НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

«На правах рукопису»
УДК 519.21

«До захисту допущено»
В.о. завідувача кафедрою
_____ М.М.Савчук
(підпис) (ініціали, прізвище)
“15” травня 2018р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 113 «Прикладна математика»

на тему: Системи доказу інтелектуальної власності, засновані на технології цифрових відбитків пальців з децентралізованим алгоритмом верифікації

Виконав (-ла): студент (-ка) 2 курсу, групи _____ФІ-63М_____
(шифр групи)

Науринський Юрій Володимирович

Керівник д.т.н. Кудін А.М.

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент к.т.н. Проскуровський Р.В.

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018року

РЕФЕРАТ

Дипломна робота: 67 с., 6 рис., 11 літературних джерел.

Об'єкт дослідження: процес захисту інтелектуальної власності цифрових мультимедійних об'єктів.

Предмет дослідження: застосування в процесі захисту розподіленої бази даних блокчейн та технології цифрових відбитків пальців.

Мета дослідження: підвищити стійкість забезпечення захисту об'єктів інтелектуальної власності при відсутності посередників.

Методи дослідження: методи теорії кодування, теорії складності алгоритмів, методи комп'ютерного та статистичного моделювання.

В даній дипломній роботі описується система доказу інтелектуальної власності, яка заснована на технологіх цифрових відбитків з децентралізованим алгоритмом верифікації. Досліджується застосування в процессі захисту розподіленої бази даних блокчейн та технології цифрових відбитків пальців.

Елементами наукової новизни є застосування технологій цифрових відбитків пальців та децентралізованого алгоритму верифікацій для систем доказу інтелектуальної власності.

Областю можливого практичного застосування є захист авторського права в мережі Інтернет.

Результатом виконання дипломної роботи є теоретичний опис такої системи доказу інтелектуальної власності, яка використовує технології цифрових відбитків пальців та децентралізований алгоритм верифікації.

СИСТЕМИ ДОКАЗУ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ, ТЕХНОЛОГІЇ ЦИФРОВИХ ВІДБИТКІВ ПАЛЬЦІВ, ДЕЦЕНТРАЛІЗОВАНИЙ АЛГОРИТМ ВЕРИФІКАЦІЇ, БЛОКЧЕЙН, СМАРТ-КОНТРАКТ, АВТОРСЬКЕ ПРАВО.

ABSTRACT

Thesis: 67 pp., 6 fig., 11 references.

Object of study: the process of protecting the intellectual property of digital multimedia objects.

Subject of research: application in the process of protection of the distributed blockchain database and the technology of digital fingerprints.

Purpose: increase the stability of the protection of intellectual property objects in the absence of mediators.

Methods: methods of coding theory, computational complexity theory, methods of computer and statistical simulation.

In this thesis described the intellectual property proof system, which is based on the technologies of digital fingerprinting with decentralized verification algorithm. The application of the distributed blockchain database and digital fingerprint technology is being studied in the process of protection.

Elements of scientific novelty are the usage of digital fingerprinting technologies and decentralized verification algorithm for the intellectual property proof systems.

The area of possible practical usage is the copyright protection on the Internet.

The result of the thesis is the theoretical description of such intellectual property proof system which uses digital fingerprinting technology and decentralized verification algorithm.

INTELLECTUAL PROPERTY PROOF SYSTEMS, DIGITAL FINGERPRINTING TECHNOLOGIES, DECENTRALIZED VERIFICATION ALGORITHM, BLOCKCHAIN, SMART-CONTRACT, COPYRIGHT.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ІВ — інтелектуальна власність

DRM — Digital Rights Management

ЦВЗ — цифровий водяний знак

ІН — ідентифікаційний номер

IPFS — InterPlanetary File System

ВСТУП

Актуальність даного дослідження та практичний аспект цієї роботи пов'язані з тим, що в наш час дуже поширена проблема захисту та доказу інтелектуальної власності в мережі Інтернет.

Інститут інтелектуальної власності є ядром сучасної глобальної економіки. У вартості більшості з продуктів частка нематеріальної складової вже досягає вісімдесяти і більше відсотків. Завдяки розвитку технологій інтелектуальна власність набуває нового масштабу і значущості. Самі об'єкти права також є товаром - за останнє десятиліття в обіг введено понад одного мільярду запатентованих об'єктів, а кількість об'єктів, що охороняються авторським правом, перевищує цю кількість на кілька порядків. У вартісному вираженні ринок інтелектуальної власності зростає темпами, що перевищують темпи зростання "матеріальних" ринків - більше 10% в рік.

Основа інтелектуальної власності - право автора, винахідника використовувати результати своєї творчої діяльності. Доступність швидкісних цифрових мереж зв'язку, можливість отримати і використовувати будь-який об'єкт в будь-якій точці світу не дозволяють автору контролювати обіг його власного інтелектуального продукту. Традиційному інституту патентування все складніше впоратися з експоненціальною зростаючою складністю об'єктів. Але виклики, кинуті системі інтелектуального права цифровими технологіями, створюють не тільки проблеми - вони є джерелом нових можливостей: сьогодні технології, народжені правом, розвивають право. Можливості сучасних технологій, такі як розподілені реєстри і смарт-контракти здатні по новому сформувати ринок інтелектуальних продуктів і послуг.

Саме тому нам потрібні нові сучасні системи доказу інтелектуальної власності, які задовольняють висунуті до них вимоги.

Актуальність теми дипломної роботи пов'язана зі значним

поширенням проблем традиційних інститутів захисту інтелектуальної власності, і полягає в необхідності розробки рекомендацій та методів вирішення цих проблем.

Об'єкт дослідження. Процес захисту інтелектуальної власності цифрових мультимедійних об'єктів.

Предмет дослідження. Застосування в процесі захисту розподіленої бази даних блокчейн та технології цифрових відбитків пальців.

Мета роботи. Підвищення стійкості забезпечення захисту об'єктів інтелектуальної власності при відсутності посередників.

Для досягнення поставленої мети необхідне виконання наступних завдань:

1) Розгляд проблеми доказу інтелектуальної власності;

2) Вивчення вже існуючих методів доказу інтелектуальної власності;

3) Аналіз систем доказу інтелектуальної власності;

4) Аналіз технологій цифрових відбитків пальців;

5) Аналіз децентралізованих алгоритмів верифікації;

6) Опис системи доказу інтелектуальної власності, яка підходить для даної дипломної роботи.

В процесі дослідження систем доказу інтелектуальної власності були використані наступні *методи збору та аналізу інформації*:

1) Збір інформації про проблеми доказу цифрового авторського права;

2) Збір інформації про системи доказу інтелектуальної власності;

3) Збір інформації про технології цифрових відбитків пальців;

4) Збір інформації про децентралізовані алгоритми верифікації;

5) Аналіз зібраної інформації;

6) Кластерний аналіз конкурентів системи.

Наукова новизна полягає у такому поєднанні компонентів системи, яка забезечує задачу вирішення проблем традиційних інститутів захисту інтелектуальної власності за допомогою сучасних цифрових технологій.

Практичне значення отриманих результатів високе, на основі опису системи, можлива її побудова та практичне використання.

Масштаби використання необмежені, кожна електронно обчислювальна машина може містити клієнтський застосунок системи. Усі вони працюють незалежно один від одного.

Структура роботи обумовлена предметом, метою і завданням дослідження. Робота складається з вступу, трьох розділів і висновку.

Введення розкриває актуальність, визначає ступінь наукової розробки теми, об'єкт, предмет, мету, завдання та методи дослідження, розкриває теоретичну і практичну значимість роботи.

У першому розділі розглядається проблема доказу авторського права в мережі Інтернет, технологіх цифрових відбитків пальців та децентралізовані алгоритми верифікації. Розглядається задача побудови системи доказу інтелектуальної власності.

У другому розділі розглядається система доказу інтелектуальної власності, її складові та можливі сценарії роботи, надається її опис, з використанням технологій цифрових відбитків пальців та децентралізованого алгоритму верифікації.

У третьому розділі розглядається вирішення задачі побудови системи доказу інтелектуальної власності за допомогою розглянутої системи. Розглядається дана система доказу інтелектуальної власності у порівнянні з іншими системами, метою яких є захист інтелектуальної власності в мережі Інтернет. Розглядається можливість застосування міжнародних стандартів до даної системи.

У висновку підводяться підсумки дослідження, формуються остаточні висновки по темі систем доказу інтелектуальної власності з технологіями цифрових відбитків пальців на основі децентралізованого алгоритму верифікації.

1 ЗАХИСТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

У даному розділи розглядається що таке інтелектуальна власність взагалі, та проблеми захисту інтелектуальної власності в мережі Інтернет. Розглядаються технічні засоби доказу інтелектуальної власності. Розглядаються технології цифрових відбитків пальців та їх застосування. Розглядається візантійська проблема та її зв'язок з децентралізованими алгоритмами верифікації. Розглядається задача побудови систем доказу інтелектуальної власності.

1.1 Захист інтелектуальної власності в мережі Інтернет

У наступному підрозділі надається загальний огляд інтелектуальної власності, та її взаємозв'язку з проблемою доказу інтелектуальної власності в мережі Інтернет.

1.1.1 Інтелектуальна власність

Визначення 1.1. Інтелектуальна власність - ноу-хау, винаходи, корисні моделі, промислові зразки, комерційна таємниця, топографія інтегральних схем, сорти рослин і породи тварин, торговельні марки (знаки для товарів і послуг), географічні позначення, літературні та художні твори, комп'ютерні програми, виконання фонограм, відеограм, передачі організації мовлення і т.д.

У більш широкому розумінні, інтелектуальна власність це

закреплені законом права на результати інтелектуальної діяльності людини у науковій, технічній, виробничій, літературній, художніх областях.

Визначення 1.2. Інтелектуальна діяльність - це творча діяльність, а творчість, це відповідно цілеспрямована розумова робота людини, результатом якої є неповторна, цінна, оригінальна та унікальна річ. Тобто випливає залежність - чим вище інтелектуальний потенціал особистості, тим цінніше цієї особистості результати творчої діяльності, а це, відповідно, інтелектуальна власність.

Об'єктом інтелектуальної власності є право на результати інтелектуальної діяльності людини.

Детальніше, право інтелектуальної власності складається з суми майнових прав та немайнових (рисунок 1.1). У свою чергу, майнові права поділяються на: право володіти, право користуватися, право розпоряджатися. Немайнові права складаються з права на авторство, право на недоторканність твору, тощо [1].

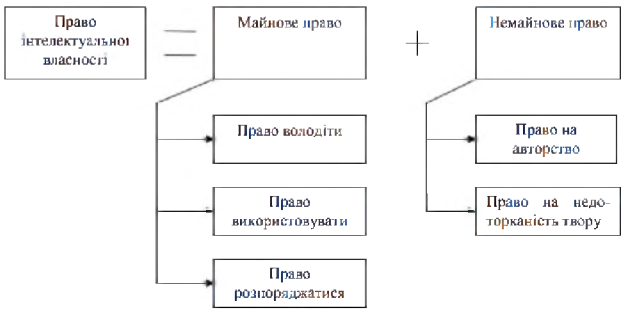

Рисунок 1.1 – Структура права інтелектуальної власності

Правова основа захисту прав інтелектуальної власності в Україні складається з десяти спеціальних законів та поняд двадцяти багатосторонніх міжнародних договорів. Але, на жаль, досі не розроблено нормативно-правового акту, за яким би предбачались способи та методи захисту прав інтелектуальної власності в мережі Інтернет. Відсутність такого нормативного акту, є також однією з перешкод для створення

української системи доказу інтелектуальної власності.

Законодавство України у сфері захисту прав інтелектуальної власності в мережі Інтернет ще тільки на етапі своєї несформованої юності. За роки існування України робилися численні спроби щодо розроблення адекватної правової бази. Наприклад, такі проекти, як закон України "Про внесення змін до деяких законодавчів актів щодо захисту авторського права і суміжних прав у мережі Інтернет", проект Національної стратегії розвитку сфери ІВ в Україні у період до 2020 р., проект стратегії іноваційного розвитку України у 2010-2020 рр. в умовах глобалізаційних ризиків.

Проте, на жаль, доля цих проектів не складає враження що вони просуваються до свого завершення. А тому, з огляду не теперішню ситуацію залишається лише керуватися загальними засадами у сфері інтелектуальної власності, які не здатні повною мірою захистити права власника об'єкта інтелектуальної власності у мережі Інтернет. З огляду на таку ситуацію, і постає задача розробки систем доказу інтелектуальної власності, які в значній мірі спростять процес доказу інтелектуальної власності, та підвищать його ефективність.

З огляду захисту прав інтелектуальної власності в мережі Інтернет, на типовому веб-сайті існує безліч мультимедійних цифрових об'єктів, які потребують захисту, тому що відповідно захищені зареєстрованими правами. Наприклад, це можуть бути такі об'єкти: текст, відео, зображення, програмні файли, макети, аудіо, тощо. Більшість цих об'єктів захищаються авторським правом. У наступному підрозділу, розгляндається детальніше, що таке авторське право.

1.1.2 Авторське право

Визначення 1.3. Авторське право - це юридичний термін, пов'язаний з використанням творів науки, літератури або мистецтва. Він використовується для опису прав, які мають автори на свої твори. Авторське право поширюється як на оприлюднені, так і на не оприлюднені твори, існуючі в будь-якій формі (письмовій, усній, тощо).

Виникає логічне питання: що саме охоплюється авторським правом і що не підпадає під цю категорію? Ми наведемо короткий список об'єктів авторського права:

– Літературні, драматичні та сценарні твори. Музичні твори, у тому числі без тексту;

– Хореографічні твори та пантоміми;

– Твори образотворчого мистецтва (скульптура, графіка, дизайн, фотографія, комікси та інше);

– Похідні твори (переклади, реферати, анотації, огляди, аранжування та інші переробки творів);

– Аудіовізуальні твори (кіно-, теле-, відеофільми та інше);

– Твори архітектури, містобудування;

– Програми для електронно-обчислювальних машин;

– Складові твори (енциклопедії, збірки, антології та інше).

Об'єктами авторського права не є: ідеї, концепції, методи, системи, відкриття, факти, мови програмування. Також авторське право не поширюється на державні символи та знаки, народну творчість, інформаційні (новинні) повідомлення [2].

Майже всі об'єкти авторського права можна перекласти у цифровий мультимедійний об'єкт.

Існує спеціальний термін для керування авторськими правами цифрових об'єктів.

Визначення 1.4. Керування цифровими правами (DRM) - термін, який використовується для посилання на технології авторизації, що застосовуються виробниками апаратного забезпечення, видавцями, власниками авторських прав або приватними особами в першу чергу для обмеження використання цифрової інформації та носіїв.

Зазвичай термін не використовується для опису інших форм захисту від копіювання, які можна оминути без внесення модифікацій в програмне забезпечення пристрою або змін самого файлу, такі, як серійний номер або цифровий ключ. Термін також може використовуватись для посилання на обмеження, безпосередньо пов'язані зі специфічними пристроями або творами в цифровій формі.

Є багато засобів захисту цифрових об'єктів за допомогою DRM, у контексті проблем, які вирішує дана робота, використовуються технології цифрових відбитків пальців.

Цифрові водяні знаки є аналогами звичайних водяних знаків, тобто метаданими, що додаються до цифрового контенту (наприклад, світлини або музичного файлу) та включають певну інформацію про нього (наприклад, про власника авторських прав). Водяні знаки можуть бути видимими для користувача або невидимими (при використанні стеганографії). Цифрові знаки не є механізмами DRM за своєю сутністю, але є частиною системи DRM, яка надає візуальну інформацію про легальність використання контенту, включаючи дані, наприклад, про дату продажу контенту, щодо продавця або покупця тощо.

Далі розглядаються деякі різні способи порушення авторського права в мережі Інтернет.

1.1.3 Порушення авторського права в мережі Інтернет

Гіпертекстові посилання

Гіпертекстове посилання об'єднує між собою два різних чи можливо один веб-сайт. У випадку різних веб-сайтів, не зрозуміло, чи таке посилання порушує авторські права на пов'язаному веб-сайті. Можливо таке, що кожен веб-сайт має нести відповідальність за кожне гіпертекстове посилання на інший веб-сайт, навіть якщо не посилання непряме. В ідеалі, потрібна згода від кожного власника веб-сайту, на кожний з яких веде кожне гіпертекстове посилання.

Обрамлення

Обрамлення дозволяє веб-сайту відображатись у так званому "фреймі", меншому вікні на іншому веб-сайті. Це дає можливість експлуатувати інший веб-сайт без згоди його власника. В ідеалі, потрібна згода від власника на експлуатацію його веб-сайту.

Завантаження та розповсюдження програмного забезпечення

На веб-сайтах, швидко легко та просто завантажувати та розповсюджувати програмне забезпечення. Однак без відповідного дозволу, так завантаження та використання є порушенням авторських прав відповідного програмного забезпечення. В ідеалі потрібно чітко знайомити користувачів з ліцензією на використання програмного забезпечення, вимагати його активної участі у прийнятті умов. В іншому випадку є небажана можливість того, що умови, які прийняв користувач, можуть бути визнані для нього необов'язковими.

Інтернет-патенти

Зазвичай, програмне забезпечення захищене авторським правом. Але якщо таке програмне забезпечення нове, факт його новизни передбачає роботу винахідника, здатну до промислового застосування, таке поєднання дає претензії на патентний захист.

Програмне забезпечення є патентоспроможним тоді, коли воно дає технічний ефект, а саме: вплив на існуючі системи, вплив на існуючи способи обробки даних.

Основними методами захисту інтелектуальної власності є патенти, захист комерційної таємниці та авторське право.

У контексті даної роботи, розглянемо проблеми доказування авторських прав в мережі Інтернет.

1.1.4 Проблеми доказування авторських прав в мережі Інтернет

Головна проблема доказування авторських прав в мережі Інтернет, це надто швидка зміна інформації, її непостійність у будь-який момент часу, так як інформація розповсюджена у мережі Інтернет може бути без попереднього повідомлення видозмінена, видалена, відредагована, будь-ким, будь-коли. З цього випливає що найголовнішим, є оперативне закріплення фактичних даних з веб-сайту, та надання їх до відповідних органів.

Найпоширенішими порушеннями щодо об'єктів права інтелектуальної власності є факт неправомірного використання об'єктів авторського права, права власності на торгівельну марку, неправомірне використання торгівельної марки у якості доменного імені.

Наведемо приклад декілька практичних способів закріплення фактів, як засобів доказування, в мережі Інтернет:

– роздруківка сторінки веб-сайту в мережі Інтернет;

– отримання нотаріального посвідчення для веб-сторінки в мережі Інтернет;

– проведення огляду доказів судом як процесуальна дія;

– надання в суд висновку експерта;

– акт огляду веб-сайту з додатком фотографій сайту, який здійснено адвокатом.

На жаль, в Україні ще не склалася повністю єдина судова практика стосовно встановлення юридичного факту та його допустимості як доказів отриманого в мережі Інтернет. Існує необхідність врегулювання таких проблем на законодавчому рівні.

Розглянемо, відповідно, технічні засоби доказу інтелектуальної власності в мережі Інтернет.

1.1.5 Технічні засоби доказу ІВ в мережі Інтернет

Відповідно до "Рекомендацій щодо вдосконалення механізму регулювання цифрового використання об'єктів авторського права і суміжних прав через мережу Інтернет" [3], є наступні технічні засоби захисту авторського права і суміжних прав в мережі Інтернет:

Ідентифікація об'єктів авторського права і суміжних прав. Ідентифікаційний код ISBN (Міжнародний стандартний книжковий номер) призначений для захисту фонограм; ISAN — номер, розроблений на Міжнародній конференції товариств авторів і композиторів (CISAC) і дозволяє ефективно захищати фільми та інші аудіовізуальні твори; цифровий ідентифікатор DOI, супроводжує твори або їхні частини, дозволяючи тим самим простежити "долю" об'єкта в торговельному обігу; існують й інші програмні коди, що дають можливість порушити цілісність твору при неправильному його використанні.

Електронний цифровий підпис. Суть цифрового підпису полягає в тому, що він дозволяє ідентифікувати справжнього автора того або іншого твору, тим самим знімаючи в контрагента будь-які сумніви про те, з ким

він має справу. Недоліком цього засобу є те, що він працює лише за умови існуючої інфраструктури відкритих ключів.

Цифрові водяні знаки. Найпоширенішою є система так званих "цифрових водяних знаків", впроваджуваних у твори (тексти, графічні зображення і т.п.) у Мережі. Їх перевага полягає в тому, що при звичайному візуальному розгляді зображення користувач не бачить яких-небудь закодованих позначень — значка копірайта ©, імені автора, року видання. Але потім при застосуванні певного програмного засобу можна довести, що файли містять додаткову інформацію, що вказує на особу, яка її записала. Можливе і застосування спеціальних "відбитків" — вони також дозволяють контролювати використання творів в інформаційних мережах, а при виявленні порушень авторського права і суміжних прав, забезпечувати належну доказову базу в суді. Саме цифрові відбитки пальців використовуються у даній роботі як технічний засіб доказу інтелектуальної власності в мережі Інтернет.

Обмеження доступу до матеріалів, що розміщені в Інтернеті, наприклад, бази даних комерційних сайтів і деяких електронних бібліотек та архівів доступні тільки за попередню плату. Можливе застосування "цифрових конвертів що передбачають укладання угоди із власниками тих або інших ресурсів у Мережі.

Метод антикопії, або антикопіювання. Суть полягає в тому, що на CD-ROM ставиться своєрідна заборона робити копії.

Створення веб-депозитаріїв, що дозволяють фіксувати об'єкти інтелектуальної власності у мережі Інтернет і закріплювати їх правовий статус, інакше кажучи, які визначають, що та кому належить.

Метод перехресного субсидування при використанні об'єктів авторського права та суміжних прав. За загальним визначенням, перехресне субсидування це:

– практика фіксації цін на рівні, який перевищує загальні середні витрати на виробництво товарів і послуг у певній галузі за рахунок перерозподілу цінового навантаження серед різних груп споживачів;

– надання фірмою внутрішніх субсидій на виробництво одних товарів або одним підрозділом за рахунок прибутку від інших товарів, діяльності інших підрозділів.

Розглянемо надалі засоби технічного контролю інтелектуальної власності в мережі Інтернет.

1.1.6 Засоби технічного контролю ІВ в мережі Інтернет

Відповідно до "Рекомендацій щодо вдосконалення механізму регулювання цифрового використання об'єктів авторського права і суміжних прав через мережу Інтернет" [3], є наступні технічні засоби контролю авторського права і суміжних прав з використанням об'єктів в мережі Інтернет:

Обмежена функціональність. За такого підходу, власник авторського права надає користувачеві примірник твору, який має функціональні обмеження. Такий підхід є одним із шляхів впровадження в життя таких бізнес-моделей як "спробуй, перед тим, як купити"та "продавай поліпшені версії".

"Годинникова бомба". Аналогічно до прийому з функціональними обмеженнями, за цього підходу власник авторських прав розповсюджує функціонально повноцінний об'єкт інтелектуальної власності, але встановлює дату, після якої доступ до нього буде неможливим. Один з варіантів такого підходу передбачає закриття продавцем доступу до твору після певної кількості користувань (наприклад, після перегляду комп'ютерного файлу 10 разів його буде неможливо більше продивитися).

Захист від копіювання. За цього підходу продавець обмежує кількість разів, коли комп'ютерний файл може бути скопійований. Захист від копіювання був нормою в 1980-х роках, але пізніше вийшов з ужитку

значною мірою тому, що користувачі скаржились на незручність, а також тому, що захист копії можна було досить легко ”зламати”.

Криптографічні конверти. Криптографічні конверти — це програмне забезпечення, яке зашифровує твори так, що доступ до них може бути отриманий лише із застосуванням належного ключа до шифру. Власники прав можуть захищати свої права на твори, розповсюджуючи їх у криптографічних конвертах і вимагаючи від користувачів плати за ключі, за допомогою яких твір можна "вийняти"з ”конверта”.

Контракти. Одним із найефективніших та, на жаль, недооцінених правовласниками засобів запобігання порушенню їхніх прав є контракти. За правильного оформлення контракти можуть надати власникам авторського права і суміжних прав ширше повноваження щодо контролю за використанням їхніх творів ніж ті, що надаються їм відповідно до законодавства. На сьогодняшний день, стрімку популярність у цій сфері набирають так звані смарт-контракти.

Запобіжні заходи. Законодавством держав-членів Світової організації торгівлі мають бути передбачені процедури, які передбачають ефективні дії проти будь-якого порушення прав інтелектуальної власності, в тому числі термінові заходи, та способи захисту прав, які стримують від подальших порушень.

У наступному підрозділі роглядаються, що таке технології цифрових відбитків пальців та їх використання у контексті даної роботи.

1.2 Технології цифрових відбитків пальців

У наступному підрозділі надається загальний огляд технологій цифрових відбитків пальців та їх взаємозв’язок з інтелектуальною власністю

1.2.1 Загальний огляд

Визначення 1.5. Алгоритм відбитків пальців або цифрового відбитку, в загальному випадку це відображення $\phi\colon D \to P$ де D — множина всіх можливих документів, P — множина всіх можливих відбитків пальців, являє собою процедуру, яка відображає відносно великий обсяг даних (комп'ютерний файл), в набагато коротший тип бітових рядків, відбиток пальця.

Також, алгоритм відбитків пальців має назви цифровий відбиток та стегосистема ідентифікаційних номерів.

Такий цифровий відбиток однозначно ідентифікує вихідні дані для всіх практичних цілей, так як відбитки пальців людини однозначно ідентифікуються лише тоді, коли мова заходить про практичні застосунки.

Відбитки пальців, як правило, використовуються, щоб уникнути порівняння і передачі великого об'єму даних. Наприклад, для того, щоб веб-браузер або проксі-сервер ефективно перевірив, чи був змінений дистанційний файл, необхідно зчитати тільки його відбитки пальців і порівняти їх з раніше отриманою копією. Також, такі відбитки можуть бути використані для цілей дедуплікації даних.

В найпростішому випадку, алгоритм відбитків пальців можна розглядати як геш-функцію $h\colon \{0,1\}^* \to \{0,1\}^n$, тобто відображення бітового рядка довільної довжини в бітовий рядок n фіксованої довжини. Тобто в алгоритмі відбитку пальця у якості бітового рядка довільної довжини виступає довільний документ, в якості бітового рядка фіксованої довжини — відбиток пальця. Але таке визначення є найпростішим, наприклад цифровий відбиток пальця для текстового файлу може складатись з множини гешів речень чи абзаців цього файлу, для відео — множина гешів кожного кадру, для зображень — множина гешів кожного

каналу кольору, наприклад.

В даний час для захисту медіаконтенту від несанкціонованого використання широко застосовуються цифрові водяні знаки (ЦВЗ). У загальному випадку ЦВЗ - це деякі мітки, впроваджувані в вихідний матеріал. Вони можуть містити інформацію про час і місце виробництва контенту, а також про користувача, якому цей контент призначався. Мітки останнього типу виділяються в окремий клас і називаються ідентифікаційними номерами (ІН).

Технологія вбудовування ідентифікаційних номерів виробників має багато спільного з технологією ЦВЗ. Відмінність полягає в тому, що в першому випадку кожна захищена копія має свій унікальний вбудований номер (звідси і назва - дослівно "відбитки пальців"). Цей ідентифікаційний номер дозволяє виробникові відстежувати подальшу долю свого дітища: чи не зайнявся хтось із покупців незаконним тиражуванням. Якщо так, то "відбитки пальців" швидко вкажуть на винного [4].

У разі застосування ІН в контейнер, призначений кожному користувачеві, впроваджується персональний номер, що дозволяє контролювати подальший шлях цього контейнера. Такі системи в даній роботі називаються стегосистемами ідентифікаційних номерів. Якщо користувач виявиться медіапіратом і почне незаконне розповсюдження контенту, то ІН дозволить швидко визначити зловмисника. При цьому передбачається, що всі контейнери однакові, тобто видані копії відрізняються тільки в тих позиціях, в які впроваджені ідентифікатори. Однією з основних відмінних рис даних систем є їх потенційна вразливість до колективних атакам, або атакам змовою. При реалізації таких атак використовуються особливості стегосистем ІН, тому забезпечення захисту за допомогою класичних для ЦВЗ методик неможливо.

Розглянемо можливі застосування стеганографічних систем індентифікаційних номерів

1.2.2 Застосування

Трансляція та загальний моніторинг ЗМІ. Відбитки пальців можуть використовуватися для відстеження часу і місця, де було показано відео. Ця можливість буде корисна рекламним агентствам та їх клієнтам, які хочуть контролювати діяльність своїх медіа. Синдикатори контенту використовуватимуть його для відстеження коли і коли програмування з'явилося. Агенції з талантів використовуватимуть це для контролю за діяльністю, за яку їх клієнти повинні сплатити роялті за продуктивність. Організації, такі як AP та Reuters, будуть стежити за тим, як їхній вміст використовується в ефірних та онлайнових новинних операціях, а також в блогах.

Контроль авторських прав. Перехресні посилання на фактичні права користування та дозволи в базі даних відбитків пальців полегшать моніторинг авторизованого та несанкціонованого використання вмісту. Виробники та дистриб'ютори вмісту використовують відбитки пальців, щоб визначити, чи містить база даних несанкціонований вміст. Постачальники запасних кадрів використовуватимуть відбитки пальців, щоб визначити кліпи, які вони мають у комерційному програмуванні.

Метадані. Метадані дозволяють розробникам вмісту зберігати всі види корисної інформації про відстеження, пов'язані з вмістом. Наприклад, метадані можуть використовуватися для додавання відбитків пальців відео, зберігаючи важливу інформацію про користувачів (наприклад, хто створив вміст і хто змінив його), історію використання, в яких операційних системах відтворюється відео та за якою версією яка технологія програвача, інформація про те, в якій мережі було поширене вміст і багато іншого. Ця інформація буде безцінною під час криміналістичних розслідувань, щоб простежити піратські операції, виявити зрадників у організаціях тощо. Програма TuneUp Gracenote для

iTunes - це одна з перших програм для об'єднання метаданих з відбитками пальців. Основне використання програми - це очищення метаданих, пов'язаних із записаною музикою. Вона також буде використовуватися для отримання обкладинки обкладинок, екскурсійних графіків, відео з веб-сайту YouTube, новин про записування виконавців тощо.

Моделювання поведінкової реклами. Рекламна кампанія, основана на інтересах або поведінці, відповідає рекламі окремим особам на основі попередніх дій користувача в Інтернеті, таких як відвідування веб-сайту або пошук інформації про певний предмет. Відбиток відбитків пальців розширює цю можливість для маркетологів, які хочуть охопити споживачів на основі інтересів перегляду відео. Він також надає поведінкові моделі реклами новим доменам, таким як послуги VOD та кабельне телебачення, де сигнали повинні проходити через приставку.

Захист копіювання. Відбитки пальців відео можуть бути використані як інструмент захисту від копіювання. Наприклад, для того, щоб файл міг бути скопійований або відтворений, може знадобитися як відбиток, так і автентифікаційний підпис.

Судова експертиза. Інша обіцянка відбитків пальців у відеоматеріалах - це інформаційна судова експертиза, де можна було б використовувати відбитки пальців, щоб визначити, чи було оброблено відеоматеріали. Дослідження проводяться у цій галузі.

Додаткові можливості для бізнесу. Цифрові відбитки пальців повинні бути сумісними з великими базами даних власності, щоб бути ефективними. Зрозуміло, що підтримка, ліцензування та управління доступом до великомасштабних баз даних з відбитками пальців є потенційним можливим доходом.

Розглянемо далі, як виглядає робочий процес стеганографічних системи ідентифікаційних номерів.

1.2.3 Робочий процес

Генерування відбитків пальців та ідентифікація є невід'ємною частиною робочого середовища медіа-дистрибутора, що дає змогу ідентифікувати, відстежувати, контролювати та монетизувати їхній вміст. Це дає право видавцям використовувати технологію для запобігання порушення авторських прав, забезпечує засоби для надання законних матеріальних вигод для законних власників вмісту та позбавляє себе юридичних зобов'язань, пов'язаних із неліцензійним розповсюдженням матеріалів, захищених авторським правом.

Типовий процес цифрового відбитка пальців включає власників вмісту / студії, які реєструють свій вміст для відбитків пальців, і створюють довідкове цифрове представлення їх вмісту, яке використовується для подальших порівнянь.

Основні кроки включають в себе

1) Витяг унікальних характеристик з цифрових мультимедійних об'єктів - відбитків пальців та надання їх в спеціальний реєстр прав разом із метаданими;

2) Визначення аудіо чи відео контенту шляхом порівняння з відбитками пальців у базі даних для перевірки на порушення;

3) Вжити відповідних заходів на основі результатів порівняння за узгодженими діловими правилами (блокування, видалення, авторизація).

У наступному підрозділі розглянемо візантійську проблему її взаємозв'язок з децентралізованими алгоритмами верифікації та блокчейном.

1.3 Децентралізований алгоритм верифікації

У даному підрозділі розглядається візантійська проблема, з якої випливає її вирішення у вигляді блокчейну.

1.3.1 Візантійська проблема

Визначення 1.6. Візантійська проблема - проблема в криптології, яка полягає у взаємодії декількох віддалених абонентів, які отримують накази з одного центра. Потрібно створити єдину стратегію дій, яка буде виграшна для цих абонентів.

Суть проблеми. Є армія, яка складається з декількох частин, кожною з яких командує свій командувач. Над усіма командувачами стоїть головнокомандуючий, якому вони підпорядковуються. Перед головним боєм, головнокомандуючий надсилає кожному командувачу наказ, атакувати чи відступати. Деякі з командувачів є зрадниками, головнокомандуючий також може бути зрадником. Є три варіанта дій у подальшому розвитку ситуації:

– армія виграє, якщо всі вірні командуючі атакують;

– армія відступає, якщо всі вірні командуючі відступають;

– якщо вірні командуючі неузгоджені, армія отримає поразку.

Візантійська проблема полягає у знаходженні зрадників, для того щоб його рішення не вплинули на вірних командуючих, та для їх сумісної згоди.

Леслі Лампорт запропонував, в 1982 році, відповідний рекурсивний алгоритм, який розв'язує окремий випадок цієї проблеми. Лампорт довів, що в системі, де m елементів працює неправильно, згоди можна досягти

лише коли $2m+1$ інших елементів працює правильно (вірних командуючих більше, ніж дві третини).

Але саме блокчейн вирішив цю проблему у випадку кількість командуючих необмежена і може динамічно змінюватись.

У наступному підрозділі розглядається що таке блокчейн, його ключові властивості та переваги і недоліки та сфери використання.

1.3.2 Блокчейн

Визначення 1.7. Блокчейн - це незмінна, децентралізована, захищена та розподілена база даних, яка підтримує постійно зростаючий список хронологічних записів, які називаються блоками. Кожен блок містить мітку часу та посилання на попередній блок. Блокчейн можна розглядати як нотаріально завірену облікову книгу.

Ключові властивості.

– *Децентралізація.* В ланцюжку немає сервера. Кожен учасник - це і є сервер. Він підтримує роботу всього блокчейна;

– *Прозорість.* Інформація про транзакції, контрактах і так далі зберігається у відкритому доступі. При цьому ці дані неможливо змінити;

– *Теоретична необмеженість.* Теоретично блокчейн можна доповнювати записами до нескінченності.;

– *Надійність.* Для запису нових даних необхідний консенсус вузлів блокчейна. Це дозволяє фільтрувати операції і записувати тільки легітимні транзакції. Здійснити підміну геша нереально.

Переваги та недоліки.

Переваги:

– *Децентралізація.* Користувачі мережі рівноправні, та обмінюються даними один з одним;

– *Прозорість.* Всі блоки доступні для публічного перегляду;

– *Універсальність.* Блокчейн може використовуватись не тільки в фінансах, а також в інших сферах життя.

Недоліки:

– *Масштабованість.* Блокчейн потребує значного розміру так як кожен користувач зберігає дані всієї системи;

– *Шахрайство.* Передання даних у блокчейні незворотнє. Через це, неможливо відмінити транзакції;

– *Атака* 51%. Якщо 51% обчислювальної потужності буде належати зловмиснику, він отримає контроль над системою.

Застосування блокчейну.

Блокчейн універсальний, його можна застосовувати у багатьох сферах життя:

– *Ідентифікація особистості.* На основі технології блокчейн працюють сервіси в області ідентифікації і підтвердження прав доступу;

– *Авторські права.* В якості реєстру, в який художники, музиканти, винахідники можуть зберігати авторські права за допомогою зашифрованих ідентифікаторів;

– *Голосування.* Поки що відкритий реєстр використовується тільки в приватних голосуваннях;

– *Управління та юриспруденція.* В ідеалі може бути створена система зі звітністю представників місцевої і державної влади, зберігання даних про бюджет;

– *Музика.* Сервіси, націлені на поширення незалежної музики і просування виконавців;

– *Благодійність.* Блокчейн з його здатністю записувати і зберігати дані дуже ефективний в сфері благодійності;

– *Нерухомість.* Впровадження блокчейну в сферу нерухомості здатне її значно вдосконалити. Прискориться процес купівлі-продажу, з'явиться інструмент надійного зберігання даних про права на власність і так далі. Технологія блокчейн застосовується в сфері послуг, біржовий і

звичайної торгівлі. Потенційно вона може бути корисною всюди, де необхідна звітність, перевірки автентичності чого-небудь, зберігання даних.

У наступному підрозділі буде розглянуто задачу побудови систем доказу інтелектуальної власності в мережі Інтернет, з застосуванням технологій цифрових відбитків пальців та децентралізованого алгоритма верифікації.

1.4 Задача побудови системи доказу ІВ

У даному підрозділі розглядається задача побудови системи доказу інтелектуальної власності в мережі Інтернет, за допомогою технологій цифрових відбитків пальців та децентралізованого алгоритма верифікації.

1.4.1 Постановка задачі

Основа інтелектуальної власності - право автора, винахідника використовувати результати своєї творчої діяльності. Доступність швидкісних цифрових мереж зв'язку, можливість отримати і використовувати будь-який об'єкт в будь-якій точці світу не дозволяють автору контролювати обіг його власного інтелектуального продукту. Відповідно, з розповсюдженням мережі Інтернет, постає проблема глобального контролювання авторських прав постійно зростаючою кількості розподіленою у часі та просторі інтелектуальної власності. Традиційному інституту патентування все складніше впоратися з настільки масштабними проблемами.

Процесс доказу інтелектуальної власності слід оптимізувати з використанням сучасних технологій, для забезпечення сучаних стандартів криптографічного захисту, для зручності користувачів.

Проблема традиційних інститутів інтелектуальної власності полягає в їх незручності для користувача, незахищеності від людського фактору, у проблемі масштабованості та прозорості їх процесів. Дані проблеми гальмують розвиток інтелектуальної власності в світовому масштабі.

За допомогою об'єднання переваг сучасних технологій, такі як цифрові відбитки пальців для маркування об'єктів інтелектуальної власності та блокчейну, який вирішує проблему масштабованості та прозорості, можливо вирішити проблему доказу інтелектуальної власності в глобальному контексті динамічного світу, що постійно розвивається.

Отже, система доказу інтелектуальної власності повинна відповідати вимогам захищеності, прозорості, масштабованості, захищеності від людського фактору.

Для спрощення, дану задачу побудови системи доказу інтелектуальної власності, можна поділити на дві підзадачі. Розглянемо ці підзадачі.

1.4.2 Маркування об'єктів ІВ

Об'єктами інтелектуальної власності є твори образотворчого мистецтва, твори образотворчого мистецтва, тощо. Так як дана система доказу інтелектуальної власності працює в контексті використання мережі Інтернет, у якості об'єкту інтелектуальної власності може виступати будь-який мультимедійний цифровий об'єкт.

Постає питання, як відрізнити ці об'єкти один від одного. Відповіддю на дане питання є технологія цифрових відбитків пальців, яка

відображає відносно великий обсяг даних (такий, як, наприклад, мультимедійний цифровий об'єкт, який зазвичай виглядає як звичайний комп'ютерний файл), в набагато коротший тип бітових рядків, відбиток пальця, який однозначно ідентифікує вихідні дані для всіх практичних цілей. У контексті використання даної системи доказу інтелектуальної власності, немає сенсу зберігати весь цифровий мультимедійний об'єкт, так як технологія цифрових відбитків пальців дає потрібні властивості унікальності та ідентифікації для потреб системи. Додатковим бонусом є значно зменшені витрати на збереження цифрових відбитків пальців, так як цифрові відбитки пальців займають набагато менше місця ніж повноцінні мультимедійні цифрові об'єкти.

Розглянему другу підзадачу.

1.4.3 Доказ унікальності об'єкту ІВ

Основною метою систем доказу інтелектуальної власності є доказ унікальності об'єктів інтелектуальної власності, для подальшого вирішення долі не пройшовшого на плагіат перевірку об'єкту інтелектуальної власності, в судовому порядку.

Процедура перевірки є доволі складною, результат не обмежується лише позитивним чи негативним значенням того, що два об'єкта є ідентичними. Уявімо таку ситуацію, коли на вхід подаються два тексти, у яких переплутан лише один рядок. Виглядає як плагіат, але якщо цей рядок був ключовим в тексті і без нього все має інший сенс? Саме для цього потрібен окремий сервіс верифікації цифрових відбитків пальців, який враховує всі ці специфічні особливості кожного цифрового мультимедійного об'єкту з якого був зроблений цифровий відбиток пальця.

Відповідно для доказу унікальності об'єкту інтелектуальної власності в контексті висунутих в задачі вимог, доцільно використовувати блокчейн, через його переваги універсальності та прозорості у використанні.

Отже, для того щоб створити систему доказу інтелектуальної власності, яка діє в контексті мережі Інтернет, потрібно вирішити задачу її побудови, яка поділяється відповідно на дві її підзадачі.

Висновки до розділу 1

У даному розділі було розглянуто, що таке інтелектуальна власність взагалі, проблеми захисту інтелектуальної власності в мережі Інтернет, зокрема технічні засоби захисту та контролю авторських прав в мережі Інтернет.

Було розглянуто технології цифрових відбитків пальців, їх робочий процес та застосування у контексті захисту інтелектуальної власності в мережі Інтернет.

Була розглянута візантійська проблема, та її рішення у вигляді блокчейну, з його ключовими властивостями, перевагами та недоліками. Блокчейн може бути використаний для проблеми вирішення захисту інтелектуальнох власності в мережі Інтернет.

Була поставлена задача побудови систем доказу інтелектуальної власності, були висунуті вимоги до системи, та відповідно розглянуті дві підзадачі, які суттєво спрощують головну задачу.

Так як існуючі традиційні інститути захисту інтелектуальної власності не задовольняють вимогам сучасного світу, існує потреба у створенні такої системи інтелектуального, яка об'єднує в собі переваги технології цифрових відбитків пальців та децентралізованого алгоритму верифікації, для потреб ефективного та загального вирішення проблем

захисту інтелектуальної власності в мережі Інтернет. Така система буде розглянута у наступному розділі.

2 ОПИС СИСТЕМИ ДОКАЗУ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

В даному розділі теоретично розглядається система доказу інтелектуальної власності, складові такої системи та сценарії її використання.

2.1 Загальний огляд

Дана система надійно зберігає цифрові відбитки пальців децентралізованим чином, використовуючи InterPlanetary File System та блокчейн. Для спрощення системи, використовуються смарт-контракти на основі Ethereum. Вони дозволяють зберегти потрібну гнучкість та вартість операційних витрат на низькому рівні.

IPFS на даний момент є найкращим рішенням для побудови та використання розподіленого сховища даних, разом з технологією цифрових відбитків пальців. IPFS надає спеціальний геш, який служить як посилання на завантажений файл. Це посилання буде зберігатися у смарт-контракті Ethereum блокчейну. Відповідно для того щоб отримати останні дані, потрібне посилання буде отримано з блокчейну, та IPFS буде запитуватись для потрібного файлу.

Система складається з декількох автономних частин:

– *Клієнтський застосунок.* Будь-яке програмне забезпечення яке взаємодіє з головним сервером. Це може бути веб-сайт, мобільний застосунок або будь-які інші програмні засоби здатні контактувати з системою. Зазвичай, це веб-сайт, надалі саме такий варіант розглядається як можливість;

– *Головний сервер.* Головний сервер, який надає зручний засіб комунікації для клієнтських застосунків. Має на увазі дві головні мети: Автентифікація користувачів в системі, та зберіганнях індексованих даних про користувачів. Індексування використовується для більш зручного пошуку в базі даних та надання кращого користувацького досвіду;

– *IPFS сховище.* IPFS нода, призначена для зберігання та отримання даних;

– *Сервер обгортки блокчейну.* Спеціальний сервер, який забезпечує відповідні дії над IPFS та Блокчейном. Тобто він дозволяє отримувати, знаходити та зберігати дані в IPFS сховищі, а також дозволить використовувати операції над блокчейном;

– *Система смарт-контрактів.* Спеціальна система розумних контрактів, яка пов'язує користувача та його інтелектуальну власність. Смарт контракти виступають у якості єдиного джерела достовірної інформації про дату, та дані, які були записані;

– *Індексована база даних.* Спеціальна індексована база даних, яка зберігає метадані та атрибути файлів, з яких створюються цифрові відбитки пальців;

– *Сервіс створення цифрового відбитку пальців.* Спеціальний сервіс призначений для аналізу вхідних даних та створення з них цифрових відбитків пальців;

– *Сервіс верифікації цифрових відбитків пальців.* Спеціальний сервіс призначений для перевірки даних зі вже існуючими цифровими відбитками пальців.

Діаграма показує взаємозв'язок між різними компонентами архітектури системи.

Тоді як технологія Блокчейн у якості використання для захисту інтелектуальної власності має багато безперечних переваг, на жаль вона також має декілька недоліків. Одним з таких недоліків є невід'ємний ефект усіх розподілених застосунків – користувацький досвід для

кінцевого користувача через використання невластивих та незручних для кінцевого користувача термінів, таких як публічні чи приватні ключі, шифрування, хешування, тощо. Ця проблема вирішується використанням кінцевим користувачем єдиного паролю для отримання даних та підписування своїх дій в системі. Технічно це виглядає як генерація спеціального файла, так званого *гаманця*, який потім зашифровується відповідно обраним кінцевим користувачем паролем.

Пароль задається кінцевим користувачем лише один раз, при генерації гаманцю. Завдяки такій технології, головний сервер зберігає зашифрований гаманець, всі дії з цим гаманцем тепер доступні лише через дозвіл кінцевого користувача та його пароль. Гаманець не має ніякого сенсу без паролю, а пароль ніде не зберігається. В якості гаманця пропонується використовувати звичайний Ethereum гаманець.

Завдяки такій технології, приватний ключ гаманця не передається через мережу Інтернет. Однак постає проблема передачі паролю на головний сервер, для того, щоб користувач міг виконувати відповідні дії зі своїм гаманцем.

Далі буде розглянутий типовий сценарій передачі паролю на головний сервер кінцевим користувачем.

Розглянемо детальніше складові системи, у наступному розділі.

2.2 Складові системи

В цьому підрозділі детально роглядаються складові системи доказу інтелектуальної власності в мережі Інтернет.

2.2.1 Головний сервер

Головний сервер – центральна частина системи, яка відповідає за взаємозв'язок інших компонентів.

Головний сервер виконує відповідно три головні ролі:

– Взаємозв'язок інших компонентів системи;

– Автентифікація користувачів системи;

– Індексація збереженої інформації.

Головний сервер додатково складається з двох модулів.

Модуль реєстрації та отримання профайлу кінцевого користувача. Реєстрація в системі, бере до уваги різні типи користувачів. В залежності від їх статусу, це можуть бути приватні підприємці, наукові співробітники, комерційні інвестори, юридичні фахівці, матимуть різний доступ до різних частин системи. Профайл користувача містить ім'я, контактну інформацію, адресу та дату народження, можливо додаткові дані. Система не розкриває приватну інформацію стороннім особам.

Модуль доказу розкриття інформації. Для практичного застосування авторських прав підтвердження розкриття інформації є необхідною вимогою судів та патентних відомств. Система буде вирішувати вимогу підтвердження розкриття інформації за допомогою відкритої архітектури своєї бази даних, яка дозволить третім сторонам отримувати доступ до всіх цифрових відбитків пальців, використовуючи функції експорту, потужну веб-пошукову систему та прямий доступ через технічні інтерфейси, що використовуються патентними відомствами та університетами. Система буде додатково документувати цей доступ. Наявність мітки часу для початкової публікації та першого доступу третьої сторони буде діяти разом як найкращий доказ публікації. Інтелектуальний інформаційний бюлетень буде взаємодіяти з доказом документації модуля розкриття першого доступу, інформуючи

користувачів про нові внесення до бази даних та в кінцевому підсумку документуючи їх доступ.

2.2.2 InterPlanetary File System сховище

Для оптимального зберігання даних децентралізованим та безпечним шляхом, використовується IPFS сховище. IPFS – це протокол, який був спеціально розроблений для постійного децентралізованого зберігання та обміну даних у формі файлів.

Визначення 2.1. InterPlanetary File System (IPFS) – це контентно-адресований, одноранговий, гіпермедійний протокол, де ноди в мережі формують розподілену файлову систему.

IPFS - це проект з відкритим кодом, розроблений з 2014 р. Protocol Labs за допомогою спільноти. Система IPFS не зберігає дані в одному місці або в базі даних і, таким чином, гарантує відсутність єдиної точки відмови. Кожен файл, що зберігається в IPFS, має свою власну та унікальну адресу, що називається хеш-адресою IPFS. Цей хеш робить IPFS ідеальним для зберігання великої кількості чутливих даних поза мережею, зберігаючи хеш на ланцюжку як засіб перевірки та зв'язування даних. Цей рядок є дієвим адресом для системи для отримання даних. Так як на блокчейні зберігається лише цей рядок, витрати залишаються мінімальними.

Причина, чому система не зберігає дані в централізованій базі даних, полягає в ризику того, що така база даних стане потенційною точкою збою через хакерські атаки. Система, включаючи в себе базу даних застосунку, в принципі не містить цінних даних для зловмисника і тому робить безглуздою саму ідею атаки. Крім того, система IPFS гарантує постійну безвідмовність завдяки розподілу даних між різними

вузлами.

2.2.3 Сервер обгортки блокчейну

Причиною використання технології блокчейн є її основне позиціонування, як постійно зростаючого ланцюжку записів, так званих блоків, які зв'язані з попередніми блоками, мітка часу, дані блоку захищені криптографією. Таким чином, дані одноразово записані, вже не можуть бути змінені в подальшому, без зміни наступних блоків, що потребує значних обчислювальних ресурсів. Саме тому блокчейн можна представити у вигляді автоматичної, нотаріально завіренної бухгалтерської книги, яка ідеально підходить для подання публікацій, які використовуються в якості юридичних доказувань. Основною метою існування даного компоненту системи є взаємозв'язок між головним сервером та IPFS сховищем, задля виконання відповідних дій на ними. Тобто він дозволяє отримувати, знаходити та зберігати дані в IPFS сховищі, а також слугує відповідно основною базою для системи розумних контрактів.

2.2.4 Система смарт-контрактів

Смарт-контракт - комп'ютерний протокол, який спрощує, верифікує, або забезпечує дотримання переговорів, або виконання договору, перевіряє непотрібні пункти договору. Смарт-контракти, зазвичай, мають інтерфейс користувача або програмний інтерфейс, вони також часто слідують логіці договірних положень.

Прихильники смарт-контрактів стверджують, що таким чином багато видів договірних положень може бути здійснено частково або повністю, самостійно або вдвох. Смарт-контракти спрямовані на забезпечення безпеки, яка перевершує традиційне договірне право, а також на зменшення операційних витрат.

Саме на смарт-контрактах побудована робота даної системи доказу інтелектуальної власності. Для того щоб система функціонувала, достатньо одного смарт-контракту: смарт-контракту, який встановлює відповідність між користувчами та їх цифровими відбитками пальців відповідно.

2.2.5 Клієнтський застосунок

Система не потребує спеціально інстальованого обладнання. Достатньо лише стандартного веб-переглядача, та доступу до мережі Інтернет. Клієнтський застосунок у вигляді веб-сайту спеціально спроєктовано для позитивного користувацького досвіду.

2.2.6 Індексована база даних

Спеціальна база даних, яка зберігає в індексованому, для швидкого доступу вигляді інформацію про метадані та атрибути файлів, з яких в системі створюються цифрові відбитки пальців.

2.2.7 Сервіс створення цифрових відбитків пальців

Спеціальний сервіс, який приймаючи на вхід довільний файл, аналізує файл на вході, створюючи цього файла цифровий відбиток пальця, не займається подальшою долею цього відбитка, лише віддає відповідний цифровий відбиток пальця тому, хто цей цифровий відбиток пальця запитав на створення.

2.2.8 Сервіс верифікації цифрових відбитків пальців

Спецільний сервіс, який призначений для перевірки двух поданих на вхід цифрових відбитків пальців. Може приймати масив значень цифрових відбитків пальців для перевірки та еталон одночасно. Не займається подальшою долею результату, який вернула перевірка, лише повертає результат перевірки тому, хто викликав цей сервіс.

Чому взагалі потрібен цей сервіс як окремий? Тому що верифікація цифрових відбитків пальців, це доволі складний процес, в якому можуть бути задіяні багато параметрів, а результат верифікаціїї не є лише позитивним чи негативним булевим значенням.

Розглянемо далі сценарії використання системи, які відповідно використовують вищеописані компоненти системи.

Рисунок 2.1 – Архітектура системи доказу інтелектуальної власності

2.3 Сценарії використання системи

У даному підрозділі описуються декілька сценаріїв використання системи, на основі використання вищеописаних компонентів системи доказу інтелектуальної власності в мережі Інтернет.

Введемо деякі визначення, які будуть використані в подальшому.

Визначення 2.2. F — мультимедійний цифровий об'єкт, який користувач завантажує в систему.

Визначення 2.3. m_F — метадані та атрибути мультимедійного цифрового об'єкта, який користувач завантажує в систему.

Визначення 2.4. $DP = \phi(F)$ — цифровий відбиток пальця, як функція від мультимедійного цифрового об'єкту.

Визначення 2.5. $IA = h(DP)$ — адреса цифрового відбитку пальця в IPFS сховищі.

Визначення 2.6. U — кінцевий користувач, як елемент системи.

Визначення 2.7. pk_U — публічний ключ електронного цифрового підпису кінцевого користувача.

Визначення 2.8. sk_U — приватний ключ електронного цифрового підпису кінцевого користувача.

Визначення 2.9. w_U — гаманець кінцевого користувача.

Визначення 2.10. p_U — секретний ключ шифрування, так званий пароль гаманця кінцевого користувача.

Визначення 2.11. M — головний сервер, як елемент системи.

Визначення 2.12. pk_M — публічний ключ електронного цифрового підпису головного серверу.

Визначення 2.13. sk_M — приватний ключ електронного цифрового підпису головного серверу.

Визначення 2.14. $\Sigma = (M, K, S, Sign, Verify)$ — асиметрична система електронного цифрового підпису, де M — множина повідомлень, K — множина пар ключів, S —- множина підписів, $Sign$: $M \times K \to M \times S$ – функція підпису, $Verify$: $M \times S \times K \to \{0, 1\}$ – функція перевірки підпису.

Опишемо типові сценарії використання системи.

2.3.1 Отримання паролю кінцевого користувача

1) Кінцевий користувач U, за допомогою клієнтського застосунку, надсилає запит на публічний ключ до головного сервера;

2) Головний сервер M генерує пару ключів (pk_M, sk_M). Публічний ключ pk_S надсилається до клієнта, приватний sk_S зберігається на сервері;

3) Кінцевий користувач U шифрує свій пароль публічним ключем головного сервера $E_{pk_M}(p_U)$, та надсилає до головного сервера;

4) Головний сервер M розшифровує $E_{pk_M}(p_U)$ своїм приватним ключем sk_M, та отримує p_U.

Рисунок 2.2 – Сценарій отримання паролю кінцевого користувача

2.3.2 Реєстрація кінцевого користувача в системі

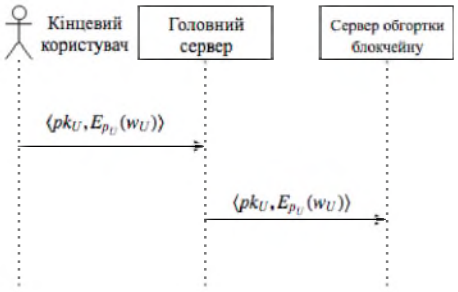

Рисунок 2.3 – Реєстрація кінцевого користувача в системі

1) Кінцевий користувач U, за допомогою клієнтського застосунку, генерує пару ключів (pk_U, sk_U). Кінцевий користувач U генерує пароль p_U, та зашифровує ним свій гаманець $E_{p_U}(w_U)$. Кінцевий користувач надсилає до головного сервера пакет даних $\langle pk_U, E_{p_U}(w_U)\rangle$;

2) Головний сервер M отримує пакет даних. Головний сервер M надсилає запит до сервера обгортки блокчейну на внесення користувача до смарт-контракту, надсилаючи йому пакет даних $\langle pk_U, w_U, E_{p_U}(w_U)\rangle$, де гаманець користувача розшифрован за допомогою процедури отриманню паролю p_U кінцевого користувача;

3) Сервер обгортки блокчейн вносить до смарт-контракту вносить

до переліку користувачів публічний ключ та зашифрований гаманець новоствореного користувача $\langle pk_U, E_{p_U}(w_U)\rangle$, та за допомогою гаманця користувача w_U списує з його балансу відповідну суму за послугу створення цього користувача.

2.3.3 Створення цифрового відбитку пальця в системі

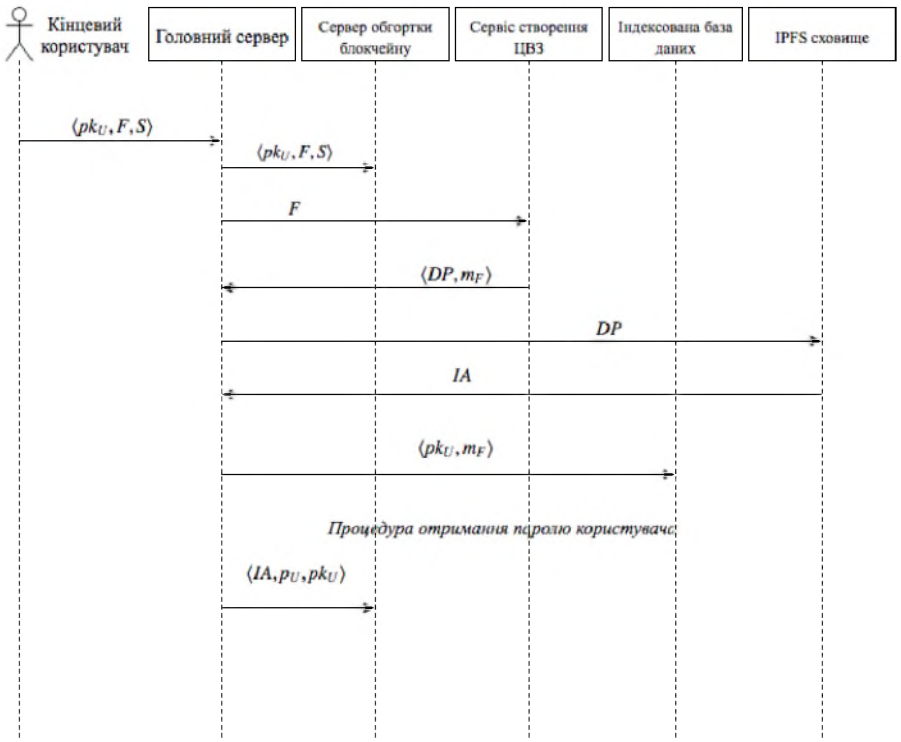

Рисунок 2.4 – Створення цифрового відбитку пальця в системі

1) Кінцевий користувач U надсилає, за допомогою клієнтського застосунку, до головного сервера M пакет даних $\langle pk_U, F, S\rangle$, де S — електронний цифровий підпис $\langle pk_U, F\rangle$;

2) Головний сервер M надсилає запит $\langle pk_U, F, S\rangle$ до сервера обгортки блокчейну;

3) Сервер обгортки блокчейну за допомогою смарт-контракту

перевіряє, чи існує такий користувач, та чи відповідно пакет даних корректно підписано існуючим користувачем та повертає результат;

4) Якщо результат некоректний, головний сервер M, повертає відповідне повідомлення на клієнтський застосунок;

5) Головний сервер M надсилає файл користувача F на створення цифрового відбитку пальців на відповідному сервісі;

6) Сервіс створення цифрових відбитків пальців повертає $\langle DP, m_F \rangle$.

7) Головний сервер M надсилає до збереження в індексовану базу даних пакет даних $\langle pk_U, m_F \rangle$;

8) Головний сервер M за допомогою вище описаної процедури отримання паролю кінцевого користувача, запитує в кінцевого користувача U його пароль p_U від гаманця w_U.

9) Головний сервер M надсилає до IPFS сховища цифровий відбиток пальця DP, звідки отримує його адресу IA

10) Головний сервер M надсилає до сервера обгортки блокчейну пакет даних $\langle IA, p_U, pk_U \rangle$;

11) Сервер обгортки блокчейну вносить до смарт-контракту адресу цифрового відбитку пальця IA відповідного користувача U, та за допомогою гаманця користувача w_U, так як серверу надіслали пароль від гаманця p_U списує з його балансу відповідну суму за послугу створення цифрового відбитку пальця для відповідного користувача.

2.3.4 Верифікація цифрового відбитку пальця в системі

У даному випадку F — файл, який кінцевий користувач бажає перевірити на унікальність. Кінцевий користувач вже має свій, завантажений в смарт-контракт, цифровий відбиток пальця DP.

1) Кінцевий користувач U надсилає, за допомогою клієнтського

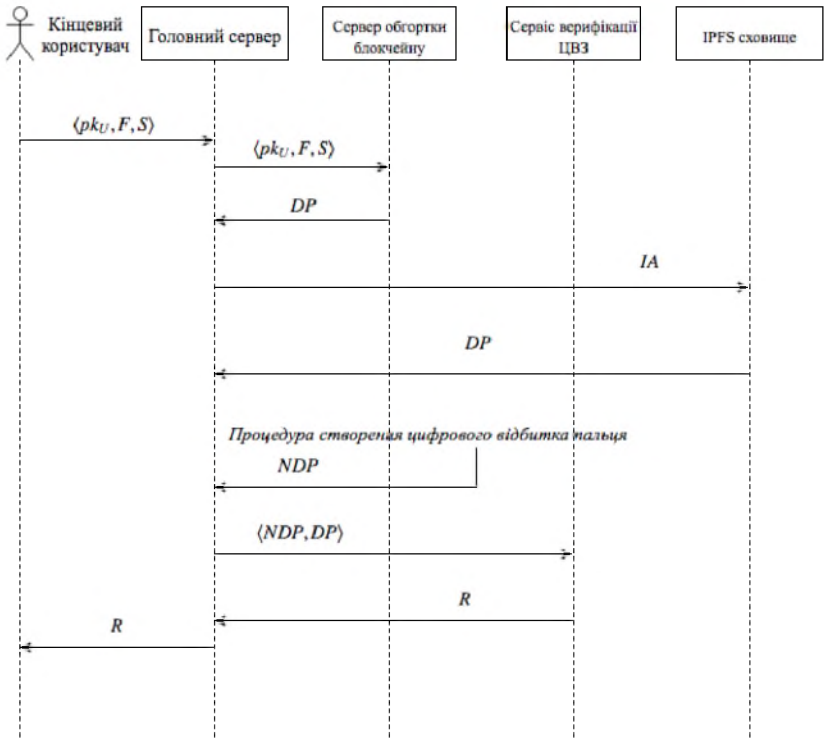

Рисунок 2.5 – Верифікація цифрового відбитку пальця в системі

застосунку, до головного сервера M пакет даних $\langle pk_U, F, S\rangle$, де S — електронний цифровий підпис $\langle pk_U, F\rangle$;

2) Головний сервер M надсилає запит $\langle pk_U, F, S\rangle$ до сервера обгортки блокчейну;

3) Сервер обгортки блокчейну за допомогою смарт-контракту перевіряє, чи існує такий користувач, та чи відповідно пакет даних корректно підписано існуючим користувачем та повертає адресу цифрового відбитка пальця IA користувача;

4) Головний сервер M надсилає до IPFS сховища адресу цифрового відбитка пальця IA, у відповідь отримує збережений цифровий відбиток пальця DP.

5) Головний сервер M створює цифровий відбиток пальця за допомогою відповідної процедури створення цифрового відбитка пальця, але в кінці така процедура не записує створений цифровий відбиток пальця NDP, а лише повертає його на сервер;

6) Головний сервер M надсилає пакет даних $\langle NDP, DP\rangle$ на перевірку до сервісу верифікації цифрових відбитків пальців;

7) Сервіс верифікації цифрових відбитків пальців повертає результат перевірки R.

8) Головний сервер M повертає результат перевірки R до клієнтського застосунку.

Висновки до розділу 2

В даному розділі було теоретично розглянуто систему доказу інтелектуальної власності засновану на технології цифрових відбитків пальців з децентралізованим алгоритмом верифікації, були розглянуті складові такої системи та можливі сценарії її використання, зокрема створення даних в системі, та верифікація даних в системі.

В результаті було представлено систему доказу інтелектуальної власності засновану на технології цифрових відбитків пальців з децентралізованим алгоритмом верифікації яка відповідає висунутим до неї вимогам у контексті задачі побудови таких систем.

Представлений варіант схеми можна модифікувати для спрощення кількості потрібних в сценаріях використання кроках, можливо також додати модулі для інших потреб, наприклад модулі експорту потрібної інформації та модулі оптимізації.

Основним недоліком даної системи є її деяка громіздкість, складність та потреба високої кваліфікації у розробці та впровадженні.

3 ПРАКТИКА СИСТЕМ ДОКАЗУ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

У цьому розділі розглядається на практиці вирішення задачі побудови системи доказу інтелектуальної власності, та порівняння запронованої у попередньому розділі системи доказу інтелектуальної власності зі вже наявними у світі системами, які оперують інтелектуальної власністю. Розглядаються міжнародні стандарти у сфері захисту інтелектуальної власності, які можливо застосувати до даної системи.

3.1 Вирішення задачі побудови системи доказу ІВ

В першому розділі була поставлена задача побудови системи доказу інтелектуальної власності. В другому розділі було наведено опис такої системи доказу інтелектуальної власності. Розглянемо як було вирішено задачу у контексті висунутих до неї вимог.

3.1.1 Вирішення задачі

Нагадаємо, що система доказу інтелектуальної власності повинна відповідати вимогам захищеності, прозорості, масштабованості, захищеності від людського фактору.

Захищеність. Система повністю криптографічно захищена, використовуються сучасні криптографічні стандарти та протоколи,

використовується сучасна технологія блокчейн, яка надає необхідний рівень захищеності.

Прозорість. Система використовує смарт-контракти та блокчейн, які повністю відкриті для доступу. Система має можливість вирішувати вимогу підтвердження розкриття інформації за допомогою відкритої архітектури своєї бази даних, яка дозволить третім сторонам отримувати доступ до всіх цифрових відбитків пальців, використовуючи функції експорту, потужну веб-пошукову систему та прямий доступ через технічні інтерфейси, що використовуються патентними відомствами та університетами. Система також додатково документує цей доступ.

Масштабованість. Масштаби використання необмежені, кожна електронно обчислювальна машина може містити клієнтський застосунок системи. Усі вони працюють незалежно один від одного. Використовуються децентралізовані розподілені системи блокчейну та IPFS сховище.

Залежність від людського фактору. Система потребує людський фактор лише при її розробці та впровадженні, що є невід'ємною складовою кожної системи. В процедурах створення та верифікації цифрового відбитку пальців задіяна лише одна людина — кінцевий користувач, що автоматично виключає можливість підробки даних верифікації.

Розглянемо далі, як були вирішені підзадачі побудови системи.

3.1.2 Маркування об'єктів ІВ

Як було вже написано у першому розділі, потрібне маркування об'єктів інтелектуальної власності. В даній системі, маркування об'єктів відбувається за допомогою технології цифрових відбитків пальців, яка

відображає відносно великий обсяг даних (такий, як, наприклад, мультимедійний цифровий об'єкт, який зазвичай виглядає як звичайний комп'ютерний файл), в набагато коротший тип бітових рядків, відбиток пальця, який однозначно ідентифікує вихідні дані для всіх практичних цілей. Цей цифровий відбиток пальця зберігається в децентралізованому файловому сховищі, для більшої надійності та зручності в зберіганні.

Розглянему другу підзадачу.

3.1.3 Доказ унікальності об'єкту ІВ

В даній системі доказ унікальності об'єкту інтелектуальної власності відбувається за допомогою децентралізованого алгоритму верифікації, який перевіряє на унікальність відповідно зареєестрований в системі об'єкт інтелектуальної власності. Для вирішення задачі складного порівняння двох цифрових відбитків пальців, був описаний окремий сервіс верифікації цифрових відбитків пальців, який враховує специфічні особливості кожного цифрового мультимедійного об'єкту з якого був зроблений цифровий відбиток пальця, та надає відповідний результат верифікації.

3.2 Аналіз конкурентів

У даній роботі було описано систему доказу інтелектуальної власності засновану на технологіях цифрових відбитків пальців та з децентралізваним алгоритмом верифікації. Саме в поєднанні таких компонентів зі специфічною метою і полягає унікальність даної системи.

Тоді як інші системи в основному базуються на захисті інтелектуальної власності, та зберігають повністю власне інтелектуальну власність, унікальність даною системи полягає у збереженні лише цифрового відбитку пальців, чого цілком достатньо для її мети підвищення стійкості забезпечення захисту об'єктів інтелектуальної власності. Використання децентралізованого алгоритма верифікації дозволяє забезпечити захист об'єктів інтелектуальної власності при відсутності посередників.

Для порівняння систем, потрібно чітко визначити критерії, за якими ці системи порівнюються.

3.2.1 Критерії порівняння

Опишемо критерії порівняння інших систем, які займаються роботою з інтелектуальною власністю.

Критерії порівняння:

– *Головний фокус.* На якому типі інтелектуальної власності фокусується захист відповідної системи

– *Мета.* Головна мета системи, те, задля чого система існує.

– *Ключова особливість.* Ключова особливість системи, те, чим система має відрізнятись від конкурентів.

– *Фокус на легальному захисті інтелектуальної власності.* Чи фокусується система на легальному захисті інтелектуальної власності, чи ні.

– *Базується на блокчейні.* Чи базується система на блокчейні, чи ні.

– *Можливість застосування для технічного розкриття інформації.* Так чи ні

– *Можливість застосування для академічних досліджень.* Так чи ні

– *Можливість застосування для зберігання комерційної таємниці.* Так чи ні

– *Можливість застосування для зображень, зокрема для фото.* Так чи ні

– *Можливість застосування для витворів мистецтва.* Так чи ні

– *Можливість застосування для текстів.* Так чи ні

– *Можливість застосування для дизайну.* Так чи ні

– *Можливість застосування для програмних файлів.* Так чи ні

– *Можливість застосування для відео.* Так чи ні

– *Можливість застосування для музики.* Так чи ні

У наступному підрозділі розглядаються схожі системи які працюють з інтелектуальною власністю, та наводиться їх відповідність критеріям порівняння.

3.2.2 Порівняння конкурентів

Наведемо далі конкурентів, та перелік їх критеріїв порівняння.

COPYTRACK

COPYTRACK призначений для того, щоб допомогти фотографам зручно вирішувати крадіжки зображень в мережі Інтернет. Він допомагає в пошуку зображень та юридичному процесі, щоб забезпечити отримання фотографами грошей, коли їх зображення використовуються в Інтернеті.

COPYTRACK дозволяє користувачам завантажувати та шукати необмежену кількість фотографій по всьому світу. Використовуючи інструменти через додаток, ви можете легко визначити суму ліцензії на зображення за свої зображення, а звідти він вирішує за вас інші проблеми.

Ключовою перевагою використання сервісу COPYTRACK є те, що

ви завжди залишаєтеся фінансово і без ризику [6].

– *Головний фокус.* Фотографії

– *Мета.* Вирішення проблеми крадіжки зображень в мережі Інтернет.

– *Ключова особливість.* Дотримання авторських прав, а не їх доведення

– *Фокус на легальному захисті інтелектуальної власності.* Ні

– *Базується на блокчейні.* Ні

– *Можливість застосування для технічного розкриття інформації.* Ні

– *Можливість застосування для академічних досліджень.* Ні

– *Можливість застосування для зберігання комерційної таємниці.* Ні

– *Можливість застосування для зображень, зокрема для фото.* Так

– *Можливість застосування для витворів мистецтва.* Так

– *Можливість застосування для текстів.* Ні

– *Можливість застосування для дизайну.* Ні

– *Можливість застосування для програмних файлів.* Ні

– *Можливість застосування для відео.* Ні

– *Можливість застосування для музики.* Ні

IP.com

IP.com була створена з метою широкого доступу до когнітивних обчислень та семантичної аналітики глибоких даних, щоб дозволити організаціям знаходити приховані явища та швидко оцінити комерційний потенціал своєї інтелектуальної власності [7].

– *Головний фокус.* Технічне розкриття інформації

– *Мета.* Реєстрування винаходів за допомогою патентного права.

– *Ключова особливість.* Спеціальні корпоративні видання продуктів

– *Фокус на легальному захисті інтелектуальної власності.* Так

– *Базується на блокчейні.* Ні

– *Можливість застосування для технічного розкриття*

інформації. Так

– *Можливість застосування для академічних досліджень.* Ні

– *Можливість застосування для зберігання комерційної таємниці.* Ні

– *Можливість застосування для зображень, зокрема для фото.* Ні

– *Можливість застосування для витворів мистецтва.* Ні

– *Можливість застосування для текстів.* Ні

– *Можливість застосування для дизайну.* Ні

– *Можливість застосування для програмних файлів.* Ні

– *Можливість застосування для відео.* Ні

– *Можливість застосування для музики.* Ні

Steemit

Steemit, нова платформа соціальних мереж, в якій кожен отримує плату за публікацію онлайн.

Steemit працює за технологією блокчейн та використовує нову криптовалюту, щоб нагороджувати користувачів, які завантажують статті, зображення, коментарі тощо.

Інші способи, за допомогою яких користувачі можуть отримувати винагородження, - це пошук популярного вмісту та популярного контенту. Чим раніше людина голосує за публікацію, яка стає популярною, тим більше вона має винагороди [8].

– *Головний фокус.* Блоги

– *Мета.* Отримання винагороди за статті в блогах

– *Ключова особливість.* Користувачі винагороджують авторів самостійно

– *Фокус на легальному захисті інтелектуальної власності.* Ні

– *Базується на блокчейні.* Так

– *Можливість застосування для технічного розкриття інформації.* Так

– *Можливість застосування для академічних досліджень.* Ні

– *Можливість застосування для зберігання комерційної таємниці.*

Ні

– *Можливість застосування для зображень, зокрема для фото.* Ні

– *Можливість застосування для витворів мистецтва.* Ні

– *Можливість застосування для текстів.* Так

– *Можливість застосування для дизайну.* Ні

– *Можливість застосування для програмних файлів.* Ні

– *Можливість застосування для відео.* Так

– *Можливість застосування для музики.* Ні

IPChain

IPChain визначає відкритий канал замкнутого циклу для цифрової асетизації різних матеріальних, нематеріальних, інноваційних продуктів, створених людським інтелектом, розробляє базовий протокол та базову структуру каналу та реалізує протокол комутації фаз із кількома сторонами [9].

– *Головний фокус.* Провайдер інфраструктури

– *Мета.* Партнерство для комерційних підприємств, які працюють з інтелектуальною власністю

– *Ключова особливість.* Новий блокчейн

– *Фокус на легальному захисті інтелектуальної власності.* Ні

– *Базується на блокчейні.* Так

– *Можливість застосування для технічного розкриття інформації.* Так

– *Можливість застосування для академічних досліджень.* Ні

– *Можливість застосування для зберігання комерційної таємниці.* Ні

– *Можливість застосування для зображень, зокрема для фото.* Ні

– *Можливість застосування для витворів мистецтва.* Ні

– *Можливість застосування для текстів.* Ні

– *Можливість застосування для дизайну.* Ні

– *Можливість застосування для програмних файлів.* Ні

– *Можливість застосування для відео.* Ні

– *Можливість застосування для музики.* Ні

Bernstein

Bernstein дозволяє компаніям створювати цифрові сліди записів про свої інноваційні процеси з використанням технології блокчейнів.

Винаходи, конструкції та докази використання можуть бути швидко зареєстровані для отримання сертифікатів блокчейнів, які підтверджують право власності, існування та цілісність будь-якого активу інтелектуальної власності.

Найголовніше, вся нотаріально завірена інформація залишатиметься абсолютно приватною завдяки унікальному криптографічному шару [10].

– *Головний фокус.* Цифровий слід записів

– *Мета.* Розміщення документів у блокчейні

– *Ключова особливість.* Отримання сертифікату на розміщений документ

– *Фокус на легальному захисті інтелектуальної власності.* Так

– *Базується на блокчейні.* Так

– *Можливість застосування для технічного розкриття інформації.* Ні

– *Можливість застосування для академічних досліджень.* Ні

– *Можливість застосування для зберігання комерційної таємниці.* Так

– *Можливість застосування для зображень, зокрема для фото.* Ні

– *Можливість застосування для витворів мистецтва.* Ні

– *Можливість застосування для текстів.* Так

– *Можливість застосування для дизайну.* Ні

– *Можливість застосування для програмних файлів.* Ні

– *Можливість застосування для відео.* Ні

– *Можливість застосування для музики.* Ні

IPStock

IPStock призначений для ілюстраторів та фотографів, які вже працюють або тільки починають працювати зі спеціальними веб-сайтам,

які продають безоплатні зображення[11].

– *Головний фокус.* Продаж зображень

– *Мета.* Управління ліцензіями на зображення

– *Ключова особливість.* Продаж зображень їх власником

– *Фокус на легальному захисті інтелектуальної власності.* Так

– *Базується на блокчейні.* Так

– *Можливість застосування для технічного розкриття інформації.* Ні

– *Можливість застосування для академічних досліджень.* Ні

– *Можливість застосування для зберігання комерційної таємниці.* Ні

– *Можливість застосування для зображень, зокрема для фото.* Так

– *Можливість застосування для витворів мистецтва.* Ні

– *Можливість застосування для текстів.* Ні

– *Можливість застосування для дизайну.* Ні

– *Можливість застосування для програмних файлів.* Ні

– *Можливість застосування для відео.* Ні

– *Можливість застосування для музики.* Ні

Були розглянуті конкуренти даної системи. У свою чергу, дана система доказу інтелектуальної власності, має такі властивості:

– *Головний фокус.* Всі типи інтелектуальної власності

– *Мета.* Доказ інтелектуальної власності

– *Ключова особливість.* Технології цифрових відбитків пальців

– *Фокус на легальному захисті інтелектуальної власності.* Так

– *Базується на блокчейні.* Так

– *Можливість застосування для технічного розкриття інформації.* Так

– *Можливість застосування для академічних досліджень.* Так

– *Можливість застосування для зберігання комерційної таємниці.* Так

– *Можливість застосування для зображень, зокрема для фото.* Так

– *Можливість застосування для витворів мистецтва.* Так

– *Можливість застосування для текстів.* Так

– *Можливість застосування для дизайну.* Так

– *Можливість застосування для програмних файлів.* Так

– *Можливість застосування для відео.* Так

– *Можливість застосування для музики.* Так

Як видно з аналізу конкурентів, в загальному випадку підтримуються не всі можливості застосування різних типів інтелектуальної власності. Надана система підтримує всі типи інтелектуальної власності.

Не всі системи базуються на блокчейні, що можна вважати за недолік, так як блокчейн забезпечує прозорість та масштабованість системи. Надана система базується на блокчейні, і відповідає висунутим до неї вимогам прозорості та масштабованості.

В цілому видно, що кожна система має свою ключову особливість та має можливість застосування лише для декількох ключових типів інтелектуальної власності. Надана система універсальна, вона вирішує більш глобальну проблему доказу інтелектуальної власності, для будь-яких типів інтелектуальної власності.

У цьому підрозділі були розглянуті конкуренти даної системи доказу інтелектуальної власності разом з їх ключовими властивостями та відмінностями. Були зроблені висновки на основі порівняння конкурентів.

Недостатньо лише розробити систему, яка оперує такими захищеними даними і нікому невідома. Такі системи потребують певний "кредит" довіри. Одним з таких варіантів та мабуть обов'язковим, є сертифікація системи міжнародними стандартами в сфері захисту інтелектуальної власності.

Далі розглядається можливість практичного застосування міжнародних стандартів в сфері захисту інтелектуальної власності до даної роботи.

3.3 Застосування міжнародних стандартів в сфері захисту ІВ

Правило 34 Договору про патентну кооперацію та пов'язаний з нею список патентної літератури встановлюють єдині високі стандарти для міжнародного пошуку через міжнародні пошукові органи. Комітет з технічного співробітництва PCT регулярно ініціює та проводить дослідження щодо складу мінімальної документації PCT та пропонує додаткові доповнення до переліку непатентованої літератури.

Тобто, потрібно, щоб дана система відповідала критеріям вибору (наприклад, доступ до рефератів, заголовків і авторів пошуків), які були використані у процесі нещодавнього відбору комітету PCT. Система повинна бути повністю оснащена такими критеріями вибору, щоб повністю відповідати мінімальному статусу документації PCT. Крім того, потрібно співвідноситися з міжнародними класифікаціями (такими як класифікація IPC), і дані, які будуть вноситися в систему, повинні відповідати стандартам, встановленим Всесвітньою організацією інтелектуальної власності (ВОІВ), якою користується більшість патентних та товарних знаків у всьому світі.

Дотримуючись вищих міжнародних стандартів, органи міжнародного пошуку, патентні експерти, патентні юристи та патентні відомства зможуть скористатися даною систему доказу інтелектуальної власності, відповідно до її мети як інструментом доказу авторського права на інтелектуальну власність в мережі Інтернет.

Щоб забезпечити патентні відомства необов'язковим використанням власних мета-інструментів пошуку, дана система має запропонувати можливість автоматичного процесу збирання та завантаження даних інтелектуальної власності через власний безпечний інтерфейс. Ці дані включають вказану метадані та атрибути завантажених в систему

об'єктів інтелектуальної власності. Для запобігання порушення авторських прав користувачі даної системи повинні погодитись надати патентним органам доступ до цієї інформації та відповідно використати ці дані, що включає надання доступу до третіх сторін.

Через безпеку платформи та формальність вимог до документів, які завантажуються в систему, які забезпечують відповідний формат високої якості, доказ авторського права на інтелектуальну власність за допомогою даної системи, а відповідно технології цифрових відбитків пальців, такий доказ буде глобально прийнятий судами як незалежне джерело доказів інтелектуального права в мережі Інтернет.

Блокчейн в даній системі буде доступний для пошуку експертами, винахідниками, дослідниками, бібліотекарями, адвокатами, науковцями, а також іншими особами особами, а також університетським персоналом, використовуючи потужний семантичний модуль пошуку та аналізу, який буде розроблено, для дотримання судових стандартів доказів та надання технічного розкриття інформації патентним бюро в усьому світі.

Висновки до розділу 3

В даному розділі було розглянуто на практиці вирішення задачі побудови системи доказу інтелектуальної власності, та порівняння запронованої у попередньому розділі системи доказу інтелектуальної власності зі вже наявними у світі системами, які оперують інтелектуальної власністю.

Надана система універсальна, вона вирішує більш глобальну проблему доказу інтелектуальної власності, для будь-яких типів інтелектуальної власності ніж її конкуренти. Надана система базується на блокчейні, і відповідає висунутим до неї вимогам прозорості та

масштабованості.

Були роглянуті міжнародні стандарти у сфері захисту інтелектуальної власності, які можливо застосувати до даної системи. Були розглянуті перспективи використання даної системи, як незалежне джерело доказів інтелектуального права в мережі Інтернет.

ВИСНОВКИ

У першому розділі було розглянуто, що таке інтелектуальна власність взагалі, проблеми захисту інтелектуальної власності в мережі Інтернет, зокрема технічні засоби захисту та контролю авторських прав в мережі Інтернет.

Було розглянуто технології цифрових відбитків пальців, їх робочий процес та застосування у контексті захисту інтелектуальної власності в мережі Інтернет.

Була розглянута візантійська проблема, та її рішення у вигляді блокчейну, з його ключовими властивостями, перевагами та недоліками. Блокчейн може бути використаний для проблеми вирішення захисту інтелектуальнох власності в мережі Інтернет.

Була поставлена задача побудови систем доказу інтелектуальної власності, були висунуті вимоги до системи, та відповідно розглянуті дві підзадачі, які суттєво спрощують головну задачу.

Так як існуючі традиційні інститути захисту інтелектуальної власності не задовольняють вимогам сучасного світу, існує потреба у створенні такої системи інтелектуального, яка об'єднує в собі переваги технології цифрових відбитків пальців та децентралізованого алгоритму верифікації, для потреб ефективного та загального вирішення проблем захисту інтелектуальної власності в мережі Інтернет.

В другому розділі було теоретично розглянуто систему доказу інтелектуальної власності засновану на технології цифрових відбитків пальців з децентралізованим алгоритмом верифікації, були розглянуті складові такої системи та можливі сценарії її використання, зокрема створення даних в системі, та верифікація даних в системі.

Представлений варіант схеми можна модифікувати для спрощення кількості потрібних в сценаріях використання кроках, можливо також додати модулі для інших потреб, наприклад модулі експорту потрібної

інформації та модулі оптимізації.

Основним недоліком даної системи є її деяка громіздкість, складність та потреба високої кваліфікації у розробці та впровадженні.

В третьому розділі було розглянуто на практиці вирішення задачі побудови системи доказу інтелектуальної власності, та порівняння запронованої у попередньому розділі системи доказу інтелектуальної власності зі вже наявними у світі системами, які оперують інтелектуальної власністю.

Надана система універсальна, вона вирішує більш глобальну проблему доказу інтелектуальної власності, для будь-яких типів інтелектуальної власності ніж її конкуренти. Надана система базується на блокчейні, і відповідає висунутим до неї вимогам прозорості та масштабованості.

Були роглянуті міжнародні стандарти у сфері захисту інтелектуальної власності, які можливо застосувати до даної системи. Були розглянуті перспективи використання даної системи, як незалежне джерело доказів інтелектуального права в мережі Інтернет.

В результаті роботи, було запропоновану систему доказу інтелектуальної власності з технологіями цифрових відбитків пальців з децентралізованим алгоритмом верифікації, придатну для подальшої побудови та використання.

Практичне значення отриманих результатів високе, на основі опису системи, можлива її побудова та практичне використання.

Масштаби використання необмежені, кожна електронно обчислювальна машина може містити клієнтський застосунок системи. Усі вони працюють незалежно один від одного.

ПЕРЕЛІК ПОСИЛАНЬ

1. Грицуленко С. И., Потапова-Синько Н. Е. Основы интеллектуальной собственности / Конспект лекций. – Одесса: ОНАС им. А.С. Попова, 2006. - 100 с.

2. Що таке авторське право? [Електронний ресурс]. — Режим доступу: http://www.uacrr.org/shho-take-avtorske-pravo/.

3. Рекомендації щодо вдосконалення механізму регулювання цифрового використання об'єктів авторського права і суміжних прав через мережу Інтернет [Електронний ресурс]. — Режим доступу: http://sips.gov.ua/ua/recomnet.html.

4. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография М.: Солон-Пресс, 2009. — 265 с. — ISBN: 5-98003-011-5

5. What is a blockchain? [Електронний ресурс]. — Режим доступу: https://blog.cdemi.io/what-is-a-blockchain/.

6. COPYTRACK [Електронний ресурс]. — Режим доступу: https://www.copytrack.com/.

7. IP.com [Електронний ресурс]. — Режим доступу: https://www.ip.com/.

8. Steemit: New Social Media Platform Which Pays You to Post [Електронний ресурс]. — Режим доступу: https://cointelegraph.com/news/steemit-new-social-media-platform-which-pays-you-to-post.

9. IPChain [Електронний ресурс]. — Режим доступу: https://www.ipcchain.org/.

10. Bernstein [Електронний ресурс]. — Режим доступу: https://www.bernstein.io/.

11. IPStock [Електронний ресурс]. — Режим доступу: https://ipstock.com/.