МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ВАСКОВЕЦЬ ВАДИМ МИКОЛАЙОВИЧ

Допускається до захисту:
В.о. завідувача кафедри
інформаційних технологій
канд. техн. наук, доцент
_____ Оксана ЗЕЛІНСЬКА
«_____» _____ 2024р.

ДОСЛІДЖЕННЯ БЛОКЧЕЙНУ ЗА ДОПОМОГОЮ ЕКСПЕРТНОЇ СИСТЕМИ

Спеціальність 122 Комп’ютерні науки
Кваліфікаційна (магістерська) робота

Науковий керівник:
Є. Є. Федоров, професор кафедри
інформаційних технологій
д-р техн. наук, професор

Оцінка: _____/_____/_____
(бали/за шкалою ЄКТС/за національною шкалою)
Голова ЕК: _____
(підпис)

Вінниця 2024

АНОТАЦІЯ

Васковець В.М. Дослідження блокчейну за допомогою експертної системи. Спеціальність 122 Комп'ютерні науки, освітня програма «Комп'ютерні технології обробки даних». Донецький національний університет імені Василя Стуса, Вінниця, 2024.

У кваліфікаційній роботі проведено дослідження використання технології розподіленого реєстру (блокчеій) з використанням експертної системи у різних галузях таких як економіка, фінансовий та банківський сектор, логістика, навчання, тощо. Об'єктом дослідження є технологія розподіленого реєстру – блокчейн і методи її реалізації у сфері навчання.

Ключові слова: розподілена база даних, освіта, блокчейн, механізм консенсусу, шардінг, генерація розподіленої випадковості, старт-контракти.

ABSTRACT

Vaskovets V.M. Blockchain research using an expert system. Specialty 122 Computer Science, educational programme "Data Science". Vasyl' Stus Donetsk National University, Vinnytsia, 2024.

In the qualification work, a study of the use of distributed ledger (blockchain) technology was conducted using an expert system in various fields such as the economy, financial and banking sectors, logistics, education, etc. The object of the research is the distributed ledger technology - blockchain and methods of its implementation in the field of education.

Keywords: distributed database, education, blockchain, consensus mechanism, sharding, generation of distributed randomness, start-contracts.

ЗМІСТ

ВСТУП

Актуальність дослідження. В останні роки технологія блокчейн розвивалася дуже швидко. Ця технологія не тільки активно обговорюється, але й починає впроваджуватися в багатьох галузях промисловості більшості розвинених країн. Метою багатьох організацій є розуміння можливих застосувань технологій для пошуку шляхів розвитку різних галузей промисловості та оптимізації поточних процесів. Потенціал цієї технології буде поступово з'являтися протягом наступних 5-10 років, але за останні кілька років проекти з використанням цієї технології були реалізовані в різних сферах, головним чином у фінансовій галузі. Використання технологій відкриває нові можливості для бізнесу та принципово оптимізує поточну діяльність підприємств і банків.

Існуючі приклади застосування технології доводять, що темпи її розвитку зростають експоненціально, а разом з цим і попит на фахівців у різних сферах діяльності. Розподілені блокчейн бази даних все більше інтегруються в системи зберігання та контролю документів. Перевага цього методу полягає в тому, що немає реальної можливості маніпулювати даними, записаними в системі, оскільки інформацію можна лише додати до бази даних, а не перезаписати. При цьому справжність документа легко перевірити, оскільки кожен бачить, хто його записав у блокчейн. Як і у випадку з фізичними особами та банківською справою, технології не оминули систему освіти. Доречним є опис самої технології, а також застосування рішення в розподіленому навчальному реєстрі. Динамічний моніторинг вимог підприємства до кандидатів зі знанням технології блокчейн, а також зростаюча популярність масових відкритих онлайн-курсів та онлайн-освіти дозволяють освітнім організаціям легко адаптуватися до тенденцій у сфері освіти та в їхніх (конкретних освітніх університетських організаціях, студенти та бізнес) встановлює непосередницькі відносини між ними та працює як єдина система через реєстрацію в блокчейні.

Метою дослідження є удосконалення методики впровадження технології блокчейн за допомогою експертних систем для подальшого застосування у сфері освіти.

Для досягнення цієї мети необхідно виконати наступні завдання:

- Проаналізувати технологію блокчейн.
- Провести дослідження алгоритмів, які використовуються у цій технології.
- Розглянути приклади впровадження технології блокчейн в освіту.
- Проаналізувати, як створюється та працює технологія блокчейн.
- Провести порівняльний аналіз існуючих методів, виявити недоліки та запропонувати альтернативні методи зберігання та передачі інформації, які є максимально надійними.

Об'єктом дослідження є технологія розподіленої книги-блокчейн.

Предмет дослідження – методи впровадження технології блокчейн у сферу освіти.

Методи дослідження – методи впровадження технології блокчейн в освіту, порівняння алгоритмів за критеріями безпеки, надійності, масштабованості та доцільності використання.

Новизна отриманих результатів полягає в тому, що швидкість, надійність та енергоефективність блокчейну забезпечуються масштабованою генерацією випадковості та модифікацією шардингу консенсусним протоколом з використанням багатофункціональних підписів.

РОЗДІЛ 1
ПОСТАНОВКА ЗАДАЧІ ДОСЛІДЖЕННЯ. ІСТОРІЯ РОЗВИТКУ ТЕХНОЛОГІЇ БЛОКЧЕЙН ТА ЕКСПЕРТНИХ СИСТЕМ

1.1 Еволюція технології блокчейн

Одну з перших ідей технології блокчейн було сформовано та викладено ще наприкінці XX сторіччя. Вона належала фізику В.С. Сторнетта та його колезі криптографу С. Хаберу, які працювали у дослідницькому центрі Bellcore. Їхня діяльність була спрямована на побудову криптографічно безпечного архіву, який би надавав спосіб зберігання записів, не розкриваючи при цьому їхній зміст.

В 1991 році вони розповіли про своє відкриття у статті «How to Time-Stamp a Digital Document», що була опублікована в журналі, присвяченому криптографії. Технологія називалась блокчейном, тому що розподілена електронна книга зберігає елементи даних у цифрових групах із часовими позначками, що називаються блоками. Кожен блок містить буквено-цифровий код, що називається «хеш», і підсумовує свої дані. Хеш кожного завершеного блоку також з’являється в наступному блоці, це означає, що для зміни одного блоку потрібно змінити також і всі пов’язані з ним. Ці криптографічні «доміно» функціонують разом для захисту від підроблень та шахрайства.

У системі було використано криптографічно пов’язану низку блоків для зберігання документів із позначкою часу, а у 1992 році в розроблення було включено «дерева Меркла», що зробило її ефективнішою, дозволивши збирати декілька документів в один блок. Проте впровадження цієї технології так і не відбулося.

В 2004 році Гарольд Томас Фінні (Harold Thomas Finney II) запропонував систему із назвою Reusable Proof of Work (далі – RPoW). Система працювала, отримавши невзаємозамінний Hashcash-токен, заснований на proof-of-work і підписаний у RSA, котрий потім міг бути переданий від людини до людини. RPoW вирішила проблему подвійної витрати, зберігши право власності на токени, зареєстровані на довіреному сервері, що був розроблений із метою

надання можливості користувачам по всьому світу перевіряти його правильність та цілісність у режимі реального часу.

31 жовтня 2008 року о 14 годині 10 хвилин за нью-йоркським часом кількасот спеціалістів криптографії, включених до закритого списку розсилання, отримали на свої електронні адреси листа від невідомого, який назвав себе Сатоші Накамото. У листі містилось посилання на дев'яти сторінковий текст статті, у якій була описана однорангова електронна мережа, призначена для прямих онлайн-платежів від однієї сторони до іншої без проходження через фінансові установи, і в якій було вирішено проблему подвійних витрат. Цю мережу було названо біткоїном. Примітно, що стаття містила у списку використаної літератури всього вісім джерел, три з яких за авторством Хабера та Сторнетта.

Основні властивості: Подвійні витрати запобігаються за допомогою пірингової мережі. Відсутність монетного двору чи інших довірених сторін. Учасники можуть бути анонімними. Нові монети зроблені з доказів роботи в стилі Hashcash. Доказ роботи для генерації нових монет також живить мережу для запобігання подвійних витрат.

Повністю пірингова версія систем електронних грошей дозволяє надсилати онлайн-платежі безпосередньо від однієї сторони до іншої, оминаючи фінансову установу. Електронний підпис частково вирішує цю проблему, але більша частина переваг втрачається, коли довірена третя сторона (посередник) повинна уникати подвійних витрат. Ми пропонуємо вирішення проблеми подвійних витрат шляхом використання однорангових мереж. Така мережа буде фіксувати час транзакцій і хешувати їх у безперервний ланцюжок доказів виконання роботи. Це створює запис, який неможливо змінити без повторного запуску всього ланцюжка обчислень. Найдовший ланцюжок не тільки слугує доказом послідовності подій, але й вказує на те, що він був створений найбільшим сегментом обчислювальних потужностей системи. Якщо більшість обчислювальних потужностей контролюється парними вузлами, вони генерують найдовший ланцюжок обчислень і випереджають вузли-атакувальники.

Структура самої мережі дуже проста. Повідомлення надсилаються за схемою негарантованої доставки, і всі вузли можуть покинути мережу або приєднатися до неї в будь-який момент, приймаючи найдовший ланцюжок і відновлюючи історію транзакцій у разі своєї відсутності. Мережа біткоїн була першою практичною реалізацією мережі блокчейн у сучасному розумінні цієї технології. Від часу її запуску минуло понад 10 років. За цей період технологія блокчейн значно еволюціонувала та пройшла декілька етапів, так званих поколінь: Блокчейн 1.0, Блокчейн 2.0 і Блокчейн 3.0.

Блокчейн, на якому була реалізована мережа біткоїн, належить до покоління Блокчейн 1.0 – пірингової децентралізованої електронної мережі, що призначена для прямого обміну віртуальними грошима (криптовалютою). Незважаючи на «революційність» технології, Блокчейн 1.0 має суттєві обмеження: труднощі інтеграції із зовнішніми системами, порівняно низьку пропускну здатність, вузькість практичного застосування. Головне призначення Блокчейну 1.0 полягає у використанні його як платіжної системи, в якій нема посередників, а об’єктами операцій виступають віртуальні валюти (криптовалюти).

Особливість Блокчейну 2.0 полягає в інтеграції моделі розумних контрактів. Розумний контракт становить цифровий протокол, що автоматично виконує заздалегідь визначені процеси транзакції та не потребує участі третьої сторони (наприклад, банку). По суті, мережі блокчейн покоління 2.0 є блокчейн-платформами для створення та реалізації розумних контрактів.

Блокчейн 3.0 – це етап розвитку технології зі здійсненням подальшого проробления концепції розумного контракту із метою створення децентралізованих, автономних організаційних одиниць, що керуються власними законами та діють практично автономно.

Так, технологія блокчейн, як і будь-яка інша технологія у світі, постійно еволюціонує, розширюючи при цьому спектр свого застосування та інтеграції.

Незважаючи на понад 10-річну історію, на сьогодні блокчейн є однією з найпопулярніших, цікавих та перспективних технологій від моменту появи Інтернету. При цьому зростання популярності технології почалося у 2013 році, про що можна стверджувати, спираючись на статистику Google Trends, згідно з якою значне збільшення кількості запитів за словом Blockchain відбулося в 2013 році. А пік популярності було зафіксовано у грудні 2017 року. Цікаво, що графік статистики таких запитів висококорельований із графіком капіталізації ринку віртуальних валют. Зазначені графіки відображено на рис. 1. Усе це в цілому демонструє динаміку інтересу до технології блокчейн.

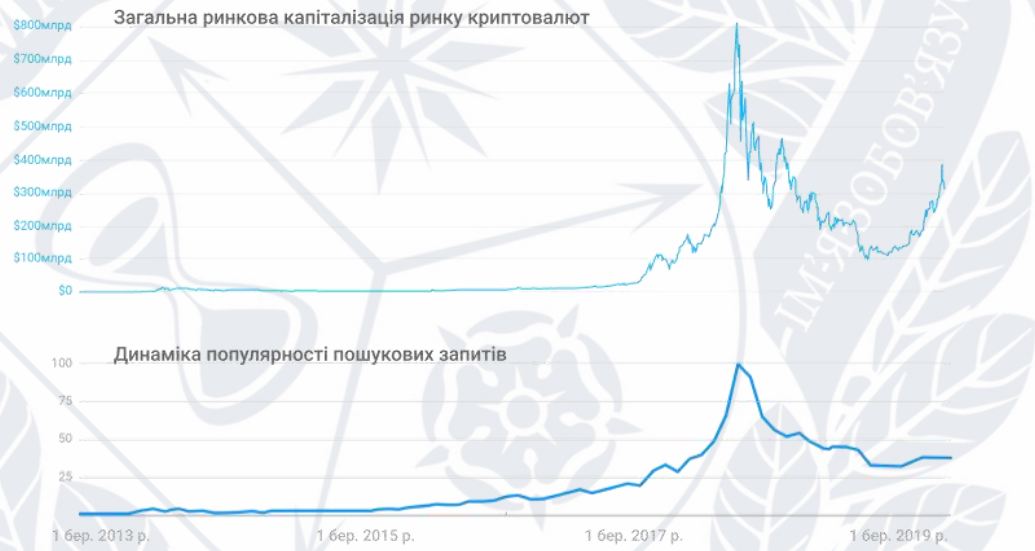

Рисунок 1.1 – Графіки, що свідчать про інтерес до технології блокчейн

Таку динаміку інтересу можна відобразити умовним «індексом інтересу до технології блокчейн», який буде візуалізацією, отриманою за результатом віднайденого середньозваженого між нормованими за віссю ординат графіками, наведеними на рис 1.1. Графік «Індекс інтересу до технології блокчейн» відображено на рис. 1.2.

Рисунок 1.2 – Графік «Індекс інтересу до технології блокчейн»

Розвиток будь-якої технології та інтерес до неї суспільства є циклічними процесами. Такий цикл було виявлено фахівцями компанії Gartner, Inc. на основі проведених досліджень, результати яких показали, що кожен етап розвитку інноваційної технології характеризується певним рівнем «інформаційного сплеску» навколо такої інновації. У результаті компанією була запропонована модель для прогнозування та аналізу тенденцій, пов'язаних із появою нових технологій. Модель показує, наскільки перспективною є конкретна технологія на основі ступеня зацікавленості в ній суспільства та фахівців. Така модель розвитку та впровадження технології отримала назву «Цикл зрілості технології», або Hype cycle. Як показано на рис. 1.3, цикл можна зобразити на графіку кривою, на якій позначено кожен етап розвитку технології. На осі Час відображаються етапи у часі, які проходить технологія, на осі Очікування – рівень очікувань від неї.

Рисунок 1.3 – Графік циклу зрілості технології

Будь-яка технологія проходить етапи своєї «зрілості» – від зародження до стабільного комерційного впровадження:

Інноваційний тригер (Innovation Trigger). У середовищі фахівців починається обговорення, у результаті чого у громадській пресі з'являються публікації з описом та обґрунтуванням концепції технології. Цей період характеризується початком просування інноваційної ідеї.

Пік завищених очікувань (Peak of Inflated Expectations). Технологія стає надзвичайно популярною та предметом широкого обговорення у суспільстві. З'являються перші компанії, що намагаються впровадити технологію, переважно невдалі, проте завдяки новизні технологія стає популярною та викликає часті й активні обговорення у суспільстві.

Прірва розчарування (Trough of Disillusionment). Унаслідок вияву недоліків технології в суспільстві з'являється розчарування нею, пов'язане з невідповідністю очікуванням.

Схил просвіти (Slope of Enlightenment). Ефективний пошук рішень уразливих місць технології дозволяє усунути її головні недоліки. З'являються перші комерційні впровадження, при цьому формується середовище постійних користувачів. Після успішних практичних застосувань зацікавленість суспільства починає підвищуватися.

Плато продуктивності (Plateau of Productivity). Технологія заслужено посіла своє місце на ринку та приймається вже не як нова, а як міцно усталена. Суспільство сприймає технологію як даність, усвідомлюючи її реальні недоліки та переваги.

Важливим моментом є те, що на кожному з етапів розвиток технології може сповільнюватись, а також тимчасово або назавжди зупинитись.

Для технології блокчейн, як і для будь-якої іншої інновації, також характерна вищезазначена модель. Перший етап циклу зрілості технології блокчейн припадає на період з 2008 по 2014 рік:

- зародження технології;
- запуск першої блокчейн-мережі;

- використання технології для краудфандингу та краудінвестингу – поява ICO;
- перші проекти на блокчейні;
- поява криптобірж;
- перші атомарні транзакції.

Так можна в цілому охарактеризувати інноваційний тригер технології блокчейн. Піком завищених очікувань для технології блокчейн можна вважати період з 2014 до початку 2018 року. Цей етап у циклі зрілості технології блокчейн характеризується створенням мереж блокчейн нового покоління та появою перших блокчейн-платформ, спробами інтеграції технології в різні сфери життя та першими законодавчими ініціативами, пов'язаними з її використанням. Потрібно зазначити, що максимальний інтерес до технології було зафіксовано у другій половині 2017 – на початку 2018 року. На цей час припадає пік ICO та інформаційний сплеск навколо блокчейну. Популярність технології та інтерес до неї були такими великими, що навіть додання одного слова «блокчейн» до назви компаній приводило до злету вартості їхніх акцій. Так, британська компанія On-line Plc, що працює у напрямі інвестування в розроблення та використання інтернет-контенту, вирішила зробити ребрединг та додала до своєї назви слово «блокчейн», перейменувавшись в On-line Blockchain Plc. У результаті її акції за день зросли на 394%. Компанія Long Island Iced Tea Corporation, яка спеціалізується на виробництві та постачанні бутильованого холодного чаю, додала до назви слово «блокчейн», що привело до початкового зростання акцій на новинах на 500%.

Услід за піком завищених очікувань цілком закономірно йде прірва розчарування. Для технології блокчейн цей етап циклу зрілості характеризує період 2018 – початок 2019 року. Посилення критики ICO та криптовалют, «здування пузиря» ICO, обвал ринку криптовалют, закриття низки криптобірж, жорсткішість регулювання з боку державних органів та зростання скептицизму й обережності щодо технології. Показовим прикладом може бути аналогія з

технологією інтернет в аспекті цього етапу в циклі зрілості технологій, зокрема з «пузирем доткомів».

2019 рік для технології блокчейн є початком етапу схилу просвіти. Технологія знову набирає популярності по всьому світу: провідні світові банки, уряди та глобальні корпорації розглядають перспективи її застосування у різноманітних сферах від фінансових технологій до логістики, компанії у сфері блокчейну пропонують нові рішення та тестують продукти на реальних прикладах. Навчальні заклади починають пропонувати різні спеціалізації у сферах блокчейну. Згідно з дослідженням, проведеним Coinbase та дослідницькою фірмою Qriously, 21 з 50 провідних університетів світу пропонують хоча б один курс, пов’язаний із блокчейном.

Цікаво, що між індексом інтересу до технології блокчейн і кривою її циклу зрілості можна побачити наочний взаємозв’язок, який можна простежити, зіставивши криві на рис. 1.4.

Рисунок 1.4 – Взаємозв’язок між циклом зрілості технології та інтересом до технології блокчейн

Високий ступінь кореляції кривих дає можливість розглядати інтерес до технології блокчейн як своєрідний індикатор. Показники такого індикатора

підтверджують світові тенденції розвитку технології блокчейн і свідчать про початок етапу схилу просвіти циклу зрілості технології.

Здається цікавим той факт, що різниця між першою статтею, присвяченою майбутній технології інтернет, і першою статтею, присвяченою майбутній технології блокчейн, становить рівно 30 років. При цьому інтернету від часу перших згадувань про майбутню технологію знадобилось 39 років для досягнення піку завищених очікувань у циклі зрілості технології, а блокчейну – всього 27 років.

Показовим також буде продемонстроване на рис. 1.5 зіставлення графіка фондового індексу NASDAQ Composite, що обчислюється на основі вартості акцій високотехнологічних компаній, і графіка «Індекс інтересу до технології блокчейн».

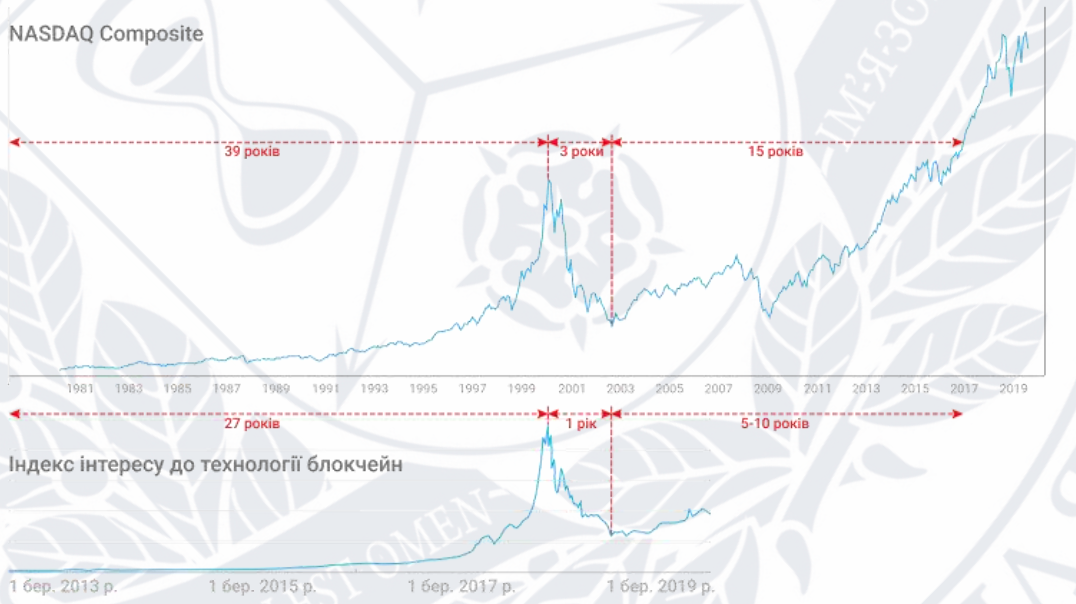

Рисунок 1.5 – Графіки, що свідчать про високий ступінь схожості в динаміці розвитку технологій

Як видно з рис. 1.5, ці графіки мають високий ступінь кореляції. На підставі наведеної вище логіки графіки можна використовувати як індикатори, показники яких порівнянні з циклом зрілості відповідних технологій. Окремо

варто зазначити, що технологія блокчейн значно швидше проходить етапи циклу зрілості, ніж технологія інтернет.

1.2 Класифікація блокчейнів

За своєю суттю блокчейн є розподіленою базою, у якій запис усіх змін здійснюється у вигляді низки блоків. Водночас сама структура блокчейну припускає різні рівні доступу до інформації. Цей параметр використовується як критерій для класифікації блокчейнів, що має умовний характер, тому що принцип технології блокчейн є при цьому єдиним.

Так, на основі цього критерію є кілька версій класифікації блокчейнів: канадська, британська та російська.

Канадська версія ґрунтується на баченні засновника блокчейн-платформи Ethereum канадця Vitaly Buterin. Його класифікація припускає наявність 3 видів блокчейну:

Public blockchain (публічний блокчейн) – це низка блоків, яку може «прочитати» будь-яка людина у світі. Також будь-яка людина може відправляти транзакції, очікувати їхнього включення, якщо вони дійсні, та брати участь у процесі консенсусу (процесі для визначення, які блоки додаються до низки та який поточний стан мережі). У якості заміни централізованої або квазіцентралізованої довіри публічні низки блоків захищені комбінацією економічних стимулів та криптографічної перевірки з використанням таких механізмів, як proof-of-work або proof-of-stake, згідно з принципом, відповідно до якого ступінь впливу учасників у процесі консенсусу пропорційна кількості економічних ресурсів, які вони можуть використовувати. Ці блокчейни зазвичай вважаються повністю децентралізованими.

Consortium blockchain (блокчейн консорціуму) – це блокчейн, у якому процес погодження контролюється заздалегідь вибраним набором вузлів. Наприклад, можна уявити консорціум із 15 фінансових установ, кожна з яких керує вузлом і 10 з яких мають підписати кожен блок, щоб він був дійсним. Право

на читання блокчейну може бути загальнодоступним або обмеженим для учасників. Такий блокчейн можна вважати «частково децентралізованим».

Fully private blockchain (повністю приватний блокчейн) – це блокчейн, що характеризується обмеженим рівнем доступу до даних. Підтвердження транзакцій у таких мережах, проведення аудиту, управління базами доступні чітко визначеному колу осіб. Якщо говорити про право на читання даних, то воно може бути як загальнодоступним, так і повністю обмеженим.

Британська версія заснована на доповіді головного наукового радника уряду Великобританії Mark Walport. У своїй доповіді Distributed Ledger Technology: beyond block chain із розподілених реєстрів та потенціалу блокчейну в сфері державного управління він поділив блокчейн на 3 види:

1. Unpermissioned public ledgers – відкриті публічні реєстри.
2. Permissioned public ledgers – закриті публічні реєстри.
3. Permissioned private ledgers – частково закриті реєстри.

Ця класифікація ідентична тій, що наводив Vitaly Buterin, та в ній аналогом Public Blockchain у британській версії є Unpermissioned public ledgers, аналогом Consortium Blockchain – Permissioned public ledgers, а аналогом Fully private Blockchain – Permissioned private ledgers. До того ж, у доповіді було запропоновано невеликий тест «Класифікація розподілених реєстрів», що дозволяє самостійно визначати, до якого виду належить той чи інший блокчейн. Цей тест відображено на рис. 1.6.

Рисунок 1.6 – Класифікація розподілених реєстрів

Російська версія поділяє блокчейни на 3 види – відкриті, закриті та гібридні. У відкритій мережі учасники не проходять реальної ідентифікації, допуск до мережі не обмежений, статус процесорів не закріплений за конкретними учасниками та нема ніяких видимих інстанцій, що керують правилами. Якщо говоримо про закриту мережу, то вона організована практично з точністю до навпаки: учасники мережі ідентифіковані, допуск до участі в мережі обмежений і у нього є правила, статус процесорів закріплений за певними контрагентами та зазвичай є деякий орган, що ці правила встановлює, регламентує, змінює. Гібридна мережа – це мережа, що може поєднувати частини елементів із відкритої мережі та частини із закритої мережі.

Спираючись на вищенаведене, можна стверджувати, що бачення фахівців із різних країн щодо класифікації блокчейну дуже схожі й в основу такої класифікації покладено ступінь відкритості блокчейну для його учасників. Так, блокчейни можна поділити на дві великі групи – публічні та приватні. Ступінь публічності (відкритості) блокчейну може залежати від декількох факторів.

Перший – доступність вихідного коду протоколу блокчейну. Вихідні коди публічних блокчейнів зазвичай відкриті від самого початку розроблення та їх зміни ведуться на одному з найпопулярніших інтернет-ресурсів, наприклад, на GitHub. Блокчейни та платформи для корпоративного застосування (приватні блокчейни) можуть бути як із відкритим, так і з частково або повністю закритим вихідним кодом. Якщо розглядати блокчейн-розробки з точки зору їхнього застосування в державному секторі, то і кількість таких розробок та продуктів, використовуваних у реальних процесах, ще занадто мала. При цьому варто очікувати, що більшість таких блокчейнів також будуть закритими (приватними).

Другий та найважливіший показник – це можливість будь-якого користувача вільно під'єднуватися до мережі без отримання будь-яких дозволів. Саме це є визначальною відмінністю публічного блокчейну від приватного. Переважна більшість відомих на цей час блокчейнів є публічними – для під'єднання до них достатньо завантажити сумісний із поточною версією протоколу клієнтський програмний додаток та встановити зв'язок з іншими рівноправними вузлами мережі.

Щоб повноцінно брати участь у роботі мережі, зокрема, перевіряти та ретранслювати транзакції інших користувачів або брати участь у створенні блоків, потрібно запустити клієнтський програмний додаток із функціональністю повного вузла. В інших випадках досить клієнтського програмного додатка з обмеженими можливостями. Проте у публічних блокчейнах рівень участі користувача завжди визначається самостійно та залежить лише від його власних (фінансових або апаратних) ресурсів. Крім того, ніхто не може від'єднати користувача від розподіленої мережі, оскільки всі учасники публічного блокчейну рівноправні. В окремих випадках вони можуть, наприклад, ігнорувати або блокувати користувача, який розсилає некоректні транзакції або намагається передати інформацію, що не відповідає протоколу, але такі ініціативи мають суто саморегулятивний характер і не встановлюються на рівні протоколу.

У приватних блокчейнах за під'єднання до мережі нових користувачів, а також за можливість їхнього від'єднання можуть відповідати певні довірені вузли або групи вузлів, що мають вищий рівень повноважень порівняно з іншими користувачами. Приватні блокчейни становлять ієрархічні структури, що складаються з двох або більше рівнів. Пари ключів, що надають доступ до системи, видаються та керуються спеціальними адміністративними вузлами та за необхідності можуть бути відкликані. Отже, приватні блокчейни не повністю реалізують головні принципи технології – децентралізацію та рівноправність учасників, тому що для корпоративних систем їх наявність може бути зумовлена суттєвими ризиками.

Наступним критерієм, що створює ще один щабель у класифікації блокчейнів, є рівень управління блокчейнами. За даним критерієм блокчейни можна поділити на чотири групи:

1. Публічні децентралізовані блокчейни.
2. Публічні блокчейни з делегованим управлінням.
3. Приватні контрольовані блокчейни.
4. Державні блокчейни.

Більшість сучасних публічних блокчейнів мають однорівневу структуру. В них всі учасники рівноправні та консенсус досягається через опосередковане голосування вузлів, що виконують функції створення блоку. Публічні децентралізовані мережі не накладають якихось обмежень на участь в управлінні, а можливості учасників визначаються лише часткою їхніх ресурсів від загальної кількості.

За понад десятирічну історію розвитку блокчейну можна зробити висновок, що повна децентралізація в саморегульованих, а точніше стихійно регульованих, мережах на практиці майже неможлива – усі публічні блокчейни рано чи пізно стикаються з однією з форм централізації. У зв'язку з цим була зроблена спроба упровадження елементів централізації для покращення функцій управління та інших показників блокчейну. Це привело до того, що в 2015 році виникли перші публічні блокчейни з дворівневою структурою, де провідну роль

виконували вузли з розширеними повноваженнями. Саме ознака наявності двох та більше рівнів управління у мережі блокчейн, із різним ступенем повноважень для кожного, є головною для публічних блокчейнів із делегованим управлінням.

Приватні контрольовані (корпоративні) блокчейни є технологічними рішеннями для корпоративних потреб. У таких системах кожен вузол має заздалегідь призначений йому рівень доступу та, на відміну від публічного блокчейну, дані не завжди загальнодоступні навіть для читання. Управління в таких блокчейнах здійснюється за допомогою спеціальних вузлів, що мають підвищені повноваження, саме вони відповідають за політику розповсюдження даних та ідентифікацію користувачів, а також засвідчують внесення даних до блокчейну.

Розподілені реєстри для державного застосування в цілому незначно відрізняються від корпоративних блокчейнів і також потребують контрольованого доступу до інформації. Проте у державних відомств є особливі вимоги до блокчейну – максимальний рівень незмінюваності вже доданої інформації та найсуворіший контроль над її додаванням. Водночас інформація, що вже міститься у блокчейні, у багатьох випадках може бути публічною, оскільки державні органи мають прагнути до підвищення прозорості своєї роботи. Так, можна сказати, що державні блокчейни становлять окремий випадок корпоративних блокчейнів зі своїми специфічними особливостями, але водночас належать до окремої групи.

Отже, класифікацію блокчейну, засновану на рівні доступу до інформації, можна уявити у вигляді дворівневої структури, у якій перший рівень визначає критерій публічності, а другий – рівень управління блокчейну. Графічно ця структура відображена на рис. 1.7.

Рисунок 1.7 – Класифікація блокчейнів

Підводячи підсумок розгляду технологічних аспектів блокчейну, потрібно зазначити, що його варто сприймати як нову технологічну парадигму. Технологія акумулює декілька концептуально різних ідей: розподілені реєстри зберігання даних, алгоритми консенсусу та криптографічні механізми захисту даних. Технологія блокчейн ґрунтується на логіці зберігання даних, що не залежить від централізованого сервера чи групи серверів. Технологія формує та зберігає список упорядкованих записів, що називаються блоками. Кожен блок містить позначку часу та, що дуже важливо, унікальний образ (хеш) попереднього блоку, таким чином технологія «пов’язує» блоки даних, виключаючи можливість їх зміни у сформованих блоках без зміни усієї послідовності блоків.

1.3 Експертна система

Експертна система (ЕС) – це інтелектуальна система, призначена для вирішення слабо формалізованих задач, на основі накопиченого в базі знань досвіду роботи експертів в проблемній області. Вона містить базу знань з набором правил і механізмом виводу, і дозволяє, на підставі наданих користувачем фактів, розпізнати ситуацію, поставити діагноз, сформулювати рішення або дати рекомендацію для вибору дії.

Експертні системи призначені для відтворення досвіду, знань професіоналів високого рівня і використання цих знань в процесі управління.

Вони розробляються з використанням математичного апарату нечіткої логіки для експлуатації у вузьких областях застосування, оскільки їх використання вимагає великих комп'ютерних ресурсів для обробки і зберігання знань. В основі побудови експертних систем лежить база знань, яка ґрунтується на моделях представлення знань. У святи з великими фінансовими і часовими витратами у вітчизняних економічних ІС експертні системи не мають великого поширення.

Вважається, що будь-яка експертна система – це система, заснована на знаннях, але остання не завжди є експертною. У системах, заснованих на знаннях, правила (або евристики), за якими вирішуються проблеми в конкретній предметній області, зберігаються в базі знань. Проблеми ставляться перед системою у вигляді сукупності фактів, що описують деяку ситуацію, і система за допомогою бази знань намагається вивести висновок з цих фактів.

Система функціонує в наступному циклічному режимі: вибір (запит) даних або результатів аналізів, спостереження, інтерпретація результатів, засвоєння нової інформації, висунення за допомогою правил тимчасових гіпотез і потім вибір наступної порції даних або результатів аналізів. Такий процес продовжується до тих пір, поки не надійде інформація, достатня для остаточного висновку.

Простіші системи, засновані на знаннях, функціонують в режимі діалогу, або режимі консультації. Після запуску система задає користувачеві ряд питань про розв’язуваної задачі, які потребують відповіді «так» чи «ні». Відповіді служать для встановлення фактів, за якими може бути виведено остаточний висновок.

У будь-який момент часу в системі міститься три типи знань:

- структуровані статичні знання про предметну область, після того як ці знання виявлені, вони вже не змінюються;
- структуровані динамічні знання – змінні знання про предметну область; вони оновлюються у міру виявлення нової інформації;
- робочі знання, що застосовуються для вирішення конкретного завдання або проведення консультації.

Всі перераховані вище знання зберігаються в базі знань. Для її побудови потрібно провести опитування фахівців, які є експертами в конкретній предметній області, а потім систематизувати, організувати і забезпечити ці знання покажчиками, щоб згодом їх можна було легко витягти з бази знань.

Формалізацією знань експерта і поданням їх в БЗ займаються інженери знань (когнітологи, аналітики). Створює ЕС програміст.

ЕС повинна володіти механізмом придбання знань для введення знань у базу і їх подальше оновлення. У простому випадку – це інтелектуальний редактор, який дозволяє вводити одиниці знань в базу, а також проводити їх аналіз на несуперечливість.

Галузі застосування ЕС– це прогнозування, планування, контроль і управління, навчання. ЕС є інструментом, що підсилює інтелектуальні здібності всієї системи в цілому, і виконує такі завдання:

1) консультація для недосвідчених (непрофесійних) користувачів;
2) допомога при аналізі різних варіантів прийняття рішення;
3) допомога з питань, що належать до суміжних областей діяльності.

Найбільш широко і продуктивно ЕС застосовуються в бізнесі, виробництві, медицині, навчанні.

Засоби побудови ЕС

- універсальні мови програмування;
- інтелектуальні мови програмування;
- середовища програмування ЕС;
- оболонки ЕС.

Універсальні мови програмування, наприклад, С++. Інтелектуальні мови програмування, наприклад, Пролог, LIPS мають вбудовані механізми для маніпулювання знаннями. Пролог – мова програмування високого рівня, орієнтована на використання концепцій і методів математичної логіки. Вона призначена для програмування в термінах логіки. Мова LIPS дозволяє обробляти спискові структури.

Загальним недоліком використання мов програмування для створення ЕС є: тривалий час розробки ЕС, необхідність залучення висококваліфікованих програмістів, труднощі з модифікацією готової системи. Все це робить застосування мов програмування для реалізації ЕС досить дорогим і трудомістким.

Середовища програмування ЕС та оболонки ЕС являють найбільшу цікавість з точки зору розробника. Середовища програмування ЕС дозволяють розробникам не програмувати деякі або всі компоненти ЕС, а вибирати їх із заздалегідь складеного набору. При застосуванні оболонок ЕС розробник повністю звільняється від робіт зі створенім програм і займається лише наповненням бази знань.

Експертні системи відрізняються від інших додатків, оскільки вони мають такі характеристики:

Експертні системи моделюють механізми людського мислення, що беруть участь у вирішенні проблем у певній галузі. Це відрізняє експертні системи від математичного моделювання та комп'ютерної анімації. Однак експертна система не відтворює повністю психологічну модель експерта в певній галузі, але повинна відтворювати за допомогою комп'ютера деякі з методів вирішення проблем, які використовує експерт.

Система не тільки виконує обчислювальний процес, але й робить певні висновки на основі власних знань. Знання в системі зазвичай записані спеціальною мовою і зберігаються окремо від програмного коду, який генерує висновки. Компонент зберігання знань зазвичай називають базою знань.

Евристичні та апроксимаційні методи відіграють важливу роль у вирішенні проблем, але, на відміну від алгоритмічних методів, їх успіх не завжди гарантований. Евристики – це, по суті, емпіричні правила, які відображають знання, набуті людьми в механічній формі разом з накопиченням практичного досвіду вирішення подібних проблем. Такі методи є наближеними в тому сенсі, що, по-перше, вони не вимагають вичерпної початкової інформації, по-друге,

існує певний ступінь впевненості (або невпевненості) в тому, що запропоноване рішення є правильним.

Експертні системи також відрізняються від інших типів програм штучного інтелекту.

Експертні системи застосовуються до об'єктів реального світу, і їхня робота зазвичай вимагає великого людського досвіду. Експертні системи мають практичну спрямованість, використовуються в науковій або комерційній сферах. Однією з основних характеристик експертних систем є їхня продуктивність, тобто швидкість отримання результатів та їхня надійність. Дослідницькі застосування штучного інтелекту можуть бути не дуже швидкими, але експертна система повинна бути здатна знайти рішення за розумний час, яке не гірше, ніж рішення, які можуть надати експерти в цій галузі.

Експертна система повинна бути здатна пояснити, чому вона прийшла саме до такого рішення, і довести його обґрунтованість. Користувачеві повинна бути надана вся інформація, необхідна для того, щоб переконатися, що запропоноване рішення є правильним.

Відомі експертні системи

Для прикладу можна згадати такі відомі експертні системи:

CLIPS-мова програмування, що використовується для створення експертних систем.

Dendral - аналіз даних мас-спектрометрії.

Dipmeter Advisor - аналіз даних, отриманих під час розвідки нафти.

Jess-Java Expert System Shell, оболонка експертної системи на основі Java; рушій CLIPS реалізований на мові програмування Java і використовується для створення експертних систем.

MQL 4-MetaQuotes Language 4, спеціалізована мова програмування для опису фінансових стратегій.

Mycin-діагностика інфекційних захворювань крові та рекомендації щодо антибіотиків.

Пролог – мова програмування, що використовується для створення експертних систем.

R1/XCON(експертна система)-обробка замовлень.

Експертна система реального часу SHINE-Spacecraft Health INference Engine, для отримання даних про стан і безпеку космічних апаратів

STD Wizard-експертна система для рекомендації та вибору медичних тестів (діагностики)

Етапи розробки ЕС

Фаза ідентифікації проблеми – визначення завдань, які необхідно вирішити, визначення цілей розробки, визначення типів експертів та користувачів.

Етап вилучення знань – проводиться змістовний аналіз проблемної області, ідентифікуються поняття та їх взаємозв'язки, визначаються методи вирішення проблем.

Етап структуризації знань – вибираються ІС, визначаються способи представлення всіх типів знань, формалізуються базові поняття, визначаються способи інтерпретації знань, моделюються операції системи та оцінюється адекватність зафіксованих понять, рішень і засобів представлення та оперування знаннями цілям системи.

Етап формалізації - експерти наповнюють базу знань. Оскільки знання є основою ЕС, цей етап є найважливішим і найбільш трудомістким етапом розробки ЕС. Процес генерації знань можна розділити на отримання знань від експертів, організацію знань для забезпечення ефективної роботи системи та представлення знань у формі, зрозумілій для ЕС. Процес отримання знань здійснюється інженерами по знаннях шляхом аналізу діяльності експертів з вирішення реальних проблем.

Реалізація ЕС-створюється один або декілька прототипів ЕС, які вирішують проблему.

Етап тестування-оцінка обраних методів представлення знань в ЕС.

Переваги та недоліки експертних систем.

Експертні системи мають певні переваги у порівнянні з експертами-людьми. Зокрема, експертні системи можуть:

перевершувати людські здібності у вирішенні надскладних проблем;

не мають упереджень;

експерти використовують побічні знання і є більш чутливими до зовнішніх факторів;

не робити поспішних висновків і не нехтувати певними етапами пошуку рішення;

можуть працювати в інтерактивному режимі;

можуть працювати з інформацією, що містить символічні змінні;

може коректно обробляти інформацію, що містить помилки, використовуючи імовірнісні методи дослідження;

дозволяє одночасно опрацьовувати різні версії;

на вимогу пояснити хід виконання кроків програми;

надає можливість обґрунтовувати рішення та відтворювати метод прийняття рішень.

Однак, навіть найкращі з існуючих експертних систем мають певні обмеження у порівнянні з експертами-людьми, зокрема:

Більшість експертних систем не зовсім придатні для широкого використання. Більшість експертних систем не зовсім придатні для широкого використання. Багато експертних систем доступні лише експертам, які створили їхню базу знань. Тому необхідно паралельно розробляти відповідні користувацькі інтерфейси і надавати кінцевим користувачам відповідні режими роботи;

Навіть якщо після експертної сесії з'являються нові знання, "навички" системи не обов'язково "зростають";

Залишається проблема приведення знань, отриманих від експерта, у форму, що гарантує їх ефективне використання;

Експертні системи, як правило, не можуть набувати якісно нових знань, які не були передбачені при розробці, а тим більше здоровим глуздом. При

вирішенні проблеми люди-експерти зазвичай покладаються на інтуїцію та здоровий глузд за відсутності формальних методів або аналогій для вирішення цієї проблеми.

1.4 Постановка задачі

В рамках кваліфікаційної роботи необхідно провести дослідження технології блокченй з використанням експертної системи. В якості прикладу обрано задачу застосування технології блокчейн у сфері освіти. Для її дослідження необхідно виконати наступні підзадачі:

- проаналізувати технологію розподіленого реєстру;
- дослідити алгоритми створення технології;
- розглянути приклади реалізацій технології блокчейн у сфері навчання;
- провести аналіз методів створення та функціонування технології блокчейн;
- виконати порівняльний аналіз існуючих методів, виявити недоліки та запропонувати інші методи, максимально надійні для збереження та передавання інформації.

РОЗДІЛ 2
ТЕХНІЧНА СТОРОНА ПРОЄКТУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН З ВИКОРИСТАННЯМ ЕКСПЕРТНОЇ СИСТЕМИ

2.1 Використання технології блокчейн для створення освітнього середовища

У контексті сучасних тенденцій розвитку освіти в умовах переходу до цифрової освіти необхідно розглянути особливості використання технології розподілених баз даних. Дана технологія може бути використана для розв'язання як традиційних, так і інноваційних педагогічних завдань в освітньому процесі на різних уроках і рівнях.

Дана технологія заслуговує на увагу освітян і дослідників як варіант передових засад для пошуку нових ідей та оновлення існуючих загальноприйнятих методів і прийомів навчання в сучасній освітній практиці. Прикладом може слугувати використання інформаційних технологій і науки "інформатика" як освітніх інструментів, таких як штучний інтелект, віртуальна реальність, доповнена реальність і масові відкриті онлайн-курси (MOOCs). Використання "блокчейна" дає змогу розробляти нові освітні ресурси для шкіл, а також нові освітні курси для підготовки майбутніх учителів у контексті "цифрової освіти"[8].

Блокчейн виник як засіб передавання цінностей, насамперед фінансових, подібно до того, як Інтернет є засобом передавання даних, наприклад файлів та електронних листів. Блокчейн-це електронна система, здатна створювати широкий спектр додатків. Як і Інтернет, блокчейн має ті самі основні принципи роботи: децентралізацію та множинні копії історії. "Інтернет цінностей" – одна з найвдаліших метафор для опису технології розподілених книг.

Блокчейн, одна з основних технологій, що лежать в основі криптовалют, є електронною книгою, в якій записано історію всіх грошових переказів (записи називаються блоками, звідси і термін blockchain - "ланцюжок блоків"). Його

відмітною особливістю є те, що багато учасників мережі зберігають копії одночасно. Це відрізняє блокчейн від централізованих систем минулого.

У двох словах, блокчейн – це безперервний ланцюжок блоків, що містять інформацію, побудований за певними правилами. Однак, будучи вічним цифровим розподіленим цифровою журналом транзакцій, блокчейн може бути запрограмований на запис не тільки фінансових операцій, а й практично будь-яких цінностей (прав власності, освітніх сертифікатів і т. д.). Сама інформація, яку клієнт А відправляє клієнту В через блокчейн, може використовуватися як "монети" (тобто валюта),"підписи", "ліцензії" або інші цінності [9].

Технологія блокчейн, як і Інтернет, має вбудований захист від помилок. Зберігаючи однакові блоки інформації в мережі, блокчейн унеможливлює контроль над системою і дає змогу їй мати єдину точку відмови (центр). Головні переваги блокчейну – надійність і децентралізація. Кожен учасник має дублікат історії всіх транзакцій. Існує кілька галузей, де блокчейн може бути використаний і навіть необхідний. Приклади застосування блокчейн в освіті включають надання студентських кредитів, ідентифікацію студентів (для заселення в гуртожитки або роботи в бібліотеці), оплату освітніх послуг, розподіл студентських стипендій та виділення грантів [10].

Використання блокчейна в освіті тільки починається. Серед університетів, які проводили експерименти, що лягли в основу звіту Єврокомісії, - Массачусетський технологічний інститут, Відкритий університет Великої Британії, Університет Нікосії та кілька навчальних закладів Мальти. На думку авторів доповіді, життєздатність запропонованого сценарію залежить від готовності країн-членів ЄС регулювати і стандартизувати блокчейн. Державним органам рекомендується створити експертні комітети для підтримки інноваційних приватних компаній і впровадження рішень на основі блокчейна. Головна цінність технології блокчейн в освіті полягає в тому, що вона гарантує надійність і безпеку під час збору та зберігання інформації, тоді як самі записи можуть містити різні типи даних. Наприклад, блокчейн можна використовувати для зберігання інформації про іспити, дипломи та сертифікати, а також

відомостей про те, хто і коли їх проводив і видавав. Таким чином, паперовий документ втрачає свою унікальність, і будь-яка людина може негайно перевірити його достовірність і отримати завірену копію, не звертаючись до архіву організації, що видала документ. Елементами збереження можуть бути не тільки дипломи та свідоцтва про закінчення навчального закладу, а й інформація про проходження онлайн-курсів і складання тестів [11].

Невід'ємною частиною освітнього процесу є підсумкове оцінювання та сертифікація. За допомогою іспитів, кваліфікаційних тестів та інших освітніх заходів студенти демонструють результати навчання (знання, навички та компетенції).

Освіта – одна з найважливіших галузей для економічного розвитку країни та для розквіту нового технологічного світу загалом. Навчання в навчальному закладі, наприклад, дає людині необхідний досвід і набір навичок, які можуть гарантувати гідну зарплату та добробут. Для того щоб проаналізувати, що технологія розподілених реєстрів може запропонувати освіті, необхідно визначити й обмежити різні галузі освіти, які можна проаналізувати з точки зору впровадження технології.

По-перше, освіту необхідно розділити на університетську та відкриту, яка сьогодні представлена так званими масовими відкритими онлайн-курсами (MOOCs, massive open online courses тощо).

По-друге, у рамках університетської освіти має сенс розглядати, з одного боку, освітній процес та пов'язані з ним адміністративно-управлінські аспекти, а з іншого - документи про освіту та сертифікати відвідуваності, що є результатом освітнього процесу, разом із даними про ці документи за межами конкретного університету[12].

Платформи масових онлайн-курсів є природним середовищем для впровадження технології розподілених реєстрів в освітній сектор. Зовсім нещодавно група наукових розробників запустила проєкт DISCIPLINA 3 – блокчейн-платформу, що пов'язує студентів, навчальні заклади, викладачів і, в майбутньому, потенційних роботодавців. Використовуючи розподілену

бухгалтерську книгу, розробники прагнуть розв'язати проблему створення єдиної бухгалтерської книги, що фіксує успішність студентів на різних курсах, які пропонуються різними навчальними закладами, та створити об'єктивну й надійну систему оцінювання студентів, яка дасть змогу визначити знання, необхідні для тієї чи іншої посади. Це значно спростить пошук відповідних кандидатів для роботодавців залежно від знань, необхідних для тієї чи іншої посади.

У такій відкритій системі оцінок і рейтингів оцінці та рейтингу підлягає все, включно з відгуками та рейтингами за конкретними курсами та програмами, репутацією вишу та роботодавців, які використовують подібні реєстри.

Питання приватності вирішується тим, що в блок записуються тільки неперсональні хеші, а безпосередні досягнення студентів зберігаються в їхніх особистих кабінетах. Доступ роботодавців до системи платний.

Токени, що циркулюють у блокчейні DISCIPLINA, використовуються для оплати платних курсів і створення блоків у ланцюжку. Схожа поведінкова логіка можлива і в класичній університетській освіті, принаймні в рамках навчальних закладів, що беруть участь у Болонському процесі. Його головна особливість - єдина система кредитів, що нараховуються за освоєння конкретних дисциплін. Певна кількість кредитів з того чи іншого предмета може призвести до отримання ступеня бакалавра, магістра або доктора [13].

Уніфікація також спрямована на спрощення процедури нострифікації (процес визнання диплома країни під час вступу до вищого навчального закладу іншої країни) під час вступу до іншого університету для здобуття наступного ступеня або просто під час переведення з одного вищого навчального закладу до іншого. Однак питання перенесення залікових одиниць з однієї й тієї самої дисципліни в різних університетах досі вважається дуже складним. Це пов'язано з тим, що навіть якщо теми, що вивчаються в рамках конкретного предмета, повністю збігаються, якість викладання та кваліфікація викладачів можуть суттєво відрізнятися.

Можна значно спростити й автоматизувати деякі процеси, які залежать від викладачів, що й пропонують автори доповіді[14]. Автори пропонують створити децентралізований, розподілений реєстр на блокчейні, доступ до якого має бути забезпечено певним механізмом для реєстрації та ідентифікації осіб, які беруть участь у реєстрі. Передбачається, що основною одиницею інформації в реєстрі будуть оцінки учня, які, зрозуміло, мають бути зашифровані для захисту персональних даних.

При отриманні оцінки на іспиті кожному студенту присвоюється випадковий ідентифікаційний номер в інформації (різний для одного й того самого студента з різних дисциплін), який звіряється з його обліковим записом, доступ до якого студент може отримати за допомогою секретного ключа. Метадані такої "залікової" транзакції мають містити інформацію про виш, у якому складали іспит, кількість залікових одиниць, кількість годин, список пройдених тем і будь-які інші необхідні дані. Якщо сталася помилка, організація повинна створити нову транзакцію, щоб вказати причину і скорегувати оцінку. Усі метадані слугують основою для створення смарт-контрактів.

Наприклад, якщо студент переводиться з одного навчального закладу до іншого і обидва навчальні заклади погоджуються приймати один в одного заліки з певних дисциплін, це фіксується у смарт-контракті. Таким чином, під час переведення студента до нового навчального закладу зарахування дисциплін і складання індивідуального навчального плану відбувається автоматично з урахуванням дисциплін, уже пройдених в іншому навчальному закладі, внаслідок перевірки їхньої відповідності вимогам, установленим у такому мережевому смарт-контракті. У майбутньому така система, що ґрунтується на технології розподілених книг, значно спростить переміщення кваліфікованих студентів, підвищивши тим самим мобільність населення як на національному, так і на міжнародному рівні, а також забезпечить облік усіх досягнень студентів у захищеному від злому реєстрі та постійні відстеження й перевірку опанування всіх дисциплін, що уможливить отримання диплома випускником. Процес видачі атестатів стане більш прозорим.

Експерти запропонували проєкт блокчейн-платформи для обліку наукових дисертацій[15]. Пропоноване рішення, засноване на розробці блокчейн-платформи Hyperledger Fabric, є закритим децентралізованим реєстром, учасниками якого мають стати великі міжнародні університети, дослідні та наукові центри, науково-дослідні інститути та видавництва. Насамперед автори вбачають потенціал блокчейна в цій галузі як ефективного інструменту для побудови процесів рецензування, перевірки посилань на джерела в реєстрі та створення простої децентралізованої системи розрахунку коефіцієнтів цитованості авторів. Останнє також пов'язано з можливістю створення прозорого механізму оцінювання якості наукових статей та їхньої значущості для наукового співтовариства загалом. Нині як основне джерело індексів цитування використовується Google Scholar, який є непрямим показником значущості тієї чи іншої публікації або внеску дослідника. Однак механізм роботи цього сервісу непрозорий, і немає впевненості в тому, що алгоритм, по-перше, знаходить усі цитати, а по-друге, індексує роботи всіх авторів. Створення аналогічного сервісу на основі децентралізованого реєстру дало б змогу подолати обмеження наявних сервісів, надавши можливість об'єктивно оцінити діяльність академічних співробітників.

2.2 Реалізація технології блокчейн

Для того щоб зрозуміти потенціал впровадження технології блокчейн, необхідно розглянути кілька основних визначень.

Транзакція: процес передачі даних у блокчейні. Для транзакцій у мережі потрібен вхід (адреса) для надсилання даних, вихід (адреса) для надсилання даних і електронний цифровий підпис (ЕЦП) для підписання транзакції.

Вузол: будь-який комп'ютер, що підтримує роботу блокчейна за протоколом P2P, вважається вузлом. Існує кілька типів вузлів у блокчейні:

- Вузли консенсусу: підтверджують транзакції і додають нові блоки відповідно до правил, встановлених консенсусом мережі;

- Вузли аудиту або повні вузли: постійно під'єднані до мережі та відповідають за зберігання і синхронізацію історії всіх транзакцій у блокчейні;
- Вузли спрощеної верифікації платежів (SPV) використовують для зберігання неповних даних блокчейна і запуску додатків і програм, таких як гаманці.

Залежно від алгоритму консенсусу в блокчейні також можуть функціонувати майстер-вузол і супер-вузол. Майстер-вузли – це спеціально налаштовані повноцінні вузли, які використовуються для виконання унікальних функцій, таких як приватні перекази та розподіл винагород. Супервузли - це високопродуктивні вузли, які гарантують безпеку і функціональність мережі та підтримують легкі гаманці, мобільні гаманці та сторонні додатки.

Алгоритми консенсусу: оскільки публічні мережі блокчейн децентралізовані, вузли використовують механізми консенсусу, щоб вирішити, наприклад, чи включати транзакції до блоку, чи включати блоки в ланцюжок. Ці механізми дають змогу групі учасників дійти єдиного рішення шляхом голосування більшістю голосів. У блокчейнах використовується низка алгоритмів, найпопулярнішими з яких є Proof of Work PoW (Доказ роботи) і Proof of Ownership PoS (Доказ частки) [29].

Хешування: це процес використання криптографічного алгоритму, який спрощує і прискорює перевірку цілісності даних, записаних у блокчейні. Хеш-функція приймає на вхід довільні дані (файл, текст, зображення, двійковий код) і генерує послідовність букв і цифр фіксованої довжини (хеш). При цьому однакові дані завжди видаватимуть однакові хеші, а різні дані в ідеалі видаватимуть різні хеші (випадки збігу дуже рідкісні, що вважається вразливістю криптографічних функцій). Тому функція, що реалізує алгоритм і виконує перетворення, називається "хеш-функцією", вхідні дані - "вхідним масивом", "ключем" або "повідомленням", а результат перетворення -"хешем", "хеш-кодом" або "хеш-сумою".

Електронні цифрові підписи (ЕЦП) використовуються для підписання транзакцій; для роботи ЕЦП мережа повинна підтримувати асиметричне шифрування. Асиметричне шифрування використовує два ключі: один для шифрування (відкритий ключ і публічний ключ) і один для дешифрування (закритий ключ і закритий ключ). Обидва ключі математично пов'язані один з одним і більш детально пояснюються нижче: ЕЦП доводить, що всі транзакції були здійснені тільки справжнім власником.

Закритий ключ - це унікальний пароль учасника мережі, який використовується для підпису вихідного повідомлення, і тому він зберігається в секреті. Закритий ключ гарантує, що тільки власник конкретної адреси може надсилати повідомлення або кошти, що зберігаються на цій адресі, іншим користувачам.

Відкритий ключ - це адреса для отримання повідомлень від інших користувачів, яка є відкритою для всіх користувачів мережі і являє собою рядок букв і цифр, згенерований на основі закритого ключа. Відкритий і закритий ключі невіддільні один від одного, і їхній зв'язок заснований на математичній функції. Вони пов'язані між собою складним незворотнім алгоритмом.

Таким чином, блокчейн функціонує як розподілена бухгалтерська книга, яка може зберігати інформацію, приховану від сторонніх осіб за допомогою шифрування, а копія цієї книги зберігається на комп'ютері кожного користувача. Зламати такий реєстр практично неможливо, а інформація, що міститься в ньому, не може бути змінена або відредагована[30].

Створення блокчейна вимагає або написання коду для вузлів блокчейна з нуля, або використання різних готових програм для створення блокчейна.

Реалізація цієї технології залежить від алгоритму консенсусу, обраного для створюваного блокчейна. Якщо алгоритм Proof of Work, то для вирішення завдання хешування блокчейну потрібен комп'ютер, наприклад, процесор комп'ютера, відеокарта або спеціальна інтегральна схема, розроблена спеціально для цього алгоритму. Що більше даних вводиться в блокчейн, то більше обчислювальних потужностей потрібно для його роботи.

2.3 Програмне забезпечення, яке використовується для створення блокчейну

Перш ніж розробляти власний блокчейн, необхідно чітко розуміти, навіщо він потрібен і який бюджет ви можете виділити на його створення та обслуговування. Розробка і запуск блокчейна мають свої нюанси. Неправильно оцінивши масштаб і складність завдання, можна легко заблукати в процесі планування.

Написання коду для вузла блокчейна з нуля практично неможливе без команди професійних розробників і експертів з досвідом багатопотокового програмування, криптографії, мережевих протоколів, складних внутрішніх алгоритмів і розумінням сучасних операційних систем. Тестування особливо важливе для блокчейн. Це пов'язано з тим, що алгоритм консенсусу може добре працювати на кількох валідаторах, але зовсім по-іншому поводитися при завантаженні десятків або сотень вузлів.

Тому рекомендується використовувати готовий програмний рушій (рушій – це центральна частина комп'ютерної програми, що виконує основні функції цієї програми і містить додаткові утиліти, описи алгоритмів тощо). З огляду на те, що існує кілька основних ядер блокчейна, на яких побудовано наявні мережі, може бути зручно називати їх рушіями (наприклад, "побудований на рушії Ethereum") [31].

Якщо блокчейн немає власної архітектури і завдання полягає в тому, щоб знайти рішення протягом певного періоду часу, найкращим варіантом буде робота з наявними рушіями. Ці движки можуть реалізувати заплановані типи консенсусу і транзакцій і по-своєму керувати мережевими валідаторами. При цьому вони можуть використовувати готовий відкритий код, протестований на реальних мережах, і не вимагають зміни коду блокчейн-вузла, лише частини, наданої розробником рушія для реалізації власної логіки[32].

Існує кілька основних блокчейн-движків, які можна використати для запуску власного блокчейна, проєктування та реалізації його внутрішньої економіки та організації запуску для виконання складних операцій:

Створення блокчейна на базі Ethereum.

Цей програмний пакет побудований на ядрі публічного блокчейна Ethereum. Публічний Ethereum використовує консенсус Proof-of-Work, а його численні тестові мережі-різні типи консенсусу Proof-of-Authority і Proof-of-Stake. Програмне забезпечення відповідає найсуворішим стандартам безпеки, протестоване на десятках реальних мереж і, на мій погляд, є найпередовішим для створення блокчейнів з усіма типами консенсусу і повноцінних, багатофункціональних смарт-контрактів POA-мереж. Роль проєкту необхідно підкреслити: розробники мережі POA виконали величезну роботу і вже запустили кілька швидких і надійних мереж; мережа POA набагато швидша за оригінальний Ethereum, але має стабільність та універсальність таку саму, а роль валідатора виконує комп'ютер, чесність роботи якого доведена юридично. Цю мережу можна розглядати як еталон для запуску корпоративного блокчейна на базі Ethereum [33].

Створення блокчейна на базі EOS

EOS-другий за надійністю рушій з точки зору продуктивності та гарантій безпеки; EOS може бути запущений як самостійна мережа, у версіях PoS або PoA. Як і Ethereum, це програмне забезпечення вже використовується на практиці, має високу безпеку і функціональність для створення власного блокчейна зі смарт-контрактами для автоматизації всіх транзакцій.

У той час як Ethereum являє собою просту систему адресації, EOS використовує ієрархічну систему безпосередніх облікових записів і правна різні дії. Це робить EOS схожою за дизайном на операційну систему або "програму для запуску інших програм"; EOS має зручну систему управління обліковими записами і швидкий консенсус, а також плагін для C++ і C++/Web Assembly. Смарт-контракти дозволяють легко інтегрувати практично будь-яку функціональність (наприклад, ви можете додати ще один шифр).

Консенсусна конструкція EOS і швидкі блоки дозволяють дуже швидко реагувати на запити користувачів. Це дуже важливо для створення розподілених додатків зі складною функціональністю (наприклад, Cyberway, Golos.io або

соціальні мережі Commun). Нещодавно компанія Cyberway провела дуже складну міграцію, під час якої всю бізнес-логіку було прозоро перенесено з попереднього блокчейна на користувацький, що ще раз доводить гнучкість і універсальність EOS [36].

Створення блокчейна на основі Parity Substrate

Substrate був створений командою Parity. Вони розробили величезну кількість програмного забезпечення, включно з гаманцями, вузлами блокчейна, системами смарт-контрактів, компіляторами, віртуальними машинами тощо. За допомогою ParitySubstrate розробники можуть створювати готові модулі зі складною логікою консенсусу та обробки транзакцій. Substrate - це конструктор блокчейна, який можна використовувати, наприклад, для створення вузлів Ethereum або Bitcoin.

Substrate є частиною більшого проєкту Polkadot, який складається з головного ланцюга і безлічі ланцюгів Chardin з індивідуальною логікою. Перевага "підключення" вашого блокчейна до Polkadot полягає в тому, що ви можете обмінюватися даними з іншими ланцюжками і використовувати контракти, рахунки і токени з інших ланцюжків без додаткового програмного забезпечення.

Код Substrate написаний мовою Rust; усі компоненти Substrate добре структуровані та розбиті на окремі модулі, містить докладні коментарі. Про гнучкість рушія свідчить наявність клієнтів для мереж Bitcoin і ZCash, заснованих на коді Substrate. Що стосується консенсусу, то ви можете вибрати один із кількох готових варіантів або написати свій власний. Більшість із них - PoA або DPoS, причому Substrate передбачає використання алгоритмів Aura і GRANDPA; продуктивність блокчейнів на базі Substrate висока, продуктивність мережі ZCash - висока, продуктивність мережі ZCash - низька. Ми протестували основний ланцюжок Polkadot у конфігурації з 99 валідаторами, розподіленими на трьох континентах, і показали відмінні результати [38].

Перевагами Substrate є продумана архітектура, стек розробки (Rust) і величезне поле для розвитку. Будучи надзвичайно гнучкою мережею, яку можна

використовувати для створення рішень будь-якого рівня складності, Substrate відрізняється від Ethereum і EOS тим, що для обробки транзакцій використовується код, розгорнутий валідаторами, а не користувачами. Цей код називається "часом виконання" і виконується віртуальною машиною WebAssembly.

Створення блокчейна на основі Cosmos SDK

Cosmos - це проєкт, заснований на одному головному ланцюжку і кількох дочірніх ланцюжках, які називаються зонами. Дочірні ланцюги побудовані на Cosmos SDK, наборі програмного забезпечення для створення блокчейнів. Cosmos працює в руслі проекту Tendermint, де ключовими технологіями є сильний консенсус і Substrateruntime-like. Як iPolkadot + Substrate, блокчейни, створені за допомогою Cosmos SDK, можуть працювати автономно або підключатися до екосистеми Cosmos у ролі дочірніх ланцюжків. Увесь набір програмного забезпечення Cosmos написано мовою Go, він добре структурований і активно використовується; набазі Cosmos уже працюють кілька проєктів, зокрема Binance Chain.

Основна концепція Cosmos називається додатками. Кожен блокчейн - це машина станів, і в Cosmos вона винесена в окрему частину коду. Розробник просто задає правила, за якими одна частина даних перетворюється на іншу під впливом зовнішніх факторів, програмуючи так звані функції переходу станів. Звучить складно, але насправді обробка транзакцій – це перехід стану, який змінює кілька балансів. Додаток приймає зовнішні впливи (транзакції) і змінює стан. Отримані зміни записуються в блокчейн. При цьому розробникам непотрібно вирішувати проблеми консенсусу або мережі. Мережа сама домовляється одна з одною і досягає консенсусу за підсумком.

Застосунок Cosmos можна розглядати як єдиний смарт-контракт, що відповідає за обробку всіх типів транзакцій. Одночасно зі створенням коду для вузлів блокчейна Cosmos SDK створює клієнтський код, який може генерувати необхідні типи транзакцій; як і в Ethereum, у Cosmos використовується газ для обмеження транзакцій. Під час виконання транзакції валідатор обчислює її

вартість у традиційних одиницях газу. Під час надсилання транзакції користувач вказує ціну, сплачену за одиницю газу, і ліміт, який необхідно використати. Це основа для розрахунку ціни одиниці транзакції[39]. Важливою для додатка Cosmos є вимога детермінізму коду. Це означає, що розроблені операції не повинні давати різні результати в різний час або в різних архітектурах, інакше блокчейн не працюватиме. Паралельно зі створенням коду застосунку, Cosmos SDK дає змогу миттєво отримати код, що викликає необхідні функції з клієнтської машини. Цей код можна використовувати у вебсайті або мережевому гаманці (клієнті), що працює на Cosmos.js-cosmos, cosmosjs і універсальна js-abci, яка реалізує інтерфейс ABCI, - ось деякі корисні бібліотеки JavaScript. Вони корисні під час взаємодії з блокчейном через браузер; ABCI дає змогу створювати додатки різними мовами, включно з Java, C++і Python. Проект Lotion, наприклад, дозволяє створювати блокчейн повністю на Javascript. Cosmos швидко розвивається, і на цьому рушії запускаються різні проекти.

2.4 Аналоги реалізації технології блокчейн

Професор Дон Тапскотт опублікував у журналі Educase статтю під назвою "Революція блокчейна і вища освіта"[16]. У ній блокчейн розглядається як основа нової ери інтернету – інтернету цінностей, а роль блокчейна у вищій освіті поділяється на чотири категорії:

- ідентифікація та облік студентів: як ідентифікувати студентів, захищати їхню конфіденційність, оцінювати їх, зберігати їхні записи, перевіряти їхню успішність і забезпечувати безпеку цих даних;
- нові педагогічні технології: як адаптувати навчання до кожного студента та створювати нові моделі навчання;
- витрати (заборгованість студентів): як оцінити вартість освіти та як її фінансувати;
- розвиток університетської освіти: як розробити абсолютно нові моделі вищої освіти.

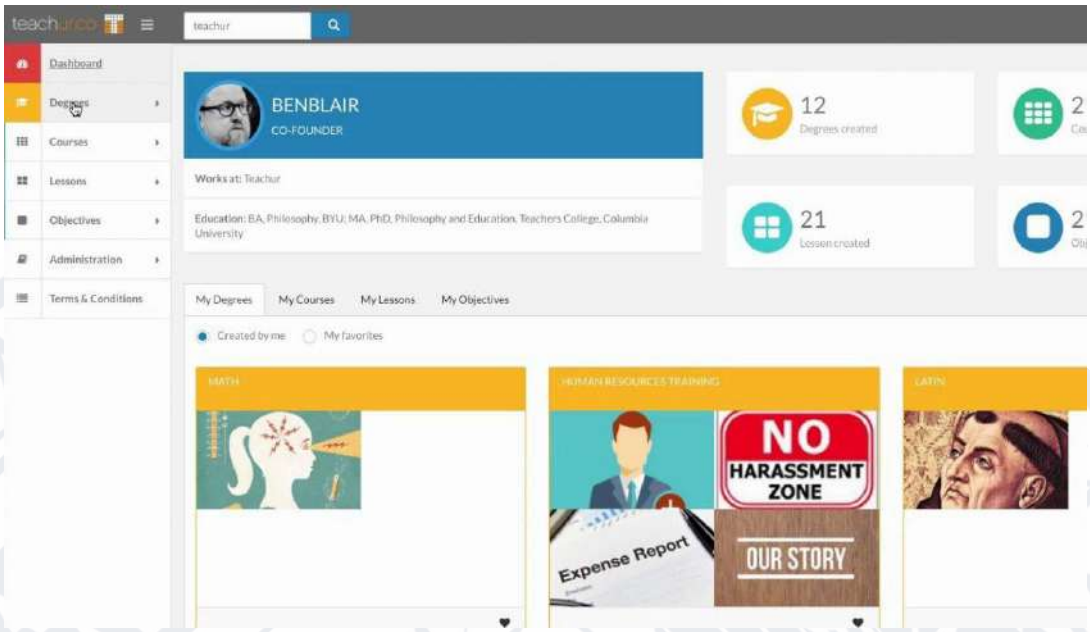

Рисунок 2.1-Інтерфейс системи Teachur

У статті [17] розглядаються проблеми початкової та середньої освіти, які може розв'язати проєкт Teachur. Його суть полягає в новому підході до оцінювання учнів за певними критеріями, системі зберігання цих даних у суворому та безпечному вигляді, а також простоті їх передачі. Характеристики цієї інноваційної системи оцінювання полягають у тому, що, подібно до ланцюжка блоків у блокчейні, оцінювання пов'язане зі знаннями та цілями, поставленими на цей момент, і що його шлях ґрунтується на попередніх знаннях, цілях та оцінках, що гарантує безпеку та простоту передавання, але водночас дає змогу бути більш творчим та дає змогу проводити експериментальне оцінювання.

У [18] описано чотири варіанти використання технології блокчейн у вищій освіті, реалізовані в проекті Teachur:

- Облік навчального процесу;
- Смарт-контракти для отримання дипломів;
- Смарт-контракти для двосторонніх ринків;
- Токен платформи Teachur.

Мета, що досягається в процесі навчання, - достовірний і повний звіт про діяльність студента, яким він може поділитися в будь-який момент за власним

бажанням, що полегшує пошук працівників і партнерів з необхідними навичками.

Диплом – це смарт-контракт, який автоматично виконується при дотриманні необхідних умов і відразу ж дає надійне підтвердження компетентності студента. Викладачі можуть отримувати часткову або повну оплату за розробку та подальше використання курсових робіт і матеріалів. Система має власний маркер, який можна отримувати за заліки та інші види робіт. Це робить роботу з цією системою економічно ефективною.

У своїй статті [20] Люк Паркер пише про те, що першим впровадив блокчейн для підтвердження сертифікатів кандидатів і сертифікатів, які відповідають необхідним компетенціям, і в загальних рисах коротко описує використання технології таким чином. Массачусетський технологічний інститут особливо зацікавлений у питанні захисту та підтвердження сертифікатів і репутаційних систем на основі блокчейна. Вони випустили кілька версій програмного забезпечення Blockcerts з відкритим вихідним кодом, яке реалізує облік і видачу сертифікатів з можливістю обміну з роботодавцями. На рис. 2.2 показано архітектуру їхньої програми.

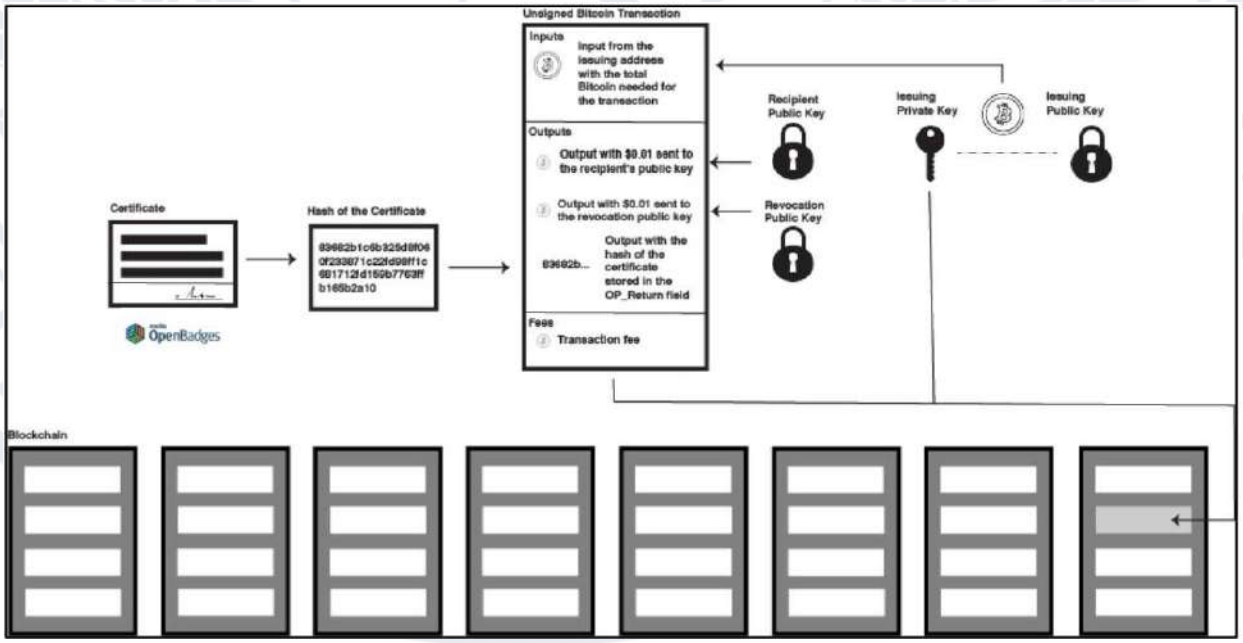

Рисунок 2.2-Архітектура програми цифрових сертифікатів MIT

Яскравим прикладом такої форми освіти є проєкт Codecademy - платформа для навчання програмування наживо. Люди не можуть дозволити собі бути байдужими, адже вони можуть отримати доступ до знань з будь-якої точки світу та пройти недороге або навіть безкоштовне навчання. Поєднання різних курсів може забезпечити студентам різні стратегії навчання.

Впровадження технології блокчейн може дати змогу стандартизувати документи, що видаються, що, своєю чергою, призведе до стандартизації освіти в усьому світі. Знання та навички підтверджених кандидатів можуть зберігатися в єдиній базі даних, що дає змогу динамічно відбирати кандидатів на основі їхнього набору навичок і вмінь, необхідних для обраної посади [26].Результатом створення цієї бази даних стане відкритий ринок кандидатів, які володіють міцними знаннями. У результаті виникне попит на конкретні компетенції та тенденція до вивчення конкретних освітніх програм, які ведуть до формування цих компетенцій. Навчальні заклади зможуть у режимі реального часу виявляти необхідних кандидатів і розробляти відповідні освітні програми та навчальні курси. У результаті можна скоротити розрив між ринком праці та ринком освіти і розв'язати проблему швидкої нереалізованості навчальних планів, прискорюваної стрімким розвитком інформаційних технологій. Сьогодні як для навчальних закладів, так і для компаній навчання і перевірка сертифікатів і дипломів кандидатів на відповідність необхідним компетенціям - дорогий і трудомісткий процес.

Японська компанія Sony, яка створила наприкінці 2017 року Sony Global Education Services, вже використовує технологію блокчейн для видачі сертифікатів. На своєму прикладі вони намагаються показати, що за цією технологією майбутнє в галузі гарантії автентичності знань, отриманих у процесі навчання. Вони також планують продемонструвати можливості цієї технології на прикладі IT-школи Next Generation Міністерства внутрішніх справ і комунікацій Японії[27].

Sony Global Education вважає, що персональні дані про успішність студентів у сфері освіти становлять такуж цінність, як, наприклад, кредитна

історія людини. При використанні технології блокчейн дані можуть бути підписані цифровим підписом і безпечно передані іншим сторонам. Зберігаючи достовірні дані, можна отримати повну історію студента (наприклад, комп'ютерні тести) на абсолютно безпечній платформі[28]. Таким чином, впровадження технології блокчейн в освіту вже знайшло своє застосування.

Звісно, основна увага приділяється реалізації можливості безпечного зберігання сертифікатів, дипломів та результатів студентів, що може вирішити подібні проблеми:

- Стандартизація та глобалізація освіти (можлива стандартизація без глобалізації);
- Наявність надійного, відкритого і єдиного ринку кандидатів із підтвердженими знаннями;
- Актуальність освітніх програм і, отже, скорочення розриву між ринком праці та ринком освіти.

Об'єднаний дослідницький центр Європейської комісії опублікував велике дослідження під назвою "Блокчейн в освіті" [29], у якому зачеплено багато аспектів різних застосувань блокчейна в освіті. На основі цього дослідження було розроблено сім сценаріїв використання технології розподілених реєстрів в освіті:

1. забезпечення постійного захисту студентських квитків.
2. використання блокчейну для багатоступеневої автентифікації.
3. інтелектуальна автентифікація та грошові перекази на основі блокчейну.
4. використання блокчейна як паспорта для безперервного навчання.
5. отримання платежів від студентів через блокчейн.
6. надання коштів студентам у вигляді ваучерів через блокчейн.
7. ідентифікація студентів у навчальних закладах.

РОЗДІЛ 3
РЕАЛІЗАЦІЯ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕНЙ У СФЕРУ НАВЧАННЯ

3.1 Метод смарт-контрактів для навчання

Технологію смарт-контрактів вперше описав Нік Сабо [41] у 1990-х роках. Він визначив смарт-контракти як інструменти, які формалізують і захищають комп'ютерні мережі шляхом поєднання протоколів і користувацьких інтерфейсів. Сабо також обговорив потенційні застосування смарт-контрактів у різних сферах, включаючи договірні соціальні відносини, такі як кредитні контракти, обробка платежів і управління авторськими правами.

В принципі, вони функціонують як цифрові контракти, підкріплені певними правилами. Ці правила визначаються комп'ютерним кодом, який реплікується і виконується всіма вузлами мережі. Смарт-контракти дозволяють створювати надійні протоколи. Це означає, що обидві сторони можуть брати на себе зобов'язання через блокчейн, не знаючи і недовіряючи одна одній. Учасникам цього процесу непотрібно турбуватися про правильність виконання своїх зобов'язань, оскільки контракт буде скасовано, якщо умови не будуть виконані. Використання смарт-контрактів також усуває потребу в посередниках, значно знижуючи транзакційні витрати. Протокол блокчейну Bitcoin підтримує смарт-контракти вже багато років і був популяризований Віталіком Бутеріним, творцем і співзасновником Ethereum. Водночас, кожен блокчейн може пропонувати різні способи реалізації смарт-контрактів; стаття Ніка Сабо [41] присвячена смарт-контрактам, що працюють на віртуальній машині Ethereum.

Як працюють смарт-контракти в мережі Ethereum

Смарт-контракти функціонують як детерміновані програми. При виконанні певних умов вона виконує певну дію. Виходячи з цього, системи смарт-контрактів часто використовують вираз "якщо..". Незважаючи на поширену термінологію, смарт-контракти не є ні контрактами, ні "розумними" в

юридичному сенсі. Це просто фрагмент коду, що виконується в розподіленій системі блокчейн[42].

У мережі Ethereum смарт-контракти відповідають за виконання транзакцій між користувачами (адресами). Адреси, які не є смарт-контрактами, називаються особистими рахунками. Таким чином, смарт-контракти управляються програмним кодом, в той час як особистими рахунками керують користувачі.

Смарт-контракт Ethereum складається з коду контракту (включаючи умови виконання) і двох відкритих ключів. Перший публічний ключ надається автором контракту; другий ключ контракт, цифровий код, унікальний для кожного смарт-контракту.

Виконання смарт-контракту відбувається під час транзакції в блокчейні і стає активним, коли його ініціює окремий обліковий запис (або інший смарт-контракт). (Однак послідовність смарт-контрактів завжди ініціюються з особистого облікового запису, тобто користувачем).

Ключові особливості смарт-контрактів Ethereum

Смарт-контракти Ethereum мають наступні характеристики:

Децентралізованість. Смарт-контракти реплікуються і поширюються по всіх вузлах мережі Ethereum. Це одна з головних відмінностей від інших рішень, які використовують централізовані сервери.

Детермінованість. Смарт-контракти виконують заплановані дії, коли виконуються вимоги. Крім того, результат завжди однаковий, незалежно від того, хто виконує вимогу.

Автономність. Смарт-контракти можуть діяти як самодостатні програми і автоматизувати будь-які завдання. У більшості випадків, якщо смарт-контракт не ініційований, він є "неактивним" і не виконує жодних дій.

Незмінність. Після того, як смарт-контракт розроблений та ініційований, процес не може бути змінений. Зміни можуть бути внесені лише в тому випадку, якщо розробник заздалегідь реалізував певні функції. Таким чином, смарт-контракти можуть забезпечити захист коду від несанкціонованого втручання шляхом підтвердження автентичності.

Кастомізація. Перед впровадженням смарт-контракти можна розробляти різними способами. У цьому відношенні технологія підходить для створення багатьох типів децентралізованих додатків. Це також пов'язано з тим, що Ethereum є повноцінною мережею блокчейн.

Конфіденційність; дві або більше сторін можуть взаємодіяти, не знаючи і недовіряючи один одному, за допомогою смарт-контрактів. Крім того, технологія блокчейн гарантує точність і облік всіх даних.

Прозорість. Оскільки смарт-контракти базуються на публічному блокчейні, їх вихідний код доступний кожному.

Після активації смарт-контракти Ethereum не можуть бути доповнені новими функціями. Однак, якщо розробник включає в код контракту функцію під назвою SELFDESTRUCT, вона може бути пізніше видалена і замінена новою функцією. І навпаки, якщо ця функція не прописана в коді, контракт не може бути видалений.

Так звані оновлюванні смарт-контракти є більш гнучкими, ніж незмінні, оскільки розробник має доступ до змін у коді. Існує багато способів створення цього типу смарт-контрактів, з різним ступенем складності.

Смарт-контракт розбивається на ряд менших контрактів. Деякі з них не можуть бути змінені, в той час як інші можуть бути видалені. Іншими словами, деякі частини коду (кількість смарт-контрактів) можна видалити і замінити іншими, але інші функції не можуть бути змінені. Як програмований код, смарт-контракти легко налаштовуються і можуть бути розроблені різними способами для надання різних типів послуг і рішень.

Смарт-контракти можуть підвищити прозорість і знизити операційні витрати, оскільки вони є децентралізованими і самодостатніми додатками. Для деяких підприємств вони також можуть підвищити ефективність і зменшити бюрократичні витрати. Переваги смарт-контрактів особливо помітні, коли йдеться про перекази та обміни між двома або більше сторонами.

Смарт-контракти можуть бути розроблені для широкого спектру випадків використання. Приклади включають створення токенізованих активів і акцій,

систем голосування, криптовалютних гаманців, децентралізованих бірж, ігрових і мобільних додатків. Його також можна впроваджувати в поєднанні з іншими блокчейн-рішеннями для таких секторів, як охорона здоров'я, благодійність, ланцюжок поставок, державне управління, децентралізовані фінанси та освіта.

Рисунок 3.1-Реалізація смарт-контрактів

Недоліки смарт-контрактів Ethereum

Смарт-контракти складаються з комп'ютерного коду, написаного людьми. Як такий, код схильний до вразливостей і помилок і несе в собі ряд ризиків. В ідеалі, вони повинні розроблятися досвідченими програмістами, особливо коли йдеться про конфіденційну інформацію або великі суми грошей.

Централізовані системи можуть забезпечити більшість рішень і функцій, пропонованих цією технологією. Основна відмінність полягає в тому, що смарт-контракти виконуються в децентралізованій, тимчасовій мережі, а не на централізованих серверах. Крім того, оскільки смарт-контракти базуються на блокчейні, вони, як правило, незмінні або процес їх зміни дуже складний.

Незмінність - це добре в одних ситуаціях і дуже погано в інших. Наприклад, коли у 2016 році була зламана децентралізована автономна організація під назвою DAO, хакери вкрали ефір на мільйони доларів через недоліки в коді смарт-контрактів. Їх смарт-контракти не були модифіковані, тому розробники не змогли виправити код. Слід зазначити, що ця проблема не була спричинена блокчейном Ethereum. Натомість помилка була спричинена неправильною реалізацією смарт-контракту. Ще одним недоліком смарт-контрактів є те, що їх правовий статус є невизначеним. Це пов'язано не лише з

тим, що технологія перебуває в "сірій зоні" в більшості країн, але й з тим, що смарт-контракти не відповідають чинній нормативній базі.

Ключовою вимогою багатьох угоді контрактів є ідентифікація учасників, які досягли 18-річного віку. Псевдоанонімність, яку забезпечує технологія блокчейн, у поєднанні з відсутністю посередників, може стати перешкодою для виконання цих вимог. Незважаючи на те, що існують потенційні рішення цієї проблеми, правові елементи смарт-контрактів залишаються одним з головних викликів, особливо щодо глобального масштабу та децентралізованих мереж.

Смарт-контракти – це передова технологія. Однак їх децентралізований і безстроковий характер, а також прозорість і часткова незмінність роблять їх менш привабливими в деяких ситуаціях.

Смарт-контракти не є вирішенням багатьох реальних проблем. Насправді, деякі організації вважають, що простіше і краще використовувати традиційні альтернативні сервери. У порівнянні зі смарт-контрактами, централізовані сервери простіше і дешевше обслуговувати, вони працюють краще з точки зору швидкості і сумісності з іншими мережами.

Впровадження смарт-контрактів в освітній галузі

Системи смарт-контрактів забезпечують технічний доступ до наступних компонентів:

- Сторони контракту - студенти, викладачі та навчальні заклади;
- Предмет контракту між студентом та навчальним закладом – свідоцтво про закінчення або диплом; між викладачем та навчальним закладом - виплата заробітної плати.

Крім того, як умова контракту, ці елементи повинні бути проаналізовані, виміряні та взаємопов'язані. Між студентом і навчальним закладом – академічна успішність; між викладачем і навчальним закладом – ефективність викладання. Децентралізована природа блокчейну дозволяє зробити це без участі третьої сторони і виконати угоду про предмет договору, як тільки будуть виконані всі необхідні умови [43].

Завдяки електронним цифровим підписам, які використовуються в блокчейні, всі дії, вчинені сторонами договору, можуть бути підтверджені і згодом перевірені. Таким чином, для реалізації смарт-контракту можуть бути виконані різні умови.

Наприклад, реєстрація постачальника освітніх послуг і навчального закладу, який є стороною договору, може пов'язувати всі дані про заклад (наприклад, поштовий індекс, номер платника податків (ІПН), причину реєстрації), контактні дані, адресу та освітні програми, які там проводяться.

Смарт-контракти укладаються для студентів, які успішно проходять контрольні точки, визначені в освітній програмі, і вписуються розробником у код. У випадку з викладачами смарт-контракт функціонує, коли викладач виконує завдання, за яке отримує заробітну плату. Як тільки система відкрита, вона також виступає гарантом виконання умов контракту, так що треті сторони можуть бачити, які освітні програми діють у навчальному закладі і наскільки ефективно вони реалізуються. Роботодавці можуть використовувати контактні форми для зв'язку з випускниками, чиї результати відповідають їхнім потребам. Заклади можуть обмінюватися освітніми програмами між собою та своїми філіями. Загалом, схема зв'язку між системами показана на рисунку 3.2.

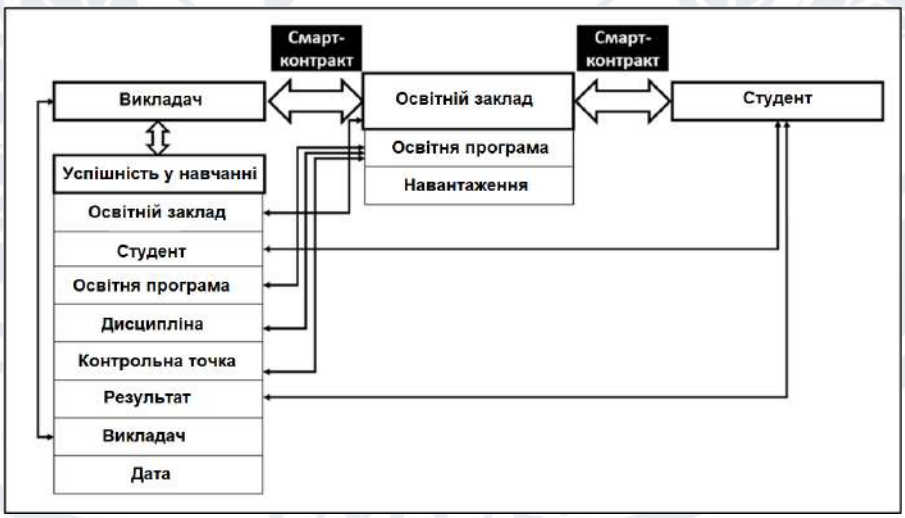

Рисунок 3.2 – Принципова схема моделі смарт-контракту

3.2 Можливості використання ICO для фінансування освітньої системи

ICO (initial coin offering) – це первинне публічне розміщення токенів (монет). Це продаж цифрових токенів інвесторам у криптовалюті або фіатних коштах (гривнях, доларах, євро). Куплені токени можна використовувати для оплати послуг.

Абревіатура ICO схожа на IPO (Initial Public Offering - первинне розміщення акцій).Однак між поняттями ICO та IPO є деякі суттєві відмінності:

- ICO в даний час не підлягають державному регулюванню, характерному для IPO та інших видів публічної фінансової та інвестиційної діяльності;
- Власники токенів не мають тих самих прав, що й акціонери компанії;
- ICO проводиться з метою залучення коштів, необхідних для запуску та розвитку проекту. Саме тому багато експертів вважають ICO формою краудфандингу (колективного фінансування проекту з метою отримання майбутніх бонусів).
- Купуючи токени, інвестори можуть розраховувати на наступне
- Прибуток від майбутнього перепродажу токенів за вищою ціною;
- Більш низькі ціни на майбутні покупки послуг компанії;
- Розвиток цікавих проектів.

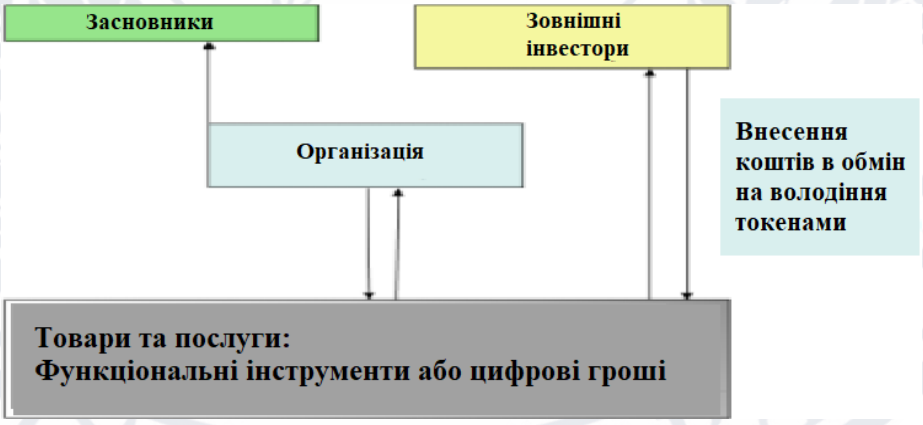

Рисунок 3.3 – Схема інвестицій у токени

Оскільки ICO зазвичай запускають маловідомі проекти, першим кроком є привернення уваги інвесторів. З цією метою в криптовалютних спільнотах, таких

як Redditi Bitcoin Talk, публікуються презентації компанії з поясненням бізнес-моделі. В ході обговорень у спільнотах модель кілька разів змінюють, роблячи її цікавою для фандрейзингу. Після досягнення домовленості між проектом та інвестором, проект готує оферту [44].

В оферті вже детально описуються всі деталі проекту та вказується бажана сума інвестицій. Також вказується грошова вартість токенів, які будуть продаватися, і права, якими вони володіють. Після підготовки оферти компанія готує документацію та оголошує дату продажу токенів. Для проведення ICO компанії можуть або створити власний блокчейн, або скористатися готовою платформою ICO. Плюси і мінуси готових платформ для проведення ICO:

- Високий рівень довіри до проекту з боку інвесторів;
- Простота адміністрування;
- Потребує менше інвестицій на початкових етапах;
- Низька вартість володіння;
- Низький ризик втрати капіталу;
- Низький ризик втрати капіталу
- Можна захистити кошти від зловмисників;
- Платформи стягують комісію.

Найвідомішою платформою для ICO є Ethereum. Ця платформа лідирує не тільки за кількістю користувачів, але й за кількістю грошей в обігу. Криптовалюта Ефір, створена на основі цього блокчейну, торгується майже на всіх біржах, а токени Ethereum легко додавати на торгові платформи, і з системою пов'язано багато гаманців.

Маючи гаманець, що містить криптовалюту і можливість здійснювати транзакції, ви можете брати участь у краудсейлах на сайтах проектів; також існують спеціальні інформаційні ресурси, такі як ICO alerts, які можуть допомогти вам знайти проекти, що проводять ICO.

Оскільки ICO не регулюється законом, а транзакції базуються виключно на довірі до засновника проекту, перед тим, як вкладати гроші, варто звернути увагу на його доступність:

- Всі необхідні договори та правила знаходяться у відкритому доступі;
- Прототип у проекті;
- Необхідні документи;
- Ескроу (спеціальний умовний рахунок, на якому зберігається майно, документи або кошти до настання певних обставин або виконання певних зобов'язань);
- Реєстрація самої компанії;
- Інформація про репутацію тих, хто ініціює проект.

Важливо, щоб схема була фінансово стійкою для забезпечення її стабільної роботи. Нові методи залучення інвестицій дозволяють залучити більше стейкхолдерів, які можуть внести не тільки гроші, але й внести свій вклад у розвиток організації. Система дозволяє створювати токени-власно у криптовалюту організації.

З токенами, завдяки зв'язкам в системі, можна здійснювати наступні операції (Рис.3.4).

Можливі наступні операції:

- оплата навчання студентами.
- виплата заробітної плати викладачам навчальними закладами; та виплата стипендій студентам навчальним закладом.
- Інші платежі в середині організації.
- Купівля токенів навчального закладу з метою інвестування.

Рисунок 3.4 – Схема шляхів залучення фінансів до освітньої системи

Таким чином, система освіти матиме власні активи, від яких залежатимуть результати її діяльності, що зробить її самодостатньою. Навчальні заклади зацікавлені в ефективності своєї освітньої діяльності. Це пов'язано з тим, що вона визначає попит, який безпосередньо виражається в ціні токенів.

3.3 Метод видачі цифрових сертифікатів та дипломів

Більшість закладів ведуть облік або на паперових носіях, або в спеціальних базах даних, до яких мають доступ лише педагогічні працівники. У більшості випадків ці заклади мають власні спеціальні системи для зберігання повних даних про студентів. Щоб забезпечити безперебійний доступ до інформації про студентів на всіх рівнях - студента, навчального закладу та роботодавця -кожна організація працює над розробкою системи управління сертифікатами на основі блокчейну. Це дозволить автоматизувати процес видачі паперових сертифікатів і надсилання запитів на перевірку сертифікатів через різні вузли блокчейну [47].

Паперові сертифікати забирають багато часу і схильні до помилок та шахрайства. Завдяки цій автоматизації дані можуть зберігатися в незмінній інфраструктурі та заповнюватися в режимі реального часу. Студентам потрібно лише зберігати посвідчення протягом усього життя, що дозволяє їм керувати правом власності. Для роботодавців, тим часом, це зменшує потребу у сторонній перевірці та мінімізує ризик отримання фальшивих заявок на отримання сертифікатів.

Дослідження Об'єднаного дослідницького центру Європейської комісії "Блокчейн в освіті" [48] надає попередній огляд технології та її потенційного застосування в Європі. Воно показує, наскільки серйозно ця технологія сприймається в освітньому секторі. Одним із застосувань технології блокчейн, описаних у цій статті, є видача цифрових сертифікатів і дипломів.

В кінці захисту публікуються оцінки всіх робіт. Дипломи підписуються ректором, головою, деканом і секретарем навчального закладу. Всі документи повинні бути скріплені печаткою навчального закладу. Диплом вручається випускнику особисто або, за його заявою, надсилається рекомендованим листом.

Анкета-заява зберігається в особовій справі випускника, там же зберігається копія виданого диплома. Всі документи зберігаються під суворим контролем і реєструються в спеціальному журналі. Для обліку всіх виданих дипломів в закладі ведеться журнал, сторінки якого пронумеровані, а сама книга скріплена печаткою закладу та позначена кількістю сторінок. Реєстр також зберігається як документ суворої звітності.

Для вирішення проблем шахрайства у вигляді підробки документів та зберігання документів було запропоновано впровадження технології блокчейн. Модель блокчейну показана на рисунку 3.5.

Рисунок 3.5 – Модель видачі диплому з використанням блокчейну

У цій моделі вищі навчальні заклади, що видають цифрові дипломи, використовують єдиний блокчейн для зберігання дипломів. Унікальні дипломи, підписані приватним ключем, надаються безпосередньо роботодавцю. Тому автентичність диплома можна перевірити, лише порівнявши його з хешем, що зберігається в блокчейні. Це вирішує проблеми шахрайства у сфері підробки документів та безпеки документів.

Спочатку створюється цифровий файл, що містить основну інформацію про диплом, таку як назва університету, ім'я одержувача, дата видачі та сертифікат. Потім вміст диплома підписується університетом за допомогою приватного ключа, до якого має доступ лише університет. Дані перевіряються

вузлами мережі і передаються в мережу. Запис прикріплюється до блоку. Університет створює хеш-файл сертифіката. Це короткий рядок букв і цифр, за допомогою якого можна перевірити, чи ніхто не втручався у зміст диплома. Цифровому файлу може відповідати лише одна комбінація букв і цифр, а зміна файлу призведе до створення іншого хешу. Потім університет знову використовує приватний ключ, щоб створити запис у блокчейні про те, що освітня організація видала конкретний сертифікат конкретній особі в конкретну дату. Відкритий ключ передається випускнику. Таким чином, користувач може перевірити, кому і ким був виданий диплом, а також зміст самого диплома [49].

Перевага над статус-кво полягає в тому, що докази видачі диплома повністю, надійно і назавжди зберігаються в блокчейні. Таким чином, навіть якщо установа, яка видала сертифікат, закриється або вся система освіти зруйнується, ці сертифікати все одно можна буде перевірити за записами, що зберігаються в блокчейні.

Крім того, як тільки навчальний заклад видасть диплом, він зможе перевірити диплом безпосередньо у вигляді блокчейн-ідентифікації і не буде витрачати додаткові ресурси на перевірку дійсності цього документа у третьої сторони.

Рисунок 3.6 – Механізм роботи технології блокчейн для видачі дипломів

ВИСНОВКИ

В даній кваліфікаційній роботі запропоновано нову блокчейн-систему, яка працює з лінійним масштабованим механізмом консенсусу, схемою вибору підтвердження шарду за часткою голосу та масштабованою генерацією випадковості з випадковими функціями перевірки та функціями відкладеної перевірки.

Такий метод створення блокчейну має практичну цінність для вдосконалення існуючих механізмів функціонування блокчейну та використання розподілених блокчейн баз даних в освітніх цілях, зокрема для ідентифікації та обліку оцінок студентів, автоматичної видачі дипломів та атестатів, проведення іспитів та залучення інвестицій.

В рамках роботи було проведено дослідження розподілених блокчейн баз даних. На основі проведеного дослідження були отримані наступні результати

1. Проаналізовано теоретичне підґрунтя основних принципів технології розподіленого реєстру та її відмінності від звичайних баз даних
2. Проведено огляд технології блокчейн та досліджено її потенціал та доцільність використання у різних сферах, зокрема, у створенні освітніх середовищ.
3. Досліджено та описано алгоритми створення блокчейнів, а також наведено приклади готових рішень для впровадження цієї технології в освіті. Розглянуто програмні інструменти та особливості, пов'язані з розробкою та функціонуванням технології блокчейн.

Розглянуто особливості застосування чотирьох способів впровадження технології блокчейн в освітню галузь.

Описано способи на основі теоретичного аналізу, в якому проаналізовано принципи використання технології блокчейн та детально описано їх алгоритми.

Запропоновано метод створення повністю масштабованого, доказово безпечного та енергоефективного блокчейну з використанням нових протоколів консенсусу, шардингу та розподіленої генерації випадковостей.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Vasin, P. (2014) Blackcoin's Proof-of-Stake Protocol v2, URL: https://blackcoin.co/blackcoin-pos-protocolv2-whitepaper.pdf
2. Holmberg A. The Theatre of Robert Wilson. Cambridge University Press, 1996. – Vol. E77 – D. – No.20, October. – P. 899-902
3. Meunier S. Blockchain technology – a very special kind of Distributed Database // Medium.com. 2016. URL: https://medium.com/@sbmeunier/blockchaintechnology-a-very-special-kind-of- distributed-database-e63d00781118
4. World Bank. Distributed Ledger Technology (DLT) and Blockchain // WBG's FinTech Note |No. 1. 2017. URL: http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-andBlockchain-Fintech-Notes.pdf
5. Як влаштований блокчейн і навіщо він потрібен / Афіша - медійно-сервісна платформа, URL: https://daily.afisha.ru/brain/6058-kak-ustroen- blokcheyn-i-zachem-on-nuzhen/
6. Kumar, C. Fischer, S. Tople, and P. Saxena, "A Traceability Analysis of Monero's Blockchain,"IACR Cryptology ePrint Archive, vol. 2017, p. 338, 2017.
7. Blockchain Technology Applications in Education», URL: https://www.researchgate.net/publication/337670514_Blockchain_Technology_Applications_in_Education
8. Blockchain in education research», URL: https://journals.uic.edu/ojs/index.php/fm/article/view/10654/9726
9. Sommer, Deppe G., Stehling V., Haberstroh M., and Hees. Request for Comments: Proposal of a Blockchain for the Automatic Management and Acceptance ofStudent Achievements // E-Prüfungs-Symposium. Aachen. 2018.

10. Novotny P., Zhang Q., Hull , Baset S., Laredo , Vaculin , Ford D., and Dillenberger D.N. Permissioned Blockchain Technologies for Academic Publishing // Information Services & Use. 2018.
11. Using blockchain to re-imagine learning, URL: https://medium.com/@KnowledgeWorks/using-blockchain-to-re-imaginelearning-fb3bf2717b09
12. Use Cases for Blockchain for Higher Ed», URL: https://www.ibm.com/blogs/blockchain/2019/02/how-blockchain-could-change-higher-education/
13. Smart Contracts for Effective Curriculum, URL: https://medium.com/@benblair_34530/smart-contracts-for-effective-curriculum-30c610067c51
14. Authenticating academic certificates on the Bitcoin blockchain, URL: https://bravenewcoin.com/insights/authenticating-academic-certificates-on-hebitcoin-blockchain
15. What we learned from designing an academic certificates system on the blockchain, URL: https://medium.com/mit-media-lab/what-welearned-from-designing-an-academic-certificates-system-on-the-blockchain34ba5874f196
16. Blockchain Technology Needs to Be Changing Education», URL: https://medium.com/age-of-awareness/blockchain-technology-needs-to-be-changing-education-2739324281e2
17. On the (Im)possibility of Obfuscating Programs, URL: https://www.iacr.org/archive/crypto2001/21390001.pdf
18. Febin, J. How Can Blockchain Technology Innovate Your EducationHackernoon, URL: https://hackernoon.com/how-can-blockchaintechnology-innovate-your-educationd1cd80c26f08
19. Sony Details Blockchain Use for Education Data / CoinDesk - компанія, що спеціалізується на цифрових медіа, події та інформаційних послугах для спільноти криптоактивів і блокчейн технологій, URL:

https://www.coindesk.com/sony-patentfiling-details-blockchain-use-managing-education-data/Watters, A.

20. The Blockchain for Education: An Introduction / Hack Education – особистий блог Одрі Уоттерс. http://hackeducation.com/2016/04/07/blockchain-education-guide
21. Grech, A., Gamilleri, AFBlockchain in Education, URL: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education(1).pdf
22. Indistinguishability Code Obfuscation research, URL: https://eprint.iacr.org/2013/451.pdf
23. Intel Software Guard Extensions, URL: https://software.intel.com/sgx
24. Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contract Execution, URL: https://arxiv.org/abs/1804.05141
25. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system,"2008, URL: https://bitcoin.org/bitcoin.pdf.
26. Miller, M. M¨oser, K. Lee, and A. Narayanan, "An Empirical Analysis of Linkability in the Monero Blockchain,"arXiv preprintarXiv:1704.04299, 2017
27. Smart Contracts: Building Blocks for Digital Markets Copyright (c) 1996 by Nick Szabo URL: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html
28. Grech, A. Camilleri, A. F. (2017) Blockchain in Education. Inamorato Santos, A. Luxembourg: Publications Office of the European Union, 2017. – 132p.
29. Blockchain in Education Alexander Grech Anthony F. Camilleri. Editor: Andreia Inamorato dos Santos 2017, URL: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education(1).pdf
30. Paul Feldman. A practical scheme for non-interactive verifiable secret sharing. In Proceedings of the 28th Annual Symposium on Foundations of Computer

Science, SFCS ’87, pages 427–438, Washington, DC, USA, 1987. IEEE Computer Society.

31. Baruch Awerbuch and Christian Scheideler. Towards a scalable and robust DHT. In Proceedings of the Eighteenth Annual ACM Symposium on Parallelism in Algorithms and Architectures, SPAA ’06, pages 318–327, New York, NY, USA, 2006. ACM. [20] Dan Boneh, Joseph Bonneau, Benedikt Bünz, and Ben Fisch. Verifiable d
32. Dan Boneh, Joseph Bonneau, Benedikt Bünz, and Ben Fisch. Verifiable delay functions. In CRYPTO 2018, 2018.
33. J.R. Douceur, The Sybil attack, in: 1st International Workshop on Peer-to-Peer Systems (IPTPS 02), 2002.
34. The Zilliqa Team. The zilliqa technical whitepaper, URL: whitepaper.pdf (zilliqa.com)
35. The QuarkChain Team. Cross Shard Transaction, URL: https://github.com/QuarkChain/pyquarkchain/wiki/Cross-Shard-Transaction
36. Miguel Castro and Barbara Liskov. Practical Byzantine Fault Tolerance. In Proceedings of the 3rd Symposium on Operating Systems Design and Implementation (OSDI ’99), New Orleans, Louisiana, February 2015.
37. M. Zamani, M. Movahedi, and M. Raykova, “RapidChain: Blockchain Protocol via Full Sharding.” Cryptology Archive, Report 2018/460, 2018., URL: https://eprint.iacr.org/2018/460
38. Baruch Awerbuch and Christian Scheideler. Towards a scalable and robust DHT. In Proceedings of the Eighteenth Annual ACM Symposium on Parallelism in Algorithms and Architectures, SPAA ’06, pages 318–327, New York, NY, USA, 2006. ACM.
39. M. F. Nowlan, J. Faleiro, and B. Ford. Crux: Locality-preserving distributed systems. CoRR, abs/1405.0637, 2014.
40. George Danezis and Sarah Meiklejohn. Centrally banked cryptocurrencies. In 23nd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016.

41. E. Syta, P. Jovanovic, E. Kokoris-Kogias, N. Gailly, L. Gasser, I. Khoffi, M. J. Fischer, and B. Ford. Scalable Bias-Resistant Distributed Randomness. In 38th IEEE Symposium on Security and Privacy, May 2017.
42. Paul Feldman. A practical scheme for non-interactive verifiable secret sharing. In Proceedings of the 28th Annual Symposium on Foundations of Computer Science, SFCS '87, pages 427–438, Washington, DC, USA, 1987. IEEE Computer Society.
43. Paul Dworzanski. A note on committee random number generation, commit-reveal, and last-revealer attacks. URL: http://paul.oemm.org/commit_reveal_subcommittees.pdf
44. E. Kokoris-Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford. Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing. In Proceedings of the 25th USENIX Conference on Security Symposium, 2016.
45. D. Boneh, B. Lynn, and H. Shacham. Short Signatures from the Weil Pairing. In Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, ASIACRYPT '01, pages 514–532, London, UK, UK, 2001. Springer-Verlag, URL: https://www.iacr.org/archive/asiacrypt2001/22480516.pdf
46. Derek Leung, Adam Suhl, Yossi Gilad, and Nickolai Zeldovich. Vault: Fast bootstrapping for cryptocurrencies. Cryptology ePrint Archive, Report 2018/269, 2018.