Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента **Цуркана Данііла Ігоровича**

академічної групи **125-17-1**

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему **Використання технології блокчейн для підтвердження права власності на об'єкти цифрового мистецтва**

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц. Сафаров О.О.			
розділів:				
спеціальний	ст. вик. Тимофєєв Д.С.			
економічний	доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. вик. Тимофєєв Д.С.			

Дніпро
2021

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту **Цуркану Даніілу Ігоровичу** **академічної групи 125-17-1**
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації

за освітньо-професійною програмою ***Кібербезпека***

на тему **Використання технології блокчейн для підтвердження права власності на об'єкти цифрового мистецтва**

Затверджену наказом ректора НТУ «Дніпровська політехніка» від_____№ _____

Розділ	Зміст	Термін виконання
1. Стан питання. Постановка задачі	Проаналізовано актуальність та стан питання у сфері підтвердження права власності предметами цифрового мистецтва	09.04.2021
2. Спеціальний розділ	Проаналізовано та порівняно компоненти архітектури програмно-апаратної реалізації підтвердження права власності предметами цифрового мистецтва за допомогою технології блокчейн	07.05.2021
3. Економічний розділ	Встановлено доцільність впровадження програмно-апаратної реалізації підтвердження права власності об'єктом цифрового мистецтва.	01.06.2021

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали) Дата видачі завдання: 06.01.2021

Дата подання до екзаменаційної комісії: 17.06.2021

Прийнято до виконання _____ Цуркан Д.І.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 55 с., 10 рис., 7 табл., 4 додатки, 30 джерел.

Об'єкт розробки: Предмети цифрового мистецтва

Предмет розробки: технологія підтвердження права власності цифровими об’єктами

Мета кваліфікаційної роботи: аналіз та розробка архітектури технології підтвредження права власності об’єктами цифрвого мистецтва за допомогою технології блокчейн

В першому розділі кваліфікаційної роботи надано загальний аналіз стану цифрового мистецтва, надано його актуальність та проаналізовано наявні засоби підтвердження права власності цифровими об’єктами

У другому розділі було розглянуто, проаналізовано та порівняно компоненти архітектури програмно-апаратної реалізації підтвердження права власності предметами цифрового мистецтва за допомогою технології блокчейн. Обрано найбліьш доцільні для використання блокчейни, стандарти токенів та було порівняно засоби збереження медіаданих при створенні токена. З отриманих результатів аналізу було вибрано найбільш доцільну для використання платформу для поширення предметів цифрового мистецтва з реалізованою технологію підтвердження права власності за допомогою технології блокчейн

В третьому розділі кваліфікаційної роботи розраховано доцільність використання та економічну ефективність впровадження технології підтвердження права власності об’єктами цифрового мистецтва за допомогою технології блокчейн

ABSTRACT

Explanatory note: 55 pages, 10 figures, 7 tables, 4 appendices, 30 sources.

Object of development: Digital art objects

Subject of development: technologies for confirmation of ownership of digital objects

The purpose of the qualification work: analysis and development of architecture of technology of confirmation of the property right by objects of digital art by means of blockchain technology

The first section of the qualification work provides a general analysis of the state of digital art, its relevance and analyzes the available means of confirming ownership of digital objects

In the second section, the components of the architecture of software and hardware implementation of the confirmation of ownership of digital art objects using blockchain technology were considered, analyzed and compared. The most appropriate blockchains, token standards were selected, and the means of storing media data when creating a token were compared. From the obtained results of the analysis the most expedient platform for distribution of objects of digital art with the implemented technology of confirmation of the property right by means of blockchain technology was chosen.

In the third section of the qualification work the expediency of use and economic efficiency of introduction of technology of confirmation of the property right by objects of digital art by means of blockchain technology is calculated.

РЕФЕРАТ

Пояснительная записка: 55 с., 10 рис., 7 табл., 4 приложения, 30 источников.

Объект разработки: Предметы цифрового искусства

Предмет разработки: технологии пидтвредження права собственности цифровыми объектами

Цель квалификационной работы: анализ и разработка архитектуры технологии пидтвредження права собственности объектами цифрвого искусства с помощью технологии блокчейн

В первом разделе квалификационной работы предоставлено общий анализ цифрового искусства, предоставлено его актуальность и проанализированы имеющиеся средства подтверждения права собственности цифровыми объектами

Во втором разделе были рассмотрены, проанализированы и сравнительно компоненты архитектуры программно-аппаратной реализации подтверждения права собственности предметами цифрового искусства с помощью технологии блокчейн. Избран найблиьш целесообразны для использования блокчейны, стандарты токенов и было сравнительно средства сохранения медиаданных при создании токена. Из полученных результатов анализа было выбрано наиболее целесообразную для использования платформу для распространения предметов цифрового искусства с реализованной технологии подтверждения права собственности с помощью технологии блокчейн

В третьем разделе квалификационной работы рассчитаны целесообразность использования и экономическую эффективность внедрения технологии подтверждения права собственности объектами цифрового искусства с помощью технологии блокчейн

СПИСОК УМОВНИХ СКОРОЧЕНЬ

NFT - non-fungible token, невзаємозамінні токени

IPFS - InterPlanetary File System, міжпланетна файлова система

ETH – Ethereum

BTC – Bitcoin

ERC - Ethereum Request for Comment

BMP – Bitmap picture

ICO – Icon

GIF - Graphics Interchange Format

JPG - Joint Photographic Experts Group

PNG - Portable Network Graphics

POW – Proof of work

POS – Proof of stake

ЗМІСТ

Вступ

Інтернет надав користувачам швидкий доступ для перегляду, створювання та розміщення контенту. У зв'язку зі стрімким розвитком інформаційних технологій, за останні роки, значно збільшилась кількість цифрового контенту, який поширюється за допомогою мережі інтернет.

Музика, фільми, графічні зображення та тексти можуть бути вільно поширені та копійовані користувачами, що дає простір для миттєвого доступу та копіювання контенту. У більшості випадків оригінальний контент копіюється та поширюється у подальшому без згоди правовласника.[1]

Беручи до увагу специфику поширення медіафайлів через інтернет постає питання підтвердження права власності тим чи іншим цифровимм медіа активом. Та якщо у випадку поширення кінофільмів та музики від ліцензованих видавців є фізична процедура закріплення права власності, яка допомагає запобігати піратству та підтверджувати власність на той чи інший актив, то у випадку поширення графічних зображень, копіювання та поширення яких є значно легшим процесом, це питання викликає значні проблеми, такі як монетизація, закріплення авторства та передача прав власності від автора/правовласника до покупця.

1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 СТАН ПИТАННЯ

У останні роки у світи поширилась популярність цифрового мистецтва.

Цифрове мистецтво — напрямок медіа-мистецтва, заснований на використанні комп'ютеру, інформаційних технологій, як основи для художнього твору. [2] Десятки тисяч творців зі всього світу створюють та поширюють свої графічні твори у мережі інтернет та мають велику базу прихильників. Сумарна аудиторія топ-10 цифрових митців у соціальній мережі Instagram сягає понад 15 млн користувачів та їх кількість постійно зростає.[3] Велика зацікавленість спільноти до цифрового мистецтва притягує гроші у цю сферу. Люди готові витрачати кошті на мистецтво у вигляді цифрових графічних файлів, так, на приклад “Christies”, відомий у світі аукціон предметів мистецтва зі штаб-квартирою в Лондоні, у 2020 році почав торгувати картинами цифрових митців. На початок 2021 року ринок цифрового мистецтва оцінюється у 2 мільярди доларів США та експерти оцінюють його зростання до 4.5 мільярдів доларів до 2023 року.

Але існують значні відмінності у продажі фізичних картин та цифрових. Будь який користувач може зберегти цифрове зображення на свій пристрій, змінити його зміст, або видати себе за власника графічного малюнку. Ці вразливості приваблюють кіберзлочинців які намагаються привласнити собі предмети цифрового мистецтва та продати їх на спеціальних платформах. Так за 2020 рік було злодіями було привласнено та продано графічних зображень на суму 15 мільйонів доларів США.

У сфері цифрового мистецтва об’єктом захисту є цифрове зображення.

Цифрове зображення - графічне зображення, представлене в цифровому вигляді. Залежно від способу збереження може існувати у різних форматах. [4]

Існує велика кількість форматів цифрових зображень, серед яких виділяють 7 основних: PNG, GIF, BMP, ICO, JPEG, WEBP, SVG. Кожен з них має особливості, а саме:

- BMP - один з перших графічних форматів. Його розпізнає будь-яка програма працює з графікою, підтримка формату інтегрована в операційні системи Windows і OS / 2. [5]
- GIF - підтримує стиснення без втрати якості. Він може зберігати стислі без втрати даних зображення в форматі до 256 кольорів. Формат GIF ідеально підходить для креслень і графіків, а так само підтримує прозорість і анімацію. [5]
- PNG - створений для заміни формату GIF, є графічним форматом, що не вимагає ліцензії для використання. На відміну від GIF, у PNG є підтримка альфа-каналу і можливість зберігати необмежену кількість квітів. [5]
- JPEG -відрізняється гнучкою можливістю стиснення даних. При необхідності зображення можна зберегти з максимальною якістю. Або стиснути його до мінімального розміру файлу для передачі по мережі. [5]
- SVG - XML мова розмітки на основі векторної графіки. По суті це текстовий файл, який є відкритим веб-стандартом для опису двовимірних векторних зображень без втрати якості при масштабуванні. [5]
- WEBP - це формат файлу, розроблений компанією Google в 2010 році. Його особливістю є просунутий алгоритм стиснення, що дозволяє скоротити розмір картинки без видимих втрат в якості. [5]
- ICO - файл містить один або кілька значків різних розмірів і дозволів. Розмір значка може бути будь-яким, але найбільш вживані квадратні значки зі стороною 16, 32 і 48 пікселів. Підтримує впровадження зображень в форматі JPEG і PNG, але зазвичай дані значків зберігаються в стислому вигляді. [6]

Таблиця 1.1 Порівняння форматів графічних зображень

ФОРМАТ ФАЙЛУ	Доступні кольори	Стиснення	Середній розмір файлу
BMP	Змінна величина	Без втрат	<2 MB
GIF	256 + прозорість	Без втрат	<1 MB

PNG	16 млн + прозорість	Без втрат	<2 MB
JPEG	16 млн	З втратами	<1 MB

Продовження таблиці 1.1

SVG	147	Без втрати	-
WEBP	16.8 млн	Втрати контрольовані	<1 MB
ICO	16	-	~2 KB

Найбільш вживаним у інтернеті, згідно статистиці W3techs.com (рис.1.1) [7], через свою здатність до стиснення без втрат, підтримку альфа каналу та прозорості є формат PNG.

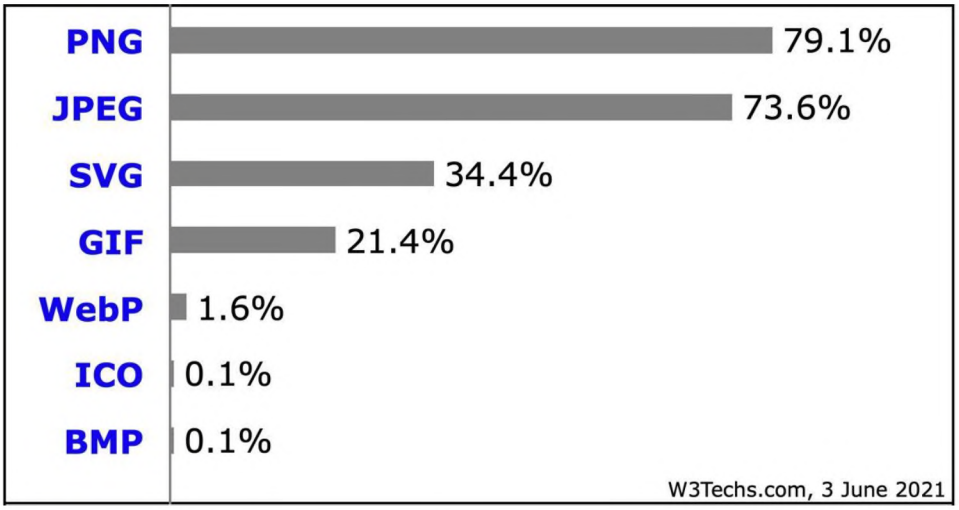

Рис.1.1 Найбільш вживані формати зображень у інтернеті

Кожен, з наведених вище форматів, може бути використаний у якості предмета цифрового мистецтва.

Цифрове мистецтво являє собою великий ринок, який потребує захисту від крадіжок та несанкціонованого доступу графічних малюнків. Ця проблема стимулює розробку нових та вдосконалення вже існуючих засобів захисту графічних зображень. Розглянемо найбільш поширені засоби захисту цифрових зображень.

На данний час найбільш поширеною технологією захисту цифрових зображень є технологія Цифрових Водяних знаків (ЦВЗ).

[8]

Цифровий водяний знак (ЦВЗ) - це спеціальна мітка, вбудована в цифровий контент (званий контейнером) з метою захисту авторських прав і підтвердження цілісності самого документа. ЦВЗ можна вбудовувати в електронні документи будь-якого типу. Поряд з різними зображеннями (фотографіями, малюнками, відсканованими паперовими документами і т.д.) зустрічаються і аудіозаписи, що несуть в собі ЦВЗ.[9]

Основні відмінності цифрових водяних знаків від звичайних (паперових) полягають в тому, що, по-перше, ЦВЗ невидимі, а по-друге, завдання зловмисника полягає не в найбільш точної імітації водяного знака, а, навпаки, в повному його знищення.

Вимога невидимості необхідно, перш за все, для того щоб зловмисник не зміг виявити ЦВЗ візуально (так як в цьому випадку його завдання спрощується). Щоб краще протистояти атакам, ЦВЗ слід розподілити по всьому цифровому контейнеру. Якщо мова йде, скажімо, про зображення (фотографії), основними атаками (методами знищення) на ЦВЗ є: масштабування, вирізання будь-яких ділянок зображення, поворот на довільний кут, конвертація в інший графічний формат, друк і подальше сканування тощо . Цифровий водяний знак повинен успішно протистояти цим атакам. Сенс в цьому є, якщо, звичайно, після такого перетворення картинка схожа на вихідний варіант.

Так званий, життєвий цикл ЦВЗ може бути описаний таким чином. (схема наведена на рис.1.1) Спочатку в сигнал-джерело в довіреної середовищі впроваджуються водяні знаки за допомогою функції. В результаті виходить сигнал. Наступний етап - поширення через мережу або будь-яким іншим способом. Під час поширення на сигнал може бути здійснена атака. У отриманого сигналу водяні знаки можуть бути потенційно знищені або змінені. На наступному етапі функція виявлення намагається виявити водяні знаки, а функція витягнути з сигналу впроваджених повідомлення. Цей процес потенційно може здійснювати зловмисник.

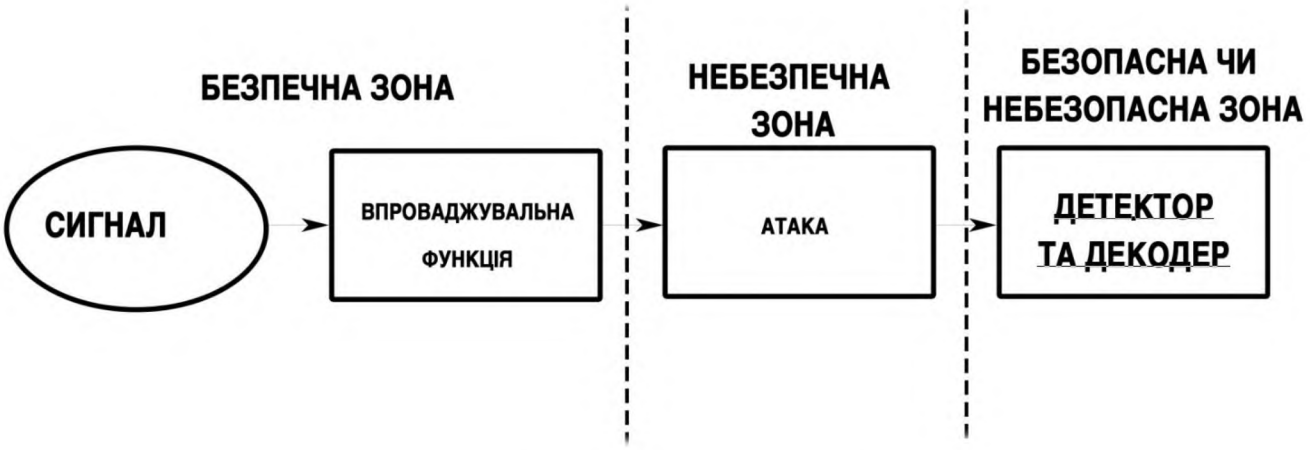

Рис.1.2 Життєвий цикл ЦВЗ

Довести свої авторські права можна скориставшись програмою що підтримує технологію ЦВЗ. Вона покаже ідентифікатор і дата створення знімка. Хоча слід зауважити, що, як правило, цифровий водяний знак, вбудований в зображення деякої програмою, не завжди можна виявити за допомогою іншого програмного продукту. Це пояснюється тим, що кожна програма є реалізацією того чи іншого методу або методів внесення ЦВЗ. І якщо програми реалізують різні методи, або навіть різні алгоритми одного методу, то показувати в якості ЦВЗ вони будуть різну інформацію.

Так відсутність чіткого стандартування та недостатня стійкість перед атаками робить ЦВЗ недостатньо повноцінним засобом захисту зображення. Через ці фактори ЦВЗ не отримали широкого розповсюдження серед користувачів, залишившись на рівні використання корпораціями, майже кожна з котрих використовує свій власний стандарт, несумісний з іншими стандартами ЦВЗ.

В основу технології захисту права власності графічного зображення має бути закладена технічна система заснована на конкретних та універсальних стандартах, доступних кожному, вона має бути відкритою для доопрацювання громадськістю, та, що найважливіше, вона має бути стійкою до зовнішніх загроз. Саме такою технологією постає Блокчейн, яка отримала широке розповсюдження в останні роки.

Блокчейн — розподілена база даних, що зберігає впорядкований ланцюжок записів (так званих блоків), що постійно довшає. Кожен блок містить часову позначку, хеш попереднього блоку та дані транзакцій, подані як хеш-дерево. Інформація про транзакції зазвичай надається відкритою, не шифрованою. Захистом від підробки та спотворення слугує включення хешу всього блоку у наступний блок. [10]. Принцип роботи блокчейну схематично зображено на рис.1.2.

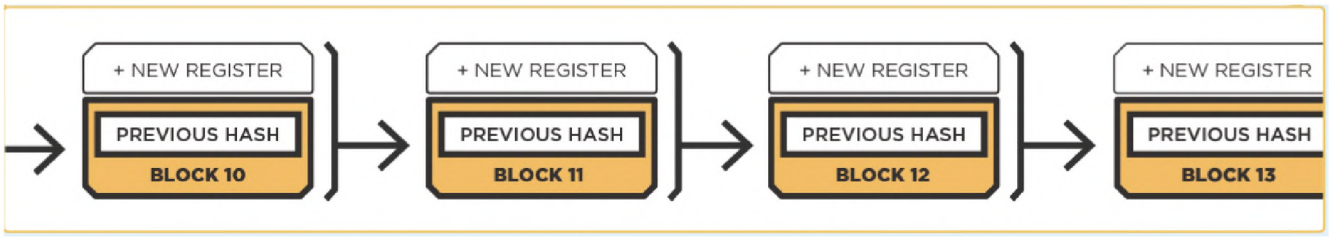

Рис.1.3 - Принцип роботи Блокчейну

Тобто дані, записані в блокчейн, зберігаються на тисячах комп'ютерів одночасно, і тому не підкоряються регулюючому органу. Дані зберігаються в блоках. Дані нових блоків не повинні суперечити даними попередніх, інакше вони не будуть внесені в ланцюжок. Ланцюги блокчейн стійкі до зломів, спробам маніпуляцій і забезпечують надійне зберігання даних за рахунок розподіленності. Через це технологія має великий потенціал у проектах пов’язаних з документообігом, державними реєстрами та фінансовими операціями.

Одним з ключових елементів, що дозволяють блокчейну працювати в якості одноранговоі (P2P) децентралізованої мережі, без необхідності участі центрального органу з третьої сторони є процес майнінгу. Це процес, в якому транзакції між користувачами перевіряються і додаються в публічний реєстр blockchain, а також процес, який використовується для введення нових монет в існуючий оборот. Майнер - це вузол в мережі, який збирає транзакції, і працює щоб організувати їх в блоки. Коли відбуваються транзакції, вузли Майнер отримують і перевіряють транзакції, додають їх у пул пам'яті і починають збирати

кілька транзакцій в блок.[11] На рисунку 1.3 зображено принцип роботи транзакцій у мережі блокчейн.

Рис.1.4 - принцип роботи транзакцій у мережі блокчейн.

Публічні (децентралізовані) блокчейни побудовані як розподілені системи, і оскільки вони не покладаються на центральні органи, розподілені вузли повинні узгоджувати валідацію транзакції. Механізм, за допомогою якого мережа що досягає того, що дотримуються правила протоколу, і гарантують, що всі транзакції відбуваються довіреною способом, тому монети можуть бути витрачені тільки один раз називається алгоритмом консенсусу. Алгоритми консенсусу є вирішальним елементом кожного блокчейна, оскільки вони відповідають за підтримку цілісності і безпеки цих розподілених систем. Перший кріптовалютний алгоритм консенсусу, це Proof of Work (PoW), який був розроблений Сатоши Накамото і реалізований в Bitcoin. Майнінг є фізичним втіленням алогоритму консенсусу. [12]

Розрізняють два основних призначення для технологій на базі блокчейн: майданчики для розрахунків і зберігання та майданчики для виконання смарт-контрактів. [12] Основними для кожного призначення технологіями є блокчейн Bitcoin та блокчейн Ethereum. [13] Обидва блокчейни використовують алгоритм Proof-of-work.

Proof-of-Work (PoW - дослівно: доказ роботи) - алгоритм захисту розподілених систем від зловживань (DoS-атак, спам-розсилок і т.д.), суть якого зводиться до двох основних пунктів:

- Необхідності виконання певної досить складною і тривалою завдання;

- Можливості швидко і легко перевірити результат.

PoW-завдання спочатку не призначені для людини, їх рішення комп'ютером завжди досяжно в кінцеві терміни, однак вимагає великих обчислювальних потужностей. При цьому перевірка отриманого рішення вимагає набагато менше ресурсів і часу. [14]

Блокчейн криптовалюти Bitcoin зберігає у собі лише дані про операції з цією криптовалютою, у той час як основною відмінністю Ethereum від Bitcoin ж можливість використання не тільки для збереження даних про транзакції, а й для виконання алгоритмів за допомогою смарт контрактів. Основні характеристики Bitcoin та Ethereum зазначені у таблиці 1.1.

Таблиця 1.2 Основні характерстики Bitcoin та Ethereum

	BITCOIN	ETHEREUM
Призначення	Цифрова валюта	Майданчик для створення створення децентралізованих алгоритмів
Алгоритм консенсусу	PROOF-OF-WORK	PROOF-OF-WORK
Емісія	Макс 21000 000	Безкінечна
Час на генерацію блока	10 хвилин	15 секунд
Стандарти	Можливість створення відсутня	Постійно створюються та доповнюються спільнотою

Смарт-контракт — Різновид угоди в формі закодованих математичних алгоритмів, укладення, зміна, виконання і розірвання яких можливо лише з використанням комп'ютерних програм в рамках мережі Інтернет. [15]

У Ethereum можна завантажити в блокчейн свою програму і вона буде виконуватися на нодах мережі. Ця програма і є смарт-контрактом. Можливість виконувати смарт-контракти - головна особливість Ethereum. Блок ланцюг, на основі смарт-контракта, видно всім користувачам зазначеного блоку. Проте, це призводить до помилок, в тому числі дірок в системі безпеки, які видно всім, але

не може бути швидко виправлено. Таким чином, була успішно виконана атака на DAO в червні 2016 року вартістю 50 млн USD у Ethereum, в той час, як розробники намагалися прийти до вирішення цієї проблеми. Обробка задачі на блокчейні вимагала часу, за який хакер може отримати доступ до ресурсів, і зняти кошти з DAO контракту. Основні характеристики смарт-контракту:

- Смарт-контракт може обслуговувати будь-яке завдання;
- Однією з найпоширеніших завдань виявилося обслуговування операцій з деякими умовними одиницями цінності – токенами;
- Токен - запис в умовній таблиці смарт-контракту;
- Забезпечує облік володіння токенами, передачу та обмін токенов, використання токенів для виконання будь-яких завдань.

У цій таблиці записано - скільки токенов належить якомусь ETH гаманцю; Передача токенов - виконання функції в смарт-контракті, яка переписує дані в таблиці володіння; створення токена - створення нового запису в цю таблицю. Токен невіддільний від смарт-контракту. Це не одиниця, яка існує сама по собі, вона існує тільки всередині системи, яка його обслуговує. Усередині смарт-контракту можна прописати унікальну механіку токена. Він буде працювати, але інші розробники (та смарт-контракти) не зможуть звертатися до нього за допомогою універсальної логіки. На допомогу приходять стандарти. Знаючи способи взаємодії з ними, творці інших смарт-контрактыв заклали в код все необхідне для роботи з токеном на певному стандарті.

Основні стандарти блокчейна ETH це ERC-20 та ERC-721. [16]

У таблиці 1.3 представлено основні характеристики обох стандартів.

Таблиця 1.3 Основні характеристики стандартів ERC-20 та ERC-721

ERC-20	ERC-721
Призначений для цифрових грошей, та токенів, що на них походять	Призначений для речей, та токенів що на них походять.
Замінний Кожен токен має однаковий набір параметрів, один токе може замінити	Незамінний Кожен токен володіє унікальним набором параметрів, у т.ч.

другий.	параметром унікального власника

Ціна остається такою самою від токена до токена.	Ціна кожного токена відрізняється.
Подільний до 18 знаків після коми.	Неподільний

Особливості стандарта ERC-721 дозволяють створювати токени з унікальним набором параметрів та прив'язувати його до цифрового або фізичного об'єкта, закладаючи основу механізма підтвердження права власності цим об'єктом. Метою цієї роботи є огляд та аналіз існуючих технологій підтвердження права власності на базі мережі блокчейн, та на основі цього аналізу запропонувати архітектуру програмних та апаратних засобів для реалізації задачі підтвердження права власності предметами цифрового мистецтва.

1.2 АНАЛІЗ НОРМАТИВНО-ПРАВОВОГО ХАБЕЗПЕЧЕННЯ

В даний час правова база неадаптована для використання токенів як сертифіката права власності у юридичному полі. З точки зору авторського права Токен - це цифрова квитанція, що показує, що власник володіє твором. Переконання покупців щодо того, чим вони володіють, не відображаються в правовій реальності.

Автором твору вважається особа, зазначена як автор на оригіналі або примірнику твору (презумпція авторства), за відсутності доказів іншого. Автору належить виключне право на дозвіл або заборону використання твору іншими особами. Для виникнення авторського права не вимагається реєстрація твору чи будь-яке інше спеціальне його оформлення. Зареєструвати авторське право за бажанням може кожен автор у відповідних державних реєстрах. Порядок такої реєстрації передбачений Постановою Кабінету Міністрів України «Про державну реєстрацію авторського права і договорів, які стосуються права автора на твір»..

Покупцеві токена належать рівно ті права, які вказані в договорі з аукціонним будинком. Тому що автором і правовласником самої картинки за

замовчуванням залишається Beeple. Передача токена сама по собі не є дійсним способом видачі ліцензії, якщо це прямо не сказано в договорі між сторонами.

“Ви визнаєте, що володіння токеном не дає ніяких прав, неявних або інших, крім прав власності на лот (зокрема цифрові зображення). Ви розумієте і погоджуєтеся з тим, що Токени випускаються третіми сторонами, а не самим Christie's.[4]

З цього формулювання випливає, що покупець не придбав ніяких виняткових прав або ліцензій на саме зображення. У всьому документі немає ні слова про перехід таких прав покупцеві.

Якщо між творцем і покупцем NFT відсутня юридичною угодою, виняткові права не переходять до покупця разом з покупкою токена. Інші правила можуть бути встановлені в правилах платформ, але на сьогоднішній типові умови найбільших платформ не містять таких норм.

1.3 ПОСТАНОВКА ЗАДАЧІ

За результатом виконаного аналізу у розділі 1.1 методів та засобів захисту та нормативно- правової бази можна сформувати наступні задачі для реалізації у спеціальний частини дипломної роботи:

Рис 1.4 – Архітектура технології підтвердження права власності об’єктами цифрового мистецтва за допомогою блокчейн

- Визначити блокчейн платформу для рішення задачі;
- Виконати порівняльний аналіз стандартів для реалізації;
- Визначити спосіб збереження сертифікату власності та предмета мистецтва, який би забезпечував конфіденційність, цілісність та доступність;
- Побудувати архітектуру задачі підтвердження права власності об'єктами цифрового мистецтва за допомогою технології блокчейн, компоненти якої зазначені у рис. 1.4
- Економічно обґрунтувати впровадження запропонованого рішення.

ВИСНОВКИ

У першому розділі було розглянуто стан питання підтвердження права власності об'єктами цифрового мистецтва та визначено актуальність доцільності імлпементування технології підтвердження права власності за допомогою блокчейн. Була проаналізована правова база питання підтвердження права власності та передачі права власності третім особам. Було сформовано задачі для спеціальної частини кваліфікаційної роботи.

2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 НЕВЗЯЄМОЗАМІННІ ТОКЕНИ. NFT

Невзаємозамінними токен (NFT, non-fungible token) - вид криптографічних токенів, кожен екземпляр з яких є унікальним і не може бути обміняний або заміщений іншим аналогічним токеном, хоча зазвичай токени взаємозамінні за своєю природою. [Wikipedia]

Унікальність токенів NFT досягається за допомогою наявності у параметрах стандарта токена функцій, що визначають його унікальність. За допомогою функції tokenMetadata токен зберігає у собі метадату – набір унікальних параметрів кожного токена, що роблять його незамінним іншим токеном. Підтвердження права власності предметом цифрового мистецтва за допомогою технології блокчейн можливо лише у томі разі, якщо стандарти певного блокчейна підтримують невзаємозамінні токени.

2.2 ПОРІВНЯЛЬНИЙ АНАЛІЗ ТЕХНОЛОГІЇ БЛОКЧЕЙН З ПІДТРИМКОЮ NFT

На даний видляють два блокчейни, що підтримують невзаємозамінни токени – Ethereum та Tezos. Існують й інші блокчейн платформи, що здійснюють підтримку NFT, але значна частина з них заснована на технологіях Ethereum та Tezos, тому порівнювати ми будемо саме ці дві платформи.

Розглянемо загальні характеристики кожної технології, проведемо їх аналіз та порівняємо між собою, визначивши найбільш придатну для рішення задачі. Під час аналізу будемо опиратися на такі фактори як: децентралізованість та захищеність платформи від несанкціонованих змін.

Управлінння Ethereum використовує поза мережею за допомогою пропозицій щодо вдосконалення Ethereum (EIP). EIP - це пропозиції щодо вдосконалення блокчейну Ethereum, який працює поза мережею.[18] Зазвичай це детальні проектні документи, що містять пропозиції щодо вдосконалення

блокчейну Ethereum. Ці процеси не представляються, не записуються, не передаються і не голосуються самим блокчейном.

Відповідно до керівних принципів Ethereum, коли йдеться про EIP, потрібно мати на увазі наступне:

- EIP повинні бути підкріплені технічними знаннями та специфікаціями;
- Автор EIP повинен мати вплив або зібрати достатню підтримку, щоб отримати EIP, не спричиняючи розрив у спільноті;
- Найважливіша частина процесу полягає в тому, що всі думки повинні бути вислухані та враховані;
- Ви можете ознайомитися з документацією EIP та всіма обговореннями, щоб всебічно побачити прогрес;
- EIP також можуть походити з запиту на коментарі Ethereum (ERC). У цьому випадку дотримується та сама процедура. [18]

ERC - це пропозиції щодо пропозицій щодо вдосконалення, які подаються на експертну перевірку через Ethereum. Стандарт токена ERC-20 з'явився в результаті ERC. Як тільки ERC зарекомендує себе достатньо перспетктивним щодо вдосконалення екосистеми Ethereum, вони обговорюються далі в межах спільноти і згодом перетворюються на EIP. [18] На цьому етапі розробники, що працюють над Ethereum, проведуть вичерпні дискусії та зустрічі щодо того, чи є розглянутий EIP достатнім для реального впровадження. Ці розробники глибоко залучені до розробки Ethereum. Якщо розробники вважають, що оновлення коду матиме позитивний вплив на екосистему, тоді і лише тоді код буде реалізований. Фаза обговорення часто є смертю для більшості EIP. Розробники неохоче впроваджують будь-які зміни, які можуть бути занадто екстремальними, щоб уникнути такої суперечки, як хард форк Ethereum Classic.

Хард форк – радикальна зміна протоколів мережі блокчейнів. Хард форк розбиває одну криптовалюту на дві частини і призводить до перевірки блоків і транзакцій, які раніше були недійсні, або навпаки. Як такий, він вимагає від усіх розробників оновлення до останньої версії програмного забезпечення протоколу. [19]

Цей процес має як недоліки, так і переваги. Звичайно, найбільшою перешкодою є те, що цей процес триває довго. Основна перевага полягає в тому, що кожен EIP досліджується настільки ретельно, що найчастіше EIP, який проходить, вносить позитивні зміни в екосистему. Механіка ERC дозволяє блокчейну постійно змінюватися та універсально функціонувати стандартам на платформах різних розробників. Це робить процес прозорим, децентралізованим, а самі стандарти можуть бути дороблені спільнотою, що позитивно впливає на механіку їх функціонування.

Управління у мережі означає голосування на платформі за запропоновану поправку. За допомогою комбінації вбудованого управління та події, що вносить зміни, процес голосування може бути модифікований, зокрема, за необхідності. Зацікавлені сторони системи (про яку ми поговоримо пізніше) дбають про голосування. Конструкція цієї системи дозволяє плавно розвивати блокчейн, замість того, щоб хард форк.

Механізм такого голосування виглядає наступним чином:

- Розробники самостійно подають пропозиції щодо оновлення протоколу та вимагають компенсації за свою роботу;
- Прохання про компенсацію гарантує, що розробники мають потужний економічний стимул робити внесок в екосистему;
- Пропозиція проходить період тестування, коли спільнота тестує протокол і критикує його за можливі вдосконалення;
- Після повторного тестування власники токенів Tezos можуть проголосувати за те, чи слід схвалити пропозицію чи ні;
- Як тільки прийнято рішення щодо законного оновлення, на протоколі відбувається "гаряча заміна", яка ініціює нову версію протокол.

Завдяки цій системі протокол децентралізовано оновлюється пасивно. Кожне оновлення протоколу проходить кілька періодів тестування та отримує відповідні відгуки від спільноти. Це гарантує, що будь-яке покращення має схвалення громади. Це запобігає будь-якому шансу на розподіл спільноти хард форком. Але основна проблема полягає у механізмі голосування Tezos. Право

голосу мають лише власники токенів Tezos, а вага голосу розраховується на основі кількості токенів у того чи іншого власника. Тобто володіючи значною кількістю токенів блокчейна можна впливати на результати голосування, ця особливість ставить під сумнів децентралізованість системи.

Алгоритм консенсусу, наразі Ethereum використовує алгоритм Proof-of-Work (POW), схема принципу роботи якого зображена на рис.2.1.

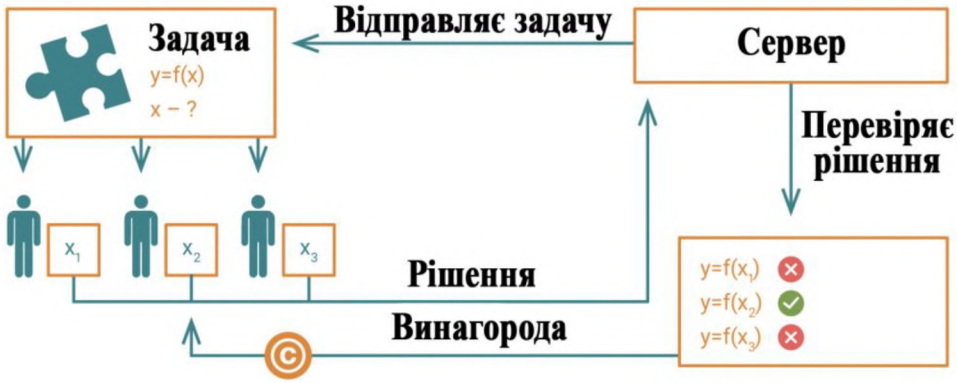

Рис. 2.1 Схема принципу роботи алгоритму Proof-of-Work

Ідея POW полягає в тому, щоб користувачі(майнери) використовували свою обчислювальну потужність для вирішення криптографічно складних головоломок. Майнер, який вирішує проблему, додає новий блок до блокчейну і отримує винагороду за цей блок. Як працює процес:

- Випадковий рядок, що називається "nonce", додається до хешу попереднього блоку;
- Отриманий рядок хешується, а потім перевіряється на наявність мережевих труднощів. Якщо хеш задовольняє умовам, тоді блок додається до ланцюжка;
- Якщо ні, процес повторюється, поки не буде досягнутий бажаний результат.

У POW закладено механізм, який передбачає ускладнення вирішення проблеми зі збільшенням обчислювальних потужністей підключених до системі. Це є значною перевагою POW через те, що він підвищує рівень захищенності системи. Tezos використовує алгоритм Proof-of-Stake, який вимагає від певної кількості токенів

Tezos взяти участь у консенсусі щодо блокчейну. Схема принципу роботи Proof-of-Stake зображена на рис.2.2.

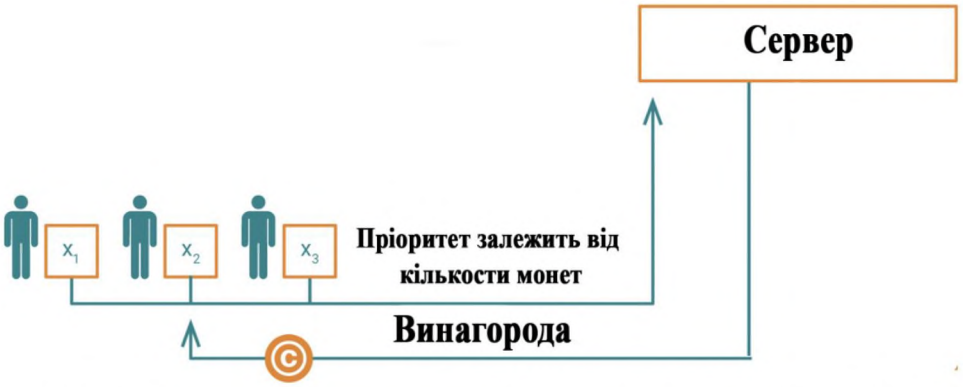

Рис. 2.2 Схема принципу роботи алгоритму Proof-of-Stake

Власники токенів можуть делегувати свої права перевірки іншим власникам жетонів без передачі права власності. Ця ідея сильно відрізняється від Ethereum, де вся мережа бере участь у механізмі консенсусу:

- Процесс добування токенів у такому алгоритмі називається бейкінг
- Бейкери отримують права на блокову публікацію, виходячи зі своєї частки;
- Кожен блок добувається випадковим бейкером, а потім нотаріально засвідчується 32 іншими випадковими бейкерами;
- Якщо блок схвалено, тоді блок додається до блокчейну;
- Успішний бейкер отримує винагороду за блок і може стягувати комісію за транзакції за всі транзакції всередині блоку.

Власники токенів мають можливість делегувати свої права добуття іншим власникам, не відмовляючись від права власності на свої токени. Після завершення процесу випікання пекар поділиться своїми винагородами з рештою делегатів.

Такий механізм видобутку, як і механізм голосування Tezos, вносить дизбаланс у процесс бейкінгу. Система залишає можливість бути власником більшої кількості токенів, та безпосередно впливати на процес бейкінгу, що

руйнує принцип децентралізації та ставить під ризик захищеність платформи від несанкціонованих змін.

Мова программуваня смарт-контракту. Мова програмування, яка використовується для побудови смарт-контрактів на платформі Tezos та Ethereum, також відрізняється. Ethereum використовує мову програмування високого рівня Solidity, тоді як Tezos використовує Michelson. Подібно до того, як Solidity була винайдена командою розробників Ethereum для програмування розумних контрактів, Michelson також є винаходом команди розробників Tezos.

Michelson - це мова програмування, яка дозволяє здійснювати верифікацію. Верифікация - це процес математичного доказування правильності алгоритму щодо специфікації. [20] Отже, щодо смарт-контрактів, побудованих на платформі Tezos за допомогою Майкельсона, можна довести, що вони математично правильні за певними властивостями. Незважаючи на те, що офіційна перевірка не гарантує цілісність коду, вона надає додатковий інструмент, який допомагає розробникам програмувати якісніші смарт-контракти, роблячи їх більш безпечними.

Три основні відмінності між технологіями Tezos та Ethereum. Ці відмінності полягають у управлінні, алгоритмі консенсусу та мові програмування смарт контрактів.

Там, де Tezos фокусується на мережевому управлінні, дозволяючи власникам токенів диктувати напрямок свого протоколу, Ethereum більше фокусується на позамережному управлінні, де команда / фонд розвитку Ethereum диктує майбутнє технології. Механізм розвитку Tezos базується на голосуванні власників токену, що ставить під сумнів принцип децентралізації та спричиняє ризик змін у системі на користь певних користувачів, що є небезпечним фактором для функціонування блокчейна Tezos.

Tezos використовує алгоритм консенсусу Proof-of-Stake, що на відміну від Proof-of-Work, який застосовується в Ethereum, є менш безпечним з точки зору обслуговування системи. Користувачі Ethereum не зацікавлені у розподілу технології, так як для майнінгу використовуються реальні ресурси електроенергії,

а при хард форку майнери будут повинні витрачати свої ресурси марно, в той час як у POS користовачі, котрі роблять свою монету, можуть проголосувати за обидва форки блокчейну і без зусиль добувати таємно. У POW це неможливо, оскільки майнери буквально витрачають енергію, видобуваючи обидві сторони вилки.

Tezos використовує мову програмування Michelson, яку команда розробників винайшла сама. Michelson допускає процес, відомий як верифікація, який дозволяє забезпечити більший рівень безпеки при створенні смарт-контрактів. І навпаки, Ethereum використовує Solidity як вибрану мову програмування.

Таблиця 2.1 Основні характеристики блокчейнів ETHEREUM та TEZOS

	ETHEREUM	TEZOS
Призначення	Майданчик для створення децентралізованих алгоритмів	Майданчик для створення децентралізованих алгоритмів
Управління	Позамережеве	У мережі
Емісія	Безкінечна	Максимум 797534902
Алгоритм консенсусу	PROOF-OF-WORK	PROOF-OF-STAKE
Мова программуваня смарт-контракту	Solidity та Vyper	Michelson

Беручі до уваги відмінності двух блокчейнів, та спираючись на критерії оцінки безпеки платформи, а саме децентралізованість та захищеність платформи від несанкціонованих змін, блокчейн Ethereum відповідає цим вимогам, завдяки своїм механізмам управління та алгоритму консесусу Proof-of-Work, в той час як особливості Tezos роблять цю платформу не придатною для вирішення задачі.

2.3 АНАЛІЗ ТА ВИБІР СТАНДАРТІВ СМАРТ-КОНТРАКТІВ

На даний момент у блокчейні Ethereum існують два стандарти, що підтримують невзаємозамінні токени, це ERC-721 та ERC-1155. Розглянемо характеристики цих стандартів, їх особливості та оберемо найбільш доцільний для використання під час рішення задачі.

ERC-721. Стандарт токена ERC-721 представляє єдиний унікальний актив, який неможливо замінити. Токени ERC-721 представляють повний актив, такий як сертифікат або токенізований товар, який не можна розділити. Кожен токен ERC-721 містить свої унікальні контрактні цінності, такі як вміло запрограмований витвір мистецтва, або дані про право власності та ідентифікацію токенізованого реального активу, наприклад будинку. Хоча існує повна гнучкість у створенні токена, ERC-721 надійні з точки зору незмінності, прозорості власності та безпеки.

Кожен токен ідентифікується унікальним ідентифікатором uint256 всередині смарт-контракту ERC-721. Цей ідентифікаційний номер не змінюється протягом усього терміну дії контракту. Набір параметрів (контрактна адреса, uint256 tokenId) буде глобально унікальним і повністю кваліфікованим ідентифікатором конкретного активу в мережі Ethereum. Хоча деякі смарт-контракти ERC-721 можуть вважати зручним розпочинати з ідентифікатора 0 і просто збільшувати на одиницю для кожного нового NFT, абоненти НЕ повинні вважати, що ідентифікаційні номери мають певний шаблон, і повинні розглядати ідентифікатор як "чорний ящик" ". NFT можуть може стати недійсними (бути знищеними).

Токени ERC721 можуть використовуватися в будь-якому обміні, але їх вартість - результат унікальності і рідкості кожного токена. Стандарт визначає функції name, symbol, totalSupply, balanceOf, ownerOf, approve, takeOwnership, transfer, tokenOfOwnerByIndex і tokenMetadata. Він також визначає дві події: Transfer і Approval.

Механізм передачі. ERC-721 стандартизує безпечну функцію передачі safeTransferFrom (перевантажену параметром байтів і без нього) та небезпечну функцію transferFrom. Передача може бути ініційована:

- Власником NFT;
- Затвердженою адресою NFT;
- Уповноваженим оператором поточного власника NFT;
- Крім того, уповноважений оператор може встановити затверджену адресу для NFT.

Це забезпечує потужний набір інструментів для гаманців, брокерів та аукціонів для швидкого використання великої кількості NFT.

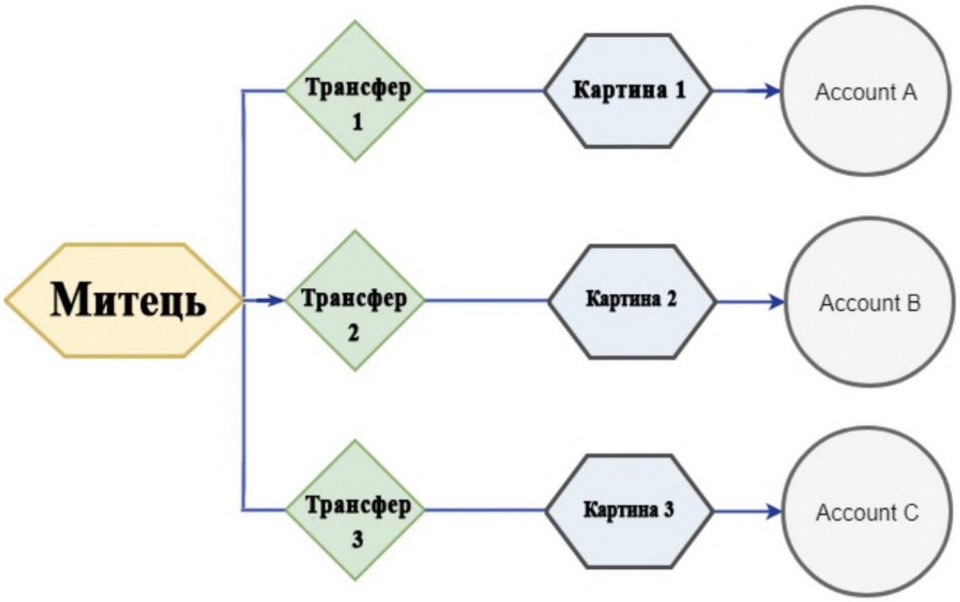

Рис. 2.3 - Схема транзакції ERC-721

Функції ERC-721

name

Призначений для повідомлення зовнішніми контрактами і додатків назви токена. Наприклад, функція може бути реалізована наступним чином:

```
contract MyNFT {
function name () constant returns (string name) {
return "My Non-Fungible Token";
}
}
```

symbol

Ця функція також забезпечує сумісність зі стандартом токенов ERC20. Вона повідомляє зовнішнім програмам коротка назва, або символ, токена.

```
contract MyNFT {
function symbol () constant returns (string symbol) {
return "MNFT";
}
```

totalSupply

Ця функція задає загальну кількість монет, доступних в блокчейне. Пропозиція не обов'язково має бути константою.

```
contract MyNFT {
// Це число може бути довільним
uint256 private totalSupply = 1000000000;
function totalSupply () constant returns (uint256 supply) {
return totalSupply;
}
}
```

BalanceOf

Ця функція використовується, щоб знайти кількість токенов, що належать конкретній адресі.

```
contract MyNFT {
```

```
mapping (address => uint) private balances;
function balanceOf (address _owner) constant returns (uint balance)
{
return balances [_owner];
}
}
```

Функції володіння

Дані функції визначають, як контракт буде розглядати права власності на токени і як ці права можуть передаватися. Найбільш значущі серед цих функцій - takeOwnership і transfer, що діють відповідно як функції зняття і пересилання і є важливими для можливості перекладу токенов між користувачами.

ownerOf

Ця функція визначає адресу власника токена. Оскільки токени ERC721 невзаємозамінні і, отже, унікальні, в блокчейне їм присвоєні унікальні ідентифікатори. Визначити власника токена можна за допомогою його ID.

```
contract MyNFT {
mapping (uint256 => address) private tokenOwners;
mapping (uint256 => bool) private tokenExists;
function ownerOf (uint256 _tokenId)
constant returns (address owner) {
require (tokenExists [_tokenId]);
return tokenOwners [_tokenId];
}
}
```

Approve

Ця функція схвалює дозвіл іншому суб'єкту переводити токен від імені власника. Наприклад, якщо Аліса володіє 1 MyNFT, вона може викликати функцію approve для свого друга Боба. Після успішного виклику Боб може пізніше розпоряджатися токеном від імені Аліси або стати його власником. Більше про передачу прав власності можна дізнатися з опису функцій takeOwnership і transfer.

```
contract MyNFT {
mapping (address => mapping (address => uint256)) allowed;
function approve (address _to, uint256 _tokenId) {
require (msg.sender == ownerOf (_tokenId));
require (msg.sender! = _to);
allowed [msg.sender] [_ to] = _tokenId;
Approval (msg.sender, _to, _tokenId);
}
```

takeOwnership

Ця функція діє як функція зняття, оскільки інша сторона може викликати її, щоб зняти маркери з рахунку користувача. Таким чином, takeOwnership може використовуватися, коли користувач отримав схвалення (approve) на володіння певною кількістю токенов і бажає зняти ці маркери з рахунку іншого користувача.

```
contract MyNFT {
function takeOwnership (uint256 _tokenId) {
require (tokenExists [_tokenId]);
address oldOwner = ownerOf (_tokenId);
address newOwner = msg.sender;
require (newOwner! = oldOwner);
require (allowed [oldOwner] [newOwner] == _tokenId);
balances [oldOwner] - = 1;
tokenOwners [_tokenId] = newOwner;
```

```
balances [newOwner] + = 1;
Transfer (oldOwner, newOwner, _tokenId);
}
}
```

Transfer

Ця функція - ще один спосіб передачі токенов. transfer дозволяє власнику токена переслати його іншому користувачеві, подібно звичайному криптовалюта. Однак переклад може бути ініційований, тільки якщо приймає рахунок раніше отримав від відправляє рахунку схвалення на володіння токеном.

```
contract MyNFT {
mapping (address => mapping (uint256 => uint256)) private ownerTokens;
function removeFromTokenList (address owner, uint256 _tokenId) private {
for (uint256 i = 0; ownerTokens [owner] [i]! = _tokenId; i ++) {
ownerTokens [owner] [i] = 0;
}
}
function transfer (address _to, uint256 _tokenId) {
address currentOwner = msg.sender;
address newOwner = _to;
require (tokenExists [_tokenId]);
require (currentOwner == ownerOf (_tokenId));
require (currentOwner! = newOwner);
require (newOwner! = address (0));
removeFromTokenList (_tokenId);
balances [oldOwner] - = 1;
tokenOwners [_tokenId] = newOwner;
balances [newOwner] + = 1;
Transfer (oldOwner, newOwner, _tokenId);
}
```

}

tokenOfOwnerByIndex

Кожен власник невзаємозамінних токенов може одночасно володіти більш ніж одним токеном. Але так як кожному токені присвоєно унікальний ідентифікатор, може бути складно відстежувати окремі маркери, що належать користувачеві. Тому контракт веде облік ідентифікаторів всіх токенов, що належать кожному користувачеві. Отже, кожен окремий токен можна знайти за його індексом в списку (масиві) токенов, що належать користувачеві. tokenOfOwnerByIndex дозволяє знайти токен даним методом.

```
contract MyNFT {
mapping (address => mapping (uint256 => uint256)) private ownerTokens;
function tokenOfOwnerByIndex (address _owner, uint256 _index) constant returns
(uint tokenId) {
return ownerTokens [
```

ERC1155, був впроваджений командою Enjin, і привносить у NFT ідею напів-взаємозамінності. У ERC1155 ідентифікатори пов'язані не з окремими активами, а з цілими класами активів. Наприклад, ідентифікатор може представляти клас «авторська репродукція», а гаманець володіти 1000 одиниць цих мечів. В цьому випадку, метод balanceOf дозволить відобразити кількість репродукцій, що належать конкретній гаманцю, і користувач зможе передати будь-яку кількість репродукцій, за допомогою методу TransferFrom.
Важливою перевагою такої системи є її ефективність: якщо з ERC721 користувач захоче передати 1000 одиниць авторської репродукції, то йому буде потрібно змінити стан смарт-контракту для кожного з мечів, використовуючи метод TransferFrom, а у випадку з ERC1155 - потрібно лише один раз викликати метод TransferFrom для всіх репродукцій відразу. Але така ефективність загрожує

втратою інформації: тепер не можна відстежити історію переміщення для кожної репродукції окремо. Але, все ж варто звернути увагу, що ERC1155 являє собою розширену версію стандарту ERC721, а це означає, що актив ERC721 може бути створений з використанням функцій ERC1155. Таким чином, у користувача буде окремий ідентифікатор і зазначення кількості «1» для кожного активу.

Функція symbol (яка використовується у ERC-721) не була включена, оскільки розробники не вважають, що це корисний фрагмент даних для ідентифікації загального віртуального активу, а також є схильним до колізій. Це є дісним, symbol використовують в біржах і торгівлі валютою, але вони не такі корисні поза цим простором.

Функція імені (для зручних для читання назв активів, ланцюжкової мережі) була вилучена зі стандарту, щоб дозволити метаданим JSON бути остаточною назвою активу та зменшити дублювання даних. Це також дозволяє локалізацію імен, що в іншому випадку було б надмірно дорогим, якби кожен рядок зберігався в ланцюжку, не кажучи вже про здуття стандартного інтерфейсу. Хоча це рішення може створити невелике навантаження на розробників для розміщення файлу JSON, що містить метадані, ми вважаємо, що будь-яка серйозна реалізація ERC-1155 вже використовуватиме метадані JSON.

Підтримка пакетних переказів. Стандарт підтримує отримання функціями safeTransferFrom та onERC1155Received, оскільки вони значно дешевші при передачах одного токена.

Стандарт підтримує лише безпечні передачі, що дозволяє контрактам приймача залежати від функціїERC1155Received або onERC1155BatchReceived, яка завжди викликається в кінці передачі.

Функція safeBatchTransferFrom дозволяє пакетно передавати кілька ідентифікаторів і значень токенів. Конструкція ERC-1155 робить можливим передачу партії без необхідності укладання контракту, як у стандарту ERC-721. Це зменшує комісію за транзакцію, коли в пакетну передачу включається більше одного типу маркера, порівняно з одиничними передачами з кількома транзакціями.

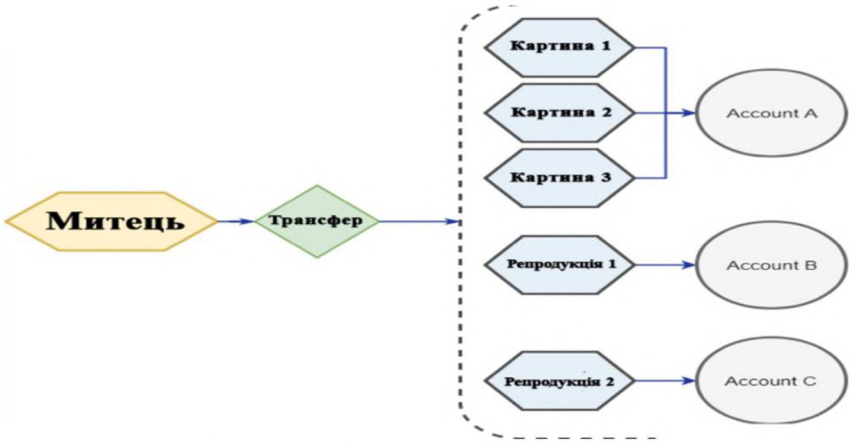

Рис.2.4 - Схема транзакції ERC-1155

Гарантований журнал відстеження. Оскільки екосистема Ethereum продовжує зростати, багато платформ покладаються на традиційні бази даних та служби API Explorer, щоб отримувати та класифікувати дані. Стандарт ERC-1155 гарантує, що журнали подій, випущені смарт-контрактом, надаватимуть достатньо даних для створення точного запису всіх поточних залишків токенів. База даних або дослідник може дивится події та мати можливість здійснювати індексований та категоризований пошук кожного токена ERC-1155 у контракті.

Схвалення. Функція setApprovalForAll дозволяє оператору управляти своїм набором токенів від імені схвалювача. Це забезпечує взаємодію без тертя з біржовими та торговими контрактами.

Обмеження затвердження певним набором ідентифікаторів токенів, кількості або інших правил може бути здійснено за допомогою додаткового стандарту або зовнішнього контракту. Обґрунтування полягає в тому, щоб зберегти стандарт ERC-1155 як можна загальнішим для всіх випадків використання без нав'язування конкретної схеми схвалення реалізаціям, які, можливо, не потребують цього. Можуть використовуватися стандартні стандарт затвердження токенів, такі як запропонований стандарт затвердження ERC-1761, який сумісний з ERC-1155.

Таблиця 2.2 Порівняльний аналіз стандартів ERC-721 та ERC-1155

	ERC-721	ERC-1155
Замінність	Невзаємозамінний	Напів невзаємозамінний

Пакетні перекази	Підтримує передачу одного токену за раз	Підтримує пакетну передачу багатьох ідентифікаторів токенів в одній транзакції.
Кількість токенів у смарт-контракті	Потрібен новий смарт-контракт, розгорнутий для кожного нового типу токена	Може бути розгорнуто в одному смарт-контракті для нескінченних типів маркерів.

Продовження таблиці 2.2

Заміна ID	Підтримує лише статичні метадані, тому кожен ідентифікатор маркера повинен мати свій URI метаданих, що зберігається або керується смарт-контрактом.	Контракти можуть вказувати на нескінченну кількість URI-токенів, не зберігаючи додаткові дані в ланцюжку. Це може бути використано для вказівки на веб-службу, яка розміщує динамічно генерований токен JSON для кожного токена в базі даних..
Розміщення метаданих	У мережі та поза нею	У мережі та поза нею
Ціна транзакції	Зазвичай велика	До 90% менша, ніж у ERC-721

ERC-721 був першим стандартизованим інтерфейсом для створення NFT та він є найпоширенішим. Це незмінна, прозора форма власності та безпеки. Він не

замінюється, він є незамінним. Він не може бути розділений і являє собою єдиний актив. Він є доцільним для створення та відстеження унікальних NFT. Хоча він є придатним для трансферу, але спроба передати цілу колекцію токенів ERC-721 може бути повільною та неефективною.

Найбільша проблема ERC-721 полягає в тому, що коли плата за транзакцію висока, митець буде повинен заплатити дуже велику ціну за створення токену. Тому, коли потрібно масово створювати токени, використовувати цей контракт не є доцільним.

ERC-1155 – стандарт який підтримує невзаємозамінні та замінні маркери. Його швидше та ефективніше використовувати при пакетній передачі токенів.

ERC-1155 може використовувати один контракт для виготовлення різних типів NFT. Плата за транзакцію знижується на 90%, що робить доступним цей стандарт більш доступним.

Вадою є те, що NFT ERC-1155 важче відстежити з точки зору власності - для збереження даних, що зберігаються на блокчейні, ERC-1155 має специфікації в журналах Etheruem, які мають менш надійну інформацію.

ERC-721 та ERC-1155 є подібними, адже ERC-1155 є поліпшенною версію ERC-721.

ERC-1155 вирішує проблеми стандарту ERC-721, такі як ціна транзакції, кількість токенів у контракті, та розмір данних, що зберігає контракт у мережі блокчейн. З точки зору цифрового мистецтва більш доцільним є використання ERC-1155, так як він надає більшу гнучкість у розміщенні даних, роблячи їх більш захищеними від несанкціонованого доступу, а також надає можливість створювати авторські репродукції картини, або лімітовані зображення, надаючи кожному зображенню унікальний порядковий номер із серії (наприклад 23/100, де 23 – порядковий номер зображення, а 100 – кількість випущених екземплярів).

2.4 ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАСОБІВ ЗБЕРЕЖЕННЯ ОБ'ЄКТА

Розглянувши засоби для створення цифрового сертифіката права власності та обравши найбільш безпечні та доцільні, не менш важливим є спосіб зберігання

самого цифрового зображення. Спосіб повинен забезпечувати цілісність зображення, конфіденційність та захищати від несанкціонованого втручання, у результаті якого зображення може бути знищено.

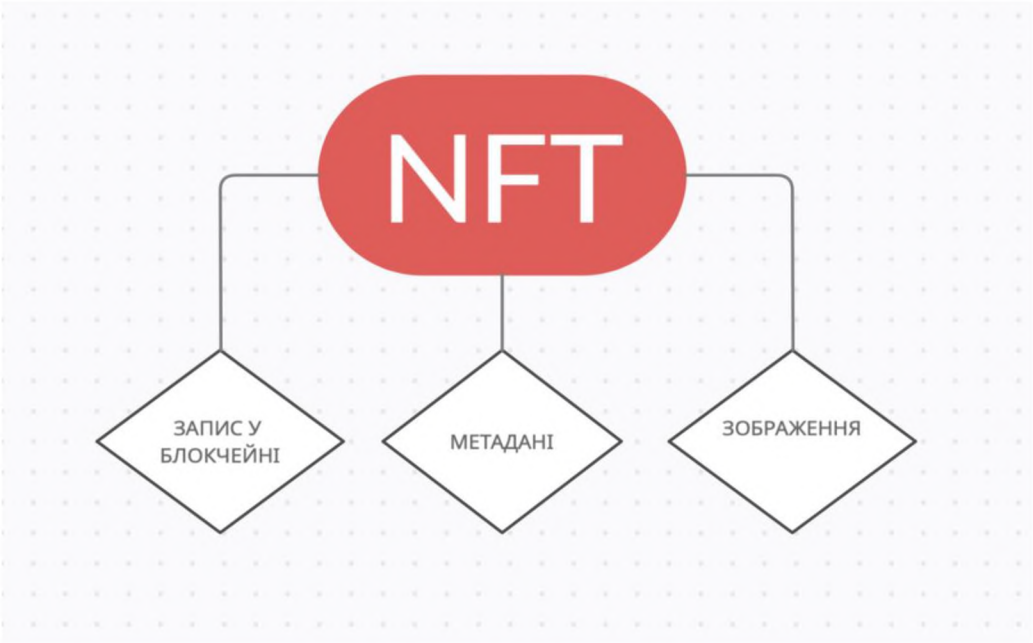

Рис. 2.5 – архітектура NFT

NFT = запис у блокчейні + метадані + медіа

Медіа і дані про ці медіа в більшості існуючих зараз токенів не зберігається у блокчейні.[21]

Зберігати великі обсяги даних у блокчейні Ehereum дуже дорого: формула ціни зберігання даних у блокчейні Etheremum: 640000 gas за 1 кілобайт даних, тобто ~35 долларів США за один кілобайт.

Так розміщення зображення у блокчейні зображення у форматі PNG розміром 800 на 800 пікселів та вагою у 16 кілобайт буде коштувати ~560 доларів США, що може значно перевищувати вартість самого предмета цифрового мистецтва.

Тому в блокчейні зазвичай зберігається тільки адреса (URI), за яким можна знайти інформацію про токени (метадані) і медіа. Через таку ситуацію сам токен і медіа виявляються не пов'язаними один з одним. Токен зберігається на блокчейні, а метадані та медіа у іншому місці. У гіршому випадку, якщо метадані та медіа зберігаються в менш надійному місці, це загрожує тим, що вони виявляться недоступними. Так, у користувача буде токен, і він як і раніше може представляти цінність, наприклад, працювати пропуском в якийсь клуб власників. Але все ж

довести, що саме цей токен був пов'язаний з конкретним медіа буде неможливо. Або медіа буде змінено. Це легко може статися, якщо метадані і саме медіа поширюються з серверів творців токена. В такому випадку, митцю залишається тільки довіряти компанії або людині, яка цей токен створив або обслуговує. Але навіть якщо допустити порядність цих суб'єктів, є ще форс-мажори. Загалом, це приводить до загальних проблем централізованих сервісів - надійність, довіра, залежність від рішень суб'єктів системи.

В NFT співтоваристві ці проблеми відомі, і всі великі гравці так чи інакше працюють над тим, щоб максимально збільшити децентралізацію зберігання медіа частини невзаємозамінних токенов. Розглянемо існуючі рішення для зберігання медіа та метаданих і оберемо найбільш доцільний для використання у межах вирішення задачі.

У мережі Ethereum є найбільш безпечним засобом для збереження цифрового зображення. Файл заванажується безпосередньо у блокчейн, та залишається там назавжди. Завдяки принципам децентралізації блокчейна предмет цифрового мистецтва ніколи не буде видалено чи змінено, але цей метод має недолік – вартість розміщення даних у блокчейні зависока, та залежить від навантаження на мережу.

При піковій завантаженості вартість збереження зображення у форматі PNG розміром 800 на 800 пікселів та вагою у 16 кілобайт може зрости з 560 доларів США до 25 тисяч доларів США.

Умовно у мережі. У блокчейні зберігається ключова інформація, за якою легко відтворюється оригінальне медіа.

Наприклад, Колір кожного пікселя визначається символом і отримуна строка записується в блокчейн. Щоб відновити картинку, потрібно прочитати строку та сформувати зображення з пікселів закодованого кольору. У разі векторного зображення – також потрібен генератор, який алогритмічно створить зображення, вектори якого описані у блокчейні. Умовно, тому що для того, щоб відновити вихідний токен додається додаткове ПО, генератор, який відновлює токен за заданами параметрами. Якщо у користувача є генератор (або він зберігається у

надійному розподіленому сховищі, як IPFS),то він перестає бути залежним від емітента токену. Параметри - назавжди в блокчейне, генератор у користувача. Тож у користувача є повний контроль і над токеном і над медіа цього токена

IPFS \ Pinata. NFT проекти зараз використовують IPFS для зберігання метаданих та зображень своїх токенов.[https://www.dwt.com/insights/2021/03/what-are-non-fungible-tokens]

IPFS розшифровується як InterPlanetary File System. - це гіпермедійний протокол зв'язку з відкритим кодом, за допомогою якого однорангові вузли здійснюють зберігання та поширення даних в єдиній розподіленої файлової системи.[https://docs.ipfs.io/concepts/what-is-ipfs/]

IPFS є одноранговою розподіленою файловою системою, яка з'єднує всі обчислювальні пристрої єдиною системою файлів. У певному сенсі IPFS схожа зі всесвітньою павутиною. IPFS можна уявити як єдиний BitTorrent-рій, обмінюються файлами єдиного Git-сховища. Іншими словами, IPFS забезпечує контентно-адресну модель блочного сховища [22]

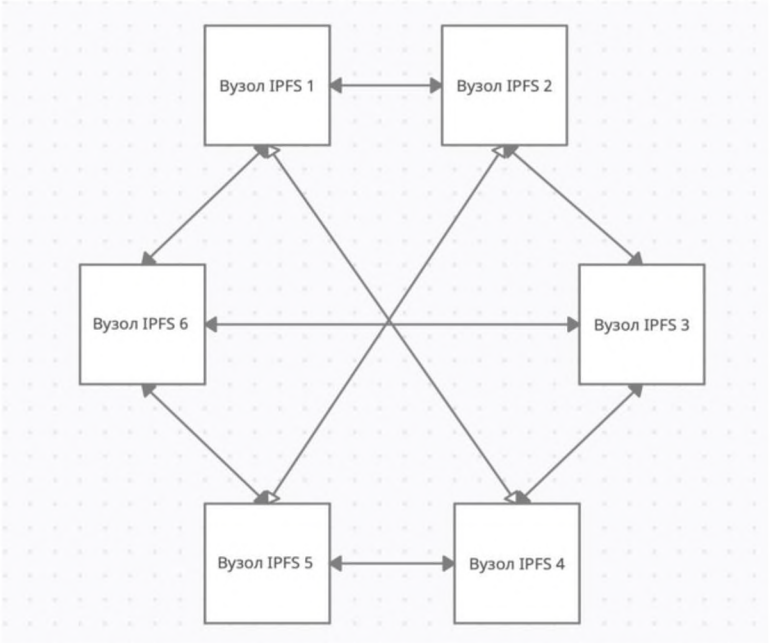

Рис. 2.6 Архітектура IPFS

Коли користувач завантажує файл або картинку в IPFS, він отримуєте хеш цього об'єкта. Цей хеш і буде визначати адресу, за якою можна отримати доступ до об'єкта в IPFS.

Приклад хеша цифрового зображення:
QmahYjHD6SayTZTdyvH7GyaeiwU85HRm7FUPvnaNmfcghA
Так як хеш це текст, цей хеш можна зручно зберігати в контракті.

Але IPFS не є ідеальним, так як його архітектура ніяк не заохочує Ноди за зберігання файлів. Тому збереження і вічна доступність об'єкта в IPFS не гарантована.

Єдиний спосіб гарантувати безпеку - закріпити цей об'єкт, піднявши власний IPFS вузол, або використати спеціальний сервіс, який створює персональний IPFS вузол користувача. Прикладом такого сервісу є Pinata. Але у разі використання IPFS 100% гарантія того, що зображення не буде втрачено залежить лише від того як довго користувач підтримує власну ноду. Тобто концепція децентралізації порушується.

Єдиним плюсом IPFS в цій ситуації залишається те, що для адресації використовується хеш. Якщо цей хеш файлу з метаданими або з медіа зберігається у блокчейні, то він буде доступний завжди. Одже, можна буде зробити резервне копіювання метаданих та медіа NFT на персональному сховищі, і в разі відмови IPFS, скористатися резервною копією, підтвердивши оригінальність файлів за допомогою хеша.

Arweave - це платформа для децентралізованого зберігання інформації.

В основі архітектури лежить концепція не ланцюжка блоків (blockchain), а полотна з блоків (blockweave) - коли кожен наступний блок пов'язаний з двома попередніми.[23]

Для підтведження транзакцій використовується механізм Proof of Access. Це схоже на Proof of Work, але воно має кілька важливих відмінностей. На відміну від PoW, метод Arweave не залежить від попереднього блоку лише для перевірки

транзакцій. Натомість він використовує попередній блок і випадковий блок у ланцюжку. Вони поєднують цей метод зі своєю структурою blockweave, новим способом структурування блокчейнів. Таким чином, майнерам не потрібен весь блокчейн, а лише один існуючий блок, який називається „блок відкликання".
Потім транзакції в цьому блоці виклику хешуються до поточного блоку, щоб створити новий блок. Коли майнери вирішують проблему і знаходять відповідний хеш, вони можуть поділитися новим блоком і відкликати блок із мережею. Для того, щоб підтвердити нову транзакцію (запис інформації), вузол повинен підтвердити швидкий доступ до вже зберігається. Таким чином, в мережі Arweave вузли фінансово мотивовані забезпечувати швидкий і безперебійний доступ до зберігаються об'єктів.

Платити за зберігання даних в Arweave потрібно тільки один раз - в момент завантаження. Розробники Arweave декларують вартість в $ 0.005 / MB. Великим недоліком arweave є модеруємість та цензуремість контенту, що розміщується у мережі. Контроль над контентом здійснюється нодами, що з одного боку є гарантією децентралізованого прийняття рішення, але залишає бекдор для знищення предмету цифрового мистецтва.

Таблиця 2.3 Порівняльний аналіз засобів збереження цифрових зображень

	У мережі	Умовно у мережі	IPFS	Arweave
Вартість	$~35 / KB	$~35 / KB	безкоштовно	$ 0.005 / MB
Залежність	Цілком незалежний метод	Існує залежність від генератора зображення	Залежний від нодів або від підтримки власного ноду	Файл може бути модеровано

Строк існування зображення	“Необмежений”	“Необмежений”	Доки існує хоча б один останній нод	Доки виконується підтримка проекту

Продовження таблиці 2.3

Ризик порушення цілісності зображення	Відстуній	Існує, якщо буде пошкоджено генератор	Відстуній	Існує

З переглянутих засобів розміщення цифрового зображення лише один повністю відповідає критеріям децентралізованності та незалежності від зовнішних чинників, що гарантує цілісність та безпеку зображення, це засіб розміщення файлу безпосередньо у мережі блокчейн. Хоча такий спосіб є достатньо дорогим, він повністю гарантує збереження файлу у незмінному вигляді назавжди. Його не можна буде не змінити чи видалити.

2.5 ПОРІВНЯННЯ ПЛАТФОРМ ДЛЯ ПОШИРЕННЯ ПРЕДМЕТІВ ЦИФРОВОГО МИСТЕЦТВА

Розглянемо відкриті для розміщення платформи для поширення об’єктів цифрового мистецтва та проаналізуємо характеристики та особливості їх реалізації. Це AsyncArt, infiNFT, KnownOrigin, MakersPlace, Mintbase, NiftyGateway, OpenSea, Rarible, SuperRare

З наведених платформ лише одна використовує та підтримує параметри, необхідні для захисту та підтвердження права власності на предмети цифрового

мистецтва. Це платформа ArtBlocks. Метадані та цифрове зображення зберігаються безпосередньо у мережі блокчейн, що гарантує їх незмінність, також платформа підтримує випуск токенів стандарту ERC-1155, що додає гнучкості у створенні робіт не у одиничному екземплярі

Назва платформи	Метадані	Цифрове зображення	Підтримувані стандарти
ArtBlocks	У мережі блокчейн	У мережі блокчейн	ERC-721 ERC-1155
AsyncArt	IPFS	IPFS	ERC-721 ERC-1155
infiNFT	У мережі блокчейн	IPFS+Arweave	ERC-721 ERC-1155
KnownOrigin	IPFS	IPFS	ERC-721
MakersPlace	IPFS	IPFS	ERC-721 ERC-1155
Mintbase	IPFS+Arweave	IPFS+Arweave	ERC-721
NiftyGateway	Назва колекції та ім'я артиста зберігаються у блокчейні. Деякі назви робіт - у блокчейні, деякі – IPFS.	IPFS	ERC-721 ERC-1155
OpenSea	Зберігаються на власному сховищі платформи	Зберігаються на власному сховищі платформи	ERC-721 ERC-1155
Rarible	IPFS	IPFS	ERC-721 ERC-1155
SuperRare	IPFS	IPFS	ERC-721 ERC-1155

Таблиця 2.4 Платформи для розміщення предметів цифрового мистецтва та технології, що вони використовують.

2.6 ПОБУДУВАННЯ АРХІТЕКТУРИ ПРОГРАМНО-АПАРАТНОЇ РЕАЛІЗАЦІЇ ТЕХНОЛОГІЇ ПІДТВЕРДЖЕННЯ ПРАВА ВЛАСНОСТІ ОБ'ЄКТАМИ ЦИФРОВОГО МИСТЕЦТВА

На основі аналізу компонентів програмно-апаратної реалізації технології підтвердження права власності об'єктами цифрового мистецтва у спеціальній частини кваліфікаційної роботи на рисунку 2.7 схематично зображено архітектуру програмно-апаратної реалізації технології підтвердження права власності об'єктами цифрового мистецтва.

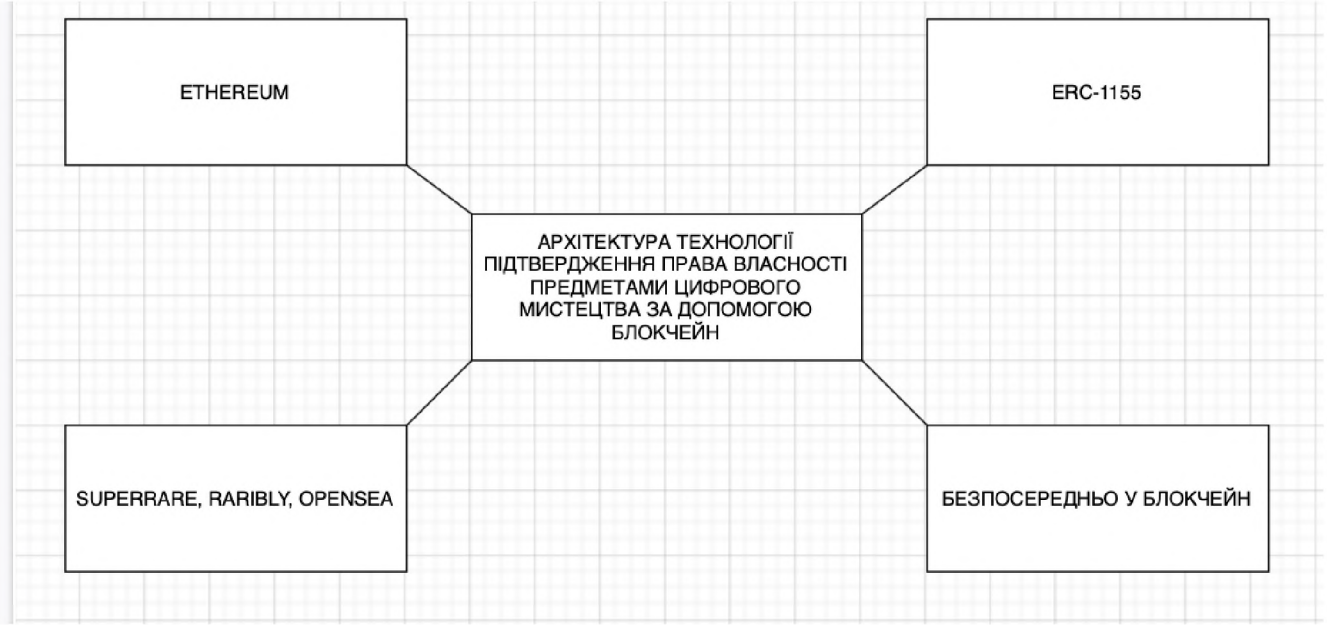

Рис 2.7 Архітектура програмно-апаратної реалізації технології підтвердження права власності об'єктами цифрового мистецтва

ВИСНОВКИ ДО ДРУГОГО РОЗДІЛУ

У другому розділі було розглянуто, проаналізовано та порівняно компоненти архітектури програмно-апаратної реалізації підтвердження права власності предметами цифрового мистецтва за допомогою технології блокчейн. Обрано найбільш доцільні для використання блокчейни, стандарти токенів та було порівняно засоби збереження медіаданих при створенні токена. З отриманих результатів аналізу було вибрано найбільш доцільну для використання платформу для поширення предметів цифрового мистецтва з реалізованою технологію підтвердження права власності за допомогою технології блокчейн

3 ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 ТЕХНІКО ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ

Основною задачею цього розділу є техніко-матеріальне обґрунтування доцільності впровадження програмно-апаратної реалізації підтвердження права власності об’єктами цифрового мистецтва за допомогою технології блокчейн.

Необхідність імплентування технології підтвердження права власності об’єктами цифрового мистецтва полягає у необхідності цифрових митців монетизувати та захистити свої роботи, наділяючи їх параметрами унікальності, роблячи їх продаж та обмін більш подібним до аналогічного процесу з фізичними картинами.

Аналізуючи запропоновані в кваліфікаційній роботі варіанти впровадження програмно-апаратної реалізації підтвердження права власності об’єктами цифрового мистецтва за допомогою технології блокчейн, результатом економічного аналізу буде доцільність використання запропонованих варіантів вирішення.

3.2 ВИЗНАЧЕННЯ ВИТРАТ НА ВПРОВАДЖЕННЯ

Основою для розрахунку витрат для на розробку політики безпеки інформації є концепція сукупності вартості володіння запропонована Gartner Group. У цій моделі враховуються наступні IT-витрати: фіксовані (капітальні) вкладення і поточні витрати.

Модель від Gartner Group пропонує наступні вагові частки кожної з наведених вище статей витрат стосовно сукупної вартості, які можна використовувати для спрощеної оцінки сукупної вартості володіння.

Таблиця 3.1

Фіксовані (капітальні) вкладення	33259 грн

Поточні витрати	3915 грн

Перш за все потрібно розрахувати капітальні інвестиції та капітальні затрати у впровадження програмно-апаратної реалізації підтвердження права власності об’єктом цифрового мистецтва. За методикою Gartner Group до фіксованих (капітальних) варто відносити наступні витрати:

– вартість розробки проекту інформаційної безпеки (впровадження програмно-апаратної реалізації підтвердження права власності об’єктами цифрового мистецтва);

– витрати на залучення зовнішніх консультантів;

– вартість первісних закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

– вартість створення основного й додаткового програмного забезпечення (ПЗ);

– витрати на первісні закупівлі апаратного забезпечення;

– витрати на інтеграцію системи інформативної безпеки у вже існуючу корпоративну систему (встановлення обладнання, програмного забезпечення та налагодження системи інформаційної безпеки);

– витрати на навчання технічних фахівців і обслуговуючого персоналу.

– Для повного визначення розробки політики безпеки інформації з точки зору економічної доцільності спочатку необхідно і доцільно розрахувати:

– Визначення трудомісткості розробки політики безпеки інформації;

– розрахунок витрат на розробку політики безпеки інформації.

З зазначених вище витрат під час впровадження програмно-апаратної реалізації підтвердження права власності об’єктами цифрового мистецтва митець несе лише наступні:

– витрати на залучення зовнішніх консультантів;

– вартість створення основного й додаткового програмного забезпечення

Капітальні вкладення для впровадження програмно-апаратної реалізації підтвердження права власності об'єктами цифрового мистецтва за допомогою технології блокчейн можуть бути обчислені за наступную формулую:

$$К= К_{пр}+К_{пз}, \text{ де} \quad (3.1)$$

$К_{пр-}$ – витрати на залучення зовнішніх консультантів;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення (ПЗ);

Згідно консультаційному агентству з питань створення та імплементуванні невзаємозамінних токенів nftraven.com година консультації спеціаліста коштує 400 доларів сша, що за курсом на 1 червня 2021 року становить 10986 гривень.

Під створенням основного й додаткового програмного забезпечення слід мати на увазі безпосередньо процес створення токена і розміщення в мережі блокчейн медіфайла.

Вартість розміщення в медіафайлу у мережі блокчейна Ethereum розраховується за наступною формулою:

$$640000 \text{ gas за } 1 \text{ кб даних} \quad (3.2)$$

Умовна одиниця gas - це одиниця обчислення, яка позначає розмір комісії за певну дію або транзакцію. Не є константою, величина залежить від напруженості мережі блокчейн та капіталізації Ethereum. [24]

Станом на 1 червня 2021 року вартість 1 одиниці gas становить 29.75 gwei,

1 gwei = 0.000000001 ETH

Станом на 1 червня 2021 року вартість 1 ETH становить 2708 доларів сша, або 73127.61 гривень

Вартість 1 кб даних у мережі блокчейн Ethereum на 1 червня 2021 року становить:

640000 * 29.75 * 0.000000001* 2708 = 51.56 доларів США, або 1392.12 гривень

(3.3)

Вартість збереження у мережі блокчейн зображення у форматі PNG розміром 800 на 800 пікселів та вагою у 16 кілобайт:

16 кб * 1392.12 грн = 22273.92 грн

(3.4)

Капітальні вкладення для впровадження програмно-апаратної реалізації підтвердження права власності об'єктами цифрового мистецтва за допомогою технології блокчейн становлять:

К= 10986 грн + 22273.92 грн = 33259.92

(3.5)

До поточних витрат можна віднести комісію, яку повинен сплатити митець під час продажу предмета цифрового мистецтва, згідно порталу для продажу NFT opensea.com сума комісії сягає 2.5% від вартості продажу роботи. [25]

Так як вартість предметів цифрого мистецтва може значно відрізнятися залежно від роботи, під час підрахунку комісії та у подальшому за вартість предмету цифрового мистецтва буде використовуватися середня ціна проданої роботи на порталі SuperRare, що становить 5800 доларів сша, або 156600 гривень.

Так комісія від продажу становить:

156600 грн * 2.5% = 3915 гривень

(3.6)

3.3 ОЦІНКА МОЖЛИВОГО ЗБИТКУ ВІД АКТАКИ

Можна виділити 3 основних типи загроз стосовно предметів цифрового мистецтва, а саме:

- Втрата ідентифікатора;
- Крадіжка ідентифікатора;
- Силовий захват предмета цифрового мистецтва.

У наслідку реалізації кожного типу загрози власник зазнає збитків у розмірі 100% від вартості предмету цифрового мистецтва, бо кожен тип загрози має на увазі під собою повну втрату права власності на роботу.

У наслідку втрати ідентифікатора автор чи власник предмету цифрового мистецтва втрачає можливість доступу до роботи, що знижує її ліквідність до 0, повністю знецінюючи ринкову вартість роботи. Збитки від такої загрози становлять 100% вартості актива.

У наслідку крадіжки ідентифікатора автор чи власник предмету також втрачає можливість доступу до роботи, але злочинник має можливість реалізувати предмет цифрового мистецтва на спеціальному майданчику. Збитки від такої загрози становлять 100% вартості актива.

У наслідку силового захвату предмета цифрового мистецтва через силове змушення передати право власності злочинникам власник втрачає власність над активом. Збитки від такої загрози становлять 100% вартості актива.

Ймовірність втрати ноутбуку, на якому зберігається ідентифікатор, складає 10%, згідно дослідженню Університету Пітсбурга.

[26]

Ймовірність крадіжки ідентифікатора складає 0.3%.

[27]

Ймовірність силового захвату активу складає 0.001%.

[28]

Ймовірність реалізації хоча б одного з трьох типів загроз можна розрахувати за формулою:

$$P(A+B+C), \text{ де}$$

A – Ймовірність втрати ідентифікатора;

B – Ймовірність крадіжки ідентифікатора;

C – Ймовірність силового захвату активу.

$$P(A+B+C)=1-(1-0.1)*(1-0.003)*(1-0.00001)=0.102, \text{ або } 10.2\% \quad (3.7)$$

Загальний ефект від для впровадження програмно-апаратної реалізації підтвердження права власності об'єктами цифрового мистецтва за допомогою технології блокчейн визначається з урахуванням ризиків безпеки становить:

$$E = B \cdot R - C$$

де B – загальний збиток від реалізації загрози, 100% або 156600 грн

R – очікувана імовірність реалізації хоча б одного типу загрози, 10.2 %

C – поточні витрати, грн.

$$E = 156600*0.102-3915 = 12058.2 \text{ грн}$$

(3.8)

Для надання повного аналізу ефективності впровадження програмно-апаратної реалізації підтвердження права власності об'єктом цифрового мистецтва необхідно розрахувати коефіцієнт повернення інвестицій.

Для розрахунку коефіцієнту ROSI необхідно знайти відношення, щодо загального ефекту впровадження програмно-апаратної реалізації підтвердження права власності об'єктом цифрового мистецтва до капітальних інвестицій, що забезпечили цей варіант.

Вважатимемо, що бажаним результатом є значення ROSI > 0

$$ROSI = E/K$$

$$ROSI = 12058.2/33259.92=0.36=36\%$$

Одиниця виміру – грн./грн.

(3.9)

Висновки

У третьому розділі, кваліфікаційної роботи було встановлено доцільність впровадження програмно-апаратної реалізації підтвердження права власності об'єктом цифрового мистецтва. Використання технології невзаємозамінних токенів на основі технології блокчейн наділяє цифрові зображення параметрами унікальності, що робить їх цифровим аналогом фізичних предметів цифрового мистецтва, отже наділяє предмет цифрового мистецтва ліквідністю. Щодо

інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки, показник ROSI при впровадженні підтвердження права власності на основі технології блокчейн складає 36%, що є задовільним результатом, враховуючи що до впровадження об'єкт захисту не є ліквідним активом. Унікальний цифровий об'єкт, право власності на який може буде підтверджено, є предметом колекціонування, що дозволяє цифровим митцям монетизувати свої роботи, аналогічно до фізичних предметів мистецтва. Предмети цифрового мистецтва з імплементованною технологією підтвердження права власності можуть бути виставлені на аукціони чи продані через прямий продаж від митця до покупця.

Висновки

Під час виконання кваліфікаційної роботи виконано наступне:

В першому розділі кваліфікаційної роботи надано загальний аналіз стану цифрового мистецтва, надано його актуальність та проаналізовано наявні засоби підтвердження права власності цифровими об’єктами

У другому розділі було розглянуто, проаналізовано та порівняно компоненти архітектури програмно-апаратної реалізації підтвердження права власності предметами цифрового мистецтва за допомогою технології блокчейн. Обрано найбільш доцільні для використання блокчейни, стандарти токенів та було порівняно засоби збереження медіаданих при створенні токена. З отриманих результатів аналізу було вибрано найбільш доцільну для використання платформу для поширення предметів цифрового мистецтва з реалізованою технологію підтвердження права власності за допомогою технології блокчейн

У третьому розділі, кваліфікаційної роботи було встановлено доцільність впровадження програмно-апаратної реалізації підтвердження права власності об’єктом цифрового мистецтва. Використання технології невзаємозамінних токенів на основі технології блокчейн наділяє цифрові зображення параметрами унікальності, що робить їх цифровим аналогом фізичних предметів цифрового мистецтва, отже наділяє предмет цифрового мистецтва ліквідністю.

Перелік посилань

1. Електроний ресурс go-gulf.com Online Piracy in Numbers – Facts and Statistics [Infographic]
Режим доступу: https://www.go-gulf.com/online-piracy/
2. Електроний ресурс wikipedia.org Комп'ютерне мистецтво Режим доступу: https://uk.wikipedia.org/wiki/Комп%27ютерне_мистецтво
3. Електроний ресурс instastatistics.com LIVE INSTAGRAM STATISTICS instastatistics.com
4. Електроний ресурс wikipedia.org Digital image Режим доступу: https://en.wikipedia.org/wiki/Digital_image
5. Електроний ресурс timeweb.com Как выбрать подходящий для web формат изображения. Катерина Филиппова Режим доступу: https://timeweb.com/ru/community/articles/kak-vybrat-podhodyashchiy-dlya-web-format-izobrazheniya-1
6. Електроний ресурс wikipedia.org ICO Режим доступу: https://uk.wikipedia.org/wiki/ICO
7. Електроний ресурс w3techs.com Usage statistics of image file formats for websites Режим доступу: https://w3techs.com/technologies/overview/image_format
8. Електроний ресурс compress.ru Цифровые водяные знаки. Светлана Шляхтина Режим доступу: https://compress.ru/article.aspx?id=9686
9. Електроний ресурс lib.itsec.ru Цифровые водяные знаки в изображениях. Борис Борисенко
Режим доступу: https://lib.itsec.ru/articles2/Oborandteh/cifrov_vodyan_znaki_v_izobrazheniyah

10.Електроний ресурс wikipedia.org Блокчейн Режим доступу: https://uk.wikipedia.org/wiki/Блокчейн

11.Електроний ресурс Binance What is cryptocurrency mining. Binance Режим доступу: https://academy.binance.com/ru/articles/what-is-cryptocurrency-mining

12.Електроний ресур Binance What is a blockchain consensus algorithm. Binance Режим доступу: https://academy.binance.com/ru/articles/what-is-a-blockchain-consensus-algorithm

13.Електроний ресурс coinmarketcap.com Капитализация криптовалют Режим доступу: https://coinmarketcap.com

14. Електроний ресурс forklog.comЧто такое Proof-of-Work и Proof-of-Stake? ForkLog Режим доступу: https://forklog.com/chto-takoe-proof-of-work-i-proof-of-stake/

15.Електроний ресурс ru.wikipedia.org Смарт-контракт Wikipedia Режим доступу: https://ru.wikipedia.org/wiki/Смарт-контракт

16.Електроний ресурс crypto.com Token Standards Режим доступу: https://crypto.com/university/article?category=crypto101&page=token-standards

17.Електроний ресурс Wikipedia

18.Електроний ресурс ethereum.org

19.Електроний ресурс corporatefinanceinstitute.com Hard fork Режим доступу: https://corporatefinanceinstitute.com/resources/knowledge/other/hard-fork/

20.Електроний ресурс mycptpedia Consortium Blockchain Explained Режим доступу: https://www.mycryptopedia.com/consortium-blockchain-explained/

21.Електроний ресурс dwt.com What are non fungible tokens Режим доступу: https://www.dwt.com/insights/2021/03/

22.Електроний ресурс ipfs.io What is ipfs Режим доступу: https://docs.ipfs.io/concepts/ /

23.Електроний ресурс Arweave.org www.arweave.org

24.Електроний ресурс decenter.org Что такое gas Режим доступу: https://decenter.org/ru/chto-takoe-gas-gas-limit-i-gas-price-v-seti-ethereum

25.Електроний ресурс opensea.io NFT COMISSION Режим доступу: https://docs.opensea.io/docs/frequently-asked-questions

26.Електроний ресурсgcu.edu Lost laptop cybersecurity threat Режим доступу: https://www.gcu.edu/blog/engineering-technology/lost-laptop-cybersecurity-threat

27.Електроний ресурс Investopedia Bitcoin safe storage cold wallet Режим доступу: https://www.investopedia.com/news/bitcoin-safe-storage-cold-wallet /

28.Електроний ресурс bjs.ojp.gov Lifetime Likelihood of Victimization Режим доступу: https://bjs.ojp.gov/content/pub/pdf/llv.pdf

29. Методічні вказівки до виконання економічної частини дипломного проекту, НТУ ДП, 2019

30. Методичні рекомендаціїдо виконання кваліфікаційних робіт бакалаврів спеціальності125 кібербезпека, НТУ ДП, 2020

ДОДАТОК А

ВІДГУК

На кваліфікаційну роботу студента групи 125-17-1 Цуркана Д.І. на тему “Використання технології блокчейн для підтвердження права власності на об’єкти цифрового мистецтва“

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 55 сторінках, 10 рис., 7 табл., 4 додатки, 30 джерел.

Мета кваліфікаційної роботи є актуальною, оскільки розглядає реалізацію підтвердження права власності об’єктами цифрого мистецтва, актуальність підтверджено у розділі 1.

При виконанні кваліфікаційної роботи автор роботи продемонстрував добрий рівень теоретичних і практичних навичок. Розглянув, проаналізував та порівняв компоненти архітектури програмно-апаратної реалізації підтвердження права власності предметами цифрового мистецтва за допомогою технології блокчейн.

Практична цінність кваліфікаційної роботи полягає в розробці архітектури технолгії підтвердження права власності, на яку можна опиратися під час імплементування технології митцями.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з деякими відхиленнями від стандартів.

В цілому кваліфікаційна робота виконана у відповідності до вимог, що ставляться до кваліфікаційної роботи і заслуговує оцінки «_____», а студент Цуркан Даніїл Ігорович присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека».

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату»

доц. Сафаров О.О.

ст. вик. Тимофєєв Д.С

ДОДАТОК Б Перелік матеріалів на електронному носії

1. Кваліфікаційна робота –
2. Презентація – Цуркан Даніїл 125-17-1.pptx

Додаток В. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	1	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	13	
6	А4	Спеціальна частина	27	
7	А4	Економічна частина	7	
8	А4	Висновки	1	
9	А4	Список літератури	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Г. ВІДГУКИ КЕРІВНИКІВ РОЗДІЛІВ

Відгук керівника економічного розділу:

Керівник розділу (підпис) (ініціали, прізвище)

РЕЦЕНЗІЯ

На кваліфікаційну роботу студента групи 125-17-1 Цуркана Д.І.

на тему

“Використання технології блокчейн для підтвердження права власності на об’єкти цифрового мистецтва“

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 55 сторінках, 10 рис., 7 табл., 4 додатки, 30 джерел.

Метою кваліфікаційної роботи є розробка архітектури підтвердження права власності об’єктами цифрового мистецтва на базі технології блокчейн.

Тема кваліфікаційної роботи безпосередньо пов’язана з об’єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз та порівняння технологій доступних для реалізації задачі, розгляд на вибір найбільш доцільних програмно-апартних складових архітектури підтвердження права власности об’єктами цифрового мистецтва

Практичне значення результатів кваліфікаційної роботи полягає у захисті на монетизації предметів цифрового мистецтва.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

Кваліфікаційна робота заслуговує оцінки «Добре».

Рецензент