

Качурінер В. Л.,кандидат юридичних наук, доцент,
доцент кафедри морського та міжнародного права

Міжнародного університету

ORCID: <https://orcid.org/0000-0003-2553-5071>

ТЕХНОЛОГІЇ РОЗПОДІЛЕНОГО РЕЄСТРУ В МІЖНАРОДНО-ПРАВОВОМУ ЗАБЕЗПЕЧЕННІ ПРОСТЕЖУВАНOSTІ СІЛЬСЬКОГОСПОДАРСЬКОЇ ПРОДУКЦІЇ

Анотація. У статті досліджено міжнародно-правові передумови, функції та межі використання технологій розподіленого реєстру, зокрема блокчейну, для забезпечення простежуваності сільськогосподарської продукції.

Встановлено, що правове регулювання у цій сфері формується на перетині міжнародного торговельного права, міжнародних стандартів безпечності харчових продуктів, права електронної торгівлі, режимів належної обачності у глобальних ланцюгах постачання, захисту персональних і комерційних даних та права Європейського Союзу.

Обґрунтовано, що блокчейн не є самостійним джерелом права, сертифікатом якості або доказом істинності первинної інформації. Його юридично значущою функцією є забезпечення цілісності, послідовності та контрольованої доступності записів після їх внесення. Помилкова, неповна або неправомірно отримана інформація не стає достовірною лише внаслідок її незмінного збереження в розподіленому реєстрі.

Запропоновано авторське визначення міжнародно-правового забезпечення цифрової простежуваності сільськогосподарської продукції як системи договірних норм, міжнародних стандартів, актів модельного права, наднаціональних приписів і процедур співробітництва, які визначають обов'язкові події простежуваності, суб'єктів внесення та перевірки даних, юридичні вимоги до електронних записів і правила їх транскордонного визнання.

Розроблено функціональну класифікацію відповідних інструментів: цілевстановлювальні, ідентифікаційно-стандартизаційні, доказово-довірчі, торговельно-контрольні, захисні та коригувальні.

Сформульовано семиелементний тест юридичної надійності блокчейн-системи простежуваності.

Доведено доцільність багаторівневої моделі, у якій міжнародні та галузеві стандарти визначають семантику даних, дозвільний розподілений реєстр фіксує події, персональні й комерційно чутливі відомості зберігаються поза ланцюгом, кваліфіковані електронні довірчі послуги підтверджують автора і час запису, а компетентний орган або незалежний аудитор забезпечує перевірку первинної події. Така модель дозволяє поєднати простежуваність із захистом прав виробників, недискримінаційною торгівлею та взаємним визнанням електронних доказів.

Ключові слова: міжнародне право, сільськогосподарська продукція, простежуваність, блокчейн, розподілений реєстр, електронний запис, належна обачність, міжнародна торгівля, захист даних, Європейський Союз.

Постановка проблеми. Глобальний ланцюг постачання сільськогосподарської продукції об'єднує виробника, заготі-

вельника, переробника, перевізника, склад, лабораторію, сертифікаційний орган, митницю, імпортера, роздрібного продавця та споживача. Кожний із них створює або використовує дані про походження продукції, земельну ділянку, технологію виробництва, застосовані речовини, результати лабораторних досліджень, температуру зберігання, переміщення партії та відповідність вимогам ринку. Фрагментація інформаційних систем ускладнює відкликання небезпечної продукції, перевірку екологічних тверджень, боротьбу з підміною походження та виконання транскордонних обов'язків належної обачності.

У попередніх працях ми розглядали міжнародно-правові інструменти як засоби перетворення погоджених цілей на регулятивний вплив у сфері виробництва [1, с. 192–196], а екологічну інформацію – як необхідну передумову участі, контролю та обґрунтованості рішення [2, с. 327–330]. Стандарти, своєю чергою, конкретизують загальні правові вимоги через показники, методики та процедури перевірки [3, р. 263–278]. Ці висновки набувають нового значення у цифрових аграрних ланцюгах: правова норма діє ефективно лише тоді, коли подія, з якою вона пов'язує наслідок, може бути ідентифікована, перевірена та співвіднесена з відповідальним суб'єктом.

Технологія розподіленого реєстру пропонує спільне середовище, у якому послідовність операцій підтверджується учасниками мережі, а зміна попереднього запису є технічно складною та помітною. Проте технічна незмінність не усуває питання про юридичну силу запису, компетентність його автора, правомірність обробки даних, відповідальність за помилку, визнання іноземного електронного документа та можливість виправлення. Тому предметом правового дослідження має бути не блокчейн як програмний продукт, а система норм і процедур, що перетворює цифровий запис на юридично значущий елемент простежуваності.

Аналіз останніх досліджень і публікацій. Технічні та організаційні можливості блокчейну в агропродовольчих ланцюгах досліджували Х. Ф. Гальвес, Х. К. Мехуто), Х. Сімаль-Гандара, А. Каміларіс, А. Фонтс та Ф. К. Пренафета-Болду. Х. Ф. Гальвес, Х. К. Мехуто та Х. Сімаль-Гандара показали потенціал розподіленого реєстру для контролю походження та аналітичних даних, водночас наголосивши на проблемі якості первинної інформації та взаємодії з фізичними об'єктами [4, р. 222–232]. А. Каміларіс, А. Фонтс і Ф. К. Пренафета-Болду систематизували аграрні блокчейн-проекти й дійшли висновку, що їх масштабуванню перешкоджають технічні, освітні, політичні та регуляторні бар'єри [5, р. 640–652].

М. Тріполі та Й. Шмідхубер пов'язують застосування блокчейну в агропродовольчій сфері зі скороченням інформаційної асиметрії, фінансуванням, страхуванням і простежуваністю, але застерігають щодо вартості інфраструктури, цифрового розриву та необхідності належного врядування [6, р. 7–18, 27–30]. У правовій доктрині М. Фінк, П. де Філіппі та А. Райт досліджують співвідношення розподілених систем із правом, захистом даних і приватним технологічним нормотворенням. Водночас міжнародно-правова архітектура аграрної простежуваності, критерії юридичної надійності запису та межі допустимої прозорості залишаються недостатньо систематизованими.

Мета статті полягає у визначенні міжнародно-правових засад використання технологій розподіленого реєстру для простежуваності сільськогосподарської продукції, розробленні функціональної класифікації відповідних інструментів і формулюванні моделі, яка забезпечує юридичну надійність записів, транскордонну сумісність, захист даних та можливість виправлення помилок.

Виклад основного матеріалу. Простежуваність доцільно розуміти як здатність відновити історію, застосування або місцезнаходження визначеного об'єкта за допомогою ідентифікованих подій і зв'язків між ними. Її юридична мета залежить від конкретного режиму: захист здоров'я, відкликання небезпечної партії, підтвердження країни чи ділянки походження, дотримання фітосанітарних вимог, доведення екологічної характеристики або виконання договірних зобов'язань. Принципи Codex Alimentarius визначають простежуваність як інструмент системи інспекції та сертифікації, який має бути обґрунтований визначеною метою, не створювати необґрунтованих торговельних обмежень і забезпечувати ідентифікацію попереднього та наступного учасника ланцюга [7, р. 1–3]. Отже, простежуваність не є самодостатнім накопиченням максимальної кількості інформації.

Стандарт GS1 розкриває операційну логіку через три взаємопов'язані дії: ідентифікувати об'єкт, зафіксувати подію та надати стандартизовані дані уповноваженому користувачеві [8]. У сільському господарстві простежуваним об'єктом може бути партія насіння, поле, урожай, тварина, сировина, перероблений продукт, транспортна одиниця або сертифікат. Подією є сімба, обробка, збирання, змішування, переробка, відбір проб, передача, зберігання чи експорт. Без уніфікованих ідентифікаторів і семантики різні блокчейн-мережі лише незмінно зберігатимуть несумісні відомості.

Міжнародно-правове забезпечення цифрової простежуваності сільськогосподарської продукції пропонується визначити як систему договірних норм, міжнародних стандартів, актів модельного права, наднаціональних приписів і процедур співробітництва, які визначають обов'язкові події простежуваності, суб'єктів внесення та перевірки даних, юридичні вимоги до електронних записів і правила їх транскордонного визнання. У цій системі технологія є способом виконання правової функції, а не заміною правової норми.

За регулятивною функцією відповідні інструменти можна поділити на шість груп. Цілевстановлювальні інструменти визначають законну мету простежуваності. Ідентифікаційно-стандартизаційні встановлюють об'єкти, події, формати та словники даних. Доказово-довірчі визначають вимоги до ідентифікації автора, електронного підпису, часу, цілісності та контролю запису. Торговельно-контрольні пов'язують дані з доступом на

ринок, сертифікацією, митним або санітарним контролем. Захисні встановлюють межі обробки персональних і комерційних даних. Коригувальні забезпечують виправлення, оскарження, аудит, відкликання продукції та відповідальність.

Для транскордонної юридичної сили важливими є принципи технологічної нейтральності та функціональної еквівалентності. Типовий закон ЮНСІТРАЛ про електронні передавані записи не надає переваги конкретній технології, але вимагає надійного методу ідентифікації запису, забезпечення контролю та збереження його цілісності [9, р. 4–11, 19–33]. Він прямо допускає моделі реєстрів, токенів і розподілених реєстрів. Для аграрного обороту це має значення щодо електронних складських свідоцтв, коносаментів, страхових і товаророзпорядчих документів. Однак функціональна еквівалентність форми не підтверджує якість товару: електронний документ має юридично відтворювати функцію паперового документа, тоді як фактичні відомості потребують окремої верифікації.

Міжнародні торговельні правила встановлюють межі обов'язкової простежуваності. Угода СОТ про застосування санітарних і фітосанітарних заходів вимагає наукової обґрунтованості, недискримінації, пропорційності та орієнтації на міжнародні стандарти [10, р. 70–74]. Угода про технічні бар'єри в торгівлі вимагає, щоб технічні регламенти не створювали зайвих перешкод і не були більш обмежувальними, ніж необхідно для досягнення законної мети [11, р. 117–137]. Отже, вимога держави використовувати виключно одну блокчейн-платформу може бути проблемною, якщо еквівалентний рівень простежуваності забезпечується іншою сумісною технологією.

Звідси випливає принцип правової нейтральності інфраструктури: міжнародне або національне правило повинно визначати функціональний результат – ідентифікацію, цілісність, доступність, перевірюваність і строк зберігання, – а не наві'язувати конкретний програмний протокол. Виняток можливий лише тоді, коли вибір єдиної інфраструктури об'єктивно необхідний для публічної системи контролю, передбачає відкриті інтерфейси та не дискримінує іноземних виробників або малих учасників.

Право Європейського Союзу демонструє перехід від загального обов'язку простежуваності до деталізованої цифрової належної обачності. Стаття 18 Регламенту (ЄС) № 178/2002 зобов'язує операторів харчового бізнесу встановлювати, від кого отримано і кому передано харчовий продукт, корм, тварину чи речовину, призначену для включення до продукту [12]. Імплементаційний регламент (ЄС) № 931/2011 деталізує інформацію про відправника, одержувача, обсяг, партію та дату для харчових продуктів тваринного походження [13]. Ці акти не вимагають блокчейну, але утворюють правову матрицю обов'язкових подій і даних.

Регламент (ЄС) 2023/1115 щодо продукції, пов'язаної зі знелісненням, виводить простежуваність за межі безпечності харчових продуктів. Оператор збирає опис і кількість продукції, країну виробництва, геолокацію всіх ділянок, дату або період виробництва, відомості про постачальників та докази відсутності знеліснення; після цього здійснює оцінювання та зменшення ризику [14]. Розподілений реєстр може пов'язати партію з геопросторовими даними й заявою про належну обачність, але не здатний самостійно встановити, чи відповідає супутникове зображення фактичній ділянці або чи законним є землекористування.

Керівництво ОЕСР–ФАО щодо відповідальних аграрних ланцюгів постачання розглядає належну обачність як безперервний процес: політика, ідентифікація ризиків, запобігання або пом'якшення впливу, перевірка результатів і повідомлення про вжиті заходи [15]. Блокчейн може зберігати докази проходження цих етапів, однак рішення про прийнятність ризику залишається юридичною та управлінською оцінкою. Автоматичне виконання смарт-контракту не повинно підмінити дискрецію там, де норма вимагає врахування контексту, прав людини або пропорційності.

Вирішальним є розмежування цілісності та достовірності. Розподілений реєстр підтверджує, що певний запис існував у визначений момент і не був непомітно змінений після погодження мережею. Він не доводить, що датчик був справним, лабораторія діяла компетентно, координати стосувалися саме цієї партії, а особа мала право вносити інформацію. Цю проблему називають проблемою «оракула»: цифрова система залежить від зовнішнього джерела, яке перетворює фізичний факт на дані. Тому юридично значуща простежуваність починається не з хешування запису, а з нормативно визначеної процедури формування первинного доказу.

Для оцінювання системи пропонується семиелементний тест юридичної надійності: перший елемент – правомірна ідентифікація учасника; другий – визначеність його повноважень на внесення, підтвердження або перегляд даних; третій – автентичність джерела, включно з калібруванням датчика, акредитацією лабораторії чи перевіркою документа; четвертий – цілісність і хронологія запису; п'ятий – семантична сумісність ідентифікаторів, одиниць вимірювання та подій; шостий – контрольований доступ, правова підстава обробки й захист конфіденційності; сьомий – процедура виправлення, оскарження, аудиту та визначення відповідальності.

Право ЄС на електронні довірчі послуги посилює доказовий компонент. Регламент (ЄС) 2024/1183 включив електронні реєстри до системи довірчих послуг і встановив для кваліфікованого електронного реєстру презумпцію унікального й точного послідовного хронологічного впорядкування та цілісності записів [16]. Імплементативний регламент (ЄС) 2025/2531 конкретизував референтні стандарти та специфікації для кваліфікованих електронних реєстрів [17]. Ці акти важливі тим, що юридична довіра пов'язується не з назвою «блокчейн», а з кваліфікованим надавачем, процедурою нагляду, стандартами безпеки та презумпціями доказової сили.

М. Фінк наголошує, що розподілена технічна архітектура не означає відсутності врядування: правила доступу, механізми консенсусу, оновлення протоколу та розподіл ролей завжди є результатом певного рішення [18, р. 17–52, 177–203]. У дозвільній аграрній мережі необхідно юридично визначити оператора, валідаторів, власника стандарту даних, орган аудиту, процедуру приєднання та виходу, порядок зміни протоколу й право застосування до консорціуму. Інакше технологічне рішення створює приватну нормативну систему без належної підзвітності.

Особливу проблему становить захист даних. У дослідженні для Європейського парламенту М. Фінк показує, що незмінність і розподілене зберігання можуть конфліктувати з визначенням контролера, мінімізацією даних, обмеженням строку зберігання, виправленням і видаленням [19, р. 21–38, 61–86]. Загальний регламент про захист даних вимагає законності, цільового обмеження, мінімізації, точності, обмеження зберігання та захисту за проєктуванням [20]. Дані одноосібного

фермера, координати господарства, ідентифікатор працівника або підпис інспектора можуть бути персональними навіть у професійному контексті.

Для узгодження прозорості із захистом прав пропонується принцип вибіркової прозорості. Виробник, регулятор, покупець і споживач не повинні бачити однаковий масив інформації. Споживачеві може бути доступне підтвердження походження й сертифікації; покупцеві – документи партії та умови зберігання; компетентному органу – повний аудиторський слід; публіці – агреговані або криптографічно підтверджені показники. Персональні дані, комерційні умови, точні рецептури та відомості, що створюють безпековий ризик, доцільно зберігати поза ланцюгом, записуючи до реєстру лише хеш, часову позначку, ідентифікатор і правило доступу.

Регламент (ЄС) 2023/2854 про дані додає вимоги справедливого доступу до даних підключених продуктів, перенесення даних, договірної справедливості та інтероперабельності сервісів обробки даних [21]. Для аграрного сектору це означає, що виробник не повинен втрачати фактичний контроль над даними трактора, датчика чи системи точного землеробства через закриту платформу постачальника. Блокчейн-система, яка технічно незмінна, але юридично та економічно замикає користувача в одному сервісі, не відповідає меті справедливого цифрового ринку.

П. де Філіппі та А. Райт характеризують блокчейн як середовище, у якому програмний код може встановлювати та автоматично виконувати правила взаємодії [22, р. 29]. Однак «код як правило» не тотожний праву. Смарт-контракт може автоматично заблокувати партію за відсутності сертифіката, але правова система повинна визначити, чи існувала поважна причина затримки, чи можна виправити помилку та хто відповідає за неправомірне блокування. Автоматизація повинна залишати можливість людського перегляду в ситуаціях, що впливають на доступ до ринку, майнові права або засоби існування виробника.

Біла книга UN/CEFACT щодо блокчейну в торговельних процедурах підтверджує, що користь технології залежить від стандартизованих даних, управління ідентичністю, правової сумісності, кібербезпеки та взаємодії з існуючими системами [23, р. 9–12]. Міжнародний ланцюг не може функціонувати як один глобальний реєстр. Реалістичним є федеративний підхід, за якого національні, галузеві та приватні системи обмінюються перевірюваними повідомленнями за спільними стандартами, а правовий ефект іноземного запису визначається через функціональну еквівалентність і взаємне визнання.

Належна архітектура аграрної простежуваності повинна мати щонайменше п'ять рівнів. На нормативно-семантичному рівні визначаються мета, обов'язкові події, ідентифікатори та словники. На реєстровому рівні дозвільна мережа фіксує хеші документів, часові позначки, статуси й передачу відповідальності. На рівні захищеного сховища поза ланцюгом зберігаються повні документи та чутливі дані. На довірчому рівні електронні підписи, печатки, часові мітки та кваліфікований реєстр підтверджують автора, час і цілісність. На контрольному рівні компетентний орган, акредитована лабораторія або незалежний аудитор перевіряє зв'язок цифрового запису з фізичною подією.

Коригування помилки не повинно здійснюватися прихованим видаленням попереднього запису. Доцільно вносити новий запис, який містить посилання на первинний, підставу виправ-

лення, автора, час і статус наслідків. Якщо ж зберігання первинної інформації суперечить закону, персональні дані мають бути видалені або зроблені недоступними у позаланцюговому сховищі, а реєстр може зберігати лише доказ факту правомірної корекції. Такий підхід поєднує аудиторський слід із правом на виправлення.

Для малих і середніх виробників цифрова простежуваність створює не лише можливості, а й ризик виключення з ринку. Вартість датчиків, підписів, сертифікації, навчання та інтеграції може бути непропорційною. Тому обов'язкова система повинна передбачати відкриті стандарти, спрощені інтерфейси, колективні рішення для кооперативів, портативність даних, перехідні періоди та технічну допомогу. Недискримінація має оцінюватися не лише за однаковим текстом вимоги, а й за фактичною доступністю способу її виконання.

Для України пріоритетом є не створення ізольованого «національного аграрного блокчейну», а сумісність державних реєстрів, систем операторів ринку, електронних сертифікатів і митних даних із міжнародними стандартами та правом ЄС. Законодавство повинно визнавати функціонально еквівалентні іноземні електронні записи, визначати доказове значення кваліфікованих електронних реєстрів, установлювати правила відповідальності операторів і валідаторів та забороняти включення надлишкових персональних даних до незмінного ланцюга. Пілотні проєкти доцільно починати з конкретних товарних ланцюгів і юридично вимірюваних цілей: швидкості відкликання, підтвердження геолокації, справжності сертифіката або збереження холодового режиму.

Висновки. Міжнародно-правове забезпечення блокчейн-простежуваності має поліцентричний характер. Воно формується нормами COT, стандартами Codex Alimentarius і GS1, актами ЮНСІТРАЛ, рекомендаціями міжнародних організацій, правом електронних довірчих послуг, захисту даних та спеціальними правилами доступу аграрної продукції на ринок ЄС. Їх системне застосування важливіше за вибір конкретної програмної платформи.

Блокчейн не створює презумпції істинності первинної інформації. Він може підтверджувати послідовність і незмінність запису після внесення, але достовірність залежить від ідентифікації автора, компетентності джерела, перевірки фізичної події та процедур аудиту. Тому юридична модель повинна поєднувати технічний реєстр із довірчими послугами, акредитацією, державним контролем і можливістю оскарження.

Запропонована функціональна класифікація охоплює цілевстановлювальні, ідентифікаційно-стандартизаційні, доказово-довірчі, торговельно-контрольні, захисні та коригувальні інструменти. Семіелементний тест юридичної надійності дозволяє оцінити не рекламовані властивості технології, а здатність конкретної системи створювати належні й допустимі електронні докази.

Принцип вибіркової прозорості та багаторівнева архітектура забезпечують баланс між простежуваністю, захистом персональних і комерційних даних та інтересами малих виробників. Для транскордонного використання необхідні технологічна нейтральність, відкриті стандарти, семантична сумісність, функціональна еквівалентність і взаємне визнання. Саме така модель перетворює розподілений реєстр із засобу незмінного збереження даних на юридично керований інструмент відповідального сільськогосподарського виробництва.

Література:

1. Качурінер В. Л. Міжнародно-правові інструменти регулювання сфери виробництва. *Підприємство, господарство і право*. 2017. № 4. С. 192–196. URL: <https://pgp-journal.kiev.ua/eng/archive/2017/4/41.pdf>.
2. Качурінер В. Л. Правове регулювання відносин в сфері інформаційних комунікацій про стан навколишнього середовища за законодавством ЄС. *Юридичний науковий електронний журнал*. 2021. № 5. С. 327–330. DOI: <https://doi.org/10.32782/2524-0374/2021-5/77>.
3. Kachuriner V. L. Establishment of Environmental Standards of Production in the Law of the European Union. The Latest Development of the Modern Legal Sciences and Education in Ukraine and EU Countries: An Experience, Challenges, Expectations : collective monograph. Riga : Izdevniecība "Baltija Publishing", 2021. P. 263–278. DOI: <https://doi.org/10.30525/978-9934-26-033-9-15>.
4. Galvez J. F., Mejuto J. C., Simal-Gandara J. Future Challenges on the Use of Blockchain for Food Traceability Analysis. *TrAC Trends in Analytical Chemistry*. 2018. Vol. 107. P. 222–232. DOI: <https://doi.org/10.1016/j.trac.2018.08.011>.
5. Kamilaris A., Fonts A., Prenafeta-Boldú F. X. The Rise of Blockchain Technology in Agriculture and Food Supply Chains. *Trends in Food Science & Technology*. 2019. Vol. 91. P. 640–652. DOI: <https://doi.org/10.1016/j.tifs.2019.07.034>.
6. Tripoli M., Schmidhuber J. Emerging Opportunities for the Application of Blockchain in the Agri-food Industry. Rome ; Geneva : FAO ; ICTSD, 2018. 30 p. URL: https://www.researchgate.net/publication/327867089_Emerging_Opportunities_for_the_Application_of_Blockchain_in_the_Agri-food_Industry
7. Codex Alimentarius Commission. Principles for Traceability/Product Tracing as a Tool within a Food Inspection and Certification System. CAC/GL 60-2006. Rome : FAO ; WHO, 2006. 3 p. URL: https://www.fao.org/input/download/standards/10603/CXG_060e.pdf
8. GS1 Global Traceability Standard. Release 2.0. Brussels : GS1 AISBL, 2017. URL: <https://www.gs1.org/standards/traceability/traceability/2-0>
9. UNCITRAL Model Law on Electronic Transferable Records with Explanatory Note. New York : United Nations, 2018. 64 p. URL: https://uncitral.un.org/sites/default/files/media-documents/uncitral/en/mletr_ebook_e.pdf
10. Agreement on the Application of Sanitary and Phytosanitary Measures. The Legal Texts: The Results of the Uruguay Round of Multilateral Trade Negotiations. Cambridge : Cambridge University Press, 1999. P. 69–83. URL: https://www.wto.org/english/docs_e/legal_e/15-sps.pdf
11. Agreement on Technical Barriers to Trade. The Legal Texts: The Results of the Uruguay Round of Multilateral Trade Negotiations. Cambridge : Cambridge University Press, 1999. P. 117–137. URL: https://www.wto.org/english/docs_e/legal_e/17-tbt.pdf
12. Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law. *Official Journal of the European Communities*. 2002. L 31. P. 1–24. URL: <https://eur-lex.europa.eu/eli/reg/2002/178/oj/eng>
13. Commission Implementing Regulation (EU) No 931/2011 of 19 September 2011 on the traceability requirements set by Regulation (EC) No 178/2002 for food of animal origin. *Official Journal of the European Union*. 2011. L 242. P. 2–3. URL: https://eur-lex.europa.eu/eli/reg_impl/2011/931/oj/eng.
14. Regulation (EU) 2023/1115 of the European Parliament and of the Council of 31 May 2023 on the making available on the Union market and the export from the Union of certain commodities and products associated with deforestation and forest degradation. *Official Journal of the European Union*. 2023. L 150. P. 206–247. URL: <https://eur-lex.europa.eu/eli/reg/2023/1115/oj/eng>.

15. OECD-FAO Guidance for Responsible Agricultural Supply Chains. Paris : OECD Publishing, 2016. DOI: <https://doi.org/10.1787/9789264251052-en>.
16. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. *Official Journal of the European Union*. 2024. L 2024/1183. 47 p. URL: <https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng>
17. Commission Implementing Regulation (EU) 2025/2531 of 16 December 2025 laying down rules for the application of Regulation (EU) No 910/2014 as regards reference standards and specifications for qualified electronic ledgers. *Official Journal of the European Union*. 2025. L 2025/2531. 7 p. URL: https://eur-lex.europa.eu/eli/reg_impl/2025/2531/oj/eng.
18. Finck M. Blockchain Regulation and Governance in Europe. Cambridge : Cambridge University Press, 2019. 214 p. DOI: <https://doi.org/10.1017/9781108609708>.
19. Finck M. Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law? Brussels : European Parliamentary Research Service, 2019. 106 p. DOI: <https://doi.org/10.2861/535>.
20. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Union*. 2016. L 119. P. 1–88. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
21. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data. *Official Journal of the European Union*. 2023. L 2023/2854. 71 p. URL: <https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng>
22. De Filippi P., Wright A. Blockchain and the Law: The Rule of Code. Cambridge, MA : Harvard University Press, 2018. 300 p. DOI: <https://doi.org/10.4159/9780674985933>.
23. United Nations Centre for Trade Facilitation and Electronic Business. White Paper: Blockchain in Trade Facilitation. Geneva : United Nations, 2023. 64 p. URL: https://unctad.org/system/files/official-document/tcsdtlinf2023d1_en.pdf.

Kachuriner V. Distributed ledger technologies in the international legal framework for the traceability of agricultural products

Summary. The article examines the international legal prerequisites, functions, and limitations of using distributed ledger technologies, particularly blockchain, to ensure the traceability of agricultural products.

It is established that legal regulation in this field is developing at the intersection of international trade law, international food safety standards, electronic commerce

law, due diligence regimes in global supply chains, personal and commercial data protection, and European Union law.

It is substantiated that blockchain is neither an independent source of law, nor a quality certificate, nor proof of the veracity of primary information. Its legally significant function is to ensure the integrity, consistency, and controlled accessibility of records after they have been entered. Incorrect, incomplete, or unlawfully obtained information does not become reliable merely because it is immutably stored in a distributed ledger.

The author proposes a definition of the international legal framework for the digital traceability of agricultural products as a system of treaty-based rules, international standards, model-law instruments, supranational provisions, and cooperation procedures that determine mandatory traceability events, the entities responsible for entering and verifying data, the legal requirements applicable to electronic records, and the rules governing their cross-border recognition.

A functional classification of the relevant instruments is developed, comprising goal-setting, identification and standardisation, evidentiary and trust-based, trade and control, protective, and corrective instruments.

A seven-element test for assessing the legal reliability of a blockchain-based traceability system is formulated.

The appropriateness of a multi-layered model is demonstrated. Under this model, international and sectoral standards determine data semantics; a permissioned distributed ledger records traceability events; personal and commercially sensitive information is stored off-chain; qualified electronic trust services authenticate the author and time of a record; and a competent authority or independent auditor verifies the underlying event. This model makes it possible to reconcile traceability with the protection of producers' rights, non-discriminatory trade, and the mutual recognition of electronic evidence.

Key words: international law, agricultural products, traceability, blockchain, distributed ledger, electronic record, due diligence, international trade, data protection, European Union.

Використання штучного інтелекту. Під час підготовки статті інструменти штучного інтелекту не використовувалися.

Конфлікт інтересів: автор є членом редакційної колегії журналу. Для забезпечення незалежності редакційного процесу рукопис розглядався редактором, який не мав конфлікту інтересів з автором. Автор не брав участі у відборі рецензентів, процесі рецензування та прийнятті рішення щодо публікації статті. Рукопис пройшов стандартну процедуру подвійного сліпого рецензування.

Дата першого надходження статті до видання: 02.08.2026

Дата прийняття статті до друку після рецензування: 30.08.2026

Дата публікації (оприлюднення) статті: 01.10.2026



Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)