DOI: https://doi.org/10.36910/6775-2524-0560-2025-58-25
УДК 004.056:004.9:623.44
Кунанець Наталія Едуардівна, д.н.с.к., професор
https://orcid.org/0000-0003-3007-2462
Яримович Юрій Андрійович, аспірант
https://orcid.org/0009-0006-1391-3214
Національний університет «Львівська політехніка», м Львів, Україна

СТВОРЕННЯ СМАРТ-КОНТРАКТІВ У ІНФОРМАЦІЙНІЙ СИСТЕМІ ОБЛІКУ ПРОДАЖУ ЗБРОЇ

Кунанець Н.Е., Яримович Ю.А. Створення смарт-контрактів у інформаційній системі обліку продажу зброї. У статті проаналізовано можливості платформи Ethereum для розроблення та впровадження смарт-контрактів в інформаційній системі обліку продажу зброї. Розглянуто архітектуру платформи, механізми забезпечення прозорості, безпеки та достовірності даних у процесах купівлі-продажу. Особлива увага приділена аналізу ключових компонентів платформи, таких як Ethereum Virtual Machine (EVM) та механізм консенсусу Proof of Stake, які забезпечують децентралізовану та захищену основу для роботи смарт-контрактів. Досліджено потенціал смарт-контрактів для автоматизації ключових етапів обліку, включаючи перевірку дозволів на придбання зброї, реєстрацію угод, контроль дотримання законодавчих норм і відстеження змін у даних у реальному масштабі часу. Визначено переваги використання блокчейн-технологій, серед яких — незмінність записів, доступність для аудиту в режимі реального часу, підвищена прозорість операцій і мінімізація людського фактору. Окремо підкреслено, що інтеграція блокчейну дозволяє створити надійні механізми запобігання несанкціонованому доступу, фальсифікації даних і шахрайству. Розглянуто приклади реалізації смарт-контрактів у системі обліку продажу зброї та описано, як автоматизація цих процесів може сприяти зменшенню адміністративного навантаження. Водночас у статті висвітлено ключові виклики впровадження системи, включаючи питання масштабованості мережі, забезпечення конфіденційності персональних даних користувачів, адаптацію існуючих законодавчих норм до блокчейн-рішень і підвищення рівня довіри між учасниками системи. Запропоновано можливі напрями подальших досліджень, зокрема щодо інтеграції смарт-контрактів з іншими цифровими технологіями для забезпечення комплексного підходу до обліку та моніторингу. Результати роботи демонструють високий потенціал використання платформи Ethereum для підвищення ефективності та прозорості процесів у сфері контролю обігу зброї. Інтеграція смарт-контрактів із сучасними інформаційними системами обліку відкриває нові можливості для створення надійних і безпечних рішень, які відповідають викликам цифрової епохи.
Ключові слова: Ethereum, смарт-контракти, облік продажу зброї, блокчейн, інформаційна система, безпека даних, автоматизація, Solidity

Kunanets N., Yarymovych Y. Creation of Smart Contracts in the Information System for Arms Sales Accounting. The article analyzes the capabilities of the Ethereum platform for developing and implementing smart contracts in an information system for arms sales accounting. The architecture of the platform, the features of the Solidity programming language, and mechanisms for ensuring transparency, security, and data integrity in purchase and sale processes are examined. The potential of smart contracts for automating key accounting stages, including permit verification, transaction registration, and compliance with legal regulations, is explored. The advantages of using blockchain technologies are identified, including immutability of records, real-time transaction auditing, and minimization of human error. Challenges associated with system implementation are outlined, particularly issues of scalability, data confidentiality, and legal compliance. The study demonstrates the prospects of integrating Ethereum to enhance the efficiency and transparency of processes in arms control systems.
Keywords: Ethereum, smart contracts, arms sales accounting, blockchain, information system, data security, automation, Solidity.

Постановка наукової проблеми. Сучасні підходи до обліку продажу зброї стикаються з низкою викликів, серед яких — необхідність забезпечення прозорості, надійності та відповідності законодавчим нормам під час реєстрації та контролю транзакцій. Традиційні інформаційні системи часто вразливі до несанкціонованого доступу, маніпуляцій даними та людських помилок. У цьому контексті використання блокчейн-технологій, платформи Ethereum, відкриває нові можливості для підвищення ефективності та безпеки процедур обліку продажу зброї.

Ethereum, завдяки своїй децентралізованій архітектурі та можливості створення смарт-контрактів, дозволяє автоматизувати ключові етапи процесу: від перевірки дозволів до реєстрації угод і контролю за їх виконанням. Однак впровадження таких технологій супроводжується низкою викликів, включаючи питання масштабованості, забезпечення конфіденційності даних та дотримання юридичних вимог.

Наукова проблема полягає у визначенні потенціалу та обмежень використання платформи Ethereum при створенні інформаційних систем та використанні у них смарт-контрактів для автоматизації процедур обліку продажу зброї, а також у розробленні рекомендацій щодо їх ефективної інтеграції для забезпечення прозорості, безпеки та відповідності нормативно-правовим вимогам.

Аналіз досліджень. Тема впровадження смарт-контрактів на платформі Ethereum в інформаційних системах отримала значний розвиток у контексті підвищення прозорості, безпеки та автоматизації бізнес-процесів. Сучасні дослідження акцентують увагу на можливостях Ethereum як однієї з найбільш популярних блокчейн-платформ для розроблення смарт-контрактів завдяки її децентралізованій архітектурі, підтримці мови програмування Solidity та здатності до угод, які можуть виконуватись самостійно. Дослідження, проведені вченими, такими як Emma Lawrence [1], підкреслюють важливість смарт-контрактів у забезпеченні прозорості та неможливості зміни вже зафіксованих транзакцій. Технологія блокчейн, яка спочатку була розроблена як базова структура для таких криптовалют, як біткойн, перетворилася на фундаментальний інструмент для безпечних, прозорих і децентралізованих транзакцій у багатьох галузях. Одним із найбільш перспективних застосувань технології блокчейн є використання смарт-контрактів, самовиконуваних контрактів з умовами угоди, записаними безпосередньо в рядки коду. Ці технології пропонують значний потенціал для зниження транзакційних витрат, підвищення прозорості та уникнення шахрайства, що має вирішальне значення в таких секторах, як фінанси, управління ланцюгами поставок, охорона здоров'я та юридичні послуги. Blockchain забезпечує децентралізовану та незмінну систему реєстру, де всі транзакції реєструються безпечним і захищеним від втручання способом. Ця функція робить його дуже цінним для галузей, які покладаються на довіру, таких як банківська справа, нерухомість і логістика. Децентралізований характер блокчейна усуває потребу в посередниках, скорочує час і витрати на транзакції, забезпечуючи при цьому цілісність даних. Дослідники відзначають, що нові рішення для боротьби з обмеженою масштабованістю Ethereum мають враховувати дисбаланс активності, у результаті системи на основі блокчейну можуть гарантувати більш високий рівень безпеки, відстежуваності та підзвітності порівняно з традиційними системами. Смарт-контракти розширюють концепцію блокчейна, автоматизуючи виконання контрактів. Ці самовиконувані контракти автоматично виконують дії на основі попередньо визначених умов, не вимагаючи втручання людини [2]. У працях Хрістідіс К. і Девецікіотіс М. розглянуто роль смарт-контрактів у спрощенні та автоматизації бюрократичних процедур, включаючи перевірку дозволів, реєстрацію транзакцій і контроль за виконанням нормативних вимог. На думку дослідників, блокчейн — це технологія, яка швидко розвивається, і стає ключовим інструментом економіки. У статті представлено блокчейн і смарт-контракт для конкретного домену, яким є нерухомість та детальний дизайн смарт-контракту, варіанти їх використання для оренди житлових і бізнес-будинків [3].

Попри очевидні переваги, проблема масштабованості залишається ключовим викликом для Ethereum. Дослідження Чжан Ф. [4] демонструють обмеження продуктивності мережі під час опрацювання великої кількості транзакцій, що є критичним фактором для інтеграції у великі інформаційні системи. Технологія блокчейн зменшує залежність від централізованого органу для сертифікації цілісності інформації та права власності, а також посередництва транзакцій та обміну цифровими активами, одночасно забезпечуючи безпечні та псевдоанонімні транзакції разом із угодами безпосередньо між взаємодіючими сторонами. Вона володіє такими ключовими властивостями, як незмінність, децентралізація та прозорість, які потенційно вирішують нагальні проблеми в охороні здоров'я, такі як неповні записи під час надання медичної допомоги та ускладнений доступ до інформації про здоров'я пацієнтів. Міллер А. вважає, що ефективна та результативна система охорони здоров'я потребує взаємодії, яка дозволяє програмному забезпеченню та технологічним платформам безпечно та безперебійно спілкуватися, обмінюватися даними та використовувати дані, якими обмінюються між організаціями охорони здоров'я та постачальниками програм. У галузі охорони здоров'я за наявності ізольованих і фрагментованих даних, Blockchain сприяє забезпеченню зручного доступу і захисту від несанкціонованого втручання до медичних записів. Питання забезпечення конфіденційності у блокчейн-системах досліджували Бенет Дж. [5] та Косба А. [6] , які акцентували увагу на необхідності балансу між прозорістю транзакцій та захистом конфіденційних даних, що є особливо важливим у системах обліку продажу зброї. Дослідники описали архітектуру блокчейну з квантовою підтримкою на основі консорціуму квантових серверів. Розроблена мережа є гібридною, використовує цифрові системи для обміну та опрацювання класичної інформації в поєднанні з оптично-волоконною інфраструктурою, квантовими пристроями для передачі та опрацювання квантової інформації. Дослідниками розглянуто деякі ключові вразливості, проаналізовано сумісність блокчейн-систем з квантовим Інтернетом і технологіями квантових обчислень.

Нові системи розумних контрактів грунтуються на децентралізованих криптовалютах і дозволяють сторонам, які не довіряють один одному, безпечно здійснювати транзакції без довірених третіх сторін[7]. Дослідники відзначають, що існуючим системам бракує конфіденційності транзакцій. Запропонована групою дослідників [8] інформаційна система Hawk використовує децентралізовану систему смарт-контрактів, яка не зберігає фінансові транзакції у відкритому вигляді, фіксує їх в блокчейні, таким чином зберігаючи конфіденційність транзакцій. Для Hawk написані смарт-контракти без використання криптографії, а компілятор системи автоматично генерує ефективний криптографічний протокол, у якому договірні сторони взаємодіють із блокчейном, використовуючи криптографічні примітиви, такі як докази з нульовим знанням.

Отже, аналіз наукових джерел засвідчує, що блокчейн має значний потенціал для інтеграції у інформаційні системи обліку продажу зброї. Проте існують виклики, такі як масштабованість, конфіденційність даних і відповідність юридичним вимогам, які вимагають подальших досліджень та розробки ефективних рішень.

Мета роботи. Метою дослідження є проаналізувати можливості платформи Ethereum для розроблення та впровадження смарт-контрактів в інформаційній системі обліку продажу зброї, визначити переваги, виклики та перспективи їх використання для забезпечення прозорості, безпеки та ефективності процесів купівлі-продажу.

Завдання статті:

1. Проаналізувати підходи до використання платформ блокчейну та смарт-контрактів.
2. Визначити переваги застосування смарт-контрактів у системі обліку продажу зброї, зокрема прозорість, безпеку та автоматизацію процесів.
3. Сформувати архітектуру платформи Ethereum та її можливості для створення смарт-контрактів.
4. Визначити вимоги до інформаційної системи.

Виконання цих завдань дозволить сформувати цілісне уявлення про потенціал платформи Ethereum у контексті розвитку інноваційних рішень для автоматизації та прозорості процесів обліку продажу зброї.

Виклад основного матеріалу й обґрунтування отриманих результатів дослідження. Переваги використання розумних контрактів. Розумні контракти є комп'ютерними програмами, що зберігаються в блокчейні та запускаються, коли визначені заздалегідь умови виконуються. Вони призначені для полегшення фінансових операцій між користувачами блокчейну, без потреби в надійних посередниках, що характеризує традиційні фінанси[9]. Завдяки відкритому коду розумні контракти вважається головним джерелом інновацій. Розрізняють різні категорії розумних контрактів в залежності від предметної галузі, в якій використовуються. Категорії смарт-контрактів відображають їхню універсальність та широке застосування в різних сферах. Завдяки прозорості, автоматизації та безпеці смарт-контракти стали ключовою технологією для побудови децентралізованих систем, таких як системи обліку продажу зброї, і включають прозорість, безпеку та автоматизацію процесів обліку. Усі дії, пов'язані з продажею зброї, записуються у блокчейн, що забезпечує високий рівень прозорості та довіри, адже ці записи неможливо змінити. Усі транзакції, включно з фінансовими, у запропонованій інформаційній системі відбуваються між псевдонімами та сумою транзакції, і відображаються в блокчейні. У разі порушення або розірвання контракту блокчейн гарантує, що сторони отримають відповідну компенсацію.

Запис дій у блокчейн для забезпечення прозорості та довіри формульно подамо так:

$$B = \sum_{i=1}^{n} T_i + H(B_{\text{prev}}),$$

де B - новий блок у блокчейні, що містить записи про дії, пов'язані з продажем зброї. T_i - і-та транзакція, яка містить інформацію про певну дію (наприклад, продаж, перевірку або передачу зброї). i=1,2,...,n, де n – кількість транзакцій у блоці. $H(B_{prev})$ - хеш попереднього блоку, що забезпечує зв'язок між блоками та незмінність записів.

Цей хеш додається до нового блоку для збереження цілісності ланцюга. Дані, записані у блокчейн, є незмінними, оскільки зміна однієї транзакції потребувала б змін усіх наступних блоків через хешування. Усі транзакції T_i доступні для перевірки учасниками мережі, що гарантує довіру до системи.

Припустимо, що в одному блоці B записані три транзакції (T_1,T_2,T_3), які стосуються продажу зброї, формально це виглядатиме так:

$B=(T_1+T_2+T_3)+H(B_{prev})$

Це забезпечує прозорість і неможливість зміни інформації про продаж зброї. Покупці, продавці та регулюючі органи можуть перевіряти інформацію про угоду, таку як дата продажу, серійний номер зброї або відповідність ліцензій. Усі транзакції зберігаються у розподіленій системі, що дозволяє авторизованим сторонам отримувати доступ до даних у режимі реального часу.

Безпека гарантується криптографічними методами блокчейну, які захищають від фальсифікації дані про угоди. Смарт-контракти гарантують доступ до інформації лише для авторизованих осіб, таких як ліцензовані продавці, покупці або регулятори. Автоматизована верифікація учасників угоди, включно з перевіркою ліцензій, може виконуватись у реальному масштабі часу. Усі дані про транзакції зберігаються у децентралізованій мережі, що мінімізує ризик злому або втрати інформації.

Автоматизація процесів дозволяє смарт-контрактам автоматично виконувати умови угоди, такі як перевірка ліцензії покупця, оплата та реєстрація зброї в базі даних, що зменшує потребу в ручному втручанні. Завдяки автоматизації знижуються ризики людських помилок, таких як недостатня перевірка документів або невірна реєстрація. Транзакції здійснюються майже миттєво після виконання всіх умов, таких як перевірка покупця та оплата. Смарт-контракти також можуть автоматично передавати інформацію про продаж зброї до відповідних регуляторних органів, спрощуючи процеси звітності.

Робота смарт-контракту у системі обліку продажу зброї включає декілька етапів. Покупець ініціює транзакцію через платформу, після чого смарт-контракт перевіряє ліцензію покупця та статус зброї (чи вона не знаходиться у розшуку). Після підтвердження умов угоди покупець здійснює оплату, яка блокується у смарт-контракті. Продавець передає товар, що підтверджується відповідним записом у системі, після чого оплата розблоковується та передається продавцю. Наприкінці смарт-контракт автоматично надсилає звіт до регуляторних органів.

Для дотримання правових норм смарт-контракти адаптуються до місцевого та міжнародного законодавства щодо обліку продажу зброї. Регулярний аудит смарт-контрактів забезпечує їхню відповідність чинним нормам. Навчання користувачів включає проведення тренінгів для продавців і адміністраторів, а також надання інструкцій для ефективного використання системи у правовому полі.

Таким чином, впровадження смарт-контрактів сприяє підвищенню ефективності, безпеки, прозорості та надійності системи обліку продажу зброї, що дозволяє знизити ризики шахрайства, оптимізувати адміністративні процеси та забезпечити відповідність правовим нормам.

Приклад роботи смарт-контракту (псевдокод)

solidity

Копіювати код

```
pragma solidity ^0.8.0;

contract WeaponSale {
    address public regulatoryAuthority;
    mapping(address => bool) public verifiedBuyers;

    constructor(address _regulatoryAuthority) {
        regulatoryAuthority = _regulatoryAuthority;
    }

    function verifyBuyer(address buyer, uint age, bool hasPermit) public {
        require(msg.sender == regulatoryAuthority, "Only the regulatory authority can verify buyers");
        if (age >= 21 && hasPermit) {
            verifiedBuyers[buyer] = true;
        }
    }

    function registerSale(address buyer, string memory weaponId) public {
        require(verifiedBuyers[buyer], "Buyer is not verified");
        // Logic to register the sale and store in the blockchain
    }
```

```
    function generateReport() public view returns (string memory) {
        // Logic to compile and return a report of all sales
    }
}
```

Продавець перед проведенням процедури продажі має можливість перевірити покупця і підтвердити його право на покупку. Смарт-контракт автоматично реєструє продаж та зберігає інформацію у блокчейні. Смарт-контракт у системі обліку продажу автоматично виконує операції, пов'язані з реєстрацією угоди та збереженням інформації у блокчейні, завдяки чітко запрограмованим умовам і діям. Ось як відбувається цей процес:

Ініціація продажу полягає в тому, що покупець створює запит на покупку (наприклад, із зазначенням ідентифікатора товару, свого особистого ідентифікатора та підписом), смарт-контракт активується й перевіряє всі необхідні дані.

Перевірка умов передбачає, що смарт-контракт перевіряє вік та дозвіл покупця (можливо, шляхом запиту до верифікаційної бази даних), достовірність цифрового підпису, який підтверджує, що запит дійсно надійшов від зазначеного покупця.

Реєстрація транзакції відбувається якщо всі умови виконані, смарт-контракт автоматично реєструє факт продажу. Інформація про угоду записується у блокчейн, включаючи ідентифікатор товару (наприклад, виду зброї), ідентифікатор покупця (анонімізовані дані для збереження конфіденційності, якщо необхідно), мітку часу транзакції.

Зберігання даних досягає коректності завдяки децентралізованій природі блокчейну, дані зберігаються у незмінному вигляді. Після запису даних про продаж вони стають доступними для перевірки, але не можуть бути змінені або видалені.

Звітність передбачає, що смарт-контракт може бути запрограмований на автоматичне створення звітів для контролюючих органів. Ці звіти можуть бути доступні лише певним авторизованим користувачам, чиї ключі дозволяють розшифрувати ці дані.

Приклад запиту

```
{
  "request_id": "12345",
  "buyer_id": "buyer_789",
  "item_id": "weapon_456",
  "quantity": 1,
  "timestamp": "2024-11-01T15:30:00Z",
  "signature": "..."
}
```

Розглянемо основні компоненти запиту:

request_id: - унікальний ідентифікатор запиту на покупку, який дозволяє системі відстежувати окремі запити.

buyer_id: - ідентифікатор покупця, який був виданий системою обліку. Він визначає покупця, що здійснює запит.

item_id: - ідентифікатор зброї або об'єкта, який покупець бажає придбати. Це може бути номер у каталозі або код товару.

quantity: - кількість одиниць зброї, яку покупець бажає придбати.

timestamp: - час створення запиту у форматі UTC. Це допомагає зберігати хронологічну точність транзакцій.

signature: - цифровий підпис, створений покупцем з використанням його приватного ключа. Підпис генерується для всього запиту, включаючи дані, що підлягають захисту, для забезпечення автентичності та цілісності.

Таким чином, використання смарт-контрактів у системі обліку продажу зброї забезпечує прозорість угод, захист даних, мінімізацію ризиків шахрайства та підвищує ефективність системи, знижуючи витрати часу та зусиль і забезпечуючи відповідність законодавчим нормам.

Блокчейн-платформа Ethereum. Існує декілька блокчейн-платформ для розроблення застосунків з використанням технології блокчейн. Їх можна класифікувати на відкриті та комерційні[10]. Ethereum є децентралізованою блокчейн-платформою, що забезпечує можливість створення та виконання смарт-контрактів — автономних програм, які автоматично виконуються при дотриманні заданих умов з відкритим кодом для децентралізованих програм. Ethereum — це

блокчейн-платформа, яка підтримує розумні контракти. Розумні контракти — це частини коду, які виконують обчислення загального призначення. Наприклад, смарт-контракти використовувалися для впровадження краудфандингових ініціатив, які зібрали 6,2 мільярда доларів США з січня по червень 2018 року [2].

Серед основних переваг Ethereum є можливість інтегрувати та використовувати смарт-контракти, тобто фрагменти коду, які забезпечують обмін цифровими активами між кількома агентами та виконання коду через розподілені програми. Ethereum також має швидке виробництво блоків, що забезпечує високу швидкість підтвердження транзакцій щодо Bitcoin та інших мереж. Крім того, вона не контролюється жодним центральним органом управління, тобто мережа Ethereum повністю децентралізована, оскільки рішення приймаються консенсусом. Крім того, це публічна мережа, яка забезпечує повну відстежуваність і прозорість інформації з універсальним доступом до даних з будь-якої точки світу.

Ключовим компонентом архітектури платформи Ethereum є Ethereum Virtual Machine, смарт-контракти, децентралізовані застосунки, протокол консенсусу, токени, трансакції.

Формально архітектуру платформи Ethereum можна описати як функціональну залежність між основними компонентами, що взаємодіють між собою для забезпечення роботи системи:

Ethereum={EVM,SC,DApps,PoS,Tokens, TA},

де EVM – Ethereum Virtual Machine, віртуальна машина для виконання смарт-контрактів. SC – Смарт-контракти, програми, які автоматично виконуються на EVM. DApps – Децентралізовані додатки, що забезпечують інтерфейс користувача та інтеграцію зі смарт-контрактами. PoS – Протокол консенсусу Proof-of-Stake, який підтримує безпеку та стабільність мережі. Tokens – Токени стандартів ERC−20 та ERC−721, що використовуються для криптовалют та інших активів. TA-механізми трансакцій.

Рис.1. Складові платформи Ethereum

Формально взаємодію компонентів архітектури можна описати через функціонування EVM як основи виконання смарт-контрактів. Робота віртуальної машини може бути описана як виконання функцій смарт-контрактів у середовищі EVM:

EVM(SCi)=Execute(SCi)

де EVM- Ethereum Virtual Machine, платформа виконання смарт-контрактів. SCi - смарт-контракт, що є автономною програмою, збереженою у блокчейні Ethereum. Execute(SCi) - процес виконання коду смарт-контракту у середовищі EVM.

EVM отримує смарт-контракт SCi, виконує його код і повертає результат виконання. EVM інтерпретує код смарт-контракту, написаний мовою програмування Solidity, компілюючи його у байт-код, зрозумілий для EVM. Код компілюється у формат, який EVM може виконувати. EVM виконує смарт-контракти в ізольованому середовищі, що забезпечує безпеку. Наявність у коді

помилки не впливає на загальну мережу Ethereum. Смарт-контракти виконують логіку, закладену у коді, яка може включати зміни стану (додавання даних у блокчейн), виклики інших смарт-контрактів, проведення обчислень. Кожна операція, виконана EVM, споживає певну кількість обчислювальних ресурсів (Gas). Gas це термін, який використовується для позначення одиниці вимірювання обчислювальної роботи, необхідної для виконання транзакцій або смарт-контрактів у мережі. З англійської "gas" перекладається як "паливо", і використовується метафорично для опису ресурсу, який споживається для виконання операцій у мережі Ethereum. Ідея полягає в тому, що для роботи смарт-контрактів або транзакцій потрібна певна кількість "палива" (обчислювальних ресурсів), які оплачується у криптовалюті Ether (ETH). Gas дозволяє обмежити кількість обчислювальних ресурсів, які може використовувати транзакція, запобігаючи можливим атакам (наприклад, нескінченним циклам у коді). Оплата за gas стимулює вузли мережі Ethereum виконувати транзакції, оскільки майнери чи валідатори отримують компенсацію за обчислення. Загальна кількість Gas_{total}, необхідна для виконання певної транзакції або смарт-контракту, дорівнює сумі газу, спожитого кожною окремою операцією $Gas_{operation}$ в рамках цієї транзакції.

$$Gas_{total} = \sum_{j=1}^{m} Gas_{operation_j}$$

де $Gas_{operation_j}$ - кількість обчислювальних ресурсів, необхідна для виконання j-ї операції, m – кількість операцій у смарт-контракті.

Кожна операція в смарт-контракті або транзакції (наприклад, додавання, збереження даних, виклик функції) має фіксовану або обчислювану вартість у обчислювальних одиницях. Вартість операцій визначається у специфікації Ethereum. Після завершення виконання смарт-контракту EVM повертає зміну стану блокчейну, дані або повідомлення користувачу, а також інформацію про використаний ресурс. Переваги виконання в EVM включають безпеку, яка гарантується ізоляцією середовища при відсутності впливу виконання одного смарт-контракту на інші частини системи. Детермінованість означає, що результат виконання смарт-контракту є передбачуваним і не залежить від зовнішніх факторів. Масштабованість дозволяє EVM підтримувати одночасне виконання багатьох смарт-контрактів, а платформна незалежність забезпечує однакову роботу EVM на всіх вузлах мережі Ethereum. Якщо смарт-контракт SC_1 має функцію Solidity код її реалізації подамо так:

```
function add(uint a, uint b) public pure returns (uint) {
   return a + b;
}
```

Тоді виклик функції у середовищі EVM з параметрами a=3, b=5 може бути описаний як:

$EVM(SC_1)=Execute(SC_1)\rightarrow Result=8$

EVM виконує код, обчислює суму, і результат 8 записується у відповідь.

EVM є фундаментальним компонентом Ethereum, який забезпечує виконання смарт-контрактів із високим рівнем безпеки, передбачуваності та ефективності.

Проаналізуємо взаємодію смарт-контрактів та DApps. Децентралізовані застосунки використовують смарт-контракти через їх виклики:

DApps→SC:Invoke(SC),

де DApps - децентралізовані застосунки, програми, які працюють на базі блокчейну Ethereum та надають користувачам доступ до функціоналу смарт-контрактів через зручний інтерфейс (веб або мобільний). DApps забезпечують інтерфейс між користувачем і смарт-контрактом, абстрагуючи технічні деталі. SC - смарт-контракт, автономна програма, розміщена в блокчейні Ethereum, яка автоматично виконує код при виклику, якщо дотримуються умови, закладені у програму. Смарт-контракт виконує логіку, яка може включати транзакції, опрацювання даних, перевірку умов тощо. Invoke(SC) - виклик смарт-контракту. Це процес передачі запиту до смарт-контракту з інструкцією виконання певної функції. Під час виклику передаються дані (наприклад, параметри функції); кошти (ETH або токени, якщо це передбачено смарт-контрактом). Запит ініціюється децентралізованим застосунком DApps, і передається смарт-контракту SC.

Розглянемо як працює ця взаємодія. Спершу відбувається ініціація запиту користувачем через DApps. Користувач, працюючи із DApps, наприклад, гаманцем Ethereum (Metamask), викликає функцію смарт-контракту. Далі натискає кнопку "Перевести токени" в інтерфейсі DApps і формує запит. DApps формує відповідь на запит, яка містить ідентифікатор смарт-контракту (адреса контракту в блокчейні), назву функції, яку потрібно викликати (наприклад, transfer), дані для

передачі функції (кількість токенів, адреса отримувача тощо), суму ETH або токенів (за потреби). Наступним кроком є відправка запиту до смарт-контракту. Виклик передається у блокчейн через транзакцію, яку підписує користувач. Цей запит відправляється до відповідного смарт-контракту. Відбувається виконання смарт-контракту. Смарт-контракт, отримавши запит, виконує вказану функцію, наприклад, переводить токени, змінює стан у блокчейні, викликає інші смарт-контракти. Виводяться результати виконання. Смарт-контракт повертає результат у вигляді зміни стану в блокчейні (наприклад, оновлення балансу), події (event), що повідомляє DApps про результат виконання. Останньою операцією є відображення результату в DApps. DApps отримує відповідь від смарт-контракту через події блокчейну або перевірку транзакції та оновлює інформацію для користувача.

Наведемо сценарій використання цієї взаємодія. Користувач хоче перевести токени через DApps. Користувач вводить кількість токенів та адресу отримувача в DApps і натискає "Перевести". DApps формує запит:

Invoke(SC)=transfer(address,amount),

де address – адреса отримувача, amount – кількість токенів.

DApps передає цей запит у блокчейн. Смарт-контракт виконує функцію transfer, змінює баланс токенів і генерує подію Transfer. DApps отримує підтвердження про успішну транзакцію та показує його користувачу.

Перевагами взаємодії DApps і SC є прозорість, оскільки код смарт-контракту доступний для перевірки, що забезпечує довіру користувачів до його виконання. Автоматизація дозволяє смарт-контрактам виконуватися автоматично, без потреби в ручному втручанні. Безпека гарантується записом усіх дій у блокчейн, що робить їх незмінними. Універсальність DApps полягає в їхній здатності використовувати різні смарт-контракти для реалізації широкого спектру функціоналу. Ця формула демонструє, як децентралізовані застосунки слугують посередниками між користувачем та смарт-контрактами, забезпечуючи зручний і безпечний спосіб взаємодії з блокчейном.

Протокол консенсусу Proof-of-Stake (PoS) підтримує опрацювання транзакцій і забезпечує збереження даних у блокчейні:

PoS(Blocki)=Validate(Blocki),

де PoS - протокол консенсусу Proof-of-Stake, який є механізмом, який використовується для досягнення згоди в децентралізованій мережі, зокрема блокчейні Ethereum. Він забезпечує перевірку транзакцій, створення нових блоків і захист мережі від атак. Blocki - і-й блок транзакцій. Блок у блокчейні – це сукупність транзакцій, даних або подій, які потрібно записати у блокчейн. Кожен блок має унікальний ідентифікатор (хеш), пов'язаний з попереднім блоком, що забезпечує цілісність даних. Validate(Blocki) - процес перевірки блоку. Ця операція включає перевірку правильності транзакцій, які містяться в блоці, та відповідності правил мережі (наприклад, наявність достатньої кількості стейків для підтвердження блоку) та додавання блоку до блокчейна після успішної валідації.

Робота Proof-of-Stake відбувається у декілька кроків.

Крок 1. Вибір валідатора.

У PoS валідатори вибираються для створення блоку на основі кількості криптовалюти, яку вони поставили на стейкінг (stake). Чим більше валідатор поставив на стейкінг, тим вища ймовірність, що він буде обраний для перевірки наступного блоку.

Крок 2. Перевірка блоку.

Обраний валідатор виконує перевірку блоку Blocki, яка включає перевірку всіх транзакцій у блоці на коректність, перевірку балансу облікових записів, що беруть участь у транзакціях, та генерацію нового хешу блоку, який прив'язує його до попереднього блоку.

Крок 3. Додавання блоку до блокчейна.

Якщо Blocki успішно перевірено, він додається до блокчейна. Інші вузли мережі отримують цей блок і погоджуються з його валідністю.

Крок 4. Нагорода валідатора.

Валідатор отримує винагороду (наприклад, у формі токенів) за успішну перевірку та додавання блоку.

Таким чином, роль PoS полягає у забезпеченні перевірки (Validate) кожного нового блоку в блокчейні. Успішна перевірка блоку (Blocki) дозволяє додати його до мережі, тим самим гарантуючи безпеку, оскільки валідація захищає блокчейн від фальшивих транзакцій. Цілісність досягається завдяки тому, що блоки додаються лише після перевірки їхньої коректності.

Децентралізацію передбачає, що валідація здійснюється кількома незалежними вузлами, які беруть участь у стейкінгу. Переваги PoS полягають у енергоефективності, оскільки PoS не потребує величезної обчислювальної потужності, як Proof-of-Work (PoW). Безпека гарантується високим рівнем стейкінгу, що мотивує валідаторів підтримувати чесність мережі. Масштабованість системи дозволяє PoS опрацьовувати більше транзакцій за одиницю часу, порівняно з іншими механізмами консенсусу.

Припустимо, у мережі Ethereum є блок $Block_1$, який містить 10 транзакцій. Тоді валідатор, обраний через механізм PoS, виконує перевірку цих транзакцій на коректність. Якщо всі транзакції дійсні, блок $Block_1$ додається до блокчейна. Код формули в цьому випадку виглядає так:

PoS(Block_1) = \text{Validate}(Block_1) \rightarrow \text{Block_1 додано до блокчейна}

PoS підтримує функціонування блокчейна Ethereum, гарантуючи його безпеку, масштабованість і надійність. Токени формуються як активи на базі смарт-контрактів. Стандарти токенів ERC−20 та ERC−721 описуються як функції смарт-контрактів:

Tokens={ERC_20(SC), ERC_721(SC)},

де Tokens - сукупність цифрових активів, які функціонують на базі смарт-контрактів у мережі Ethereum. Токени є важливим елементом екосистеми Ethereum, оскільки вони є різноманітними цінностями, включаючи криптовалюти, сертифікати, права доступу чи цифрові активи. ERC_20(SC) - токени стандарту ERC-20, що визначають взаємозамінні активи. Кожен токен ERC_20 є ідентичним іншому в межах одного смарт-контракту.

Основна функція SC у цьому випадку – це набір правил, що визначають поведінку токенів, таких як трансфер - передачу токенів між обліковими записами, баланс - перевірка балансу токенів у гаманці, затвердження - надання дозволу іншій стороні з використанням токенів. ERC_721(SC) - токени стандарту ERC-721, які представляють невзаємозамінні активи. Кожен токен ERC_721 є унікальним, має свій ідентифікатор і його не можна обміняти на інший токен. Смарт-контракт SC забезпечує функції, пов'язані з невзаємозамінним токеном (Non-Fungible Token, NFT), такі як визначення власника токена, передача унікальних активів, управління правами. NFT - це унікальний цифровий актив, створений за допомогою технології блокчейн, який підтверджує право власності на конкретний об'єкт або актив. NFT відрізняються тим, що вони не взаємозамінні, на відміну від таких криптовалют, як Bitcoin чи Ether, які є взаємозамінними. Кожен NFT є унікальним і має власний ідентифікатор (зазвичай у вигляді хешу). Це означає, що жоден NFT не може бути повністю однаковим із іншим. Оскільки NFT існує в блокчейні, інформація про нього, включаючи право власності, записується у децентралізованому реєстрі, і ці дані не можуть бути змінені або видалені. На відміну від традиційних токенів чи валют, які є взаємозамінними (1 Bitcoin = 1 Bitcoin), NFT представляє унікальний актив, який не можна замінити на ідентичний. NFT підтверджує справжність та право власності на цифрові або фізичні активи. NFT створюються (або "мінтуються") за допомогою смарт-контрактів на блокчейні, зазвичай на платформі Ethereum. Основні стандарти для NFT ERC-721 -стандарт для унікальних токенів, ERC-1155 - удосконалений стандарт для створення як унікальних, так і масових токенів. NFT — це технологія, яка відкриває нові можливості для підтвердження автентичності, права власності та монетизації цифрових активів. Вони революціонізують способи взаємодії із цифровим контентом, мистецтвом, іграми та навіть фізичними активами.

Робота стандартів відбувається наступним чином. Припустимо є токени ERC_20, які представляють криптовалюту проекту. Функція смарт-контракту використовується для передачі 100 токенів на інший гаманець. Якщо токен ERC - невзаємозамінний токен він дозволяє створити NFT для цифрового зображення. Функція смарт-контракту використовується для перевірки, хто володіє цим унікальним токеном. Взаємозв'язок із блокчейном Ethereum забезпечується через смарт-контракти та токени як активи. Смарт-контракти реалізують функціонал токенів на Ethereum, забезпечуючи виконання умов передачі, контроль за балансом токенів та взаємодію з іншими контрактами й застосунками. Токени стандартизовані для зручності взаємодії між користувачами, застосунками та смарт-контрактами. ERC-20 забезпечує стандартизовані функції, які спрощують інтеграцію токенів у гаманці, біржі та застосунки, а їхня взаємозамінність робить ці токени ідеальними для криптовалют чи систем лояльності. ERC-721 завдяки своїй унікальності відкриває можливості для нових бізнес-моделей, таких як цифрові колекції, реєстрація активів або сертифікація.

Токени в Ethereum базуються на роботі смарт-контрактів, які стандартизують їхню поведінку та функціонал. Це створює основу для масштабованих, гнучких і прозорих цифрових

активів у децентралізованій мережі. Інтегровано архітектуру Ethereum можна подати як систему, де всі компоненти працюють у взаємодії:

$$\text{Ethereum} = \text{PoS}(\sum_{i=1}^{n} \text{EVM}(\text{SC}_i)) + \sum_{j=1}^{m} \text{DApps}(\text{SC}_j) + \sum_{k=1}^{l} \text{Tokens}(\text{SC}_k),$$

де n – кількість смарт-контрактів, що виконуються на EVM. m – кількість децентралізованих додатків, що взаємодіють зі смарт-контрактами. l – кількість токенів, створених за стандартами ERC−20 або ERC−721.

Компоненти Ethereum забезпечують децентралізовану, енергоефективну та гнучку платформу для розробки смарт-контрактів, застосунків і токенів. Розглянемо детальніше кожен з елементів. EVM надає ізольоване середовище для безпечного виконання коду смарт-контрактів. Програми для EVM пишуться мовою програмування Solidity, що забезпечує високу гнучкість і функціональність для розробників. Смарт-контракти зберігаються у блокчейні Ethereum і є важливим інструментом для автоматизації процесів, забезпечення прозорості та безпеки даних. Ethereum підтримує стандарти токенів, такі як ERC-20 для взаємозамінних токенів і ERC-721 для невзаємозамінних активів, що розширює можливості платформи для ідентифікації прав власності та управління цифровими активами. Крім того, архітектура платформи передбачає інтеграцію децентралізованих застосунків (DApps), які взаємодіють зі смарт-контрактами та забезпечують зручний користувацький інтерфейс для кінцевих користувачів. Протокол консенсусу PoS підвищує енергоефективність і масштабованість мережі, що є важливим фактором для стабільного функціонування платформи.

Ethereum пропонує низку можливостей для розроблення інформаційних систем, зокрема автоматизацію ключових процесів обліку, перевірку дозволів, реєстрацію угод і контроль дотримання законодавчих вимог. Смарт-контракти забезпечують прозорість транзакцій, оскільки всі зміни фіксуються у блокчейні та доступні для аудиту. Незмінність даних гарантує їх достовірність, а вбудовані механізми безпеки мінімізують ризик несанкціонованого доступу. Платформа дозволяє легко інтегруватися з іншими системами завдяки API та стандартним інтерфейсам.

Однак існують певні виклики, пов'язані з використанням Ethereum при розробленні смарт-контрактів. Масштабованість залишається однією з головних проблем, оскільки пропускна здатність мережі обмежена, що може призводити до затримок у транзакціях під час пікових навантажень. Вартість Gas, необхідного для виконання контрактів, також може бути високою, що обмежує доступність платформи для менш масштабних проєктів. Конфіденційність даних є ще однією проблемою, оскільки інформація в блокчейні є відкритою і доступною для всіх учасників мережі. Додатково слід враховувати юридичні аспекти впровадження, оскільки регуляторні вимоги можуть відрізнятися залежно від юрисдикції.

Незважаючи на ці виклики, Ethereum залишається однією з найпотужніших платформ для створення смарт-контрактів, що забезпечує ефективність, прозорість і безпеку інформаційних систем. Завдяки своїй архітектурі, автоматизації процесів та інтеграційним можливостям, Ethereum має значний потенціал для використання у складних і критично важливих сферах, таких як облік продажу зброї.

Вимоги до інформаційної системи обліку продажу зброї. На основі аналізу особливостей смарт-контрактів та платформи Ethereum можемо сформулювати вимоги до інформаційної системи обліку продажу зброї. Інформаційна система повинна забезпечувати прозорий механізм обліку всіх операцій купівлі-продажу зброї з можливістю аудиту в реальному часі. Інформація про транзакції має бути доступною для перевірки уповноваженими органами, зберігаючи конфіденційність персональних даних. Дані про транзакції, дозволи, угоди та реєстрації зброї повинні бути записані у блокчейн, забезпечуючи їх незмінність та захист від фальсифікації. Система повинна гарантувати високий рівень захисту даних користувачів та запобігати несанкціонованому доступу, зокрема, з використанням криптографічних методів для шифрування даних та підтвердження автентичності користувачів. Система має підтримувати автоматизацію ключових процесів через смарт-контракти, таких як перевірка дозволів на придбання зброї, реєстрація угод купівлі-продажу та контроль відповідності операцій нормативно-правовим вимогам. Смарт-контракти повинні виконуватись лише за умови дотримання всіх необхідних умов, включаючи перевірку особи та дозвільних документів. Важливим аспектом є масштабованість системи, що забезпечить підтримку великої кількості транзакцій без зниження продуктивності. Конфіденційність даних покупців і продавців також має бути гарантована за рахунок використання сучасних методів анонімізації та чіткого

розмежування доступу до інформації на основі ролей користувачів. Система повинна відповідати чинному законодавству щодо обігу зброї, захисту персональних даних та запобігання фінансуванню тероризму. Необхідно забезпечити можливість інтеграції з державними реєстрами, базами даних правоохоронних органів та іншими інформаційними системами. Архітектура повинна бути децентралізованою, щоб уникнути залежності від єдиного адміністратора або сервера, а також підтримувати механізми токенізації для управління правами на об'єкти, наприклад, створення цифрових токенів, які підтверджують право власності на зброю. Система має включати журнал подій для збереження всіх транзакцій та оновлень, забезпечуючи можливість моніторингу та аналізу. Вона повинна бути доступною на різних пристроях і платформах, забезпечуючи зручний інтерфейс для користувачів. Транзакції мають виконуватися з мінімальними затримками, навіть за високих навантажень. Також необхідно впровадити механізми резервного копіювання та швидкого відновлення даних у разі технічних збоїв. Система повинна бути гнучкою і масштабованою, з можливістю адаптації до нових вимог, розширення функціональності та інтеграції з іншими блокчейн-мережами. Ці вимоги дозволяють створити ефективну, надійну та безпечну інформаційну систему обліку продажу зброї, яка відповідає сучасним технологічним та нормативним стандартам.

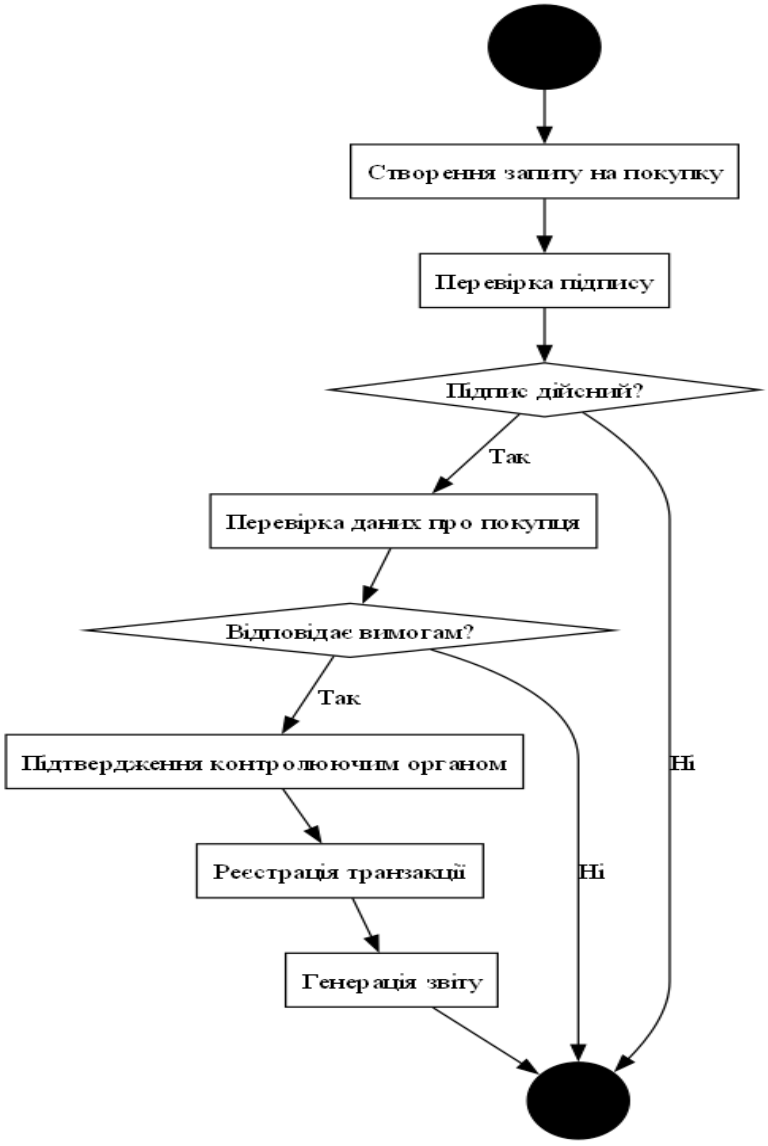

Рис.1. Діаграма діяльності інформаційної системи обліку продажу зброї

Діаграма діяльності демонструє послідовність кроків, які виконує інформаційна система обліку продажу зброї. Кожен елемент діаграми представляє певний етап процесу, що забезпечує перевірку та реєстрацію транзакцій. Користувач або система ініціює запит на придбання зброї, який стає початковою точкою процесу. Система виконує перевірку цифрового підпису для встановлення автентичності запиту. Це допомагає визначити, чи є запит легітимним. Перевірка підпису на дійсність. На наступному етапі система перевіряє, чи є підпис дійсним. Якщо підпис недійсний,

запит завершується (гілка "Ні"). У разі успішної перевірки процес переходить до наступного етапу. Система аналізує надані дані про покупця, включаючи дозвільні документи, відповідність законодавчим нормам тощо. Після аналізу даних система перевіряє, чи відповідає покупець усім вимогам. У разі невідповідності запит завершується (гілка "Ні"). Якщо дані відповідають вимогам, процес триває. У разі відповідності всім вимогам контролюючий орган підтверджує операцію. Після підтвердження система реєструє транзакцію в базі даних або у блокчейні, забезпечуючи збереження даних про угоду. Заключним етапом є створення звіту, який може бути використаний для аудиту чи подальшого аналізу операцій.

Процес починається з ініціювання запиту та проходить кілька етапів перевірок. Якщо будь-який із критеріїв не виконується, запит завершується. У разі успішного проходження всіх етапів дані реєструються, і формується звіт. Ця діаграма відображає систематичний підхід до обліку продажу зброї, де важливими аспектами є перевірка, відповідність вимогам і прозорість операцій.

Проблема конфіденційності даних у інформаційній системі пов'язана з публічним доступом до інформації, де всі транзакції є відкритими, що може призводити до витоку конфіденційної інформації, зокрема адрес гаманців. Це зумовлено дизайном публічних блокчейнів, орієнтованих на прозорість, та відсутністю вбудованих механізмів шифрування даних. Вирішення цієї проблеми полягає у використанні процедур шифрування даних, приватних блокчейнів, міксерів для об'єднання транзакцій та технологій Zero-Knowledge Proofs, які дозволяють підтвердити транзакцію без розкриття деталей. Кожен вузол і дія представляють кроки, які виконуються у смарт-контракті або зовнішніх системах. Це дозволяє визначати альтернативні шляхи у процесі роботи і чітко візуалізувати логіку роботи інформаційної системи на основі Ethereum. Рис.1 відображає основні етапи процесу роботи, включаючи створення запиту на покупку, перевірку підпису, дозволів, даних про покупця, підтвердження реєстрації транзакції та генерацію звіту. Проблеми масштабованості, конфіденційності даних та ризики є ключовими аспектами при впровадженні технологій блокчейну. Обмежена пропускна здатність блокчейн-систем, таких як Bitcoin і Ethereum, є значною проблемою, оскільки вони можуть опрацьовувати обмежену кількість транзакцій за секунду. Наприклад, Bitcoin опрацьову близько 7 TPS, Ethereum — 15-30 TPS, у той час як централізовані системи, такі як Visa, опрацьовують до 24 000 TPS. Основні причини цього обмеження включають ліміт розміру блоку та час, необхідний для досягнення консенсусу між вузлами. Можливими рішеннями є шардінг, що розподіляє блокчейн на частини для опрацювання транзакцій. Безпека системи посилюється через шифрування даних для захисту конфіденційної інформації, контроль доступу через багаторівневі механізми, що перевіряють права користувачів, та використання біометричних або цифрових підписів для ідентифікації учасників транзакцій. Підвищення надійності досягається завдяки дублюванню даних у децентралізованих вузлах, постійному оновленню інформації про транзакції та створенню резервних копій через смарт-контракти. Система забезпечує підвищення ефективності за рахунок швидкого опрацювання транзакцій, автоматизації процесів, зниження адміністративних витрат і інтеграції смарт-контрактів з іншими інформаційними системами, такими як державні реєстри.

Висновки. Ethereum є потужною платформою для створення децентралізованої інформаційної системи обліку продажу зброї, яка забезпечує високий рівень безпеки, прозорості та автоматизації. Водночас слід враховувати обмеження щодо масштабованості, витрат, потенційних вразливостей коду смарт-контрактів та необхідності забезпечення конфіденційності. Завдяки інтеграції з розробленими сервісами додатково підвищено функціональність системи.

Платформа забезпечує досить високий рівень безпеки для контролю над записами транзакцій та автентичністю користувачів завдяки низці своїх архітектурних особливостей та криптографічних принципів. У статті проаналізовано можливості платформи Ethereum для розроблення та впровадження смарт-контрактів в інформаційну систему обліку продажу зброї, що дозволило сформувати цілісне уявлення про її потенціал у цій сфері. Розглянуто архітектуру платформи, включаючи ключові компоненти, такі як Ethereum Virtual Machine (EVM), мова програмування Solidity та механізм консенсусу Proof of Stake, які забезпечують стабільне, децентралізоване та безпечне середовище для виконання смарт-контрактів.

Визначено, що використання смарт-контрактів дозволяє значно підвищити прозорість операцій, забезпечити безпеку даних і автоматизувати ключові етапи обліку, включаючи перевірку дозволів, реєстрацію угод та контроль за дотриманням законодавства. Особливу увагу приділено зниженню впливу людського фактора, що сприяє мінімізації помилок і шахрайства.

Водночас виявлено основні виклики впровадження блокчейн-технологій, серед яких проблеми масштабованості мережі, захисту конфіденційних даних користувачів і відповідності нормативно-правовим вимогам. Для їх подолання рекомендовано поступове впровадження технологій, розробку гнучких моделей для масштабування, забезпечення юридичної відповідності та створення додаткових механізмів захисту інформації.

Результати дослідження підтверджують, що платформа Ethereum має значний потенціал для підвищення ефективності інформаційних систем обліку продажу зброї. Її інтеграція сприятиме зростанню рівня довіри між учасниками ринку, забезпеченню прозорості операцій та вдосконаленню контролю за дотриманням нормативно-правових вимог. Таким чином, впровадження смарт-контрактів відкриває нові перспективи для створення інноваційних рішень у цій сфері.

Список бібліографічних описів

1. Lawrence Emma Blockchain and smart contracts for secure and transparent transactions / Lawrence Emma.-URL: https://www.researchgate.net/publication/386337137_Blockchain_and_smart_contracts_for_secure_and_transparent_transactions
2.Gustavo A. Oliva. An exploratory study of smart contracts in the Ethereum blockchain platform / Gustavo A. Oliva, Ahmed E. Hassan, Zhen Ming (Jack) Jiang. // Empirical Softw. Engg. – Dordrecht, 2020.-P. 1864–1904. https://doi.org/10.1007/s10664-019-09796-5
3. Christidis K. Blockchains and Smart Contracts for the Internet of Things / Christidis K., Devetsikiotis M. // IEEE Access. – 2016. – Vol. 4. – P. 2292–2303. – DOI: https://doi.org/10.1109/ACCESS.2016.2566339.
4. Blockchain Technology Use Cases in Healthcare / Zhang P., Schmidt D. C., White J., Lenz G. // Advances in Computers. – Elsevier. – 2018. – Vol. 111. – P. 1–41.
5. Bennet A. J Energy-Efficient Mining on a Quantum-Enabled Blockchain Using Light / Bennet A. J., Daryanoosh S. // Ledger. – 2019. – Vol. 4. – P. 82–107. – DOI: https://doi.org/10.5195/ledger.2019.143.
6. Mohanta Bhabendu An Overview of Smart Contract and Use Cases in Blockchain Technology / Mohanta, Bhabendu, Panda, Soumyashree, Jena, Debasish. // 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bengaluru, India, 2018. - Bengaluru, 2018.-P. 1-4, doi: 10.1109/ICCCNT.2018.8494045.
7. Towards Model-Driven Engineering of Smart Contracts for Cyber-Physical Systems / Garamvölgyi P., Kocsis I., Gehl B., Klenik A. // Proceedings of DSN-W 2018. – 2018. – P. 134–139. – DOI: 10.1109/DSN-W.2018.00052.
8. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts / Kosba A., Miller A., Shi E., Wen Z., Papamanthou C. // IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA. – 2016. – P. 839–858. – DOI: 10.1109/SP.2016.55.
9. Benetti Z. Decentralised Finance: A Categorisation of Smart Contracts / Benetti Z., Piazza F. // ESMA Working Paper. – 2024. – No. 3. – P. 2–29. – DOI: https://doi.org/10.1016/bs.adcom.2018.03.006.
10. Rosa-Bilbao J. Ethereum Blockchain Platform / Rosa-Bilbao J., Boubeta-Puig J. // Distributed Computing to Blockchain. – 2023. – P. 267–282. – DOI: https://doi.org/10.1016/B978-0-323-96146-2.00006-1.

References

1. Lawrence Emma Blockchain and smart contracts for secure and transparent transactions / Lawrence Emma.-URL: https://www.researchgate.net/publication/386337137_Blockchain_and_smart_contracts_for_secure_and_transparent_transactions
2.Gustavo A. Oliva. An exploratory study of smart contracts in the Ethereum blockchain platform / Gustavo A. Oliva, Ahmed E. Hassan, Zhen Ming (Jack) Jiang. // Empirical Softw. Engg. – Dordrecht, 2020.-P. 1864–1904. https://doi.org/10.1007/s10664-019-09796-5
3. Christidis K. Blockchains and Smart Contracts for the Internet of Things / Christidis K., Devetsikiotis M. // IEEE Access. – 2016. – Vol. 4. – P. 2292–2303. – DOI: https://doi.org/10.1109/ACCESS.2016.2566339.
4. Blockchain Technology Use Cases in Healthcare / Zhang P., Schmidt D. C., White J., Lenz G. // Advances in Computers. – Elsevier. – 2018. – Vol. 111. – P. 1–41.
5. Bennet A. J Energy-Efficient Mining on a Quantum-Enabled Blockchain Using Light / Bennet A. J., Daryanoosh S. // Ledger. – 2019. – Vol. 4. – P. 82–107. – DOI: https://doi.org/10.5195/ledger.2019.143.
6. Mohanta Bhabendu An Overview of Smart Contract and Use Cases in Blockchain Technology / Mohanta, Bhabendu, Panda, Soumyashree, Jena, Debasish. // 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bengaluru, India, 2018. - Bengaluru, 2018.-P. 1-4, doi: 10.1109/ICCCNT.2018.8494045.
7. Towards Model-Driven Engineering of Smart Contracts for Cyber-Physical Systems / Garamvölgyi P., Kocsis I., Gehl B., Klenik A. // Proceedings of DSN-W 2018. – 2018. – P. 134–139. – DOI: 10.1109/DSN-W.2018.00052.
8. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts / Kosba A., Miller A., Shi E., Wen Z., Papamanthou C. // IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA. – 2016. – P. 839–858. – DOI: 10.1109/SP.2016.55.
9. Benetti Z. Decentralised Finance: A Categorisation of Smart Contracts / Benetti Z., Piazza F. // ESMA Working Paper. – 2024. – No. 3. – P. 2–29. – DOI: https://doi.org/10.1016/bs.adcom.2018.03.006.
10. Rosa-Bilbao J. Ethereum Blockchain Platform / Rosa-Bilbao J., Boubeta-Puig J. // Distributed Computing to Blockchain. – 2023. – P. 267–282. – DOI: https://doi.org/10.1016/B978-0-323-96146-2.00006-1