Науковий вісник НЛТУ України
Scientific Bulletin of UNFU
https://doi.org/10.36930/40360319
Article received: 27.03.2026
Article accepted: 27.05.2026
Article published: 29.06.2026
Correspondence author: N. E. Kunanets nek.lviv@gmail.com
ISSN 1994-7836 (print)
ISSN 2519-2477 (online)

UDC 004.[65+056]:623.44

Н. Е. Кунанець, Ю. А. Яримович
Національний університет "Львівська Політехніка", м. Львів, Україна

ВИКОРИСТАННЯ СМАРТ-КОНТРАКТІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОБЛІКУ ТОРГІВЛІ ЗБРОЄЮ

Досліджено проблему підвищення ефективності, безпеки та прозорості інформаційних систем обліку торгівлі зброєю в умовах посилення регуляторного контролю та зростання вимог до правомірності транзакцій. Обгрунтовано актуальність застосування сучасних децентралізованих підходів, зокрема – технології блокчейн і смарт-контрактів, для забезпечення надійного обліку операцій, мінімізації ризиків незаконного обігу зброї та підвищення рівня довіри до інформаційних систем у критично важливих середовищах. Запропоновано багаторівневу архітектуру інформаційної системи, що інтегрує мікросервісний підхід із блокчейн-інфраструктурою та забезпечує розподілене зберігання даних, їх незмінність і відстежуваність. Розроблено метод формалізованої перевірки умов правомірності транзакцій на основі кон'юнктивної логічної моделі, відповідно до якої виконання операції можливе тільки за умови одночасного дотримання всіх встановлених нормативних вимог. Смарт-контракти реалізовано як ключовий механізм автоматизованого контролю, який забезпечує превентивну валідацію транзакцій, мінімізує вплив людського фактора та підвищує достовірність ухвалення управлінських рішень. Проведене експериментальне дослідження на основі імітаційного моделювання підтвердило ефективність запропонованого підходу: точність визначення правомірності транзакцій становить 0,98–0,99, ймовірність виявлення некоректних операцій перевищує 0,97, а тривалість оброблення транзакцій змінюється в допустимих межах і зростає лінійно залежно від кількості умов перевірки. Встановлено компроміс між рівнем безпеки та продуктивністю системи, що зумовлює необхідність оптимізації структури смарт-контрактів. Новизна результатів дослідження полягає в інтеграції смарт-контрактів як механізму формалізованого контролю правомірності транзакцій у системах обліку торгівлі зброєю. Практична значущість результатів визначається можливістю їх застосування в інформаційних системах контролю обігу зброї та інших критичних середовищах, що потребують високого рівня довіри, прозорості та автоматизації контролю.

Ключові слова: блокчейн-технології; децентралізовані реєстри; автоматизований контроль операцій; валідація транзакцій; логічні моделі перевірки умов проходження транзакції; кібербезпека; відстежуваність даних; цифрові реєстри; управління доступом; розподілені системи.

Вступ / Introduction

За сучасних умов зростання глобальних безпекових викликів та посилення контролю за обігом озброєння особливої ваги набуває проблема забезпечення прозорого, надійного та контрольованого обліку операцій із торгівлі зброєю. Ефективне функціонування відповідних інформаційних систем є критично важливим як для державного управління, так і для міжнародного співробітництва у сфері нерозповсюдження та протидії незаконному обігу зброї. Водночас, традиційним централізованим підходам до організації обліку характерні обмежена довіра до даних, ризики несанкціонованого втручання, складність аудиту та відсутність повної відстежуваності життєвого циклу об'єктів обліку.

Відповідно до зазначених викликів активно розвиваються підходи, засновані на використанні технології блокчейн, яка забезпечує децентралізоване зберігання даних, їх незмінність та криптографічний захист. Одним із ключових елементів цієї технології є смарт-контракти – програмні механізми, що автоматично виконують заздалегідь визначені умови угод. Їх застосування дає змогу формалізувати правила оброблення транзакцій, забезпечити автоматичний контроль відповідності операцій нормативним вимогам, а також мінімізувати вплив людського фактора під час ухвалення управлінських рішень.

Попри значну кількість досліджень у сфері застосування блокчейн-технологій у фінансових та логістичних системах, питання інтеграції смарт-контрактів в інформаційні системи обліку торгівлі зброєю залишаються недостатньо опрацьованими. Зокрема, потребують подальшого дослідження аспекти формалізації умов правомірності транзакцій, побудови архітектури системи з урахуванням вимог безпеки та нормативного регулювання, а також забезпечення ефективної взаємодії між суб'єктами обліку.

Отже, запропоноване дослідження спрямоване на роз-

Кунанець Наталія Едуардівна, д-р наук із соціальних комунікацій, професор, кафедра інформаційних систем та мереж.
Email: nek.lviv@gmail.com; https://orcid.org/0000-0003-3007-2462
Яримович Юрій Андрійович, аспірант, кафедра інформаційних систем та мереж.
Email: yuyarym@gmail.com; https://orcid.org/0009-0006-1391-3214
Цитування за ДСТУ: Кунанець Н. Е., Яримович Ю. А. Використання смарт-контрактів в інформаційній системі обліку торгівлі зброєю. Науковий вісник НЛТУ України. 2026, т. 36, № 3. С. 180–187.
Citation APA: Kunanets, N. E., & Yarymovych, Yu. A. (2026). Use of smart contracts in the information system of accounting of arms trade. *Scientific Bulletin of UNFU*, 36(3), 180–187. https://doi.org/10.36930/40360319

виток теоретичних і практичних засад побудови інформаційної технології у сфері обліку торгівлі зброєю з використанням сучасних децентралізованих підходів.

Об'єкт дослідження – процеси обліку та контролю операцій у сфері торгівлі зброєю, що реалізуються в інформаційних системах.

Предмет дослідження – методи і засоби використання смарт-контрактів у складі інформаційної системи обліку торгівлі зброєю, що забезпечують формалізацію умов виконання транзакцій, автоматизований контроль їх правомірності, а також зменшення впливу людського фактора.

Мета роботи – розробити метод використання смарт-контрактів в інформаційній системі обліку торгівлі зброєю, який забезпечить автоматизацію контролю операцій, підвищення надійності, прозорості та продуктивності роботи системи, а також інтеграцію механізмів перевірки умов правомірності транзакцій у єдиний інформаційний контур.

Для досягнення зазначеної мети визначено такі основні *завдання дослідження*:

- проаналізувати особливості обліку торгівлі зброєю та визначити вимоги до інформаційної системи, що дасть можливість обґрунтувати функціональні та безпекові характеристики інформаційної системи;
- розробити концептуальну модель використання смарт-контрактів для автоматизації контролю транзакцій, що дасть можливість підвищити рівень надійності, прозорості та продуктивності інформаційної системи, а також вилучити вплив людського фактора;
- формалізувати умови правомірності виконання операцій і механізми перевірки умов проходження транзакції в інформаційній системі, що дасть можливість забезпечити автоматичний контроль відповідності транзакцій нормативним вимогам.

Аналіз останніх досліджень та публікацій. У дослідженні [19] автори проаналізували застосування блокчейн-технологій у поєднанні з цифровими двійниками для прогнозування станів у медичних системах та показали, що інтеграція смарт-контрактів забезпечує автоматизацію процесу оброблення транзакції даних і підвищення достовірності ухвалення управлінських рішень, що підтверджує ефективність використання технології блокчейну в критичних інформаційних системах. У роботі [7] дослідники запропонували підхід до використання цифрових двійників для моделювання смарт-контрактів, що дає змогу підвищити їх надійність і передбачуваність поведінки, а також забезпечити формалізований контроль виконання логіки контрактів у складних системах. У дослідженні [1] автори розглянули використання смарт-контрактів для побудови безпечних цифрових двійників у медичних інформаційних системах і довели, що технологія блокчейн дає змогу забезпечити захист даних, їх цілісність та контроль доступу в розподіленому середовищі.

У роботі [18] дослідники проаналізували використання технології блокчейну та цифрових двійників у системах управління IoT і показали, що смарт-контракти можна використовувати як механізм координації та автоматизації взаємодії між компонентами розподілених систем. У дослідженні [8] автори вказали на можливості використання блокчейн-технологій для підвищення безпеки та прозорості цифрових двійників, зокрема – шляхом використання смарт-контрактів для контролю операцій і забезпечення незмінності даних. У роботі [22] дослідники запропонували метод забезпечення безпеки транзакцій у розподілених системах на основі технології блокчейну та доказів із нульовим розголошенням, що дає змогу підвищити рівень захисту даних і конфіденційності під тривалість виконання транзакцій.

У дослідженні [25] автор розглянув використання гомоморфного шифрування та zero-knowledge proof у блокчейн-системах і показав, що такі підходи дають змогу реалізувати безпечні механізми перевірки умов проходження транзакції без розкриття конфіденційної інформації. У роботі [4] дослідники проаналізували використання блокчейн-технологій у ланцюгах постачання та відзначили їх здатність забезпечувати прозорість, відстежуваність та контроль операцій, що є релевантним для систем обліку та контролю транзакцій. У працях [12, 16] автори дослідили застосування блокчейн-технологій у системах обліку та контролю, зокрема – у ланцюгах постачання, де було показано ефективність використання розподілених реєстрів для забезпечення відстежуваності об'єктів, підтвердження їх походження та формування прозорих механізмів аудиту транзакцій.

У дослідженні [9] автори проаналізували протоколи другого рівня блокчейн-мереж і показали, що їх використання дає змогу підвищити масштабованість і продуктивність систем, що є важливим для оброблення транзакції великої кількості транзакцій. У роботі [17] дослідники запропонували інтеграцію zk-rollup із блокчейн-технологіями для підвищення масштабованості та безпеки систем оброблення транзакції даних, що підтверджує перспективність використання сучасних криптографічних підходів у розподілених інформаційних системах.

Отже, аналіз останніх досліджень та публікацій свідчить про активний розвиток підходів до використання блокчейн-технологій і смарт-контрактів у різних галузях, зокрема – у сфері безпеки, аудиту, управління доступом та обробленням транзакцій. Водночас, питання застосування цих технологій у системах обліку торгівлі зброєю з урахуванням жорстких вимог до правомірності операцій, формалізації умов перевірки умов проходження транзакції та інтеграції у комплексні інформаційні системи залишаються недостатньо дослідженими, що обґрунтовує необхідність проведення цього дослідження.

Водночас, проведений аналіз літературних джерел інформації показав, що у розглянутих дослідженнях недостатньо висвітлено питання застосування смарт-контрактів саме у сфері обліку торгівлі зброєю, де необхідним є забезпечення підвищених вимог до правомірності операцій, багаторівневого контролю та жорсткої валідації транзакцій. Окрім цього, у наявних роботах обмежено розглянуто інтеграцію смарт-контрактів у комплексні інформаційні системи, що поєднують модулі збирання даних, аналітики та ухвалення управлінських рішень, а також недостатньо досліджено формалізацію умов виконання транзакцій у вигляді строгих логічних моделей з урахуванням нормативно-правових вимог.

Отже, на відміну від наявних підходів, виникає науково-практична потреба у розробленні методів використання смарт-контрактів в інформаційних системах обліку торгівлі зброєю, які забезпечують формалізований контроль проходження транзакцій, підвищений рівень безпеки та автоматизацію перевірки умов правомірності транзакцій.

Матеріали та методи дослідження. У роботі використано методи системного аналізу, логічного моделю-

вання та формалізації контролю транзакцій для опису процесів обліку торгівлі зброєю і перевірки умов правомірності транзакцій. Для обґрунтування використання смарт-контрактів застосовано підходи до моделювання бізнес-процесів та методи побудови розподілених інформаційних систем. Архітектуру системи сформовано на основі поєднання мікросервісного підходу та блокчейн-інфраструктури з інтеграцією смарт-контрактів як компонента контролю виконання операцій. Ефективність запропонованих рішень оцінено з використанням методів порівняльного аналізу та імітаційного моделювання за показниками безпеки, надійності, прозорості та продуктивності інформаційної системи.

Результати дослідження та їх обговорення / Research results and their discussion

Інформаційна система обліку торгівлі зброєю належить до класу критично важливих систем, для яких ключовими є вимоги безпеки, достовірності даних, повної відстежуваності операцій та строгого дотримання нормативно-правових обмежень. У таких системах будь-яка транзакція повинна проходити багаторівневу перевірку, що охоплює ідентифікацію суб'єктів, наявність відповідних дозволів, відповідність операції встановленим правилам та обмеженням. Традиційні централізовані підходи не завжди забезпечують належний рівень довіри, оскільки передбачають наявність єдиного центру управління, що може бути вразливим до зовнішніх і внутрішніх загроз.

Задля підвищення ефективності та надійності обліку пропонують використання технології блокчейн із інтеграцією смарт-контрактів як механізму автоматизованого контролю виконання операцій. Смарт-контракт у цьому контексті розглядають як формалізовану програмну модель, що реалізує перевірку умов проходження транзакції та ухвалення управлінського рішення щодо її виконання.

Формально процес перевірки умов контракту можна подати у вигляді такого функціонального відображення:

$$P_i = f(c_i),\ i = \overline{1,n}\,, \tag{1}$$

де: $C = \{c_i,\ i = \overline{1,n}\}$ – множина умов, які мають бути виконані для здійснення i-ої транзакції з придбання вогнепальної зброї; P_i – результат перевірки i-ої умови проходження транзакції, що визначає можливість здійснення операції.

У системах обліку торгівлі зброєю доцільним є використання жорсткої логічної моделі контролю, яка передбачає проходження транзакції тільки за умови дотримання всіх потрібних вимог:

$$P_i = \bigwedge_{j=1}^{n} c_j,\ i = \overline{1,n}\,. \tag{2}$$

Модель, подана на рис. 1, означає, що i-та транзакція може бути виконана тільки у випадку, якщо всі без винятку умови виконані одночасно, зокрема – наявність дійсної ліцензії у продавця, відповідність покупця встановленим правовим вимогам, наявність дозволу на конкретний тип зброї, перевірка походження та реєстрації об'єкта обліку, відсутність обмежень або заборон на проведення операції, а також відповідність транзакції регламентованим процедурам контролю.

Якщо хоча б одна з умов C_j не виконується (тобто $C_j = 0$), то результат всієї логічної функції також дорівнює нулю ($p_i = 0$), і транзакція автоматично відхиляється смарт-контрактом. Такий підхід забезпечує жорсткий контроль правомірності операцій, неможливість часткового виконання умов, автоматичне блокування ризикових або незаконних транзакцій та відповідність нормативним вимогам і стандартам безпеки.

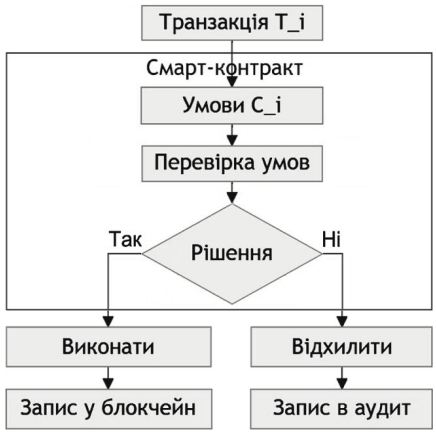

Рис. 1. Формалізована модель смарт-контракту для перевірки умов проходження транзакції та ухвалення управлінського рішення щодо її виконання / Formalised smart contract model for verifying the conditions for a transaction to proceed and making a management decision regarding its execution

Використання кон'юнктивної логічної моделі є обґрунтованим для критичних систем, зокрема – у сфері торгівлі зброєю, де ключовим є принцип: *"дозволено тільки те, що повністю відповідає всім встановленим вимогам"*. Така модель вилучає можливість часткового виконання умов і гарантує повну правомірність операції, що є критично важливим для цієї предметної області.

Архітектура запропонованої інформаційної системи обліку продажу зброї реалізується як багаторівнева структура, що поєднує традиційні компоненти оброблення транзакції даних із блокчейн-інфраструктурою. Основними складовими системи є:

- модуль збирання та інтеграції даних (журнали подій, реєстри, зовнішні інформаційні джерела);
- модуль попереднього оброблення транзакції та нормалізації даних;
- модуль аналітики та формування умов транзакцій;
- модуль смарт-контрактів, що реалізує перевірку та виконання операцій;
- блокчейн-реєстр для зберігання інформації про транзакції;
- інтерфейс взаємодії з користувачами та зовнішніми системами.

Взаємодія між компонентами здійснюється через API та механізми обміну повідомленнями, що забезпечує масштабованість і гнучкість системи. Смарт-контракти виступають центральним елементом контролю, оскільки саме вони реалізують логіку перевірки умов правомірності транзакцій і фіксації отриманих результатів транзакцій у розподіленому реєстрі.

Процес проходження транзакції в інформаційній системі містить послідовність взаємопов'язаних етапів, кожен із яких можна формалізувати математично (рис. 2).

На етапі ініціації операції користувач формує запит транзакції:

$$T_i = \langle u_i,\ o_i,\ t_i \rangle,\ i = \overline{1,m}\,, \tag{3}$$

де: u_i – i-ий суб'єкт (користувач) операції; o_i – i-ий об'єкт операції (зброя); t_i – i-ий часовий параметр. Цей етап забезпечує фіксацію наміру здійснення операції та ідентифікацію її учасників.

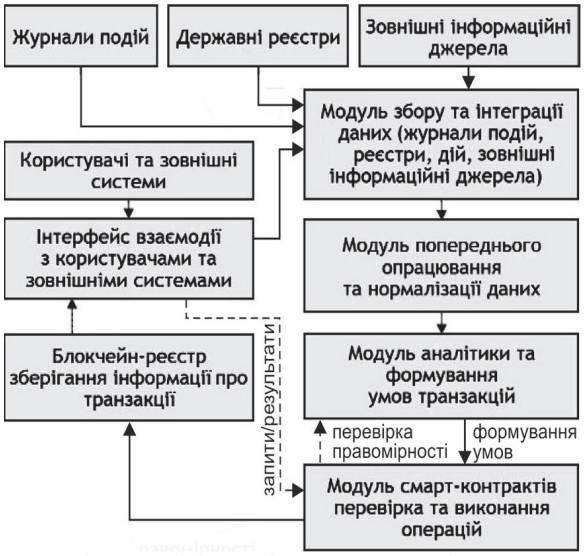

Рис. 2. Архітектура інформаційної системи обліку продажу зброї / Architecture of the information system for recording weapons saes

На етапі формування набору умов визначається множина критеріїв правомірності транзакції згідно з формулою (1), де кожна умова c_j відображає окрему перевірку (ліцензія, дозволи, обмеження тощо). Формально кожну умову можна подати як булеву функцію:

$$c_j = f_j(T) \in \{0,1\},\ j = \overline{1,n}\ , \tag{4}$$

де: $T = \{t_i,\ i = \overline{1,m}\}$ – виконана i-та транзакція, яка містить усі вхідні дані операції (суб'єкт, об'єкт, параметри, час тощо); $f_i(\cdot)$ – функція перевірки j-ої умови проходження транзакції, яка аналізує транзакцію T_i та визначає, чи виконується відповідний критерій; c_j – результат перевірки умов проходження j-ої транзакції (логічна змінна).

На етапі передачі умов у смарт-контракт відбувається виклик функції контракту

$$SC : (T_i, C_i) \to P_i,\ i = \overline{1,m}\ , \tag{5}$$

де: SC – смарт-контракт, що реалізує логіку перевірки умов проходження транзакції; P_i – результат виконання i-ої функції контракту.

Етап автоматичної перевірки умов проходження транзакції базується на кон'юнктивній логічній моделі (2), згідно з якою транзакція можлива тільки у разі виконання всіх умов, передбачених для здійснення транзакції з придбання вогнепальної зброї (зокрема перевірки правомірності покупця, наявності ліцензії продавця, відповідності типу зброї, відсутності обмежень та коректності оформлення документів). Це забезпечує строгий контроль і вилучає часткову валідність.

На етапі ухвалення управлінського рішення результат перевірки умов проходження транзакції інтерпретується як:

$$P_i = \begin{cases} 1, \text{ якщо транзакцію дозволено;} \\ 0, \text{ якщо транзакцію відхилено,} \end{cases} \tag{6}$$

де: $P_i = 1$ означає дозвіл виконання i-ої функції контракту; $P_i = 0$ – відхилення i-ої транзакції (рис. 3).

Завершальним є етап запису результату у технології блокчейн, який можна подати як операцію додавання нового запису до розподіленого реєстру:

$$B_{k+1} = B_k \cup \{T_i, P_i\},\ \forall i \in m; \forall k \in K\ , \tag{7}$$

де: B_k – поточний стан реєстру; B_{k+1} – оновлений стан після додавання транзакції; K – кількість розподілених реєстрів, для яких можна здійснити операцію додавання нового запису. Це забезпечує незмінність, відстежуваність та можливість аудиту всіх операцій.

Рис. 3. Процес проходження транзакції в інформаційній системі обліку торгівлі зброєю з використанням смарт-контрактів / The process of transaction execution in the information system for recording weapons trade using smart contracts

Отже, формалізація кожного етапу дає змогу подати процес проходження транзакції як послідовність математично визначених перетворень, що підвищує обґрунтованість і надійність функціонування інформаційної системи. У разі невиконання хоча б однієї з умов транзакція відхиляється, а відповідна інформація фіксується для подальшого аудиту.

Важливим аспектом є забезпечення безпеки та довіри до системи. Використання криптографічних механізмів технології блокчейн гарантує незмінність записів, а децентралізована природа системи усуває ризики, пов'язані з централізованим управлінням. Окрім цього, реалізація смарт-контрактів дає змогу мінімізувати вплив людського фактора, автоматизуючи процес ухвалення управлінських рішень.

Запропонований підхід до використання смарт-контрактів в інформаційній системі обліку торгівлі зброєю забезпечує формалізацію та автоматизацію ключових процесів, підвищує рівень безпеки, прозорості та ефективності функціонування системи, а також створює передумови для побудови довіреної цифрової інфраструктури у даній предметній області.

Унаслідок цього проведеного дослідження розроблено концептуальну модель інформаційної системи обліку торгівлі зброєю, у якій смарт-контракти інтегровані як ключовий механізм автоматизованого контролю транзакцій. Запропонована модель передбачає побудову єдиного інформаційного контуру, що об'єднує модулі збирання даних, перевірки умов правомірності транзакцій, ухвалення управлінських рішень та виконання операцій, при цьому смарт-контракти виконують функцію формалізованого контролера правомірності.

Експериментальне дослідження. Експериментальне дослідження спрямоване на оцінювання ефективності запропонованого підходу до використання смарт-контрактів в інформаційній системі обліку торгівлі зброєю за показниками безпеки, надійності, продуктивності та коректності виконання транзакцій.

Дослідження проводилося на основі моделювання розподіленої інформаційної системи, що містить мікросервісну архітектуру з інтегрованим блокчейн-рівнем.

Система складалася з модулів збирання та оброблення транзакції даних, аналітики, смарт-контрактів та блокчейн-реєстру. Для реалізації смарт-контрактів використовувалася модель, що базується на кон'юнктивній логічній перевірці умов проходження транзакції.

В експерименті було змодельовано набір транзакцій (формула (4)), де кожній транзакції характерна множина умови (1).

Перевірка транзакцій здійснювалася відповідно до моделі (4). Для оцінювання ефективності було використано таку метрику, як точність контролю транзакцій, що визначається як відношення коректно класифікованих транзакцій до загальної кількості [11]:

$$Accuracy = \frac{Ncorrect}{N},$$

де: *Accuracy* – точність роботи інформаційної системи, тобто частка правильно класифікованих транзакцій (як дозволених, так і відхилених); *Ncorrect* – кількість транзакцій, для яких система прийняла правильне рішення (правильно дозволила або правильно відхилила); *N* – загальна кількість усіх опрацьованих транзакцій у системі.

Використовуючи цю формулу, визначимо, яку частину всіх транзакцій система опрацювала коректно. Значення $Accuracy \in [0,1]$, де $Accuracy \approx 1$ – система працює дуже точно; $Accuracy \approx 0$ – система працює некоректно. У контексті системи обліку торгівлі зброєю цей показник є критично важливим, оскільки висока точність означає мінімізацію ризику як пропуску незаконних операцій, так і помилкового блокування дозволених транзакцій.

У табл. 1 подано результати розрахунків точності роботи інформаційної системи для різних сценаріїв. Значення точності наведено з урахуванням варіації, отриманої шляхом моделювання декількох сценаріїв із незначним варіюванням вхідних параметрів. Невелике відхилення пояснюється детермінованим характером логічної моделі перевірки умов транзакцій. Отримані результати демонструють, що точність системи перебуває в межах 0,96–0,98 для розглянутих сценаріїв. Це дає змогу зробити попередній висновок про потенційно високий рівень ефективності запропонованого підходу. Водночас, наведені значення отримано в межах окремих сценаріїв і потребують додаткової статистичної верифікації на розширених вибірках даних.

Табл. 1. Результати розрахунку точності роботи інформаційної системи / Results of accuracy calculations for the operation of the information system

№ сценарію	Загальна кількість транзакцій *N*	Правильно класифіковані $N_{correct}$	Accuracy
1	1000	970	$0{,}97^{\pm 0{,}01}$
2	1500	1440	$0{,}96^{\pm 0{,}015}$
3	2000	1920	$0{,}96^{\pm 0{,}012}$
4	2500	2450	$0{,}98^{\pm 0{,}01}$
5	3000	2910	$0{,}97^{\pm 0{,}013}$

Розглянемо можливість оцінювання ефективності роботи інформаційної системи за показником ймовірності виявлення некоректних операцій [11]:

$$P_{detect} = \frac{N_{invalid\,detected}}{N_{invalid}},$$

де: $N_{invalid\ detected}$ – кількість некоректних (нелегітимних) транзакцій, які система успішно виявила; $N_{invalid}$ – загальна кількість фактично некоректних транзакцій у системі.

Табл. 2. Результати розрахунків виконання сценаріїв / Results of scenario execution calculations

№ сценарію	Некоректні транзакції $N_{invalid\ detected}$	Виявлені некоректні $N_{invalid}$	$T_{proc} = 85$
1	200	190	0,95
2	300	285	0,95
3	400	392	0,98
4	500	485	0,97
5	600	582	0,97

Отримані значення (табл. 2) $P_{detect} \in [0{,}95;\ 0{,}98]$ свідчать про високий рівень здатності системи виявляти некоректні або незаконні транзакції. Це означає, що більшість порушень ефективно ідентифікуються смарт-контрактами, ризик пропуску незаконних операцій є мінімальним, а система забезпечує високий рівень безпеки та контролю. Навіть за зростання кількості некоректних транзакцій система зберігає стабільно високий рівень виявлення, що підтверджує ефективність запропонованого підходу для критичних систем, зокрема – у сфері торгівлі зброєю.

Розглянемо можливість оцінювання ефективності роботи інформаційної системи за показником тривалості оброблення транзакції [24]:

$$T_{proc} = T_{check} + T_{exec} + T_{blockchain},$$

де: T_{check} – тривалість перевірки умов проходження транзакції; T_{exec} – тривалість здійснення операції; T_{proc} – загальна тривалість оброблення транзакції; $T_{blockchain}$ – тривалість запису результату у технології блокчейн.

Для дослідження сформовано п'ять типових сценаріїв оброблення транзакцій, що відрізняються рівнем складності перевірки умов, кількістю задіяних механізмів контролю та інтенсивністю взаємодії з блокчейн-середовищем. Сценарії відображають поступове ускладнення процесу оброблення транзакції – від базової перевірки до комплексної багаторівневої верифікації із фіксацією результатів у розподіленому реєстрі. Характеристики кожного сценарію та відповідні значення параметрів наведено в табл. 3. Отримані результати свідчать, що зі зростанням складності перевірки умов проходження транзакції і збільшенням тривалості запису у технології блокчейн загальна тривалість оброблення транзакції також зростає. Водночас, навіть у п'ятому сценарії значення T_{proc} = 85 мс залишається прийнятним для практичного використання в інформаційній системі обліку торгівлі зброєю.

Табл. 3.. Результати розрахунків загальної тривалості оброблення транзакції / Results of calculations of the total transaction processing time

№ сценарію	T_{check}, мс	T_{exec}, мс	$T_{blockchain}$, мс	T_{proc}, мс
1	12	8	25	45
2	15	10	30	55
3	18	12	34	64
4	22	14	39	75
5	25	16	44	85

Узагальнено можна зазначити, що основний внесок у затримку оброблення транзакції робить блокчейн-компонент, тоді як тривалість перевірки умов проходження транзакції та здійснення операції є меншим. Це підтверджує доцільність оптимізації саме механізмів

фіксації транзакцій у розподіленому реєстрі для підвищення загальної продуктивності інформаційної системи.

Для тексту роботи це можна подати так: за результатами розрахунків на гіпотетичних даних встановлено, що загальна тривалість оброблення транзакції змінюється в межах від 45 до 85 мс залежно від складності перевірки умов проходження транзакції, тривалості здійснення операції та тривалості запису в технології блокчейн, при цьому найбільший вплив на значення T_{proc} має блокчейн-компонент.

У процесі проведення експерименту було змодельовано різні сценарії навантаження (від 100 до 10 000 транзакцій), а також варіанти з різною кількістю умов n. Результати показали, що зі збільшенням кількості умов зростає тривалість перевірки умов проходження транзакції, проте зберігається висока точність контролю.

Зокрема, встановлено, що точність визначення правомірності транзакцій наближається до 1 (≈0,98-0,99), ймовірність виявлення некоректних операцій перевищує 0,97, а середня тривалість оброблення транзакції залишається прийнятною для практичного використання та зростає лінійно залежно від кількості умов.

Порівняльний аналіз із традиційними централізованими системами показав, що запропонований підхід забезпечує вищий рівень достовірності перевірок і значно знижує ризик пропуску некоректних операцій. Окрім цього, використання блокчейн-реєстру гарантує незмінність результатів і можливість аудиту.

Водночас, експеримент підтвердив наявність компромісу між рівнем безпеки та продуктивністю системи, збільшення кількості перевірок підвищує надійність, але впливає на затримки оброблення транзакції. Це вимагає оптимізації структури смарт-контрактів та балансування кількості умов.

Отже, результати експериментального дослідження підтверджують ефективність використання смарт-контрактів для автоматизованого контролю транзакцій у системах обліку торгівлі зброєю та демонструють доцільність впровадження запропонованого підходу в практичні інформаційні системи.

Обговорення результатів дослідження. Отримані результати підтверджують, що використання смарт-контрактів в інформаційній системі обліку торгівлі зброєю є доцільним з погляду забезпечення прозорості, контрольованості та автоматизації перевірки умов проходження транзакції. Високі значення точності визначення правомірності транзакцій і ймовірності виявлення некоректних операцій узгоджуються з висновками праць, у яких технологію блокчейн розглядають як засіб підвищення прозорості, простежуваності та підзвітності в системах обліку й ланцюгах постачання [12, 16].

На відміну від робіт, де основний акцент зроблено на загальних перевагах технології блокчейну для управління ланцюгами постачання, зокрема – підвищенні прозорості, зниженні ризиків та покращенні простежуваності [16], у запропонованому підході увагу зосереджено саме на жорсткому логічному контролі правомірності транзакцій у критичній предметній області. Це дає змогу не тільки фіксувати факт здійснення операції, а й блокувати її ще до виконання, якщо не виконано хоча б одну нормативну умову. Такий результат розвиває ідеї превентивного, а не тільки реєстраційного контролю.

Отримані висновки також узгоджуються з дослідженням [6], у якому смарт-контракти визначаються як механізм автоматизації багатокрокових процесів у середовищі взаємодії учасників без єдиного довіреного посередника. У контексті цієї роботи це положення набуває прикладного розвитку, оскільки смарт-контракт інтерпретується як формалізований програмний модуль перевірки умов проходження транзакції ліцензій, дозволів, походження об'єкта обліку та інших регламентних обмежень. Водночас, результати дослідження підтверджують і ті обмеження, на які вказують інші автори. Зокрема, в роботі [2] показано, що смарт-контракти можуть містити вразливості, пов'язані з помилками програмної логіки, а в роботі [14] наголошують на необхідності автоматизованого аналізу коду смарт-контрактів для виявлення небезпечних конструкцій. Це означає, що для практичного впровадження запропонованої системи у сфері обліку торгівлі зброєю недостатньо тільки формалізувати правила контролю; також потрібно забезпечити верифікацію та аудит коду самих контрактів, оскільки помилка в реалізації може призвести до некоректного дозволу або блокування транзакції.

Результати щодо прийнятної тривалості оброблення транзакцій також узгоджуються з науковими публікаціями, у яких технологія блокчейн одночасно створює нові можливості для підвищення довіри й аудиту, але може обмежувати продуктивність через додаткові операції консенсусу, запису та перевірки умов проходження транзакції [16, 20]. Тому в межах запропонованого підходу доцільним є використання не публічної, а permissioned-архітектури технології блокчейну, оскільки саме такі моделі спеціально орієнтовані на керованість, аудитованість і безпечне адміністрування в корпоративних або міжорганізаційних системах [3].

Окремо потрібно відзначити, що отримані результати корелюють із підходами до побудови захищених журналів подій та аудиту на основі permissioned blockchain. У дослідженні [15] показано, що технологія блокчейн-орієнтована інфраструктура журналювання забезпечує цілісність і невідмовність записів. Для системи обліку торгівлі зброєю це особливо важливо, оскільки результати перевірки умов проходження транзакції мають бути не тільки коректними, а й доказово збереженими для подальшого контролю, розслідування чи регуляторного аудиту.

У дослідженні [5] автори проаналізували сучасний стан застосування блокчейн-технологій, класифікували основні напрями їх використання та вказали на наявність відкритих проблем, зокрема – недостатню формалізацію прикладних сценаріїв у специфічних предметних областях, що підтверджує актуальність запропонованого підходу до формалізації контролю транзакцій у сфері обліку торгівлі зброєю.

У роботі [10] дослідники здійснили системний аналіз питань безпеки та конфіденційності блокчейн-систем і наголосили на важливості інтеграції механізмів захисту та верифікації смарт-контрактів, що узгоджується з отриманими результатами щодо потреби забезпечення надійності програмної реалізації логіки перевірки умов проходження транзакції. У дослідженні автори розглянули використання смарт-контрактів у системах аудиту та показали, що їх застосування дає змогу автоматизувати перевірку відповідності операцій встановленим правилам.

У дослідженні [13] автори проаналізували основні загрози безпеці блокчейн-систем та класифікували вразливості, пов'язані зі смарт-контрактами, що підтвер-

джує доцільність використання формалізованих моделей перевірки умов проходження транзакції для мінімізації ризиків некоректних або небезпечних операцій.

У дослідженні [22] автори розглянули питання забезпечення безпеки транзакцій у розподілених системах і відзначили роль блокчейн-технологій як механізму гарантування цілісності, незмінності та захищеності даних, що корелює з отриманими результатами щодо підвищення достовірності та відстежуваності облікових транзакцій. У дослідженні [21] автори запропонували архітектурні підходи до побудови блокчейн-застосунків і визначили ключові компоненти інтеграції смарт-контрактів в інформаційні системи, що узгоджується із запропонованою в роботі багаторівневою архітектурою та підтверджує її практичну обґрунтованість.

У роботі [23] дослідники розглянули використання смарт-контрактів для управління доступом у розподілених середовищах та довели їх ефективність для автоматизованого ухвалення управлінських рішень, що підтверджує доцільність застосування смарт-контрактів як механізму перевірки умов правомірності транзакцій у запропонованій системі.

Отже, порівняння з науковими публікаціями показує, що отримані результати загалом узгоджуються з відомими висновками щодо переваг технології блокчейну і смарт-контрактів у частині прозорості, простежуваності, автоматизації та аудиту, але, водночас, конкретизують їх для значно жорсткішої предметної області – обліку торгівлі зброєю. На відміну від більшості наявних праць, де розглядають логістичні, IoT- або загальноуправлінські сценарії, у цій роботі акцент зроблено на попередньому блокуванні неправомірних транзакцій на основі кон'юнктивної моделі контролю, що є істотною відмінністю запропонованого підходу.

Отже, внаслідок виконаної роботи можна сформулювати такі наукову новизну та практичну значущість результатів дослідження.

Наукова новизна отриманих результатів дослідження – отримав подальший розвиток метод формалізованого контролю транзакцій в інформаційних системах обліку торгівлі зброєю, який, на відміну від наявних методів, базується на використанні жорсткої кон'юнктивної логічної моделі перевірки умов проходження транзакції, забезпечує інтеграцію процесів валідації та виконання операцій у єдиний автоматизований контур, що дає змогу підвищити рівень безпеки, достовірність та правомірність облікових транзакцій.

Практична значущість результатів дослідження – можливість впровадження запропонованого підходу з використання смарт-контрактів в інформаційні системи обліку торгівлі зброєю, що забезпечує підвищення рівня безпеки, прозорості та достовірності транзакцій, автоматизацію контролю їх правомірності, зменшення впливу людського фактора та забезпечення повної відстежуваності операцій у розподіленому середовищі.

Висновки / Conclusions

Розроблено метод використання смарт-контрактів в інформаційній системі обліку торгівлі зброєю, який забезпечує автоматизацію контролю операцій, підвищення надійності, прозорості та продуктивності інформаційної системи, а також інтеграцію механізмів перевірки умов правомірності транзакцій у єдиний інформаційний контур. За результатами проведеного дослідження можна зробити такі основні висновки:

1. Систематизовано підходи до використання блокчейн-технологій і смарт-контрактів в інформаційних системах контролю транзакцій на підставі аналізу сучасних наукових досліджень, внаслідок чого сформовано концептуальну основу їх застосування у сфері обліку торгівлі зброєю.
2. Запропоновано архітектуру інформаційної системи обліку торгівлі зброєю, що поєднує мікросервісний підхід із блокчейн-інфраструктурою та інтегрує смарт-контракти як компонент автоматизованого контролю, внаслідок чого забезпечено підвищення прозорості, відстежуваності та надійності оброблення транзакцій.
3. Розроблено метод формалізованого контролю транзакцій на основі жорсткої кон'юнктивної логічної моделі перевірки умов правомірності транзакцій, внаслідок чого забезпечено автоматичне блокування некоректних операцій і підвищено рівень безпеки системи.
4. Сформовано модель процесу проходження транзакції з використанням смарт-контрактів, що містить етапи ініціації, перевірки умов проходження транзакції, ухвалення управлінського рішення та фіксації отриманих результатів, внаслідок чого забезпечено формалізацію та автоматизацію життєвого циклу транзакцій.
5. Проведено експериментальне дослідження ефективності запропонованого підходу на основі гіпотетичних даних і метрик точності, ймовірності виявлення некоректних операцій та тривалості оброблення транзакцій, внаслідок чого підтверджено високий рівень точності (≈0,98–0,99), ефективність виявлення порушень (>0,97) та прийнятну продуктивність системи.
6. Встановлено, що використання смарт-контрактів дає змогу зменшити вплив людського фактора та забезпечити превентивний контроль проходження транзакцій, що дало змогу підвищити рівень достовірності та правомірності облікових операцій у критичній предметній області.
7. Визначено напрями подальших етапів дослідження, що передбачають оптимізацію продуктивності блокчейн-компонентів, удосконалення механізмів верифікації смарт-контрактів, а також адаптацію інформаційної системи до змін нормативно-правових вимог, внаслідок чого створено передумови для розширення практичного застосування запропонованого підходу.

References

1. Amofa, S., Xia, Q., Xia, H., Obiri, I. A., Adjei-Arthur, B., Yang, J., et al. (2024). Blockchain-secure patient digital twin in healthcare using smart contracts. *PLOS ONE, 19*(2), article ID e0286120. https://doi.org/10.1371/journal.pone.0286120
2. Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts (SoK). In M. Maffei & M. Ryan (Eds.), *Principles of Security and Trust* (*POST 2017*) (Lecture Notes in Computer Science, vol. 10204, pp. 164–186). Springer. https://doi.org/10.1007/978-3-662-54455-6_8
3. Bao, Z., Wang, K., & Zhang, W. (2019). An auditable and secure model for permissioned blockchain. *Proceedings of the ACM International Conference*, 112–116. https://doi.org/10.1145/3343147.3343170
4. Baranidharan, K., Mahalakshmi, R., & Anagha, S. (2025). Blockchain technology for enhancing supply chain transparency: Opportunities and challenges. *International Journal of Advanced Research in Science, Communication and Technology, 5*(2), 345–353. https://doi.org/10.48175/ijarsct-23039
5. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36, 55–81. https://doi.org/10.1016/j.tele.2018.11.006

6. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE ACCESS*, 4, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339
7. Corradini, F., Marcelletti, A., Morichetta, A., Re, B., & Ruschioni, L. (2024). A digital twin approach for blockchain smart contracts. In *Proceedings of the 2024 IEEE International Conference on Software Analysis, Evolution and Reengineering – Companion* (*SANER-C*) (pp. 1–11). IEEE. https://doi.org/10.1109/saner-c62648.2024.00007
8. Ferone, A., & Verrilli, S. (2025). Exploiting Blockchain Technology for Enhancing Digital Twins' Security and Transparency. *Future Internet*, *17*(1), article number 31. https://doi.org/10.3390/fi17010031
9. Gangwal, A., Gangavalli, H. R., & Thirupathi, A. (2023). A survey of layer-two blockchain protocols. *Journal of Network and Computer Applications, 209*, article ID 103539. https://doi.org/10.1016/j.jnca.2022.103539
10. Guo, X., Li, D. A., & Zuo, Y. (2025). When auditing meets blockchain: A study on applying blockchain smart contracts in auditing. *International Journal of Accounting Information Systems*, 56, article ID 100730. https://doi.org/10.1016/j.accinf.2025.100730
11. Han, J., Kamber, M., & Pei, J. (2012). *Data Mining: Concepts and Techniques* (3rd ed.). Morgan Kaufmann. URL: https://myweb.sabanciuniv.edu/rdehkharghani/files/2016/02/The-Morgan-Kaufmann-Series-in-Data-Management-Systems-Jiawei-Han-Micheline-Kamber-Jian-Pei-Data-Mining.-Concepts-and-Techniques-3rd-Edition-Morgan-Kaufmann-2011.pdf
12. Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, 39, 80–89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005
13. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A Survey on the Security of Blockchain Systems. *Future Generation Computer Systems*, 107, 841–853. https://doi.org/10.48550/arXiv.1802.06993
14. Luu, L., Chu, D. H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making smart contracts smarter. *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, pp. 254–269. https://doi.org/10.1145/2976749.2978309
15. Putz, B., Menges, F., & Pernul, G. (2019). A secure and auditable logging infrastructure based on a permissioned blockchain. *Computers & Security*, 87, article ID 101602. https://doi.org/10.1016/j.cose.2019.101602
16. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, *57*(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261
17. Salunkhe, V., & Sujatha, R. (2025). Integrating Zk-Rollup and Blockchain for Scalable and Secure Healthcare Data Management. *Ksii Transactions on Internet and Information Systems*, *19*(1), 176–195. https://doi.org/10.2139/ssrn.5070850
18. Samaniego, M., & Deters, R. (2023). Digital twins and blockchain for IoT management. In *Proceedings of the ACM Asia Conference on Computer and Communications Security* (*ASIA CCS '23*), pp. 1357–1369. ACM. https://doi.org/10.1145/3594556.3594611
19. Upadrista, V., Nazir, S., & Tianfield, H. (2025). Blockchain-enabled digital twin system for brain stroke prediction. *Brain Informatics*, 12, article number 1. https://doi.org/10.1186/s40708-024-00247-6
20. Wafaa, A. H. Ahmed, MacCarthy, Bart L., & Treiblmaier, Horst. (2022). Why, where and how are organizations using blockchain in their supply chains? Motivations, application areas and contingency factors. *International Journal of Operations & Production Management*, 42, 1995–2028. https://doi.org/10.1108/IJOPM-12-2021-0805
21. Xu, X., Weber, I., & Staples, M. (2019). *Architecture for Blockchain Applications*. Bern: Springer Nature, 307 p. https://doi.org/10.1007/978-3-030-03035-3
22. Zhang, B., Pan, H., Li, K., Xing, Y., Wang, J., Fan, D., & Zhang, W. (2024). A Blockchain and Zero Knowledge Proof Based Data Security Transaction Method in Distributed Computing. *Electronics*, *13*(21), article ID 4260. https://doi.org/10.3390/electronics13214260
23. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018). Smart contract-based ACCESS control for the Internet of Things. *arXiv preprint arXiv:1802.04410*. https://doi.org/10.48550/arXiv.1802.04410
24. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, *14*(4), 352–375. https://doi.org/10.1504/IJWGS.2018.095647
25. Zhuo, Y. (2024). Research on Blockchain Interactive Zero Knowledge Proof Privacy Protection Scheme Based on Improved Paillier Homomorphic Encryption. *Frontiers in Science and Engineering*, *4*(10), 57–73. https://doi.org/10.54691/9xb96p64

N. E. Kunanets, Yu. A. Yarymovych

Lviv Polytechnic National University, Lviv, Ukraine

USE OF SMART CONTRACTS IN THE INFORMATION SYSTEM OF ACCOUNTING OF ARMS TRADE

The problem of improving the efficiency, security, and transparency of information systems for firearms trade accounting under conditions of increased regulatory control and stricter transaction compliance requirements is investigated. The relevance of the study is substantiated by the need to ensure reliable transaction recording, minimize the risks of illegal firearms circulation, and enhance trust in information systems operating in critical environments. The object of the study is defined as the processes of accounting and control of transactions in firearms trade systems, while the subject of the study is the methods and models for automated verification of transaction legality using smart contracts. The purpose of the study is formulated as the development of an approach to the use of smart contracts for automated transaction control and ensuring compliance with regulatory requirements. The main research tasks include formalizing the transaction execution process, developing a model for verifying transaction legality conditions, and designing the architecture of the information system. Methods of system analysis, logical modeling, and formalization are applied, which made it possible to represent the transaction execution process as a sequence of interrelated stages. A multi-level architecture of the information system is proposed, combining a microservices approach with blockchain infrastructure to ensure distributed data storage and immutability of records. Smart contracts are introduced as a key component of transaction control. A method for formalized verification of transaction legality based on a conjunctive logical model is developed, according to which a transaction is executed only if all defined conditions are simultaneously satisfied. An experimental study based on hypothetical data is conducted, and high efficiency of the proposed approach is established: the accuracy of determining transaction legality is 0.98-0.99, the probability of detecting incorrect operations exceeds 0.97, and the transaction processing time increases linearly depending on the number of verification conditions. For the first time, the integration of smart contracts into an information system for firearms trade accounting as a mechanism for formalized control of transaction legality based on conjunctive logic is proposed. The practical significance of the results lies in the possibility of implementing the proposed approach in firearms circulation control systems and other critical systems requiring a high level of trust, transparency, and automated transaction control.

Keywords: blockchain technology; decentralised ledgers; automated transaction monitoring; transaction validation; logical models for verifying transaction conditions; cybersecurity; data traceability; digital ledgers; ACCESS control; distributed systems.