МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ

ФАКУЛЬТЕТ МЕХАТРОНІКИ ТА КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Математичні і алгоритмічні компоненти програмного комплексу застосування блокчейн технологій в освітній сфері»

Рівень вищої освіти другий (магістерський)

Спеціальність 122 Комп'ютерні науки

Освітня програма Комп'ютерні науки

Виконав: студент групи МгІТ-21

Поліщук Михайло Михайлович

Науковий керівник к.т.н., доц. Колиско О.З.

Рецензент

Київ 2023

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ

Факультет мехатроніки та комп'ютерних технологій
Кафедра комп'ютерних наук
Рівень вищої освіти другий (магістерський)
Спеціальність 122 Комп'ютерні науки
Освітня програма Комп'ютерні науки

ЗАТВЕРДЖУЮ
Завідувач кафедри КН
_____Володимир ЩЕРБАНЬ.
"____" _____2023 року

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Поліщуку Михайлу Михайловичу

1. Тема кваліфікаційної роботи Математичні і алгоритмічні компоненти програмного комплексу застосування блокчейн технологій в освітній сфері, науковий керівник роботи Колиско Оксана Зенонівна, доц.,к.т.н. затверджені наказом КНУТД від "_12_"вересня_2023 року №_210-уч_

2. Вихідні дані до роботи: Розробки кафедри комп'ютерних наук; рекомендована література, додатки.

3. Зміст дипломної роботи: Вступ; РОЗДІЛ 1 Постановка задачі; РОЗДІЛ 2 Проектування; РОЗДІЛ 3 Програмна реалізація; Висновки; Список літератури; ДОДАТОК А Окремі фрагменти програмного коду; ДОДАТОК Б Презентація.

4. Дата видачі завдання 1 вересня 2023

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапу кваліфікаційної роботи	Орієнтовний термін виконання	Примітка про виконання
1	Вступ	*15.09.2023*	
2	Розділ 1. Постановка задачі	*20.09.2023*	
3	Розділ 2 Проектування	*30.09.2023*	
4	Розділ 3. Програмна реалізація	*10.10.2023*	
5	Висновки	*25.10.2023*	
6	Оформлення (чистовий варіант)	*1.11.2023*	
7	Подача кваліфікаційної роботи науковому керівнику для відгуку (за 14 днів до захисту)	*4.11.2023*	
8	Подача кваліфікаційної роботи для рецензування (за 12 днів до захисту)	*6.11.2023*	
9	Перевірка кваліфікаційної роботи на наявність ознак плагіату (за 10 днів до захисту)	*8.11.2023*	
10	Подання кваліфікаційної роботи на затвердження завідувачу кафедри (з 7 днів до захисту)	*10.11.2023*	

З завданням ознайомлений:

Студент _____ Михайло ПОЛІЩУК

Науковий керівник _____ Оксана КОЛИСКО

АНОТАЦІЯ

«Математичні і алгоритмічні компоненти програмного комплексу застосування блокчейн технологій в освітній сфері»

Дипломна робота складається з вступу, 3-х розділів, висновків та пропозицій і включає: 75 с., 23 рис., 6 таблиць, 18 джерел.

Об’єкт дослідження: Технологія блокчейн.

Предмет дослідження: Впровадження технології блокчейн в освітній процес.

Мета роботи: Проаналізувати можливість переведення всього або частини функціоналу віртуального освітнього середовища на блокчейн; Знайти програмні інструменти та механізми для взаємодії з технологією та додатками блокчейн. Дипломна робота містить опис і розгляд основних алгоритмів і концепцій, включених у технологію блокчейн. В процесі впровадження були вивчені провідні інструменти для розробки та тестування додатків з використанням блокчейну.

Результатом проведеного критичного огляду та аналізу передових технологій розробки смарт-контрактів є прототип електронного кабінету студента, здатного проходити тести, отримувати бали та фіксувати результати за допомогою блокчейну

Ключові слова: блокчейн, технології, освіта, освітні технології.

ABSTRACT

"Mathematical and algorithmic components of the software complex for the application of blockchain technologies in the educational sphere"

The thesis consists of an introduction, 3 chapters, conclusions and suggestions and includes: 75 p., 23 figures, 6 tables, 18 sources.

Object of research: Blockchain technology.

Subject of research: Implementation of blockchain technology in the educational process.

Purpose of the study: Analyze the possibility of transferring all or part of the functionality of the virtual educational environment to the blockchain. Find software tools and mechanisms for interacting with blockchain technology and applications. The thesis contains a description and consideration of the basic algorithms and concepts included in blockchain technology. During the implementation process, the leading tools for developing and testing blockchain applications were studied.

The result of the research and analysis of advanced technologies for the development of smart contracts is a prototype of a student's electronic cabinet capable of taking tests, receiving points and recording results using the blockchain

Keywords: blockchain, technology, education, educational technologies

ЗМІСТ

ВСТУП

У наш час численні учні та студенти з усіх куточків земної кулі стикаються з проблемами під час здобуття освіти. Ці питання варіюються від перевірки автентичності документів про освіту, що підтверджують рівень отриманих знань, до випадків корупції під час виставлення оцінок під час навчального процесу.

Ці проблеми пов’язані, насамперед, з різною та неоднаковою кількістю документів, які вимагають різні заклади, або з відсутністю посередників при отриманні оцінок з того чи іншого предмету, і навпаки, з тривалим ланцюгом підтверджень, які потрібні при його повторній здачі.

Децентралізований і відкритий підхід до отримання доказів щодо навчального процесу та його результатів може запропонувати вирішення поставлених проблем. Цей підхід реалізований завдяки технології блокчейн, яка є однією з найбільш широко використовуваних і швидко розвиваються технологій. Блокчейн функціонує на основі цієї моделі, і це вважається надійною та стійкою технологією, оскільки інформація зберігається та перевіряється на багатьох різних комп’ютерах, і жоден окремий користувач не може самостійно контролювати всю мережу.

Технологія забезпечує конфіденційність і безпеку, а також прозорість і публічний доступ. Ці характеристики є одночасно унікальними та цінними для цифровізації освіти та освітніх процесів.

Об’єкт дослідження: Технологія блокчейн.

Предмет дослідження: Впровадження технології блокчейн в освітній процес.

Мета роботи: Проаналізувати можливість переведення всього або частини функціоналу віртуального освітнього середовища на блокчейн. Знайдіть програмні інструменти та механізми для взаємодії з технологією та додатками блокчейн. Розробити прототип електронного офісу з використанням технології блокчейн для проведення освітніх процесів та фіксації успіхів користувачів у блокчейні.

Дипломна робота містить опис і розгляд основних алгоритмів і концепцій, включених у технологію блокчейн. Проаналізовано переваги та недоліки децентралізованих додатків, а також варіанти їх використання у сфері освіти. У процесі впровадження були вивчені провідні інструменти для розробки та тестування додатків з використанням блокчейну.

Результатом дослідження та аналізу передових технологій розробки смарт-контрактів є прототип електронного кабінету студента, здатного проходити тести, отримувати бали та фіксувати результати за допомогою блокчейну.

Дипломна робота складається з вступу, 3-х розділів, висновків та пропозицій і включає: 75 с., 23 рис., 6 таблиць, 18 джерел.

РОЗДІЛ 1. ОГЛЯД ТЕХНОЛОГІЇ ТА ВИКОРИСТАННЯ ЇЇ НЕ У СФЕРІ КРИПТОВАЛЮТ

1.1. Історія поняття блокчейн та його складові

Блокчейн складається з послідовності блоків, і кожен блок, наступний за початковим, містить хеш попереднього блоку. По суті, це набір взаємопов'язаних записів, які захищені криптографічними засобами та працюють через мережу P2P. Концепція PoW (proof-of-work) є невід'ємною частиною його функціональності.

Рухаючись далі, ми досліджуватимемо, як окремі технології, що використовуються в блокчейні, походять з літературних джерел і як ці технології сприяють його створенню. Дисертація Девіда Чаума на тему «Комп'ютерні системи, створені, підтримувані та з використанням довіри взаємно підозрілих груп» у 1982 році є першим зафіксованим випадком системи, яка нагадує технологію блокчейн.

У роботі детально описано, як різні організації та системи можуть ефективно співпрацювати через систему, якій довіряють усі сторони, незважаючи на взаємну недовіру. Ця концепція дуже схожа на ідею Web of Trust, яку започаткував Філ Циммерман у 1992 році (див. рис. 1.1).

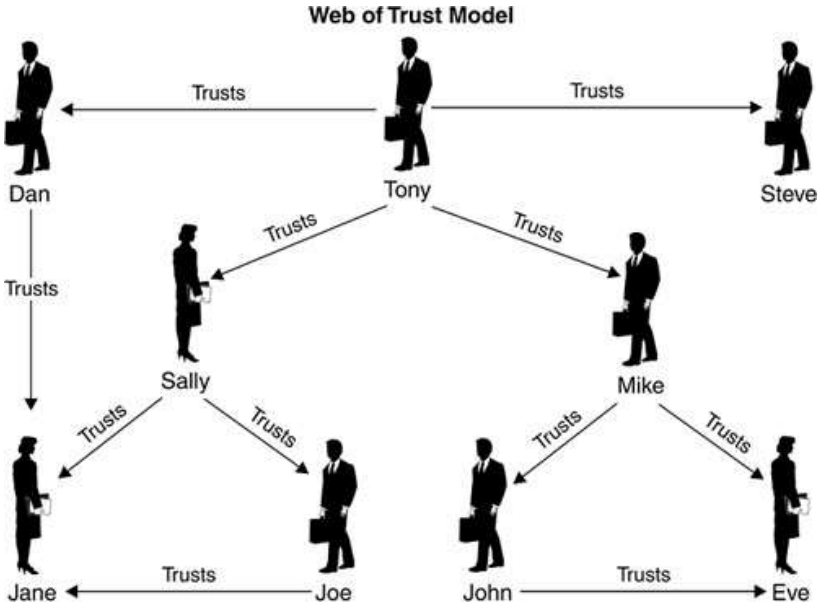

Рис. 1.1 – Зображення моделі Web of Trust

Робота Чаума також підкреслює важливість довіри до комп'ютерних систем, яким довіряють учасники цієї «мережі довіри», а не покладатися на інші організації. Це особливо актуально у світлі стрімкого технологічного прогресу, який знизив рівень довіри між сторонами. [1]

Ще в 1991 році Стюарт Хабер і Скотт Сторнетта представили опис ланцюга блоків, який був захищений за допомогою криптографії. Метою цього дослідження було вирішення питання підтвердження прав інтелектуальної власності в контексті створення та публікації електронних документів.

Головне занепокоєння викликало відсутність довіри до сторонніх систем, які вручну реєстрували ці права без будь-якого втручання комп'ютеризованих систем. Автори запропонували метод встановлення хронологічного порядку двох записів і навпаки шляхом включення бітів попередньої послідовності в сертифікат нового документа. Ця концепція була додатково вдосконалена в пізніших роботах шляхом використання хеш-дерева, також відомого як дерево Merkle, для об'єднання кількох підписаних сертифікатів в один блок.

Завдяки значному комерційному потенціалу було розроблено сервіс сертифікації на основі часових позначок, щоб перенести цю ідею від теорії до практики. На підтвердження свого успіху New York Times продовжує публікувати хеші сертифікатів документів, отримані з цієї служби.

Ральф Меркл винайшов дерево Меркла (рис. 1.2) у 1988 році з наміром покращити цифрові підписи. Стюарт Хабер і Скотт Сторнетт змогли об'єднати кілька підписаних сертифікатів в один блок, використовуючи хеш-дерево Merkle, як було зазначено раніше. Дерево Merkle — це бінарне хеш-дерево, яке слідує певному процесу. По-перше, кожен аркуш хешується окремо за допомогою хешу Leaf Tiger. Потім листя об'єднуються попарно та хешуються за допомогою внутрішнього хешу Tiger. Цей процес повторюється до тих пір, поки не залишиться лише один вузол, чий хеш буде отримано з двох попередніх хешів, які отримані з попередніх чотирьох хешів

їхніх відповідних дітей. Ця технологія дозволяє перевіряти цілісність великих обсягів даних. [1]

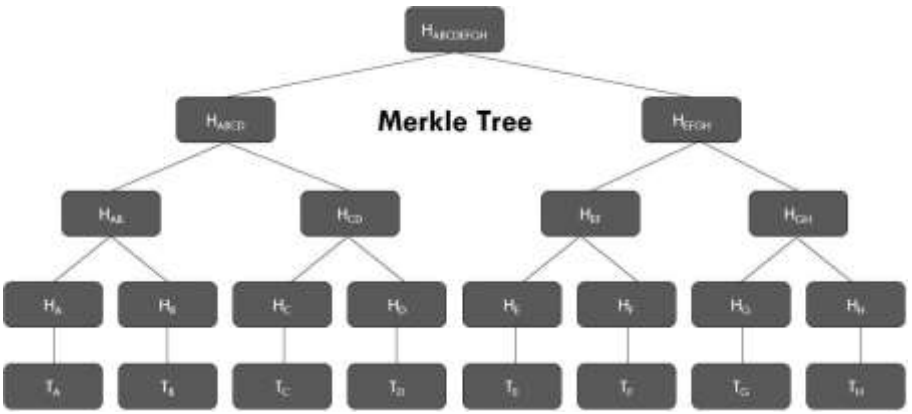

Рис. 1.2 – Зображення Дерева Меркле

На початкових етапах розвитку блокчейну численні інші підприємства також зіграли значну роль у його створенні. Одним із них є народження однорангової мережі (P2P) у цей період (як показано на малюнку 1.3).

Ця мережа дозволила побудувати децентралізовану систему, яка могла б гарантувати надійність системи та конфіденційність шляхом використання колективної обчислювальної потужності та ємності пам’яті тисяч окремих комп’ютерів.

Рис. 1.3 – Зображення моделі децентралізованої мережі

Концепція мережі P2P (однорангова мережа) спочатку була представлена в проекті IBM, який мав на меті оптимізувати мережеву архітектуру в 1984-1986 роках. Основною метою цієї архітектури було

встановлення з'єднання між вузлами без порушення центральної комп'ютерної мережі.

Розробка Advanced Peer-to-Peer Networking (APPN) сприяла децентралізованій взаємодії між великими та малими комп’ютерними вузлами як у глобальних, так і в локальних мережах. Прикладом більш ефективного та широкого використання мережі P2P є протокол зв’язку BitTorrent, який був розроблений у 2001 році. Цей протокол зменшує навантаження на сервер і мережу, завантажуючи файли з кількох вузлів послідовно замість того, щоб покладатися на один ресурс.

Архітектура одноранговової мережі (P2P) надає своїм користувачам численні переваги, такі як: Завдяки розширеній одноранговій мережі обмін файлами стає легким. Навіть на великій відстані файлами можна швидко та легко ділитися. Крім того, ці файли завжди доступні незалежно від часу.

Однією з головних переваг використання мережі P2P є економія коштів. Налаштування мережі P2P позбавляє від необхідності вкладати кошти у виділений комп’ютер-сервер. Крім того, немає вимоги до мережевої операційної системи або штатного системного адміністратора. Це може призвести до значної фінансової економії для підприємств, які хочуть запровадити мережеве рішення.

Однією з найважливіших переваг одноранговової (P2P) мережі є її адаптивність. Мережа може легко інтегрувати нових користувачів, що робить її більш гнучкою, ніж традиційні клієнт-серверні мережі. Ця масштабованість дозволяє мережам P2P рости та розвиватися відповідно до потреб користувачів, що робить їх надійним вибором для тих, хто шукає універсальну та динамічну мережу.

Надійність P2P-мереж відрізняє їх від клієнт-серверних мереж. Якщо сервер виходить з ладу в мережі клієнт-сервер, мережа виходить з ладу разом з ним. Навпаки, мережа P2P може продовжувати функціонувати, навіть якщо центральний сервер виходить з ладу, оскільки кожен комп’ютер зберігає свої робочі можливості.

Крім того, мережі P2P розподіляють трафік між кількома комп'ютерами, уникаючи вузьких місць. Рівень продуктивності в мережі «клієнт-сервер» може знизитися, коли приєднуються додаткові клієнти, але в мережі P2P продуктивність може фактично підвищитися з більшою кількістю клієнтів. Це пов'язано з тим, що кожен клієнт у мережі P2P є сервером, який може запропонувати мережеві ресурси.

Поява нових мереж P2P полегшила співпрацю та координацію між пристроями, які мають різні ресурси, що призвело до переваг усієї мережі з точки зору ефективності. На ранніх етапах розвитку блокчейна було введено поняття підтвердження роботи (PoW) як спосіб перевірки обчислювальних зусиль і захисту від кібератак. Адам Бек відіграв ключову роль у розвитку цієї концепції, створивши hashcash, алгоритм PoW, який діє як механізм захисту від відмови в обслуговуванні.

Спочатку Бек розробив hashcash у 1997 році для боротьби зі зростанням спаму електронною поштою. Ідея вимагати від користувача виконання помірно складної, але розв'язуваної функції була вперше представлена Синтією Дворк і Моні Наор у їхній статті 1992 року «Ціноутворення через обробку чи боротьбу зі спамом». За допомогою hashcash відправник електронного листа повинен обчислити та додати хеш листа до заголовка, перш ніж його можна буде надіслати, фактично вимагаючи від нього витратити певну кількість часу процесора для обчислення хешу. Цей механізм гарантує, що відправник навряд чи буде спамером, і є прикладом алгоритму PoW (Proof-of-Work) [2].

Намір алгоритмів підтвердження роботи полягає не в тому, щоб продемонструвати, що певне завдання було виконано, чи розгадати обчислювальну загадку, а радше в тому, щоб перешкоджати маніпулюванню даними, дотримуючись суворих вимог до енергії та обладнання. Екологи ретельно перевірили енергоспоживання систем підтвердження роботи.

Існує дві варіації робочого дизайну алгоритму PoW; а саме протокол «запит-відповідь» та «перевірка рішення». На малюнку 1.4 протоколи запит-

відповідь використовуються для забезпечення прямого та інтерактивного зв’язку між клієнтом (запитувачем) і сервером (провайдером). Постачальник вибирає конкретний запит, наприклад елемент у наборі, який має певний атрибут, а запитувач шукає відповідну відповідь у наборі. Знайшовши відповідь, відповідь надсилається назад постачальнику, який перевіряє її точність.

Оскільки постачальник визначає складність завдання на місці, її можна скоригувати відповідно до поточного навантаження. Якщо протокол виклик-відповідь має відоме рішення (вибране провайдером) або відомо, що існує в обмеженому просторі пошуку, робота запитувача може бути обмежена.

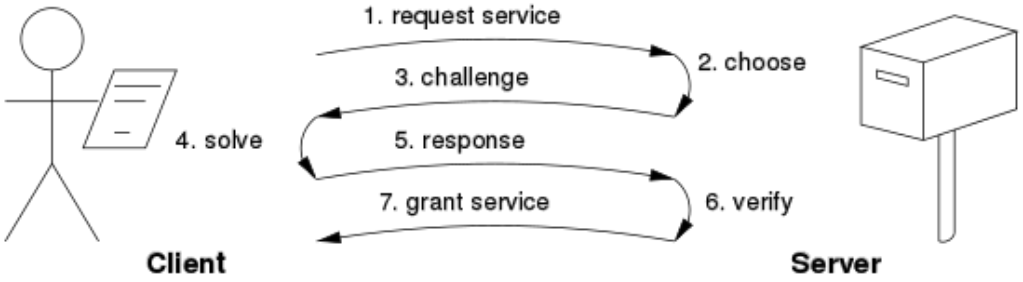

Рис. 1.4 – Зображення протоколу Запит-Відповідь у концепті PoW.

Протоколи перевірки рішень не встановлюють зв’язку між проблемою та її вирішенням. Отже, запитувач повинен самостійно визначити проблему, перш ніж шукати рішення, а постачальник повинен перевірити як вибір проблеми, так і знайдене рішення.

Дисперсія протоколів із відомим рішенням, як правило, трохи нижча, ніж у необмежених імовірнісних протоколів, оскільки прямокутний розподіл має меншу дисперсію, ніж розподіл Пуассона (з тим самим середнім). Щоб мінімізувати дисперсію, використовується кілька незалежних підзадач, оскільки середнє значення численних вибірок матиме меншу дисперсію.

Більшість із цих процедур є необмеженими, імовірнісними та ітеративними, наприклад Hashcash.

1.2. Узагальнення терміну блокчейн

Узагальнення терміну блокчейн є складною та багатогранною темою.

Він охоплює широкий спектр ідей і концепцій, пов'язаних із технологією децентралізованої розподіленої книги. Хоча немає універсального визначення блокчейну, загалом його можна розуміти як безпечний і прозорий метод зберігання та обміну даними. Ця технологія має потенціал для революції в галузях, починаючи від фінансів і закінчуючи охороною здоров'я, і її застосування все ще досліджується та розвивається.

При дослідженні літератури, що стосується технології блокчейн, один документ виділяється як важливе: «Bitcoin: однорангова електронна грошова система». Багато джерел простежують походження технології блокчейн до цієї роботи, яка була опублікована 31 жовтня 2008 року. Цього дня Сатоші Накамото (анонімний творець біткойна) поширив своє бачення платіжної системи, яка базується на мережі P2P і Концепція підтвердження роботи (PoW) для небагатьох обраних.

Згідно з офіційною документацією, базова інфраструктура блокчейну сприятиме безпечним одноранговим транзакціям, не покладаючись на посередницькі організації, такі як банки чи уряди. Фреймворк Bitcoin/Blockchain вперше був представлений у 2008 році та включає в себе концепції та технології попередніх трьох десятиліть.

План Накамото також представив нову концепцію «ланцюжка блоків», яка дозволила додавати нові блоки без необхідності отримання підписів від надійних третіх сторін. У 1998 році Вей Дай, студент Вашингтонського університету, запропонував децентралізовану платіжну систему під назвою B-Money, яка використовує криптографічні алгоритми. Дай був самопроголошеним криптоанархістом, який вважав, що насильству можна запобігти, якщо не можна ідентифікувати людей за допомогою криптографії. Він визнавав важливість взаємних послуг та фінансових інструментів у будь-якому суспільстві, але традиційні державні та банківські системи, які монополізували емісію грошей, могли обмежити доступ до цих інструментів для тих, хто не дотримувався.

Пам'ятаючи про це, Дай придумав ідею першої у світі криптовалюти.

На жаль, ніхто з ентузіастів, які поділяли його бачення, не зміг втілити його в реальність. Накамото влучно узагальнив раніше створені роботи, які не можна оскаржувати, оскільки він ідентифікував дослідження Хабера та Сторнетта щодо реалізації ланцюжків електронних підписів документів, концепцію Адама Бека щодо hashcash і PoW та проект платіжної системи B-Money Вей Дая. При цьому Сатоші визначив електронну монету як «ланцюжок цифрових підписів», у якій кожен власник передає монету наступному власнику із записом про цю передачу в попередньому блоці ланцюжка. Це досягається шляхом «цифрового підпису хешу попередньої транзакції та відкритого ключа наступного власника та додавання їх у кінець монети», як зазначено в документі.

Термін «блокчейн» відноситься до системи записів, які пов’язані між собою в блоки. Кожен блок пов’язаний з попереднім через хеш попереднього блоку. Ця система підтримується та підтримується розподіленою одноранговою мережею та записує транзакції блоками.

Поняття «доказ роботи» використовується для додавання нової інформації в блокчейн, і для цього не потрібна автентифікація або залучення третьої сторони. Натомість консенсус більшості учасників дозволяє додавати нові дані в блокчейн. Після досягнення консенсусу транзакція додається до блоку, а потім блок додається до блокчейну. Цей консенсус визначається алгоритмом підтвердження роботи учасника, і він забезпечує анонімність учасників, зберігаючи при цьому цілісність блокчейну.

У блокчейні будь-який блок, який був записаний, може бути змінений або видалений за згодою більшої групи учасників. Комп’ютерні системи, які підтримують блокчейн, регулярно перевіряють узгодженість історії транзакцій і блоків один з одним. У випадку, якщо деякі системи мають іншу послідовність блоків та інформації, ніж інші, довший ланцюжок вважається правильним[3].

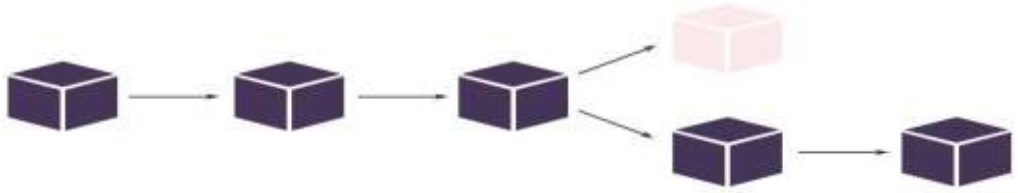

Рис. 1.5 – Зображення принципу вибору дійсного ланцюжку блокчейну

Блокчейн складається з окремих блоків, кожен з яких має власний хеш, дані блоку та хеш попереднього блоку (як показано на рис. 1.6).

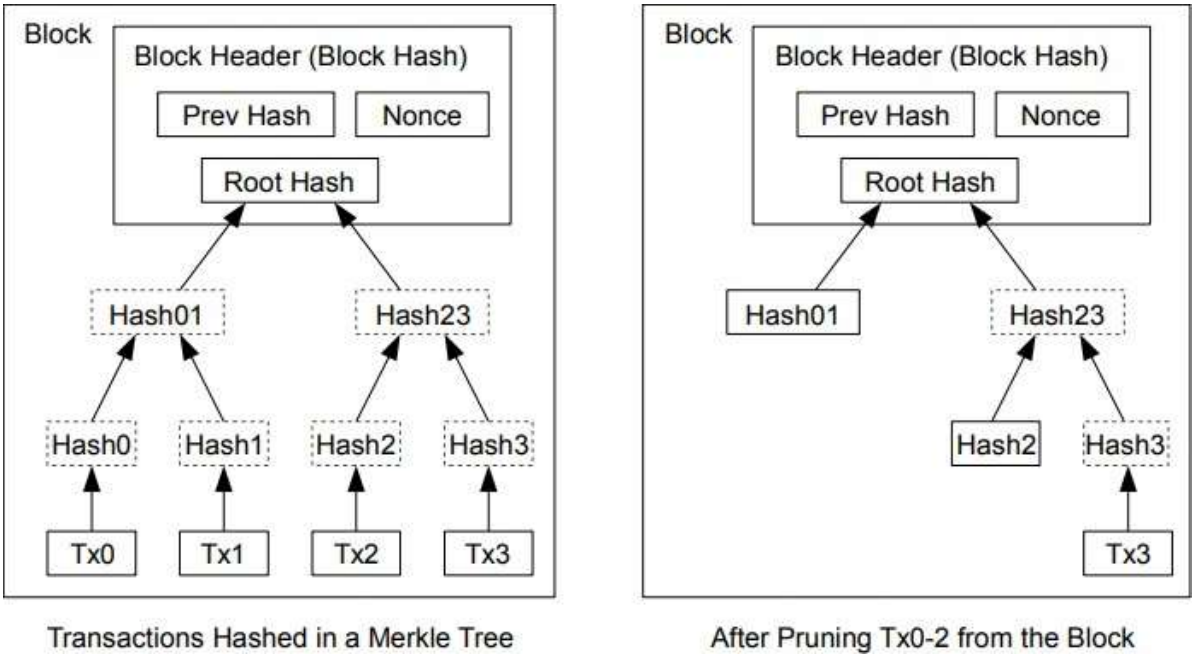

Рис. 1.6 – Зображення структури блоку у блокчейні Біткоїна.

Хеш блоку генерується за допомогою хеш-дерева Merkle, яке дозволяє зберігати кілька транзакцій в одному блоці, таким чином зберігаючи обчислювальну потужність мережі.

Під час ініціалізації блокчейна необхідно створити перший блок, відомий як блок генезису. Однак визначити, який хеш використовувати як хеш попереднього блоку, може бути складно. Рішення полягає в тому, щоб призначити попереднє хеш-поле в блоці генезису нулями

У структурі блоку є три ключові компоненти: хеш, хеш попереднього блоку (як показано на рисунку 1.7) та інформація, що міститься в блоці (як показано на рисунку 1.8). Інформація в блоці не обмежується простим

переліком транзакцій. Кожен блок унікально ідентифікується числовим значенням, відомим як висота блоку, яке представляє кількість разів, коли його хеш-значення було обчислено під час майнінгу блоку. Крім того, блок містить мітку часу, яка генерується після додавання блоку в блокчейн.

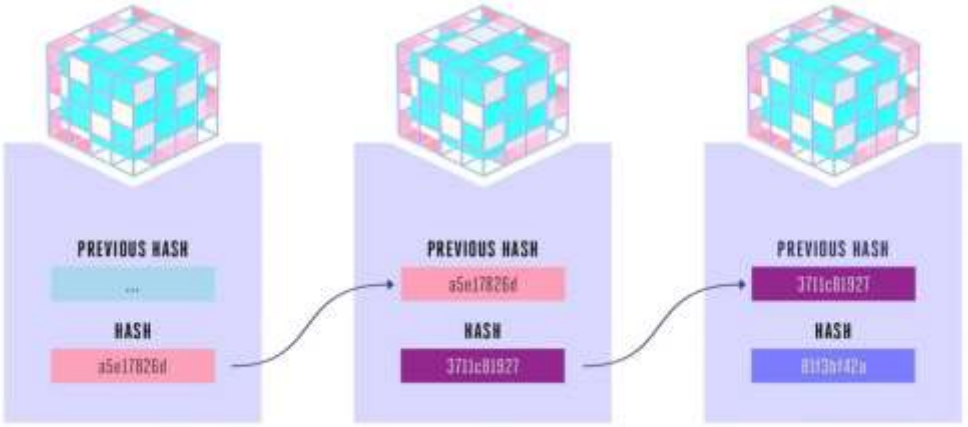

Рис. 1.7 – Принцип зв'язування блоків у блокчейні.

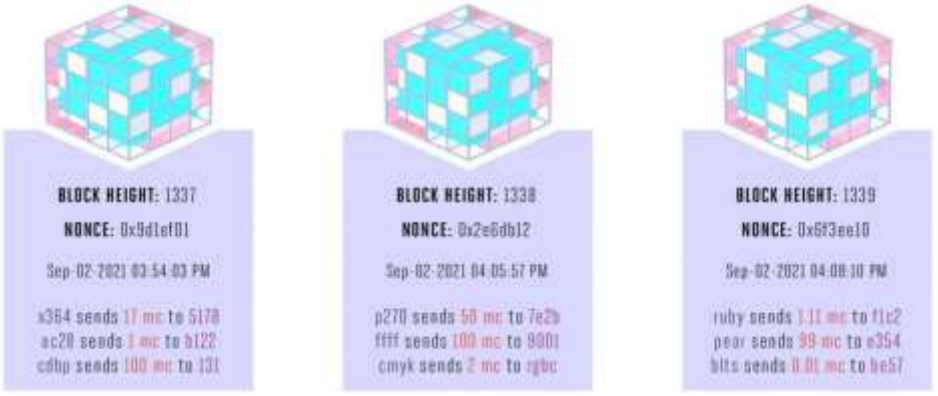

Рис. 1.8 – Інформація, що зберігається у блоках.

.

На рисунку 1.9 показано, що коли транзакція надсилається з комп'ютера, вона вимагає додавання до списку транзакцій блоку. Потім цей блок ділиться цією інформацією з учасниками мережі P2P і очікує на підтвердження доданої транзакції від них.

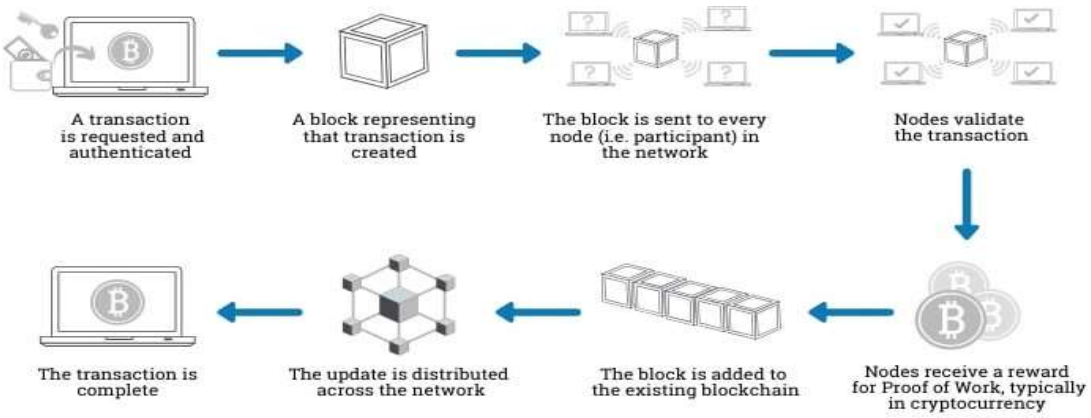

Рис. 1.9 – Життєвий цикл транзакції у блокчейні

Після успішної перевірки транзакції блок додається до блокчейну, а оновлений ланцюжок передається учасникам мережі P2P. Ці кроки зрештою завершуються успішною транзакцією. Формування нової транзакції в блоці передбачає електронний підпис, який поєднує відкритий ключ одержувача з хешем попередньої транзакції (див. рис. 1.10)[3].

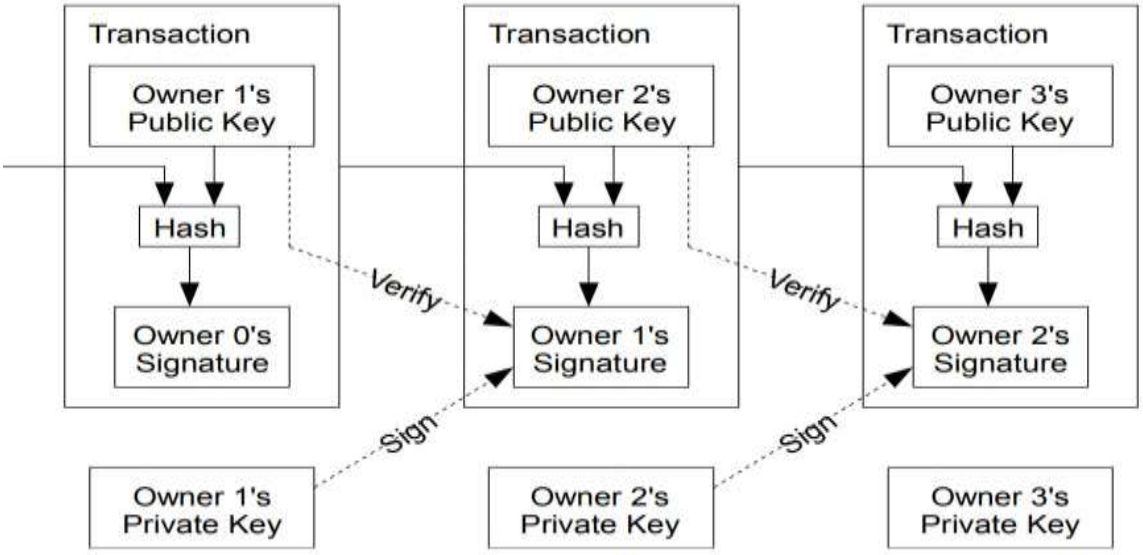

Рис. 1.10 – Принцип зв'язування транзакцій у блокчейні.

Модель транзакцій у блокчейні (як показано на рис. 1.11) за своєю суттю відрізняється від моделі транзакцій традиційної банківської системи (як показано на рис. 1.12).

Основні розбіжності між цими двома моделями полягають у тому, що в традиційній банківській системі деталі транзакцій зазвичай є конфіденційними, а за перевірку транзакцій відповідають сторонні організації. Крім того, банківська модель підтримує зв'язок між

ідентичністю відправника й одержувача та транзакцією. І навпаки, модель транзакцій блокчейну є загальнодоступною, тобто будь-хто, хто має доступ до блокчейну, може переглядати транзакції в межах певного блоку або на певну дату, але жодна конкретна особа не пов’язана з блокчейном.

Хоча деякі сервіси відстежують транзакції, що включають значні суми, і попередньо приписують їх конкретним особам або компаніям на основі повідомлень новин, ця інформація не може бути цілком достовірною, доки ці особи або компанії не розкриють фактичну адресу свого гаманця.

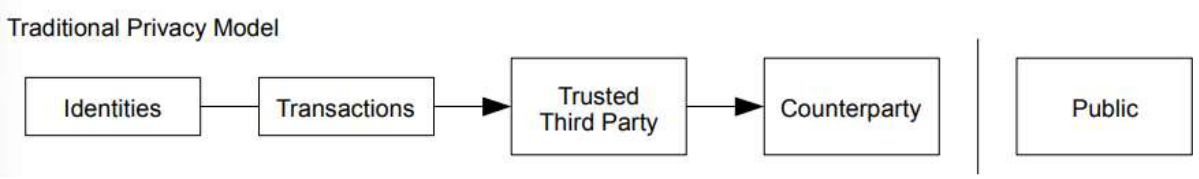

Рис. 1.11 – Традиційна модель транзакції.

Рис. 1.12 – Модель транзакції у блокчейні.

Створення блокчейну Ethereum знаменує важливу віху у світі технології блокчейну, концепція представлена в 2014 році. Мета Ethereum — створити новий протокол для розробки децентралізованих програм, пропонуючи унікальний набір переваг, які будуть задовольняють широкий спектр таких застосувань. Ці переваги включають можливість швидкого створення додатків, забезпечення безпеки для невеликих додатків і підвищення ефективності додатків, які підтримують велику кількість користувачів.

Для досягнення цих цілей Ethereum створює абстрактний базовий рівень, який служить блокчейном, із вбудованою мовою програмування, повною за Тьюрингом. Ця мова дозволяє користувачам писати розумні контракти та децентралізовані програми, де вони можуть встановлювати власні правила власності, форматів транзакцій і функцій переходу.

У мережі кожен вузол має обмежену кількість з’єднань, відомих як

«однолітки». Коли вузол бажає додати нову транзакцію до блокчейну, він розповсюджує копію транзакції кожному зі своїх однорангових вузлів, які потім поширюють її своїм одноранговим вузлам, і процес повторюється. Це призводить до того, що транзакція стає широко поширеною по всій мережі. Майнери — це спеціальні ноди, які складають список усіх цих нових транзакцій і використовують їх для створення нових блоків. Потім ці блоки надсилаються до решти мережі. Коли вузол отримує блок, він перевіряє дійсність блоку та всіх транзакцій, що містяться в ньому. Якщо блок проходить цей тест, вузол додає його до власного ланцюжка блоків і підтверджує всі транзакції.

Оскільки для створення та розповсюдження блоків не потрібна попередня авторизація, вузол може отримати кілька блоків, які претендують на те, щоб стати наступниками певного блоку.

1.3. Використання блокчейну в різних сферах

З появою Ethereum почалася нова епоха в технології блокчейн. Це було пов’язано з тим, що до Ethereum блокчейн використовувався лише як система підтримки криптовалюти. У тому ж році на блокчейні Ethereum були розроблені перші децентралізовані програми. Це стало можливим завдяки швидкому поширенню концепції смарт-контрактів і децентралізованих блокчейн-додатків, які швидко набули популярності серед великих корпорацій, таких як Microsoft, Intel, Samsung, Mastercard, Visa, JP Morgan, Cisco Systems та інших.

Децентралізовані програми (DApps) спочатку визначалися як програми з відкритим кодом, які використовують загальнодоступний децентралізований блокчейн для підтримки криптографічного запису даних, який включає історичні транзакції.

Однак із розширенням криптовалютної індустрії відбулося зростання кількості повністю та частково закритих програм DApps. Станом на 2019 рік відсоток DApps з повністю відкритим вихідним кодом становить лише 15,7%, тоді як повністю закриті DApps становлять 25% DApps.

По суті, існує менша частка DApps, які мають як код програми, так і смарт-контракти, порівняно з DApps, які не розкривають свій код. Коли справа доходить до класифікації DApps, їх можна розділити на дві окремі групи залежно від того, чи працюють вони на власному блокчейні чи на блокчейні іншого DApp.

Використовуючи цей конкретний метод класифікації, можна визначити три різні типи DApps: DApp типу I працюють на власному блокчейні. Приклади цих блокчейнів включають Bitcoin і Ethereum, які також можна віднести до категорії DApp типу I. DApps типу II — це, по суті, протоколи, які працюють на інфраструктурі блокчейну DApps типу I. Ці конкретні протоколи покладаються на токени, необхідні для виконання призначених завдань[5].

DApp типу III функціонують за допомогою протоколів DApp типу II. Як і DApps типу II, DApps типу III також потребують маркерів для ефективної роботи [5]. Нова концепція, яка виникла з появою Ethereum, — це поняття смарт-контрактів. Як зауважує автор, ці криптографічні «контейнери», які зберігають цінність і вивільняють її лише після виконання певних вимог, можуть бути створені за допомогою більш потужної платформи, ніж та, яка доступна з біткойнами.

Іншими словами, смарт-контракт аналогічний юридичній угоді, хоча умови в ній написані в сценарії, а їх виконання контролюється програмним шляхом і документується в блокчейні.

Ще в 1998 році Нік Сабо висунув ідею про те, що інфраструктуру смарт-контрактів можна створити, використовуючи повторювані облікові книги активів і виконання контрактів через криптографічні хеш-ланцюжки. Підхід до перереєстрації активів і забезпечення виконання контрактів за допомогою біткойнів відомий як «кольорові монети».

У численних проектах реалізовано відтворюване право власності на різні форми власності та тиражований контракт виконання. Розумні контракти є важливим компонентом децентралізованих програм, оскільки

вони дозволяють зберігати та керувати записами про транзакції та взаємодіяти з об’єктами всередині програми на блокчейні, а не на сервері чи базі даних.

Розробники використовують смарт-контракти як для підтримки даних у блокчейні, так і для проведення транзакцій. Більш складні операції можна виконувати шляхом створення кількох смарт-контрактів для одного DApp. Приблизно 75% DApps підтримуються одним смарт-контрактом, а решта 25% використовують кілька смарт-контрактів.

Програми блокчейну не були зосереджені лише на криптовалютах із самого початку. Augur, заснований у 2014 році, був першим децентралізованим блокчейн-додатком. Він слугував платформою прогнозування, де користувачі робили ставки на результат відомих подій, які були як категоричними, так і скалярними. Наприклад, користувачі можуть робити ставки на переможця президентських виборів, спрогнозувавши «Чи переможе кандидат А на виборах?» або "Хто зі списку переможе на виборах?" або навіть «Якою буде ціна акцій Apple 1 січня 2021 року?»

Одним із найперших і найпопулярніших додатків у блокчейні Ethereum був CryptoKitties. Розроблена у 2017 році гра дозволяла користувачам купувати, доглядати, розводити та продавати віртуальних котів. Це була перша спроба використання технології блокчейн для дозвілля та розваг. Через кілька місяців після випуску гра призвела до збою мережі Ethereum через рекордну кількість транзакцій, які вона згенерувала.

Сфера блокчейн-додатків наразі велика та різноманітна. Починаючи з травня 2017 року, їх кількість неухильно зростає, і з лютого 2018 року щодня з’являється новий блокчейн-додаток. Серед цих додатків, безсумнівно, найпопулярнішою темою є біржі криптовалют і фінансові інструменти, на які припадає 61,5% і 25,6% загальна, відповідно. На третьому та четвертому місцях із відривом йдуть додатки та ігри з передбаченнями (5% та 2,5% відповідно). Незважаючи на зростаючу

кількість блокчейн-додатків, 80% із них, створених на основі Ethereum, мають менше 1000 користувачів, що вказує на менший розподіл децентралізованих блокчейн-додатків порівняно з їх більш традиційними аналогами.

Одна проблема полягає в тому, що типовий користувач не вміє розрізняти будь-які відмінності. У той час як DApp зазвичай надають перевагу стабільності, тривалому обслуговуванню та конфіденційності над інтерфейсом користувача, ера блокчейн-додатків ще не повністю проявилася [5].

Децентралізовані додатки демонструють відмінні характеристики через їх розгортання в розподілених системах і відсутність власності з боку окремих осіб або корпорацій. Збої можуть виникнути в будь-якій системі чи процесі, і визначення конкретних точок, де ці збої можуть статися найімовірніше, має вирішальне значення для запобігання їх виникненню. Ці точки, які зазвичай називають «точками відмови», можуть відрізнятися залежно від системи або процесу.

Важливо розуміти фактори, які сприяють виникненню таких точок збою, щоб розробити ефективні стратегії їх пом’якшення. Децентралізовані програми (DApps), на відміну від традиційних програм, не мають єдиної точки вразливості. Це пов’язано з тим, що машина кожного користувача працює незалежно і не покладається на центральний сервер для керування процесами.

У випадках, коли програма централізована, потенціал відмови значно зосереджений. Якщо на централізованому сервері виникнуть труднощі, уся мережа додатків стане недоступною, доки проблему не буде вирішено. Це дає зрозуміти, що в централізованих програмах будь-які проблеми, які можуть виникнути, матимуть більш виражений вплив на систему в цілому.

Збереження безпеки даних є важливим аспектом захисту конфіденційної інформації від несанкціонованого доступу, крадіжки або пошкодження. Це передбачає низку заходів, включаючи впровадження

надійних паролів, методів шифрування та брандмауерів для захисту від кіберзагроз. Крім того, впровадження заходів фізичної безпеки, таких як використання біометричних сканерів, камер спостереження та систем контролю доступу, є обов'язковим для запобігання несанкціонованому фізичному доступу до сховищ даних. Належне навчання працівників методам обробки даних і регулярні перевірки безпеки також відіграють важливу роль у забезпеченні безпеки даних. Коли дані зберігаються на централізованому сервері, можуть виникнути проблеми з безпекою. Якщо сервер буде зламано, уся інформація користувача, включаючи особисті дані, текстові повідомлення, фотографії та відео, може бути розкрита.

Конфіденційність користувачів є основною функцією DApps. Щоб створювати або взаємодіяти з DApps, користувачі не зобов'язані розкривати свою фактичну особу. Жоден уряд не має юрисдикції над спільною базою даних, де зберігаються дані користувачів. Інформація користувача може бути розшифрована виключно самим користувачем.

Витрати: Як правило, централізовані програми несуть більші витрати. Наприклад, операційні витрати YouTube на обробку даних і маркетинг компенсуються частиною доходу, отриманого від відео, завантажених користувачами на їхній платформі.

Децентралізовані програми, або DApps, можуть бути економічно ефективнішими завдяки своїй здатності працювати без посередників, які отримують прибуток від комісій за транзакції. Це означає, що користувачі можуть брати участь у транзакціях безпосередньо з використанням криптовалюти, не потребуючи посередників.

Поняття «Правила вмісту» є фундаментальним у світі створення контенту. Загальновизнано, що створюваний контент має бути оригінальним і актуальним для аудиторії, щоб мати успіх. Створення інформативного та привабливого вмісту є ключовим для охоплення ширшої аудиторії. Крім того, важливо оптимізувати контент для пошукових систем і платформ соціальних мереж. Правильно оформлений вміст може створити авторитет

бренду та збільшити відвідуваність веб-сайту. Визначаючи, який вміст публікувати, централізовані програми дотримуються правових норм своєї країни та власних внутрішніх положень та умов. Ці умови часто визначаються довільно.

Повідомлялося, що YouTube показує рекламу відомих корпорацій у відео, які містять ворожнечу. З іншого боку, TikTok зіткнувся з звинуваченнями в тому, що трансгендерні користувачі не можуть ділитися своїм контентом. DApps, або децентралізовані програми, не мають централізованого органу, який би міг цензурувати їхній вміст. Це означає, що користувачі можуть вільно відправляти транзакції, розробляти DApps і отримувати доступ до даних з блокчейну без будь-яких обмежень. Однак це також означає, що користувачі несуть відповідальність за будь-які юридичні чи нормативні наслідки, які можуть виникнути через вміст, який вони створюють або переглядають.

Розробники стикаються зі значною проблемою, коли справа доходить до підтримки коду DApp у блокчейні. Після того, як код було розгорнуто, його не можна змінити або підробити, що ускладнює оновлення та виправлення помилок у їхніх DApps.

Процес KYC (знай свого клієнта) може бути досить важким і складним. Через те, що користувачі не зобов’язані надавати справжні облікові дані для використання або впровадження DApps, процес підтвердження ідентифікації клієнтів є складним завданням. Зараз мережі DApp можуть обробляти лише 10-15 транзакцій на секунду, і це обмеження спричинене перевантаженням мережі. У випадку, якщо один DApp споживає значну кількість обчислювальних ресурсів, уся мережа стає насиченою, а підтвердження транзакцій затримується, створюючи відставання.

Минулого року компанія PricewaterhouseCoopers (PwC), яка займається консалтингом і аудитом, провела опитування серед провідних компаній світу. Опитування мало на меті визначити, які галузі виграють найбільше від впровадження технології блокчейн. Виходячи з висновків, представлених на малюнку 1.13, більшість респондентів віддали перевагу фінансовим послугам як найбільш перспективній галузі для впровадження блокчейну. Промисловість, енергетика, охорона здоров'я та державний сектор слідували з невеликим відставанням за перевагами.

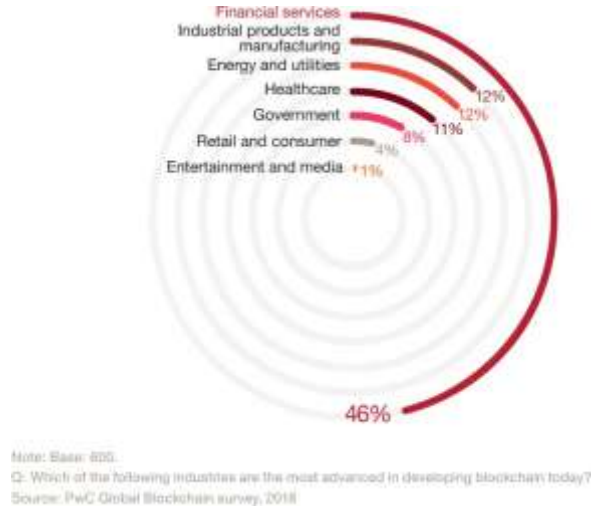

Рис. 1.13 – Результати опитування компанії PwC у 2019 році.

Використання технології блокчейн у фінансових послугах є відносно простим, в основному залучаючи біржі криптовалют і цифрові гаманці. Однак впровадження блокчейну в нефінансових секторах, які не мають зв’язку з електронною валютою, є новаторською та недавньою концепцією.

Компанії у виробничому та промисловому секторах можуть отримати значну користь від впровадження децентралізованих програм. Зараз виробники розробляють технологію блокчейну, щоб підвищити свою операційну ефективність, отримати кращу видимість у ланцюгах постачання та досягти відстеження активів із неперевершеною точністю.

Потенціал технології блокчейн поширюється на революцію в усьому процесі проектування продукту, розробки, виробництва та масштабування. Крім того, завдяки встановленню довіри між конкурентами, які працюють у спільних екосистемах, це повністю змінює спосіб взаємодії компаній.

В автомобільній промисловості керування великими та заплутаними ланцюжками поставок може бути складним завданням. Виробники транспортних засобів несуть відповідальність перед клієнтами та регуляторами за безпеку та надійність своєї продукції. На жаль, часто бракує прозорості щодо походження деталей автомобіля та їхнього шляху від шахти до виставкового залу.

Використовуючи технологію блокчейн, автомобільні дистриб'ютори можуть відстежувати кожен крок ланцюга постачання на всіх рівнях, покращуючи управління запасами та реагування на відкликання. Застосовуючи знання, отримані в результаті використання технології блокчейн у фінансовому секторі, до енергетичної галузі, стає очевидним, що вона має потенціал для створення децентралізованої системи енергопостачання. В даний час енергетична система є складною і має кілька рівнів функціонування, включаючи виробників електроенергії, операторів систем передачі та розподілу, а також постачальників. Ця система з'єднує виробників із споживачами, але її можна спростити, якщо ми змінимо спосіб керування мережами відповідно до нових вимог.

Деякі споживачі також є виробниками енергії, маючи можливість виробляти енергію за допомогою сонячних систем, невеликих вітрових генераторів або теплових електростанцій. Використовуючи блокчейн, вони могли б напряму продавати надлишкову енергію, яку вони виробляють, своїм сусідам.

Транзакції в системах блокчейн ініціюються та передаються шляхом запису таким чином, що неможливо підробити. Ці операції між особами здійснюються через пряму однорангову мережу. Коли справа доходить до блокчейн-додатків, пов'язаних з енергією, повністю децентралізована система транзакцій і постачання вважається найсучаснішим рівнем. [6]

Процеси, які здійснюють організації охорони здоров'я, є складними, вимогливими та трудомісткими, частково через численні посередники, які обробляють конфіденційні дані. Смарт-контракти, які самостійно

виконуються в блокчейні, можуть виконувати офісні завдання, такі як обробка платежів, аудит і керування контрактами, таким чином усуваючи потребу в ручному нагляді та звірці. Дані пацієнтів, які часто розкидані по кількох системах і недоступні між ними, можуть бути консолідовані та доступні уповноваженими особами на розсуд пацієнта. Крім того, технологія блокчейн може оптимізувати обробку даних клінічних випробувань ліків і платежів, зменшуючи затримки.

Для організацій охорони здоров'я, які працюють зі сторонніми постачальниками, блокчейн може полегшити відстеження розширених перевірок і перевірку відповідності, пропонуючи надійні та легкодоступні дані для всіх зацікавлених сторін. Групи лікарів або лікарні, які наймають лікаря, мають перевірити наявність кількох облікових даних, процес, який може тривати кілька місяців.

Цей процес перевірки передбачає звернення до багатьох організацій, таких як університети, ліцензійні комісії та колишні роботодавці. Ці організації також витрачають багато часу на перевірку повноважень багатьох інших лікарів. Ця затримка верифікації призводить до значної втрати прибутку як для лікаря, так і для клініки.

Оновлення реєстрів також є дорогим для постачальників медичних послуг, а разом із додатковою складністю страхування стає тягарем. Однак, якщо оновлений запис облікових даних і інформації про страхування був доступний у блокчейні, він міг би оновлюватися в режимі реального часу та мати доступ до нього кількома користувачами, у результаті чого процес завершувався б за кілька днів.

Інтеграція технології блокчейн в державний сектор має потенціал для захисту даних, спрощення процедур і мінімізації випадків обману, марнотратства та експлуатації, одночасно сприяючи довірі та відповідальності. У рамках урядової моделі, зосередженої на блокчейні, громадяни, компанії та державні установи співпрацюють і об'єднують ресурси за допомогою децентралізованої книги, яка захищена

криптографічними засобами. Ця структура усуває можливість єдиної точки відмови та захищає конфіденційну інформацію громадян і уряду. Прийняття уряду на основі блокчейну може вирішити давні проблеми та запропонувати такі переваги: Безпека державних, корпоративних і публічних даних є надзвичайно важливою. Згортання затяжних процедур. Головною метою є скорочення непомірних витрат, пов'язаних з управлінням звітністю.

Однією з ефективних стратегій боротьби з корупцією та зловживаннями є обмеження випадків, коли такі дії можуть мати місце. Зменшуючи можливості для такої негативної поведінки, людям стає набагато важче брати участь у корупції чи зловживанні владою.

Однією з головних цілей як державних, так і онлайнових цивільних систем є сприяння зростанню довіри. Ця мета досягається різними засобами, включаючи, але не обмежуючись, прозорість операцій, підзвітність за дії та встановлення надійних каналів зв'язку. Віддаючи пріоритет довірі, обидві інституції можуть покращити свою ефективність і здатність задовольняти потреби своїх виборців.

Потенційні застосування технології блокчейн в уряді різноманітні та численні, починаючи від цифрових валют і платежів до реєстрації землі, управління ідентифікацією, реєстрації бізнесу, оподаткування та навіть голосування як на виборах, так і на виборах. Крім того, цю технологію також можна використовувати в корпоративному управлінні. [6]

Висновок до Розділу 1.

У цьому розділі описано концепцію технології блокчейн. Також надається огляд літератури щодо цієї технології, яка переважно складається з офіційних документів і досліджень її розробників або тих, хто бере участь в алгоритмі її роботи. Крім того, було проведено дослідження, щоб вивчити використання технології блокчейн в секторах, не пов’язаних з криптовалютою. Результатом цього дослідження є перелік галузей з теоретичними прикладами успішного впровадження цієї технології, що призводить до зниження витрат і прискорення робочих процесів.

РОЗДІЛ 2. ПРОГРАМНА СКЛАДОВА БЛОКЧЕЙНУ

2.1 Мови програмування для розробки блокчейн-застосунків

Solidity, провідна мова блокчейн-програмування для створення смарт-контрактів і децентралізованих програм, черпає натхнення з Javascript, Powershell і C++. Віталік Бутерін, творець Ethereum, також відповідає за розробку Solidity. Ця мова пропонує численні переваги для компаній-розробників блокчейну, зокрема:

Розробники високо цінують зручність, особливо коли мова йде про інструменти та ресурси, які використовуються в їхній роботі. Мати доступ до інфраструктури, налагоджувачів та різноманітних інших інструментів, пов'язаних із JavaScript, є неймовірно цінним. Статично типізоване програмування передбачає визначення типів даних змінних та інших значень у коді перед виконанням програми. Розумні контракти мають можливість успадковувати властивості. Java є офіційною мовою розробки, на якій покладаються мобільні додатки Android, а також є найкращим вибором для розробки серверів.

Крім того, вона широко визнана як одна з найбільш широко використовуваних мов програмування для розробки додатків на блокчейні, а її популярність пояснюється її здатністю створювати складні смарт-контракти та DApps. Похідна від синтаксису C, Java може похвалитися кількома властивостями, які роблять її сприятливою мовою для розробки блокчейнів. Надійна допомога в техніках об'єктно-орієнтованого програмування.

Концепція сприяння процесу очищення пам'яті є основною темою цього обговорення. Наявність безлічі бібліотек є легкодоступними та багатими. NEM, IOTA, NEO та Hyperledger Fabric є одними з найбільш виняткових моделей блокчейн-рішень, створених за допомогою Java. Python — це мова програмування, яка домінує у сферах розробки додатків Інтернету речей, мережевих серверів і розробки додатків для блокчейну. Навіть на арені Blockchain-asa-service, Python став перевагою.

Розроблений у 1991 році Python зарекомендував себе як видатний інструмент у створенні смарт-контрактів і DApps завдяки своїм чудовим функціям. Деякі з функцій, які роблять Python популярним вибором для кодування Blockchain, включають:

Навчання програмуванню за допомогою технології блокчейн за допомогою Python є відносно простим процесом. Динамічна архітектура надає унікальну можливість доступу, яку не можна ігнорувати. Підходить для різноманітних ситуацій, будь то прості чи складніші. Допомога щодо програмного забезпечення з відкритим кодом доступна через різні канали. Python є ефективною мовою для створення прототипів у кодуванні блокчейну. JavaScript дуже універсальний і підходить для різноманітних галузей, включаючи розробку ігор і блокчейн-додатків[9].

Для останнього JavaScript є однією з найоптимальніших мов програмування, яка пропонує розробникам безліч переваг завдяки фреймворкам, таким як популярний Node.js. Ці переваги включають: Завдяки використанню JavaScript для програмування на блокчейні процес виходу на ринок стає доступнішим і може бути здійснений на більш ранньому етапі.

Використання JavaScript у блокчейн-програмуванні сприяє підвищенню масштабованості блокчейн-систем. Кілька фреймворків для Blockchain у JavaScript легко доступні для використання. Оскільки JavaScript класифікується як «мова веб-переглядача», серед іншого немає жодних ускладнень в інтеграції відповідних ресурсів.

C++, представлений у 1985 році Б’ярном Страуструпом, широко вважається оптимальною мовою програмування для розробки криптовалют[9]. Ця мова дотримується методології об’єктно-орієнтованого програмування та часто використовується для створення криптовалют, таких як Bitcoin, Litecoin, Ripple, Stellar і EOS. Серед заслуговують на увагу характеристик і можливостей C++: Ефективне управління процесорами і пам'яттю. Простота реалізації паралельних і непаралельних потоків є вирішальним фактором, який слід враховувати. Здатність передавати

значення у спосіб, який сприяє швидкому й ефективному дублюванню даних.

Реалізація поліморфізму під час компіляції може значно підвищити продуктивність. Ізоляція коду для різних структур даних є важливою практикою в програмуванні. Це передбачає відокремлення коду, який є специфічним для кожної структури даних, гарантуючи, що він функціонує незалежно та не заважає іншим структурам. Microsoft розробила нову мову, щоб замінити Java для розробки блокчейнів. Ця об'єктно-орієнтована мова програмування розроблена з безліччю інструментів для корпоративних програм, хмарних обчислень і кросплатформної розробки. Він поєднує функції фреймворків C, SQL і .NET, що робить його ідеальним для розробки блокчейнів. Стверджується, що це проект з відкритим кодом.

Вивчення синтаксису цієї мови є легким заняттям завдяки її подібності до C++ і тому факту, що вона базується на кодуванні Java, орієнтованому на блокчейн. Завдяки цьому розробники блокчейнів можуть створювати код, який можна транспортувати між різними пристроями сприятливих технологій. Використання програми BizSpark забезпечує економічну вигоду, що робить її вигідним вибором. Основним використанням цієї конкретної мови програмування є розробка DApps, смарт-контрактів та інфраструктури в контексті Blockchain.

Незважаючи на свою складність, ця мова програмування містить найкращі компоненти як JavaScript, так і Python, включаючи простоту використання, потенціал для розширення, адаптивність і швидкість. Ці характеристики роблять його оптимальним вибором для розробки унікальних рішень, необхідних для створення блокчейн-додатків. Крім того, мова легко інтегрується з OpenGL, бібліотекою відкритої графіки, що, у свою чергу, надає значні переваги розробникам у галузі блокчейну з точки зору обчислювальної потужності GPU. [9] Цей атрибут служить для того, щоб зробити його оптимальним вибором для встановлення однорангових мереж у контексті середовища блокчейн. На поточному ринку є два виняткових блокчейн-рішення, які використовують мову програмування Go: Go-Ethereum

і Hyperledger Fabric.

2.2 Програми та бібліотеки для взаємодії з блокчейном при розробці веб-застосунків

Початкова фаза проекту блокчейн передбачає вибір відповідного стека технологій. Бажано визначити передбачуване використання блокчейну: чи буде він використовуватися для публічної, приватної мережі чи мережі консорціуму. Це визначення допоможе визначити інструменти розробки та ресурси, які найкраще підходять для проекту. Після створення фундаменту наступним кроком є вибір основи для прогресу.

Найбільш часто використовуваними альтернативами є Corda, Ethereum або Hyperledger Fabric, і існує можливість розгортання програми у відповідних мережах. Технологія, відома як Blockchain, забезпечує децентралізований метод автентифікації та авторизації. Це означає, що немає необхідності використовувати сторонні системи автентифікації, такі як OAuth або OpenID Connect (OIDC). Це інноваційне рішення дає розробникам змогу розробляти користувацькі інтерфейси, не залежачи від складного серверного коду, який може не працювати належним чином, коли користувачі отримують доступ до нього з різних куточків земної кулі.

Як розширення веб-браузера Chrome, MetaMask має можливість взаємодії з DApps. Це децентралізований гаманець з відкритим кодом, який дозволяє користувачам легко обмінюватися цифровими активами. Цей інноваційний гаманець стає можливим як надсилати, так і отримувати цифрові активи. Завдяки зручному інтерфейсу та вражаючій функціональності MetaMask став найкращим вибором для розробників браузерів DApp. Цей веб-додаток DApp може похвалитися не лише базовими можливостями веб-перегляду, але й такими функціями, як керування ідентифікацією, вхід, реєстрація тощо. [10]

Коли ви спочатку запускаєте програму MetaMask, вона автоматично імпортує ваш обліковий запис Ethereum (за умови, що у вас уже є гаманець Ethereum). Ця функція особливо корисна для тих, хто хоче без будь-яких

ускладнень перенести свої цифрові активи на нові облікові записи. MetaMask дозволяє обробляти ETH та інші токени ERC-20, доступні в мережі, і взаємодіяти з вашими децентралізованими програмами. Крім того, ви можете використовувати його у веб-браузері.

Для роботи інструментів аналізу блокчейну не потрібен активний вузол Ethereum, тому підключення через мережу Ethereum є простим процесом. Є кілька важливих атрибутів MetaMask, які можна підкреслити: Встановлення та налаштування MetaMask на персональних комп'ютерах і різних пристроях є простим процесом. Просто створіть один гаманець і використовуйте початкову фразу з 12 слів, щоб імпортувати його на всі пристрої. Metamask — це суто цифровий гаманець, а не платформа для обміну криптовалютами.

Доступ до гаманця можна отримати, просто завантаживши програму, і користувачам не потрібно надавати будь-яку особисту інформацію. Встановивши MetaMask, люди можуть генерувати кілька адрес гаманців у різних блокчейнах. Це надає їм підвищений рівень конфіденційності та дає змогу легше отримувати доступ до гаманців для певних платежів.

Гаманці служать рішенням для зберігання для користувачів як токенів, так і незамінних токенів (NFT) у різних блокчейнах. Це включає, але не обмежується основним ланцюгом Ether, ланцюгом Binance BNB, Polygon, Avalanche, а також іншими тестовими мережами. MetaMask справді має власний набір недоліків, які слід враховувати. Якщо ви втратили або забули код безпеки свого гаманця, на жаль, немає іншого способу відновити його, окрім використання оригінальної фрази з 12 слів, яка була встановлена під час створення гаманця.

Служба підтримки не може надати допомогу особам, які намагаються відновити свої облікові дані для входу або вихідні фрази, оскільки MetaMask не призначений для зберігання.

Допомога з питань, пов'язаних з комп'ютером, обмежується лише питаннями, пов'язаними з програмою, і доступ до неї можна отримати лише через сайти самодопомоги, дошки оголошень спільноти та електронну пошту.

Embark — це платформа для розробки блокчейнів, розроблена для децентралізованих мереж. Він служить інструментом керування блокчейном, який дозволяє користувачам ефективно керувати своїми DApps і надає всі необхідні ресурси для створення та запуску нової версії. [10]

Використовуючи цю структуру, можна створити програму HTML5, яка використовує доступні можливості децентралізації. Крім того, він надає можливість розробляти нові смарт-контракти, які потім можна розгортати за допомогою коду JS.

Найбільш привабливою характеристикою цих інструментів управління блокчейном є їхня здатність записувати будь-які зміни, внесені в контракти. У разі модифікації коду фреймворк негайно оновить контракти та поширить програмне забезпечення децентралізованим способом. Однією з переваг використання цього програмного забезпечення є те, що воно дозволяє переміщувати смарт-контракти. Користувачі мають можливість використовувати будь-яку звичайну структуру для створення веб-додатків, включаючи, але не обмежуючись, Meteor, Angular, React та інші. Web3j — це утиліта, створена спеціально для технології блокчейн розробниками, які створили Java WebSocket API. Цей практичний інструмент дозволяє розробникам взаємодіяти з децентралізованими програмами (DApps) на основі Ethereum у блокчейні.

Крім того, він здатний підтримувати специфікацію Generic JSON RPC, яка дозволяє підключатися до віддалених або локальних вузлів Ethereum. [10] Однією з переваг використання цього програмного забезпечення є те, що воно усуває необхідність налаштування різних мов програмування або інфраструктури для зв’язку з цими транзакціями.

Крім того, це знімає зобов’язання розуміти, як працює консенсус або як майнери беруть участь у цих контрактах. Цей інструмент, який використовує технологію блокчейн, працює через JavaScript, що дозволяє йому бути сумісним з будь-яким веб-браузером. Щоб використовувати цей інструмент, потрібен вузол Ethereum, який може підключатися до мережі Ethereum через

HTTP. Крім того, використання розширення MetaMask з Web3.js для підключення до мережі Ethereum також є життєздатним варіантом. Створений за допомогою мови програмування Go, Geth є реалізацією вузла Ethereum.

Програмне забезпечення пропонує три різні інтерфейси, а саме сервер JSON-RPC, інтерфейс командного рядка та інтерактивну консоль. Geth є універсальним і може бути використаний для розробки блокчейну в будь-якій з основних операційних систем, включаючи Windows, Mac і Linux [10].

Geth має безліч додатків у блокчейні Ethereum, таких як передача токенів, майнінг токенів ether, розробка смарт-контрактів і аналіз історії блоків. Після встановлення Geth дозволяє як створити новий блокчейн, так і підключитися до існуючих. Крім того, Geth спрощує процес, автоматично підключаючись до основної мережі Ethereum.

Розробники можуть використовувати Prysm як ресурс для створення децентралізованих програм. Цей інструмент надає всеосяжний посібник зі створення початкової децентралізованої програми, включаючи класичну "Hello World!" програма. [10]. Проект Prysm — це протокол на основі Go, створений за зразком офіційного протоколу Ethereum 2.0. Цей проект включає повний вузол для маяка та діє як клієнт для валідаторів, дозволяючи йому брати участь у консенсусі для блокчейну.

Prysm використовує сучасні інструменти як для виробничого сервера, так і для міжпроцесного зв’язку. Впровадження бібліотек Google gRPC і BoltDB забезпечує ефективне, постійне зберігання ключів і сховищ ключів. Крім того, Prysm використовує бібліотеку libp2p від Protocol Labs для всіх однорангових мереж.

Remix Project — це програмна платформа, яка використовує архітектуру на основі плагінів для інструментів розробки. Сюди входять такі підкомпоненти, як Remix Plugin Engine, бібліотеки Remix і широко використовувана Remix IDE[10]. Remix IDE — це настільна та веб-програма з відкритим кодом. Він створений для забезпечення швидкого процесу

розробки та має колекцію плагінів із зручним для користувача інтерфейсом.

Розробники використовують Remix для повного процесу розробки контракту з мовою Solidity. Це також чудовий навчальний інструмент для тих, хто хоче дізнатися про Ethereum.

Фреймворк, відомий як Truffle, — це середовище розробки, спеціально розроблене для створення додатків на основі Ethereum у блокчейні Ethereum. У Truffle є велика бібліотека користувальницьких розгортань, які пропонують різні варіанти для створення нових смарт-контрактів.

Truffle Suite може похвалитися багатьма помітними функціями, про які варто згадати. Цей інструмент полегшує керування життєвим циклом смарт-контрактів. Він має можливість керувати артефактами контрактів і підтримує користувацькі розгортання, складні програми Ethereum і зв'язування бібліотек. Можна переконатися, що їхні контракти функціонують правильно, часто проводячи тестування контрактів.

Цей блокчейн-інструмент може допомогти у створенні нескладних і добре відрегульованих сценаріїв розгортання, які постійно враховують зміни смарт-контракту. Це дозволяє з легкістю виконувати міграції та розгортання за сценарієм. Якщо Truffle інтегровано у ваш проект, вам не потрібно турбуватися про будь-які проблеми чи ускладнення, пов'язані з мережею.

Truffle спритно впорається з цими питаннями, дозволяючи розробникам повністю зосередитися на розробці своїх DApps. З Truffle контрактна взаємодія ніколи не була такою простою завдяки його потужній інтерактивній консолі. Тепер ви можете отримати доступ до зручного для користувача інтерфейсу, який простий у навігації та вивченні, що дозволить вам легко взаємодіяти з вашими контрактами. Через непрактичність і високі витрати, пов'язані з впровадженням повномасштабного наскрізного блокчейн-рішення, з'явилася нова концепція:

BaaS. Модель BaaS схожа на модель SaaS тим, що дозволяє хмарним рішенням створювати, розміщувати та виконувати спеціальні програми, смарт-контракти та функції блокчейну. Постачальник хмарних послуг

відповідає за керування всіма основними завданнями та функціями, необхідними для підтримки надійної та гнучкої інфраструктури блокчейну. [10] Для тих підприємців або компаній, які не змогли впровадити технологію блокчейн через технічні труднощі або фінансові обмеження, BaaS представляє практичне рішення. Сьогодні існує багато постачальників BaaS, таких як Azure від Microsoft, AWS Amplify від Amazon і SAP.

2.3 Приклади впровадження блокчейну в освітній процес

Щоб розробити стандартизовану відкриту платформу для сертифікації на основі блокчейну, Learning Machine співпрацює з MIT Media Lab для створення Blockcerts.

Ця інновація дозволяє компаніям створювати, поширювати та підтверджувати дійсність записів, таких як академічні стенограми та облікові дані, за допомогою технології блокчейн. Створюючи незмінний запис академічних досягнень, включаючи оцінки, стенограми та дипломи, у блокчейні Blockcerts, компанії можуть легко перевіряти справжність документів і виявляти випадки фальсифікованої інформації. У прикладі понад 600 випускників 2018 року випуску Массачусетського технологічного інституту вирішили отримати цифрові копії своїх дипломів через блокчейн Blockcerts. Це означає, що навчальні досягнення цих студентів будуть постійно зареєстровані та легкодоступні для потенційних роботодавців. [8]

APPII використовує технологію блокчейн для автентифікації кваліфікації. Організація об’єднує блокчейн, смарт-контракти та машинне навчання для перевірки освітніх кваліфікацій як викладачів, так і студентів.

Щоб розпочати процес перевірки, користувачі APPII створюють особистий профіль і надають своє академічне резюме, яке містить інформацію про освіту та академічні довідки. Потім блокчейн використовується APPII для перевірки особи користувача та збереження інформації про користувача у власному блокчейні.

Співпраця між APPII та Відкритим університетом призвела до створення платформи для кваліфікацій та акредитації. Ця платформа

призначена для нагляду за прийомом нових студентів і встановлення постійного академічного запису для тих, хто отримав ступінь. Вплив цього розвитку на галузь є значним. [8]

Gilgamesh — це платформа для обміну знаннями, яка використовує розумні контракти Ethereum. Він працює подібно до сайту соціальної мережі, дозволяючи читачам, студентам і авторам збиратися та спілкуватися про книги та інші письмові твори. Однак те, що відрізняє його від інших, так це те, що користувачі мотивовані брати участь у цих обговореннях через присудження токенів GIL. Це означає, що вони заохочуються взаємодіяти з вмістом, ділячись, обговорюючи та навіть пишучи про нього. Пізніше ці токени можна використовувати для отримання інших академічних електронних книг.

Додаток Gilgamesh, який зараз доступний лише для iOS, має значний вплив на галузь. Він надає користувачам рекомендації щодо книг, стрічки соціальних мереж і навіть цифровий гаманець для зберігання токенів GIL. Потім ці токени можна використовувати для взаємодії з іншими особами, які шукають знання. [8]

ODEM служить ринком для освітніх послуг і продуктів, побудованих на децентралізованій платформі, яка використовує технологію блокчейн. Завдяки цій інновації ODEM об’єднує студентів, викладачів і професіоналів із широким спектром курсів і ресурсів. Платформа також використовує смарт-контракти, щоб полегшити угоду між студентами та викладачами щодо конкретних курсів, які покращать їхні знання та професійний досвід.

Крім того, ODEM веде реєстр, який підтверджує кожен курс, пройдений викладачами та студентами, таким чином покращуючи їхню репутацію на платформі. Крім того, токени ODEM приймаються як оплата за курси, надаючи студентам більш гнучкі варіанти оплати. Вплив ODEM на галузь очевидний у створенні «знаків навичок» як для студентів, так і для викладачів, щоб продемонструвати їхню майстерність у певних сферах.

Метою цієї ініціативи є залучення більшої кількості студентів до

курсів, які викладають професори з численними значками ODEM, а також заохочення більшої кількості професорів працювати зі студентами, які виявили бажання розширити свої навички. Все це викладено в посиланні [8].

У співпраці з IBM компанія Sony Global Education створила систему блокчейну, яка дозволяє багатьом установам вводити інформацію про студентів, наприклад про академічні досягнення та інші відповідні дані, до реєстру, який зберігає незаперечні записи про студентів, які або перевелися, або продовжили навчання. Використовуючи технологію блокчейн, навчальні заклади мають ефективний і прозорий метод відстеження цифрової транскрипції кожного студента разом із детальною книгою їхніх записів і платежів.

Технологія блокчейн від Sony викликала хвилю в галузі, видавши учасникам сертифікати про участь у Global Math Challenge 2018. Ці сертифікати функціонують як довготривалий запис результатів, який може виявитися корисним для майбутніх освітніх або професійних починань. Використовуючи технологію блокчейн, платформа Disciplina працює як централізований архів академічних досягнень і сертифікатів.

За допомогою децентралізованого алгоритму компанія автоматично виставляє оцінки особам на основі їх академічних досягнень і кваліфікації. Оцінки, присвоєні студентам, можуть бути використані університетами для розробки індивідуальних планів навчання, які спеціально адаптовані до того, чого студент навчився або чого ще має досягти.

Disciplina нещодавно запустила альфа-версію своєї системи блокчейн, призначену для використання університетами та студентами. Цей крок має на меті допомогти користувачам ближче ознайомитися з програмою. Унікальний студентський додаток компанії дозволяє студентам переглядати свою академічну освіту.

Водночас програма Educator надає доступ до профілів викладачів, методик викладання та пропозицій курсів[8], тим самим маючи значний вплив на галузь. Parchment надає низку послуг цифрової акредитації

студентам, навчальним закладам і роботодавцям. Викладачі K-12 використовують технологію блокчейн компанії для завантаження будь-яких значущих показників прогресу учнів. Водночас вищі навчальні заклади використовують платформу для підтвердження академічних досягнень, обробки заявок і видачі постійних дипломів. Крім того, студенти отримують повний доступ до своєї освітньої інформації та можуть безперешкодно ділитися своїми академічними досягненнями з потенційними роботодавцями.

Партнерство між Parchment і x2VOL мало значний вплив на галузь. Щоб забезпечити всебічне розуміння академічного та особистісного зростання студента, компанія створює постійні записи, які складаються з журналу часу та самороздумів особи щодо свого освітнього досвіду. Ця інформація може бути використана потенційними університетами та роботодавцями, щоб отримати цілісну перспективу подорожі студента.

Інтегрувавши блокчейн-реєстри та токенізацію, BitDegree створив онлайн-освітню платформу, яка фокусується на технологіях. Компанія проводить такі курси, як «Криптовалюта для чайників: Ethereum проти Bitcoin тощо», щоб допомогти людям отримати знання про технологію розподіленої книги та потенційно продовжити кар'єру в блокчейні. BitDegree також заохочує навчання, пропонуючи токенізовані стипендії як винагороду за проходження курсів і досягнення певних етапів.

На галузь значно вплинула поява онлайн-платформ, які пропонують різноманітні заняття, деякі з яких безкоштовні, а інші вимагають оплати. Ці заняття охоплюють широкий спектр тем, таких як впровадження блокчейну, криптовалюти та гейміфіковане кодування [8].

2.4 Функціонал віртуальних навчальних середовищ, що може бути перенесений на блокчейн

Функціональність віртуальних освітніх середовищ, які можна перенести на блокчейн, є темою, яка викликає великий інтерес і має потенціал. Перенесення таких середовищ на блокчейн може забезпечити

низку переваг, таких як підвищення безпеки, доступності та прозорості. Передача також може надати можливості для створення нових освітніх платформ, які використовують унікальні функції блокчейну.

Google Classroom — віртуальне навчальне середовище, яке набуло найбільшої популярності серед навчальних закладів. Ця платформа містить різні освітні програми Google, такі як Google Drive, Google Docs, Google Sheets, Google Slides, Google Forms, Google Sites і Gmail, які допомагають у переході до віртуальної безпаперової системи.

Завдяки інтеграції календаря Google планування занять і дедлайнів стало більш здійсненним. Запис на заняття можна здійснити через базу даних установи, приватний код, який можна додати до інтерфейсу користувача студента, або автоматично імпортувати з домену школи. Кожен клас створює окрему папку на Google Drive вчителя, а також папку для учнів на своєму Google Drive, куди вони можуть завантажити свою роботу для подальшого оцінювання.

У разі зміни файлів або додавання викладачем до папки курсу нових файлів у вкладці «Стрічка» з’являтиметься повідомлення про цю операцію (рис. 2.1).

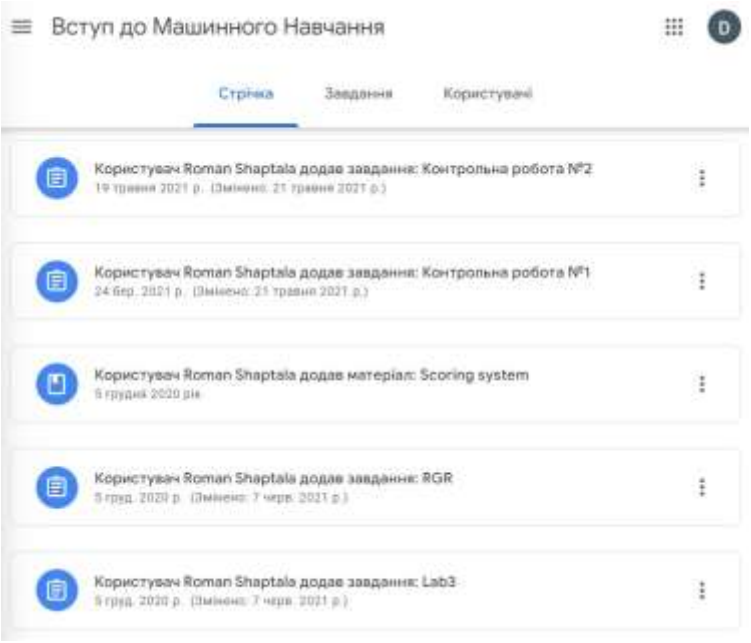

Рис. 2.1 – Вкладка «Стрічка» у Google Classroom.

Програми Google пропонують комплексне рішення для оцінювання та організації завдань, сприяючи продуктивності та зручності. Ці програми забезпечують безперебійну співпрацю між викладачами та студентами, а також між самими студентами.

Замість того, щоб викладачі ділилися документами, які зберігаються на Дисках Google їхніх студентів, файли автоматично надсилаються на оцінювання. У Google Classroom викладачі можуть створювати завдання за допомогою різних шаблонів і форматів, а також пропонувати різні параметри доступності, наприклад «студент може переглядати файл», «студент може редагувати файл» або «зробити копію для кожного студента».

Завдання можуть бути подані для відгуку та оцінювання викладачем. Студенти також можуть додавати до завдання будь-які необхідні підтверджуючі документи зі свого Диска. До призначених завдань можна легко отримати доступ і керувати ними через список «Завдання» (рис. 2.2).

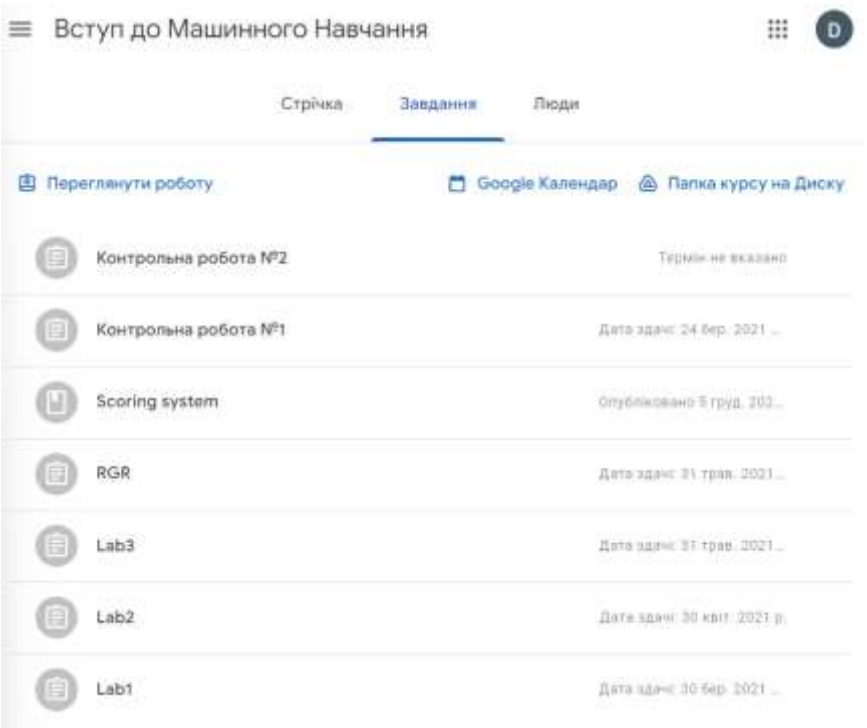

Рис. 2.2 – Вкладка «Завдання» у Google Classroom.

Google Classroom підтримує безліч систем оцінювання, доступних викладачам. Викладачі можуть завантажувати файли та вибирати засоби, за допомогою яких студенти матимуть доступ до цих матеріалів.

У міру виконання завдання студенти створюють власні файли, додають їх до завдання або надсилають викладачеві для перегляду, якщо вони зробили копію вихідного файлу. Тим часом вчитель стежить за прогресом кожного учня, пропонуючи коментарі або редагуючи роботу.

Викладачі можуть залишати відгуки про ціле завдання або окремі частини документа на Google Drive, що дозволяє студенту отримувати найбільш зрозумілі коментарі щодо своєї роботи.

Коли студент надсилає завдання, документ може редагувати лише викладач, якщо він ще не повернув завдання (як показано на рис. 2.3).

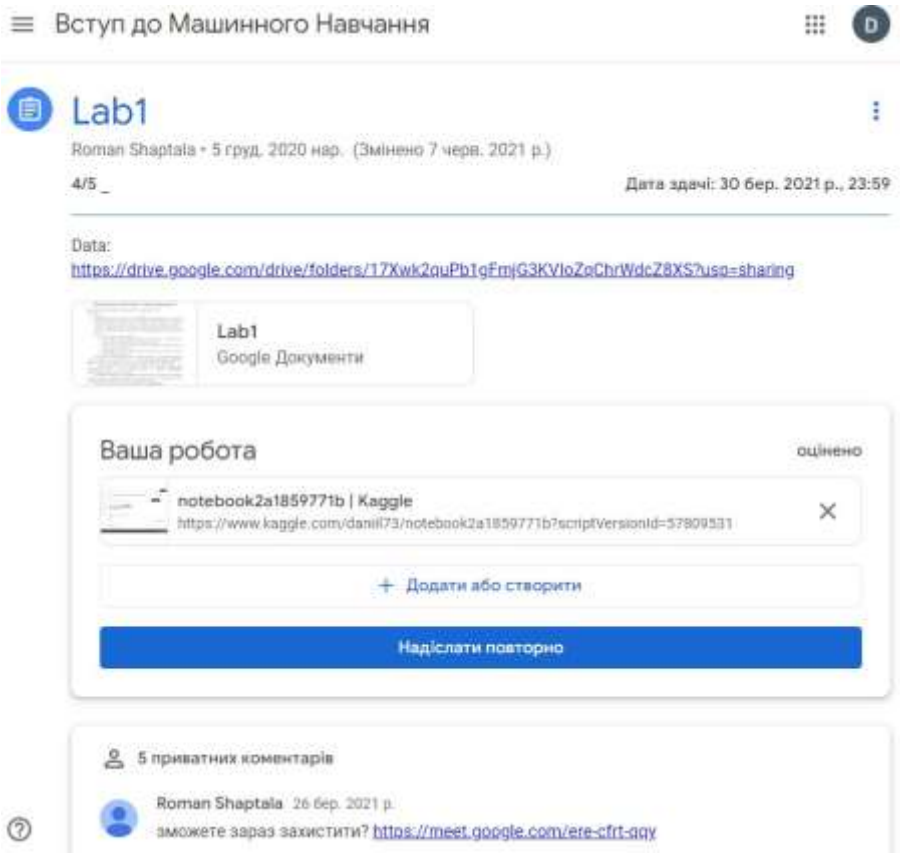

Рис. 2.3 – Вигляд окремого завдання у Google Classroom.

У Google Class (рис. 2.4) інструктори мають можливість публікувати коментарі та оновлення без необхідності надсилати електронні листи всім учням. Крім того, відео YouTube і файли Google Drive можуть бути додані до цих оголошень і записів для повного обміну інформацією.

Gmail також пропонує альтернативні варіанти електронної пошти, які дозволяють викладачам надсилати електронні повідомлення одному чи кільком учням в інтерфейсі Google Classroom.

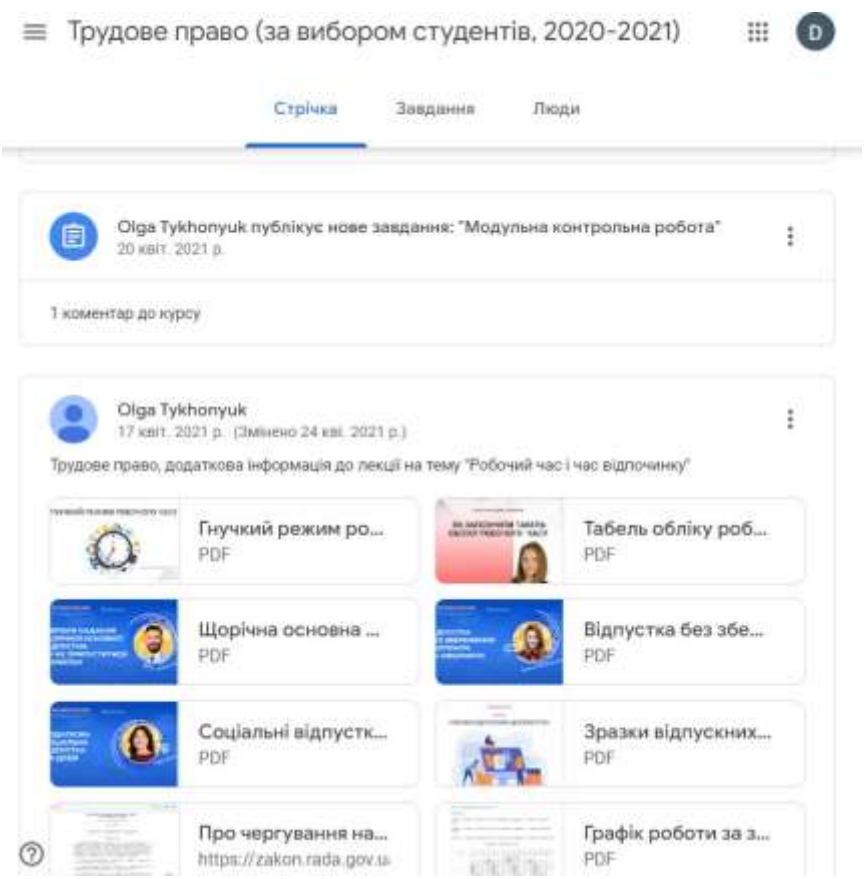

Рис. 2.4 – Коментарі від викладача у Google Classroom.

У січні 2020 року було подано звіт про оригінальність. Цей звіт корисний як для викладачів, так і для студентів, оскільки він дозволяє їм переглядати конкретні частини та сегменти роботи, які містять фрази, ідентичні або подібні до інших джерел. Для студентів це привертає увагу до вихідного матеріалу та позначає випадки, коли цитати відсутні, тим самим допомагаючи покращити їх написання.

Викладачі також мають доступ до звіту про оригінальність, який дає їм можливість перевірити академічну доброчесність студента в поданій роботі.

2.5 Шляхи удосконалення функціональної складової віртуальних навчальних середовищ за допомогою блокчейну

Технологія блокчейн використовується для зберігання даних у базі даних, яка розподілена між кількома вузлами. Дані впорядковані в хронологічному порядку за допомогою часових позначок і не можуть бути видалені після додавання блоку. Це пояснюється тим, що для запобігання

шахрайській діяльності використовується криптографічний алгоритм, що значно ускладнює підробку даних.

Незважаючи на зростання кількості децентралізованих освітніх онлайн-платформ, якість пропонованих курсів часто є непостійною. Крім того, відсутність уніфікованої системи сертифікації означає, що результати навчання не є загальновизнаними, що призводить до незадовільних результатів. Для вирішення цих проблем ефективним рішенням може бути запис навчальних даних у блокчейні в хронологічному порядку.

Використовуючи блокчейн, навчальні дані студентів, такі як час навчання, файли курсів і результати тестів, можна записувати в хронологічному порядку з міткою часу для точності. За допомогою методу криптографічного запису цілісність даних захищена від підробки або видалення.

Децентралізація та колективне обслуговування блокчейну дозволяє освітнім організаціям записувати історію та навчальні плани студентів у різних регіонах і в різні часи, зрештою підвищуючи ефективність платформи та знижуючи витрати на обладнання. Крім того, навчальний запис на основі блокчейну служить запобіжним заходом проти підробки та видалення, забезпечуючи автентичність навчальних даних студентів.

Завдяки технології шифрування роботодавці можуть легко поширювати та завантажувати навчальні дані, пропонуючи надійний засіб перевірки статусу навчання студента. Як наслідок, технологія блокчейн допомагає запобігти паперовому шахрайству, підробленим академічним документам та іншим порушенням у вищій освіті, зрештою створюючи надійну платформу для студентів, освітніх організацій і роботодавців.

Популярність онлайн-освітніх платформ незаперечна, але студентам часто не вистачає ентузіазму після закінчення кількох курсів через відсутність визнання та офіційної сертифікації їхніх результатів навчання. В першу чергу це пов’язано із запізнілим просуванням протоколів сертифікації. Зараз сторонні агентства не сертифікують онлайн-навчання ефективно і не

можуть задовольнити вимоги майбутнього зростання онлайн-освіти.

У процесі пошуку роботи сертифікати студента архівуються на освітній платформі або в школі та підлягають перевірці потенційними роботодавцями. Якщо сертифікат втрачено, учень повинен пройти через складний і неефективний процес, щоб отримати заміну від платформи або школи.

Технологія Blockchain пропонує просте та ефективне рішення для сертифікації результатів навчання, зокрема академічної сертифікації. Навіть у разі втрати студентські сертифікати можна легко перевірити за допомогою алгоритму асиметричного шифрування блокчейну в криптографії, який забезпечує безпеку та цілісність даних. Можна було б використати цей підхід для створення комплексної системи акредитації для результатів освіти.

Для початку освітня організація або онлайн-платформа записувала б інформацію про навчання студентів у системі на основі блокчейну. Ця інформація включатиме основні дані, такі як ім’я студента, інформація про курс, результати курсу та дата випуску, серед іншого. Після цього інформація буде зашифрована за допомогою закритого ключа організації або платформи, а цифрові сертифікати будуть видані студентам та іншим одержувачам у мережі. У цьому випадку роботодавці зможуть підтвердити точність цифрових сертифікатів, виконавши хеш-перевірку за допомогою відкритого ключа платформи або організації.

Технологія блокчейн ідеально підходить для забезпечення надійної системи сертифікації результатів навчання через криптографічний і довготривалий характер даних блокчейна. Ця система позбавляє студентів тягаря недоречних сертифікатів, оптимізує процес видачі сертифікатів для платформи чи організації та зменшує витрати роботодавця, пов’язані з перевіркою результатів навчання.

У результаті практичне застосування результатів онлайн-освіти може бути ефективнішим. У наш час існує широкий спектр освітніх онлайн-платформ, які пропонують безліч курсів із багатим вмістом. Однак ці курси не сумісні через такі обмеження, як спосіб навчання та закони про авторське

право. Це становить серйозну проблему для студентів, які вивчають різні типи курсів, оскільки їм доводиться входити на різні платформи. Не менш важко для студентів вищих навчальних закладів вивчати знання в іншій школі чи дисципліні.

Відсутність рівномірності у використанні якісних ресурсів курсу призводить до їх розтрати. Економічний спільне використання (наприклад, спільне використання велосипедів) зросло в геометричній прогресії, і суспільство вимагає більш ефективного використання ресурсів. У сфері освіти розподіл ресурсів прогнозує майбутній напрямок розвитку.

Технологія блокчейн, як типовий додаток, дозволяє обмінюватися ресурсами в онлайн-освіті. Розумні контракти, які є програмними системами, заснованими на механізмах криптографічної безпеки, виконують складні операції без втручання людини. Ця програмна система також підтримує автоматичне виконання та перевірку. Використання технології смарт-контрактів може спростити транзакції, уможлививши інтелектуальні, децентралізовані та автоматизовані процеси, що в кінцевому підсумку призведе до підвищення безпеки транзакцій.

У сфері онлайн-освіти ця технологія сприяла формуванню масивної платформи для обміну ресурсами. За допомогою смарт-контрактів закупівлі курсу, розрахунки та прийняття можуть бути виконані ефективно та точно без потреби в трудових витратах.

Завдяки розподіленому сховищу блокчейну та колективному обслуговуванню студенти можуть отримати доступ до ресурсів з різних платформ, увійшовши в єдиний вузол мережі блокчейн.

Дані освітніх ресурсів також захищені від недійсності, навіть якщо окремі вузли пошкоджені атаками, що забезпечує надійну гарантію безпеки даних. Крім того, завдяки технології блокчейн глобальні системи знань, такі як Вікіпедія, академічні дослідницькі установи та журнали, можуть бути додані до мережі блокчейн, створюючи глобальну базу знань, доступну для вузлів у будь-якій мережі блокчейн. Це значно підвищує ефективність

навчання та доповнює доступні методи навчання.

Протягом минулого століття численні наукові рукописи зазнавали відхилень з різних причин. Незважаючи на згодом визнання та престижні нагороди, такі як Нобелівські премії, початкова відмова в публікації була невтішним досвідом для багатьох науковців, випускників та експертів. Подібним чином незліченна кількість педагогів, студентів і дослідників створюють високоякісний матеріал, якому важко отримати видавничу силу.

Однак впровадження технології блокчейн у навчальних закладах може змінити ці обставини. Використовуючи публікації на блокчейні, студенти та співробітники можуть легко поширювати свої дослідження, надаючи можливості новим письменникам і дослідникам, уникаючи ризику інтелектуальної крадіжки.

Завдяки використанню відкритих і приватних сховищ ключів власник кожної публікації може контролювати доступ і використання. Зрештою, вони вирішують, коли дозволити чи відмовити в результатах своєї праці. Проблема плагіату викликає серйозне занепокоєння в академічних колах.

Крадіжка або копіювання наукової роботи може призвести до втрати років наполегливої праці, тоді як виконання чужого завдання може призвести до нижчих оцінок. Одним із можливих рішень цієї проблеми є впровадження систем блокчейн. Використовуючи цю технологію, захищений авторським правом матеріал можна контролювати та безпечно поширювати онлайн.

Основною функцією цієї технології є безпечне зберігання інформації, яка є незмінною завдяки вдосконаленому шифруванню. Ця система забезпечує безпечний доступ до навчальних матеріалів, а також записує використання та дозволяє власникам легко контролювати доступ. Право власності можна легко перевірити, а використання можна відстежувати онлайн через мережу.

Висновки до Розділу 2.

Наступний розділ стосується засобів, за допомогою яких розробники можуть взаємодіяти з блокчейном під час програмування програм.

Що стосується мов програмування, які використовуються для сценаріїв смарт-контрактів, то найвідомішою є C++. Ця конкретна мова була використана для написання блокчейну Bitcoin. Інша мова, яка зазвичай використовується, — Solidity, яку створили творці криптовалюти Ethereum з явною метою складання смарт-контрактів.

У центрі уваги цього розділу – вивчення віртуальних навчальних середовищ, таких як можливості Google Classroom. На основі цього аналізу було зроблено пропозицію щодо реалізації найбільш часто використовуваних функцій цих платформ на технології блокчейн. Ці функції включають зберігання історії навчання, сертифікацію, обмін інформацією між студентами та викладачами, а також захист від фальсифікації робіт і плагіату. Крім того, представлено успішні та надійні приклади інтеграції блокчейну в навчальний процес.

РОЗДІЛ 3. РОЗРОБКА ПРОПОЗИЦІЇ УДОСКОНАЛЕННЯ НАВЧАЛЬНИХ СЕРЕДОВИЩ НА ОСНОВІ БЛОКЧЕЙН

3.1 Використання технологій блокчейн для автоматизації роботи з освітніми документами

Оскільки технології продовжують розвиватися, це впливає на швидку еволюцію інтернет-інструментів і появу нових загроз. Зі зростанням технологій зростає і попит на зловмисні дії, такі як хакерство, крадіжка, незаконна торгівля, шантаж і підрив влади. Однак було вжито заходів для протидії цим загрозам, включаючи захисні методи та підходи, які гарантують безпеку потенційних жертв, наприклад звичайних осіб, які покладаються на онлайн-сервіси для надсилання ідентифікаційних документів і отримання авторизації на своїх робочих місцях.

Після закінчення вищої, середньої професійної або середньої освіти кожному випускнику видається диплом, свідоцтво або свідоцтво про успішне проходження відповідної освітньої програми. Цей документ слугує роботодавцям інструментом для оцінки професійних навичок потенційного працівника на основі їх наявності. Крім того, це дає змогу приймальним комісіям навчальних закладів переконатися, що кожен вступник здобув необхідний рівень освіти, необхідний для наступного рівня. Сам документ є паперовою гарантією, яка підтверджує отримання освіти, а його підробку ускладнюють різні захисні елементи, такі як мікрошрифти та водяні знаки.

Хоча ідея абсолютної автентичності є бажаною, жоден фізичний метод захисту не може її гарантувати. Це призводить до численних проблем з точки зору перевірки дипломів і сертифікатів. Найбільш важливою проблемою є велика кількість шахрайських копій, доступних на незаконному ринку. Це скрутне становище стосується як роботодавців, так і приймальних комісій навчальних закладів, оскільки вони не можуть повністю покладатися на надані їм освітні документи.

Навіть ті, хто є справжніми отримувачами документів про освіту, не застраховані від ризиків. Навіть якщо навчальний заклад не акредитований,

він все одно може приймати студентів, стягувати плату за навчання та надавати фальшиві документи після завершення періоду навчання. Крім того, існує вразливість, коли йдеться про зміну цих документів. Наприклад, особа може маніпулювати своїми оцінками або додавати додаткові курси до свого диплому. Як наслідок, питання автентичності документів про освіту є актуальним для всіх сторін освітнього процесу, включаючи студентів, навчальні заклади та роботодавців.

Хоча наявність фізичної копії документа може дати певну впевненість, це не надійний спосіб підтвердження його автентичності. Тому потрібно шукати альтернативні методи. Перший варіант – подати запит до державних органів, уповноважених завіряти документи. Другий варіант – звернутися до навчального закладу, який видав документ. Важливо зазначити, що ці методи перевірки вимагають бюрократичної підготовки та тривалого періоду очікування до отримання результатів.

Наша серія випусків стала каталізатором для створення системи, яка б запобігала будь-якій підробці документів про освіту, а також оптимізувала процес їх роботи. Ця система, по суті, повинна забезпечувати гарантію автентичності, незмінності та безпеки даних. Крім того, він повинен забезпечити захищений доступ із можливістю розширення прав доступу за запитом власників документів. Система також має сприяти плавній міграції вже існуючих даних про видані освітні документи без необхідності будь-якої фізичної модифікації попередніх даних.

Серед нинішньої ери цифровізації та стрімкого технологічного прогресу суспільства найбільш підходящим методом гарантування виконання вищезазначених критеріїв є використання технології блокчейн.

Технологія блокчейн пропонує широкий набір варіантів використання.

В основі багатьох процвітаючих підприємств лежить ефективний ланцюг поставок. Основною функцією цього ланцюга є обробка та транспортування товарів від постачальника до споживача. Традиційно координація багатьох зацікавлених сторін у цій галузі виявилася

стомлюючою та трудомісткою задачею. Однак технологія блокчейну створила можливість для взаємосумісної екосистеми, яка зосереджена навколо довготривалої бази даних. Це потенційно може призвести до безпрецедентного рівня прозорості для різноманітних галузей.

Ігрова індустрія перебуває під сильним впливом компаній, які контролюють ігрові сервери, що фактично диктує дії геймерів. У цій галузі кінцеві користувачі фактично не володіють внутрішньоігровими активами, оскільки вони існують лише у сфері спекуляцій. Однак завдяки застосуванню підходу, заснованого на блокчейні, користувачі отримують можливість справді володіти своїми активами за допомогою взаємозамінних і незамінних токенів (NFT), які можна передавати між різними іграми та ринками.

Прозорість і безпека, які забезпечує технологія блокчейн, робить її винятковою платформою для зберігання медичних записів. Індустрія охорони здоров'я складається з великої кількості установ, таких як лікарні, клініки та постачальники медичних послуг, і ця фрагментація робить конфіденційну інформацію пацієнтів чутливою до кібератак.

Централізовані сервери, які зберігають цю інформацію, особливо вразливі. Використовуючи технологію блокчейн, медичні записи можна криптографічно захистити для захисту конфіденційності пацієнтів, а інформацію можна легко обмінювати між закладами охорони здоров'я, підключеними до глобальної бази даних.

Надсилання грошей за кордон може бути проблемою, якщо покладатися на традиційні банківські системи. Комісія та умови цих переказів роблять їх дорогими та ненадійними, особливо для тих, кому потрібні термінові перекази коштів. Крім того, навігація через складну мережу посередників може ще більше ускладнити процес. Проте криптовалюти та блокчейни з'явилися як потенційне рішення цієї проблеми. Усунувши потребу в посередниках, кілька проектів змогли використати цю технологію для сприяння швидким і недорогим міжнародним грошовим переказам.

Інтернет речей (IoT) — це зростаюча мережа фізичних пристроїв, підключених до Інтернету, і деякі експерти вважають, що цю мережу можна значно покращити за допомогою інтеграції технології блокчейн як у житлових, так і в промислових умовах.

Розповсюдження цих пристроїв вимагає впровадження нової платіжної моделі під назвою «машина-машина» (M2M), яка вимагає системи з високою пропускною здатністю для розміщення мікроплатежів. IoT — це комп'ютерна концепція, яка передбачає мережу фізичних об'єктів, оснащених технології для взаємодії один з одним або навколишнім середовищем, і ця мережа має потенціал для реструктуризації соціальних і економічних процесів шляхом автоматизації певних дій і операцій.Хоча централізовані послуги наразі є домінуючою моделлю в галузі Інтернету речей, вони не є життєздатними в довгостроковій перспективі рішення для масового виробництва пристроїв Передача даних і внутрішніх послуг із централізованих серверів у децентралізовану блокчейн-систему може стати ключем до реалізації повного потенціалу мережі IoT.

Не дивно, що розподілені мережі можна застосовувати для процесів деінтермедіації на місцевому, національному або міжнародному рівнях, оскільки вони реалізують власний метод регулювання. Публічне управління на блокчейні гарантує, що кожен учасник залучений до процесу прийняття рішень і пропонує чітке бачення політичної діяльності завдяки своїй прозорості.

Благодійні організації часто стикаються з обмеженнями через фінансові обмеження. Однак концепція «криптоблагодійності» з'явилася з використанням технології блокчейн для подолання цієї проблеми. Унікальні властивості цієї технології забезпечують прозору платформу для всіх операцій, дозволяючи благодійникам брати участь, не обмежуючись місцезнаходженням. Крім того, операційні витрати зменшуються, створюючи можливість для швидкого зростання та розвитку в цій галузі.

В епоху цифрових технологій сучасному світу необхідні рішення для

ідентифікації особистості. З такою кількістю людей, схильних до підробок, традиційні заходи безпеки неможливі для багатьох звичайних користувачів. На щастя, технологія блокчейн пропонує рішення. За допомогою цієї технології особисту суверенну ідентифікацію (відому як самосуверенна ідентичність англійською мовою) можна записати в реєстрі мережі блокчейн і пов'язати з її законним власником. Це дозволяє вибірково розкривати особисту інформацію третім особам, зберігаючи при цьому конфіденційність і безпеку.

Використання технології блокчейн залишається дуже затребуваною тенденцією серед різних міжнародних організацій, починаючи від фінансового, урядового та комерційного секторів. Нещодавно журнал ForkLog опублікував огляд деяких найбільш інтригуючих ініціатив. Одна з цих ініціатив стосується постачальника медичних послуг із Сінгапуру, Zuelling Pharma, який займається впровадженням блокчейн-системи eZTracker, яка дозволить негайно перевіряти автентичність сертифікатів про вакцинацію проти COVID-19.

Медичний персонал і власники сертифікатів зможуть не тільки засвідчити зазначені сертифікати, але й відстежувати історію вакцинації та бали. Впроваджуючи цю систему, Zuelling Pharma прагне пом'якшити інциденти, які можуть виникнути внаслідок використання препаратів із вичерпаним терміном придатності, які є підробленими або які зберігалися неналежним чином.

Азіатський банк розвитку (ADB) запустив нову систему операцій з цінними паперами на основі блокчейну. АБР планує співпрацювати з великими фірмами в галузі для розробки проекту для проведення міжнародних операцій з цінними паперами через блокчейн. Їхня мета полягає в тому, щоб з'єднати центральні банки та депозитарії цінних паперів Асоціації держав Південно-Східної Азії, дозволяючи пряму взаємодію та скорочуючи транзакційні витрати, одночасно усуваючи ризики неточностей.

Цей проект також має на меті прискорити транскордонні операції з

цінними паперами в регіоні, які зазвичай обробляються через міжнародну мережу зберігачів, проходять через США чи Європу та можуть тривати кілька днів.

Основною характеристикою технології блокчейн є її надійність. Ця якість є результатом того, як дані зберігаються в системі розподіленої книги: на комп'ютерах кожного окремого учасника. Зокрема, комп'ютер кожного учасника зберігає частину інформації у вигляді блоків або копій цих блоків, які криптографічно захищені. Така конструкція робить систему практично непроникною.

Крім того, механізм гаманців дозволяє унікально та гарантовано ідентифікувати автора збережених даних. Хоча одного цього може здатися недостатнім, реалізація смарт-контрактів – комп'ютерних алгоритмів, які працюють на блокчейні – дозволяє створити логіку для доступу, додавання або зміни інформації, що зберігається в блокчейні, за допомогою коду, написаного мовою програмування, що підтримується платформа. Ця гнучка логіка дозволяє керувати політиками транзакцій і рівнями доступності даних у системі.

Технологія автоматизації навчального документообігу здатна вирішити багато завдань. У результаті було визначено, що цю технологію слід використовувати при його розробці. Є численні програми з відкритим кодом, які можуть допомогти в інтеграції блокчейну у ваші рішення. У глобальному масштабі ці програми можна розділити на два типи: програми з обмеженим доступом до блокчейну (приватні) і програми з необмеженим доступом (публічні).

Публічні блокчейн-платформи підходять для використання у відкритих системах, які мають загальнодоступні дані. Наприклад, публічну платформу блокчейн можна використовувати для системи купівлі квитків у кіно. Ці платформи дуже надійні з точки зору безпеки завдяки своїй прозорості, що дозволяє будь-кому приєднатися до блокчейну та читати інформацію, що міститься в його блоках. Однак ця функція також робить публічні платформи

непридатними для систем, які зберігають конфіденційні дані.

У результаті поточні вимоги щодо обмеженого доступу до освітніх документів вимагають використання виключно приватних блокчейн-платформ. Структура приватних мереж схожа на публічні, але вони відрізняються реєстрацією учасників. Для ілюстрації система вимагає, щоб у мережу входили лише законні освітні організації.

Вибираючи з різноманітних доступних приватних блокчейн-платформ, важливо вибрати ту, яка пропонує всі необхідні функції для впровадження системи зберігання та перевірки документів. Hyperledger Fabric є ідеальним вибором, оскільки він був спеціально розроблений для задоволення вимог безпечних децентралізованих корпоративних систем.

Крім того, ця платформа дозволяє встановити політику транзакцій, яка відповідає потребам проекту. Він може похвалитися гнучкою конфігурацією та набором API високого рівня, які полегшують інтеграцію зі сторонніми програмами на трьох широко використовуваних мовах програмування: Java, Go та JavaScript. Linux Foundation запустила цю платформу в грудні 2015 року за сприяння IBM, Intel і SAP Ariba. Усі ці фактори разом роблять Hyperledger Fabric кращою блокчейн-платформою для цілей розробки.

У нинішній системі всі навчальні заклади підключені до єдиного логічного каналу. Це з’єднання надає кожній установі доступ до спільної мережі та розумного договір, що діє в його межах. Щоразу, коли учасник мережі видає диплом або будь-який інший документ, активується відповідний метод смарт-контракту, ініціюючи створення транзакції для додавання даних у блокчейн. Потім цю транзакцію перевіряють усі інші учасники мережі.

Якщо більшість учасників підтверджують достовірність інформації в рамках транзакції, запис про видачу документа додається в блокчейн мережі.

Виконання пробного розгортання приватної мережі та налаштування політики додавання даних є життєздатним варіантом, який можна легко застосувати до реальних вузлів мережі. Далі можна скласти і вивчити модель

майбутнього смарт-контракту.

Ці результати представляють суть розуміння, впровадження та аналізу екосистеми блокчейнів і вимагають значної кількості часу. Після того, як ці аспекти виконані, завдання, що залишилися, включають завершення розробки смарт-контракту, встановлення зв'язку між блокчейном і сервером та інтеграцію інтерфейсу користувача.

Таким чином, цю систему можна впровадити в будь-якому навчальному закладі, який бажає убезпечити себе та своїх випускників, а також запобігти фальсифікації документів про освіту відразу після її створення. Безпека та надійність мережі лише зростатиме зі збільшенням кількості учасників завдяки властивим блокчейну функціям, які нададуть додаткові гарантії.

Інтеграція технології блокчейн в державне управління України, зокрема сферу освіти, забезпечить високий рівень довіри суспільства до державних структур, а також прозорість цифрової взаємодії між державними органами, громадянами та суб'єктами господарювання. Це призведе до економії бюджету за рахунок прозорих державних закупівель та зниження рівня корупції.

Одним з напрямків майбутнього розвитку є комерціалізація системи через надання різноманітних інформаційних послуг тим, хто хоче аналізувати дані, які вона містить. Одну з таких послуг роботодавці можуть використовувати для пошуку кандидатів із певною кваліфікацією та навичками, використовуючи різні критерії для звуження кола претендентів. Потім їм буде надана контактна інформація тих, хто дав згоду на перегляд.

3.2 Загальна характеристика прототипу застосунку

Використовуючи FAV (функціональний аналіз і аналіз витрат), можна оцінити важливість і практичність прототипу програми, незалежно від організаційної структури компанії. Це обстеження дозволяє зробити висновок про найбільш ефективний розподіл ресурсів для проекту.

Спочатку проводиться ретельна оцінка функцій, щоб оцінити відносну важливість кожного фунта. Наступний крок передбачає розподіл функцій на дві категорії, визначені їх впливом на загальну вартість продукту. Перша категорія складається з функцій, які мають пряме відношення до вартості продукту, тоді як друга категорія включає функції, які цього не роблять.

Далі оцінка переходить до оптимізації послідовності функцій шляхом виключення кроків з другої групи, що призводить до уточненої послідовності, яка є більш ефективною. Нарешті виконується аналіз для визначення вартості всіх функцій після оптимізації.

Для розробки прототипу електронного студентського кабінету проведено техніко-економічний аналіз. Аналіз включає як функціональну оцінку, так і оцінку вартості. Оскільки кожне рішення, прийняте під час проекту, впливає на всю систему, підсистеми також повинні відповідати необхідним вимогам.

Так, ФВА, або функціональний аналіз, використовується для оцінки функцій програмного продукту – прототипу електронного кабінету для студентів. Цей прототип буде використовувати технологію блокчейн. Технічні характеристики кінцевого результату такі: З електронним офісом можна легко взаємодіяти через веб-браузер.

Двома основними проблемами, коли мова заходить про електронні шафи, є забезпечення безпеки користувача та сприяння обізнаності громадськості про їхні дії. Інтуїтивно зрозумілий дизайн характеризується зручним інтерфейсом і простотою взаємодії.

Однією з ключових переваг цієї системи є її просте та безпроблемне налаштування, а також безперебійна можливість розширення та налаштування розміру відповідно до потреб користувача. Крім того, обслуговування системи є легким, оскільки всі необхідні оновлення та модифікації є простими та зрозумілими. Програмний продукт може бути реалізований з мінімальними витратами. Основним призначенням F0 є створення програмного продукту.

Отже, його основні функції можна відрізнити від програмного продукту. Коли мова йде про блокчейн, рішення про те, яку мову програмування використовувати, є вирішальним. Процес вибору фреймворку для розробки веб-інтерфейсів вимагає ретельного розгляду.

Відбір має здійснюватися з наміром і метою, враховуючи унікальні потреби та цілі проекту. Вибір середовища розробки, зокрема F3, відіграє вирішальну роль у створенні та виконанні проектів програмного забезпечення. Хоча кожна з основних функцій має щонайменше два рішення, також можливо, що доступних рішень буде кілька.

F1):

А) C++

Б) Solidity

F2):

А) Vue.js

Б) React

F3):

А) Visual Studio Code

Б) Web Storm

Після того, як методи включення функцій визначені, можна використати морфологічну карту (рис. 3.1), щоб відобразити всі можливі варіанти функцій.

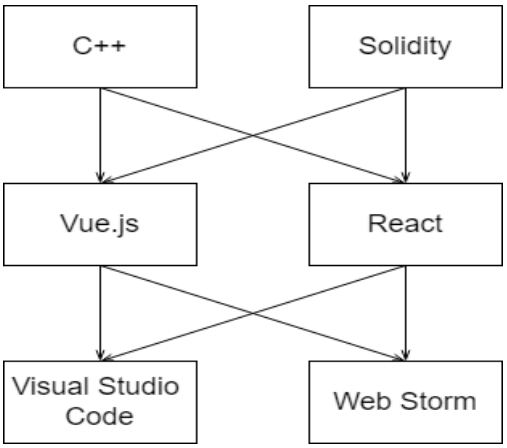

Рисунок 3.1 – Морфологічна карта програмного продукту

Таблиця 3.1 Позитивно-негативна матриця варіантів основних функцій

Функція	Варіант реалізації	Переваги	Недоліки
F1	А	Використовувався при написанні блокчейну біткоїна, швидкий	Складний для вивчення, ручне управління пам’ятю
	Б	Створювався спеціально для написання програм на блокчейні	Майже немає додаткових бібліотекдля розробки
F2	А	Легкий та зрозумілий у використанні, зручний CLI	Надмірна гнучкістькоду
	Б	Зручне налаштування SEO та тестування	Використовує JSX, погана документація
F3	А	Підтримує багато мов програмування, вбудований інтерфейс роботи з контролем версії	Споживає багато оперативної пам’яті, не може самостійно запускати код, а лише редагувати
	Б	Може запускати проєкти, Багатофункціональний інтерфейс	Підтримує лише проєкти веб-застосунків

Використовуючи позитивно-негативну матрицю, можна ефективно оцінити, які функції є життєздатними, а якими слід знехтувати. Коли справа доходить до функції F1, C++ становить більшу складність для тих, хто хоче її вивчити, через її вищий поріг входу.

Навпаки, Solidity може не мати додаткових бібліотек, але сама мова є досить універсальною. Зрештою, ми обираємо варіант Б, щоб досягти швидкого та зручного налаштування відповідно до вимог проекту.

Коли справа стосується функції F2, вибір веб-фреймворку не є суттєвим фактором. Це пов’язано з тим, що обидва варіанти широко поширені та мають необхідні бібліотеки для взаємодії з інструментами блокчейну. Як результат, будь-який вибір можна використовувати без проблем.

Використовуючи Web Storm під час розробки, з легкістю налаштувати блокчейн-проект неможливо.

У результаті функція F3 матиме порівняльні функції в обох редакторах, що робить Web Storm застарілим для цього конкретного проекту. Варіант А є кращим вибором через його менший розмір і підтримку кількох мов. Як тільки морфологічна карта була використана для усунення невідповідних варіантів, лише пара з початкових шести варіантів залишалася життєздатною.

- F1(Б) – F2(А) – F3(А);

- F1(Б) – F2(Б) – F3(А);

Оцінці якості програмного продукту сприятиме система параметрів. Були обрані такі параметри:

Тривалість, необхідна для побудови веб-проекту та реалізації смарт-контрактів, позначена X1. Обсяг оперативної пам'яті, який використовувався під час роботи проекту, вдвічі перевищував початковий обсяг (X2).

Необхідна кількість програмного коду для написання розробником потроюється, представлена як X3.

Час, необхідний для підтвердження транзакції в блокчейні, позначений абревіатурою X4, є критичним аспектом технології блокчейну.

Таблиця 3.2 – Основні параметри програмного продукту

Опис параметру	Умовні позначення	Одиниці виміру	Значення параметру		
			гірші	середні	кращі
Час на збірку проекту	X1	хв	6	4	2
Об’єм оперативної пам’яті	X2	Мб	100	60	40
Об’єм коду програми	X3	рядкикоду	1500	1000	800
Час підтвердження транзакції ублокчейн	X4	мс	5000	500	200

Використовуючи таблицю 3.2, ми можемо створити візуальне представлення параметрів за допомогою серії графіків, які представлені на рис. 3.2 - рис. 3.5.

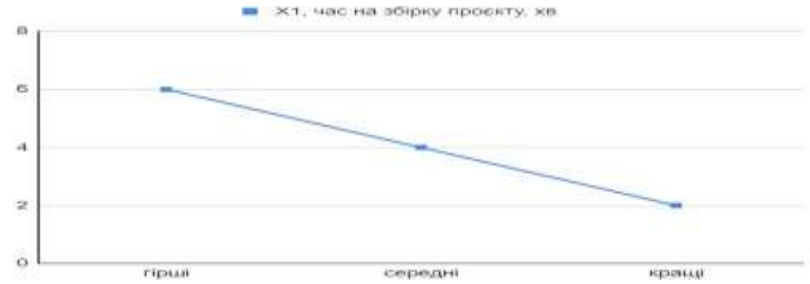

Рисунок 3.2 – Час на збірку проєкту

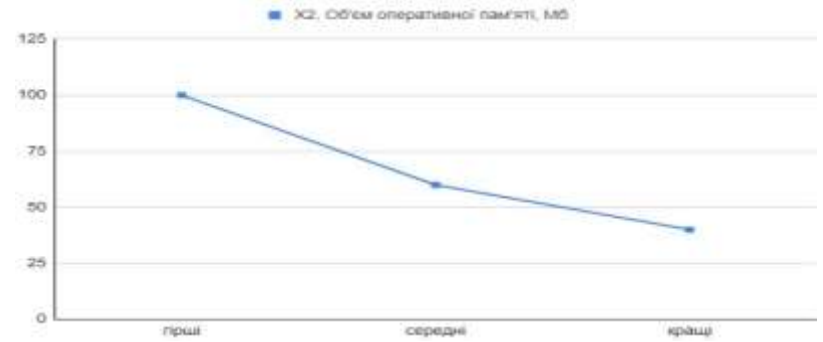

Рисунок 3.3 – Об’єм оперативної пам’яті

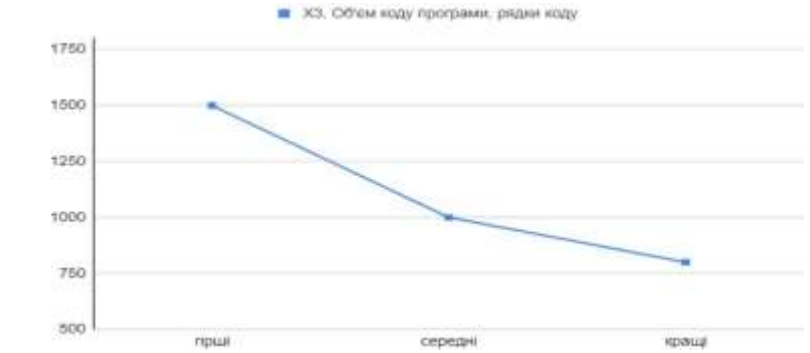

Рисунок 3.4 – Об’єм коду програми

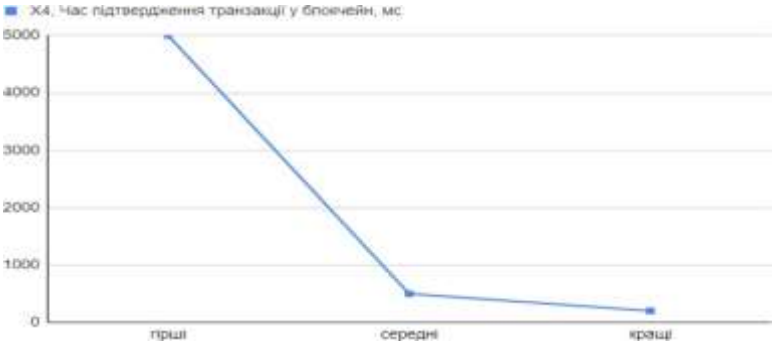

Рисунок 3.5 – Час запису транзакції у блокчейн

За даними графіками ми можна візуально зобразити основні параметри прототипного проекту.

3.3 Аналіз експертного оцінювання параметрів прототипу

За допомогою методу попарного порівняння можна з'ясувати важливість окремих параметрів. Експертна комісія складається з п'яти осіб.

Для розрахунку коефіцієнтів значущості для кожного параметра необхідно виконати наступні кроки: Присвоєння різних рангів — це метод визначення рівня важливості певного параметра.

Важливо оцінити відповідність експертних оцінок для можливого майбутнього застосування. Розрахунок відносної важливості кожного параметра по відношенню до інших передбачає визначення приблизної оцінки їх парного пріоритету.

Після збору даних наступним кроком є аналіз значущості результатів. Це передбачає обробку даних і обчислення коефіцієнтів значущості. У таблиці 5.3 представлені результати.

Таблиця 3.3 – Результати ранжування показників

Параметр	Ранг параметра за оцінкою експерта					Сума рангів	ВідхиленняΔi	Δ_i^2
	1	2	3	4	5			
X1	2	4	3	4	4	17	+4,5	20,25
X2	4	3	4	3	3	17	+4,5	20,25
X3	3	2	2	2	1	10	-2,5	6,25
X4	1	1	1	1	2	6	–6,5	42,25
Разом	10	10	10	10	10	50	0	89

Для оцінки рівня надійності в експертних оцінках встановлюємо такі параметри: Формули 3.1 і 3.2 дають підсумовування рангів кожного параметра і сукупне підсумовування всіх рангів відповідно.

$$\boldsymbol{R = \sum_{i=1}^{n} r = 50} \qquad \textit{(3.1)}$$

де N – число експертів;

r – ранг і-го параметра, визначений j-м експертом.

б) середня сума рангів T:

$$T = \frac{1}{n} R_i = 12.5 \qquad (3.2)$$

в) відхилення суми рангів кожного параметра від середньої суми рангів:

$$\Delta_i = R_i - T = 10 \qquad (3.3)$$

г) загальна сума квадратів відхилення:

$$S = \sum_n \Delta_i = 35 \qquad (3.4)$$

д) коефіцієнт узгодженості (конкордації):

При розрахунку коефіцієнта узгодженості виявлено, що він перевищує нормативний коефіцієнт 0,67 і досягає значення 0,7. Це свідчить про те, що рейтинг можна вважати надійним. Результати можна використовувати для порівняння параметрів у парах. Таблиця 5.4 відображає результати порівняння. Щоб визначити чисельні коефіцієнти переваги для даного параметра над іншим, можна використати формулу 3.5.

$$a_{ij} = \{1{,}5 \;\; x_i > x_j;\; 1{,}0 \;\; x_i = x_j;\; 0{,}5 \;\; x_i < x_j. \qquad (3.5)$$

де x_i, x_j – параметри оцінювання.

Таблице 3.4 Попарне порівняння параметрів

Параметри	Експерти					Кінцеваоцінка	Числове значення
	1	2	3	4	5		
X1, X2	<	>	<	>	>	>	1,5
X1, X3	<	>	>	>	>	>	1,5
X1, X4	>	>	>	>	>	>	1,5
X2, X3	>	>	>	>	>	>	1,5
X2, X4	>	>	>	>	>	>	1,5
X3, X4	>	>	>	>	<	>	1,5

Ми створюємо матрицю шляхом ранжування параметрів і отримання числових оцінок. Формула 3.6 використовується для обчислення відносних оцінок.

Ця формула повторно застосовується, поки значення поточної ітерації

не зменшаться принаймні на 2% порівняно з попередніми значеннями.

$$K_{B_i} = \frac{b_i}{\sum_{i=1}^{n} b_i} \quad (3.6)$$

де, $\sum_{i=1}^{n} a$ вартість і-го параметра за результатами оцінок всіх експертів;

a_{ij} – коефіцієнт переваги і-го над j-тим параметром.

Розрахунки вагомості параметрів наведені у таблиці 3.5

Таблиця 3.5 Розрахунок вагомості параметрів

I	J				Перша ітерація		Друга ітерація	
	X1	X2	X3	X4	B_i	K_{Bi}	B^1_i	K^1_{Bi}
X1	1,0	1,5	1,5	1,5	5,5	0,344	21,25	0,36
X2	0,5	1,0	1,5	1,5	4,5	0,281	16,25	0,275
X3	0,5	0,5	1,0	1,5	3,5	0,219	12,25	0,208
X4	0,5	0,5	0,5	1,0	2,5	0,156	9,25	0,157
Разом					16,0	1,0	59,0	1,0

З даних, представлених у таблиці 3.5, очевидно, що зміна вагових коефіцієнтів не перевищує 2% після четвертої ітерації, що вказує на те, що подальші ітерації не потрібні. Щоб забезпечити точну оцінку, якість кожної варіації основних функцій буде оцінено окремо.

Технічним вимогам програмного продукту відповідають абсолютні значення X1, що відноситься до часу складання проекту, і X2, що позначає обсяг оперативної пам'яті, який використовується програмою.

При виборі абсолютного значення параметрів X3 і X4 вибране значення не представляє найгірший сценарій. Замість цього він відповідає або варіанту Б), або В) на основі параметрів. Ці параметри включають 1000 або 800 рядків коду, який повинен написати розробник, і 500 або 200 мс, необхідних для запису транзакції в блокчейні. Подальші розрахунки наведено в таблиці 3.6

Таблиця 3.6 – Розрахунок показників якості

Основні функції	Варіант реалізації	Параметр	Абсолютне значення параметра	Бальна оцінка параметра	Коефіцієнт вагомості параметра	Коефіцієнт рівня якості
F1	Б	X4	500	9,625	0,157	1,51
F2	А	X3	800	10	0,208	2,08
	Б	X1	4	5	0,36	1,8
F3	А	X2	64	7	0,208	1,46

За даними таблиці визначимо рівень якості кожного з варіантів:

- F1(Б) – F2(А) – F3(А) = 1,51 + 2,08 + 1,46 = 5,05;

- F1(Б) – F2(Б) – F3(А) = 1,51 + 1,8 + 1,46 = 4,77.

Найоптимальніший вибір функцій визначається варіантом з найвищим коефіцієнтом технічної підготовки. У цьому випадку рекомендованим вибором функцій буде F1(В), потім F2(А), а потім F3(А).

Економічний аналіз варіантів розробки програмного продукту

Початковий крок у обчисленні вартості розробки полягає в оцінці кількості необхідної праці. Кожен із доступних варіантів складається з пари завдань.

Розробка технології блокчейн для урядових потреб зараз триває в кабінеті міністрів. Наразі відбувається створення веб-додатку для офісного використання. У таблиці 3.8 подано класифікацію завдань за рівнем складності та новизни.

Таблиця 3.7 – Класифікація завдань

Номер завдання	Ступінь новизни	Складність алгоритму
1	А	1
2	Б	1

Завдання 1 передбачає використання даних у різних формах, тоді як

завдання 2 використовує звичайні методи збору даних.

Щоб визначити нормативні терміни виконання кожного завдання, необхідно розрахувати відповідні норми часу. Загальну кількість праці, необхідну для виконання кожного завдання, можна розрахувати за формулою:

$$T_O = T_p * K_П * K_{СК} * K_M * K_{СТ} * K_{СТ.М} \quad (3.8)$$

де $T_р$ – трудомісткість розробки програмного продукту; $К_П$ – поправочний коефіцієнт;

$К_{СК}$ – коефіцієнт на складність вхідної інформації; $К_М$ – коефіцієнт рівня мови програмування;

$К_{СТ}$ – коефіцієнт використання стандартних модулів і прикладних програм;

$К_{СТ.М}$ – коефіцієнт стандартного математичного забезпечення.

При розгляді нормативів часу для розрахунку ступеня новизни А та групи складності алгоритму 1 визначено трудомісткість 90 людино-днів. Крім того, важливу роль відіграє тип вхідної інформації.

Для першого завдання визначено поправочний коефіцієнт KP 1,7, а також враховано коефіцієнт складності вхідної інформації. Перше завдання, позначене CSC = 1, під час розробки буде використовувати стандартні модулі.

В результаті коефіцієнт використання як прикладних програм CST, так і стандартних модулів встановлено на рівні 0,8. Маючи цю інформацію, ми можемо приступити до обчислення загальної складності програмування та розробки завдання.

Рівняння T1 дорівнює 90, помноженому на 1,7, помноженому на 0,8, що дає 122,4 людино-дня.

Що стосується другого завдання (яке підпадає під групу новизни B і алгоритм складності 1), загальний час, необхідний для виконання, становить 64 людино-дні. CP (або рівень складності) обчислюється як 1,021, зі значеннями KSK і KST 1 і 0,8 відповідно.

Щоб визначити загальну складність розробки цього завдання, необхідно провести розрахунок.

Розрахунок для Т2 виглядає наступним чином: 64 помножити на 1,021, а потім на 0,8, в результаті чого для завершення потрібно 52,3 людино-дня. Об’єднаємо всі варіанти в одну групу, враховуючи, що всі вони вимагають рівноцінної трудомісткості.

Загальний обсяг необхідної праці становить: Загальну кількість людино-годин, необхідних для технічного обслуговування, можна розрахувати за такою формулою: (122,4 + 52,3) помножити на 8, отримати 1397,6 людино-годин.

Команда розробників складається з двох учасників: автора смарт-контрактів, який отримує місячну зарплату 30 000 гривень, і розробника веб-додатків, який отримує місячну зарплату 25 000 гривень.

Щоб розрахувати їх погодинну оплату праці, ми повинні розділити їхню відповідну зарплату на кількість робочих годин у місяці.

$$C = \frac{30000 + 25000}{2 * 21 * 8} = 163,7 \text{ грн.}$$

Розрахуємо заробітну плату розробників:

$C_{ЗП} = 163,7 * 1397,6 * 1,2 = 274\,544,54$ грн.

Відрахування на соціальний внесок становить 22%:

$C_{СВ} = C_{ЗП} * 0,22 = 60\,399,8$ грн.

Тепер можна розрахувати витрати на оплату однієї машино-години. Одна ЕОМ обслуговується одним інженером апаратного забезпечення з окладом 15000 грн. та коефіцієнтом зайнятості $К_З = 0,2$:

$C_Г = 12 * 15000 * 0,2 = 36000$ грн.

З урахуванням додаткової заробітної плати:

$C_{ЗП} = C_Г * (1 + К_З) = 36000 * 1,2 = 43200$ грн.

Відрахування на соціальний внесок становить 22%:

$C_{СВ} = C_{ЗП} * 0,22 = 86400 * 0,22 = 19008$ грн.

Амортизаційні відрахування розраховуємо за формулою при амортизації

25% та вартості ЕОМ – 32000 грн.:

$C_А = 1,15 * 0,25 * 32000 = 9200$ грн.

Витрати на ремонт розраховуємо за формулою:

$C_р = 1,15 * 0,05 * 30000 = 1840$ грн.

Ефективний годинний фонд часу ПК за рік:

$Т_{еф}= (365 - 104 - 12 - 12) * 8 * 0,9 = 1706,4$ год.

Витрати на оплату електроенергії:

$C_{ел} = 1706,4 * 0,65 * 0,2 * 3,0293 = 671,99$ грн.

Накладні витрати розраховуємо за формулою:

$C_Н = Ц_{ПР} * 0,67 = 30000 * 0,67 = 20100$ грн.

Річні експлуатаційні витрати:

$C_{ЕК} = C_{ЗП} + C_{СВ} + C_А + C_р + C_{ЕЛ} + C_Н =$ 93919,99 грн.

Собівартість однієї машино-години ЕОМ становить:

$$C_{МГ} = \frac{C_К}{Т_Ф} = \frac{93919,99}{1706,4} = 55,04 \text{ грн/год.}$$

Оскільки роботи, що будуть проводитися під час розробки програмного продукту будуть вестися на комп'ютерах, то оплата машинного часу буде складати:

$C_М = C_{МГ} * Т = 55,04 * 1397,6 = 76923,9$ грн.

Накладні витрати складають 67% від заробітної плати:

$C_Н = C_{ЗП} * 0,67 = 274\,544,54 * 0,67 = 183\,944,84$ грн.

Отже тепер можна порахувати вартість розробки програмного продукту за варіантами:

$C_{ПП} = C_{ЗП} + C_{СВ} + C_М + C_Н =$

$= 274\,544,54 + 60\,399,8 + 76\,923,9 + 183\,944,84$

$= 595\,813,08$ грн.

Порахуємо коефіцієнт техніко-економічного рівня за формулою 3.9:

$К_{ТЕР} = 5,05 / 595\,813,08 = 8,476 * 10^{-5}$

Висновки до розділу 3

Після функціонально-вартісного аналізу програмного продукту було проаналізовано функції програмного забезпечення, порівняно систему параметрів і остаточно визначено найбільш оптимальний вибір. В якості мови для написання смарт-контрактів було обрано ланцюжок Solidity, Vue.js — фреймворк для розробки веб-додатку, а Visual Studio Code — редактор коду.

Саме цей варіант має найвищий техніко-економічний коефіцієнт рівня 8,476 * 10-5. Зазначимо, що реалізація функцій програмного проекту коштуватиме приблизно 595 813,08 грн.

ВИСНОВОК

У дипломній роботі було проведено дослідження теоретичних аспектів технології блокчейн. Це включало ретельний аналіз історії технології та передумов, а також детальне вивчення різних алгоритмів і концепцій, таких як дерево Меркла, децентралізована мережа та алгоритм підтвердження роботи. Текст також заглибився в структуру блоку, життєвий цикл транзакції та механізм, який використовується для зв'язування блоків у ланцюг.

Щоб отримати повне розуміння механізму блокчейну, автор також надав детальний опис принципу роботи децентралізованих програм, а також їхні переваги та недоліки.

Було виявлено, що децентралізовані програми є більш безпечними, стійкими до збоїв і економічно ефективними з точки зору підтримки робочого стану програми, головним чином завдяки додатковим послугам і комісії за транзакції, які зазвичай стягують централізовані програми.

Щоб покращити впровадження та реалізацію технології блокчейн, було досліджено як теоретичне, так і практичне застосування цієї технології за межами криптовалюти.

Зокрема, було проаналізовано основні функції віртуальних освітніх середовищ, а також розглянуто конкретні приклади використання блокчейну у сфері освіти для глибшого розуміння предмета дослідження.

Зокрема, серед успішних прикладів – фіксація досягнень студентів і навчальних програм, а також достовірна сертифікація результатів студентів. Для розміщення віртуальних освітніх середовищ веб-браузери виявилися найуспішнішим варіантом, що призвело до поглибленого вивчення інструментів блокчейну, які можуть взаємодіяти з веб-додатками.

Після розгляду багатьох мов програмування смарт-контрактів C++ і Solidity стали найпопулярнішими варіантами. Зрештою, для реалізації програмного забезпечення було обрано Solidity. Найбільш зручними та зрозумілими програмами та бібліотеками визнано розширення MetaMask, а також середовища розробки смарт-контрактів Remix Project та Truffle Suite.

З них Remix Project було обрано для впровадження програмного забезпечення через його здатність підключатися до веб-проектів, графічний інтерфейс і більший набір функцій порівняно з інтерфейсом консолі Truffle Suite. Причини вибору мови програмування та фреймворків детально описано в розділі 3.

Після проведення аналізу предметної області та механізмів, необхідних для вирішення поставленої задачі, був створений прототип електронного кабінету. Ця програма дозволяє студентам реєструватися та авторизуватися, складати іспити та реєструвати результати своїх тестів із різних курсів у смарт-контракті. Крім того, він пропонує список оцінок за пройдені курси.

Основними перевагами цього додатку є можливість фіксувати та отримувати результати оцінювання знань без залучення посередників. У порівнянні з популярною централізованою системою ця модель забезпечує більшу зручність і прозорість, що робить її привабливою як для студентів, так і для викладачів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A first look at blockchain-based decentralized applications [Електронний ресурс] / Wu, Kaidong; Ma, Yun; Huang, Gang; Liu, Xuanzhe. – 2021. – Режим доступу до ресурсу: https://www.semanticscholar.org/paper/A-first-look-at-blockchain%E2%80%90based-decentralizedWuMa/300393bc8c0684bfb2f31be579055941fcea792a
2. Bitcoin: A Peer-to-Peer Electronic Cash System [Електронний ресурс] / Satoshi Nakamoto. – 2008. – Режим доступу до ресурсу: https://bitcoin.org/bitcoin.pdf
3. Blockchain Education Companies Earning Straight A's [Електронний ресурс] / Sam Daley. – 2019. – Режим доступу до ресурсу: https://builtin.com/blockchain/blockchain-education
4. Create Your Blockchain DApp with Ethereum and VueJS [Електронний ресурс] / Daniele Havi. – 2019. – Режим доступу до ресурсу: https://www.danielefavi.com/blog/create-your-blockchain-dapp-with-ethereum-and-vuejs-part-1/
5. Ethereum Solidity + Vue.js Tutorial [Електронний ресурс] / Hayata Satomi. – 2019. – Режим доступу до ресурсу: https://medium.com/openberry/ethereum-solidity-vue-js-tutorial-simple-auction-dapp-within-10-minutes-76ba48156b2
6. Ethereum Whitepaper [Електронний ресурс] / Vitalik Buterin. – 2014. – Режим доступу до ресурсу: https://ethereum.org/en/whitepaper
7. Hashcash – A Denial of Service Counter-Measure [Електронний ресурс] / Adam Back. – 2002. – Режим доступу до ресурсу: http://www.hashcash.org/hashcash.pdf
8. information systems perspective. Int. J . Inf. Manag. 2019. № 47. P. 88–100.
9. Ismagilova E., Hughes L., Dwivedi Y. K., Raman K. R. Smart cities: Advances in research – An
10. Jangirala S., Chakravaram V. Authenticated and Privacy Ensured

Smart Governance Framework for

11. Most Used Blockchain tools In 2022 For Blockchain Development [Електронний ресурс] / upGrad. – 2021. – Режим доступу до ресурсу: https://www.upgrad.com/blog/top-blockchain-tools/

12. PwC’s Global Blockchain Survey 2018 [Електронний ресурс] / PwC. – 2018. – Режим доступу до ресурсу: https://theblockchaintest.com/uploads/resources/PwC%20-%20Global%20Blockchain%20Survey%202018%20-%202018.pdf

13. Smart City Administration. ICCCE: Springer Singapore, 2020. P. 931–942.

14. The Role Of Blockchain In Web 3.0 [Електронний ресурс] / Diego Geroni. 2021. – Режим доступу до ресурсу: https://101blockchains.com/blockchain-in-web-3-0/

15. Tools to Know as a Blockchain Developer [Електронний ресурс] / Ruby Goyal. – 2022. – Режим доступу до ресурсу: https://geekflare.com/finance/blockchain-development-tools/

16. Treiblmaier H., Rejeb A., Strebing A. Blockchain as a Driver for Smart City Development: Application Fields and a Comprehensive Research Agenda. Smart Cities. 2020. № 3. P. 853–872.

17. YASHCHYK Oleksandr. The Impact of the Informatization of Society on the Labor Market / Valentyna SHEVCHENKO , Viktoriia KIPTENKO , Oleksandra RAZUMOVA , Iryna KHILCHEVSKA , Maryna YERMOLAIEVA // Postmodern Openings ISSN: 2068-0236 | e-ISSN: 2069-9387 – 2021, Volume 12, Issue 3Sup1, Pages: 155–167. DOI: https://doi.org/10.18662/po/12.3Sup1/357

18. Ніколіна І. І., Гулівата І. О. Моделювання кіберзлочинності як загрози цифровізації економіки. Комп’ютерно-інтегровані технології: освіта, наука, виробництво. 2020. № 39. С. 190–196.