інформаційного простору бухгалтерського обліку [15; 59]. У децентралізованому середовищі, де облікові дані формуються, зберігаються та підтверджуються без єдиного центру контролю, питання стандартизації набуває не лише методологічного, а й технічного змісту. Йдеться про створення єдиних правил формування цифрових записів, структурування облікових даних, їхнього кодування та верифікації, що забезпечує сумісність між різними обліковими системами, корпоративними мережами та регуляторними платформами. Саме узгодженість форматів і процедур стає тим механізмом, що дає змогу блокчейн-технології інтегруватися в глобальну систему фінансової звітності без втрати достовірності й правової сили [26; 67].

У традиційній системі обліку стандартизація спирається на єдині методичні принципи, стандарти фінансової звітності та формальні вимоги до первинних документів; у децентралізованому середовищі ці правила потребують цифрового втілення у вигляді уніфікованих схем даних, які визначають не лише зміст окремого реквізиту, а й його роль у загальній семантиці операції. Схема даних повинна задавати структуру запису – набір полів, їхній тип, допустимі значення, порядок заповнення та зв’язки між полями – так, щоб будь-яка система, що підтримує цю схему, могла без додаткового тлумачення прочитати, інтерпретувати та обробити запис. Уніфікація на такому рівні усуває неоднозначності в тлумаченні понять і створює передумови для автоматичної перевірки й обробки інформації.

Практичне наповнення схем має містити стандартизовані елементи: уніфіковані ідентифікатори контрагентів, коди видів операцій і номенклатури, валютні та кількісні формати, часові відмітки з погодженими часовими зонами, посилання на застосовані методики оцінки та джерела даних. Важливим компонентом є метадані – інформація про походження запису, авторство, рівень довіри, версію схеми та параметри валідації. Саме метадані дають змогу не лише встановити економічний зміст операції, а й автоматично провести первинні

процедури контролю: перевірку повноти, відповідності типів даних, відповідності контролям цілого процесу й віднесення до відповідного рахунку чи класифікації.

З технічного погляду уніфікація передбачає погодження на рівні синтаксису та семантики. Синтаксичний рівень визначає формати обміну повідомлень, протоколи підключення й базові механізми перевірки цілісності; семантичний рівень задає правила інтерпретації полів і бізнес-логіки. Методично доцільно застосовувати багаторівневий підхід: базову, обов'язкову схему для найважливіших реквізитів; розширювальні модулі для галузевих або функціональних особливостей; словники термінів і правила мапінгу до національних і міжнародних облікових стандартів. Такий підхід забезпечує одночасно необхідний рівень уніфікації й гнучкість для специфічних випадків.

Уніфікація дає можливість автоматичної генерації фінансової звітності без ручних перетворень: стандартизовані записи підлягають безпосередній трансформації в звітні форми завдяки визначеним правилам агрегування й віднесення до статей звітності. Це зменшує трудовитрати на консолідацію, знижує ризики помилкового перекладу даних і пришвидшує закриття звітних періодів. Водночас для досягнення таких результатів потрібні погоджені правила консолідації, стандартизовані довідники рахунків і алгоритми трансформації, які гарантують тотожність економічного змісту після перетворень.

Необхідною складовою є система управління схемами: реєстр затверджених схем, механізми версіонування, правила зворотної сумісності та процедури тестування і сертифікації рішень. Без чіткої політики зміни схем виникає ризик семантичного розходження між учасниками мережі; тому зміни мають проходити формалізовану процедуру погодження з етапами пілотування та обов'язковим періодом переходу. Крім того, має бути визначена відповідальність за підтримку та оновлення словників, контроль якості даних і механізми вирішення суперечностей у тлумаченні реквізитів.

Не менш важливими є питання захисту конфіденційності та селективного розкриття інформації: уніфіковані формати повинні містити механізми позначення рівнів доступу, псевдонімізації чутливих полів і процедур запиту додаткових офчейн-доказів. Це дає змогу поєднати прозорість мережевого реєстру з вимогами захисту персональних і комерційно чутливих даних, зберігаючи можливість верифікації за допомогою криптографічних доказів без публікації всіх деталей операції.

Важливо також створити інститут взаємного визнання: регуляторні акти, професійні організації та галузеві об'єднання мають погодити базові правила та визнати відповідні цифрові формати як прийнятні для звітності та контролю. Така зовнішня легітимація зменшує бар'єри впровадження і підвищує довіру до даних, що циркулюють у децентралізованому середовищі. Лише поєднання технічної уніфікації, методичного узгодження та інституційної підтримки створює стійку основу для повсюдного використання блокчейн-технологій у системі бухгалтерського обліку.

Гармонізація облікових норм і технічних протоколів є центральним елементом створення єдиних стандартів обліку в умовах використання децентралізованих технологій. Це вимагає не простого перенесення традиційних правил у цифрову площину, а їхнього формалізованого відтворення у вигляді алгоритмічних правил, що реалізуються в коді розумних контрактів та протоколах реєстру. Інакше кажучи, кожне бухгалтерське правило – критерій визнання, метод оцінювання, класифікація об'єкта обліку, порядок визначення моменту виникнення доходу чи витрат – має бути перекладене у формалізований набір умов і процедур, які можуть бути однозначно виконані та перевірені мережею. Такий переклад неможливий без тісної кооперації між фахівцями з обліку, розробниками програмного забезпечення та правознавцями [14; 36].

Практично це означає, що смартконтракти повинні містити логіку, що відтворює критерії визнання згідно зі стандартами фінансової звітності: наприклад, для визнання доходу – настання події, передбаченої договором, передача контролю над товаром або послугою, надійне визначення суми та очікування економічної вигоди. Код має містити перевірки вхідних даних, часові рамки і механізми фіксації доказів їх виконання, а також можливість збереження інформації про застосовані методики оцінювання та припущення. Таке програмне відтворення зменшує простір для суб'єктивних інтерпретацій, але не усуває потреби професійного судження: складні випадки, що вимагають дискреційних рішень, повинні мати визначені процедури винятків, які переводять обробку в офчейн-режим або передбачають участь уповноважених осіб.

Особлива увага має бути приділена процедурі встановлення моменту визнання у блокчейн-системах. Момент визнання доходу чи

активу має бути узгоджений із моментом технічного підтвердження виконання зобов'язань у мережі – досягненням консенсусу про настання певної події. Однак для збереження відповідності обліковим правилам потрібно встановити, які саме блокчейн-події й які криптографічні докази вважаються еквівалентними настанню економічної події: одиночне повідомлення від зовнішнього джерела, набір узгоджених повідомлень від кількох незалежних джерел, чи підтвердження від визначеної групи довірених вузлів. Такі рішення повинні бути формалізовані в політиках визнання й відображені у структурі смарт-контрактів.

Гармонізація також охоплює питання оцінки й класифікації: методики розрахунку первісної і наступної оцінки активів повинні бути імплементовані як частина цифрових процедур, з чіткою фіксацією вихідних даних, моделей і параметрів. Наприклад, для активів, що оцінюються за справедливою вартістю, смартлогіка має забезпечувати прийом ринкових котирувань або агрегованих даних від зовнішніх постачальників, фіксацію часу отримання даних і механізми вирішення ситуацій нестабільності або відсутності ринкових даних. Водночас потрібно передбачити політики щодо вибору джерел, перевірки їх достовірності й застосування процедур агрегування та фільтрації.

Міждисциплінарний підхід має також охоплювати правові аспекти: код смартконтракту та формати цифрових записів повинні відповідати вимогам законодавства про електронні документи, доказове право та регулятивні вимоги щодо звітності. Це вимагає визначення юридично значущих елементів запису (автентифікація підпису, часові мітки, сертифікація вузлів) і процедур їхнього надання у вигляді доказів у разі спорів. Відсутність юридичної узгодженості може призвести до ситуації, коли технічно верифікований ончейн-запис не матиме ефективної правової сили, що підриває саму мету стандартизації.

Розроблення стандартів потребує формалізованих процедур тестування, валідації та сертифікації систем: перед впровадженням важливо проводити симуляції, аудити коду смартконтрактів, тестування на кейсах специфічних бізнес-сценаріїв та підтверджувати відповідність реалізації обліковим правилам. Такі процедури повинні бути частиною процесу управління версіями стандартів – зміни в методології обліку або оновлення протоколів мають супроводжуватися процесом погодження, переходу та зворотної сумісності, аби уникнути семантичних розходжень між учасниками.

Нарешті, стандартизація вимагає інституційної підтримки: національні органи, професійні об'єднання та міжнародні організації мають брати участь у розробленні й визнанні цифрових стандартів, забезпечуючи їхню легітимність та практичну реалізацію [14]. Таке поєднання бухгалтерської методології, інформаційних технологій і правового регулювання створює інтегровану основу, яка дає змогу гарантувати одночасно методологічну коректність обліку, технічну верифікованість і правову допустимість цифрових записів у децентралізованому середовищі.

У контексті інтеграції блокчейн-технологій у систему бухгалтерського обліку особливого значення набуває уніфікація термінології та семантичних структур. Різниця у тлумаченні таких базових понять, як «транзакція», «подія», «факт господарської діяльності», «цифровий актив» або «смартзапис», створює ризик неоднозначного відображення економічних операцій, що в кінцевому підсумку призводить до розбіжностей у формуванні облікових результатів та фінансової звітності. Тому першочерговим завданням є розроблення й прийняття єдиних словників даних і семантичних правил, які б однозначно визначали зміст кожного реквізиту, структуру відношень між об'єктами та правила їхнього облікового представлення. Такі словники мають охоплювати не лише назви полів, але й допустимі формати значень, одиниці виміру, можливі значення переліків, правила агрегації й інтерпретації – тобто всі ті атрибути, які забезпечують семантичну стабільність даних в процесі їхньої передачі та обробки.

Створення словників даних має ґрунтуватися на міждисциплінарному підході: у їхню розробку повинні бути залучені фахівці з бухгалтерського обліку, аудиту, інформаційних технологій, представники регуляторних органів та бізнес-асоціацій. Практично це означає визначення канонічних трактувань понять, деталізацію реквізитів для кожного типу облікового елемента та побудову моделі зв'язків між ними. Наприклад, у випадку «транзакції» має бути зафіксовано, чи вона охоплює лише переміщення прав власності, чи також охоплює пов'язані зобов'язання; для «події» – критерії фіксації моменту виникнення й вимоги щодо доказової бази; для «цифрового активу» – набір атрибутів, що дають змогу відрізнити права власності, права користування та технічні маркери (ідентифікатори, версії, посилання на метадані). Така деталізація дає змогу уникнути «перекладу» понять між локальними інформаційними системами, звести до мінімуму людський чинник і забезпечити відтворюваність облікових операцій.

Реалізація словників даних на рівні протоколів блокчейн-мереж є технологічно ефективним і концептуально оправданим кроком. Інтегрування семантичних правил безпосередньо в протокол означає, що кожна операція в мережі здійснюється з формальним описом реквізитів, їхнього типу та валідаційних правил, що виконуються до моменту запису в розподіленому реєстрі. Це дає змогу досягти двох важливих цілей: по-перше, забезпечити «білінгвізм» даних – однакове розуміння інформації усіма учасниками мережі; по-друге, забезпечити автоматичну перевірку відповідності записів встановленим обліковим правилам ще на етапі реєстрації, що підвищує надійність і зменшує потребу в ручній постфактум перевірці.

У міжорганізаційному вимірі уніфіковані словники даних є засобом міжсистемної інтероперабельності. Коли партнери, контролювальні органи та аудиторські структури використовують загальний набір семантичних правил, обмін інформацією не вимагає дорогих трансформацій чи узгоджувань «вручну». Це особливо важливо для накладання податкових, статистичних або регуляторних вимог, де відмінності в трактуванні реквізитів можуть призвести до суперечок і штрафів. Уніфікація спрощує також автоматизовану звірку: алгоритми порівнюють не просто числові значення, а повні семантичні профілі записів, що дає змогу виявляти не лише розбіжності в сумах, а й невідповідності в сутності операцій.

Архітектурно важливо, щоб словники даних передбачали механізми версіонування, управління змінами та зворотної сумісності. Бізнес-процеси, законодавчі вимоги та технічні стандарти еволюціонують, тому словник має підтримувати контроль версій, чіткі процедури схвалення змін і можливість одночасного існування кількох версій з визначенням правил трансформації старих записів у нові формати. Також потрібні механізми підписання та сертифікації версій словників, щоб учасники мережі могли довіряти джерелу семантичних правил. У поєднанні з розподіленими правами доступу це створює керований процес еволюції облікових стандартів у децентралізованому середовищі.

З позиції аудиту та контролю важливо, щоб уніфіковані словники інтегрувалися з правилами доказовості й трасування походження даних. Кожен смартзапис у реєстрі має містити достатню метаінформацію про джерело, час фіксації, контекст події та застосовані валідації, щоб зовнішній аудитор міг відтворити інформаційну хронологію і

підтвердити відповідність обліку нормативним вимогам. Це також спрощує застосування алгоритмічних процедур контролю відповідності й ризик-орієнтованого аудиту, оскільки аудитор може оперувати не лише агрегованими звітами, а й первинними семантично верифікованими записами.

Не менш важливо уніфікувати й ідентифікаційні підходи: реквізити, що ідентифікують контрагентів, активи, договори та операції, повинні мати єдині формати й стандартизовані коди. Відсутність уніфікованих ідентифікаторів ускладнює кореляцію даних між реєстрами і підвищує ймовірність дублювання та помилкових зіставлень. Впровадження глобально впізнаваних ідентифікаторів або перекладних кодувальних схем у межах словників створює передумови для ефективної автоматичної звірки, консолідації даних та застосування аналітики в режимі реального часу.

Нарешті, у процесі стандартизації потрібно враховувати питання інформаційної безпеки та захисту персональних даних. Семантичні правила мають містити класифікацію чутливості реквізитів, вимоги до шифрування, права доступу та умови розкриття інформації третім особам. У поєднанні з протоколами контролю доступу в мережі це створить баланс між прозорістю обліку та дотриманням конфіденційності, що особливо важливо під час передавання даних між суб'єктами господарювання та державними органами. Узагальнено, уніфікація термінології та семантичних структур, реалізована через формалізовані словники даних на рівні блокчейн-протоколів, є базовою передумовою достовірного, інтероперабельного й підзвітного бухгалтерського обліку в умовах цифрової децентралізації.

Технологічна уніфікація в контексті бухгалтерського обліку на основі децентралізованих технологій має на меті забезпечити однорідні формати облікових повідомлень і чітко визначені протоколи взаємодії між усіма учасниками облікового процесу – від суб'єктів господарювання до податкових органів і аудиторів. Така уніфікація охоплює формалізацію структури повідомлення (набір реквізитів, порядок їхнього розташування, типи даних та обов'язковість заповнення), правила серіалізації для передачі між системами, а також контрактні інтерфейси прикладного рівня, що гарантують сумісність реалізацій на різних технологічних платформах. Єдиний формат повідомлення створює технічну передумову для однозначного машинного опрацювання первинних записів без необхідності ручних трансформацій або інтерпретацій.

Ключовим елементом таких протоколів є правила формування ідентифікаторів записів. Ідентифікатор має бути унікальним у глобальному або визначеному домені, незмінним у часі та детермінованим від змісту запису й контексту його створення. Практично це означає застосування канонічних процедур побудови, які можуть охоплювати хешування змісту запису з додаванням контекстних метаданих (ідентифікаторів суб'єкта, номера договору, версії словника даних). Детерміновані ідентифікатори дають змогу однозначно зіставляти записи, виявляти дублікати та трасувати походження інформації в розподіленому середовищі.

Часова мітка в обліковому записі є не лише технічною ознакою, а й елементом юридичної доказовості. Протоколи мають регламентувати формат часових міток, джерела часу та процедури їхнього верифікування. Оскільки локальний час вузлів може відрізнятися, необхідне використання довірених зовнішніх джерел часу або механізмів узгодження часу в мережі. У критичних випадках потрібно передбачати вбудовані процедури перевірки консистентності часових міток і маркування записів, у яких виявлено значні розбіжності, щоб забезпечити коректну хронологію подій у ланцюзі облікових фактів.

Цифровий підпис є основою цілісності й автентичності облікових записів. Протоколи повинні визначати криптографічні алгоритми, формати підписів, процедури перевірки та механізми управління ключами, включно з обробкою зміни ключів, відкликанням і відновленням доступу. Для бізнес-процесів, що долучають кількох співвиконавців, потрібно стандартизувати підходи до колективного підпису – наприклад, багатосигнатурні схеми або порогові підписи – і встановити правила інтерпретації таких підписів у бухгалтерському контексті. Важливим є також визначення метаданих підпису: ідентифікатор підписувача, роль у процесі, часові мітки підпису та посилання на діючі версії політик довіри.

Механізми досягнення згоди в мережі – механізм узгодження стану – мають бути інтегровані в протоколи як обов'язкова складова, оскільки від них залежить порядок і допустимість фіксації облікових подій. Протоколи повинні містити чіткі правила щодо того, які записи вважаються остаточними, які можуть бути тимчасовими, а які підлягають додатковій валідації. Визначення цих правил має враховувати властивості обраного механізму узгодження – наприклад, час до остаточності, ризик розгалужень, поведінку під тиском – і встановлювати

процеси для обробки аномалій, таких як розбіжності блоків або відхилені транзакції.

Процедури внесення корегувань потребують особливої формалізації: у децентралізованому недеформованому реєстрі неможливо просто «видалити» запис, тому стандарти повинні встановлювати модель корегувальних записів, взаємозв'язок між первинним і корегувальним записом та правила для відображення таких змін у зведених звітах. Це може реалізуватися через створення корегувальних операцій, які посилаються на ідентифікатор первісного запису, містять мотив корекції, авторизацію відповідних ролей і часові мітки. Потрібно також врегулювати правило видимості: як і в яких звітах і для яких категорій користувачів відображаються історичні й корегувальні записи, аби зберегти прозорість та одночасно відповідність законодавчим вимогам.

У технічному плані важливо забезпечити детермінованість серіалізації та канонічну нормалізацію даних перед їхнім підписуванням і хешуванням. Навіть мінімальні відмінності у форматуванні або порядку полів призводять до різних хешів і, як наслідок, до невідповідності ідентифікаторів. Тому протоколи повинні описувати канонічні схеми серіалізації, охоплюючи правила нормалізації тексту, кодування символів, представлення числових значень та оброблення відсутніх полів. Така технологічна дисципліна забезпечує відтворюваність і правову доказовість записів незалежно від платформи-реалізатора.

Потрібно передбачити механізми для міжмережевої взаємодії та масштабування: формати повідомлень і протоколи мають підтримувати анкерування записів у зовнішніх мережах, поділ на сегменти або шардінг, а також стандартизовані інтерфейси для бічних ланцюгів і шлюзів. Це дасть змогу зберігати безперервність ланцюга облікових фактів навіть за умов географічного розподілу даних, різних політик зберігання або вимог до продуктивності. Водночас потрібно детально визначити процедури верифікації й цілісності в процесі передавання даних між мережами, аби уникнути втрат або підміни інформації під час інтеграції.

Нарешті, технологічна уніфікація не може існувати поза рамками управління – специфікація протоколів повинна супроводжуватися механізмами стандартизації, тестування та сертифікації реалізацій. Це охоплює набори тестових векторів, формальні верифікації критичних

компонентів (наприклад, реалізацій підписів і процедур серіалізації), процедури оновлення протоколів і сумісності між версіями. Така організаційна складова гарантує, що технічні стандарти будуть інтерпретовані однозначно і що впровадження в різних системах призведе до сумісних та юридично значущих облікових результатів.

Технологічна уніфікація форматів і протоколів формує єдину логіку документування господарських подій у блокчейн-середовищі: кожен елемент облікових даних отримує визначений і перевірюваний зв'язок з попереднім і наступним, що робить ланцюг облікових фактів безперервним, верифікованим у часі та придатним для автоматизованого контролю, аналізу й аудиту. Такий підхід закладає технічні та організаційні засади для довірчого, прозорого й ефективного ведення обліку в умовах цифрової децентралізації.

Управлінський аспект стандартизації у сфері бухгалтерського обліку в умовах цифрової децентралізації вимагає формування багаторівневої системи регламентів, що поєднує обов'язкові норми та рекомендаційні вказівки. Така система повинна забезпечувати однозначне тлумачення економічних операцій, правила їхнього документування в розподіленому реєстрі та процедури контролю й верифікації, а також створювати механізми координації між внутрішніми бізнес-процесами і зовнішніми регуляторними вимогами. Управління стандартами в цьому сенсі – це не лише технічна специфікація форматів даних, але й сукупність організаційних рішень, що визначають відповідальність, повноваження та процеси прийняття рішень у життєвому циклі облікової інформації.

На рівні окремого підприємства імплементація управлінських регламентів починається з розробки внутрішніх політик, які визначають формат, методику та послідовність внесення облікових даних у блокчейн-систему. Політики мають охоплювати правила підготовки первинних документів, порядок формування ідентифікаторів, вимоги до часових міток і метаданих, процедури формування корегувальних записів і правила їхнього відображення у звітах. Важливим елементом є визначення ролей та відповідальності: хто має право створювати первинні записи, хто їх перевіряє, хто ініціює корекції, і які процедури застосовуються в разі виявлення невідповідностей. Чітка сегрегація обов'язків зменшує ризик фальсифікацій і помилок, а також полегшує відстеження відповідальності в аудиті.

Регламенти доступу й управління ідентичністю в межах підприємства повинні встановлювати механізми аутентифікації, авторизації та управління ключами. Практика охоплює використання багаторівневих ролей, обов'язкових процедур перевірки уповноважень перед підписанням операцій та процедур відкликання прав у разі зміни трудових відносин або ризиків компрометації. Політики також мають передбачати вимоги до збереження приватних ключів, процедур їхнього резервного копіювання й відновлення, а також стандартизовані дії у випадку інцидентів інформаційної безпеки. Наявність таких правил забезпечує баланс між доступністю даних для робочих процесів і захистом від несанкціонованого втручання.

Процедури контролю та аудиту в управлінській системі повинні інтегруватися із протоколами мережі: заплановані внутрішні перевірки, автоматичні механізми виявлення аномалій, вимоги щодо збереження доказової бази й формалізовані шаблони аудиторських висновків. Важливим елементом є забезпечення судової та нормативної доказовості ончейн-документів: внутрішні регламенти повинні містити положення про збереження метаданих, які дають змогу відтворити контекст операції (джерело, авторизація, часові мітки, версія словника даних). Для забезпечення надійності аудиту потрібно запровадити вимоги до форензичної готовності – можливості оперативно надати незмінну і водночас структуровану інформацію для перевірки.

На наднаціональному рівні ефективна стандартизація вимагає ухвалення нормативних актів, які уніфікують вимоги до цифрових доказів, визначають правовий статус смартконтрактів і визнають юридичну силу документів, зареєстрованих у розподіленому реєстрі. Законодавство повинно встановлювати критерії автентичності, цілісності та допустимості ончейн-записів як доказів у адміністративних та судових процесах. Окрему увагу потрібно приділити питанням підпису, сертифікації ключів та вимогам до акредитації довірчих центрів або реєстрів, які забезпечуватимуть довіру до цифрових підписів і часових міток.

У контексті міжнародної сумісності потрібна координація нормативних підходів між юрисдикціями. Відмінності у правовому статусі електронних підписів, різні вимоги до зберігання персональних даних та конкуренція норм про публічні реєстри створюють бар'єри для вільного обміну обліковими даними. Тому на міждержавному рівні

доцільно просувати гармонізацію правил через міжнародні угоди або стандартизаційні ініціативи, які визначатимуть мінімальні вимоги до юридичної визнаності ончейн-документів, процедури трансграничного доступу та умови співпраці з контролювальними органами. Гармонізація сприятиме створенню міжнародної цифрової інфраструктури бухгалтерського обліку, що дасть змогу підприємствам вести одноманітний облік у різних юрисдикціях.

Комплексний підхід до управління стандартизацією повинен враховувати процедури сертифікації і контролю впроваджень. Регуляторні органи і професійні асоціації мають розробити методики оцінювання відповідності впроваджень затвердженим політикам і протоколам, охоплюючи тестування реалізацій, моніторинг відповідності та періодичні ревізії. Сертифікація реалізацій, вузлів мережі або постачальників послуг гарантує, що технічні й організаційні рішення відповідають вимогам до безпеки, сумісності й доказовості, а також створює механізми відповідальності в разі невідповідності.

Необхідною складовою управлінського аспекту є механізм навчання і підвищення кваліфікації персоналу. Стандартизація втратить ефективність, якщо користувачі не володітимуть знаннями щодо правил реєстрації, підписування, корекцій та процедур контролю. Програми підготовки мають бути формалізовані у внутрішніх політиках і містити як технічні, так і правові аспекти використання блокчейн-систем у бухгалтерському обліку.

Управлінський блок стандартів повинен передбачати механізми врегулювання суперечок і вирішення конфліктів правового характеру. Оскільки транскордонні транзакції залучають різні правові системи, стандартні процедури для арбітражу, визначення застосовного права та взаємодії з державними реєстрами суттєво знижують юридичні ризики і підвищують довіру користувачів до ончейн-документів. Така правова інфраструктура у поєднанні з технічними й організаційними регламентами утворює цілісний підхід до стандартизації, здатний забезпечити сумісність і прийнятність облікових даних у глобальному масштабі.

Узагальнюючи викладений вище матеріал, структуруємо його у вигляді характеристики напрямів стандартизації бухгалтерського обліку в умовах цифрової децентралізації (табл. 2.7).

Таблиця 2.7 – Характеристика напрямів стандартизації бухгалтерського обліку в умовах цифрової децентралізації

Напрям стандартизації	Змістовна характеристика	Очікуваний ефект
1	2	3
Методологічна стандартизація	Формування єдиних правил створення цифрових записів, структур облікових даних, їх кодування й верифікації; цифрове відтворення облікових принципів у вигляді уніфікованих схем даних	Сумісність між системами, відтворюваність і порівнянність даних, усунення неоднозначності трактувань
Семантична уніфікація	Розробка словників даних та єдиної термінології («транзакція», «подія», «цифровий актив», «смартзапис» тощо); формалізація реквізитів, значень, одиниць виміру, зв'язків між об'єктами	Єдине трактування економічних понять, автоматична інтерпретація облікових фактів усіма системами
Технічна уніфікація	Визначення форматів повідомлень, правил серіалізації, протоколів підключення; уніфікація ідентифікаторів, підписів, часових міток, механізмів консенсусу, процедур корекцій	Гарантована технічна сумісність, відтворюваність записів, можливість автоматичної обробки без ручних трансформацій
Алгоритмічна гармонізація облікових норм	Переклад облікових правил у програмний код смартконтрактів (визнання, оцінка, класифікація, момент фіксації доходу / витрат)	Автоматичне виконання облікових процедур, мінімізація суб'єктивізму, підвищення достовірності
Метадані та доказовість	Внесення в облікові записи відомостей про джерело, авторство, час, рівень довіри, версію схеми, параметри валідації	Автоматична перевірка повноти й достовірності; юридична доказовість цифрових документів
Конфіденційність і селективне розкриття	Механізми псевдонімізації, рівнів доступу, офчейн-доказів; криптографічні гарантії приватності	Баланс між прозорістю та захистом даних, відповідність вимогам безпеки й права
Інституційна гармонізація	Участь регуляторів, професійних організацій, міжнародних інституцій у розробці цифрових стандартів	Легітимність і прийнятність цифрових форматів звітності на національному та міжнародному рівнях

Продовження таблиці 2.7

1	2	3
Управлінська стандартизація	Розробка внутрішніх політик обліку в блокчейн-системах: правила внесення даних, контролю, ролей і відповідальності	Зменшення ризиків помилок і фальсифікацій, чітка сегрегація обов'язків, прозорість процесів
Правове забезпечення	Визнання смартконтрактів і ончейн-документів як юридично значущих; визначення критеріїв автентичності й допустимості цифрових доказів	Юридична сила цифрових записів, зменшення правових ризиків і спорів
Міжнародна координація	Гармонізація норм щодо електронних підписів, персональних даних, публічних реєстрів; угоди про транскордонну звітність	Глобальна сумісність облікових систем, єдина цифрова інфраструктура звітності
Сертифікація та контроль впроваджень	Розробка методик тестування, акредитація постачальників, моніторинг відповідності реалізацій стандартам	Гарантія безпеки, якості й інтероперабельності облікових рішень
Освітньо-кадрова підготовка	Формування компетенцій у сфері блокчейн-обліку, цифрових підписів, смартконтрактів і правових аспектів	Професійна готовність персоналу, правильне використання стандартів і протоколів
Механізми вирішення спорів	Встановлення процедур арбітражу, визначення застосовного права, взаємодія з державними реєстрами	Зниження юридичних ризиків, стабільність і довіра в міжнародних операціях

Джерело: складено авторами.

Отже, стандартизація та уніфікація облікових процедур у децентралізованому середовищі є не лише питанням технічної узгодженості, але й фундаментальним напрямом розвитку теорії бухгалтерського обліку. Вони формують основу для нової епістемології облікової інформації – такої, де достовірність, прозорість і порівнянність даних забезпечуються не адміністративним контролем, а алгоритмічними гарантіями системи. Уніфікація процедур стає запорукою довіри до цифрового обліку, оскільки забезпечує однаковість підходів до фіксації, оцінки та перевірки фактів господарської діяльності в будь-якому середовищі, що використовує технології блокчейн.

Висновки до розділу 2

Архітектура децентралізованого облікового середовища постає як цілісна система техніко-економічних і правових механізмів, у межах якої суб'єкти, об'єкти та інформаційні потоки взаємодіють у режимі алгоритмічно забезпеченої довіри, що вилучає потребу в централізованому адмініструванні. Її сутність полягає у трансформації бухгалтерського обліку з інституційно керованої функції в саморегульовану, криптографічно захищену інформаційну екосистему, де кожен суб'єкт виконує роль одночасно генератора, верифікатора й користувача даних, а кожен об'єкт набуває ознак автономної цифрової сутності з юридично підтвердженим статусом. Інформаційні потоки в такій архітектурі формують безперервний, трасований і синхронізований цикл облікової інформації, у якому принципи достовірності, інваріантності та прозорості реалізуються через консенсусні алгоритми й смартконтракти. У підсумку децентралізоване облікове середовище стає основою нової парадигми бухгалтерського мислення – обліку як технологічно детермінованої системи довіри, що забезпечує автоматизоване формування, перевірку й визнання облікових даних у режимі реального часу.

Механізм функціонування блокчейн-реєстру у відображенні господарських операцій формує концептуально нову модель бухгалтерського обліку, у якій технічна інфраструктура децентралізованої мережі, криптографічний захист і алгоритми консенсусу інтегруються в єдину систему математично доведеної достовірності. У межах цієї системи обліковий запис набуває властивостей самоверифікованого цифрового факту, що підтверджується колективною згодою учасників мережі, а не інституційним контролем. Кожна господарська операція проходить шлях від ініціації до підтвердження через алгоритмічну валідацію, у результаті чого формується безперервний, незмінний і синхронізований ланцюг подій, який забезпечує повну простежуваність активів та дій усіх суб'єктів. Смартконтракти трансформують облік із реактивної у проактивну систему, що автоматично формує та верифікує облікові дані в момент їх виникнення, тоді як криптографічна архітектура гарантує захист, автентичність і селективну прозорість інформації. Отже, блокчейн-реєстр є не лише технологічним інструментом фіксації господарських фактів, а методологічною основою нової

парадигми бухгалтерського мислення – обліку як самоверифікованої системи довіри, у якій істинність даних забезпечується математичною логікою децентралізованого консенсусу.

Смартконтракти в системі децентралізованого бухгалтерського обліку є концептуальною основою переходу до нової моделі цифрової автономії облікових процесів, у межах якої визнання, оцінювання, відображення та контроль господарських операцій здійснюються алгоритмічно, без участі посередників і людського чинника. Завдяки властивостям автоматичного виконання, криптографічної верифікації та незмінності записів смартконтракти забезпечують подвійний рівень достовірності облікової інформації – технологічний і економічний, що унеможливлює маніпуляції з даними та гарантує їхню повну відповідність принципам бухгалтерського обліку. Вони перетворюють облікову політику з нормативного документа на діючий програмний алгоритм, який забезпечує безперервне дотримання методологічних вимог у момент формування записів. Так, смартконтракти створюють підґрунтя для реалізації концепції «самоперевірного обліку», у якому процес фіксації господарської події одночасно є її підтвердженням і контролем, що забезпечує формування прозорого, інтегрованого та достовірного інформаційного простору бухгалтерії нового покоління.

Методика облікової оцінки, визнання та верифікації фактів господарської діяльності у блокчейн-системах становить системно-інтегрований підхід до відображення економічних процесів, у якому відбувається органічне поєднання традиційних облікових принципів із технологічними механізмами децентралізованих реєстрів. Її сутність полягає в перетворенні бухгалтерського обліку з документально-процедурної системи в самоверифіковану цифрову платформу, де достовірність даних забезпечується не постфактумними перевірками, а вбудованими алгоритмами консенсусу, смартконтрактами та криптографічними доказами. Така методика формує нову парадигму облікової достовірності, у межах якої факт господарської діяльності визнається, оцінюється та підтверджується одночасно в момент його фіксації, а кожен запис набуває статусу автономного доказу економічної події. У результаті блокчейн-технологія стає не лише інструментом технічної фіксації, а методологічним каркасом для побудови облікової системи майбутнього, що характеризується прозорістю, математичною доказовістю, невідворотністю змін і високим рівнем довіри між усіма учасниками економічного середовища.

Стандартизація та уніфікація облікових процедур у контексті використання децентралізованих технологій становлять фундаментальний інструмент формування інтегрованого, достовірного та юридично визнаного цифрового бухгалтерського середовища. Їхня сутність полягає не лише в гармонізації методологічних принципів обліку, але й у формалізації цих принципів у вигляді уніфікованих схем даних, протоколів взаємодії, семантичних словників та алгоритмічних правил, реалізованих у коді блокчейн-протоколів і смартконтрактів. Саме така багаторівнева система – методологічна, технічна, правова та управлінська – забезпечує сумісність між суб'єктами облікового процесу, гарантує верифікованість і безперервність облікових записів, зменшує ризики суб'єктивних інтерпретацій і створює основу для автоматизованого формування фінансової звітності в режимі реального часу. У кінцевому підсумку, стандартизація й уніфікація є не лише засобом технічної інтеграції блокчейн-технологій у бухгалтерський облік, а й концептуальним чинником еволюції самої облікової парадигми – від централізованого документування фактів господарського життя до децентралізованої, алгоритмічно контрольованої системи довіри.

РОЗДІЛ 3
ОРГАНІЗАЦІЙНО-ПРИКЛАДНІ АСПЕКТИ БУХГАЛТЕРСЬКОГО ОБЛІКУ В УМОВАХ ЗАСТОСУВАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ

«Ідеї, які змінюють світ,
завжди починаються як моделі, створені у свідомості»
Норберт Вінер (американський математик,
творець основ кібернетики)

3.1. Модель організації облікового процесу в середовищі цифрової децентралізації

Модель організації облікового процесу в середовищі цифрової децентралізації ґрунтується на принципово новій архітектурі облікової системи, де ключовим елементом є розподілений реєстр, що забезпечує фіксацію, верифікацію та збереження даних без централізованого контролю [35; 44]. У традиційній системі бухгалтерського обліку відповідальність за достовірність інформації покладена на центрального суб'єкта – підприємство або його облікову службу. У децентралізованому середовищі функція довіри переноситься на алгоритмічний рівень, де достовірність господарських фактів гарантується криптографічними механізмами та колективною валідацією учасників мережі [43]. Так, обліковий процес перетворюється з ієрархічно підпорядкованої системи в горизонтально розподілену мережу взаємопов'язаних інформаційних вузлів.

Структурно модель організації облікового процесу в середовищі цифрової децентралізації являє собою складну багаторівневу систему, яка інтегрує в собі технологічні, аналітичні, нормативні та кадрові компоненти, забезпечуючи єдність облікових, контрольних і управлінських функцій. Її архітектура побудована на взаємодії восьми взаємопов'язаних елементів: інфраструктурного, інтеграційного, аналітичного та звітного, механізму цифрового консенсусу, архітектури даних, внутрішнього контролю та криптографічної безпеки, а також юридично-нормативного і кадрового компонентів (табл. 3.1).

Таблиця 3.1 – Характеристика моделі організації облікового процесу в середовищі цифрової децентралізації

Назва елементу моделі	Змістовна характеристика елементу моделі	Ключові інструменти / технології	Роль бухгалтера
1	2	3	4
Інфраструктурний (технічна база обліку)	Забезпечує функціонування розподіленого реєстру, фіксацію, верифікацію та збереження даних без централізованого контролю. Охоплює мережеву архітектуру, вузли, криптографічний захист, протоколи консенсусу та політики безпеки	Блокчейн-платформи; алгоритми консенсусу (Proof of Work, Proof of Stake, BFT); цифрові підписи, хешування; керування криптографічними ключами (HSM, мультипідпис)	Контролює параметри підтвердження транзакцій; забезпечує відповідність налаштувань протоколу внутрішнім політикам; моніторить технічну надійність і достовірність записів
Інтеграційний (зв'язок ERP і блокчейну)	Перетворює господарські події у транзакції, визначає правила формування метаданих, трансляції бухгалтерських проводок, взаємодії ончейн- та офчейн-компонентів	ERP-системи; API та адаптери обміну даними; смартконтракти; механізми валідації бізнес-правил	Формує і перевіряє транзакції; визначає облікові атрибути та метадані; забезпечує коректність трансляції бізнес-подій у облікові записи; реалізує принцип розподілу обов'язків (SoD) через цифрові підписи
Аналітичний та звітний	Виконує агрегацію, нормалізацію та інтерпретацію даних з блокчейну для створення бухгалтерських регістрів і фінансової звітності. Реалізує контрольні процедури й механізми безперервного аудиту	BI-системи та аналітичні панелі; системи індексації та агрегації даних; алгоритми перевірки цілісності та відповідності записів	Забезпечує формування звітності на основі ончейн-даних; здійснює алгоритмічний аудит і контроль відповідності записів обліковим стандартам; аналізує відхилення та аномалії у транзакціях

Продовження таблиці 3.1

1	2	3	4
Механізм цифрового консенсусу	Система узгодження технічних, організаційних і облікових правил. Забезпечує довіру до записів без централізованого посередника через колективну валідацію та криптографічні докази	Протоколи консенсусу; механізми колективного підтвердження; метрики узгодженості та цілісності даних	Узгоджує облікові політики з параметрами протоколу; формує корпоративні стандарти взаємодії з мережею; визначає критерії остаточного визнання транзакцій
Архітектура даних (ончейн / офчейн)	Поділ інформаційного простору на цифрові записи (ончейн) і зовнішні сховища (офчейн), з'єднані криптографічними хеш-прив'язками. Забезпечує баланс між незмінністю, масштабованістю й конфіденційністю	Хеш-функції та прив'язки; зовнішні бази даних (IPFS, хмарні сховища); метадані транзакцій	Контролює коректність і повноту метаданих; забезпечує цілісність зв'язку між ончейн- і офчейн-даними; здійснює аудит схем зберігання і доступу до даних
Внутрішній контроль і криптографічна безпека	Заміщує паперовий контроль криптографічними процедурами. Реалізує принципи SoD, ротацію ключів, управління ризиками і контроль доступів	Політики управління ключами (KMS); мультипідпис; журнали доступу і подій безпеки	Забезпечує відповідність дій правилам безпеки; контролює доступи, підписи і ключі; аналізує ризики цифрових операцій
Юридично-нормативний	Забезпечує легітимність цифрових записів як доказів. Узгоджує структуру транзакцій із законодавством, нормами збереження та конфіденційності (GDPR тощо)	Цифрові сертифікати; політики архівації; стандарти електронного документообігу	Перевіряє відповідність цифрових записів правовим вимогам; розробляє внутрішні регламенти архівації; забезпечує готовність до надання доказів у разі спорів

Продовження таблиці 3.1

1	2	3	4
Кадровий	Трансформація функцій бухгалтера з реєстратора даних у координатора цифрових процесів, аналітика та гаранта достовірності й безпеки облікової інформації	Інструменти управління блокчейн-вузлами; системи моніторингу транзакцій; алгоритми аудиту смартконтрактів	Керує параметрами цифрових протоколів; узгоджує правила облікового відображення зі смартконтрактами; моніторить цілісність і достовірність даних; розвиває компетенції у сфері IT, блокчейну та аналітики

Джерело: складено авторами.

Організаційна модель облікового процесу в середовищі цифрової децентралізації має внутрішню логіку, що визначається перехідним домінантним об'єктом – транзакцією як носієм інформації про господарський факт. Кожна така транзакція формується в межах операційної підсистеми підприємства або у взаємодії корпоративної ERP-системи зі смартконтрактом і завжди супроводжується метаданими, які визначають її економічний зміст, облікові категорії, часові мітки та ідентифікатори учасників. Структурно транзакція підписується електронними ключами сторін (диджитал-підпис або підпис, заснований на криптографії з відкритим ключем), що забезпечує автентичність відправника, після чого вона транслюється у вузли мережі для верифікації. Важливо підкреслити, що в організаційній моделі блокчейн-реєстр є не простим архівом, а операційним рівнем з фіксацією факту: запис у ланцюзі набуває статусу первинного доказового елемента, оскільки поєднує в собі дані про подію, криптографічні докази її походження та часову ознаку, що підтверджена консенсусом мережі.

Механізм додавання транзакції до блоку і подальшої інкрустації блоку в ланцюг реалізується через протокол консенсусу, який фактично заміщує функцію централізованої верифікації. В організаційній практиці це означає, що управління параметрами консенсусу – швидкістю підтвердження, рівнем підтверджень для фінальної валідації, політикою фіналізації – стає частиною внутрішнього контролю підприємства та корпоративного регламенту взаємодії з мережею.

Трансформація традиційної ролі первинного документа як автономного носія доказової сили не усуває потреби в формалізації доказів через структуру та криптографічні властивості запису. Сама транзакція або блок повинні містити достатній набір атрибутів для ідентифікації сутності господарської операції, бухгалтерських рахунків та умов облікового визнання; коли частина додаткових даних зберігається офчейн (наприклад, великі документи або конфіденційні вкладення), їх цілісність підтверджується за рахунок запису хэш-відбитків у ланцюжку. Тому практична модель передбачає двокомпонентну архітектуру з «ончейн» записами для диджиталізованих сутностей та «офчейн» сховищами, пов'язаними з першими через криптографічні прив'язки; це дає змогу поєднати вимоги до незмінності та масштабованості з потребою у конфіденційності й ефективному зберіганні.

Управління доступом і криптографічний захист у цій моделі набувають центрального значення. Підприємство формує політику ключового менеджменту, що охоплює генерацію ключів, їх безпечне зберігання (з використанням апаратних модулів безпеки), процедури ротації і відкликання ключів, а також механізми мультипідпису для операцій з підвищеними ризиками. Роль внутрішніх контролів переходить від перевірки паперів до нагляду за дотриманням криптографічних процедур і правил доступу: реалізація принципів SoD (Segregation of Duties) відбувається через налаштування смартконтрактів і політик накладання підпису, а не виключно через кадровий розподіл обов'язків. Організаційна відповідальність за ці функції розподіляється між операційними підрозділами, відповідальними за інформаційні технології, службою безпеки та бухгалтерією, яка стає власником семантичної моделі обліку та правил трансляції бізнес-подій у транзакції.

Зміна акцентів в організації обліку торкається також процедур аудиту та звітування. Оскільки блокчейн надає повний цифровий слід операцій, традиційна вибірка аудиту може замінюватися підходами до аудиту відповідності та безперервного аудиту, де аудиторські процедури налаштовуються на перевірку криптографічних доказів, відповідності смартконтрактів та алгоритмічних правил віднесення транзакцій до облікових категорій [13]. Водночас аудитор повинен оцінювати ризики, пов'язані з фіналізацією записів (наприклад, ризик реорганізації ланцюга), а також перевіряти коректність інтеграції між операційними системами підприємства й блокчейн-платформою: важливим

елементом є підтвердження того, що автоматично сформовані транзакції точно відображають господарські факти, а метадані відповідають обліковим правилам.

Технічно-організаційні питання управління параметрами протоколу консенсусу та політиками валідації потребують формалізації у корпоративних стандартах взаємодії з мережею. Це охоплює встановлення критеріїв для прийняття транзакцій як кінцево визнаних (наприклад, кількість підтверджень), процедури у випадку розбіжностей, визначення ролей вузлів, а також механізмів реагування на інциденти: «компроміс-відповідь», процедури повернення на крок назад або виконання корегувальних операцій, співпраця з іншими учасниками мережі для вирішення колективних технічних ризиків. Для підприємства це означає необхідність формування окремих регламентів, що інтегрують технологічні та облікові процедури.

Юридичні та нормативні виклики, пов’язані з відмовою від класичного первинного документа, також трансформують організаційну модель: підприємство повинно забезпечити відповідність транзакційної структури вимогам законодавства щодо збереження інформації, її автентичності та доступності для контролювальних органів. Це вимагає розвитку внутрішніх юридичних процесів для визнання цифрових записів як доказових, узгодження з політиками конфіденційності (включно з механізмами, сумісними з вимогами на кшталт GDPR – наприклад, зберігання персональних даних офчейн з криптографічними прив’язками ончейн) та визначення процедур для випадків спорів, що можуть супроводжуватися необхідністю надання оригіналів або доказів походження записів.

Модель організації облікового процесу в умовах цифрової децентралізації – це комплексна система, де технічні рішення (структура транзакції, алгоритми консенсусу, механізми підпису та зберігання даних) тісно інтегровані з організаційними інститутами (регламенти, ролі, внутрішні контролі, юридичні процедури). Перехід від збору паперових первинних документів до управління доступом, криптографічним захистом і параметрами протоколу викликає необхідність побудови нової моделі компетенцій, що поєднує класичну облікову експертизу з розумінням архітектури блокчейну, управління ризиками інформаційної безпеки та нормативно-правової відповідності. Це створює передумови для формалізованого, автоматизованого та верифікованого обліку, але водночас ставить вимогу до ретельного проєктування організаційних процесів і стандартів взаємодії всіх зацікавлених сторін.

Функціонування облікової системи в умовах цифрової децентралізації потребує чітко структурованої та взаємопов'язаної багаторівневої моделі управління даними, яка забезпечує технічну надійність, облікову коректність і відповідність нормативним вимогам на всіх етапах життєвого циклу інформації. Перший рівень такої моделі – інфраструктурний – охоплює апаратно-програмні елементи і протоколи, що забезпечують роботу розподіленого реєстру. Сюди входять конфігурація та рольова модель вузлів мережі (повні вузли, верифікатори, легкі клієнти), механізми взаємного підтвердження записів, криптографічні методи захисту (підписи, хешування, обернене шифрування для зберігання паролів) та механізми керування ключами. Інфраструктурний рівень визначає характеристики надійності й тимчасової визначеності записів: від вибору алгоритму цифрового консенсусу залежать швидкість підтвердження транзакцій, ризик реорганізації реєстру і правила остаточного визнання запису як доказового елемента. Одночасно цей рівень встановлює технічні засади інтеграції з зовнішніми середовищами, політики резервування та безперервності роботи, вимоги до продуктивності і масштабованості.

Другий рівень – інтеграційний – забезпечує зв'язок між операційними обліковими підсистемами підприємства і блокчейн-реєстром. Він охопдює модулі перетворення бізнес-подій у транзакції, механізми валідації бізнес-правил перед записом, шари трансляції семантики облікових проводок та інтерфейси обміну (прикладні інтерфейси, брокери повідомлень, адаптери для ERP-систем). На цьому рівні формалізуються правила віднесення господарських фактів до облікових рахунків, встановлюються шаблони метаданих для транзакцій (ідентифікатори контрагентів, класи операцій, часові мітки, економічні атрибути), визначаються умови для розміщення супутніх даних офчейн і методи прив'язки їх до ончейн-записів через хеші. Інтеграційний рівень реалізує також механізми транзакційної оркестрації: гарантує атомарність операцій у випадках, коли одна бізнес-подія породжує кілька взаємопов'язаних записів, і встановлює політики відкладеного чи пакетного запису для оптимізації навантаження. Крім технічних рішень, цей рівень визначає організаційні процедури – хто формує транзакції, які підрозділи затверджують їх перед підписом, як реалізується принцип розподілу обов'язків через механізми множинних підписів та процедурні права доступу.

Третій рівень – аналітичний та звітний – трансформує розподілені технічні записи у фінансову й управлінську інформацію, придатну для складання звітності відповідно до вимог облікових стандартів і проведення аудиту. Цей рівень охоплює інструменти індексації, агрегації та нормалізації даних, модулі побудови регламентованих регістрів, системи контрольних правил та механізми постійного контролю за відповідністю облікових проводок затвердженим політикам. У рамках аналітичного рівня здійснюється відображення ончейн-транзакцій у бухгалтерські рахунки, розрахунок амортизації, визнання доходів і витрат з урахуванням часових ознак та умов господарської операції, а також підготовка звітів для зовнішніх користувачів і контролювальних органів. Особливу роль тут відіграють засоби забезпечення прозорості та відтворюваності облікових процедур: збереження криптографічних доказів походження даних, журналів доступу та історії змін, що дає змогу здійснювати безперервний аудит і швидко відтворювати ланцюжок подій у випадку перевірок або спорів.

Взаємодія цих трьох рівнів відбувається за принципом «цифрового консенсусу», який означає узгодження технічних та організаційних правил на всіх шарах системи. Практично це виражається в координації параметрів консенсусного протоколу з політиками формування транзакцій і вимогами до звітності: наприклад, визначення мінімальної кількості підтверджень для фіксації операції в регламенті бухгалтерії, або встановлення правил тимчасової проміжної валідації для аналітичних цілей. Цифровий консенсус мінімізує ризик помилок та маніпуляцій тим, що забезпечує однакові правила перевірки для всіх учасників, прозорі алгоритмічні механізми верифікації та неминучість фіксації змісту транзакції після досягнення технічного завершення. Крім того, цей підхід передбачає системи моніторингу та індикатори цілісності, які на рівні управління відстежують показники узгодженості даних, частоту конфліктів під час валідації і час досягнення завершеності, що дає змогу оперативно корегувати як технічні налаштування, так і організаційні процедури.

У моделі управління даними також потрібно закласти комплекс заходів щодо конфіденційності й відповідності правам суб’єктів даних: шифрування чутливих полів, псевдонімізація, зберігання персональної інформації поза реєстром з криптографічною прив’язкою, встановлення правил доступу на основі ролей і журналювання всіх

операцій з даними [76]. Для забезпечення практичної застосовності важливими є стандартизація метаданих, уніфікація кодів операцій і створення централізованих довідників, які підтримуються на рівні інтеграційного шару і використовуються аналітичними модулями для коректного зіставлення ончейн-записів зі статтями звітності. Невід'ємною частиною моделі є також визначення процедур збереження та архівації даних, термінів зберігання, правил доступу для контролювальних органів і механізмів відновлення після інцидентів.

Багаторівнева модель управління даними в середовищі цифрової децентралізації є одночасно технічною та організаційною конструкцією, що поєднує інфраструктурні рішення, інтеграційні механізми й аналітичні процедури в єдину систему, де цифровий консенсус є гарантом достовірності та незмінності облікових записів, а водночас дає змогу зберегти гнучкість і відповідність регуляторним вимогам.

Особливість організації облікового процесу в умовах цифрової децентралізації полягає у глибокій трансформації професійної ролі бухгалтера, який із виконавця рутинних операцій перетворюється на активного учасника управління цифровими обліковими системами. У традиційній моделі обліку основна увага бухгалтера зосереджувалася на реєстрації первинних документів, складанні бухгалтерських проведень і формуванні звітності. У децентралізованій цифровій системі ці функції дедалі більше автоматизуються завдяки алгоритмічній фіксації господарських фактів у блокчейн-мережі, що робить людину не стільки виконавцем, скільки координатором та аналітиком процесу. Його завдання полягає в забезпеченні коректності параметрів облікових записів, узгодженні правил функціонування смартконтрактів із чинними нормами фінансової звітності, а також у контролі за безпечністю та цілісністю транзакційних даних.

Роль бухгалтера в децентралізованому обліковому середовищі набуває системно-управлінського характеру. Він є адміністратором облікової інфраструктури, відповідальним за налаштування параметрів протоколів підтвердження транзакцій, за розмежування прав доступу до вузлів мережі, а також за формування політик перевірки та авторизації користувачів. Його функції охоплюють також моніторинг стану облікових даних у розподіленому реєстрі, визначення ступеня достовірності записів, контроль за відповідністю алгоритмічних правил нарахування чи визнання доходів обліковим стандартам. У цьому

контексті бухгалтер виконує роль сполучної ланки між технічними фахівцями, які підтримують функціонування блокчейн-платформи, та управлінською командою підприємства, що ухвалює рішення на підставі облікової інформації.

Трансформація змісту професійної діяльності бухгалтера передбачає переосмислення структури його компетентності. Якщо раніше основу професійної підготовки становили знання нормативного регулювання, облікових стандартів і методики ведення рахунків, то тепер до цього додаються навички, пов'язані з цифровою аналітикою, управлінням даними та технологічною безпекою. Бухгалтер має володіти розумінням принципів функціонування блокчейн-мереж, логіки побудови смартконтрактів, методів токенізації активів і процедур їхнього облікового відображення. Він повинен уміти оцінювати ризики, що виникають унаслідок децентралізованої обробки інформації, включно з ризиками втрати приватних ключів, несанкціонованих змін даних чи технічних збоїв у протоколах консенсусу.

Смартконтракти, що є алгоритмічними формами реалізації господарських угод, висувають до бухгалтера вимогу володіння навичками перевірки логічних умов їх виконання, визначення точок бухгалтерського визнання операцій, а також співвіднесення автоматизованих дій програми з чинними обліковими принципами. У цьому контексті бухгалтер стає не просто реєстратором події, а аналітичним спостерігачем і регулятором цифрових процесів, який має забезпечити їхню економічну та правову коректність. Аналогічно, у випадках токенізації активів – коли матеріальні або нематеріальні цінності перетворюються на цифрові одиниці обліку – бухгалтер повинен забезпечити ідентифікацію кожного токена як об'єкта активу, визначити критерії його визнання в балансі, правила переоцінки та амортизації, а також способи відображення операцій з токенами у фінансовій звітності.

Не менш важливою складовою нової компетентності є володіння криптографічними механізмами безпеки. Бухгалтер повинен розуміти принципи створення, зберігання та управління ключами доступу до цифрових рахунків і облікових вузлів, знати механізми перевірки електронних підписів, вміти аналізувати хеш-записи для підтвердження автентичності даних. Його діяльність повинна спрямовуватись не лише на точність числових показників, а й на забезпечення захисту інформації, що є фундаментальною складовою облікової довіри в умовах цифрової децентралізації.

У децентралізованій системі бухгалтер також виконує функцію координатора цифрового контролю. Завдяки доступу до розподіленого реєстру він може здійснювати безперервний моніторинг облікових подій, використовуючи аналітичні алгоритми для виявлення аномалій або потенційних відхилень. Це перетворює аудит і внутрішній контроль на постійно діючий процес, інтегрований у саме середовище даних. Так, бухгалтер не лише фіксує результати минулих операцій, а й активно впливає на поточне управління ризиками, забезпечуючи прозорість і достовірність інформаційних потоків.

В умовах цифрової децентралізації бухгалтер перестає бути виключно носієм традиційних знань і набуває статусу фахівця міждисциплінарного типу – управлінця даними, технологічного аналітика та гаранта інформаційної безпеки. Ця еволюція професії є закономірною відповіддю на виклики цифрової доби, у якій довіра, достовірність і контроль реалізуються через технологію, а не через формальні процедури, і де бухгалтер постає ключовою ланкою між економічною сутністю операцій та їхнім технічним відображенням у децентралізованому обліковому середовищі.

Отже, модель організації облікового процесу в середовищі цифрової децентралізації трансформує не лише технічну основу бухгалтерського обліку, а й його концептуальні засади. Облік стає безперервним, прозорим і самоверифікованим процесом, у якому довіра формується не через контроль і перевірку, а через алгоритмічну надійність та колективну валідацію даних. Це відкриває перспективи створення глобальної інтегрованої облікової екосистеми, у межах якої забезпечується повна прозорість економічних процесів, автоматизація звітності та підвищення рівня економічної безпеки.

3.2. Ризики та етичні виклики блокчейн-орієнтованого обліку

Функціонування бухгалтерського обліку на засадах блокчейн-технологій супроводжується появою нових ризиків та етичних викликів, які потребують системного аналізу й адаптації традиційних принципів обліку до умов цифрової децентралізації [31]. Висока автоматизація облікових процесів, розподілений характер збереження даних і

використання алгоритмів консенсусу формують нове середовище, у якому ризики мають багатовимірний характер – технічний, організаційний, правовий і професійний (табл. 3.2).

Таблиця 3.2 – Характеристика ризиків функціонування бухгалтерського обліку в умовах цифрової децентралізації (на засадах блокчейн-технологій)

Вид ризику	Ризик	Характеристика ризику
1	2	3
Технологічні ризики	Алгоритмічні вразливості протоколів консенсусу	Помилки чи збої в алгоритмах узгодженості транзакцій призводять до тимчасової невизначеності статусу операцій, подвійного відображення або розбіжностей у записах
	Централізація обчислювальних потужностей (атака 51 %, домінування верифікаторів)	Концентрація контролю над мережею створює загрозу маніпуляції транзакціями, їх відміни чи затримки, що підриває достовірність і сталість бухгалтерського реєстру
	Ризик квантової вразливості криптографічних алгоритмів	Розвиток квантових обчислень може зруйнувати криптографічні механізми захисту, поставивши під сумнів автентичність історичних записів і вимагатиме ревалідації даних
	Помилки в реалізації смартконтрактів	Логічні або синтаксичні помилки в коді смартконтрактів можуть спричиняти автоматичні некоректні облікові записи, хибні нарахування чи перекази, які неможливо змінити без порушення цілісності реєстру
	Автоматичне формування некоректних записів унаслідок технічних збоїв	Помилки в даних призводять до спотворення фінансових результатів, невідповідності стандартам звітності та втрати доказової сили облікової інформації під час аудиту

Продовження таблиці 3.2

1	2	3
Організаційно-інституційні ризики	Невизначеність розподілу відповідальності між учасниками мережі	Відсутність централізованого власника або адміністратора облікових даних ускладнює встановлення суб'єкта, відповідального за достовірність і цілісність інформації
	Відповідальність за помилки автоматизованих алгоритмів	Неможливо однозначно визначити, хто несе відповідальність за наслідки помилок смартконтрактів – розробник, користувач чи аудитор системи
	Ризики колективного прийняття рішень (форки, зміна правил)	Консенсусні механізми без централізованого управління можуть призвести до розщеплення ланцюга, дублювання записів або втрати узгодженості бухгалтерських реєстрів
	Складність інтеграції з наявними системами управління та звітності	Відсутність стандартизації форматів даних і протоколів ускладнює взаємодію між вузлами, створюючи ризик розбіжностей у первинних записах і затримок звітності
	Відсутність нормативного закріплення ролей учасників блокчейн-обліку	Недостатнє правове регулювання статусу розробників, верифікаторів і користувачів призводить до правової невизначеності та потенційного уникнення відповідальності
	Ослаблення функцій внутрішнього контролю	Відсутність централізованого контролера та складність перевірки правильності записів до їх внесення в реєстр підвищує ризик накопичення помилок та порушень достовірності облікових даних

Продовження таблиці 3.2

1	2	3
Ризики управління доступом і конфіденційністю	Неправильне налаштування прав доступу	Делегування прав у розподіленому середовищі без належного контролю може дозволити несанкціоновані зміни записів або блокування облікових рахунків
	Втрата чи компрометація криптографічних ключів	Порушення процедур керування ключами призводить до втрати доступу до активів, неможливості підтвердження операцій чи доведення їх легітимності
	Конфлікт між прозорістю і конфіденційністю даних	Відкритість публічних блокчейнів спричиняє ризик витоку фінансової та персональної інформації, тоді як надмірна закритість ускладнює аудит і зовнішній контроль
	Недостатній технічний захист даних	Відсутність комплексного криптографічного захисту і механізмів відновлення доступу збільшує імовірність компрометації або втрати облікових даних
	Правові колізії щодо статусу блокчейн-записів	Неврегульованість правового статусу блокчейн-записів та конфлікт із законодавством про персональні дані створюють невизначеність у судових спорах, перевірках і регуляторних процедурах

Джерело: складено авторами.

Найбільш вагомими технологічними ризиками, що загрожують стабільності роботи блокчейн-мережі й достовірності облікових записів, є комплекс взаємопов’язаних вразливостей як на рівні алгоритмів, так і на рівні реалізації програмного коду. Алгоритмічна частина ризику пов’язана з протоколом досягнення узгодженості, який визначає порядок підтвердження записів у реєстрі: збої або оптимізаційні помилки в цих протоколах можуть призводити до тимчасової невизначеності статусу транзакцій, до реорганізацій ланцюга записів або до ситуацій, коли одна й та сама подія фіксується в різних версіях реєстру. Наслідком таких явищ для бухгалтерії може стати невпевненість у

моменті визнання операції, подвійне або неповне відображення господарських фактів та складнощі з установленням остаточності запису як доказового елемента.

Централізація обчислювальних потужностей у мережі є ще одним критичним ризиком: хоча архітектура мережі передбачає розподіл навантаження між багатьма учасниками, концентрація ресурсів у руках невеликої групи учасників створює умови для технічного підпорядкування мережі зовнішнім силам. Така концентрація може реалізуватися у вигляді так званої атаки «51 %», підкупу верифікаторів або домінування постачальників обчислювальних послуг. Для обліку це означає потенціал навмисного чи випадкового спотворення послідовності транзакцій, затримок у їх підтвердженні або створення умов для відміни раніше визнаних записів, що підриває довіру до реєстру як до джерела істинних даних.

Ризик, пов'язаний із розвитком квантових обчислень, має фундаментальний характер і стосується криптографічної бази системи. Сучасні механізми аутентифікації та цілісності даних опираються на криптографічні функції, які в перспективі можуть стати вразливими перед квантовими алгоритмами. У практичному сенсі це означає, що приватні ключі й цифрові підписи, що сьогодні гарантують неможливість підробки запису, у майбутньому можуть бути скомпрометовані, а відповідно – ставиться під сумнів автентичність і незмінність історичних облікових записів. Наслідком для бухгалтерської практики може стати потреба ще раз верифікувати старі записи або запровадити механізми додаткової криптографічної репутації.

Вразливість реалізації програмного коду проявляється передусім у помилках смартконтрактів – автоматизованих алгоритмів, що закріплюють логіку облікових і розрахункових операцій. Помилка в коді, логічна невідповідність або пропущена умова можуть призвести до того, що система автоматично здійснить некоректні нарахування, перегрупування активів або розподіл доходів, і ці дії, записані в реєстрі, стануть фактом обліку. Оскільки зміна вже закріпленого запису в мережі часто технічно або юридично ускладнена, виправлення таких помилок вимагає розробки нових процедур – від створення компенсаторних транзакцій до загальних оновлень протоколу – що само собою не завжди можливе оперативно та без наслідків для звітності.

У бухгалтерському вимірі ці технологічні ризики можуть виражатися у вигляді автоматичного формування некоректних записів, викривлення фінансових результатів, порушення відповідності звітності чинним стандартам та втрати доказової сили інформації під час перевірок. Якщо операція автоматично зафіксована з помилковими реквізитами або з неправильним обліковим визнанням, аудит не завжди зможе апелювати до «оригіналу» в традиційному розумінні, бо «оригінал» – це сам незмінний запис у реєстрі. Це ставить під питання можливість звичайних корегувальних записів і вимагає від бухгалтера та аудитора нових процедур для виявлення, документування і виправлення таких ситуацій.

Для мінімізації цих ризиків потрібно запровадження багатопланових заходів: формальна перевірка та сертифікація протоколів і смарт-контрактів до їхнього введення в експлуатацію; застосування механізмів моделювання і тестування в умовах, близьких до реальних, з імітацією атак і негативних сценаріїв; використання архітектур з розподілом ролей і контролю (наприклад, приватні або консорціальні мережі для критичних облікових процесів); впровадження політик управління життєвим циклом криптографічних засобів з урахуванням перспектив квантового опору; а також розбудова процедур документування всіх змін і створення автономних резервних журналів, які дають змогу відтворити послідовність обліку в разі сумніву в достовірності основного реєстру. Тільки поєднання технічних, організаційних та нормативних заходів здатне зменшити негативний вплив технологічних ризиків на бухгалтерський облік у середовищі цифрової децентралізації.

Ризики, пов’язані з управлінням доступом і конфіденційністю в блокчейн-орієнтованому обліку, мають системний характер та охоплюють як технічні, так і організаційно-правові виміри [60; 62]. У розподіленому середовищі відсутність єдиного централізованого адміністратора даних зумовлює необхідність делегування прав і відповідальності між численними учасниками мережі, що ускладнює контроль за тим, хто саме має право формувати, підписувати та ініціювати облікові транзакції. Неправильне або неповне налаштування рівнів доступу може призвести до сценаріїв, коли особи без належних повноважень отримують можливість змінювати або ініціювати записи, а втручання у процедури керування ключами – до втрачених ключів,

блокування рахунків або неможливості підтвердити легітимність операції. Усе це ставить під загрозу безперервність облікового процесу та здатність підприємства відтворити історію господарських фактів у разі перевірки.

Проблема конфіденційності в блокчейні має два конфліктні вектори: вимогу прозорості для забезпечення довіри з боку зовнішніх користувачів та необхідність захисту комерційної та персональної інформації. Публічні ланцюги за своєю сутністю схильні до широкого відкритого доступу, що може призводити до небажаного витоку фінансових показників, контрагентської інформації чи оперативних даних підприємства. Навпаки, надмірна закритість або сувора сегментація доступу унеможливлює належний зовнішній контроль та ускладнює процедури аудиту. Тому в організаційній практиці постає завдання збалансувати прозорість і приватність через гібридні підходи: виділення частин даних для загальнодоступного реєстру та зберігання чутливих елементів у зовнішніх, контрольованих сховищах з криптографічними прив'язками до ончейн-записів.

Технічні рішення щодо захисту конфіденційності мають поєднуватися з організаційними заходами. До перших належать шифрування даних у стані спокою та під час передавання, псевдонімізація та агрегування операцій перед записом у реєстр, використання офчейн-сховищ для чутливих документів з записом хеш-відбитків на ланцюзі, застосування механізмів мультипідпису та розподіленого підписування для операцій із підвищеним ризиком. До других – формальні політики управління ключами (генерування, зберігання, ротація, відкликання), визначення ролей і прав на рівні організації, укладання міжсуб'єктних угод про взаємні зобов'язання з безпеки, а також процедур відновлення доступу у випадку втрати ключів. Важливим є також впровадження журналювання доступів і подій, що забезпечує трасованість дій та дає змогу оперативно розслідувати інциденти.

Правові колізії значною мірою підсилюють ризики управління доступом і конфіденційністю. У більшості юрисдикцій відсутнє однозначне визначення статусу блокчейн-запису як офіційного первинного документа, а також уніфіковані правила щодо зберігання, доступу і видалення даних у розподілених системах. Це породжує невизначеність під час проведення перевірок, у судових спорах або за взаємодії з контролювальними органами. Додатково, наявні вимоги до захисту

персональних даних (право на виправлення чи «видалення») конфліктують із властивою блокчейну незмінністю записів. Наслідком може стати правова невизначеність щодо процесів надання доступу інспекторам, або навпаки – ризик порушення регуляторних вимог за надмірної відкритості реєстру.

Можливі практичні наслідки цих ризиків для обліку охоплюють: витік конфіденційної інформації контрагентів і клієнтів; неможливість коректно і своєчасно підтвердити походження операції через втрату ключа; підвищені репутаційні та фінансові ризики в разі розкриття стратегічних даних; складнощі з наданням потрібної інформації для аудиту в разі збереження вимог конфіденційності; а також ризик юридичної незахищеності в разі оскарження записів у суді. Тому для мінімізації таких ризиків підприємствам доцільно розробити комплексну модель управління доступом, яка охоплює технічні засоби, організаційні процедури та механізми юридичного захисту.

У числі практичних заходів зниження ризиків потрібно виокремити: впровадження розмежованих мережевих архітектур (публічні – для загальної довіри, приватні або консорціальні – для критичних облікових процесів); стандартизацію форматів метаданих і процедур псевдонімізації; використання криптографічних прив'язок ончейн- до офчейн-документів; формалізацію політик керування ключами та застосування апаратних модулів безпеки для їхнього зберігання; розробку юридичних угод і процедур співпраці між учасниками мережі, що визначають відповідальність за доступ і відновлення даних; а також впровадження протоколів взаємодії з контролювальними органами, які дають змогу зберігати конфіденційність комерційної інформації, одночасно забезпечуючи необхідну прозорість для перевірок. Лише комплексний підхід, що поєднує технічні, організаційні та правові інструменти, здатен забезпечити прийнятний рівень управління доступом і конфіденційністю в облікових системах на засадах цифрової децентралізації.

До групи організаційно-інституційних ризиків у блокчейн-орієнтованому бухгалтерському обліку належать насамперед проблеми визначення меж і розподілу відповідальності між учасниками децентралізованої мережі. У традиційній системі обліку існує чітка ієрархія – суб'єкт господарювання володіє базою даних, бухгалтер відповідає за достовірність записів, а керівництво – за затвердження фінансової

звітності. У цифрово-децентралізованому середовищі ці межі розмиваються: інформаційна база формується колективно, а функції контролю і зберігання розподіляються між численними вузлами мережі, які можуть належати різним організаціям або навіть бути географічно розташованими в різних юрисдикціях. За таких умов стає складно визначити єдиного власника або адміністратора облікової інформації, а отже – і суб'єкта, який несе відповідальність за її цілісність, повноту та достовірність.

Проблема відповідальності набуває особливої гостроти у випадках, коли в процесі виконання смартконтрактів або інших автоматизованих алгоритмів виникають помилки, некоректні транзакції чи блокування доступу до активів. У традиційній системі можна встановити людський чинник – бухгалтера чи оператора, який допустив неточність, або програмне забезпечення, що вийшло з ладу. У блокчейні ж усі дії відбуваються автоматично, а кожен запис набуває незмінного характеру. Це породжує запитання: хто має нести відповідальність – розробник програмного протоколу, який створив помилковий алгоритм; користувач, що ініціював транзакцію, не усвідомлюючи наслідків; чи аудитор системи, який не виявив потенційних загроз під час перевірки. Така ситуація створює правову невизначеність, що ускладнює застосування традиційних механізмів внутрішнього контролю, аудиту та страхування професійних ризиків.

Окрему групу становлять ризики, пов'язані з колективною природою прийняття рішень у блокчейн-мережах. Алгоритми консенсусу, що забезпечують узгодження транзакцій між вузлами, не передбачають централізованого органу управління, здатного оперативно втрутитися в разі помилки або зловживання. Якщо певна частина учасників мережі об'єднується з метою змінити правила або створити «форк» системи, це може призвести до розходження даних, дублювання записів чи втрати узгодженості між версіями бухгалтерських реєстрів. У таких випадках питання відповідальності за наслідки стає майже нерозв'язним: чи можна покласти провину на групу учасників, що ініціювала зміни, якщо ці дії були підтримані більшістю мережі? Відсутність регламентованого механізму вирішення конфліктів між вузлами зумовлює підвищену вразливість системи в організаційному вимірі.

Додатковим проявом організаційно-інституційних ризиків є складність інтеграції блокчейн-реєстрів у чинні системи управління підприємством і фінансової звітності. Децентралізовані облікові моделі потребують узгодження між різними суб'єктами – бухгалтерами, аудиторами, ІТ-фахівцями, контрагентами та регуляторами. Відсутність єдиного координувального центру породжує ситуацію, коли навіть незначна помилка в параметрах протоколу або у форматі даних може призвести до невідповідності інформації між вузлами. З практичного погляду це означає ризик виникнення розбіжностей у первинних записах, затримок у формуванні звітності, а також втрату довіри до даних, що обертається фінансовими наслідками для підприємства.

Організаційна невизначеність тісно переплітається з правовими ризиками. У більшості національних систем права наразі відсутні чіткі норми, що визначають статус учасників блокчейн-мережі як суб'єктів облікових правовідносин. Незрозуміло, чи може розробник протоколу нести юридичну відповідальність за наслідки його використання, чи визнається блокчейн-запис офіційним доказом у суді, а також як має забезпечуватися відповідність операцій вимогам фінансового контролю. У результаті формуються «сірі зони» у сфері правозастосування, що можуть бути використані для уникнення відповідальності або маніпуляцій з обліковими даними.

Невизначеність щодо розподілу ролей і відповідальності негативно впливає і на функцію внутрішнього контролю. У децентралізованій системі немає чітко визначеного контролера, який перевіряє правильність записів до внесення у реєстр, а кожен учасник виконує функцію часткового нагляду лише в межах власного вузла. Це знижує ефективність запобіжних процедур і створює загрозу накопичення неузгоджених або помилкових даних, які потім важко виправити через незмінність блокчейну. У підсумку, організаційно-інституційні ризики проявляються в підвищенні ймовірності технічних, правових та управлінських збоїв, що безпосередньо впливають на достовірність облікової інформації й стійкість системи фінансового управління в умовах цифрової децентралізації.

Безпекові аспекти блокчейн-орієнтованого бухгалтерського обліку формують багатошарову систему захисту, що виходить далеко за межі технічної архітектури мережі [61]. Йдеться не лише про програмно-технічні засоби збереження даних, а й про організаційні, процедурні

та нормативні компоненти, які забезпечують цілісність, достовірність і стійкість облікової інформації. Безпечне функціонування такої системи вимагає створення цілісної політики управління криптографічними ключами, що охоплює процеси їх генерування, зберігання, регулярного оновлення (ротації) та знищення в разі компрометації або втрати чинності. Оскільки саме ключі забезпечують автентичність і підтвердження кожної господарської транзакції, їх захист набуває статусу базового елемента цифрової безпеки. Втрата або несанкціоноване копіювання приватного ключа рівнозначне крадіжці бухгалтерської печатки в традиційному обліку, адже відкриває можливість для фальсифікації записів або несанкціонованого доступу до облікових даних.

У контексті блокчейн-орієнтованих систем важливим є забезпечення автентичності кожної транзакції, що підтверджується електронним підписом учасників мережі. Водночас система має унеможливлювати його компрометацію через повторне використання ключів, фішингові атаки або маніпуляції в середовищі користувача. Тому безпека транзакцій потребує комплексного підходу: криптографічного захисту з боку системи, належної кібергігієни з боку користувача і постійного моніторингу мережевих аномалій з боку адміністратора. Для підприємств, що інтегрують свої облікові платформи з блокчейн-мережами, необхідним стає впровадження багаторівневої моделі захисту. Вона має охоплювати мережеву безпеку (захист каналів зв'язку та серверної інфраструктури), шифрування даних під час їх передавання та зберігання, автентифікацію користувачів із використанням кількох рівнів підтвердження особи, а також систему журналювання доступів для фіксування всіх спроб взаємодії з обліковими записами.

Особливої уваги потребує захист облікової інформації від внутрішніх загроз, що часто є не менш небезпечними, ніж зовнішні атаки. У децентралізованому середовищі немає центрального адміністратора, який би повністю контролював дії користувачів, тому контроль за безпекою має бути розподіленим і багатовимірним. Організаційна складова передбачає впровадження принципу розподілу повноважень – жоден користувач не повинен мати змоги самостійно ініціювати й затвердити важливу транзакцію без підтвердження іншого учасника. Впровадження процедур багатофакторного підтвердження, ведення журналів змін, систем сповіщення про аномальні дії користувачів, а

також постійний аудит внутрішніх операцій сприяють мінімізації ризиків зловживань. Такий підхід дає змогу перетворити систему з реактивної, яка лише фіксує порушення, на проактивну, здатну запобігати їм у реальному часі.

Стійкість і надійність облікового середовища визначаються також його готовністю до реагування на інциденти та надзвичайні ситуації. Жодна система, навіть найзахищеніша, не може бути повністю ізольованою від ризику технічних збоїв або цілеспрямованих кібернападів. Тому безпечне функціонування блокчейн-обліку передбачає створення механізмів резервного копіювання даних, що забезпечують можливість відновлення ланцюга транзакцій у разі часткової втрати вузлів або пошкодження інформаційних блоків. Планування безперервності роботи містить не лише технічні дії, а й розроблення детальних протоколів реагування – визначення відповідальних осіб, каналів комунікації, порядку ізоляції уражених вузлів та відновлення функціонування мережі. Такі заходи формують основу для побудови системи інформаційної стійкості, здатної швидко повернутися до нормального режиму навіть після масштабного інциденту.

У корпоративному вимірі питання безпеки блокчейн-орієнтованого обліку має бути інтегрованим у загальну систему управління підприємством. Це потребує створення спеціалізованих підрозділів або визначення уповноважених осіб, відповідальних за контроль інформаційної безпеки облікових процесів, проведення аудиту цифрової інфраструктури, тестування вразливостей і навчання персоналу. Ефективна безпекова політика повинна поєднувати технічні засоби захисту з управлінськими процедурами, нормативним регулюванням і підвищенням цифрової компетентності працівників [61; 62]. У підсумку, безпека блокчейн-орієнтованого бухгалтерського обліку постає не лише як технічна функція, а як системоутворювальний чинник довіри до фінансової інформації, що забезпечує стабільність, легітимність і достовірність цифрової економіки загалом.

Етичні виклики, що постають перед бухгалтерією в умовах впровадження блокчейн-технологій та автоматизованих виконавчих механізмів (зокрема смартконтрактів), мають фундаментальний характер і вимагають переосмислення меж людської відповідальності (табл. 3.3).

Таблиця 3.3 – Характеристика етичних викликів функціонування бухгалтерського обліку на засадах блокчейн-технологій

Етичний виклик	Характеристика етичного виклику	Етичне значення для бухгалтерського обліку
1	2	3
Автономність смартконтрактів і зменшення людської участі	Смартконтракти виконують дії без втручання людини, що може призводити до результатів, які суперечать економічній сутності операції або принципам справедливості	Потребує переосмислення меж професійної відповідальності бухгалтера як інтерпретатора економічних фактів, а не лише спостерігача технічних процесів
Розподіл відповідальності між учасниками цифрових процесів	Виникає невизначеність, хто несе відповідальність за дії автоматизованого алгоритму – розробник, користувач, оператор чи замовник	Необхідність нормативного врегулювання обов'язків і механізмів відповідальності за автоматизований облік і виконання договірних зобов'язань
Феномен «технічної правоти»	Операція технічно коректна, але суперечить її економічному змісту або принципу достовірності інформації	Загрожує втраті змістовності облікових даних; бухгалтер має бути гарантом економічного сенсу, а не формальної правильності запису
Нівелювання професійного судження бухгалтера	Надмірна автоматизація зменшує участь фахівця у процесах визнання, оцінки та контролю господарських подій	Призводить до формалізації обліку, втрати аналітичності мислення й ослаблення контролю за достовірністю фінансової звітності
Баланс між технологічною ефективністю та людською відповідальністю	Автоматизація підвищує швидкість і точність обліку, але знижує рівень людського контролю	Необхідність збереження процедурної участі людини в критичних точках процесу: перевірка смартконтрактів, аудит алгоритмів, незалежна експертиза змін
Алгоритмічна упередженість і непрозорість коду	Алгоритми можуть містити неявні упередження, що спричиняють дискримінаційні або несправедливі результати	Потребує від бухгалтера контролю справедливості оброблення даних, ініціювання тестів і забезпечення механізмів оскарження та виправлення упереджених дій

Продовження таблиця 3.3

1	2	3
Принцип прозорості та пояснюваності цифрових систем	Необхідність розуміння не лише результату транзакцій, а й логіки, за якою алгоритм їх здійснює	Формує новий етичний стандарт: бухгалтер відповідає за пояснюваність облікових рішень, джерела даних та обґрунтування дій системи
Недопущення маніпуляцій даними	Можливість навмисного чи випадкового спотворення первинної інформації або умов смартконтрактів	Вимагає дотримання принципів чесності, об'єктивності й активної протидії маніпулятивним практикам у цифровому середовищі
Організаційне забезпечення етичної поведінки	Відсутність усталених політик етичної поведінки під час впровадженні автоматизованих систем	Необхідне створення внутрішніх механізмів: реєстрація смартконтрактів, верифікація операцій, системи «червоних прапорців», людська валідація ризикових дій
Етична компетентність і цифрова освіта бухгалтерів	Класична освіта не охоплює питань алгоритмізації, кіберетики та цифрової безпеки	Вимагає підготовки бухгалтерів нового типу – з технікоетичними компетенціями, здатних критично оцінювати алгоритми та приймати морально зважені рішення
Міждисциплінарна етична взаємодія	Етичні виклики виходять за межі однієї професії та потребують спільних підходів юристів, аудиторів, ІТ-фахівців і регуляторів	Забезпечує системну відповідальність у цифровому обліку, узгоджені стандарти справедливості, прозорості та верифікації даних

Джерело: складено авторами.

Смартконтракти виконують запрограмовані алгоритми без прямої участі людини, отже технічно бездоганна операція може істотно відрізнятися від її економічної сутності або від загальноприйнятих принципів справедливості. Такі розбіжності породжують етичну дилему: чи достатньо апелювати лише до коректності коду, коли наслідком автоматичного виконання є дискримінація контрагентів, умисне обходження регуляторних вимог або непропорційні економічні втрати для однієї зі сторін? Це питання виходить за межі технічної компетенції розробника або системного адміністратора та торкається професійної відповідальності бухгалтера як інтерпретатора економічних фактів.

У центрі цього етичного виклику лежить проблема розподілу відповідальності. Коли автоматичний алгоритм виконує дію, що призводить до порушення законодавства або етичних норм бізнесу, потрібно встановити, хто саме несе відповідальність: автор коду, замовник розгортання рішення, оператор платформи, безпосередній користувач чи суб'єкт, що надав первинні дані. Відповідь не може бути формальною – вона повинна враховувати ступінь контролю над алгоритмом, ступінь можливості передбачення шкідливих наслідків, а також наявність процедур тестування, верифікації та повідомлення про ризики. У цьому сенсі виникає потреба в законодавчому та нормативному врегулюванні, яке б установлювало обов'язки та механізми відповідальності за автоматизований облік і виконання договірних умов.

Поява автоматичного виконання операцій підсилює значення професійної етики цифрового бухгалтера. Ця етика повинна ґрунтуватися на принципах прозорості, недопущення маніпуляцій даними, пріоритету економічного змісту над формальною коректністю запису та на вимозі документованого професійного судження. Прозорість повинна охоплювати не лише видиму історію транзакцій у мережі, а й пояснюваність алгоритмів, логіку прийняття рішень та джерела первинних даних. Недопущення маніпуляцій означає активну протидію навмисним або випадковим спотворенням інформації, що може здійснюватися як на рівні підготовки первинних записів, так і через підлаштовування умов смартконтрактів під певні цілі.

Окремий етичний ризик породжує феномен «технічної правоти» – ситуації, коли операція виконана згідно з алгоритмом і кодом, але суперечить економічній сутності події. Така розбіжність підриває принцип достовірності облікової інформації: бухгалтерський запис перестає відображати реальний економічний зміст і перетворюється на відбиток технічної дії. Вихід унеможливлює лише технічні заходи; потрібна активна позиція бухгалтера як гаранта економічного сенсу операцій, здатного ініціювати перегляд умов, корегування алгоритмів або застосування виняткових регламентів у випадках очевидної невідповідності.

Автоматизація також створює ризик нівелювання професійного судження: коли всі господарські події автоматично відображаються в системі без участі бухгалтера, зменшується простір для аналітичної оцінки, критичного мислення та застосування професійних знань. Наслідком може стати формалізація обліку, коли документи та записи

генеруються і верифікуються алгоритмічно, але без належного аналізу їхньої економічної логіки. Це підриває якість фінансової звітності та підвищує ймовірність системних помилок, що залишаються непоміченими до моменту їхнього матеріалізування у вигляді збитків або правових претензій [29].

З огляду на вищезазначене етичний аспект полягає також у збереженні балансу між технологічною ефективністю та людською відповідальністю. Бухгалтер повинен залишатися остаточним гарантом достовірності та осмисленості даних. Це означає формування професійних стандартів, які зобов'язують забезпечувати процедурну участь людини в критичних точках процесу: атестація підготовлених шаблонів смартконтрактів, перевірка невідповідностей між кодом та економічною логікою, регулярний аудит алгоритмів і незалежне експертне оцінювання змін у правилах їхньої роботи.

Етичні виклики пов'язані також із проблемою алгоритмічної упередженості та непрозорості коду. Смартконтракти й механізми обробки даних можуть містити упередження, що призводять до нерівного ставлення до контрагентів або до непропорційних наслідків для вразливих учасників ринку. У цьому контексті бухгалтеру належить роль контролера не лише кількісної точності, але й справедливості обробки: оцінювання ризиків упередженості, ініціювання тестів на різні сценарії, забезпечення механізмів оскарження та відкату операцій у разі виявлення неправомірностей.

Важливо виробити організаційні механізми, що підтримують етичну поведінку в цифровому обліку. До таких механізмів належать політики належної уваги під час впровадження автоматизованих систем, обов'язкова реєстрація і версифікація смартконтрактів у внутрішніх реєстрах, встановлення процедур «червоних прапорців» для нетипових операцій, а також вимога наявності людської валідації для операцій понад певного ризикового порога. Корпоративні правила повинні фіксувати обов'язки щодо своєчасного інформування регуляторів і зацікавлених сторін про передбачувані та фактичні наслідки застосування автоматизованих рішень.

Професійна освіта і сертифікація цифрових бухгалтерів мають бути адаптовані до нових вимог: наряду з класичними знаннями з обліку, аудиту та права, потрібні компетенції з інформаційної безпеки, базового розуміння алгоритмів та принципів розробки смартконтрактів,

а також навички етичного аналізу та управління ризиками [17]. Така освіта дасть змогу фахівцям не лише інтерпретувати висновки системи, а й визначати межі її застосування, здійснювати незалежний контроль та ухвалювати етичні рішення в неоднозначних ситуаціях.

Нарешті, для ефективного подолання етичних викликів необхідне міждисциплінарне співробітництво між бухгалтерами, юристами, розробниками, аудиторами та регуляторами. Лише узгоджені підходи до нормотворення, стандартизації форматів даних, протоколів верифікації і процедур розслідування забезпечать справжню відповідальність у цифровому обліку. У підсумку, етична трансформація бухгалтерії в умовах блокчейн-орієнтованих систем – це не відмова від автоматизації, а побудова нової парадигми професійної відповідальності, яка гарантує, що технологічна точність завжди підпорядкована економічній правді та загальноприйнятим етичним нормам.

Отже, блокчейн-орієнтований облік формує нову систему взаємопов’язаних ризиків та етичних викликів, що виходять за межі традиційного уявлення про бухгалтерську діяльність. Його надійність та етична легітимність залежатимуть від того, наскільки вдало буде вибудувано баланс між технологічною довершеністю, організаційним контролем та моральною відповідальністю професійної спільноти. У майбутньому роль бухгалтера в такій системі визначатиметься не лише здатністю працювати з цифровими інструментами, а й умінням забезпечити гармонію між безпекою, довірою й етикою в глобальному цифровому обліковому середовищі.

3.3. Перспективи розвитку нормативно-правового забезпечення та професійних стандартів у сфері децентралізованого обліку

Розвиток нормативно-правового забезпечення бухгалтерського обліку в умовах цифрової децентралізації постає одним із ключових чинників інтеграції блокчейн-технологій у систему регулювання фінансово-економічних процесів. Децентралізований характер реєстрів, відсутність єдиного контролювального центру та автономність виконання смартконтрактів зумовлюють необхідність переосмислення традиційних підходів до регламентації облікових процедур, визначення

правового статусу цифрових активів, а також встановлення стандартів достовірності, автентичності та юридичної сили даних, зафіксованих у блокчейн-мережі. Зазначені зміни не можуть бути локальними або фрагментарними – вони мають охоплювати як систему національного законодавства, так і методологічну основу професійних стандартів бухгалтерської діяльності.

Першочерговим напрямом нормативного розвитку є чітке унормування статусу записів у розподілених реєстрах як офіційних доказових джерел бухгалтерської інформації, оскільки юридичне визнання таких записів визначає їх застосування у звітності, податкових відносинах, судовій практиці та аудиторських процедурах. Незмінність записів у блокчейн-системах потенційно підвищує надійність та довіру до облікових даних, однак для переходу від технічної можливості до правової сили потрібні ясні критерії автентичності, цілісності та походження інформації. Нормативні положення мають встановлювати, які елементи транзакції визнаються як первинні дані (наприклад, повний текст операції, підпис автора, часовий маркер, метадані) та як ці елементи документально фіксуються й зберігаються з урахуванням вимог законодавства про облік та архівування.

Критерії автентичності електронних транзакцій повинні базуватися на поєднанні криптографічних засобів та організаційних гарантій. Законодавство має визначити вимоги до застосовуваних засобів електронного підпису, процедури управління ключами, механізмів довірчої інфраструктури (сертифікаційних центрів) та умов, за яких цифровий підпис або інший криптографічний маркер прирівнюється до підпису фізичної особи чи печатки організації. Окремо потрібно врегулювати вимоги до часових міток і синхронізації часу, оскільки точне та неминуче встановлення моменту виникнення облікового факту є ключовим для визначення порядку віднесення операцій до звітних періодів і для розв’язання суперечок про пріоритети транзакцій.

Юридичне визнання записів у розподіленому реєстрі вимагає також визначення носіїв доказів і процедур їх пред’явлення у правових відносинах. Потрібно встановити порядок формування представницьких доказових комплектів: як отримується і надається доказ походження запису (наприклад, повний блок, хеш-ланцюжок, меркл-доказ), які формати прийнятні для суду і які додаткові сертифікати або атестації повинні супроводжувати такі дані. Водночас треба врегулювати,

як здійснюється верифікація записів, хто має право проводити незалежну перевірку цілісності й достовірності записів у мережі, та які наслідки має встановлення факту фальсифікації або технічної помилки.

Питання архівування та збереження первинних документів у контексті блокчейн-систем набуває специфічного характеру: незмінність запису не звільняє від вимог щодо збереження повних первинних даних, доступності для перевірок і забезпечення можливості відновлення інформації у випадку втрати локальних даних. Норматив має окреслити вимоги до місця зберігання метаданих і відомостей, що не містяться безпосередньо в блокчейні (наприклад, скан-копії додаткових документів), а також процедури їх зв'язування з ончейн-записами. Важливо запропонувати засади офіційного архівування, які враховують як технічну неможливість змінювати вже зафіксовані блоки, так і потребу в законних механізмах доступу, редагування чи видалення інформації у випадках, передбачених правом (наприклад, правом на видалення, виправлення помилок).

Нормативні акти повинні диференціювати підходи до публічних і приватних мереж, оскільки ступінь децентралізації, наявність уповноважених валідаторів і правила консенсусу визначають ризики довіри й легітимності записів. Для приватних або консорціумних мереж може бути доцільним встановлення вимог до реєстрації операторів мережі, процедури акредитації вузлів та обов'язкових аудитів інфраструктури. Закон має передбачати механізми відповідальності операторів та учасників мережі за забезпечення цілісності даних, а також процедури повідомлення й виправлення технічних збоїв, які можуть вплинути на правовий статус записів.

Важливим елементом є визначення механізмів аудиторського підтвердження облікових фактів, зафіксованих у блокчейн-середовищі. Аудиторські стандарти мають бути доповнені методиками перевірки розподілених реєстрів: порядком формування вибірки для тестування ончейн-транзакцій, критеріями оцінювання систем внутрішнього контролю, процедурами підтвердження джерел первинних даних та стандартами документування висновків аудитора. Це охоплює запровадження вимоги до надання криптографічних доказів (наприклад, доказів долучення транзакції у блок, відповідних хешів, сертифікатів часу) та встановлення форм взаємодії між аудиторами, операторами мережі й регуляторами під час проведення перевірок.

Потрібно також розробити норми щодо сертифікації програмного забезпечення та смартконтрактів, які використовуються для автоматичного проведення облікових операцій. Встановлення вимог до тестування коду, аудиту безпеки, процесу внесення змін і ведення реєстру версій дасть змогу знизити ризики, пов'язані з технічними помилками або зловмисними модифікаціями. Регуляторні положення можуть передбачати обов'язок забезпечити публічну декларацію логіки смартконтракту у формі, зрозумілій для фахівців з обліку та права, а також механізми зупинки або відкату операцій у випадках системних збоїв чи виявлених протиправних наслідків.

Крім того, нормативні підходи мають враховувати міжнародні та міжгалузеві аспекти: транскордонний характер блокчейн-транзакцій ставить питання щодо застосовності національних норм і узгодження процедур взаємного визнання доказів. Важливо передбачити правила взаємодії з іноземними реєстрами, уніфіковані формати обміну даними та правові механізми визнання ончейн-записів, щоб забезпечити юридичну визначеність у міжнародних операціях.

У підсумку, формування нормативних положень щодо статусу записів у розподілених реєстрах має поєднувати технічні стандарти криптографічної автентифікації та часової фіксації з організаційними вимогами архівування, сертифікації, аудиту та відповідальності учасників мережі. Така система регулювання має забезпечити правову визначеність, практичну реалізацію записів у бухгалтерському обліку та довіру зацікавлених сторін, зберігаючи водночас баланс між захистом правової безпеки й інноваційним розвитком цифрових реєстрів.

Подальший розвиток правового поля вимагає системного підходу до захисту персональних даних, комерційної таємниці та конфіденційної інформації в середовищі розподіленого зберігання, оскільки технічні властивості блокчейн-систем – незмінність записів, розподіл даних по вузлах та неможливість централізованого вилучення інформації – створюють якісно нові ризики для суб'єктів господарювання та фізичних осіб. Нормативні акти мають прямо визнавати особливість ончейн-даних і встановлювати вимоги не лише до змісту та формату збережених даних, а й до способів їх обробки, доступу й контролю, враховуючи, що традиційні механізми «видалення» або «зміни» записів технічно ускладнені або неможливі. У цьому контексті законодавство повинно оперувати поняттями, що відображають специфіку розподілених реєстрів, і визначати допустимі практики обробки чутливої інформації.

Правове врегулювання має встановити чіткі межі відповідальності учасників мережі: власників і розпорядників даних, операторів вузлів (валідаторів), розробників програмного забезпечення та користувачів, які ініціюють транзакції. Для кожної з цих категорій потрібно закріпити обов'язки щодо забезпечення конфіденційності, цілісності й доступності інформації, відповідні механізми управління ключами та процедури реагування на інциденти. Законодавчі норми повинні визначати, у яких випадках відповідальність лежить на тому, хто ініціював внесення даних, а в яких – на тих, хто відповідає за інфраструктуру зберігання й обробки; водночас потрібно передбачити принципи встановлення вини з урахуванням можливості прогнозування шкоди та ступеня контролю над технологічним процесом.

З метою захисту персональних даних потрібно імплементувати принцип мінімізації даних: норматив має вимагати обмеження обсягу та деталізацію інформації, що заноситься в розподілений реєстр, застосовуючи псевдонімізацію, криптографічні маркери або зберігання чутливих елементів офчейн з посиланням (хешем) в ончейні. Такий підхід дає змогу поєднати збереження доказової цінності запису з дотриманням прав суб'єктів даних, зокрема прав на доступ, виправлення і видалення інформації, що вимагає розроблення спеціалізованих процедур реалізації права на «видалення» в рамках децентралізованих систем – наприклад, через видалення офчейн-джерел та інвалідацію відповідних посилань ончейн.

Норматив має регламентувати механізми контролю доступу в децентралізованих середовищах. Це передбачає встановлення вимог до схем управління криптографічними ключами, процедур мультипідписів для критичних операцій, правил акредитації вузлів, а також обов'язкових політик зберігання ключів і їх резервного копіювання. Окрему увагу потрібно приділити питанням розподілу повноважень і ролей, щоб уникнути ситуацій, коли кожен вузол одночасно є носієм даних і потенційним джерелом витоку інформації; регуляторні інструменти можуть вимагати впровадження технічних та організаційних бар'єрів, що обмежують необґрунтований доступ до чутливих полів записів.

Питання знищення або модифікації інформації у випадках, передбачених законодавством, вимагають розробки спеціальних процедур та технічних механізмів. Оскільки пряме видалення ончейн-записів є

проблематичним, законодавець може передбачити допустимі сценарії, наприклад: зберігання чутливої інформації офчейн з контролем доступу та її фізичне знищення за запитом; створення механізмів «анкерації» з можливістю інвалідації посилань; застосування криптографічного шифрування з подальшим знищенням ключів як способу ефективного «розкодування» запису. Закон має врегулювати правові наслідки таких дій, визначити процедури підтвердження знищення та порядок інформування зацікавлених сторін і регуляторів.

Відсутність чітких юридичних норм щодо обробки конфіденційної інформації в децентралізованих реєстрах створює ризики для правової визначеності господарських відносин і надійності доказової бази. Судова практика може зіткнутися з проблемою прийнятності ончейн-доказів, якщо не будуть встановлені стандарти формування та пред'явлення доказових комплектів, процедур їх верифікації та атестації. Тому нормативні акти повинні визначати допустимі формати доказів, порядок залучення технічних експертів, стандарти оформлення супровідних сертифікатів та процедури офіційної верифікації походження й цілісності даних.

З метою мінімізації правових ризиків доцільно ввести вимоги щодо обов'язкової оцінки впливу обробки даних (перед впровадженням системи) та періодичних аудитів безпеки і відповідності. Такі оцінки мають охоплювати аналіз ризиків для конфіденційності й цілісності, сценарії побічних витоків інформації внаслідок збоїв консенсусу або несанкціонованого доступу до вузлів, а також заходи пом'якшення таких ризиків. Норматив мусить передбачати обов'язок повідомлення про інциденти та механізми компенсації збитків суб'єктам, постраждалим від порушення захисту даних.

Особливу увагу потрібно приділити транскордонним аспектам обігу даних: правила експорту, доступу іноземних юрисдикцій, судових запитів і міжнародної взаємодопомоги повинні бути узгоджені з урахуванням розподіленого розміщення вузлів та можливості доступу до реєстрів з різних країн. Законодавство має визначити процедури координації з іноземними регуляторами, стандарти взаємного визнання доказів та правила, що дають змогу балансувати між забезпеченням доступу правоохоронних органів і захистом прав суб'єктів даних.

Нарешті, ефективне правове регулювання захисту даних у децентралізованих системах неможливе без міждисциплінарного підходу й

участі зацікавлених сторін: законодавців, суддів, розробників, експертів із кібербезпеки, представників бізнесу та громадськості. Потрібно створити механізми консультацій, атестацій і стандартизації, які дадуть змогу оперативно адаптувати правові вимоги до технічних змін, забезпечити прозорість процедур і сформувати довіру до розподілених реєстрів як надійного джерела бухгалтерської інформації в правовому полі.

Формування національних положень (стандартів) бухгалтерського обліку, здатних відобразити специфіку функціонування розподілених цифрових систем, є одним із ключових напрямів розвитку сучасної методології обліку в умовах цифрової децентралізації. Традиційна модель облікового процесу, заснована на централізованому документообігу, передбачає наявність єдиного сховища даних, контрольованого визначеним суб'єктом, що забезпечує створення, оброблення та архівування первинних документів. Однак поява блокчейн-технологій радикально змінює цю парадигму: облікові записи формуються одночасно в багатьох вузлах мережі, підтверджуються через алгоритми консенсусу, а перевірка достовірності здійснюється не адміністративно, а криптографічно. У таких умовах постає потреба в переосмисленні базових засад нормативного регулювання бухгалтерського обліку – від визнання фактів господарського життя до формування фінансової звітності.

Наявні національні положення (стандарти) бухгалтерського обліку, методичні рекомендації та інструкції не враховують особливостей автоматизованого виконання умов договорів (смартконтрактів), токенізації активів і зобов'язань, часткової автономності транзакцій та їх автоматичного документування в межах блокчейн-мережі. Наприклад, у разі коли господарська операція ініціюється та завершується без прямого втручання людини, постає питання про момент її визнання в обліку, а також про документ, що підтверджує її здійснення. Відсутність нормативно визначеного підходу до таких операцій ускладнює застосування єдиних методів оцінювання, відображення та розкриття інформації. Тому національні стандарти мають бути доповнені положеннями, які враховуватимуть технічну специфіку розподілених систем, визначаючи порядок підтвердження та документування фактів господарської діяльності, зафіксованих у блокчейні.

Особливого значення набуває визначення облікових критеріїв для цифрових активів і токенізованих ресурсів, які можуть бути як об'єктами інвестування, так і засобом розрахунків або елементом корпоративного управління. Питання ідентифікації цих об'єктів, їх класифікації як нематеріальних активів, фінансових інструментів чи запасів потребує методологічного узгодження з положеннями міжнародних стандартів, але з урахуванням національних реалій правового визнання цифрових форм власності. До того ж має бути нормативно визначено порядок оцінювання таких активів – первісного, справедливого, переоціненого – залежно від типу операції, ступеня ліквідності токенів і наявності ринкових котирувань. Це вимагатиме чітких інструкцій щодо визначення джерел інформації про ринкову вартість, її верифікації та аудиторського підтвердження.

З огляду на трансформацію облікового середовища, доцільним є розроблення комплексного нормативного документа – спеціалізованого національного положення (стандарту) бухгалтерського обліку «Облік операцій у розподілених цифрових реєстрах». Такий стандарт мав би забезпечити єдність підходів до класифікації, документування, визнання та відображення операцій у децентралізованих системах. Він повинен визначати принципи побудови облікової політики для суб'єктів, які використовують блокчейн як технологічну основу облікової інфраструктури, зокрема встановлювати порядок підтвердження автентичності записів, вимоги до електронних підписів, процедури перевірки цілісності даних і способи формування аудиторських доказів на підставі блокчейн-записів. Невід'ємною складовою такого стандарту мають стати правила обліку смартконтрактів, які, будучи самовиконуваними цифровими угодами, поєднують правову й облікову функцію, що зумовлює потребу у фіксації їх статусу як первинних документів та одночасно як елементів облікового запису.

Методологічна система, що регулюватиме облік у розподілених цифрових середовищах, має також передбачати вимоги до розкриття інформації у фінансовій звітності. Вона повинна містити положення щодо опису застосовуваних технологічних рішень, характеристик цифрових активів, способів управління ризиками, пов'язаними з автоматизацією транзакцій, а також рівня контролю, який здійснює підприємство над алгоритмами смартконтрактів. Це забезпечить прозорість звітності та підвищить рівень довіри користувачів до даних, сформованих у децентралізованому середовищі.

Водночас формування нового стандарту вимагає узгодження із суміжними нормативними сферами – цивільним, фінансовим, податковим та інформаційним правом, оскільки блокчейн-технології створюють міждисциплінарне поле регулювання. Зокрема, облік операцій із токенами, що мають ознаки фінансових інструментів, повинен узгоджуватися з вимогами регулятора ринку капіталу, а порядок обліку цифрових активів – із положеннями податкового законодавства щодо визначення доходів і витрат, пов'язаних із їх обігом. Так, новий стандарт має виконувати функцію методологічного містка між бухгалтерською практикою та цифровими технологіями, створюючи підґрунтя для правової визначеності, стабільності звітності й підвищення інституційної довіри до даних, сформованих у блокчейн-середовищі.

Розроблення національного стандарту «Облік операцій у розподілених цифрових реєстрах» стане важливим кроком до систематизації теоретичних і практичних підходів до бухгалтерського обліку в умовах цифрової децентралізації. Його впровадження сприятиме формуванню єдиної нормативної бази для суб'єктів господарювання, що застосовують блокчейн, забезпечить узгодженість між технологічними процесами та обліковими принципами, а також створить умови для інтеграції української облікової системи в глобальний цифровий простір на засадах прозорості, безпеки та достовірності облікових даних.

Розбудова нормативного простору децентралізованого обліку має ґрунтуватися на принципі гармонізації з міжнародними регуляторними ініціативами, оскільки блокчейн-системи за своєю сутністю є міжнародними і вимагають узгоджених підходів для забезпечення порівнянності й прийнятності даних у транснаціональних операціях. Узгодження національних норм із положеннями Міжнародних стандартів фінансової звітності, документами Ради з міжнародних стандартів бухгалтерського обліку та рекомендаціями органів, що регулюють цифрові ринки, створює основу для забезпечення єдності принципів визнання, оцінювання й розкриття інформації про цифрові активи та операції, здійснені в розподілених реєстрах. Це узгодження сприяє збереженню порівнянності фінансової звітності, полегшує проведення аудиту та підвищує довіру інвесторів і контрагентів до інформації, сформованої з використанням децентралізованих технологій.

Водночас гармонізація не може і не повинна бути механічним запозиченням іноземних норм: її потрібно здійснювати з урахуванням

національної правової традиції, економічних умов, структури національних ринків та специфіки регулювання цифрових активів. Це означає принципово важливий підхід інтеграції міжнародних принципів у локальний контекст – із визначенням ключових концептів, адаптацією процедур визнання та оцінювання, а також зі створенням перехідних механізмів, які дадуть змогу суб'єктам господарювання поступово пристосувати облікові політики та внутрішні контрольно-аудиторські процедури до нових вимог. Такий підхід мінімізує ризики юридичної невизначеності та регуляторної конфліктності в період трансформації системи обліку.

Особливу увагу під час гармонізації потрібно приділити технічній сумісності та стандартам обміну даними. Для забезпечення взаємопроникнення облікових систем, які спираються на різні архітектури розподілених реєстрів, потрібні уніфіковані формати записів, стандартизовані метадані, методики формування доказових комплектів (наприклад, формати для представлення хеш-ланцюжків, меркл-доказів та часових міток) і загальні протоколи доступу до ончейн- і офчейн-джерел. Міжнародні й національні регулятори мають сприяти розробленню таких технічних стандартів у співпраці з ІТ-спільнотою та професійними організаціями бухгалтерів, що дасть змогу зменшити трансакційні витрати і підвищити оперативність аудиторських процедур у кросбордерних ситуаціях.

Гармонізація також повинна враховувати суміжні правові сфери: податкове регулювання, право власності, договірне право, антимонопольне та банківське регулювання, а також норми щодо захисту персональних даних. Узгоджені підходи до класифікації цифрових активів, їхнього оподаткування та правового статусу дадуть змогу уникнути ситуацій подвійного оподаткування або правових колізій, що негативно впливають на інвестиційний клімат. У зв'язку з цим корисним є впровадження міжнародних угод або меморандумів про взаємне визнання певних правил і доказів, а також активна участь у роботі міжнародних ініціатив з метою вироблення узгоджених підходів.

Практичне впровадження гармонізації повинно супроводжуватися створенням гнучких механізмів перегляду і тестування нормативів: пілотні проєкти та співпраця з експертними групами дадуть змогу оцінити ефективність норм у реальних умовах і оперативно виправляти недоліки. Такі механізми мають охоплювати процедури сертифікації

програмних продуктів і смартконтрактів, стандарти аудиту алгоритмів і правила спільної роботи аудитора, розробників і регулятора під час розслідування інцидентів. Це зменшить ризики, пов'язані з помилками в коді або недоліками систем внутрішнього контролю, та сприятиме формуванню довіри до нових практик.

Не менш важливою є кадрова та інституційна підготовка: професійні організації, вищі навчальні заклади та регулятори мають координувати програми навчання, перекваліфікації та сертифікації, що забезпечать розуміння міжнародних стандартів у поєднанні з локальними особливостями. Така підготовка повинна охоплювати як методологічні аспекти обліку й аудиту, так і технічні компетенції щодо роботи з розподіленими реєстрами та криптографічними доказами. Підвищення професійного рівня сприятиме більш ефективному імплементуванню гармонізованих норм у практику.

Ефективна гармонізація національного нормативного простору з міжнародними ініціативами має поєднувати принципову узгодженість із адаптивністю до національного контексту, технічну уніфікацію форматів і протоколів обміну даними, міжгалузеву координацію правового регулювання та активні заходи з тестування й навчання фахівців. Лише такий комплексний підхід забезпечить сумісність облікових даних у міжнародному обміні, сприятиме спрощенню аудиторських процедур і зміцненню довіри інвесторів до інформації, що генерується в умовах цифрової децентралізації.

Особливе місце в процесі становлення нормативного поля децентралізованого обліку посідає формування нових професійних стандартів та етичного кодексу цифрового бухгалтера, що визначатимуть основи професійної ідентичності фахівця в умовах глибокої автоматизації облікових процесів. Технологічна трансформація, зумовлена впровадженням блокчейн-технологій, призводить до зміни сутності професійних завдань бухгалтера: від рутинного виконання облікових операцій до стратегічного управління інформаційними потоками, аналізу алгоритмічних ризиків і забезпечення достовірності даних, створюваних автоматизованими системами. У цих умовах професійні стандарти мають охоплювати не лише традиційні компетентності у сфері обліку, фінансової звітності й аудиту, а й нові вимоги, пов'язані з цифровою компетентністю, розумінням принципів функціонування

розподілених систем та здатністю до контролю алгоритмічних процесів, що формують облікові записи.

Ключовим завданням нових професійних стандартів є переорієнтація ролі бухгалтера з виконавця технічних операцій на аналітика й етичного арбітра, відповідального за змістовну достовірність і справедливість облікових даних. Автоматизація, незважаючи на свою ефективність, не усуває потреби в людському судженні, адже саме людина несе відповідальність за тлумачення економічної сутності операцій, їх правову обґрунтованість та етичну прийнятність. У цьому контексті професійні стандарти мають встановити вимоги до здатності бухгалтера оцінювати ризики алгоритмічних помилок, перевіряти адекватність моделей обробки даних, здійснювати аудит смартконтрактів і контролювати правильність їх виконання з погляду економічного змісту. Особливу увагу потрібно приділяти навичкам аналізу цифрових доказів, розумінню принципів криптографічної верифікації транзакцій, умінню виявляти потенційні загрози маніпуляції інформацією в блокчейн-середовищі.

Етичні принципи діяльності цифрового бухгалтера повинні гарантувати збереження людської відповідальності за наслідки облікових рішень. У системах, де автоматизовані алгоритми приймають рішення на основі закладених логічних правил, існує небезпека зниження усвідомленої участі людини в процесі формування фінансової інформації. Тому професійна етика має визначати межі застосування автоматизації, вимагати збереження контролю людини над алгоритмічними процесами, а також забезпечувати пріоритет змісту економічної операції над її технічною формою. Недопущення маніпуляцій цифровими даними, захист конфіденційної інформації, неупереджене ставлення до цифрових джерел та обґрунтованість професійних висновків повинні залишатися основоположними моральними орієнтирами в діяльності бухгалтера майбутнього.

Розвиток професійних стандартів неможливий без активної участі професійних об’єднань бухгалтерів та аудиторів, які мають бути провідними ініціаторами розроблення рекомендацій, сертифікаційних програм і методичних матеріалів, спрямованих на підготовку фахівців нового покоління. У цьому процесі важливо забезпечити співпрацю з державними регуляторами, науковими установами та представниками

ІТ-сфери, що дасть змогу поєднати теоретичні принципи облікової науки з практичними потребами цифрової економіки. Визначальним напрямом має стати розроблення програм підвищення кваліфікації, що поєднуватимуть знання з бухгалтерського обліку, права, кібербезпеки та аналітики даних, формуючи інтегровану модель компетентності цифрового бухгалтера.

У перспективі можлива поява нових професійних кваліфікацій, які відображатимуть спеціалізацію у сфері цифрової облікової діяльності. Такі напрями, як «цифровий бухгалтер-аналітик», «експерт із смартконтрактів у бухгалтерському обліку», «аудитор децентралізованих систем» або «фахівець із цифрової звітності та верифікації даних», можуть стати основою для нових освітніх програм і сертифікаційних стандартів. Формування цих спеціалізацій дасть змогу структурувати професійне середовище, підвищити його прозорість і створити передумови для міжнародного визнання компетентності українських фахівців у глобальному цифровому просторі.

Впровадження нових професійних стандартів та етичного кодексу цифрового бухгалтера матиме стратегічне значення для розвитку нормативного поля децентралізованого обліку. Воно сприятиме підвищенню довіри до технологій блокчейн, формуванню стабільного середовища професійної діяльності, а також зміцненню ролі бухгалтера як гаранта достовірності, законності та справедливості фінансової інформації. У результаті облік на засадах блокчейн-технологій зможе розвиватися не лише як технічна інновація, а як соціально відповідальний інститут, заснований на високих етичних принципах, професійній компетентності та науково обґрунтованих стандартах діяльності.

Узагальнюючи викладений вище матеріал, структуруємо його у вигляді систематизації напрямів розвитку нормативно-правового забезпечення бухгалтерського обліку в умовах цифрової децентралізації (табл. 3.4).

Таблиця 3.4 – Основні напрями розвитку нормативно-правового забезпечення бухгалтерського обліку в умовах цифрової децентралізації

Напрям розвитку	Змістовна характеристика	Очікувані результати впливу на систему обліку
1	2	3
Юридичне визнання записів у розподілених реєстрах	Визначення записів у блокчейн-системах як офіційних доказових джерел бухгалтерської інформації. Установлення критеріїв автентичності, цілісності, походження даних, їх фіксації та архівування	Підвищення достовірності облікових даних; забезпечення можливості використання ончейн-записів у звітності, податкових та судових відносинах
Автентичність і правовий статус електронних транзакцій	Нормування застосування електронних підписів, криптографічних засобів, управління ключами, сертифікаційних центрів, часових міток та синхронізації часу	Законодавче прирівнювання цифрових підписів до підписів фізичних осіб; однозначне визначення моменту виникнення облікового факту
Процедури доказування і верифікації ончейн-записів	Визначення порядку формування доказових комплектів (блок, хеш-ланцюг, меркл-доказ), вимоги до форматів для судів, правил перевірки достовірності та наслідків фальсифікації	Формування юридично захищених процедур аудиту і судового використання блокчейн-записів
Архівування та збереження даних у блокчейн-середовищі	Регламентація збереження метаданих, зв’язування ончейн- і офчейн-інформації, порядок доступу, редагування та видалення в передбачених законом випадках	Забезпечення довгострокового збереження даних і правомірного доступу без порушення принципу незмінності блоків
Диференціація вимог до публічних і приватних мереж	Визначення статусу операторів приватних мереж, акредитація вузлів, аудит інфраструктури, відповідальність за технічні збої	Зміцнення довіри до приватних реєстрів; підвищення кіберстійкості облікових систем
Аудиторська верифікація ончейн-операцій	Розроблення методик перевірки транзакцій у розподілених реєстрах, критеріїв внутрішнього контролю, процедур підтвердження даних та надання криптографічних доказів	Стандартизація аудиту децентралізованих систем; забезпечення доказової сили аудиторських висновків

Продовження таблиці 3.4

1	2	3
Сертифікація програмного забезпечення і смартконтрактів	Встановлення вимог до тестування, аудиту безпеки, ведення реєстру версій, публічної декларації логіки смарт-контрактів і механізмів їх зупинки	Зниження ризиків технічних помилок; підвищення правової надійності автоматизованих облікових операцій
Міжнародно-правова інтеграція і транскордонне визнання записів	Узгодження національних норм з іноземними системами, створення уніфікованих форматів обміну даними, взаємне визнання доказів	Забезпечення правової визначеності в міжнародних операціях та спрощення транснаціональних аудитів
Захист персональних і конфіденційних даних	Визначення специфіки ончейн-даних, правил обробки, доступу, контролю, принципів мінімізації даних, псевдонімізації, офчейн-зберігання чутливої інформації	Забезпечення балансу між прозорістю записів і захистом приватності суб'єктів
Механізми знищення або модифікації даних	Розробка технічних сценаріїв для реалізації права на видалення (офчейн-видалення, анкеринг, шифрування зі знищенням ключів)	Реалізація правових гарантій суб'єктів без порушення принципу незмінності блокчейну
Оцінка впливу обробки даних і аудит безпеки	Запровадження обов'язкових оцінок впливу, аудитів відповідності, повідомлень про інциденти та компенсаційних механізмів	Зниження правових ризиків, підвищення кіберстійкості та довіри користувачів
Транскордонне переміщення даних	Регулювання експорту, доступу іноземних юрисдикцій, міжнародної взаємодопомоги та правового захисту суб'єктів даних	Гармонізація правового простору для міжнародного обігу бухгалтерських даних
Міждисциплінарна координація та участь стейкхолдерів	Формування консультаційних і стандартизаційних механізмів за участю законодавців, IT-фахівців, аудиторів, бізнесу та громадськості	Підвищення адаптивності правового поля до технологічних змін; зміцнення інституційної довіри

Продовження таблиці 3.4

1	2	3
Розроблення національного стандарту «Облік операцій у розподілених цифрових реєстрах»	Створення єдиного нормативу, що регламентує класифікацію, документування, оцінювання та відображення операцій у блокчейні, зокрема смартконтракти	Формування методологічної основи обліку в децентралізованих системах; узгодженість з іншими галузями права
Облік і оцінювання цифрових активів та токенізованих ресурсів	Визначення облікових критеріїв, класифікації, методів оцінювання цифрових активів і токенів, узгодження з міжнародними стандартами	Забезпечення достовірного відображення цифрових активів у звітності; підвищення інвестиційної привабливості
Розкриття інформації у фінансовій звітності	Вимоги до опису технологічних рішень, управління ризиками, контролю над алгоритмами та прозорості цифрових процесів	Підвищення довіри користувачів до звітності в децентралізованому середовищі
Гармонізація з міжнародними стандартами	Узгодження НП(С)БО з МСФЗ, документами IASB, рекомендаціями органів цифрового регулювання; технічна уніфікація форматів	Сумісність облікових даних на міжнародному рівні; спрощення аудиту й інвестиційної аналітики
Кадрова і професійна підготовка	Розробка навчальних програм, сертифікаційних курсів, міждисциплінарної підготовки (облік, IT, право, кібербезпека)	Формування компетентного кадрового потенціалу цифрової облікової професії
Професійні стандарти та етичний кодекс цифрового бухгалтера	Визначення нових ролей бухгалтера: аналітик, контролер алгоритмів, аудитор смартконтрактів. Закріплення принципів етичної відповідальності, недопущення маніпуляцій, пріоритету змісту над формою	Підвищення професійної ідентичності бухгалтера; зміцнення довіри до облікових даних у цифровому середовищі
Нові професійні кваліфікації	Введення спеціалізацій: цифровий бухгалтер-аналітик, експерт зі смартконтрактів, аудитор децентралізованих систем, фахівець із цифрової звітності	Формування нових напрямів професійної діяльності; міжнародне визнання компетентностей українських фахівців

Джерело: складено авторами.

Отже, перспективи розвитку нормативно-правового забезпечення та професійних стандартів у сфері децентралізованого обліку визначаються поєднанням правової адаптації, методологічної уніфікації та етичного оновлення. Формування таких засад дасть змогу не лише забезпечити юридичну визначеність і надійність бухгалтерської інформації в умовах цифрової децентралізації, а й створить підґрунтя для нової парадигми бухгалтерського обліку – гнучкої, технологічно інтегрованої та заснованої на довірі до цифрових доказів економічної діяльності.

3.4. Напрями подальшої еволюції облікової науки під впливом цифрової децентралізації

Подальша еволюція облікової науки під впливом цифрової децентралізації визначається глибокими трансформаційними процесами, що відбуваються у глобальній економічній системі. Зміщення акцентів від централізованих форм зберігання, обробки та контролю інформації до децентралізованих, розподілених середовищ зумовлює потребу в перегляді фундаментальних засад бухгалтерського обліку як соціально-економічного інституту. Блокчейн-технології, які забезпечують прозорість, незмінність та верифікованість облікових записів, є не лише технічним інструментом, а й чинником формування нової методологічної парадигми, у якій поняття довіри, істинності та відповідальності набувають нового змісту. У цих умовах облік поступово перетворюється з системи реєстрації господарських операцій на багатовимірну платформу обміну достовірними даними між учасниками економічних процесів, що вимагає узгодження наукових підходів із логікою функціонування цифрового простору.

Наукова еволюція бухгалтерського обліку в умовах цифрової децентралізації має розпочинатися з переосмислення фундаментальних категорій, які лежать в основі облікової теорії. Поняття власності перестає бути однозначно пов’язаним з фізичним носієм або правовою особою; цифрові активи можуть існувати виключно у вигляді записів у розподіленому реєстрі, а право розпорядження такими активами часто прив’язане до контролю над криптографічним ключем. Отже, теоретичні моделі власності мають охоплювати три взаємопов’язані виміри: юридичне право (набори прав, закріплені законом

або договором), фактичний контроль (можливість розпоряджатися активом через володіння засобами доступу) та економічна вигода (потенціал отримання майбутніх економічних вигод). Наукові дослідження повинні з'ясувати пріоритетність і взаємодію цих вимірів у різних правових і технологічних сценаріях, визначити правила встановлення пріоритетів у випадку колізій та розробити критерії для колективного визнання права власності в бухгалтерському обліку.

Категорія контролю в децентралізованих системах також вимагає корекції. Традиційні ознаки контролю – можливість визначати політику використання активу та отримувати переваги від його використання – у цифровому середовищі набувають технічного втілення через механізми управління ключами, ролі учасників мережі, правила консенсусу та наявність модулів управління в смартконтрактах. Наукові підходи мають розробити методи встановлення факту контролю для цілей визнання та відображення активів. Ці питання важливі для визначення моменту відображення активу на балансі, порядку врахування ризиків та формування пов'язаних резервів.

Розгляд ризику в цифровому контексті повинен охоплювати як традиційні економічні ризики, так і специфічні технологічні ризики – ризик компрометації ключів, вразливості смартконтрактів, помилок у логіці автоматичних угод, ризику відключення вузлів або зміни правил консенсусу (форки). Наукові дослідження мають спрямуватися на розроблення моделей кількісної оцінки таких ризиків, методик стрес-тестування облікових систем, а також підходів до капіталізації майбутніх очікуваних збитків, з урахуванням високоінтенсивної волатильності ринкових котирувань цифрових активів. Окремим напрямом є вивчення взаємозв'язку між технічною надійністю платформи та вартістю активів в обліку з метою обґрунтування дисконтних ставок, корегування оцінок та формування страхових механізмів.

Категорія капіталу в цифровому середовищі вимагає нових концептуальних положень. Токенізовані ресурси, права на майбутні потоки, активи, забезпечені даними або інтелектуальною власністю, змінюють природу капіталу: капітал може бути фрагментований, підлягати динамічному переоцінюванню залежно від правил мережі та рівня її прийнятності. Наукові дослідження повинні розробити підходи до розмежування власного та позикового капіталу в умовах, коли токени одночасно виконують функцію платежу, права голосу і джерела доходу (наприклад, через стейкінг або розподіл прибутку). Питання

визнання прибутку пов'язане з моментом виконання смартконтракту, остаточністю транзакції в мережі та відповідністю економічної суті операції – науковцям потрібно запропонувати критерії для визнання доходів, які враховують особливості автоматичного розподілу винагород і можливості їх відкату під час виявлення неспівпадіння з економічним змістом.

Щодо обліку цифрових активів, потрібно формалізувати їхню класифікацію та критерії ідентифікації економічної сутності. На практиці цифрові активи можуть мати ознаки товарів, прав вимоги, фінансових інструментів або нематеріальних активів – і їх класифікація має визначатися не лише за правовою формою, а за економічним змістом і можливостями отримання вигод. Наукові дослідження повинні запропонувати системи класифікації, що враховують ліквідність токенів, наявність вторинних ринків, технологічні ризики та регуляторний статус; розробити методики первісної оцінки, щоденного переоцінювання та документування джерел цінової інформації.

Методи підтвердження права власності у блокчейн-середовищі становлять окрему науково-практичну проблему. Криптографічні докази включно з доказами долучення у блок, хеш-ланцюгами та підтвердженням часу забезпечують технічну верифікацію походження записів; проте для цілей обліку й права важливі також офчейн-докази – договори, реєстраційні записи, рішення судів або сертифікати третіх осіб. Отже, подальші наукові дослідження мають передбачати побудову «пакетів доказів», які поєднують ончейн-елементи з офчейн-атестаціями, визначити стандарти їх оформлення та процедури верифікації, а також розробити правила, які дають змогу бухгалтеру встановлювати достатність доказів для визнання права власності в обліку.

Особливу увагу потрібно приділити ролі програмних агентів та алгоритмів як суб'єктів господарської діяльності. Поява автономних агентів, здатних ініціювати угоди, отримувати винагороди та виконувати розпорядження, ставить питання щодо юридичної правосуб'єктності таких агентів, критеріїв їх ідентифікації у бухгалтерському обліку та порядку віднесення результатів їх діяльності до балансу певного економічного суб'єкта. Наукові дослідження мають запропонувати концептуальні рамки для віднесення дій програмних агентів до конкретних економічних суб'єктів, механізми розподілу відповідальності та методи документування операцій, здійснених автономними алгоритмами.

Для успішного вирішення перелічених завдань потрібна міждисциплінарна дослідницька програма, яка об'єднає фахівців з обліку, права, криптографії, теорії інформації та економіки. Така програма повинна продукувати прикладні методики, моделі оцінювання ризиків, інструменти для формування доказових пакетів, критерії визнання та оцінювання, а також пропозиції до національних стандартів. Водночас важливо розвивати емпіричні дослідження – пілотні проєкти, кейс-стаді та експериментальні впровадження, які дадуть змогу перевірити теоретичні розробки в реальному середовищі та адаптувати методики до практичних викликів цифрової децентралізації.

Розроблення методологічних засад фіксації облікової інформації в розподілених реєстрах вимагає системного переосмислення самих процедур реєстрації, підтвердження та верифікації господарських фактів. У класичній системі подвійного запису кожна операція відображається в парній кореспонденції рахунків у межах одного суб'єкта або між учасниками через централізований обмін документами; у розподіленому середовищі одна й та сама господарська операція може бути одночасно зафіксована в усіх зацікавлених вузлах, утворюючи єдину «спільну книгу обліку». Це змінює логіку облікового запису: замість фіксації двосторонньої бухгалтерської кореспонденції виникає потреба визначити правила генерації, узгодження і міжнародної ідентифікації записів, що забезпечують рівноцінність відображення у всіх учасників.

Принципи визнання господарських фактів мають бути адаптовані до особливостей незмінності та хронологічної впорядкованості записів у розподіленому реєстрі. Потрібно встановити чіткі критерії моменту визнання операції в обліку з урахуванням поняття остаточності транзакції: за відсутності централізованої інстанції остаточність залежить від властивостей мережі та механізмів досягнення консенсусу, що може передбачати затримки або ризик тимчасових розгалужень блокчейну (форків). Методологія повинна визначати, за яких технічно-правових умов запис вважається таким, що надає підстави для відображення в обліку та долучення до звітного періоду.

Питання оцінювання інформації в «спільній книзі» набуває додаткової складності через різнохарактерність об'єктів цифрового обліку і динамічну змінність вартості токенізованих активів. Методики оцінювання мають враховувати джерела вартісної інформації, механізми

її формування в онлайнових ринках, ступінь ліквідності та технологічні ризики, що впливають на реальну економічну корисність активу. Наукові підходи повинні запропонувати алгоритми інтеграції ончейн-ціновихіндикаторів з офчейн-оцінками, правила корекції оцінок у разі технічних інцидентів і процедури документування джерел інформації для цілей аудиту.

Процедури перевірки інформації в умовах багатостороннього запису не можуть обмежуватися класичними методами контролю та звірки документів. Потрібно розвивати методики криптографічної верифікації доказів: формування пакетів доказів, що поєднують ончейн-елементи (хеш-ланцюжки, докази долучення у блок, часові мітки) з офчейн-атестаціями (договірні умови, сертифікати, протоколи операцій). Методологія аудиту має визначити формат таких пакетів, мінімальний набір необхідних доказів для різних категорій операцій та стандарти документування процедур перевірки, включно з порядком залучення технічних експертів у випадках спорів.

Автоматизація синхронності даних істотно знижує потребу в тривалій ручній звірці, але навпаки підвищує вимоги до контролю первинних даних та механізмів управління джерелами інформації. Майбутні наукові дослідження повинні передбачати інструменти контролю на вході: стандарти оформлення первинних записів, процедури валідації даних перед їх ончейн-реплікацією, правила застосування ораклів (постачальників зовнішніх даних) та вимоги до їх сертифікації. Особливу увагу потрібно приділити механізмам розмежування прав і ролей у мережі: хто має право ініціювати запис, хто – підтверджувати, які транзакції вимагають людської валідації і які – автоматичного відпрацювання.

Складовою методології має стати врегулювання процесів обробки спорів. Оскільки блокчейн-фіксація часто є незворотною, потрібно передбачити процедури, які дають змогу документувати помилки, ініціювати компенсаційні записи або застосовувати механізми зміни ончейн-операції за погодженою процедурою (наприклад, через створення коректувальних операцій або активацію механізмів відкату на рівні смартконтракту). Це вимагає взаємодії технічних і правових механізмів – стандарти повинні окреслити порядок фіксації диспутів, часові рамки для їх вирішення та правила відображення наслідків у фінансовій звітності.

Не менш важливою є розробка підходів до безперервного аудиту і реального часу звітності: наукові моделі мають визначити, які елементи облікової інформації можуть підлягати постійному автоматичному моніторингу, а які – вимагатимуть періодичного інструментального огляду [54; 65]. Методологія повинна долучати критерії ризику для автоматичного тригера людської перевірки, стандарти вибіркового тестування ончейн-транзакцій і правила документування висновків аудиту в умовах потокового формування даних.

Нарешті, формування методологічних засад має супроводжуватися створенням стандартизованих форматів метаданих, уніфікованих класифікацій операцій та описів бізнес-процесів, що дасть змогу забезпечити сумісність між різними розподіленими реєстрами і полегшить інтеграцію даних у корпоративні системи обліку. Така стандартизація створить підґрунтя для подальшого розвитку інструментів аналітики, наукового моделювання і порівняльних досліджень, що в підсумку забезпечить перехід від ізольованих пілотних впроваджень до масштабного практичного застосування концепції «спільної книги обліку» в економічному середовищі.

У перспективі розвитку облікової науки виникає потреба у формуванні нової системи теоретичних координат, яка дасть змогу розглядати бухгалтерський облік не лише як інструмент фіксації господарських операцій, а як інтегровану складову комплексної інформаційної екосистеми управління. У такому підході облік стає платформою для узгодження даних між усіма учасниками економічних процесів, поєднуючи фінансові, управлінські, правові та технологічні аспекти. Це передбачає інтеграцію класичних підходів до обліку з новими принципами, що враховують динамічність цифрового середовища, прозорість транзакцій та незмінність розподілених записів. Теоретичні координати повинні забезпечувати цілісність, достовірність і своєчасність інформації, формуючи основу для прийняття управлінських рішень у реальному часі.

Розвиток технологій штучного інтелекту, машинного навчання та смартконтрактів створює передумови для появи концепції «самооновлюваного обліку», у межах якої облікові дані формуються автоматично на основі алгоритмів, здатних адаптуватися до змін у господарському середовищі. Така автоматизація забезпечує миттєве відображення операцій, усуваючи затримки, характерні для традиційних

систем, та знижуючи ймовірність помилок у процесі введення інформації. Водночас вона висуває нові вимоги до наукового осмислення обліку: потрібно розробити механізми контролю за правильністю алгоритмів, перевірки достовірності вхідних даних та захисту від технічних або логічних викривлень інформації.

Одним із ключових завдань науки стає визначення ролі людського контролю в умовах автономного функціонування цифрових платформ. Навіть за високого рівня автоматизації бухгалтер повинен залишатися гарантом достовірності даних, здатним оцінювати економічний зміст операцій, виявляти потенційні ризики та контролювати етичні аспекти виконання смартконтрактів. Це вимагає розроблення методологій поєднання автоматизованих процесів із процедурою аналітичної верифікації, визначення критичних точок втручання людини та встановлення правил реакції на аномалії або конфлікти в даних.

Наукові дослідження в цьому напрямі повинні охоплювати питання надійності систем самооновлюваного обліку, зокрема оцінку алгоритмічних ризиків, вразливості криптографічних механізмів та потенційні загрози з боку зовнішніх або внутрішніх акторів. Важливим є розроблення стандартів та процедур аудиту автономних облікових платформ, що дасть змогу не лише підтвердити достовірність даних, але й забезпечити юридичну та етичну відповідність облікової інформації.

Еволюція облікової науки в контексті цифрової децентралізації орієнтується на побудову системи, в якій технологічні інновації та класичні принципи бухгалтерського обліку взаємодіють гармонійно, забезпечуючи цілісність, прозорість і надійність інформації. Ця інтеграція відкриває перспективи для створення нових наукових парадигм, методик управління цифровими активами, стандартів оцінювання та верифікації інформації, а також формує підґрунтя для підготовки фахівців, здатних працювати в середовищі високої автоматизації, зберігаючи відповідальність за змістовну достовірність облікових даних.

У контексті цифрової децентралізації виникає принципова потреба в переосмисленні сутності бухгалтерської звітності як кінцевого продукту облікового процесу. Традиційна концепція, орієнтована на періодичне формування звітів за визначеними проміжками часу, в децентралізованому середовищі поступово втрачає свою первинну значущість. Фінансова інформація може бути доступною в режимі реального

часу для всіх учасників мережі, що дає змогу одержувати актуальні дані про стан активів, зобов'язань та результатів діяльності без потреби очікування формальних звітних дат. Це створює фундамент для побудови «живої» бухгалтерської звітності, яка постійно оновлюється та відображає фактичний стан господарських процесів.

Наукове осмислення таких змін вимагає розроблення нових підходів до структурування та узагальнення інформації. Потрібно визначити принципи агрегування даних у цифровому середовищі, порядок формування ключових показників та алгоритми перетворення великих обсягів транзакцій у зрозумілі, порівняльні й аналітично придатні показники. Особлива увага має бути приділена механізмам верифікації даних, що охоплюють криптографічні підтвердження транзакцій, відстеження історії записів у блоках та застосування смартконтрактів для автоматичного контролю умов угод.

Проблема формування довіри до автоматизованих даних стає центральною в науковому аналізі. В умовах, коли облік здійснюється безпосередньо в розподілених реєстрах, важливо встановити методологічні та організаційні засади аудиту блокчейн-записів. Це передбачає розроблення процедур перевірки достовірності транзакцій, стандартизованих методів підтвердження їх автентичності та комплексних підходів до оцінювання ризиків маніпуляцій або технічних збоїв у мережі. Наукові дослідження мають визначити критерії, за якими автоматизовані записи вважаються повноцінним доказом для фінансової звітності, а також процедури документування та сертифікації результатів аудиту.

Ключовим завданням стає стандартизація способів підтвердження достовірності транзакцій та їх інтеграція у звітні системи. Це охоплює визначення єдиних форматів криптографічних доказів, правил верифікації даних між різними вузлами мережі, а також методів забезпечення узгодженості показників у масштабі всієї економічної системи. Наукові підходи повинні поєднувати технічні аспекти блокчейну з класичними принципами бухгалтерського обліку, забезпечуючи баланс між автоматизацією і контролем людини, що гарантує достовірність, повноту та прозорість інформації для прийняття управлінських рішень.

Еволюція бухгалтерської звітності в умовах цифрової децентралізації передбачає перехід від формальної періодичної звітності до

безперервного, аналітично придатного потоку інформації, де довіра, аудит і стандартизація стають невід'ємними складовими методологічної системи, що забезпечує повноцінне функціонування інтегрованої інформаційної екосистеми управління.

Еволюція облікової науки в умовах цифрової децентралізації вимагає системного інтегрування міждисциплінарних знань для адекватного осмислення трансформацій облікових процесів. Сучасні технології, зокрема блокчейн, смартконтракти та алгоритми машинного навчання, змінюють не лише способи реєстрації господарських фактів, а й принципи їх визнання, оцінки та контролю. У цьому контексті економічні категорії власності, капіталу, прибутку та ризику потрібно розглядати крізь призму нових технологічних можливостей, їх взаємодії з правовим полем та етичними нормами. Відтак формування наукової парадигми цифрового обліку неможливе без глибокого поєднання економічного аналізу, юридичних засад регулювання цифрових активів, інформаційних технологій та етичних стандартів поведінки учасників економічних процесів.

Особливої значущості набуває взаємозв'язок технологічної автоматизації і людської відповідальності. Технологічні рішення забезпечують незмінність записів, швидкість обробки та прозорість, проте без професійної компетентності бухгалтера чи аудитора неможливо гарантувати повноту, обґрунтованість і справедливість відображення господарських операцій. Нові методологічні підходи повинні визначати, які аспекти обліку можуть виконуватися автономними алгоритмами, а які потребують контролю, перевірки та підтвердження людиною. Така інтеграція є основою для побудови довіри до цифрових систем обліку, забезпечення стабільності й прозорості економічних процесів.

Ключовим завданням наукової парадигми стає визначення стандартів взаємодії між різними компонентами інформаційної екосистеми: цифровими платформами, органами регулювання, аудиторами та учасниками ринку. Теоретичні засади мають окреслити принципи гармонізації технологічних рішень із фундаментальними правилами бухгалтерського обліку, включно з вимогами до достовірності, своєчасності та повноти даних. Це передбачає створення концептуальних моделей, які поєднують властивості розподілених реєстрів із класичними методами аналізу і контролю, забезпечуючи цілісність та надійність інформації в умовах автоматизації та автономності.

Водночас міждисциплінарний підхід відкриває можливості для формування нових наукових концепцій, що виходять за межі традиційного обліку. Облік перестає бути суто технічною процедурою фіксації даних і перетворюється на механізм забезпечення прозорості, довіри та сталості цифрової економіки. Теоретична база цифрового обліку повинна формуватися так, щоб одночасно підтримувати інновації в технологічних процесах і зберігати принципи обґрунтованості, відповідальності та етичності, які традиційно визначали професійну сутність бухгалтерського обліку.

Отже, подальший розвиток облікової науки орієнтований на побудову цілісної, інтегрованої теоретичної системи, яка поєднує технологічну ефективність, правову визначеність, економічну логіку та етичні засади, створюючи надійний фундамент для функціонування та розвитку децентралізованих цифрових систем обліку.

Висновки до розділу 3

Модель організації облікового процесу в середовищі цифрової децентралізації являє собою системно-інтегровану конструкцію, у якій технологічна архітектура блокчейну поєднується з організаційними, аналітичними та правовими механізмами забезпечення достовірності й безперервності бухгалтерського обліку. У цій моделі функції контролю, верифікації та збереження даних реалізуються не через централізовані інститути, а через алгоритмічні протоколи консенсусу, криптографічні засоби підтвердження і смартконтракти, що заміщують традиційні документообіг і процедури перевірки. Роль бухгалтера до того ж трансформується з реєстратора первинних даних у координатора цифрових процесів, аналітика й адміністратора довіри, відповідального за правильність параметрів транзакцій, коректність метаданих і відповідність алгоритмічних правил чинним стандартам обліку. Така модель забезпечує прозорість, відтворюваність і юридичне визнання облікових записів, створюючи передумови для формування глобальної децентралізованої екосистеми бухгалтерського обліку, у якій достовірність фінансової інформації гарантується не суб’єктивними процедурами контролю, а об’єктивною технологічною інфраструктурою довіри.

Впровадження блокчейн-технологій у сферу бухгалтерського обліку радикально змінює не лише технічні, але й етичні засади професії, формуючи нову парадигму відповідальності, довіри та контролю в умовах цифрової децентралізації. Сукупність технологічних, організаційно-інституційних, правових та етичних ризиків визначає потребу в інтегрованій системі управління, яка поєднує криптографічний захист, нормативне врегулювання, організаційну структурованість і морально-етичні стандарти поведінки фахівців. У центрі цієї системи має залишатися бухгалтер як носій професійного судження, здатний критично інтерпретувати результати автоматизованих алгоритмів, забезпечуючи не лише технічну коректність, а й економічну та етичну обґрунтованість облікових рішень. Саме людський інтелект і моральна відповідальність мають бути гарантом справедливості, достовірності та пояснюваності цифрових процесів, що забезпечить стійкість бухгалтерського обліку до ризиків блокчейн-дезінтермедіації та сприятиме формуванню довіри до облікової інформації в цифровій економіці.

Перспективи розвитку нормативно-правового забезпечення та професійних стандартів у сфері децентралізованого бухгалтерського обліку визначаються потребою в інтеграції правових, методологічних і технологічних компонентів у єдину систему регуляторного управління цифровими процесами. Формування правового поля, здатного легітимізувати записи в розподілених реєстрах, потребує розроблення чітких критеріїв їх автентичності, цілісності й доказової сили, унормування порядку архівування та контролю доступу до ончейн-даних, а також узгодження положень із міжнародними стандартами фінансової звітності. Одночасно має відбутися трансформація професійних стандартів бухгалтера – від традиційної моделі обліку до цифрової, що базується на компетенціях у сфері криптографічної верифікації, управління даними й етики алгоритмічних процесів. Розбудова нормативного простору децентралізованого обліку повинна спиратися на принципи юридичної визначеності, технологічної нейтральності та професійної відповідальності, забезпечуючи баланс між безпекою інформації, довірою користувачів та динамічним розвитком цифрової інфраструктури бухгалтерського обліку.

Подальша еволюція облікової науки під впливом цифрової децентралізації означає перехід від класичної концепції бухгалтерського обліку як інструменту ретроспективної фіксації фактів господарського

життя до інтегрованої моделі динамічного управління достовірною інформацією в реальному часі. У межах нової парадигми блокчейн-технології, штучний інтелект і смартконтракти є не лише технічними інструментами, а й методологічними чинниками, що формують нову систему координат бухгалтерської науки, у якій поняття власності, контролю, капіталу, ризику та довіри набувають цифрово-алгоритмічного змісту. Розвиток облікової теорії в цих умовах потребує інтеграції економічних, правових, інформаційно-технологічних та етичних підходів у єдину концептуальну систему, орієнтовану на забезпечення прозорості, незмінності та справедливості фінансової інформації. Водночас ключова роль бухгалтера трансформується – він стає не лише користувачем, а й куратором цифрових алгоритмів, гарантуючи їх відповідність економічному змісту, нормативним вимогам і суспільним цінностям. Отже, цифрова децентралізація стає каталізатором глибокої теоретико-методологічної модернізації бухгалтерського обліку, спрямованої на формування інтелектуальної, етично вивіреної та технологічно стійкої системи облікової науки нового покоління.

ВИСНОВКИ

Еволюція наукових підходів до розуміння сутності бухгалтерського обліку в умовах цифрової економіки засвідчує глибоку трансформацію його теоретико-методологічних основ – від централізованої парадигми документального контролю до децентралізованої цифрової моделі, інтегрованої у глобальні інформаційні мережі. Облік поступово втрачає ретроспективний характер і перетворюється на динамічну, аналітичну та інтегровану інформаційну систему, що функціонує в режимі реального часу, забезпечуючи прозорість, автоматичну верифікацію та незмінність даних.

Використання блокчейн-технологій формує нову концепцію бухгалтерського обліку, в основі якої лежить принцип децентралізованої довіри та алгоритмізованого контролю. Це зумовлює перехід від інституційних гарантій достовірності до технологічних механізмів консенсусу та криптографічного підтвердження, завдяки чому кожна транзакція набуває статусу одночасно факту, доказу і документа господарської діяльності.

Цифрова децентралізація стає фундаментальною інституційною трансформацією бухгалтерського обліку, яка переосмислює природу довіри, контроль і механізми організації облікових процесів. Вона спричиняє перехід від централізованих систем обробки даних до розподілених мереж, де достовірність і цілісність інформації забезпечуються алгоритмічно. У таких умовах облік набуває функції інтегратора цифрової інфраструктури, відповідального за проєктування, валідацію та інтерпретацію даних у блокчейн-екосистемах.

Запровадження принципів децентралізованої довіри, алгоритмічної перевірки та прозорості даних формує нову методологію бухгалтерського мислення, у якій контроль і звітність стають внутрішніми характеристиками облікових процесів. Такий підхід перетворює бухгалтерський облік на самоверифіковану цифрову систему, що забезпечує безперервність, достовірність і стійкість фінансової інформації.

У контексті цифрової децентралізації бухгалтерський облік трансформується в саморегульовану, криптографічно захищену інформаційну екосистему, де суб’єкти є одночасно генераторами, верифікаторами й користувачами даних, а об’єкти набувають статусу автономних цифрових сутностей. Архітектура децентралізованого облікового середовища формує алгоритмічно забезпечену систему довіри, що усуває

потребу в централізованому адмініструванні, забезпечуючи безперервний, трасований і синхронізований цикл облікової інформації, у межах якого принципи достовірності, інваріантності та прозорості реалізуються через консенсусні алгоритми й смартконтракти. Так, облік постає як технологічно детермінована система довіри, у якій істинність даних формується в момент їх виникнення, а перевірка та підтвердження здійснюються автоматично.

Функціонування блокчейн-реєстру у відображенні господарських операцій створює нову модель бухгалтерського обліку, засновану на принципах математично доведеної достовірності. У цій моделі кожна господарська операція проходить алгоритмічну валідацію, перетворюючись на самоверифікований цифровий факт, підтверджений колективною згодою учасників мережі. Безперервний ланцюг подій забезпечує повну простежуваність активів та дій суб'єктів, тоді як смартконтракти переводять облік у проактивну площину, де формування та перевірка даних відбуваються в реальному часі, а криптографічні механізми гарантують їх автентичність і захист. Блокчейн-реєстр у такому вимірі стає не лише технічним інструментом, а методологічним ядром парадигми «самоверифікованого обліку».

Смартконтракти формують концептуальну основу цифрової автономії облікових процесів, у межах якої визнання, оцінка, відображення та контроль господарських операцій здійснюються без посередників, виключно через алгоритмічні процедури. Вони втілюють принцип подвійної достовірності – технологічної та економічної – забезпечуючи повну відповідність даних методологічним вимогам бухгалтерського обліку. У цьому контексті облікова політика трансформується у програмний алгоритм, що гарантує автоматичне дотримання стандартів у момент фіксації господарських подій, формуючи основу «самоперевірного обліку» – прозорої та самоконтрольованої системи нового покоління.

Методика оцінювання, визнання та верифікації господарських фактів у блокчейн-системах поєднує класичні принципи обліку з технологічними механізмами децентралізованих реєстрів. Достовірність даних у ній забезпечується не зовнішнім контролем, а внутрішніми алгоритмами консенсусу, смартконтрактами й криптографічними доказами. У результаті кожен обліковий запис стає автономним цифровим підтвердженням економічної події, а сама система набуває властивостей прозорості, невідворотності та довіри, що визначають її як методологічну основу цифрового обліку майбутнього.

Стандартизація та уніфікація процедур у децентралізованому бухгалтерському середовищі постають ключовими умовами його цілісності та легітимності. Вони передбачають формалізацію облікових принципів у вигляді уніфікованих схем даних, протоколів взаємодії й алгоритмічних правил, що інтегруються в код блокчейн-протоколів. Такий підхід забезпечує сумісність суб'єктів обліку, безперервність і верифікованість записів, усуває ризики суб'єктивних тлумачень і створює основу для автоматизованого формування фінансової звітності в режимі реального часу. Отже, децентралізована технологічна інфраструктура стає не лише технічним середовищем, а рушійною силою еволюції бухгалтерського мислення – переходу від централізованого документування до алгоритмічно керованої системи економічної довіри.

Організація бухгалтерського обліку в умовах цифрової децентралізації набуває рис системно-інтегрованої моделі, у якій технологічна архітектура блокчейну поєднується з організаційними, аналітичними та правовими механізмами забезпечення достовірності й безперервності облікових процесів. Функції контролю, верифікації та збереження даних реалізуються через алгоритми консенсусу, криптографічні протоколи та смартконтракти, що усувають потребу в централізованих структурах і традиційних процедурах документообігу. Роль бухгалтера при цьому еволюціонує – він перетворюється на координатора цифрових потоків і адміністратора довіри, відповідального за правильність параметрів транзакцій та узгодженість алгоритмічних правил із методологічними стандартами. Така модель створює передумови для глобальної децентралізованої екосистеми бухгалтерського обліку, у якій достовірність інформації забезпечується не суб'єктивними перевірками, а об'єктивною технологічною інфраструктурою довіри.

Інтеграція блокчейн-технологій у бухгалтерський облік змінює не лише технічні, але й етичні засади професії, формуючи нову парадигму відповідальності й контролю. Вона потребує комплексного управління ризиками, що поєднує технологічні, нормативні, організаційні та морально-етичні компоненти. У центрі цієї системи залишається бухгалтер як носій професійного судження, здатний інтерпретувати результати алгоритмічних рішень та забезпечувати їх економічну й етичну обґрунтованість. Саме людський інтелект і моральна компетентність є гарантією справедливості та стійкості облікових процесів, забезпечуючи довіру до даних у децентралізованому середовищі.

Розвиток нормативно-правового забезпечення децентралізованого обліку вимагає формування цілісної системи регуляторного управління, що інтегрує правові, методологічні та технологічні аспекти. Легітимізація облікових записів у розподілених реєстрах потребує визначення критеріїв їх автентичності, цілісності та доказової сили, унормування процедур збереження ончейн-даних і гармонізації з міжнародними стандартами фінансової звітності. Водночас професійні стандарти бухгалтера мають еволюціонувати до цифрової моделі, що ґрунтується на компетенціях у сфері криптографічної верифікації, управління даними та етики алгоритмічних процесів. Така нормативна система повинна забезпечувати баланс між безпекою, прозорістю й гнучкістю цифрової інфраструктури обліку.

Подальша еволюція облікової науки в умовах цифрової децентралізації визначається переходом від ретроспективного фіксування фактів до динамічного управління достовірною інформацією в реальному часі. Блокчейн, штучний інтелект і смартконтракти стають не лише технічними засобами, а методологічними чинниками формування нової наукової парадигми, у якій економічні категорії набувають цифрово-алгоритмічного змісту. Розвиток теорії бухгалтерського обліку потребує синтезу економічних, правових, технологічних і етичних підходів, орієнтованих на забезпечення справедливості, прозорості та стійкості фінансової інформації. У цьому контексті бухгалтер постає куратором алгоритмів і гарантом їхньої економічної та етичної легітимності. Отже, цифрова децентралізація є каталізатором глибокої методологічної модернізації бухгалтерського обліку, спрямованої на формування інтелектуально керованої, етично вивіреної та технологічно надійної системи обліку нового покоління.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бабінська С. Ведення бухгалтерського обліку в умовах впровадження сучасних інформаційних технологій. *Економіка та суспільство*. 2021. № 26. DOI : https://doi.org/10.32782/2524-0072/2021-26-1

2. Балазюк О. Вплив технології блокчейн на систему бухгалтерського обліку. *Економіка та управління в XXI ст.: виклики та перспективи розвитку* : зб. тез Міжн. наук.-практ. конф., м. Умань, 30 трав. 2019 р. Умань, 2019. С. 150–152.

3. Балазюк О., Пилявець В. Технологія блокчейн: дослідження суті та аналіз сфер використання. *Економіка та суспільство*. 2022. № 43. DOI : https://doi.org/10.32782/2524-0072/2022-43-13

4. Бардаш С. В., Грабчук І. Л. Цифрові технології в сфері бухгалтерського обліку: основні можливості та ризики. *Ефективна економіка*. 2021. № 9. URL : http://www.economy.nayka.com.ua/?op=1&z=9301 (дата звернення: 17.10.2025).

5. Бухгалтерський облік та оподаткування в умовах застосування інформаційних технологій: теорія і практика : монографія / В. О. Осмятченко, С. В. Шевчук, Я. О. Ізмайлов та ін. ; за заг. ред. В. О. Осмятченка ; Ун-т держ. фіск. служби України. Ірпінь : Ун-т ДФС України, 2020. 394 с.

6. Вакульчик О. М., Брайко В. С. Перспективи та проблеми впровадження блокчейн-технологій в обліку та аудиті. *Науковий погляд: економіка та управління*. 2021. № 1 (71). С. 63–70.

7. Гузь М. М., Соколенко Л. Ф., Ткаль Я. С. Інноваційний потенціал технології блокчейн у бухгалтерському обліку. *Інвестиції: практика та досвід* : наук.-практ. журн. 2023. № 2. С. 19–25.

8. Blockchain-технологія як засіб трансформації бухгалтерського обліку / М. В. Дубініна, С. В. Сирцева, О. В. Буганов, Н. О. Тусова. *Modern Economics*. 2018. № 12. С. 75–80.

9. Жиглей І. В., Лайчук С. М., Поліщук І. Р. Використання інформаційних технологій у бухгалтерському обліку. *Економіка, управління та адміністрування.* 2024. № 1 (107). С. 95–102. URL : https://eztuir.ztu.edu.ua/jspui/bitstream/123456789/8461/1/95.pdf (дата звернення: 17.10.2025).

10. Ілляшенко К. В. Перспективи застосування технології блокчейн в бухгалтерському обліку. *Інфраструктура ринку: науково-практичний журнал*. 2020. № 40. С. 198–202. DOI : https://doi.org/10.32843/infrastruct40-35

11. Легенчук С. Ф., Городиський М. П., Майстренко Н. М. Захист бухгалтерських даних в умовах використання Інтернету речей: проблеми і перспективи діджиталізації обліку. *Облік і фінанси*. 2021. № 1. С. 12–19. URL : http://nbuv.gov.ua/UJRN/Oif_apk_2021_1_4 (дата звернення: 17.10.2025).

12. Лемішовська О., Лінинська В. Бухгалтерський облік в умовах впровадження інформаційних технологій і систем. *Економіка та суспільство*. 2022. № 44. DOI : https://doi.org/10.32782/2524-0072/2022-44-23

13. Манчур І. Рівень використання блокчейн-технології підприємствами України в сфері бухгалтерського обліку та аудиту. *Економічний аналіз*. 2021. № 3. С. 183–189.

14. Застосування технології блокчейн у бухгалтерському обліку та аудиті: досвід України та Казахстану / Г. Мацьків, І. Смірнова, А. Малікова, О. Пугаченко, М. Дубініна. *Financial and credit activity problems of theory and practice*. 2023. Т. 1, № 48. С. 180–192. DOI : https://doi.org/10.55643/fcaptp.1.48.2023.3955

15. Мельниченко О., Гартінгер Р. Роль технології блокчейн у розвитку бухгалтерського обліку та аудиту. *European cooperation*. 2016. № 7 (14). С. 9–19. URL : https://we.clmconsulting.pl/index.php/we/article/viewFile/191/1146

16. Муравський В. В. Комп'ютерно-комунікаційна форма обліку : монографія. Тернопіль : ТНЕУ, 2018. 486 с.

17. Нашкерська Г. В. Технологія блокчейн у бухгалтерському обліку: переваги та обмеження. *Фінанси України*. 2023. № 3. С. 88–102.

18. Перспективи розвитку бухгалтерського обліку, аналізу та аудиту в умовах інноваційних інформаційних технологій : монографія / Є. А. Карпенко, О. В. Карпенко, А. І. Мілька та ін. Полтава : ПУЕТ, 2021. 410 с.

19. Пілевич Д. С. Теоретико-прикладні засади використання blockchain-технології в бухгалтерському обліку. *Проблеми економіки*. 2020. № 1 (43). С. 267–273.

20. Попівняк Ю. М. Технологія блокчейн у бухгалтерському обліку й аудиті: сучасний стан, можливості та перспективи застосування. *Економіка, управління та адміністрування.* 2019. № 3 (89). С. 137–144. DOI : https://doi.org/10.26642/ema-2019-3(89)-137-144

21. Правдюк Н. Л., Обнявко М. В. Впровадження блокчейну в облікову систему: кроки назустріч. *Ефективна економіка*. 2022. № 1. URL : http://www.economy.nayka.com.ua/?op=1&z=9913 ; DOI 10.32702/2307-2105-2022.1.12

22. Пушкар М. С. Креативний облік (створення інформації для менеджерів) : монографія. Тернопіль : Карт-бланш, 2006. 334 с.

23. Пушкар М. С. Створення інтелектуальної системи обліку : монографія. Тернопіль : Карт-бланш, 2007. 152 с.

24. Пушкар М. С., Чумаченко М. Г. Ідеальна система обліку: концепція, архітектура, інформація : монографія. Т. : ТНЕУ ; Карт-бланш, 2011. 335 с.

25. Пушкар М. С., Пушкар М. Р. Інформаційні ресурси для бізнесу: формування та використання : монографія. Тернопіль : Карт-бланш, 2021. 207 с.

26. Роєва О. С., Цікало Є. І., Яцко М. В. Інтеграція блокчейн-технологій у процеси фінансового обліку та податкового аудиту. *Актуальні питання економічних наук*. 2024. № 3–4. DOI : https://doi.org/10.5281/zenodo.13934604

27. Розвиток цифровізації обліку, оподаткування, аналізу і контролю в управлінні підприємствами : монографія / Р. Ф. Бруханський, П. Р. Пуцентейло та ін. Тернопіль : ВПЦ «Університетська думка», 2021. 194 с.

28. Семанюк В. З. Інформаційна теорія обліку в постіндустріальному суспільстві : монографія. Тернопіль : ТНЕУ, 2018. 392 с.

29. Скрипник С., Сливка Я., Музиченко Т. Блокчейн-технології в бухгалтерії: нові підходи до забезпечення прозорості та надійності фінансової звітності. *Економіка та суспільство*. 2024. Вип. 66. URL : https://economyandsociety.in.ua/index.php/journal/article/view/4556/4499

30. Сторожук Т. М., Моргуненко А. С. Інтеграція блокчейн-технології в систему обліку та аналізу контрольованих операцій. *Проблеми сучасних трансформацій. Серія: економіка та управління*. 2024. № 12. DOI : https://doi.org/10.54929/2786-5738-2024-12-09-03

31. Тесак О. В. Облікова політика підприємства: аналіз ризиків використання технології блокчейн в бухгалтерському обліку та аудиті. *Академічні візії*. 2022. № 13. DOI : http://dx.doi.org/10.5281/zenodo.7331052

32. Шевчук О., Муравський В. Блокчейн та електронні транс-акції в обліку. *Вісник економіки*. 2023. № 3. С. 212–237. DOI : https://doi.org/10.35774/visnyk2023.03.212

33. Шишкова Н. Л. Перспективи впровадження блокчейну в бухгалтерському обліку. *Облік і фінанси*. 2018. № 2. С. 61–68.

34. Шот А. П., Андрусяк В. М., Яцко М. В. Вплив блокчейн технологій на трансформацію корпоративного бухгалтерського обліку. *Scientific Notes of Lviv University of Business and Law*. 2024. Вип. 42. С. 15–22. URL : https://nzlubp.org.ua/index.php/journal/article/view/1373/1196

35. Юрченко О. А., Савченко Р. В. Роль і місце блокчейн-технологій для ведення бухгалтерського обліку та складання фінансової звітності. *Економічний простір.* 2025. № 198. С. 269–274.

36. Ярощук О., Белова І. Технологія блокчейн в бухгалтерському обліку та аудиті. *Інститут бухгалтерського обліку, контроль та аналіз в умовах глобалізації* : міжнар. наук. журн. 2020. Вип. 3–4. С. 28–44. DOI : https://doi.org/10.35774/ibo

37. Appelbaum D., Nehmer R. Designing and auditing accounting systems based on blockchain and distributed ledger principles. *Feliciano School of Business*. 2017. URL : https://pdfs.semanticscholar.org/edc2/4c3ae8cb7f4f978c9353d47986168265fe03.pdf

38. Atanasovski A., Trpeska M., Lazarevska Z. B. Th e Block Chain Technology and Its Limitations for True Disruptiveness of Accounting and Assurance. *Journal of Applied Economic Sciences*. 2020. Vol. XV. № 4 (70). Pp. 738–748. URL : http://cesmaa.org/Docs/Winter/JAES%20VolumeXV%20Issue4(70)Winter2020_3.pdf

39. Bellucci M., Cesa Bianchi D., Manetti G. Blockchain in Accounting Practice and Research. *Systematic Literature Review. Meditari Accountancy Research*. 2022. Vol. 30. Iss. 7. Pp. 121–146. DOI : https://doi.org/10.1108/MEDAR-10-2021-1477

40. Bonson E., Bednarova M. Blockchain and its implications for accounting and auditing. *Meditari Accountancy Research*. 2019. № 5. Pp. 725–740.

41. Breuer W., Knetsch A. Recent trends in the digitalization of finance and accounting. *Journal of Business Economics*. 2023. Vol. 93. Pp. 1451–1461. DOI : https://doi.org/10.1007/s11573-023-01181-5 (date of access: 17.10.2025).

42. Cai C. Triple-entry accounting with blockchain: How far have we come? *Accounting and Finance*. 2019. Vol. 61 (2). Pp. 71–93. DOI : https://doi.org/10.1111/acfi.12556 (date of access: 17.10.2025).

43. Chowdhury E., Khan I., Dhar B. Strategy for implementing blockchain technology in accounting: Perspectives of stakeholders in a developing nation. *Business Strategy & Development*. 2023. № 6. DOI : https://doi.org/10.1002/bsd2.256

44. Chowdhury E., Stasi A., Pellegrino A. Blockchain Technology in Financial Accounting: Emerging Regulatory Issues. *Review of Financial Economics*. 2023. № 21. Pp. 862–868. DOI : https://doi.org/10.55365/1923.x2023.21.94

45. Coyne J. G., McMickle P. L. Can Blockchains Serve an Accounting Purpose? *Journal of Emerging Technologies in Accounting*. 2017. Vol. 14 (2). Pp. 101–111. DOI : https://doi.org/10.2308/jeta-51910 (date of access: 17.10.2025).

46. Dai J., Vasarhelyi M. A. Toward Blockchain-Based Accounting and Assurance. *Journal of Information Systems.* 2017. Vol. 31 (3). Pp. 5–21. DOI : https://doi.org/10.2308/isys-51804 (date of access: 17.10.2025).

47. Fang B., Liu X., Ma C., Zhuo Y. Blockchain Technology Adoption and Accounting Information Quality. *Accounting & Finance*. 2023. DOI : https://doi.org/10.1111/acfi.13088

48. Fuller S. H., Markelevich A. Should Accountants Care About Blockchain? *Journal of Corporate Accounting & Finance*. 2019. Vol. 31, Iss. 2. Pp. 34–46. DOI : http://dx.doi.org/10.1002/jcaf.22424

49. Grosu V., Botez D., Melega A., Kicsi R., Mihaila S., Macovei A. Bibliometric analysis of the transformative synergies between blockchain and accounting in the uprooting of economic criminality. 2022. № 9. Pp. 77–105. DOI : https://doi.org/10.9770/jesi.2022.9.4(3)

50. Han H., Shiwakoti R. K., Jarvis R., Mordi C., Botchie D. Accounting and auditing with blockchain technology and artificial Intelligence: A literature review. *International Journal of Accounting Information Systems*. 2023. Vol. 48. Pp. 1–16. DOI : https://doi.org/10.1016/j.accinf.2022.100598 (date of access: 17.10.2025).

51. Ibañez J., Bayer C., Tasca P., Xu J. REA, Triple-Entry Accounting and Blockchain: Converging Paths to Shared Ledger Systems. *Journal of Risk and Financial Management*. 2023. № 16, 382. DOI : https://doi.org/10.3390/jrfm16090382

52. Karajovic M., Kim H. M., Laskowski M. Thinking Outside the Block: Projected Phases of Blockchain Integration in the Accounting Industry. *Australian Accounting Review*. 2019. Vol. 29 (10). Pp. 319–330. DOI : https://doi.org/10.1111/auar.12280 (date of access: 17.10.2025).

53. Kokina J., Mancha R., Pachamanova D. Blockchain: Emergent industry adoption and implications for accounting. *Journal of Emerging Technologies in Accounting*. 2017. Vol. 14, Iss. 2. Pp. 91–100. DOI : http://dx.doi.org/10.2308/jeta-51911

54. Kozlowski S. An Audit Ecosystem to Support Blockchain-based Accounting and Assurance. *Continuous Auditing: Theory and Application*. 2018. Pp. 229–313. DOI : https://doi.org/10.1108/978-1-78743-413-420181015 (date of access: 17.10.2025).

55. Kravchenko O., Nebaba N., Aiyedogbon J. Blockchain technologies in accounting: bibliometric analysis. *Accounting and Financial Control*. 2023. № 4. Pp. 14–29. DOI : https://doi.org/10.21511/afc.04(1).2023.02

56. Kupenova Zh., Baymukhanova S., Isaeva A. Blockchain in accounting in the digital economy. *The Journal of Economic Research & Business Administration*. 2022. № 142. DOI : https://doi.org/10.26577/be.2022.v142.i4.09

57. Kwilinski A. Implementation of blockchain technology in accounting sphere. *Academy of Accounting and Financial Studies Journal*. 2019. № 23 (2). URL : https://www.abacademies.org/articles/Implementation-of-BlockchainTechnology-in-Accounting-Sphere-1528–2635–23-SI-2–412.pdf (дата звернення: 25.12.2020).

58. Liu M., Wu K., Xu J. How Will Blockchain Technology Impact Auditing and Accounting: Permissionless Vs. Permissioned Blockchain. *Current Issues in Auditing*. 2019. Vol. 13 (2). Pp. 19–29. DOI : https://doi.org/10.2308/ciia-52540 (date of access: 17.10.2025).

59. Maffei M., Casciello R., Meucci F. Blockchain Technology: Uninvestigated Issues Emerging from an Integrated View Within Accounting and Auditing Practices. *Journal of Organizational Change Management*. 2021. Vol. 34, Iss. 2. Pp. 462–476. DOI : http://dx.doi.org/10.1108/JOCM-09-2020-0264

60. Mahtani U. Fraudulent Practices and Blockchain Accounting Systems. 2022. URL : https://ssrn.com/abstract=4036726

61. Muravskyi V. Accounting and Cybersecurity : monograph / Scientific Editor Z.-M. Zadorozhnyi. Kindle Publishing, KDP, Seattle. USA, 2021. 200 p.

62. Muravskyi V., Khoma N., Khokhlova L., Chengyu L. Open Document Flow Based on Blockchane Technology for Cyber Security of the Accounting System. *Herald of Economics*. 2021. № 4. Pp. 156–170. DOI : https://doi.org/10.35774/visnyk2021.04.156

63. Mustapha I., Grine A., Calabro G. The Digital Transformation of Accounting, Through Implementing Blockchain Technology : a conceptual model. 2023. № 6. Pp. 47–62.

64. Nalini G. V. S. Impact of blockchain technology on accountancy. *The Management Accountant*. 2018. Vol. 53, No. 6. Pp. 55–59.

65. Nehmer R., Appelbaum D. Auditing Cloud-Based Blockchain Accounting Systems. *Journal of Information Systems*. 2019. № 34. DOI : https://doi.org/10.2308/isys-52660

66. O'Leary D. E. Configuring Blockchain Architectures for Transaction Information in Blockchain Consortiums: The case of accounting and supply chain systems. *Intell Sys Acc Fin Mgmt*. 2017. № 24. Pp. 138–147. DOI : https://doi.org/10.1002/isaf.1417

67. Önkan Ö., Arikan Z. The Impact of Blockchain Technology on Tax and Accounting Practices. 2022. DOI : https://doi.org/10.4018/978-1-7998-8493-4.ch001

68. Pflueger D., Kornberger M., Mouritsen J. What is Blockchain Accounting? A Critical Examination in Relation to Organizing, Governance, and Trust. *European Accounting Review*. 2022. Pp. 1–26. DOI : https://doi.org/10.1080/09638180.2022.2 147973

69. Qadir A., Dolpamuee R. Blockchain Technology and Accounting: The Triple-Entry Affecting Transparency. 2023. № 21. Pp. 20–22.

70. Rahmawati M. A Bibliometric Analysis of Accounting in the Blockchain Era. *Journal of Accounting and Investment*. 2022. № 23. Pp. 66–77. DOI : https://doi.org/10.18196/jai.v23i1.13302

71. Rao L., PandurangiahS. Blockchain technology: will it disrupt or discipline accountants? *The Management Accountant*. 2018. Vol. 53. № 6. Pp. 42–46.

72. Rindasu S.-M. Blockchain in accounting: Trick or treat? Quality – Access to Success. 2019. № 170 (20). Pp. 143–147.

73. Rückeshäuser N. Do we really want blockchain-based accounting? *Decentralized consensus as enabler of management override of internal controls :* 13th Int. Conf. on Wirtschaftsinformatik. February 12–15. St. Gallen, Switzerland. 2017. Pp. 16–30. URL : https://wi2017.ch/images/wi2017–0112.pdf (дата звернення: 25.12.2020).

74. Saraiva H., Vieira P. Accounting Systems With Smart Contracts: Building Accounting Records in Blockchain Step by Step. 2023. DOI : https://doi.org/10.4018/978-1-6684-7293-4.ch003

75. Sarwar M. I., Nisar K., Khan I., Shehzad D. Blockchains and Triple-Entry Accounting for B2B Business Models. Ledger. 2023. № 8. Pp. 37–57. DOI : https://doi.org/10.5195/LEDGER.2023.288

76. Shao H., Zhang Z., Wang B. Research on Accounting Information Security Management Based on Blockchain. *Mobile Information Systems*. 2021. Pp. 1–11. DOI : https://doi.org/10.1155/2021/9926106

77. Suta A., Toth A. Systematic Review on Blockchain Research for Sustainability Accounting Applying Methodology Coding and Text Mining. *Cleaner Engineering and Technology*. 2023. № 14, 100648. DOI : https://doi.org/10.1016/j.clet.2023.100648

78. Tan B. S., Low K. Y. Blockchain as the database engine in the accounting system. *Australian Accounting Review*. 2019. № 2. Pp. 312–318.

79. Thies S., Kureljusic M., Karger E., Krämer T. Blockchain-Based Triple- Entry Accounting: A Systematic Literature Review and Future Research Agenda. *Journal of Information Systems*. 2023. DOI : https://doi.org/10.2308/ISYS-2022-029

80. Tiron-Tudor A., Deliu D., Farcane N., Dontu A. Managing Change with and Through Blockchain in Accountancy Organizations: a Systematic Literature Review. *Journal of Organizational Change Management*. 2020. Vol. 34, Iss. 2. Pp. 477–506. DOI : https://doi.org/10.1108/JOCM-10-2020-0302

81. Wu C., Zhou Z. The Impact of Digital Currency on Accounting and Management under the Blockchain Architecture. *International Journal of Education and Humanities*. 2022. № 5. Pp. 23–27. DOI : https://doi.org/10.54097/ijeh.v5i3.2440

82. Wu Y., Wang X. Application of Blockchain Technology in the Integration of Management Accounting and Financial Accounting. 2020. DOI : https://doi.org/10.1007/978-3-030-43309-3_4

83. Zadorozhnyi Z.-M., Muravskyi V., Shevchuk O. Management Accounting of Electronic Transactions with the Use of Cryptocurrencies. *Financial And Credit Activity: Problems Of Theory And Practice*. 2018. № 3 (26). Pp. 169–177. DOI : http://dx.doi.org/10.18371/fcaptp.v3i26.144368

84. Zhang Y., Ardakani S., Han W. Smart ledger: The Blockchain-based Accounting Information Recording Protocol. *Journal of Corporate Accounting & Finance*. 2021. № 32. DOI : https://doi.org/10.1002/jcaf.22515

85. Zheng C. Research on Accounting Information Integrity Verification Method based on Blockchain. *Academic Journal of Management and Social Sciences*. 2023. № 3. Pp. 202–205. DOI : https://doi.org/10.54097/ajmss.v3i3.11192

Наукове електронне мережеве видання

Мискін Юрій Ігоревич,
Краєвський Володимир Миколайович,
Мискіна Оксана Олександрівна,
Іщенко Віталій Вікторович

Концепція бухгалтерського обліку в умовах цифрової децентралізації (на засадах блокчейн-технологій)

Монографія

Відповідальний за випуск	*Н. Б. Добрянська*
Редактор	*М. П. Клименко*
Форматування та комп'ютерна верстка	*Д. П. Завальніцька*

Здано до друку 09.10.2026. Формат 29,7 × 41,99
Папір офсетний № 1. Гарнітура «Times New Roman»
Ум. друк. арк. 5.0
Наклад 300 прим. Замовлення № 1189

Підготовлено до друку науково-організаційним відділом
Державного податкового університету
08205, вул. Університетська, 31, м. Ірпінь, Київська область,
Україна

Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції
Серія ДК № 7669 від 20.09.2022