Науковий вісник НЛТУ України
Scientific Bulletin of UNFU
ISSN 1994-7836 (print)
ISSN 2519-2477 (online)
https://doi.org/10.36930/40350215
Article received 17.03.2025
Article accepted 02.05.2025
UDC 004.9:339.1
Correspondence author: N. E. Kunanets nek.lviv@gmail.com

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

ВИКОРИСТАННЯ ДЕЦЕНТРАЛІЗОВАНИХ ДОДАТКІВ ДЛЯ СТВОРЕННЯ ТОРГОВЕЛЬНОЇ ІНФОРМАЦІЙНО-ТЕХНОЛОГІЧНОЇ ПЛАТФОРМИ

Досліджено можливості використання децентралізованих додатків для створення інформаційно-технологічної платформи, орієнтованої на торгівлю зброєю. Аналіз наявних підходів до цифровізації стратегічних ринків свідчить про актуальність застосування блокчейн-технологій та смарт-контрактів для підвищення безпеки, прозорості та ефективності торгових операцій зі зброєю. Встановлено, що децентралізовані додатки, завдяки своїм характеристикам, таким як відсутність єдиного центру управління, криптографічна захищеність та розподілена архітектура, можуть істотно удосконалити процеси ведення торгівлі стратегічними товарами. Вказано на те, що застосування блокчейн-технології забезпечує незмінність даних, унеможливлюючи підроблення або несанкціоноване втручання, що є критично важливим для ведення операцій у сфері торгівлі зброєю. Виявлено, що смарт-контракти дають можливість автоматизувати ключові етапи торгових угод, враховуючи верифікацію продавців та покупців, управління транзакціями, а також контроль виконання договірних зобов'язань. Запропоновано концептуальну модель інформаційно-технологічної платформи, яка інтегрує систему ідентифікації користувачів, що забезпечує багаторівневу верифікацію учасників торгівлі, блокчейн-реєстр транзакцій, що гарантує незмінність записів та їхню перевірку всіма учасниками ринку, зменшуючи ризики шахрайства та корупції, а також смарт-контракти, які автоматизують процес виконання торгових угод та мінімізують потребу у посередниках, підвищуючи ефективність виконання транзакцій. Окрім цього, прозорість інформаційних потоків забезпечує відкритий доступ до історії транзакцій із дотриманням регуляторних вимог, що підвищує рівень довіри між учасниками ринку, а механізм розподіленого управління дає змогу учасникам екосистеми приймати колективні рішення щодо змін у платформі, підвищуючи рівень децентралізації та демократизації процесів. Оцінено досвід впровадження подібних децентралізованих технологій у суміжних галузях, зокрема у фінансовому секторі, логістиці та постачанні стратегічних ресурсів. Виявлено, що подібні платформи мають значний потенціал для впровадження у сфері торгівлі зброєю, оскільки усувають основні недоліки традиційних систем, такі як обмежена прозорість, складнощі у верифікації контрагентів та високий рівень бюрократичних процедур. Розглянуто ключові виклики впровадження інформаційно-технологічної платформи, серед яких дотримання міжнародних норм і стандартів контролю за торгівлею зброєю, потребу узгодження з національними та міжнародними регуляторними органами, а також забезпечення кібербезпеки системи. Вказано на те, що успішна інтеграція децентралізованих рішень можлива тільки за умов чіткої взаємодії між державними структурами, бізнесом та технологічними компаніями, які розробляють рішення для сфери безпеки. Отримані результати дослідження вказують на значні перспективи використання децентралізованих додатків для побудови прозорої та безпечної платформи для торгівлі стратегічними товарами. Запропонована концептуальна модель дає змогу удосконалити процеси управління торгівлею, знизити операційні ризики та сприяти створенню ефективного механізму контролю, що є важливим етапом у розвитку сучасних інформаційно-технологічних систем у стратегічному секторі економіки.

Ключові слова: децентралізовані платформи; блокчейн-технології; смарт-контракти; безпека; операції з озброєнням.

Вступ / Introduction

У сучасному світі, де технологічні інновації стрімко змінюють способи ведення бізнесу, виникає нагальна потреба розроблення нових рішень для ефективного управління торгівлею стратегічними товарами, зокрема зброєю. Виявлено, що застосування децентралізованих додатків, побудованих на базі блокчейн-технологій, може значно підвищити прозорість, безпеку та ефективність здійснення торгових операцій. Встановлено, що інтеграція смарт-контрактів забезпечує автоматизацію бізнес-процесів, зменшення витрат і усунення посередників, що є критично важливим для регулювання операцій у сфері торгівлі зброєю. З'ясовано, що сучасні інформаційно-технологічні платформи, що базуються на децентралізованих додатках, дають можливість забезпечити високий рівень автентифікації та авторизації учасників ринку за допомогою цифрових сертифікатів, що відповідає міжнародним стандартам безпеки. Оцінено вплив цих технологій на зниження ризиків шахрайства та незаконних операцій, що сприяє підвищенню довіри до системи торгівлі. Розроблено концептуальну модель інформаційно-технологічної платформи

Інформація про авторів:
Кунанець Наталія Едуардівна, д-р н. соц. ком., 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 децентралізованих додатків для створення торговельної інформаційно-технологічної платформи. Науковий вісник НЛТУ України. 2025, т. 35, № 2. С. 132–139.
Citation APA: Kunanets, N. E., & Yarymovych, Yu. A. (2025). Using decentralized applications to create an information technology platform for arms trade. *Scientific Bulletin of UNFU*, 35(2), 132–139. https://doi.org/10.36930/40350215

для торгівлі зброєю, яка забезпечує придатні умови для проведення торгових операцій завдяки використанню децентралізованих додатків, смарт-контрактів та блокчейн-технологій, а також запропонувати практичні підходи до її впровадження в умовах сучасного ринку.

За останні роки стрімкий розвиток технологій блокчейну та децентралізованих додатків відкрив нові можливості для багатьох галузей, враховуючи торгівлю та управління активами. У контексті торгівлі зброєю, де безпека, прозорість та контроль є критично важливими, використання децентралізованих додатків може запропонувати значні переваги. Децентралізовані додатки, побудовані на блокчейн-технології, забезпечують високий рівень безпеки та прозорості. Кожна транзакція записується у незмінний розподілений реєстр, що унеможливлює фальсифікацію даних. Це особливо важливо для торгівлі зброєю, де необхідно забезпечити легітимність та законність здійснення всіх операцій.

Об'єкт дослідження – створення торговельної інформаційно-технологічної платформи

Предмет дослідження – методи і засоби застосування децентралізованих додатків для створення інформаційно-технологічної платформи, яка забезпечить безпеку, прозорість, ефективність та відповідність регулятивним вимогам у процесах торгівлі зброєю.

Мета роботи – розробити концептуальну модель інформаційно-технологічної платформи для торгівлі зброєю на підставі децентралізованих додатків, яка забезпечить прозорість, безпеку та ефективність здійснення торгових операцій засобами блокчейн-технологій.

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

- розробити концептуальну модель інформаційно-технологічної платформи, що міститиме основні компоненти, такі як безпека, ідентифікація користувачів, смарт-контракти та забезпечення прозорості, що забезпечить високий рівень надійності обліку торговельних операцій та захисту даних, автоматизацію процесів укладання та виконання угод, мінімізацію шахрайських схем, підвищення довіри між учасниками ринку, а також відповідність міжнародним стандартам регулювання торгівлі стратегічними товарами;
- запропонувати процедури для надійної ідентифікації користувачів з використанням цифрових сертифікатів та методів безпечного зберігання криптографічних ключів, які допоможуть гарантувати автентичність учасників платформи, запобігти несанкціонованому доступу, забезпечити відповідність нормативним вимогам щодо верифікації особи, знизити ризики шахрайства та підвищити загальний рівень безпеки та довіри у процесі торгівлі стратегічними товарами.

Виконання цих завдань дослідження сприятиме розвитку ефективних, прозорих та безпечних інформаційно-технологічних платформ для торгівлі зброєю, що, водночас, підвищить економічну ефективність та конкурентоспроможність компаній, що працюють у цій сфері.

Аналіз останніх досліджень та публікацій. Блокчейн-технології пропонують унікальні можливості для торгівлі, зокрема, завдяки децентралізації та високому рівню безпеки. Автори роботи [9] аналізують потенціал технології блокчейн для підвищення прозорості та запобігання незаконній торгівлі зброєю. Дослідження показало, що блокчейн-технологія може значно знизити ризики, пов'язані з фальсифікацією даних і незареєстрованими транзакціями.

У роботі [2] відзначено, що компанії охоче впроваджують нові технології, такі як штучний інтелект (ШІ), хмарні обчислення, великі дані тощо, оскільки вони є свідками успішних бізнес-застосувань. Як одна з революційних технологій, технологія Blockchain привертає увагу через поширення криптовалют (наприклад, Bitcoin та Ethereum), для яких Blockchain є основою. У науковій розвідці проведено комплексний огляд літератури щодо функцій Blockchain, впровадження та наслідків для бізнесу. Зокрема, переглядаючи та аналізуючи 2265 останніх статей, які розкривають застосування Blockchain у різних сферах, це дослідження орієнтоване на блокчейн, розкриває статус дослідження та окреслює майбутні напрями досліджень. Показано, що серед різноманітних характеристик Blockchain простежуваність є основною характеристикою, що сприяє застосуванню Blockchain в управлінні ланцюгом поставок. Відзначено, що дослідження, пов'язані з Blockchain, надзвичайно зростають у охороні здоров'я та уряді, а в банківській сфері та кібербезпеці зменшуються.

У роботі [11] розглянуто особливості застосування децентралізованих програм, які працюють у децентралізованій мережі, наприклад Ethereum. На відміну від традиційних додатків, які контролює центральний орган влади, децентралізовані додатки – з відкритим кодом і ніхто не контролює. Це робить їх неймовірно привабливими для розробників, які цінують децентралізацію та стійкість до цензури.

Безпека ідентифікації користувачів є критично важливою у торгівлі зброєю. У роботі [10] досліджують використання децентралізованого управління ідентифікацією за допомогою блокчейну в глобальних організаціях для підтримки безпечного використання інформаційних ресурсів. Блокчейн, як технологія, спочатку була представлена як криптовалюта, і виникли проблеми з її впровадженням для корпоративних програм, таких як управління ідентифікацією. Децентралізоване управління ідентифікацією стає одним із сильних варіантів використання технології блокчейн. У цій дослідницькій роботі автори використовують якісну вторинну методологію дослідження на підставі конкретних випадків, щоб зрозуміти проблеми поточного ландшафту управління цифровою ідентифікацією та вивчити його можливі переваги як нової парадигми управління ідентифікацією. Вони пропонують концептуальну структуру куба для аналізу та вивчення різних платформ децентралізованого управління ідентифікацією, цим самим сприяючи як теорії, так і практиці цифрової безпечної ідентифікації.

Смарт-контракти є ключовим елементом автоматизації процесів обліку на платформі для торгівлі зброєю. У роботі [3] аналізують переваги смарт-контрактів для автоматизації транзакцій та забезпечення дотримання договорів. Проаналізували процес впровадження смарт-контрактів для автоматизації бізнес-процесів, спрямованих на досягнення високої надійності та кібербезпеки під час виконання контрактів, оптимізацію транзакційних витрат та максимізацію продуктивності внутрішніх операцій підприємства. Дослідження виявило потенціал смарт-контрактів на підставі технології блокчейн для підвищення ефективності бізнес-процесів, зниження витрат та забезпечення інноваційного розвитку в українському бізнес-середовищі.

Прозорість і довіра серед учасників торгівлі є важливими для успішного функціонування платформи. У

роботі [1] розглядають проблеми безпеки, довіри та конфіденційності. Технологію блокчейн вважають життєздатним рішенням для підтримки безпеки, прозорості, можливості перевірки, незмінності та конфіденційності децентралізованим способом без сторонніх посередників. Основна мета цієї статті базується на порівняльному аналізі наявної літератури, що містить механізми консенсусу, смарт-контракти, архітектури, сервісні платформи та варіанти використання додатків у IoT на підставі технології блокчейн. У цьому документі наведено всебічний огляд публікацій, починаючи з величезних додатків IoT та основних викликів у їх прийнятті, інтеграції технології блокчейна з IoT та програмами. Аналіз наукових публікацій показує, що використання децентралізованих додатків для створення інформаційно-технологічної платформи для торгівлі зброєю має значний потенціал.

Матеріали та методи дослідження. Методологія дослідження містить комплекс методів і підходів, спрямованих на розроблення та аналіз інформаційно-технологічної платформи для торгівлі зброєю на підставі децентралізованих додатків (dApps). Це дослідження зосереджене на вивченні технологій, що знаходяться в основі децентралізованих додатків, і їх застосуванні для забезпечення безпеки, прозорості та ефективності торгових операцій. Методологія дослідження передбачає системний підхід до розроблення та аналізу інформаційно-технологічної платформи для торгівлі зброєю на підставі децентралізованих додатків. Використання передових технологій та інструментів забезпечить безпеку, прозорість та ефективність здійснення торгових операцій, сприяючи підвищенню довіри та зниженню витрат. Метод аналізу та синтезу використано для вивчення та узагальнення наукових джерел, визначення вимог і розроблення концептуальної моделі. Метод моделювання використовують для проєктування архітектури платформи та схем смарт-контрактів. Методи криптографії використовують для забезпечення безпеки функціонування платформи, враховуючи ідентифікацію користувачів та зберігання сертифікатів.

Результати дослідження та їх обговорення / Research results and their discussion

Вимоги до інформаційно-технологічної платформи для торгівлі зброєю. Створення інформаційно-технологічної платформи для торгівлі зброєю з використанням децентралізованих додатків може значно підвищити прозорість, безпеку та ефективність таких операцій. Децентралізовані додатки на блокчейн-технології дають можливість автоматизувати процеси, знизити витрати та забезпечити високий рівень довіри між учасниками ринку. Для побудови концептуальної моделі інформаційно-технологічної платформи для торгівлі зброєю сформулюємо її основні функції. Розподіл популярності блокчейн-рішень у межах екосистеми Ethereum подано на рис. 1.

Серед вимог до загального функціоналу важливим є забезпечення прозорості операцій. Кожну транзакцію з купівлі-продажу зброї потрібно записувати в технології блокчейн, забезпечуючи повну прозорість і можливість аудиту. Це допоможе уникнути нелегальних операцій та забезпечити відповідність нормативним вимогам. Використання смарт-контрактів дасть змогу автоматизувати виконання умов угод, забезпечуючи виконання зобов'язань всіма сторонами. Це знижує ризики шахрайства та забезпечує безпечну передачу коштів і товарів. Відсутність централізованого контролю знизить ризики зловживань та залежність від однієї точки збою, усім учасникам надаватимуться рівні права і можливості. Доцільним є використання токенів для здійснення платежів та винагороди користувачів за використання платформи. Токени можуть представляти різні види зброї або інші активи, продаж яких здійснюють на платформі.

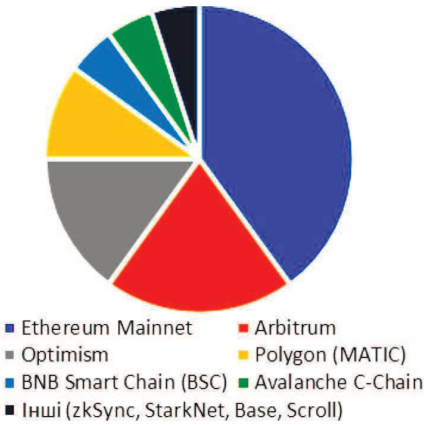

Рис. 1. Розподіл популярності блокчейн-рішень у межах екосистеми Ethereum / Distribution of popularity of blockchain solutions within the Ethereum ecosystem

Вимоги до технологічних компонент інформаційно-технологічної платформи для торгівлі зброєю передбачають наявність блокчейн-платформи, смарт-контрактів, технологій децентралізованого зберігання даних, дружніх інтерфейсів користувачів. Для формування цих компонент потрібно: здійснити вибір блокчейн-платформи, наприклад Ethereum або Polkadot, яка підтримує смарт-контракти та забезпечує високу безпеку і масштабованість; розробити смарт-контракти для автоматизації процедур формування угод, враховуючи умови купівлі-продажу, передачі прав власності та проведення платежів; захистити смарт-контракти ретельною перевіркою для забезпечення їхньої безпеки та надійності; використати децентралізовані рішення для зберігання даних, таких як IPFS (англ. *InterPlanetary File System*, міжпланетна файлова система) або Filecoin, для забезпечення безпеки і доступності інформації про види зброї та учасників ринку; розробити зручні і безпечні інтерфейси для кожної категорії користувачів – продавців, покупців та регуляторів. Інтерфейси повинні забезпечувати легкий доступ до функціоналу платформи та можливість взаємодії із смарт-контрактами та перевірки даних користувачів.

Під час формування концептуальної моделі інформаційно-технологічної платформи для торгівлі зброєю потрібно враховувати юридичні та етичні особливості, серед яких відповідність законодавству та етичних правил. Платформа повинна відповідати вимогам міжнародного та державного законодавства щодо торгівлі зброєю, що містить ідентифікацію користувачів, ліцензування та звітність про всі транзакції, забезпечення відповідальності учасників ринку та запобігання використанню платформи для незаконної торгівлі або порушення прав людини. Отже, інформаційно-технологічна платформа для торгівлі зброєю має відповідати перерахованим вимогам.

Характеристика децентралізованих додатків. Децентралізовані додатки – це програми, що працюють на

децентралізованих мережах, таких як технологія блокчейн. Вони відрізняються від традиційних додатків тим, що не залежать від центрального сервера або централізованого контролю. Децентралізовані додатки працюють на децентралізованій мережі, зазвичай на технології блокчейн, що означає відсутність єдиного центрального вузла управління, що робить їх більш стійкими до збоїв та атак.

Децентралізовані додатки використовують смарт-контракти – автоматизовані контракти, що виконуються самостійно за виконання певних умов. Смарт-контракти забезпечують прозорість та безпеку транзакцій. Усі транзакції та зміни, що відбуваються в децентралізованих додатках, записуються в технологію блокчейн, що робить їх відкритими для перевірки та аудиту, забезпечуючи високий ступінь прозорості та довіри. Завдяки децентралізованій природі та криптографічним механізмам технології блокчейн, децентралізовані додатки мають високий рівень безпеки. Дані зберігаються розподілено, що ускладнює їхню компрометацію. Децентралізовані додатки складніше закрити або цензурувати, оскільки вони працюють на децентралізованій мережі. Жоден окремий учасник не може контролювати всю систему. Децентралізовані додатки часто використовують токени – цифрові активи, що можуть представляти цінності, права або привілеї. Токени можуть використовуватися для внутрішньої економіки додатку, винагородження користувачів або управління.

Під час розроблення інформаційно-технологічної платформи для торгівлі зброєю доцільно використовувати децентралізовані додатки для аутентифікації та ідентифікації користувачів. Використання цифрових сертифікатів та криптографічних механізмів дасть змогу надійно ідентифікувати кожного учасника платформи, мінімізуючи ризики шахрайства та неправомірного доступу. Це створює додатковий рівень захисту даних користувачів платформи – як продавців, так і для покупців. Відсутність централізованого контролю унеможливлює вплив з боку окремих зацікавлених осіб або організацій, що підвищує рівень довіри до платформи. Це особливо важливо в умовах торгівлі зброєю, де питання незалежності та неупередженості є критичними. Смарт-контракти дають можливість автоматизувати більшість бізнес-процесів, пов'язаних з торгівлею зброєю, враховуючи платежі, підтвердження доставки та відповідність регулятивним вимогам. Це значно знижує витрати та підвищує ефективність операцій. Децентралізовані додатки сприяють розробленню інформаційно-технологічної платформи з урахуванням усіх необхідних регулятивних норм та вимог, що забезпечує їхню відповідність як на національному, так і міжнародному рівнях. Це сприяє легальності та легітимності торгівлі зброєю. Поєднання блокчейн-технології та децентралізованих додатків забезпечують доступ до платформи з будь-якої точки світу, що робить її зручною для користувачів з різних країн та регіонів. Це сприяє розширенню ринків збуту та залученню нових учасників. Такий підхід сприятиме забезпеченню надійного зберігання та передачі даних про транзакції та учасників торгівлі. Для підтвердження особи користувачів платформи доцільне використання цифрових сертифікатів та інших криптографічних методів, а також розподіленого реєстру для забезпечення незмінності та доступності даних для всіх учасників торгівлі. Децентралізовані фінансові додатки надають послуги кредитування, позичання, торгівлі та інші фінансові послуги без посередників. Децентралізовані додатки можуть використовуватися для відстеження товарів у ланцюгу постачань, забезпечуючи прозорість та автентичність продуктів

Проаналізуємо переваги та недоліки децентралізованих додатків. Серед переваг можемо виокремити надійність, можливість проводити трансакції без посередників, забезпечення глобальної доступності, прозорості та довіри. Децентралізовані додатки працюють на децентралізованій мережі, що забезпечує високу надійність, стійкість до збоїв та атак. Оскільки смарт-контракти – це програмний код, що автоматично виконує угоди та правила безпосередньо в блокчейні Ethereum, вони є основою для всіх типів децентралізованих додатків. Дані про доцільність використання децентралізованих додатків для Ethereum при розробленні інформаційно-технологічної платформи обліку торгівлею зброєю подано на рис. 2.

Рис. 2. Дані про децентралізовані додатки для Ethereum / Data on decentralized applications for Ethereum

Завдяки смарт-контрактам, користувачі інформаційно-технологічної платформи можуть обходитись без посередників, що знижує витрати та підвищує ефективність. Завдяки використанню децентралізованих додатків користувачі інформаційно-технологічної платформи отримують до неї доступ для будь-кого пристрою, під'єднаного до мережі Інтернет, що забезпечує глобальний доступ до усіх послуг. Фіксація всіх операцій у блоках технології блокчейн забезпечує прозорість та підвищує рівень довіри користувачів.

Серед основних недоліків варто відзначити масштабованість, складність розроблення, ймовірність ризиків, обмежений користувацький досвід. Деякі блокчейн-платформи, на яких працюють децентралізовані додатки, мають проблеми з масштабованістю, що може призводити до затримок та високих комісій за транзакції. Розроблення децентралізованих додатків може бути складнішим порівняно із традиційними додатками, через потребу врахування специфіки технології блокчейн та смарт-контрактів. Незважаючи на високу безпеку технології блокчейн, помилки в смарт-контрактах можуть призводити до втрати коштів або інших проблем. Через технічні обмеження технології блокчейн та децентралізованих мереж, користувацький досвід може бути менш зручним порівняно з використанням традиційних додатків.

Отже, децентралізовані додатки відкривають нові можливості для створення безпечних, прозорих та надійних програм, що працюють без посередників та забезпечують високий рівень довіри користувачів.

Ідентифікація користувача інформаційно-технологічної платформи для торгівлі зброєю з використ-

танням цифрового сертифіката. Ідентифікація особи користувача інформаційно-технологічної платформи для торгівлі зброєю на базі технології блокчейн з використанням цифрового сертифіката є важливим елементом для забезпечення безпеки, відповідності законодавчим вимогам і запобігання незаконній торгівлі. Метод ідентифікації може бути реалізований у кілька етапів:

Крок 1. Реєстрація користувача.

Крок 2. Генерація цифрового сертифіката.

Крок 3. Інтеграція із платформою.

Крок 4. Підписання транзакцій.

Крок 5. Зберігання та управління сертифікатами.

Під час реалізації методу користувач надає необхідні документи для ідентифікації, такі як паспорт, ліцензія на торгівлю зброєю, дозвіл на придбання зброї або інші офіційні документи, що підтверджують особу і право на участь у торгівлі. Адміністратори платформи перевіряють автентичність наданих документів. Далі відбувається генерація цифрового сертифіката та створення ключової пари. Користувач генерує публічний і приватний ключі за допомогою криптографічного алгоритму (наприклад, RSA (абревіатура від прізвищ *Rivest, Shamir* та *Adleman*) або ECDSA (англ. *Elliptic Curve Digital Signature Algorithm*). Приватний ключ зберігає користувач, а публічний ключ буде використовуватися для створення сертифіката. Публічний ключ користувача, разом із підтвердженою інформацією про особу, відправляється до сертифікаційного центру (CA). CA створює цифровий сертифікат, підписуючи його своїм приватним ключем. Цей сертифікат підтверджує автентичність особи користувача і пов'язує його з відповідним публічним ключем. Далі користувач завантажує свій цифровий сертифікат на платформу і асоціює його з обліковим записом. Щоразу, коли користувач входить на платформу, він використовує свій приватний ключ для підписання повідомлення. Платформа використовує відповідний публічний ключ із сертифіката для перевірки підпису. Якщо перевірка успішна, користувач отримує доступ до свого облікового запису.

Під час створення транзакції (наприклад, купівліпродажу зброї), користувач підписує транзакцію своїм приватним ключем. Платформа або блокчейн-мережа використовує публічний ключ із сертифіката для перевірки підпису транзакції, забезпечуючи, щоб транзакція була створена авторизованим користувачем. Сертифікати і приватні ключі зберігатимуться в захищеному середовищі, у криптографічних апаратних модулях. У разі компрометації або втрати приватного ключа, сертифікат може бути відкликаний сертифікаційним центром, і користувачеві видається новий сертифікат. Використання цифрових сертифікатів для ідентифікації користувачів на платформі для торгівлі зброєю забезпечує високий рівень безпеки та відповідність законодавчим вимогам. Цей підхід допомагає захистити особисті дані користувачів, забезпечити автентичність транзакцій і запобігти незаконній торгівлі.

Створення криптографічного апаратного модуля для зберігання сертифікатів і ключів. Криптографічний апаратний модуль забезпечує високий рівень безпеки для зберігання та управління криптографічними ключами. Власне створення HSM (англ. *Hierarchical Storage Management*) є складним і вимагає високих технічних знань та ресурсів, нижче наведено основні алгоритм процесу, а саме:

Крок 1. Визначення вимог.

Крок 2. Проєктування апаратної архітектури.

Крок 3. Розроблення програмного забезпечення.

Крок 4. Прототипування та тестування.

Під час встановлення вимог визначається рівень необхідної безпеки (відповідність стандартам FIPS 140-2 або Common Criteria), типи ключів і алгоритми, що підтримуються (RSA, ECC, AES тощо), проєктування системи захисту від фізичного втручання та інших загроз. Функціональність криптографічного апаратного модуля повинна забезпечити підтримку управління ключами, генерацію ключів, підписання, шифрування / дешифрування та функціонування інтерфейсів для інтеграції з іншими системами (API, PKCS#11, KMIP тощо). При цьому має бути висока продуктивність, яка передбачає високу швидкість операцій, ємність зберігання ключів.

Під час побудови апаратної архітектури здійснюється вибір криптографічного процесора або спеціалізованого мікроконтролера, здатного виконувати криптографічні операції. Для зберігання ключів і сертифікатів формується захищена пам'ять та неволатильна пам'ять для зберігання прошивки та конфігураційних даних. Розробляються фізичні інтерфейси для під'єднання до хост-системи (USB, PCIe, Ethernet) та логічні інтерфейси (API, драйвери).

Безпека апаратного рівня досягається завдяки захисту від фізичного втручання, виявлення та реагування на атаки та використанню засобів знищення ключів у разі виявлення втручання.

Розроблення програмного забезпечення передбачає створення легкої та безпечної операційної системи для управління ресурсами HSM, реалізацію криптографічних алгоритмів і протоколів для забезпечення придатної продуктивності та безпеки для генерування, зберігання, ротації, резервного копіювання та відновлення ключів, забезпечення можливості інтеграції з іншими додатками та системами, підтримки стандартних API (PKCS#11, KMIP).

Наступним кроком є створення прототипу для тестування та перевірки функціональності, проведення ретельного тестування апаратної та програмної частин та перевірки на відповідність стандартам безпеки.

Створення криптографічного апаратного модуля для зберігання сертифікатів і ключів вимагає комплексного підходу, який містить визначення вимог, проєктування апаратної та програмної частин, тестування та впровадження. Дотримання високих стандартів безпеки є критично важливим для захисту криптографічних ключів і забезпечення надійної роботи системи.

Підтримка алгоритму RSA у криптографічному апаратному модулі. Підтримка алгоритму RSA (англ. *Rivest-Shamir-Adleman*) є важливою функцією для сучасних криптографічних апаратних модулів (HSM). Ці алгоритми використовують для забезпечення конфіденційності, цілісності та автентичності даних. Для забезпечення підтримки кожного алгоритму RSA криптографічний апаратний модуль використовує криптографічно безпечні генератори випадкових чисел для створення двох великих простих чисел, які використовуються для формування ключової пари. Модуль (n) обчислюють як добуток двох простих чисел. Відкритий ключ складається з модуля (n) та експоненти (e), а закритий ключ – з модуля (n) та приватної експоненти (d), обчисленої з використанням розширеного алгоритму Евкліда.

Наведемо приклад обчислення відкритого та закритого ключів RSA. Для демонстрації обчислень відкритого та закритого ключів у алгоритмі RSA здійснимо:

Крок 1. Обираємо прості числа p і q: $p = 61$, $q = 53$.

Крок 2. Обчислюємо модуль n: $n = p \cdot q = 61 \cdot 53 = 3233$.

Крок 3. Обчислюємо функцію Ейлера [6]:

$$\varphi(n) = (p-1)(q-1) .$$

Функцію Ейлера, або φ-функцію, для цілого числа n визначають як кількість цілих чисел від 1 до n, які є взаємно простими з n, де

$$n = \prod_{j=1}^{m} p_j^{k_j} ,$$

де: $p_1, p_2, \ldots, p_m$ – прості числа, а $k_1, k_2, \ldots, k_m$ – їх степені, то функцію Ейлера позначають як $\varphi(n)$ й обчислюють за формулою: $\varphi(n) = (61 \cdot 53)(1 - 1/61)(1 - 1/53)$.

Обчислимо вирази в дужках: $1 - 1/53 = 52/53$.

Підставимо їх назад у формулу: $N(a, b) = ax + by$.

Спростимо вираз: $\varphi(n) = 60 \cdot 52 = 3120$.

Крок 4. Проводимо вибір відкритої експоненти e, де e має бути взаємно простою з $\varphi(n)$ і $1 \le e \le \varphi(n)$. Нехай $e = 17$ (17 взаємно проста з 3120).

Крок 5. Проводимо обчислення закритої експоненти d за допомогою розширеного алгоритму Евкліда:

Ми хочемо знайти d таке, що $e \cdot d = 1 \bmod \varphi(n)$. Використовуємо розширений алгоритм Евкліда для обчислення d. Розширений алгоритм Евкліда використовують для знаходження найбільшого спільного дільника двох чисел та для його вираження у вигляді лінійної комбінації цих чисел. Основна формула, яка лежить в основі розширеного алгоритму Евкліда, є такою:

$$2 \cdot (3120 - 17 \cdot 183) - 17 = 1, \; N(a, b) = ax + by,$$

де a і b – цілі числа, а x і y – коефіцієнти, які можна знайти за допомогою розширеного алгоритму Евкліда.

Основний алгоритм Евкліда знаходить N двох чисел a і b через послідовне ділення зі залишком:

$a = bq_1 + r_1$; $b = r_1 q_2 + r_2$;

$r_1 = r_2 q_3 + r_3$; . . . $r_{k-2} = r_{k-1} q_k + r_k$; $r_{k-1} = r_k q_{k+1} + 0$,

де r_k – це $N(a, b)$.

Розширений алгоритм Евкліда також знаходить коефіцієнти x і y для лінійної комбінації a і b для $N(a, b) = ax + by$.

Під час виконання алгоритму, ми зберігаємо коефіцієнти x і y для кожного кроку, починаючи з початкових умов: $x_0 = 1$, $y_0 = 1$, $x_1 = 0$, $y_1 = 0$.

Для кожного наступного залишку r_1, коефіцієнти обчислюють за формулами: $x_i = x_{i-2} - q_{i-1} \cdot x_i$, $y_i = y_{i-2} - q_{i-1} \cdot y_i$, де q_{i-1} – це частка від ділення a_{i-2} на a_{i-1}.

Проведемо розрахунки: $M = 2557^{2753} \bmod 3233 = 42$; $9 \cdot 1 + 8 = 17$; $8 \cdot 1 + 1 = 9$; $1 \cdot 8 + 0 = 8$.

Тепер повертаємося назад, щоб знайти коефіцієнти:

$9 - 8 \cdot 1 = 1$; $9 - (17 - 9 \cdot 1) \cdot 1 = 1$;

$2 \cdot (3120 - 17 \cdot 183) - 17 = 1$.

Тому: $d = -367 \bmod 3120 = 2753$.

Відкритий ключ (e, n): (17, 3233).

Закритий ключ (d, n): (2753, 3233).

Відкритий ключ: використовують для шифрування даних і перевірки цифрових підписів.

Закритий ключ: використовують для дешифрування даних і створення цифрових підписів.

Перевірка правильності ключів. Для перевірки правильності обчислення ключів потрібно здійснити шифрування та дешифрування повідомлення. Шифрування: $C = M^e \bmod n$, дешифрування: $M = C^d \bmod n$. Для повідомлення $M = 42$ шифрування буде таким:

$$C = 42^{17} \bmod 3233 = 2557.$$

Дешифрування виглядає так:

$$M = 2557^{2753} \bmod 3233 = 42.$$

Отже, правильність обчислення ключів підтверджується, оскільки отримане повідомлення збігається з початковим. Для шифрування використовують відкритий ключ. Шифрування виконують піднесенням повідомлення до степеня, рівного експоненті (e), і обчислення залишку від ділення на модуль (n). Для дешифрування використовують закритий ключ. Дешифрування виконують піднесенням зашифрованого повідомлення до ступеня, рівного приватній експоненті (d), і обчислення залишку від ділення на модуль (n).

Для підписання смарт-протоколу використовують закритий ключ. Підпис генерують підписанням хешу повідомлення. Перевірка підпису відбувається з використанням відкритого ключа шляхом обчислення хешу повідомлення та порівняння з підписом. Ключі зберігаються в захищеній пам'яті HSM, доступ до якої контролюється за допомогою строгих політик безпеки з дотриманням політики управління життєвим циклом ключів, враховуючи генерацію, ротацію, резервне копіювання та відновлення ключів.

Обговорення результатів дослідження. Унаслідок проведеного дослідження виявлено, що застосування децентралізованих додатків для створення інформаційно-технологічної платформи для торгівлі зброєю сприяє значному підвищенню рівня безпеки та прозорості торгових операцій завдяки використанню блокчейн-технологій та смарт-контрактів.

Встановлено, що інтеграція цифрових сертифікатів для автентифікації та авторизації учасників ринку дає змогу знизити ризик шахрайства та незаконних операцій, що підтверджується дослідженнями, наприклад, як зазначено в роботі [3].

З'ясовано, що підтримка алгоритму RSA у криптографічних апаратних модулях, на відміну від підходів, описаних у роботі [10], забезпечує вищий рівень безпеки в обміні даними, що є ключовим чинником у регулюванні торгівлі стратегічними товарами. Оцінено вплив платформи на автоматизацію бізнес-процесів, що дає змогу удосконалити витрати та усунути посередницькі операції, що позитивно впливає на оперативність прийняття рішень у динамічних ринкових умовах. Охарактеризовано закономірності впровадження децентралізованих додатків у процес прийняття рішень, що забезпечують гнучкість та адаптивність системи, що підтверджується також в дослідженні [2]. Понад це, результати аналізу публікацій свідчать, що використання сучасних технологій, зокрема хмарних рішень, сприяє досягненню високого ступеня масштабованості платформи, що дає змогу оперативно реагувати на зміни умов ринку та забезпечувати інтеграцію з іншими інформаційними системами.

У роботі [8] запропоновано рішення про те, як може відбуватися передача зброї між дилером і продавцем за допомогою цифрових підписів і цифрового сейфа для зброї, схожого на біткойн-гаманець, який надійно зберігає кожну інформацію про особу, і це допомагає нам визначити, чи є в особи, яка має зброю, оригінальна ліцензія на зброю чи підроблена, а також перевірити, чи

має ця особа раніше судимість на своє ім'я. Автори відзначають, що технологія блокчейн незмінна і захищена від злому, і її можна використовувати для усунення зазначених вище претензій і покращення прав власності, відстеження зброї та надійного зберігання записів у цифровому сейфі. Проте, на відміну від запропонованого дослідниками рішення, ми врахували, що використання технології блокчейн має певні обмеження, тому запропоновано власний підхід до вирішення питання безпеки записів про продажі зброї.

Дослідники [5], проаналізувавши різні засоби для використання технологій блокчейну, відзначили, що Ethereum, підтримуючи структуру технології блокчейн, дає змогу користувачам створювати власні програми (смарт-контракти), використовуючи поняття розумного контракту для сприяння розвитку нових операцій. Саме це концептуальне бачення стало своєрідним поштовхом до використання платформи Ethereum як основи нашої інформаційної системи.

Застосування такого підходу підвищує ефективність здійснення торговельних операцій, зменшує витрати та скорочує тривалість виконання транзакцій, що знаходить підтвердження у наукових дослідженнях, здійснених у роботах [7, 12]. Причому в роботі [4] показано декілька передбачуваних потоків, що містять технологію блокчейн з використанням самосуверенної ідентифікації, яка охоплює різні особливості системи управління ідентифікацією, що має бути характерним і для інформаційної системи, яку ми розробляємо.

Отже, запропонована концептуальна модель платформи демонструє високу практичну значущість і перспективність у сфері торгівлі зброєю, відкриваючи можливості для її адаптації в інших галузях, де критично важливими є безпека, прозорість та оперативність прийняття рішень. Проаналізовані дослідження допомагають обґрунтувати переваги використання децентралізованих додатків для створення інформаційно-технологічної платформи для торгівлі зброєю та доводять, що інтеграція сучасних технологій (смарт-контрактів, цифрових сертифікатів, криптографічних алгоритмів) сприяє підвищенню безпеки, прозорості та ефективності торгових операцій.

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

Наукова новизна отриманих результатів дослідження – набули подальшого розвитку технологічні особливості впровадження смарт-контрактів у складних бізнес-процесах торгівлі зброєю, що дає змогу враховувати різні рівні юрисдикцій.

Практична значущість результатів дослідження – підвищено безпеку процесів обліку торгівлі зброєю через впровадження інноваційних децентралізованих технологій, зокрема блокчейн-технологій, що дає змогу забезпечити незмінність та доступність записів про всі операції з торгівлі зброєю та знижує ризики шахрайства та корупції.

Висновки / Conclusions

Розроблено концептуальну модель інформаційно-технологічної платформи для торгівлі зброєю на підставі децентралізованих додатків, яка забезпечує прозорість, безпеку та ефективність здійснення торгових операцій засобами блокчейн-технологій. За результатами проведеного дослідження можна зробити такі основні висновки.

1. Систематизовано та проаналізовано релевантні темі дослідження наукові публікації, що охоплюють питання використання децентралізованих технологій у сфері цифровізації стратегічних ринків, зокрема у фінансовому секторі, логістиці та системах постачання стратегічних ресурсів. Визначено ключові наукові підходи до впровадження блокчейн-технологій та смарт-контрактів, а також їхній вплив на підвищення прозорості, безпеки й ефективності обліку та контролю торгових операцій. Проведений аналіз дав змогу виявити переваги та обмеження наявних рішень, а також визначити напрями їхнього вдосконалення в контексті розроблення інформаційно-технологічної платформи для обліку торгівлі зброєю.
2. Встановлено, що використання децентралізованих додатків у сфері обліку торгівлі зброєю має значний потенціал для підвищення прозорості, безпеки та ефективності проведення торговельних операцій. Водночас, впровадження блокчейн-технологій забезпечує незмінність та достовірність виконання транзакцій, мінімізуючи при цьому можливість шахрайства, а використання смарт-контрактів дає змогу автоматизувати процеси перевірки контрагентів, здійснювати управління угодами та забезпечувати контроль за виконанням договірних зобов'язань.
3. Наведено концептуальну модель інформаційно-технологічної платформи, що містить систему ідентифікації користувачів, блокчейн-реєстр транзакцій та механізм розподіленого процесу управління, сприяє мінімізації бюрократичних процедур, покращенню рівня довіри між учасниками ринку та підвищенню ефективності торгівлі стратегічними товарами. Досвід впровадження аналогічних технологій у фінансовому секторі та логістиці демонструє їхню ефективність у забезпеченні прозорості виконання операцій та автоматизації процесів, що підтверджує доцільність їхнього використання у сфері торгівлі зброєю.
4. З'ясовано, що впровадження подібних рішень потребує врахування низки викликів, зокрема дотримання міжнародних норм і стандартів контролю за обігом зброї, необхідності інтеграції із чинними державними регуляторними системами та забезпечення належного рівня кібербезпеки. Ефективна реалізація запропонованої платформи можлива тільки за умов тісної взаємодії з державними структурами, бізнесом та технологічними компаніями, що розробляють рішення для сфери безпеки.
5. Встановлено, що використання алгоритмів RSA та ECC у HSM забезпечує високий рівень безпеки для криптографічних операцій, що є критично важливим для захисту даних у сучасних інформаційних системах. Реалізація цих алгоритмів в HSM вимагає як апаратної, так і програмної підтримки, а також суворих політик управління ключами.

Отже, результати дослідження підтверджують перспективність використання децентралізованих додатків для побудови сучасної інформаційно-технологічної платформи, яка сприятиме розвитку цифрових інструментів контролю та управління торгівлею стратегічними товарами, мінімізуючи ризики нелегального обігу та покращуючи ефективність регуляторних механізмів. Розроблення інформаційно-технологічної платформи сприятиме підвищенню ефективності торговельних процесів за рахунок зниження витрат та усунення посередників, інтеграції вимог національних та міжнародних регуляторів у функціонал платформи, забезпечення доступу до платформи з будь-якої точки світу для всіх потенційних учасників ринку.

References

1. Ali, J., & Sofi, S. (2022). Ensuring security and transparency in distributed communication in IoT ecosystems using blockchain technology: Protocols, applications and challenges. *International Journal of Computing and Digital Systems,* 11, 20. https://doi.org/10.12785/ijcds/110101
2. Chang, A., El-Rayes, N., & Shi, J. (2022). Blockchain technology for supply chain management: A comprehensive review. *FinTech,* 1, 191–205. https://doi.org/10.3390/fintech1020015
3. Chikov, I., Koliadenko, S., Supryhan, V., Tabenska, O., Nitsenko, V., & Holinko, O. (2023). Smart contracts and business process automation: The technical aspect. *Scientific Bulletin of the National Mining University*, 186–192. https://doi.org/10.33271/nvngu/2023-5/186
4. Ferdous, M. S., Chowdhury, F., & Alassafi, M. O. (2019). In search of self-sovereign identity leveraging blockchain technology. *IEEE Access*, 7, 103059–103079. https://doi.org/10.1109/ACCESS.2019.2931173
5. Gupta, S., & Sadoghi, M. (2019). Mohammad blockchain transaction processing. *In Encyclopedia of Big Data Technologies*, 366–376. Springer International Publishing. https://doi.org/10.1007/978-3-319-77525-8_333
6. Kadubovsky, O. (2009). Generalization of the Euler function and some of its applications. *Conference of young scientists on modern problems of mechanics and mathematics named after academician Ya. S. Pidstryhach.* Lviv: Institute of Applied Problems of Mechanics and Mathematics named after Ya. S. Pidstryhach, NAS of Ukraine. https://doi.org/10.13140/RG.2.1.3755.7604
7. Kumari, R., & Sriramulu, S. (2024). Exploring advanced techniques for enhancing data privacy and security in digital systems. In *Proceedings of the 1st International Conference on Advances in Computing, Communication and Networking* (ICAC2N), 327–334. https://doi.org/10.1109/ICAC2N63387.2024.10895522
8. Lokre, S., Naman, V., Daliyet, S. P., & Panda, S. (2021). Gun tracking system using blockchain technology. https://doi.org/10.1007/978-3-030-69395-4_16
9. Min, H., & Joo, S.-J. (2022). Blockchain technology for international arms trade. *International Journal of Logistics Systems and Management*, 42(2), 223–239. URL: https://www.researchgate.net/publication/362055653_Blockchain_technology_for_international_arms_trade
10. Singla, A., et al. (2023). Decentralized identity management using blockchain: Cube framework for secure usage of IS resources. *Journal of Global Information Management*, 31(2), 1–24. https://doi.org/10.4018/JGIM.315283
11. Verma, S., Dash, S., Joshi, A., & Kavita. (2022). A detailed study of blockchain and dApps. *Proceedings of the International Conference on Cyber Resilience* (ICCR), 1–5. https://doi.org/10.1109/ICCR56254.2022.9996003
12. Wood, G., et al. (2014) Ethereum: A Secure Decentralized Generalised Transaction Ledger. *Ethereum Project Yellow Paper*, 151, 1–32. URL: https://www.docsity.com/pt/docs/ethereum-a-secure-decentralised-generalised-transaction-ledger/8599956/

N. E. Kunanets, Yu. A. Yarymovych

Lviv Polytechnic National University, Lviv, Ukraine

USING DECENTRALIZED APPLICATIONS TO CREATE AN INFORMATION TECHNOLOGY PLATFORM FOR ARMS TRADE

The article explores the potential of using decentralized applications (dApps) to create an information technology platform focused on arms trade. An analysis of existing approaches to the digitalization of strategic markets indicates the relevance of applying blockchain technology and smart contracts to enhance the security, transparency, and efficiency of trade operations. It has been established that decentralized applications, due to their characteristics such as the absence of a single control center, cryptographic security, and distributed architecture, can significantly optimize trade processes for strategic goods. It is emphasized that the use of blockchain ensures data immutability, preventing forgery or unauthorized interference, which is critically important for conducting transactions in the arms trade sector. It has been found that smart contracts allow for the automation of key stages of trade agreements, including the verification of sellers and buyers, transaction management, and the enforcement of contractual obligations. A conceptual model of an information technology platform has been proposed, integrating a user identification system that ensures multi-level verification of trade participants, a blockchain transaction registry that guarantees the immutability of records and their verification by all market participants – reducing the risks of fraud and corruption – as well as smart contracts that automate trade agreements and minimize the need for intermediaries, thereby improving transaction efficiency. Additionally, information flow transparency provides open access to transaction histories while adhering to regulatory requirements, which enhances trust among market participants. A decentralized governance mechanism allows ecosystem members to make collective decisions regarding platform modifications, increasing the level of decentralization and democratization of processes. The study evaluates the implementation experience of similar decentralized technologies in related industries, particularly in the financial sector, logistics, and strategic resource supply. It has been identified that such platforms hold significant potential for adoption in the arms trade sector as they eliminate key drawbacks of traditional systems, such as limited transparency, difficulties in verifying counterparties, and a high level of bureaucratic procedures. Key challenges in implementing the information technology platform have been examined, including compliance with international arms trade regulations and standards, alignment with national and international regulatory bodies, and ensuring the cybersecurity of the system. It is emphasized that the successful integration of decentralized solutions is possible only under conditions of clear interaction between governmental structures, businesses, and technology companies developing security solutions. Thus, the study results indicate significant prospects for using decentralized applications to build a transparent and secure platform for trading strategic goods. The proposed conceptual model allows for the optimization of trade management processes, the reduction of operational risks, and the establishment of an effective control mechanism, which is a crucial step in the development of modern information technology systems in the strategic economic sector.

Keywords: decentralized platforms; blockchain technologies; smart contracts; security; weapon transactions.