Міністерство освіти і науки України
Харківський національний університет радіоелектроніки
Факультет Комп'ютерних наук
(повна назва)

Кафедра Системотехніки
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

другий (магістерський)
(рівень вищої освіти)

ГЮИК.502130.034 ПЗ
(позначення документа)

Дослідження технології блокчейн для проектування автоматизованих освітніх систем
(тема роботи)

Виконав: здобувач групи ІТПм-20-1
спеціальності 122 – «Комп'ютерні наукиї»
(код і повна назва спеціальності)

освітньої програми «Інформаційні технології проектування»
(повна назва освітньої програми)

Керівник *доцент Тітов С.В.*
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри СТ _____ *проф. Гребеннік І.В.*
(підпис) (прізвище, ініціали)

2021 р.

Харківський національний університет радіоелектроніки

Факультет *Комп'ютерних наук*
Кафедра *Системотехніки*
Рівень вищої освіти *другий(магістерський)*
Спеціальність *122 – «Комп'ютерні науки»*
(код і повна назва)

Освітня програма ОПП Інформаційні технології проектування
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри

(підпис)

" ___ "_____ *2021 р.*

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
здобувачеві Яворському Вадиму Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження технології блокчейн для проектування автоматизованих освітніх систем*
затверджена наказом по університету від «8» листопада 2021р. № 1663 СТ
2. Термін подання здобувачем роботи до екзаменаційної комісії 10.12.2021
3. Вихідні дані до роботи: методи та механізми застосування технології розподіленого реєстру у навчанні, підходи до створення блокчейн середовища.
4. Перелік питань, що потрібно опрацювати в роботі: проаналізувати існуючі методи застосування технології розподіленого реєстру у сфері навчання, проаналізувати існуючі програмні та апаратні засоби для функціонування технології, запропонувати рішення, що дозволяють підвищити якісні характеристики застосування технології розподіленого реєстру для навчання, розробити та дослідити систему блокчейн, що може бути використана для навчальних потреб.
5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) Слайди презентації: титул, мета роботи, схема блокчейну, діаграма розподіленої бази даних, діаграма розподіленого реєстру, форк блокчейну через шкідливі вузли хочуть створити блоки, модель видачі диплому з використанням блокчейну, механізм роботи технології блокчейн для видачі дипломів, схема зв'язків моделі для смарт-контрактів, мережева комунікація під час одного раунду консенсусу, шардінг шляхом голосування акцій.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів	Примітка
1	Написання першого розділу: Аналітичний огляд технологій розподіленого реєстру для створення освітнього середовища	03.10.2021	
2	Написання другого розділу: Технічні аспекти створення та реалізації технології блокчейн	14.10.2021	
3	Написання третього розділу: Особливості застосування різних методів реалізації технології блокчейн у сфері навчання	28.10.2021	
4	Написання четвертого розділу: Дослідження технології блокчейн з використанням масштабованого протоколу консенсусу і удосконаленого методу шардінгу	30.11.2021	

Дата видачі завдання 8 листопада 2021 р.

Здобувач _____ Яворський В.В.
(підпис)

Керівник роботи _____ *доцент Тітов С.В.*
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Розподілена база даних, освіта, блокчейн, механізм консенсусу, шардінг, генерація розподіленої випадковості, старт-контракти.

Актуальність теми роботи полягає у тому, що використання технології розподіленого реєстру набуло широкого розповсюдження 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.

Метою дослідження є покращення існуючих методів реалізації технології блокчейн для подальшого застосування у сфері освіті. Для досягнення поставленої мети необхідно виконати такі завдання:

- 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.

ABSTRACT

Actuality of work is than the fact that there is a wide distribution of technology in the distribution of the reestrue in young women such as economics, financial and banking sector, logistics, modernization and etc.

The object of the research is technology of the distributed restructuring – blockchain and methods of implementation in the sphere of science.

The aims of the work to abbreviating new methods of implementing blockchain technology for the purpose of further storing in the sphere of education. To achieve this goal it is necessary to perform the following tasks:

- analyze the technology of the distributed database;
- to follow the algorithms of the technology;
- consider examples at the implementation of blockchain technology in the sphere of modernization;
- to analyze the an analysis of the methods for the implementation and function of blockchain technology;
- perform a comparative analysis of methods, finding shortcomings and proponents of other methods, as much as possible for saving and transmitting information.

Зміст

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ASIC – Application-specific integrated circuit (Інтегральна схема для спеціального застосування) ;

CPU – Central processing unit (Центральний процесор) ;

GPU – Graphics processing unit (Графічний процесор) ;

PBFT – Practical Byzantine Fault Tolerance (Метод візантійських генералів) ;

POS – Proof of Stake (Доказ долі) ;

POW – Proof of Work (Доказ роботи) ;

PVSS – Public Verified Secret Sharing (Публічно перевіренийанонімний шард) ;

SPV – Simplified Payment Verification (Спрощена перевірка транзакції) ;

VDF – Verifiable Delay Function (Функція перевірки затримки) ;

VRF – Verifiable Random Function (Функція перевіркивипадковості).

ВСТУП

Актуальність дослідження. Протягом останнього часу дуже стрімко розвивається технологія розподіленого реєстру. Дана технологія не тільки активно обговорюється, а й стала впроваджуватися в більшості розвинених країн у багатьох галузях. Багато організацій мають на меті розібратися в можливому застосуванні технології як для пошуку шляхів розвитку різних індустрій так і для оптимізації поточних процесів. На даний час технологія розподіленого реєстру має значення, порівнянне з такими інноваціями свого часу, як інтернет і телеграф. Потенціал технології буде розкритий поступово в найближчі 5-10 років, але вже за кілька останніх років реалізовані проекти із застосуванням даної технології у різних сферах, основною з яких є фінансова індустрія. Застосування технології відкриває нові бізнес-можливості і кардинально оптимізує поточну діяльність підприємств і банків.

Існуючі приклади застосувань технології свідчать про те, що швидкість її розвитку зростає в геометричній прогресії, а разом з нею зростають і вимоги до фахівців у всіх сферах роботи. Розподілена база даних блокчейн все більше інтегрується в системи зберігання та контролю документів. Перевага цієї технології полягає у відсутності практичної можливості маніпуляції даними, записаними в систему, завдяки тому, що інформацію в базу даних можна тільки додавати, але не перезаписувати. У той же час, істинність документа легко підтверджується, так як кожен бачить, ким він був записаний у блокчейн. Нарівні з особи і банківським сектором, технологія не обійшла стороною і систему освіти. Актуальним є опис як самої технології, так і застосування рішень на розподіленому реєстрі для навчання. Наявність динамічного моніторингу вимог компаній до кандидатів із знанням технології блокчейн, а також зростання популярності масових відкритих онлайн курсів і онлайн освіти в цілому, дозволяє освітнім організаціям безболісно підлаштовуватися під тенденції розвитку в галузі освіти, а також налагодити відносини без посередників між ними (конкретними

університетами освітніми організаціями, учнями і підприємствами, працюючи як єдина система завдяки блокчейн регістру.

Метою дослідження є покращення методів реалізації технології блокчейн для подальшого застосування у сфері освіті.

Для досягнення поставленої мети необхідно виконати такі завдання:

- 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.

Об'єкт дослідження – технологія розподіленого реєстру – блокчейн.

Предмет дослідження – методи реалізації технології блокчейн у сфері навчання.

Методи дослідження – методи впровадження технології блокчейн у сферу навчання, порівняння алгоритмів по критеріям безпеки, надійності, масштабованості та доцільності використання.

Наукова новизна отриманих результатів: модифікація шардингу шляхом масштабованої генерації випадковості та протокол консенсусу, в якому використовується багатофункціональний підпис, що забезпечує швидкодію, надійність та енергоефективність блокчейну.

Практична цінність отриманих результатів: можливість використання запропонованих методів для створення масштабованого та надійного блокчейну та доцільність використання методів для їх подальшого застосування у сфері навчання.

1 АНАЛІТИЧНИЙ ОГЛЯД ТЕХНОЛОГІЙ РОЗПОДІЛЕННОГО РЕЄСТРУ ДЛЯ СТВОРЕННЯ ОСВІТНЬОГО СЕРЕДОВИЩА

1.1 Технологія розподіленого реєстру

Розподілений реєстр – це база даних, яка розподілена між декількома мережевими вузлами або обчислювальними пристроями. Кожен вузол отримує дані з інших вузлів і зберігає повну копію реєстру. Оновлення вузлів відбуваються незалежно один від одного [1].

Ключова особливість розподіленого реєстру – відсутність єдиного центру управління. Кожен вузол становить і записує оновлення реєстру незалежно від інших вузлів. Потім вузли голосують за поновлення, щоб упевнитися, що більшість вузлів згідно з остаточним варіантом. Голосування і досягнення згоди щодо однієї з копій реєстру називається консенсусом, цей процес виконується автоматично за допомогою алгоритму консенсусу. Як тільки консенсус досягнутий, розподілений реєстр оновлюється, і остання узгоджена версія реєстру зберігається в кожному вузлі.

Подібна технологія зберігання даних розподіляє інформацію між безліччю вузлів зв'язку або обчислювальними пристроями. Вона має кілька ключових особливостей:

- відсутність центрального адміністратора;
- спільне використання з синхронізацією за заданим алгоритмом;
- децентралізований географічний розподіл копій бази даних між усіма вузлами зв'язку.

За своєю суттю це перша база даних, яка позбавляє необхідності задіяти центральний сервіс, розподіляє базу по всіх вузлах зв'язку, покладаючи на них відповідальність за підтримку системи і перевірку інформації [2].

Класичка база даних – це організована структура, призначена для зберігання, зміни і обробки взаємозалежної інформації, переважно великих обсягів. Бази даних активно використовуються для функцінування мережі Інтер-

нет, зокрема динамічних сайтів зі значними обсягами даних - часто це інтернет-магазини, портали, корпоративні сайти. Такі сайти зазвичай розроблені за допомогою серверного мови програмування (як приклад, PHP) або на основі CMS (як приклад, WordPress), і не мають готових сторінок з даними за аналогією з HTML-сайтами. в результаті взаємодії скриптів і баз даних після відповідного запиту клієнта до веб-сервера.

У розподіленій базі даних кожен вузол вносить зміни до реєстру незалежно від інших вузлів, потім всі вони голосують за внесення змін і при досягненні консенсусу реєстр доповнюється новими даними. Кожен учасник мережі при цьому володіє власною ідентичною копією реєстру, а самі зміни додаються протягом декількох хвилин.

Технологія розподіленого реєстру істотно зменшує витрати на довіру. Використання розподілених реєстрів допоможе зменшити залежність від банків, державних органів, юристів, нотаріальних контор і регламентують органів [3].

Розподілені реєстри представляють нову парадигму збору і передачі інформації. Вони здатні докорінно змінити способи взаємодії між фізичними особами, підприємствами та державними органами.

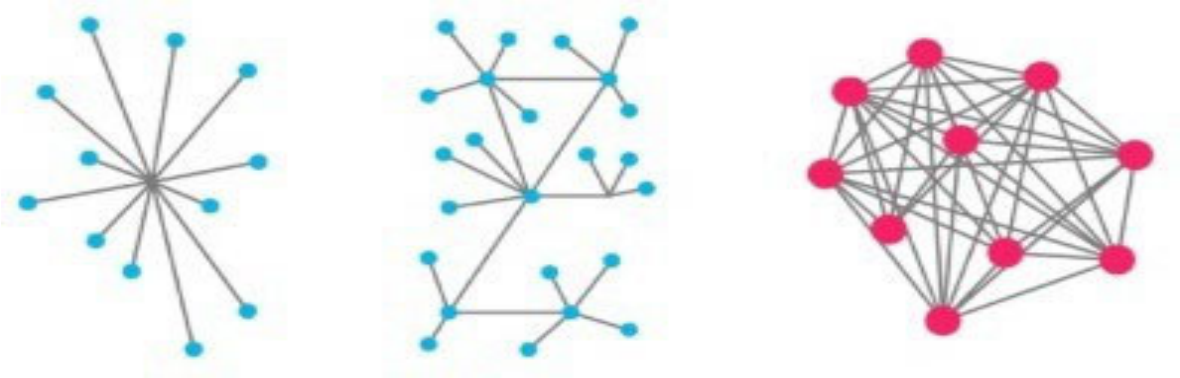

Рисунок 1.1 – Централізований, децентралізований та розподілений реєстри

Розподілений реєстр став відомий широкому колу людей в основному завдяки його застосуванню в блокчейні криптовалюті, але вноситися в нього можуть будь-які дані: фінансові, юридичні, статистичні, електронні та інші.

Розподілений реєстр цифрових транзакцій - лише один з різновидів баз даних, заснованих на реєстрах. Їх усіх можна розділити на:

Публічні – застосовуються в більшості криптовалютах і являють собою базу даних з відкритим вихідним кодом. Вони працюють на алгоритмах Proofof Work. У такій системі кожен учасник може завантажити собі на локальний пристрій базу даних і брати участь в узгодженому процесі внесення змін. Також усі охочі можуть переглянути всю додану інформацію.

Федеративні – бази даних працюють під управлінням групи людей. На відміну від відкритих реєстрів вони не підтримують внесення нових даних усіма бажаючими. Процес зміни реєстру контролюється виключно заздалегідь вибраними вузлами зв'язку. Застосовуються вони переважно в банківському секторі і забезпечують більшу конфіденційність.

Приватні – право на внесення змін до такого реєстру має тільки певна централізована організація. Інформація може бути відкрита для публічного читання або бути обмеженою в довільній ступеня. Приватні розподільні реєстри, як правило, використовуються компаніями для зберігання внутрішньої інформації та проведення аудиту. Такі системи більш уразливі, ніж публічний блокчейн, але дозволяє модернізувати застарілі системи зберігання інформації в компаніях[3].

Технологія DLT (Distributed Ledger Technology) досить різноманітна і дозволяє зберігати інформацію будь-якого роду, що робить її легко застосовної в усіх галузях, де потрібне безпечне зберігання даних.

Блокчейн - це один з видів розподіленого реєстру. Не всі розподілені реєстри використовують послідовність блоків для досягнення достовірного консенсусу в розподіленої системі захищеним від зловживань способом. Блокчейн розподілений в тимчасову мережу та управляється за допомогою цієїмережі. Так як це окремий випадок розподіленого реєстру, він може існувати без центральної влади або керуючого сервера, а якість даних в блокчейнеі забезпечується реплікацією бази даних і довірою, заснованому наобчисленнях.

Однак структура блокчейна відрізняється від структури інших видів розподілених реєстрів. Дані в блокчейні згруповані і організовані в блоки. Блоки з'єднані один з одним і захищені криптографічними методами.

Блокчейн – це постійно зростаючий реєстр записів. У блокчейн можна тільки додавати дані. Не можна видаляти або змінювати дані, збережені в попередніх блоках. Тому технологія блокчейн добре підходить для запису подій, управління записами, обробки транзакцій, відстеження операцій з активами і голосувань. Блокчейн складається з ланцюжка блоків - баз даних, куди записується інформація про всі схвалені транзакції в мережі, що робить їх свого роду регістром. Всі блокчейн-мережі починають свою роботу з первинного блоку (Genesis block), до якого приєднуються всі наступні блоки. Блок – це регістр, в якому міститься інформація за останніми транзакціях, і розмір кожного блоку обмежений. Це означає, що повна історія всіх транзакцій ніяк не поміститься в єдиний блок, відповідно, для роботи мережі необхідна ланцюжок блоків - буквально, блокчейн. На рисунку 1.2 зображено схематичне представляння блокчейну.

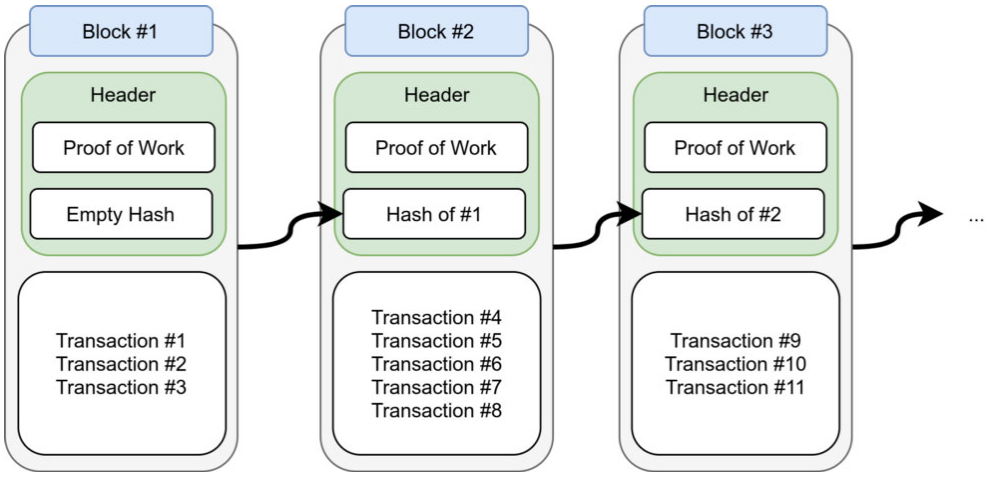

Рисунок 1.2 – Схема блокчейну

Кожен блокчейн - це розподілений реєстр, але не кожен розподілений реєстр – блокчейн. Обидва ці поняття мають на увазі децентралізацію і досягнення консенсусу між вузлами. Крім того, у блокчейні дані організованів блоки, і дозволено тільки додавати нові дані. Розподілені реєстри в цілому іблокчейн

зокрема являють собою концептуальні прориви в управлінні даними,які напевно знайдуть застосування у різних галузях.

Вперше технологія блокчейн була застосована в криптовалютах, таких як Bitcoin. Вибухове зростання Bitcoin в кінці 2017 і вибуховий навколо нього ажіотаж в ЗМІ привернули увагу громадськості до криптовалюти. Тепер уряд, комерційні організації, економісти і ентузіасти шукають інші способи застосування блокчейн-технології.

Перевагами розподіленого реєстру є:

- Високий рівень прозорості, ефективність, автоматизація. Контроль над мережею переданий самим користувачам і розподілений по всій мережі.
- Потенціал здійснення швидких і дешевих транзакцій через скасування необхідності посередників, третіх осіб або центрального контролюючого органу.
- Високий рівень безпеки завдяки інноваційній системі зберігання інформації в розподіленої по всій мережі базі даних. Таку систему вкрай важко зламати, а дані - змінити або підробити

Традиційні бази данихБаза даних, за визначенням, - це організований, систематизований набір деякої інформації. Найпоширенішим на сьогоднішній день видом баз даних є реляційна база даних (relational database). Популярність запитів бази даних можна представити у вигляді деякої таблиці (сутності), що складається з стовпців і рядків (кортежів).

Реляційна база даних, в свою чергу, являє собою набір взаємопов'язаних між собою деякими відносинами кількох таких таблиць (сутностей). Такий вид баз даних заснований на реляційній моделі даних - логічної моделі даних, сформульованої ще в 1970 році британським вченим Е.Ф. Коддом. Для роботиз такими базами зазвичай використовується декларативний мову програмування SQL. Найпопулярнішими реляційними системами управління баз даних є

рішення, що надаються компаніями Oracle (Oracle Database), IBM (IBM DB2) і Microsoft (Microsoft SQL Server).

Реляційні бази даних відрізняються високим ступенем централізації: будь-які операції з даними (запит, зміна, додавання, видалення та ін.) Обробляються єдиним центром (процесором, CPU), сервера якого, частіше завсе, фізично розташовані в одному місці і адміністрування яких здійснюється таким собі спеціальним особою / організацією. Користувачі в такій системі працюють з даними в форматі «запит - відповідь».

Інший великий вид баз даних - розподілена база даних (distributed database, DDB), яка, по суті, являє собою мережу з декількох взаємопов'язаних баз даних (нодов), розподілених у комп'ютерній мережі. Будь-які операції з даними в такій базі обробляються децентралізовано - мережею з декількох центрів (процесорів, CPU), при цьому дані розподілені по різним сховищ (серверів) і навіть можуть частково дублюватися. З розвитком інтернету,потреби компаній у зберіганні та обробці великої кількості структурованих і неструктурованих даних росла, а розподілені бази даних виявилися найбільш відповідними у плані підвищеного рівня відмовостійкості (відсутність єдиної точки відмови, вихід із ладу якої спричинить за собою непрацездатність всієї бази) і масштабованості (віддалена оренда хмарного сервера обходитися дешевше і вигідніше для деяких видів бізнесу, ніж покупка нового фізичного сервера).

Відомими розподіленими базами даних є: розподілені SQL бази (від Microsoft, Oracle, IBM і ін.); нереляційні NoSQL бази (MarkLogic, MongoDB ін.); NewSQL (Google Spanner, Clustrix), які об'єднують в собі перші двапідходу; проект Hadoop, який використовується для обробки і зберігання т.зв. "Великих даних". Всі вище перераховані бази, так чи інакше, побудовані на архітектурі "клієнт-сервер" - клієнти посилають деякі запити на читання або редагування даних, а сервера, об'єднані в розподілену мережу, їх виконують, зберігаючи ці дані у себе[4].

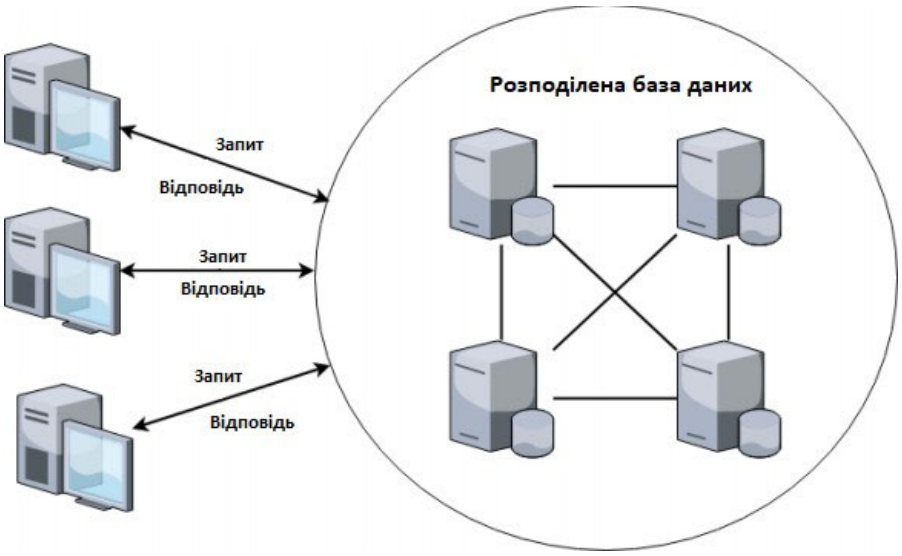

Рисунок 1.3 – Архітектура мережі типу клієнт-сервер для розподіленої бази даних

Існує й інший вид розподіленої мережі, званий одноранговою пірінговою мережею (peer2peer network), в якій можуть бути відсутні виділені сервери, а кожен клієнт одночасно є ще й сервером.

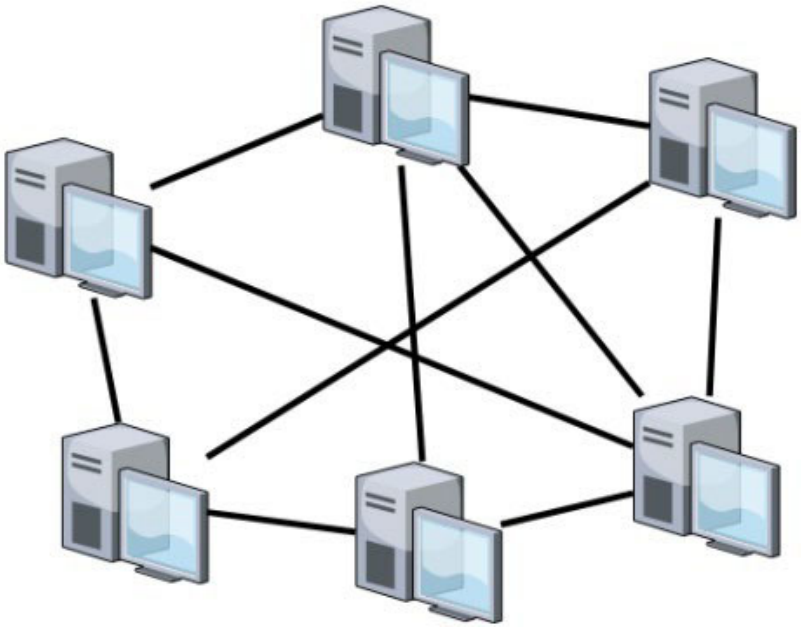

Рисунок 1.4 – Однорангова мережа

В явному вигляді пірінгові мережі, як мережі без виділених серверів, не використовувалися для побудови корпоративних баз даних. Проте, однією з найвідоміших реалізацією такої мережі став протокол BitTorrent, що дозволяє

користувачам надавати ("роздавати") різні файли для скачування іншим користувачам, які зберігши файл у себе також виступають в ролі "роздає".

Таким чином, файли реплікуються по мережі і доки хоч один з власників бере участь в процесі обміну, файл залишається доступний для інших. Варто зазначити, що така мережа є частково децентралізованої, так як без BitTorrent-трекера, умовно кажучи, сайту, який зводить користувачів один з одним, користувачі просто не зможуть взаємодіяти. Таким чином, можна виділити кілька важливих особливостей традиційних і розподілених баз даних.

Першою особливістю таких баз є централізація, так як за їх функціонування відповідає, зазвичай, один або кілька центрів відповідальності. Передбачається, що ці центри діють в умовах повної довіри один до одного, а також користуються довірою з боку користувачів. Під довірою в даному контексті розуміється неспотворене, несуперечливе і достовірне відображення інформації, що зберігається, а також забезпечення безперебійного доступу до неї. Більш того, на плечах центру лежить відповідальність за проведення та затвердження (схвалення або відмову) транзакцій - послідовності операцій над базою (наприклад, внесення або коригування даних), що переводять базу з одного цілісного стану в інший.

Друга особливість, це відбиваності даних в поточний момент часу. Кожен раз, коли клієнт в певний момент часу звертається до бази, він бачить її поточний стан, причому найчастіше без можливості побачити дані в тому вигляді, в якому вони були вчора, тиждень назад або рік тому. Звичайно ж, сучасні бази найчастіше пропонують можливості перегляду історії зміни того чи іншого елемента (так звані тривалі структури даних).

Адміністраторами баз на регулярній основі створюються резервні копії (бекапи), що представляють собою набір "зліпків" бази в певний момент часу. Проте, в таких базах абсолютно відсутній механізм верифікації того, що інформація не була змінена заднім числом, що знову призводить до проблеми довіри до адміністратора.

Третя особливість, це можливість клієнтом виконувати базові операції з даними, які охоплюють акронімом CRUD (create, read, update, delete) – створювати записи в базі, читати їх (можливість переглядати), оновлювати і видаляти їх.

1.2 Відмінності технології розподіленого реєстру від традиційних баз даних

Місце розподіленого реєстру в ієрархії видів баз даних представляєтьсяне зовсім очевидним. В першу чергу це пов'язано з плутаниною термінів база даних (database) і реєстр (ledger), які найчастіше вживаються як синоніми

Деякі експерти визначають розподілений реєстр як один з видів розподіленої бази даних [5]. Варто зазначити, що використання терміну реєстр (ledger), швидше за все, обумовлено його використанням також як термін, що позначає книгу записів деякої фінансової інформації в грошовому вираженні. В тому числі, головна бухгалтерська книга в англійській мові носить назву general ledger. Отже, цілком логічно, що перший створений блокчейн, а саме блокчейн біткоінів, який виконує функцію обліку транзакцій в деякій цифровий валюті, на сьогоднішній день визначають найчастіше як якусь базу даних, розподілену в комп'ютерній мережі між різними центрами (нодамі).

Незважаючи на загальну схожість даного визначення з визначенням розподіленої бази даних, розподілене реєстр має ряд особливостей. На відміну від класичної розподіленої бази даних, де різні частини бази зберігаються на різних вузлах, в розподіленому реєстрі передбачається зберігання всієї повної і актуальної бази на кожному з нодов. Дана, на перший погляд, надмірність обумовлена іншою характеристикою розподіленого реєстру - відсутністю довіри користувачів один до одного або до центру [6].

Такі умови можуть виникнути, наприклад, у випадку, коли у користувачів бази даних є підстави вважати, що центр, який її адмініструє, має можливість

маніпулювати даними. На рисунку 1.6 і 1.7 зображена діаграма, яка схематично демонструє розподілену базу даних і розподілений реєстр.

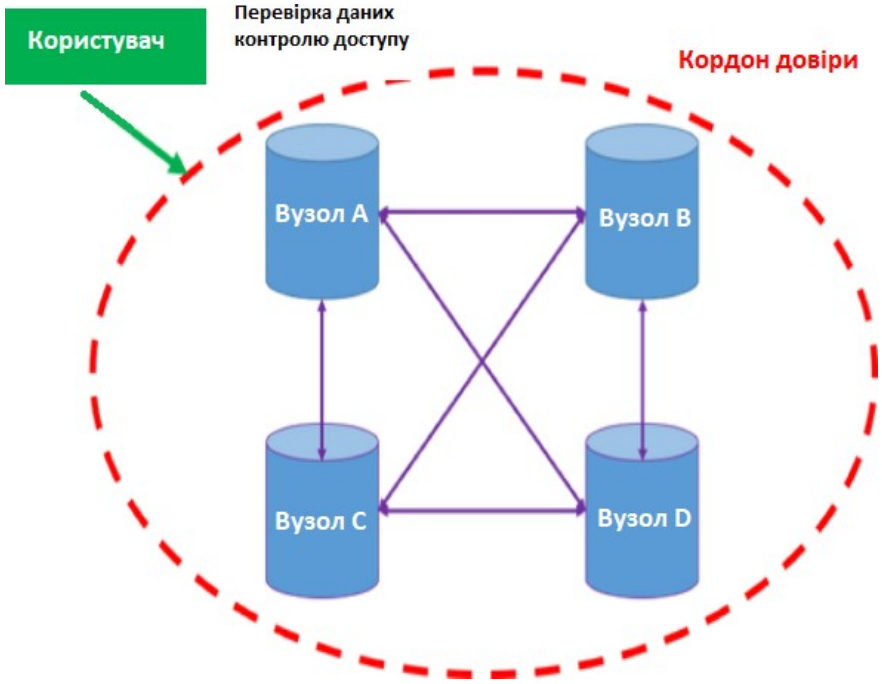

Рисунок 1.5 – Діаграма розподіленої бази даних

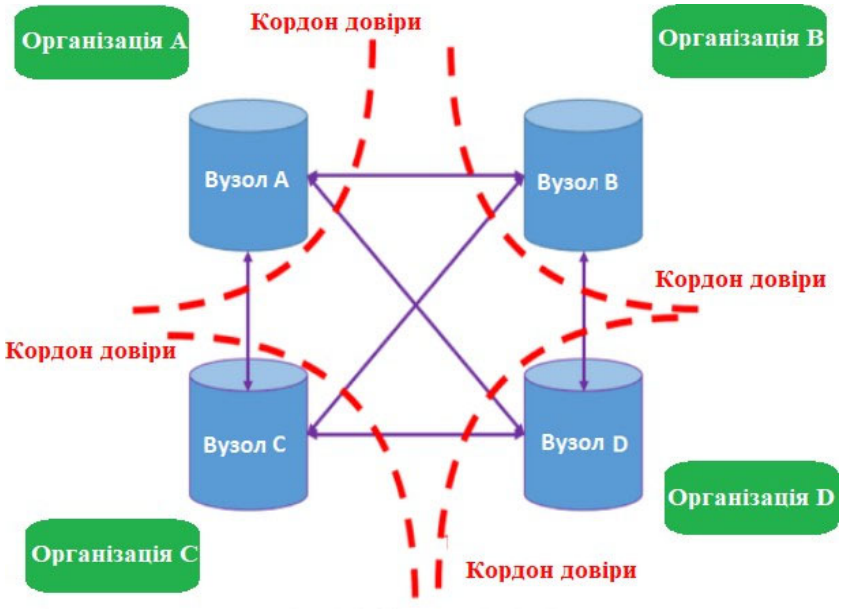

Рисунок 1.6 – Діаграма розподіленого реєстру

Червоним пунктиром на діаграмах позначені умовні "кордони довіри". У разі розподіленої бази даних всі ноди діють в умовах повної довіри, коли яку

разі розподіленого реєстру – довіра відсутня, а кожна нода, за якою стоїть окрема організація, вимагає верифікації одержуваних даних.

Виходячи з діаграми, слід також додати, що в умовах відсутності довіри база даних, побудована за технологією розподіленого реєстру, є одноранговою піринговою мережею. Ноди при такій архітектурі бази стають повноцінно рівнозначними учасниками. На відміну від традиційної бази даних, де вся відповідальність за правильність відображеної інформації лежить на деякому центрі, в розподіленому реєстрі всі ноди беруть участь в даному процесі.

За рахунок того, що кожен учасник постійно вносить нові записи в базу, виникає потреба в механізмі, який зможе залучити кожну ноду в процедуру узгодження внесення змін до бази, підмінивши, таким чином, функції центру в традиційній базі даних. Такий механізм носить назву механізм (алгоритм) консенсусу.

Механізм консенсусу являє собою певний комп'ютерний алгоритм, який лежить в основі розподіленого реєстру. На сьогоднішній день існує безліч механізмом консенсусу. Вибір конкретного механізму обгрунтовується цілями створення реєстру, а також природою активів в ньому відбитих.

Завданням механізму консенсусу є визначення легітимності (коректності) кожної виробленої в базі транзакції і винесення вердикту про можливість її проведення, з використанням заздалегідь певного методу криптографічного валідації, прийнятого в даному розподіленому реєстрі.

Також, даний механізм автоматизує процедуру вироблення єдиної думки серед учасників мережі щодо коректності відображення даних на поточний момент часу в розподіленому реєстрі. Іншим важливим завданням механізму консенсусу є вирішення конфліктів між деякими такими, що суперечать транзакціями, проведеними одночасно (проблема подвійного витрачання). Наприклад, операція над будь-яким активом в базі, ініційована в один і той же момент різними нодамb. Механізм коненсуса, таким чином, забезпечує послідовне виконання всіх транзакцій, а також виконує захисну функцію від захоплення кон-

тролю над розподіленим реєстром групою осіб, для проведення некоректних (нелегальних, що забезпечують, наприклад, подвійне витрачання) транзакцій (особливо, в разі загальнодоступногорозподіленого реєстру).

Іншою відмінною рисою розподіленого реєстру є активне, в порівнянні з традиційними базами даних, використання криптографічних методів. В першу чергу, мова йде про криптографічно стійкої хеш-функції (hash- function), яка являє собою односторонню функцію $h(\square\square)$, яка перетворює масив вхідних даних довільної довжини в бітний рядок встановленої довжини.

Другим технологічним аспектом, пов'язаним з криптографією в розподіленому реєстрі, є використання пари цифрових закритого і відкритого ключів. Відкритий ключ є похідним від закритого, причому створюється такожза допомогою деякої односторонньої криптографічно-стійкої функції. Дана пара ключів служить аналогом звичайного підпису на фізичних документах і виконує, по суті, ту ж саму функцію.

Можна провести аналогію з фізичної підписом, можна умовно порівняти відкритий ключ з тим, як підпис виглядає на папері, а закритий ключ - безпосередньо з рукою підписанта. Спостерігаючи відкритий ключ, одержувач має всі підстави вважати, що вхідне повідомлення / транзакція була підписана саме за допомогою закритого ключа певного підписанта.

При відправці деякого цифрового повідомлення відправник використовує свою пару відкритого і закритого ключів. Закритий ключ використовується для здійснення безпосереднього підпису повідомлення на етапі відправки, в той час як відкритий ключ - для перевірки цього підпису одержувачем. У разі якщо дана перевірка пройдена, приймач за допомогою свого закритого ключа може схвалити це повідомлення / транзакцію, і тоді інформація про неї буде виставлена в умовну чергу на схвалення іншими вузлами за допомогою механізму консенсусу. Після схвалення мережі, дане повідомлення / транзакція буде внесено до реєстру і проведено його копії всіміншим учасникам мережі.

Ще однією важливою особливістю розподіленого реєстру є зберігання всієї історії транзакцій. На відміну від традиційних баз даних, в яких основною одиницею обліку є актуальний стан або значення будь-якого атрибута, основною одиницею обліку розподіленого реєстру є транзакція. Маючи в розпорядженні всю історію транзакцій, можна дізнатися поточне значення того чи іншого атрибута. У зв'язку з цим фактом розподілені реєстри вважаються необоротними базами, так як зміна вже завершилися транзакцій, що мають підписану цифровим підписом певне значення хеш-функції, неможливо.

Хеш від підписаної транзакції, яка, наприклад, являє собою договір про передачу будь-якого активу від однієї особи іншій, спостерігається усіма учасниками мережі і схвалюється механізмом консенсусу, чинним в даному розподіленому реєстрі. Раз схвалена транзакція не може бути змінена, так як зміни хоча б одного символу в властивості транзакції призведе до кардинального перерахунку значення хеш-функції. Так як кожен нод зберігає у себе копію бази, то така зміна стане в ту ж секунду відомо іншим учасникам. Аналогічним чином неможливо провести і процедуру видалення або скасування транзакції, якщо вона вже одного разу була схвалена іншими нодамі в процесі роботи механізму консенсусу [7].

Отже, будь-яка зміна бази даних розподіленого реєстру може бути здійснено лише за допомогою нової транзакції, видалення ж або внесення правок, особливо у відкритих публічних реєстрах - неможливо. Варто також відзначити, що інформація в розподіленому реєстрі, в більшості випадків, носить псевдоанонімний характер, особливо в разі відкритого децентралізованого реєстру. Так як всі учасники можуть переглядати всю базу транзакцій, знаючи, яка особа стоїть за тим чи іншим якимось ідентифікаційним номером (в мережі біткоіни, наприклад, це номер гаманця), будь-хто може простежити історію транзакцій особи, яка цікавить. Таким чином, раз взявши участь в якій-небудь транзакції, врахованої в реєстрі, анонімність порушується, адже тепер обидві сторони транзакції знають, комуналежать дані гаманці / облікові записи.

1.3 Використання технологій розподіленого реєстру для створення освітнього середовища

В контексті актуальних напрямків розвитку освіти в умовах переходу до цифрової освіти виникає необхідність розглянути специфіку і особливості використання технології розподілених баз даних. Вказану технологію можна використовувати для вирішення як традиційних педагогічних завдань навчально-виховного процесу різного класу і рівня, так і інноваційних.

Дана технологія заслуговує на увагу педагогів і дослідників як варіант передової основи для пошуку нових ідей, оновлення існуючих і популярних сьогодні в педагогічній практиці методик навчання і технологій. Наприклад, використання як засіб навчання інформаційних технологій і науки

«Інформатика», таким як штучний інтелект, віртуальна і доповнена реальність, а також масові навчальні онлайн курси, або МУК (MOOC, massive open online course). Завдяки використанню «ланцюжків блоків» можливе проектування не тільки нових освітніх ресурсів для школи, а й нових освітніх курсів для навчання майбутніх учителів в умовах «цифрового освіти» [8].

Блокчейн створювався як середовище для передачі цінностей, перш за все фінансових, приблизно так само, як Інтернет - це середовище для передачі даних, наприклад, файлів, електронної пошти. Блокчейн являє собою електронну систему, в якій можна створювати різні додатки. Як і Інтернет, блокчейн має свої основні принципи функціонування - це децентралізація і множинне копіювання історії. «Інтернет цінність» - одна з найбільш вдалих метафор, що описують технологію розподіленого реєстру.

Блокчейн, одна з основних технологій, що лежать в основі криптовалюти - це електронна бухгалтерська книга, куди записується історія всіх грошових переказів (запис називається блоком, тому і «ланцюжок блоків» - blockchain). Відрізняє її те, що копії зберігаються у багатьох учасників мережі одночасно.Це і відрізняє блокчейн від централізованих інститутів минулого.

Максимально стисло блокчейн (Blockchain) можна охарактеризувати як вибудувану за певними правилами безперервну послідовну ланцюжок блоків, що містять інформацію. Однак блокчейн як вічний цифровий розподілений журнал транзакцій може бути запрограмований для запису не тількифінансових операцій, але і практично всього, що має цінність (права власності, дипломи про освіту і т.д.). Сама інформація, яку клієнт А передав клієнтові Б через блокчейн, може бути і «монетою» (тобто використовуватися як валюта), і «підписом», і «ліцензією» або якоюсь іншою цінністю [9].

Блокчейн-технологія, як і Інтернет, має вбудовану стійкість до помилок. Зберігаючи блоки інформації, ідентичні у всій мережі, блокчейн не дає можливості: контролювати систему комусь одному, мати єдину точку відмови (центр). Основні переваги блокчейна - надійність і децентралізація. У кожного учасника дублюється історія всіх транзакцій. кілька напрямків, де можливо і навіть необхідно використовувати блокчейн. Застовування блокчейну серед областей застосування у сфері освіти - надання кредитів на навчання, ідентифікація особистості учня (для заселення в гуртожиток або роботи в бібліотеці), оплата освітніх послуг, розподіл студентських стипендій і виділення грантів [10].

Роботи в галузі використання блокчейн в освіти поки знаходяться в початковій стадії. Серед вузів, чиї експерименти лягли в основу доповіді Єврокомісії, - Массачусетський технологічний інститут, Відкритий університет Великобританії, Університет Нікосії і кілька навчальних закладівМальти. На думку авторів доповіді, можливість реалізації запропонованих сценаріїв залежить від зусиль країн-учасниць ЄС з регулювання і стандартизації блокчейн. Державним органам пропонується підтримувати інноваційні приватні компанії і сформувати експертні комітети для впровадження блокчейн-рішень. Головна цінність технології блокчейн для освіти в тому, що вона гарантує надійність і безпеку збору і зберігання інформації, при цьому самі записи можуть містити різні типи даних.

Наприклад, за допомогою блокчейн можна зберігати інформацію про іспити, виданих дипломах і сертифікатах разом з інформацією про те, хто і коли

їх проводив або видавав. Таким чином, паперовий документ втрачає свою унікальність - тут всі бажаючі можуть негайно, не звертаючись до архівів видала його організації, переконатися в його автентичності та отримати його завірену копію. Елементами зберігання можуть бути не тільки дипломи і атестати про закінчення навчання, але і відомості про закінчення онлайн- курсів, здачі контрольних робіт [11].

Складовою частиною освітнього процесу є підсумкове оцінювання та атестація - іспити, кваліфікаційні роботи і інші навчальні заходи, в ході яких ті, яких навчають демонструють свої навчальні досягнення (знання, вміння, навички та здібності).

Освіта є одним з найбільш важливих секторів розвитку економіки країнита розквіту епохи «Нового технологічного світу» в цілому. Наприклад, навчання в інституті дає людині необхідну спеціалізацію і набір навичок, здатних забезпечити гідну зарплату і добробут. Для щоб проаналізувати, що може запропонувати технологія розподіленого реєстру у навчанні, варто визначити і обмежити різні галузі освіти, які можна буде проаналізувати з точки зору перспектив впровадження технології.

По-перше, необхідно розділити освіту на університетську і відкриту, що представляється сьогодні так званими масовими відкритими онлайн курсами (MOOC, Massive open online courses і т.д).

По-друге, у рамках університетського навчання має сенс розглядати безпосередньо освітній процес і супроводжуючі його адміністративно-управлінські аспекти з одного боку, а з іншого боку – результати освітнього процесу, документи про освіту або сертифікати про прослухані курси, укупі з урахуванням даних документів за межами окремого університету [12].

Природним середовищем для впровадження технології розподіленого реєстру в область освіти є майданчики масових онлайн-курсів. Відносно недавно вченою командою розробників був запущений проект DISCIPLINA 3,який представляє собою блокчейн платформу, що зводять разом студентів, навчальні

заклади, викладачів, а також, в перспективі, потенційних роботодавців. Використовуючи переваги розподіленого реєстру, розробники прагнуть вирішити проблему створення єдиного реєстру для обліку успішності студента за різними курсами, що надаються різними навчальними закладами, створити об'єктивну і достовірну систему рейтингування студентів, що значно може спростити пошук роботодавцями необхідних претендентів у відповідність з необхідними знаннями для заняття тієї або іншої позиції.

В такій відкритій системі оцінки і рейтингування може піддаватися абсолютно все - відгуки та рейтинги того чи іншого курсу або програми, репутація університету і роботодавців, що використовують такий реєстр.

Проблема оперування персональними даними, при цьому, вирішується тим, що в блоках будуть фіксуватися лише знеособлені хеші, коли як безпосередні досягнення студентів будуть зберігатися в їх особистих кабінетах. Доступ для роботодавців в систему передбачається платним.

Токени, обертаються у блокчейні DISCIPLINA, передбачається використовувати для оплати платних курсів і роботи по створенню блоків у ланцюзі. Аналогічна логіка дій можлива і в класичному університетському освітньому процесі, як мінімум в рамках освітніх установ, що беруть участь в Болонському процесі. Основний його рисою є уніфікована система кредитів, одержуваних за освоєння тієї чи іншої дисципліни. Певна кількість набраних кредитів за певними предметів дозволяє студенту отримати ступінь бакалавра, магістра або доктора наук [13].

Уніфікованість також полягає в тому, щоб спростити процедуру нострифікації (процедура визнання диплома країни при вступі до навчального закладу іншої країни) під час вступу до іншого університету для отримання наступному ступені освіти або навіть при простому переході з одного вищого навчального закладу до іншого. Проблема сумісності кредитів по одній і тій же дисципліні в різних університетах, проте, до сих пір вважається досить складною, тому що

навіть при повній відповідності освоюваних тим в рамках певного предмета, якість виклад і кваліфікація викладача може разюче відрізнятися.

Частина описаного процесу, котрий залежить від безпосередньо викладача, можливо значно спростити і автоматизувати, що і пропонують автори доповіді [14]. Автори передбачають створити децентралізований розподілений реєстр на блокчейні, доступ до якого повинен буде здійснюватися деяким механізмом реєстрації та ідентифікації осіб до нього приєднуються. Передбачається, що основною одиницею інформації в реєстрі будуть досягнення студентів, які, звичайно ж, з метою збереження персональних даних, повинні шифруватися.

Якщо студент отримує оцінку за іспит, то кожному студенту в рамках відомості присвоюється деякий випадковий ідентифікаційний номер (різний для одного і того ж студента на інших дисциплінах), який ставиться у відповідність його облікового запису, доступ до якої студент має за допомогою закритого ключа. У метаданих такий "залікової" транзакції про виставлення оцінки повинна міститися інформація про те, в якому університеті був іспит, кількість кредитів, кількість годин на освоєння, списокосвоєних тим і інші необхідні дані. У разі помилки організація повинна буде створити нову транзакцію про коригування балів із зазначенням причини. Всіметадані будуть є основою для створення смарт-контрактів.

Наприклад, якщо дві освітні організації домовляються про прийняття кредитів один одного за певними дисциплін при русі контингенту студентів між ними, то це фіксується смарт-контрактом. Таким чином, при перекладі студента взаємозалік дисциплін і складання індивідуального навчального плану відбувається автоматично за рахунок обліку вже пройдених дисциплін в іншому навчальному закладі внаслідок перевірки на відповідність вимог, встановлених смарт-контрактами в такій мережі. У перспективі побудова такої системи на базі технології розподіленого реєстру змогло б значно спростити рух контингенту, тим самим збільшуючи мобільність населення як в рамках країн, так і за

їх межами, фіксувати всі досягнення студентів у захищеному від підробки реєстрі, а процедура видачі дипломів стала б більш прозорою, з огляду на те, що освоєння всіх дисциплін завжди можна було б відстежити і перевірити.

Фахівці запропонували проект блокчейн платформи для обліку наукових публікацій [15]. Рішення, запропоноване на базі розробки блокчейн- платформи Hyperledger Fabric, являє собою закритий розподілений реєстр, учасниками якого передбачаються провідні міжнародні університети, дослідницькі та наукові центри та інститути, а також видавництва. В першу чергу, автори бачать перспективи блокчейна в даному сегменті як ефективний інструмент для вибудовування процесу рецензування публікацій, перевірки посилань на джерела, що знаходяться в рамках реєстру, створення системи для простого, децентралізованого підрахунку показників цитованості авторів. Останнє також пов'язане з можливістю побудови системи прозорого механізму оцінки якості академічних публікацій, їх значимості для всього наукового співтовариства. В даний час Google Академія (Google Scholar)використовується як основний джерело показника цитованості в якості проксі для значущості тієї чи іншої публікації або вкладу дослідника. Однак механізми, що лежать в основі даного сервісу непрозорі і немає впевненості втому, що алгоритм, по-перше, знаходить все цитати, а по-друге, індексує всі роботи автора. Створення аналогічного сервісу на базі розподіленого реєстру дозволило б подолати обмеження існуючих сервісів, надавши можливістьоб'єктивної оцінки діяльності академічних працівників.

Висновки до розділу

У даному розділі розкрито такі аспекти:

- Визначення і опис основних принципів роботитехнології розподіленого реєстру
- Поняття традиційної баз даних

- Встановлено переваги технології розподіленого реєстру відтрадиційної та розподіленої бази даних
- Можливості використання технології розподіленого реєстру врізних сферах
- Досліджено доцільність застосування технології розподіленного реєстру у сфері навчання

Встановлено, що головними перевагами технології розподіленого реєстру є висока швидкість операцій, безпека, можливість повноцінного контролю даних, децентралізація, багатофункціональність, універсальність, відкритість, публічність; простота, зручність і доступність. Головні недоліки: необхідність у стійкому криптографічному захисті, необхідність в інструментах передачі, користування і зберігання інформації, відсутність належного юридичного врегулювання і гарантій, недостатня поширеність,зацікавленість кіберзлочинності до нових технологій.

2 ТЕХНІЧНІ АСПЕКТИ СТВОРЕННЯ ТА РЕАЛІЗАЦІЇ ТЕХНОЛОГІЇ БЛОКЧЕЙН

2.1 Готові рішення для реалізації технології блокчейн у навчанні

У професора Дона Тапскотт вийшла стаття в журналі «Educase» під назвою «The Blockchain Revolution and Higher Education» [16]. У ній блокчейн виступає як основа для нової ери Інтернету - Інтернету цінностей, а його роль у вищій освіті підрозділяється на чотири категорії:

- ідентифікація та студентський облік: як ідентифікувати студентів,захищати їх конфіденційність, оцінювати, вести облік, перевіряти досягнення,зберігаючи ці дані в безпеці;
- нова педагогіка: як налаштувати викладання під кожного учня і створювати нові моделі навчання;
- витрати (студентські заборгованості): як оцінювати і фінансувати освіту, як винагороджувати студентів за якість їх роботи;
- розвиток університетської освіти: як розробляти абсолютно нові моделі вищої освіти.

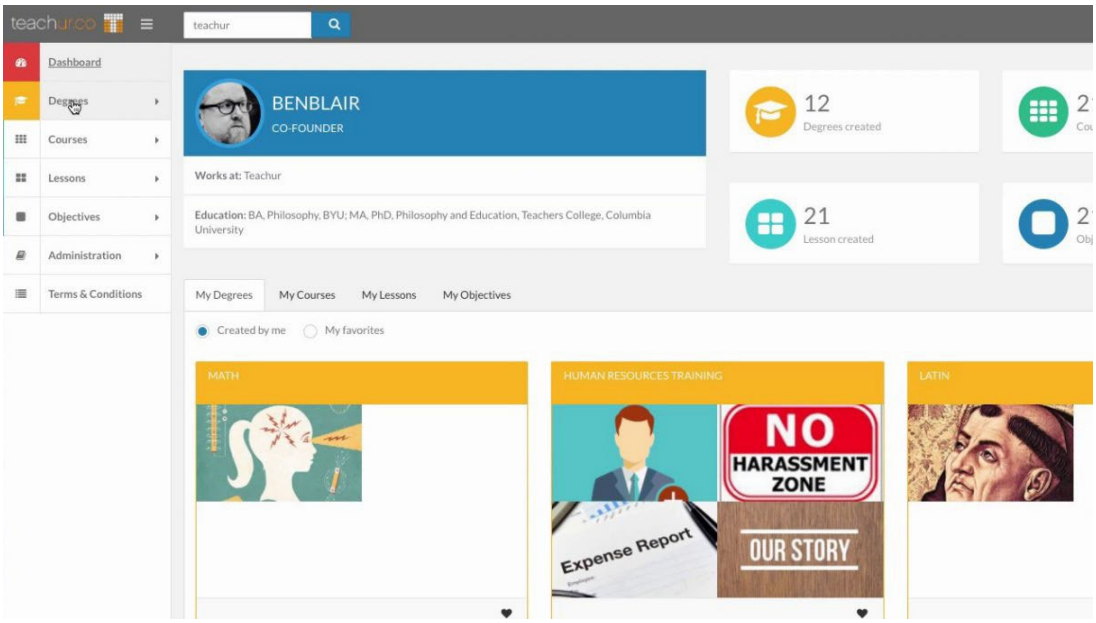

Рисунок 2.1 – Інтерфейс системи Teachur

Співзасновником проекту Teachur Беном Блейр на платформі для соціальної журналістики «Medium» розміщені ряд корисних для темидослідження статей, зокрема, наводяться особливості самого проекту Teachur, реалізованого на технології блокчейн.

В статті [17] розглянуто проблеми в освіті початкової та середньоїшколи, який може вирішити проект Teachur. Його суть полягає в новому підході для оцінювання учнів з тих чи інших стандартів, суворої і безпечної системі зберігання цих даних і в легкості її перенесення. Особливість інноваційної системи оцінювання полягає в тому, що оцінка зв'язується з тимизнаннями і цілями, які були поставлені з той чи інший момент часу, і шлях яких грунтується на попередніх знаннях, метою і оцінках, подібно до того, якзв'язуються в ланцюжка блоки у блокчейні, гарантуючи безпеку і легкість їх перенесення, при цьому дозволяючи здійснювати оцінку більш творчо і експериментально, на відміну, наприклад, від тестування.

В [18] розповідається про чотири способи застосування технології блокчейн у вищій освіті, реалізованих в проекті Teachur:

- облік процесу навчання;
- смарт-контракти для отримання диплома;
- смарт-контракти для двостороннього ринку;
- токени платформи Teachur.

Цілі, досягнуті в процесі навчання, вдають із себе надійний і повний звіт про діяльність учня, яким вони можуть в будь-який момент поділитися, якщо побажають, що дозволяє легко знаходити співробітників і партнерів з необхідними навичками.

Отримання диплома вдає із себе смарт-контракт, що виконується автоматично при виконанні необхідної умови, що відразу стає достовірним підтвердженням здібностей учня. Викладачі можуть отримувати відрахуванняза частку або цілу частину від розробки і подальшого використання курсовихробіт, нав-

чальних матеріалів. В системі реалізовані власні маркери, які можна отримати як раз в вигляді відрахувань або за інший вид роботи. Таким чином,робота з системою стає економічно вигідною.

Дослідженнями в області застосування смарт-контрактів в процесі навчання поділився Бен Блейр в роботі [19], де смарт-контракти використовуються для всього навчального плану, коли досягнення певної контрольної точки навчального плану пов'язано з певним жорстко прописаними умовою, а всі навчальні матеріали є інтелектуальною власністю їх творця, за використання яких він отримує відрахування. Успішна робота по навчальних матеріалів певних викладачів збільшує попит на них, що стимулює їх до створення високоякісних матеріалів.

Про те, щоб стати першими, хто запровадить блокчейн для підтвердження дійсності атестатів і сертифікатів кандидата на його відповідність необхідним компетенцій, написав Люк Паркер в статті [20], яка,по суті, є коротким оглядом застосування технології таким чином.

Питаннями захисту та підтвердження дійсності сертифікатів, а також системою репутації за допомогою блокчейна особливо займаються в Массачусетському технологічному інституті. Ними були випущено кілька версій програми Blockcerts з відкритим вихідним кодом, що реалізує облік і видачу сертифікатів з можливістю ділитися ними з роботодавцями. На рисунку 2.2 представлена архітектура їх програми.

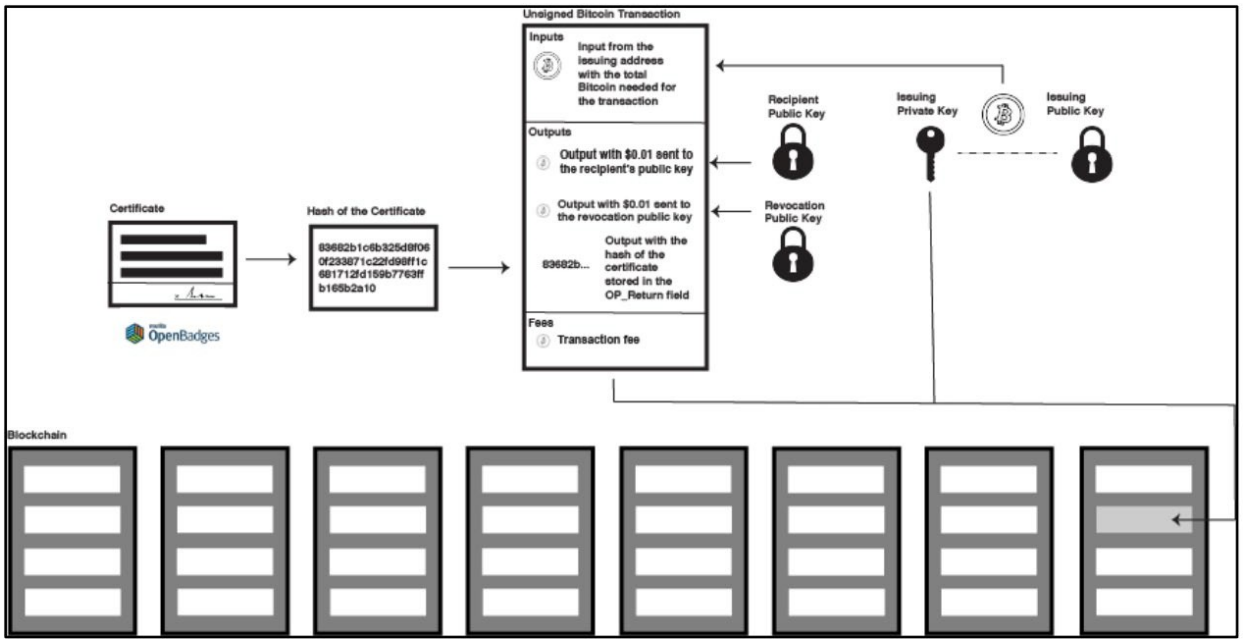

Рисунок 2.2 – Архітектура програми цифрових сертифікатівМассачусетського технологічного інституту

Опис програми наведений у статті [22], також вказані проблеми, з якими вони стикаються в своїй роботі: забезпечення можливості ділитися своїми академічними досягненнями з одними, але при цьому тримати їх в таємниці від інших. Більш того, Массачусетський технологічний університет в цьому році надає можливість студентам отримати цифрову версію їхніх дипломів на блокчейні в рамках експериментальної програми, що дозволяє зробити академічні дані безпечними і портативними.

Також на платформі «Medium» опублікована ще одна стаття, що стосується технології блокчейн в освіті [23]. У ній блокчейн виступає в ролі захисту навчальних даних учнів, які формуються і підлаштовуються під учня адаптивними системами діагностики (наприклад, i-Ready, Edulastic). Вособистому блозі Одрі Уоттерсом було проведено розбір спочатку історії і роботи технології блокчейн, а потім розглянуті можливості її застосування в освіті [24].

На сайті Hackernoon, де розміщуються статті, що стосуються хакінгу (взлому), розробки штучного інтелекту та криптовалют, розміщена стаття [25], в якій розглядаються інноваційні ідеї для освіти із застосуванням блокчейна,

платформа для навчання LiveEDU, проводяться деякі паралелі з дистанційним навчанням, поняттям масових відкритих онлайн-курсів (MOOC).

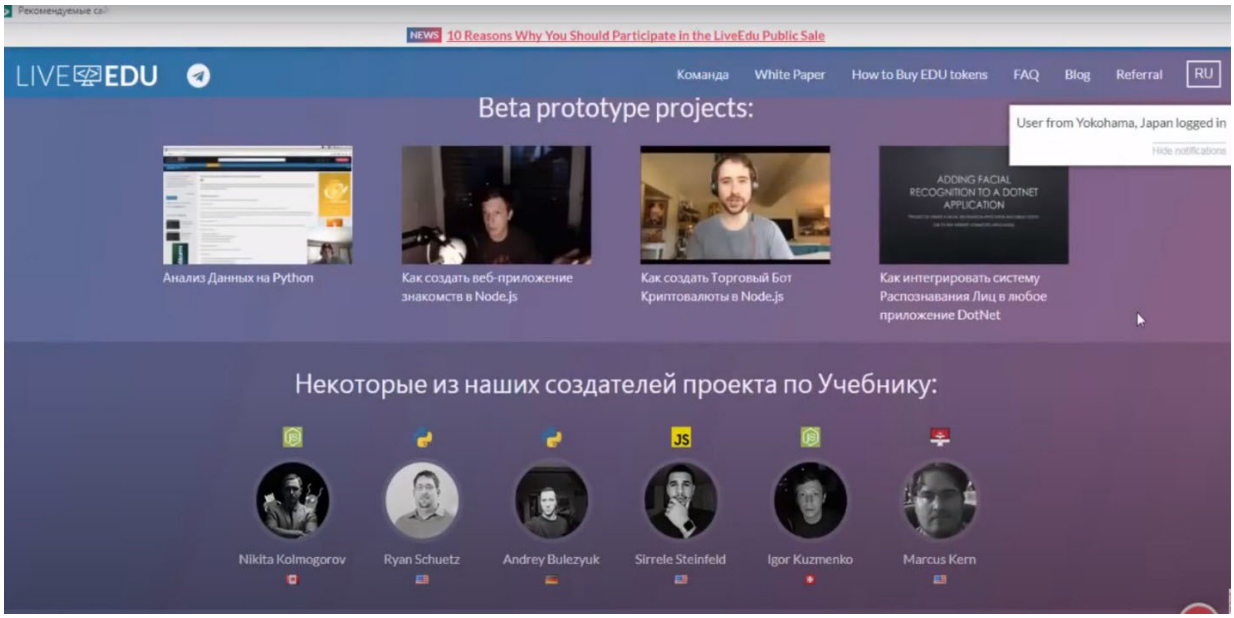

Рисунок 2.3 – Сервіс для навчання LiveEDU

Подібний приклад уже траплявся, коли на тлі розвитку мережі Інтернет багато процесів стали приймати електронний вигляд, в тому числі це торкнулося і освіти, так з'явилося електронне навчання (e-learning), а потім і масові відкриті онлайн-курси (MOOC), зав'язані на навчанні дистанційно.

Яскравим прикладом такої форми навчання став проект Codecademy, що вдає із себе майданчик для вивчення програмування в прямому ефірі. Можливість отримати знання з будь-якої точки світу, а також більш низьку вартість або зовсім безкоштовне навчання не могла залишити людей байдужими. Комбінування різних курсів дозволяє пропонувати учнем різні стратегії навчання.

Впровадження технології блокчейн, дозволить стандартизувати видавані документи, що в свою чергу може стандартизувати освіту в усьому світі. Підтверджені знання і навички кандидатів можуть зберігатися в єдиній базі да-

них, що дозволить вибирати кандидатів по динамічному відбору виходячи з їх набору умінь і необхідних навичок для обраної посади [26].

Підсумком створення даної бази даних буде наявність відкритого ринку кандидатів з підтвердженими знаннями. А це в свою чергу дозволить створити попит на конкретні компетенції і створить тенденції на вивчення певних освітніх програм, в результаті яких і формуються ці компетенції. Освітні організації будуть в реальному часі бачити картину необхідних кандидатів і випускати відповідні освітні програми або навчальні курси. В результаті це дозволить скоротити розрив між ринком праці і ринком освіти, а також вирішити проблему стрімкої деактуалізації навчальних програм, жваво в ході стрімкого зростання інформаційних технології. Сьогодні навчання та підтвердження дійсності атестатів і сертифікатів кандидата на його відповідність необхідним компетенцій є дорогим і тривалим процесом як для освітнього закладу, так і для підприємства.

Підприємство, в разі невідповідності кандидата певним вимогам, в майбутньому може зазнати збитків. Деякі школи звернулися за допомогою дотехнології блокчейн, як до недорогого і надійного способу запису академічних успіхів учня, який представляє з себе децентралізований регістр, надійнозберігає дані в Інтернеті з відкритим доступом для публіки [26]. Один з таких прикладів - Holberton School of software engineering (школа розробників програмного забезпечення), яка була створена як проект-альтернатива коледжам. У жовтні 2015 року школа оголосила про 54 намір зберігати атестати студентів на блокчейн, починаючи з 2017 року.

Японська компанія Sony, яка створила сервіс Sony Global Education, в кінці 2017 роки вже використовує технологію блокчейн при видачі сертифікатів. Своїм прикладом вони збираються показати, як дана технологіястане майбутнім в області забезпечення достовірності знань, які навчаються в освіті. Так само планується показати можливості технології на прикладі «наступного покоління IT-школи» для Міністерства внутрішніх справ Японії [27].

Sony Global Education вважають, що індивідуальні дані про продуктивність якого навчають в освіті так само цінні, як, наприклад, персональна кредитна історія. При використанні технології блокчейн дані будуть захищені цифровим підписом і можуть бути безпечно передані іншим зацікавленим особам. Збереження достовірних даних дозволить отримати повну історію учня (наприклад, комп'ютерний тест) на повністю захищеною платформі [28]. Таким чином, реалізація технології блокчейн в освіті вже зараз знаходить своє застосування.

Звичайно, основний упор зроблений на реалізацію можливості безпечного зберігання сертифікатів, атестатів, дипломів та успішності учнів, що може вирішити такі завдання:

- стандартизація та глобалізація освіти (можлива стандартизація без глобалізації);
- наявність достовірного, відкритого і єдиного ринку кандидатів з підтвердженими знаннями;
- актуальність освітнім програм, а отже, скорочення розриву між ринком праці і ринком освіти.

В Об'єднаному науково-дослідному центрі Європейської комісії опубліковано велике дослідження «Blockchain in Education» [29], що зачіпають багато аспектів тих чи інших способів застосування блокчейна у сфері освіти. На основі проведеного дослідження виведено сім сценаріїв застосування технології розподіленого реєстру в освіті:

1 Забезпечення постійної захисту сертифікатів учнів.
2 Використання блокчейна для багатоступінчастої акредитації.
3 Інтелектуальне розпізнання та передача коштів за допомогою блокчейна.
4 Використання блокчейна як паспорта з навчання на все життя.
5 Отримання платежів від студентів через блокчейн.
6 Надання студентам фінансування через блокчейн у форме ваучерів.

7 Ідентифікація студентів в освітніх організаціях.

Існує декілька прикладів впроваджених застосувань розглянутогометоду.

Медіалабораторія MIT почала використовувати блок-схеми для видачі цифрових сертифікатів групам людей у своїй розгалуженій мережі. Протягом усього часу MIT став захисником одержувачів, які мають більше повноважень щодо сертифікатів, які вони отримують, і не залежачи від сторонніх посередників, як університети та роботодавці, записи,перевіряти та перевіряти часто за додаткові витрати. Інновації Blockchain тапотужна криптографія були використані для розробки відкритої платформиBlockcerts для цифрових сертифікатів. У 2017 році MIT використовувавсертифікати Learning Machine, бізнес-рішення, створене за допомогоюBlockcerts, для надання дипломів студентам MIT Media Lab (Media Arts andSciences) та Sloan School of Business. Це перший приклад видачі такихсертифікатів, з використанням технології LM та єдиним прикладом дипломів,що належать одержувачам. (Schmidt, 2015; MIT Media Lab, 2016).

У той час як навчальні заклади прагнуть розмістити дипломи на своїх власних блокчейн-системах, японський гігант Sony вже займаєтьсяоб'єднанням документів про освіту в єдиному онлайн-сховище.

Побудована на блокчейні база працює на Hyperledger Fabric 1.0, система буде об'єднувати дані з «кількох навчальних закладів» та «дозволить записувати і посилатися на освітні дані і цифрові дипломи». В кінцевому підсумку Sony прагне синхронізувати всі види даних, пов'язаних з утворенням, починаючи від реєстрації учнів, відвідуваності, оцінок і планів уроків викладачів до записів результатів навчання учнів і т.д. Крім того, студенти зможуть збирати всі свої академічні оцінки і записи в цифровий об'єкт для офіційного використання.

Також одним із працюючих на даний момент навчальним ресурсом, що використовує технологію блокчейн є Фінансова академія Актив.

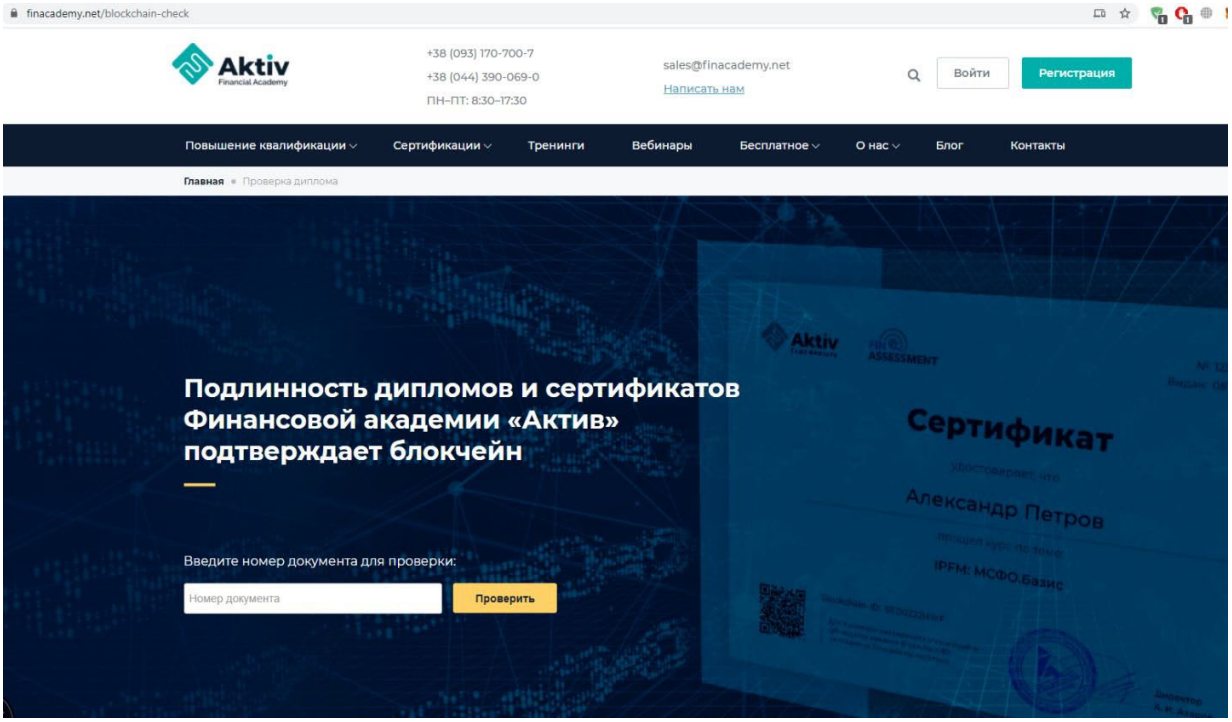

Рисунок 2.4 – Сайт фінансової академії «Актив».

На сайті академії завдяки блокчейн-технології, можна перевірити справжність дипломів і сертифікатів, а також переглянути "історію" їх отримання. Дані оцінювання і процесу навчання заносяться в блокчейн і мають більш високу цінність для роботодавця, так як їх неможливо підробити або замінити заднім числом. Документ в потрібний момент під рукою - досить знати його номер. Історія проміжного тестування і навчання показує роботодавцю прагнення студента регулярно навчатися і підвищувати свій рівень професійних знань. Для роботодавця це дає можливість наймати в компанію висококваліфікованих фахівців, чиї навички записані в блокчейні за номером або QR-кодом документа. В такому разі перевірити можна не тільки його справжність, а й переглядати історію його отримання. Також є можливість перевірити, "термін придатності" кваліфікації співробітника.

У своїй роботі Фінансова академія «Актив» використовує блокчейн Emercoin. Emercoin (Емеркойн, EMC) - блокчейн платформа, працює з 2013 року. Відмінні риси блокчейну: висока надійність, стійкість до помилок і гібрид-

ний тип Майнінг «три в одному» (PoW + MergedMining + PoS). Спеціалізація: рішення в сфері безпеки, конфіденційності, захисту авторських прав, підробок, обміну даними та мікроплатежів. Для видачі та перевірки сертифікатів використовуються ідентифікатори, які містять 10 символів і генеруються випадковим чином для кожного клієнта. Наприклад, «X0FTBV6E09».

Як тільки людина вступає на будь-який з курсів або тренінгів, система Фінансової академії «Актив» в автоматичному режимі передає в блокчейн ключову інформацію:

- вхідне оцінювання;
- факт вступу на навчання;
- підсумкове тестування;
- факт закінчення навчання.

Всі дані закріплюються за ідентифікатором. Після першого запису унікального номера в блокчейні, дані по ньому незмінні, захищені від підробки і можуть доповнюватися тільки його творцем - Фінансовою академією «Актив».

Рисунок 2.5 – Приклад запису у блокчейн Emercoin

Записи в блокчейні зберігаються суто в технічному вигляді і складні для більшості користувачів. Тому академія має спеціальну сторінку перевірки і розшифровки цих даних за номером або QR-кодом документа.

На цій сторінці можна виводити ключову інформацію за номером документа. В поле для перевірки потрібно ввести унікальний ідентифікатор і натис-

нути «Пошук». Система робить запит на пошук даних по конкретному номеру. Блокчейн видає відповідь в такому технічному вигляді:


```
09:42:15 [
  {
    "txid": "0e7ea3663d577ca3cbd0ee738d6c0539e374bc09a363891f909ce23dd481f7c1",
    "time": 1542630179,
    "height": 325401,
    "address": "EZkoDreFxEe9FcmonR4UByG88t4Fq2zyPq",
    "operation": "name_new",
    "days_added": 9999,
    "value": "type=testing\n,position_id=4\n,position_name=Функции Excel (PRO)
\n,value=85\n,end_time=1574158505160\n,company=Finacademy"
  }
]
```


Рисунок 2.6 – Отримана інформація від блокчейну післявідповідного запиту

Отримана блокчейном інформація дешифрується і виводиться на сторінці сайту.

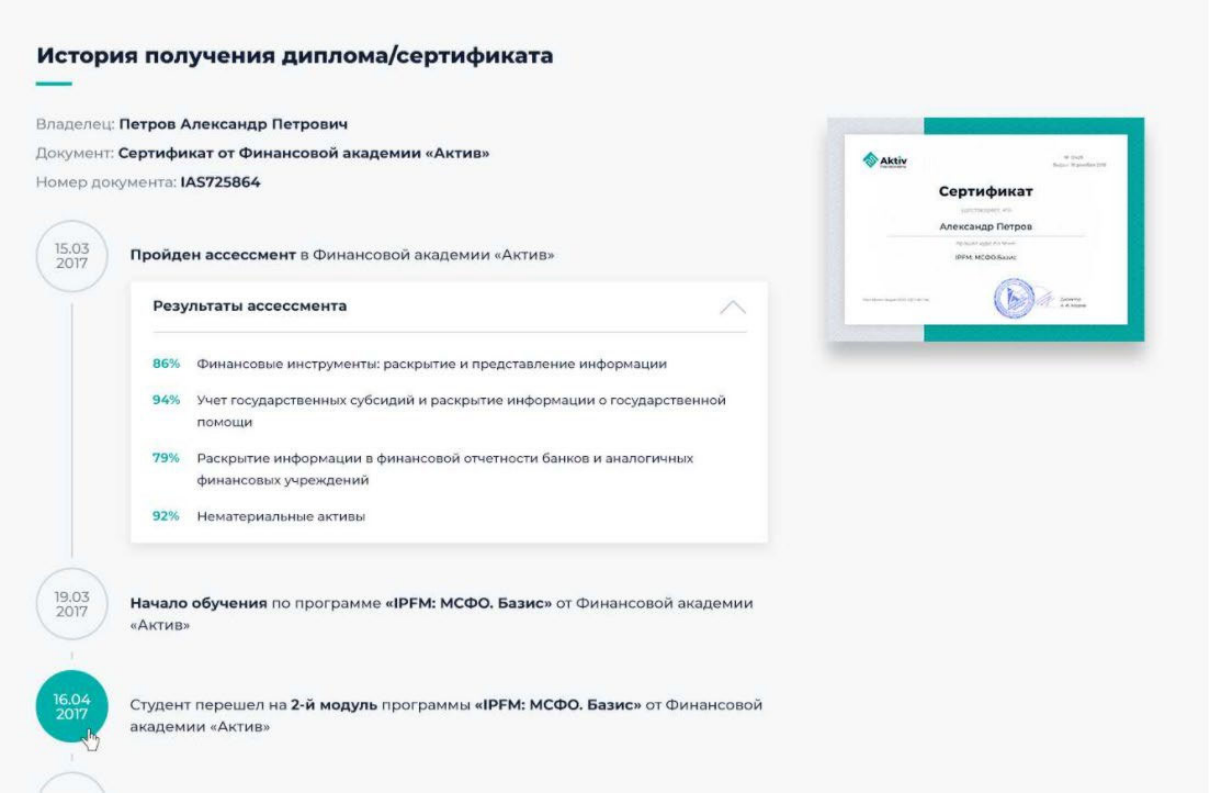

Рисунок 2.6 – Дешифрована інформація на сайті академії

2.2 Особливості реалізації технології блокчейн

Для розуміння можливості реалізації технології блокчейн необхідно розглянути основні визначення:

Транзакція: процес передачі даних в блокчейні. Для проведення транзакції в мережі необхідно мати вхід, або адреса, з якого надсилаються дані; вихід, або адреса, на який надсилаються дані; а також електронний цифровий підпис (ЕЦП), якій підписується транзакція.

Вузол або нода: будь-який комп'ютер, що використовує P2P-протокол для підтримки роботи блокчейна, вважається вузлом або нодою. У блокчейні працює кілька типів нод:

- ноди консенсусу, які підтверджують транзакції і додають нові блоки згідно з правилами, заданим консенсусом мережі;
- ноди-аудитори або повні ноди, які постійно підключені до мережіі відповідають за зберігання і синхронізацію всієї історії транзакцій блокчейна;
- SPV (Simplified Payment Verification) ноди, які зберігають неповні дані блокчейна, і використовуються для роботи додатків або програм, наприклад, гаманців.

Також в блокчейні, в залежності від їх алгоритму консенсусу, можуть працювати мастерноди і суперноди. Мастернода - це спеціально налаштована повна нода, яка використовується для виконання унікальних функцій, таких як приватні перекази або роздача винагороди. Суперноди – це високопродуктивний вузол, завдяки якому забезпечується безпека і функціональність мережі, підтримка легких і мобільних гаманців, а також додатків третіх сторін.

Алгоритм консенсусу: для ухвалення рішень, наприклад, про включення транзакцій в блок, і для подальшого включення блоку в ланцюжок, нодамі використовуються механізми консенсусу, оскільки публічні блокчейн- мережі є децентралізованими. Дані механізми дозволяють групі учасників прийти до єдиного рішення через процес голосування на користь більшості. Існують без-

ліч алгоритмів, використовуваних в блокчейні, серед яких найпопулярніші - це доказ роботи PoW (Proof of Work) і доказ володіння PoS (Proof of Stake) [29].

Хешування: це процес використання криптографічного алгоритму, який спрощує і прискорює перевірку цілісності даних, що записуються в блок. Хеш-функція приймає на вхід будь-які дані (файл, текст, картинку, двійковий код) і генерує з них послідовність літер і цифр фіксованої довжини - хеш. При цьому однакові дані завжди дають в результаті однаковий хеш, а різні - в ідеалі, різний (бувають дуже рідкісні випадки збіги, і це вважається вразливістю криптографічного функції). Таким чином, функція, яка втілює алгоритм і виконує перетворення, називається «хеш-функцією», вихідні дані називаються «вхідним масивом», «ключем» або «повідомленням», а результат перетворення називається «хешем», «хеш-кодом», або « хеш-сумою ».

Електронний цифровий підпис (ЕЦП): використовується для підписання транзакцій. Для роботи ЕЦП мережа повинна підтримувати асиметричне шифрування, яке використовує два ключа: один для шифрування (відкритий і публічний), інший для розшифрування (закритий і приватний). Обидва ключі математично пов'язані один з одним, і більш докладно про них ми розповімо далі. ЕЦП є доказом того, що всі транзакції були здійснені тільки справжніми власниками.

Приватний ключ – це унікальний пароль учасника мережі, яким підписується відправлене повідомлення, в зв'язку з чим даний ключ зберігається в секреті. Приватний ключ гарантує, що тільки власник певного адреси може відправити повідомлення або зберігаються на ньому кошти іншому користувачеві.

Публічний ключ – це адреса для прийому повідомлень від інших користувачів, він є відкритим для всіх користувачів мережі і являє собою рядок букв і цифр, що згенерувала на основі приватного ключа: вона ідентифікує відправника або отримувача коштів. Публічний і приватний ключі невіддільні одна від

одної, їх зв'язок заснована на математичних функціях. Вони з'єднані в комплексний незворотний алгоритм.

Таким чином, блокчейн працює як розподілений реєстр, де можна зберігати будь-яку інформацію, яка буде прихована від неавторизованих осіб завдяки криптографічного шифрування, а копії даного реєстру будуть зберігатися на комп'ютерах усіх користувачів. Зламати такий реєстр практично неможливо, а інформацію, яка міститься в ньому, не можна підробити, змінити або відредагувати [30].

Щоб створити блокчейн необхідно чи написати з нуля код блокчейн- ноди, чи створити блокчейн завдяки вже готовому різноплановому програмному забезпеченню.

Реалізація роботи технології залежить від обраного працюючого у створеному блокчейні алгоритму консенсусу. Якщо алгоритмом буде роботиProof of Work, для функціонування блокчейну необхідна буде обчислювальна машина щоб вирішувати задачі хешування, наприклад: процессор комп’ютера,відеокарта чи спеціалізовані інтегральні схеми, які створенні спеціально для цього алгоритму. Чим більше даних буде внесено до блокчейну, тим більше необхідно буде обчислювальної потужності для його функціонування.

Якщо алгоритмом консенсусу буде обраний доказ володіння Proof of Stake, то достатньо буде відкритого працюючого блокчейну на комп’ютері чи сервері.

2.3 Програмне забезпечення для створення блокчейну

Перед розробкою власного блокчейна необхідно чітко розуміти, для чого необхідний блокчейн і який бюджет можна виділити на його створення іутримання. Проектування і запуск блокчейна мають свої нюанси. Їх можна легко втратити при плануванні, якщо невірно оцінено обсяг і складність завдання.

Написання з нуля коду блокчейн-ноди майше неможливе без команди професіоналів-розробників, і фахівців, що мають досвід роботи з багатопотоко-

вим програмуванням, криптографією, мережевими протоколами,складними внутрішніми алгоритмами і розуміють роботу сучасних операційних систем. Особливе місце для блокчейнів займає тестування, так як алгоритми консенсусу можуть себе добре вести на декількох валідаторах і зовсім по-іншому при наявності десятків і сотень вузлів під навантаженням.

Тому доцільно використовувати готові програмні двигуни (двигуни – центральна частина комп'ютерної програми, що виконує основні функції цієї програми, вміщує у себе додаткові утиліти, опис алгоритмів і багато іншого). З огляду на існування декількох основних ядер блокчейнов, на базі яких побудовані вже існуючі мережі, буде зручно називати їх саме двигунами (наприклад, «побудований на двигунові Ethereum») [31].

Якщо блокчейн не володіє унікальною архітектурою і завдання роботи – знайти рішення за певний проміжок часу, найкращим варіантом буде робота з вже існуючими двигунами. Вони дозволяють реалізувати запланований вид консенсусу і транзакцій, по-своєму організувати управління валідаторами мережі. В такому випадку можна використовувати готовий відкритий код, перевірений в реальних мережах, недоведеться змінювати код блокчейн-ноди,а для реалізації своєї логіки потрібно буде міняти тільки частину, передбаченурозробниками движків [32].

Є декілька основних блокчейн-двигунів, використовуючи які можназапустити власний блокчейн, спроектувати і реалізувати його внутрішню економіку та організувати запуск для проведення складних операцій:

2.3.1 Створення блокчейну на базі Ethereum

Цей комплекс ПЗ побудований на базі ядра публічного блокчейна Ethereum. Публічний Ethereum використовує консенсус типу Proof-of-Work, а його численні тестові мережі – різні види Proof-of-Authority і Proof-of-Stake консенсусів. ПО відповідає найсуворішим критеріям безпеки, перевірено в десятках реально працюючих мереж і, на мій погляд, є найбільш розвиненим для

створення блокчейнов з будь-якими видами консенсусів та повноцінними, багатофункціональними смарт-контрактами. Потрібно відзначити роль проекту POA Network, чиї розробники виконали величезну роботу і запустили вже кілька швидких і надійних мереж. POA Network істотно швидше оригінального Ethereum, але при цьому має ту ж стійкістю і універсальністю для укладення будь-яких угод, а роль валідаторів виконують комп'ютери, чесна робота яких засвідчується юридично. Цю мережу можна вважати еталоном для запуску корпоративних блокчейнів на базі Ethereum [33].

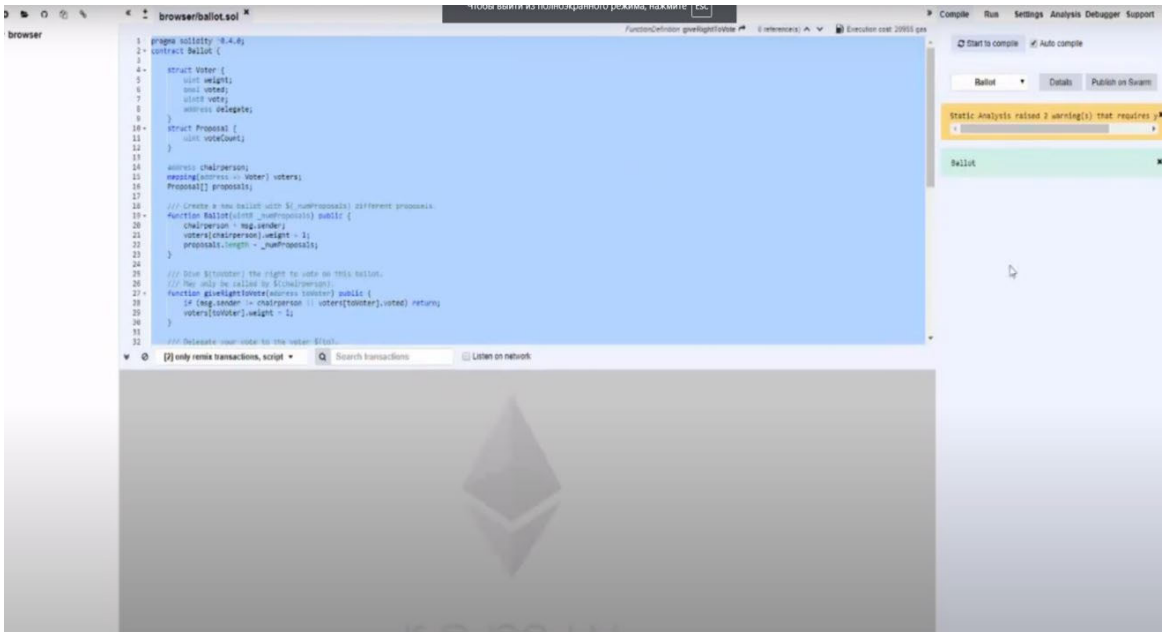

Рисунок 2.8 – Процес створення блокчейну на базі Ethereum

Існують дві основні імплементації коду Ноди Ethereum: на мові Rust (код, назви: poa-parity (старе) або openethereum (нове)) і на Go (код, назва: geth). На момент написання при побудові PoA-мережі на geth (Go) вам доступний тільки консенсус Clique - це найпростіший і небезпечний протоколбез фіналізації, який можна використовувати тільки в тестових цілях [34].

Консенсус, реалізований в poa-parity (Rust), складається з двох алгоритмів: schedule валідаторів Aura і finality gadget GRANDPA. Саме цей варіант, перевірений і безпечний, працює в POA-мережах на базі Ethereum. POA

Network працюють також над імплементацією перспективного BFT-консенсусу HoneyBadger. Окремої згадки заслуговує нова блокчейн-нода Nethermind, написана на C # для платформи .NET Core. Вона повністю підтримує Ethereum, велике число операційних систем і є відмінним вибором для компаній, які використовують .NET Core.

POA Ethereum використовує віртуальну машину EVM і смарт- контракти, які найкраще писати на мові Solidity. EVM давно стала стандартомдля віртуальних машин з великою кількістю готового коду і патернів розробки. Код контрактів під EVM відповідає за великі суми криптовалюта, і будь-яка знайдена уразливість викликає потужну реакцію спільноти та ЗМІ, тому безпека контрактів EVM на поточний момент украй висока.

Управління списком валідаторів здійснюється за допомогою смарт- контрактів – це приголомшливо зручно. Можна оперувати одним або декількома токенами або взагалі позбутися від них. Можна зробити процедуру додавання валідаторів гнучкою або максимально спростити, додавши «всемогутній» аккаунт. Міць цієї схеми в тому, що буквально один розробник контрактів може створити повну економіку мережі на одній платформі звисоким рівнем безпеки і переносимості, реалізувавши відразу і управління мережею, і логіку угод, і інші властивості [35].

З Ethereum можна використовувати JavaScript-бібліотеки web3.js, незалежно від консенсусу, валідаторів і її розташування.

Для POA Ethereum існує репозитарій для автоматизації операцій з розгортання готової мережі — deployment-playbooks.

2.3.2 Створення блокчейну на базі EOS

EOS є другим за гарантіями працездатності і безпеки двигуном. EOS можна запустити в якості окремої мережі, в PoS- або PoA-варіантах. Як і Ethereum, це ПО вже перевірено на практиці, володіє високою безпекою і

функціоналом, який дозволяє запустити власний блокчейн зі смарт- контрактами для автоматизації будь-яких угод.

Якщо Ethereum має просту систему адресу, то в EOS відразу ж використовується ієрархічна система акаунтів і права на різні дії. Все це робить EOS схожою по дизайну на операційну систему - «програму длязапуску інших програм». EOS дозволяє одразу отримати зручну систему управління акаунтами і швидкий консенсус, а також легко інтегрувати практично будь-який функціонал за допомогою плагінів на C ++ і смарт- контрактів на C ++ / WebAssembly (наприклад, можна додати іншу криптографію).

Дизайн консенсусу в EOS і швидкі блоки дозволяють досягти дуже швидкого часу відповіді користувачу, що вкрай важливо для побудови децентралізованих додатків зі складним функціоналом (наприклад, проекти Cyberway, Golos.io або соцмережа Commun). Cyberway недавно справив надзвичайно складну міграцію всієї бізнес-логіки з попереднього блокчейна прозоро для користувачів, що зайвий раз доводить гнучкість і універсальністьEOS [36].

2.3.3 Створення блокчейну на базі Parity Substrate

Substrate створюється командою компанії Parity. Розроблено величезна кількість ПО: гаманці, блокчейн-ноди, системи смарт-контрактів, компілятори, віртуальні машини. Parity Substrate дозволяє розробнику досить легко створити свій варіант блокчейна з готових модулів зі складним консенсусом і логікою обробки транзакцій. Substrate - це конструктор блокчейнов, на якому, наприклад, можна зробити блокчейн-ноду Ethereum абобіткоіни.

Substrate – це частина великого проекту Polkadot-системи, що складається з основної ланцюжка і безлічі ланцюжків-Шардена з індивідуальною логікою. Перевага «підключення» свого блокчейна до Polkadot полягає в можливості ончейн-обміну даними з іншими ланцюжками і можливістю використовувати їх контракти, акаунти, токени без додаткового ПЗ.

Код Substrate написаний на мові Rust. В структурі Substrate всі компоненти відмінно структуровані, розділені на окремі модулі, а в коді присутні докладні коментарі. Доказом гнучкості цього движка є існування клієнта для мережі біткоіни і ZCash на основі коду Substrate. Для консенсусу можна вибрати з декількох готових варіантів або написати свій власний. У більшості випадків це PoA або DPoS, що в разі Substrate означає використання алгоритму Aura і GRANDPA. Продуктивність блокчейнів на базі Substrate висока. Основний ланцюжок Polkadot була протестована нами в конфігурації з 99 валідаторами, розподіленими по трьох континентах і показала відмінні результати [38].

Перевагою Substrate є продуманість архітектури, стек розробки (Rust), і величезне поле для розвитку. Це вкрай гнучка мережа, на базі якої можна побудувати рішення будь-якого рівня складності. Substrate, на відміну від Ethereum і EOS, обробляє транзакції за допомогою коду, який розміщується валідаторами, а не користувачами. Це код називається "runtime" і виповнюється віртуальною машиною WebAssembly.

2.3.4 Створення блокчейну на базі Cosmos SDK

Cosmos – це проект на базі однієї основної ланцюжка і безлічі дочірніх блокчейнів, званих «zones». Дочірні ланцюжка будуються на основі Cosmos SDK-набору ПЗ для побудови блокчейнов. Cosmos – це продовження проекту Tendermint, з якого ключовими технологіями є надійний консенсус і концепція Application, подібна до runtime в Substrate. Як і в разі Polkadot + Substrate, блокчейн, створений за допомогою Cosmos SDK, може жити окремо або підключитися до екосистемі Cosmos як дочірня ланцюжок. Весь комплекс ПО Cosmos написаний на Go і відмінно структурований і активно використовується. На його основі вже працюють кілька проектів, серед яких Binance Chain.

Головна концепція Cosmos називається Application. Будь блокчейн є машиною станів, і в Cosmos вона винесена в окрему частину коду. Розробник просто задає правила, за якими одні дані перетворюються в інші при зовнішньому

впливі, програмуючи так звану функцію state transition. Це складно звучить, але по факту обробка транзакції - це state transition, яка змінює кілька балансів. Саме цим займається Application - приймає деяке вплив ззовні (транзакцію) і змінює свій стан (state). Утворені зміни фіксуються в блокчейні. При цьому розробник не повинен вирішувати проблеми консенсусу і мережі – мережа сама домовиться між собою і прийде до консенсусу щодо результатів.

Application в Cosmos можна розглядати як єдиний смарт-контракт, відповідальний за обробку всіх видів транзакцій. Одночасно зі створенням коду для блокчейн-нод, Cosmos SDK створює код клієнта, який вміє формувати транзакції потрібних типів. Для обмеження транзакцій в Cosmos, як в Ethereum, використовується газ. Виконуючи транзакцію, валідатори обчислюють її вартість в умовних одиницях «gas». Відправляючи транзакцію, користувач вказує ціну, яку він готовий платити за одиницю газу і ліміт, який він готовий витратити. Це є підставою для обчислення ціни за транзакцію [39]. Важливим для Application в Cosmos є вимоги до детермінізму коду, тобто розробляються операції не повинні породжувати різні результати в різні моменти часу або на різних архітектурах, інакше блокчейн не працюватиме. Паралельно зі створенням коду Application, Cosmos SDK дозволяє відразу ж отримати код, який викликає потрібні функції з клієнтських машин. Цей код можна використовувати на сайті, що працює з Cosmos, або в гаманці (клієнта) мережі. На JavaScript є кілька корисних бібліотек: js-cosmos, cosmosjs і універсальну js-abci, що реалізує інтерфейс ABCI. Їх зручно використовувати, якщо взаємодія з блокчейном планується з браузера. ABCI дозволяє створювати Application на різних мовах, серед яких Java, C ++, Python. Проект lotion, наприклад, дозволяє створити блокчейн повністю на Javascript. Cosmos бурхливо розвивається, на цьому движку запускається багато різних проектів.[39].

Рисунок 2.9 – Процес створення блокчейну на базі EOS

Код EOS написаний на C ++ і розвивався на основі досвіду, отриманого розробниками при роботі над двигунами Graphene, Bitshares, Steemit. Використовується власний варіант DPoS-консенсусу. Майже всі проекти, що використовують DPoS, будують свої алгоритми дуже схожим на EOS чином: це акаунти, «голосують» балансом токена за топ валідаторів. Валідатори підписують блоки поодинці, але кожен в призначений квант часу, згідно з розкладом. Потім вони колективно фіксують так званий Last Irreversible Block(LIB), на якому збирається 2/3 + 1 підписів від валідаторів. Перехід до корпоративного POA-консенсусу не викликає ускладнень, так як список валідаторів управляється системними смарт-контрактами.

Смарт-контракти в EOS використовують модифіковану віртуальну машину WebAssembly, зазвичай пишуться на мові C ++ і можуть створюватися і використовуватися будь-яким профілем. Писати смарт-контракти не складно, багато в чому вони перегукуються з Solidity.

В EOS, як і в POA Ethereum, управління мережею, основний токен (або токени) і типи транзакцій можна реалізувати в системних смарт-контрактах (ось, наприклад, системний токен). Цікавою особливістю контрактів EOS є використання абстракції table для зберігання даних контракту. У Ethereum в основному використовується mapping (асоціативний масив). Одна із особливостей смарт-контрактів в EOS – upgradeability. Власник контракту може замінити його, оновивши логіку або виправивши помилку. Це сильно відрізняється від Ethereum, де незмінність контрактів - важлива умова, яке гарантуватиме, що логіка контракту ніколи вже не буде змінена, якщо не відбудеться хардфорк. В EOS можливо організувати «спонсорські» транзакції, оплачувані власниками контракту, а не самими користувачами. Це найпотужніша можливість для залучення нових користувачів [37].

BOSCore, Telos, Haya і ще десяток проектів EOS доводять, що це ПО цікаво великій кількості проектів. Для EOS існує досить інструментів, і користувачеві не доведеться з нуля реалізовувати супутнє ПО. Eosjs - аналог web3.js, дозволяє працювати з контрактами будь-якої мережі на базі EOS з браузера і будь-яких додатків. У EOS немає одного великого і потужного інтегратора, як POA Network для Ethereum, тому кожен проект будує власне рішення. Проте, основний код Ноди стабільний і працює під серйозними навантаженнями без збоїв.

Висновки до розділу:

У даному розділі визначено та досліджено технічні аспекти створення та реалізації технологій блокчейн, середу для розробки та основні складові для забезпечення функціонування технології. Розглянуто існуючі приклади застосування технології блокчейн для створення навчального середовища.

Виходячи з проведеного аналізу визначені існуючі підходи застосування технології блокчейн у сфері навчання:

- Ідентифікація та облік успішності студента

- Оплата навчання, стипендії та заохочення
- Автоматична видача дипломів, атестатів і сертифікатів при досягненні певного результату
- Підтвердження дійсності дипломів, атестатів і сертифікатів, безпечне зберігання і передача інформації.
- Проведеннятестувань, опитувань і голосувань, залучення інвестицій.
- Акредитація та контроль за освітньою установо, система репутаціїі портфоліо.

3 ОСОБЛИВОСТІ ЗАСТОСУВАННЯ РІЗНИХ МЕТОДІВ РЕАЛІЗАЦІЇ ТЕХНОЛОГІЇ БЛОКЧЕЙН У СФЕРУ НАВЧАННЯ

3.1 Метод смарт-контрактів для навчання

Вперше технологію смарт-контрактів в 1990-х роках описав Нік Сабо [41]. Він визначив смарт-контракти як інструмент, який формалізує і захищає комп'ютерні мережі шляхом об'єднання протоколів з призначеним для користувача інтерфейсом. Сабо також обговорював потенційне застосування смарт-контрактів в різних областях, які включають в себе суспільні відносини договірного характеру, такі як кредитні угоди, обробка платежів і управління авторськими правами.

У світі блокчейну смарт-контракт – це додаток (або програма). Як правило, він виступає в якості цифрової угоди, яке підкріплюється певним набором правил. Ці правила визначені комп'ютерним кодом, який реплікується і виконується всіма вузлами мережі. Смарт-контракти дозволяють створювати довірчі протоколи. Це означає, що обидві сторони можуть взяти на себе зобов'язання через блокчейн, без знання або довіри один до одного. Учасники даного процесу можуть не турбується про правильність виконання зобов'язань, оскільки якщо умови не будуть задоволені то контракт анулюється. Крім цього, використання смарт-контрактів може усунути необхідність в посередниках, значно знижуючи операційні витрати. Хоча протокол блокчейну Bitcoin вже багато років підтримує смарт-контракти, вони були популяризовані творцем і співзасновником Ethereum Віталіком Бутеріним. При цьому кожен блокчейн може уявити інший метод реалізації смарт-контрактів. У центрі уваги статті Ніка Сабо [41] смарт-контракти, які працюють на віртуальній машині Ethereum, яка є найважливішою частиною блокчейна Ethereum.

3.1.1 Робота смарт-контрактів у мережі Ethereum

Смарт-контракт працює як детермінована програма. Вона виконує певні дії, коли дотримані задані умови. Виходячи з цього, система смарт-контрактів часто використовує "if ... then ..." вираження. Незважаючи на загальноприйняту термінологію, смарт-контракти не є ні контрактами в юридичному сенсі, ні "розумними". Це всього лише фрагменти коду, запущеного в розподіленої системі блокчейну [42].

У мережі Ethereum смарт-контракти відповідають за виконання операцій між користувачами (адресами). Будь-яку адресу, який не є смарт-контрактом,називається особистим обліковим записом. Таким чином, смарт-контракти управляються програмним кодом, а особисті акаунти - користувачами.

Смарт-контракти Ethereum складаються з коду контракту (що містить умови виконання) і двох публічних ключів. Перший публічний ключ надано творцем контракту. Інший ключ являє собою сам контракт, будучи цифровимкодом, унікальним для кожного смарт-контракту.

Виконання будь-якого смарт-контракту відбувається при блокчейн- транзакції, і вони можуть бути активовані під час ініціації особистим обліковим записом (або іншим смарт-контрактом). Однак запускається послідовність смарт-контрактів завжди з особистого облікового запису, тобтокористувачем).

3.1.2 Основні характеристики смарт-контрактів Ethereum

Смарт-контракт Ethereum мають такі характеристики:

Розподіленість. Смарт-контракти реплікуються і розподілені по всіхвузлах мережі Ethereum. Це одне з головних відмінностей від інших рішень, що використовують централізовані сервера.

Детермінованість. Смарт-контракти виконують дії, для яких вони призначені, після досягнення задоволених вимог. Крім того, результат завждибуде однаковим незалежно від того, хто виконує вимоги.

Автономність. Смарт-контракти можуть автоматизувати всі види завдань, працюючи як програма, котра самостійно виконується. У більшості випадків, якщо смарт-договір не ініційований, він знаходиться "в бездіяльності" і не виконує будь-яких дій.

Незмінність. Не можна змінити процес роботи смарт-контракту після його розробки і активації. Зміни можуть бути внесені тільки в тому випадку, якщо розробники до цього реалізували певну функцію. Таким чином, смарт- контракти можуть забезпечити захист від зломів для коду за допомогою докази справжності.

Налаштованість. Перед реалізацією, смарт-контракти можуть розроблятися різними способами. У зв'язку з цим, дана технологія підходить для створення багатьох типів децентралізованих додатків. Це також пов'язано з тим, що Ethereum є завершеною блокчейн-мережею.

Конфіденційність. Дві або більше сторони можуть взаємодіяти за допомогою смарт-контрактів, без знання і довіри один до одного. На додаток до цього, технологія блокчейн забезпечує точність і облік всіх даних.

Прозорість. Оскільки смарт-контракти засновані на публічному блокчейне, їх вихідний код доступний для кожного.

В смарт-контракт Ethereum не можна додавати нові функції після активації. Однак, якщо розробник включає в код контракту функцію під назвою SELFDESTRUCT, в подальшому він зможе видалити його і замінити на новий. У свою чергу, якщо ця функція не була написана в коді, контракт не можна буде видалити.

Так звані оновлювані смарт-контракти забезпечують розробникам доступ до змін коду, тим самим надаючи велику гнучкість в порівнянні з незмінними контрактами. Існує безліч способів створення подібного виду смарт-контрактів різного ступеня складності.

Смарт-контракт ділиться на кілька невеликих контрактів. Деякі з них не можна змінити, в той час як інші можна видалити. Це означає, що частина коду

(кількість смарт-контрактів) можна видалити і замінити на інший, в той час як інші функціональні можливості залишаються незмінними. Оскільки це програмований код, смарт-контракти легко налаштовуються і можуть розроблятися різними способами, пропонуючи різні види послуг і рішень.

Смарт-контракти можуть забезпечити підвищену прозорість і знизити експлуатаційні витрати, оскільки являються децентралізованими та програми, що самостійно реалізуються. Залежно від напрямку діяльності, вони також можуть підвищити ефективність і знизити бюрократичні витрати. Переваги смарт-контрактів особливо проявляються, коли мова йде про грошові перекази або обміні коштів між двома або більше сторонами.

Смарт-контракти можуть бути розроблені для широкого спектра варіантів використання. Деякі з прикладів включають в себе створення токенізованих активів або акцій, систем голосування, криптовалютних гаманців, децентралізованих бірж, ігр та мобільних додатків. Вони також можуть бути реалізовані спільно, поряд з іншими рішеннями на блокчейні, які зачіпають такі області як: охорона здоров'я, благодійність, ланцюжки поставок, державне управління та децентралізоване фінансування, навчання.

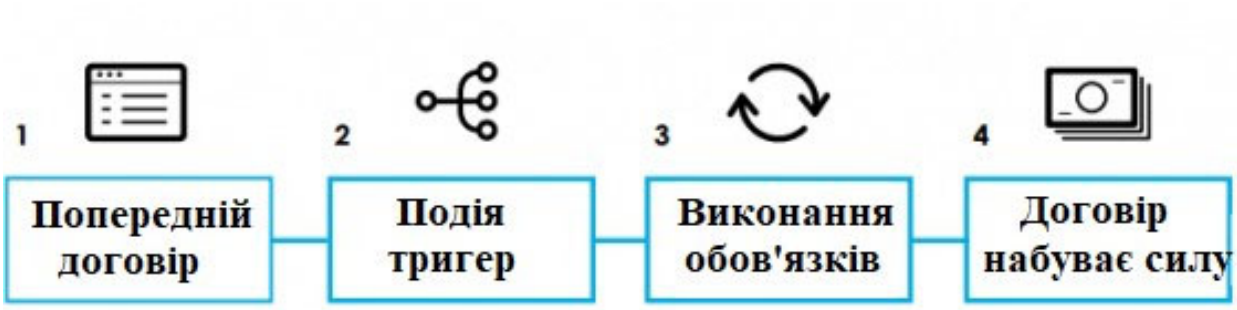

Рисунок 3.1 – Реалізація смарт-контракту

3.1.3 Недоліки смарт-контрактів Ethereum

Смарт-контракти складаються з комп'ютерного коду, написаного людьми. Це є причиною численних ризиків, оскільки код схильний вразливостей і помилок. В ідеалі, розробка повинна здійснюватися досвідченими програмістами, особливо коли мова йде про конфіденційну інформацію або великі суми грошей.

Централізовані системи можуть забезпечити більшість рішень і функцій, пропонованих даною технологією. Основна відмінність полягає в тому, що смарт-контракти виконуються в розподіленої тимчасової мережі, а не на централізованому сервері. І оскільки смарт-контракти засновані на блокчейні, вони як правило незмінні, або процес внесення змін дуже складний.

Незмінність, це добре в одних ситуаціях, але дуже погано в інших. Наприклад, коли децентралізована автономна організація під назвою «DAO» була зламана в 2016 році, хакери вкрали ефіру на мільйони доларів через недоліки в коді смарт-контракту. Оскільки їх смарт-контракт був незмінним, розробники не змогли виправити код. Слід зауважити, що проблема виникла не через роботу блокчейна Ethereum. Замість цього, помилка була викликана неправильною реалізацією смарт-контракту.

Ще один недолік смарт-контрактів пов'язаний з їх невизначеним юридичним статусом. І це пов'язано не тільки з тим, що в більшості країн дана технологія знаходиться в «сірій зоні», а й через те, що смарт-контракти не відповідають їх поточної нормативно-правовій базі.

Основною вимогою безлічі договорів і контрактів є ідентифікація учасників вік яких становить 18 або більше років. Псевдонімного, що забезпечується технологією блокчейн, в поєднанні з відсутністю посередників, може виступити перешкодою для відповідності таким вимогам. Незважаючи на те, що існують потенційні вирішення даного питання, юридична складова смарт-контрактів є однією з головних проблем, особливо коли мова йде про всесвітньому масштабі і розподілених мережах.

Смарт-контракти розвинена технологія. Але в зв'язку з розподіленим і детермінованим характером, а також прозорістю і часткової незмінністю, робить її менш привабливою для використання в деяких ситуаціях.

Смарт-контракти не є рішенням для безлічі реальних проблем. І зафактом, деяким організаціям простіше і краще використовувати звичайні альтернативні сервера. У порівнянні зі смарт-контрактами, централізовані сервера простіше і

дешевше в обслуговуванні, крім цього, вони також можуть забезпечити більш високу ефективність з точки зору швидкості роботи і взаємодії з іншими мережами (функціональної сумісності).

3.1.4 Реалізація смарт-контрактів у сфері навчання

В системі смарт-контрактів існує можливість технічно отримати доступдо таких компонентів, як:

- учасники договору – це студент, викладач, освітній заклад;
- предмет договору – між студентом і освітнім установою це сертифікатабо диплом про закінчення навчання, між викладачем і освітньою установою – це виплата заробітної плати.

А також аналізувати, вимірювати і взаємодіяти з таким компонентом, як умова договору. Між студентом і освітнім установою – це показники успішності, між викладачем і освітньою установою – це ефективність викладацької діяльності. Децентралізований характер блокчейна дозволяє обходитися без третьої сторони і виконувати угоду, що стосується предмета договору, відразу ж як виконані всі необхідні умови [43].

Завдяки електронно-цифровим підписам, що використовуються в блокчейні, кожна дія, виконана учасниками договору, буде підтверджена і зможе потім перевіритися. Таким чином, для роботи здійснення смарт- контрактів можуть виконуватися різні умови.

Наприклад, реєстрація безпосередньо постачальника освітніх послуг і учасника договору – освітнього закладу, до якого можна прив'язати всі реквізити установи (індекс, індивідуальний номер платника податків (ІНП), код причини постановки на облік і т.д.), контактну інформацію, адресу та реалізовані в ньому освітні програми.

Смарт-контракт буде виконуватися для студентів за успішне проходження контрольних точок, закладених в освітніх програмах і описанихрозробниками в коді, в результаті яких буде видаватися диплом або сертифікат з електронно-

цифровим підписом про успішне завершення навчання за певною освітньою програмою. А для викладача смарт-контракт буде працювати при виконанні навантаження, за виконання якої він буде отримувати заробітну плату. Завдяки тому, що система буде відкритою і в той же час виступати гарантом виконання умов договору, сторонні особи зможуть дізнатися, які освітні програми реалізуються в освітньому установі, і наскільки вони ефективно реалізуються. роботодавці можуть через форму для зв'язку зв'язатися з тими випускниками, успішність яких буде задовольняти їх запитам. Освітні установи можуть ділитися освітніми програмами між собою і своїми філіями. У загальному вигляді схема зв'язків в системі представлена на рисунку 3.3.

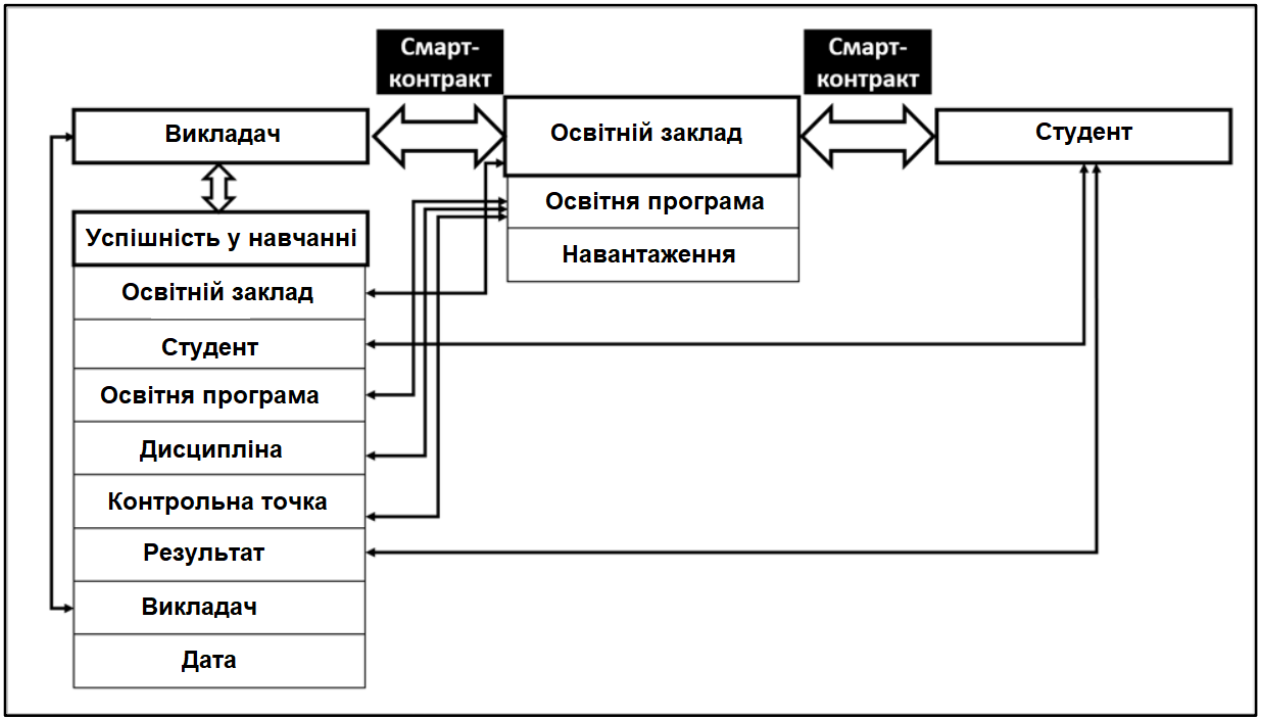

Рисунок 3.2 – Схема зв'язків моделі для смарт-контрактів

3.2 Можливості використання ICO для фінансування освітньоїсистеми

ICO (Initial Coin Offering) - первинне розміщення токенів (монет).

Це продаж інвесторам цифрових токенів за криптовалюту або фіатні кошти (гривні, долари, євро). Куплені токени згодом можна використовувати на оплату послуг. Абревіатура ICO утворена за аналогією з IPO (первинне розміщення акцій компанії на біржі). Але при цьому у понять ICO і IPO є ряд істотних відмінностей:

- У ICO відсутнє на сьогоднішній день державне регулювання, характерне для IPO і будь-яких інших публічних фінансових і інвестиційних видів діяльності;
- Власники токенів не мають корпоративних прав, аналогічних тим, що отримують власники акцій;
- ICO проводиться для збору і фінансування, необхідного для запуску і розвитку проекту. Тому багато фахівців відносять ICO дооднієї з форм краудфандінга (колективного фінансування проектудля отримання будь-яких бонусів в майбутньому).
- Купуючи токени, інвестори можуть розраховувати:
- На отримання вигоди від перепродажу токенов за вищою ціною в майбутньому;
- На нижчу ціну при покупці послуг компанії в майбутньому;
- На розвиток цікавого для себе проекту.

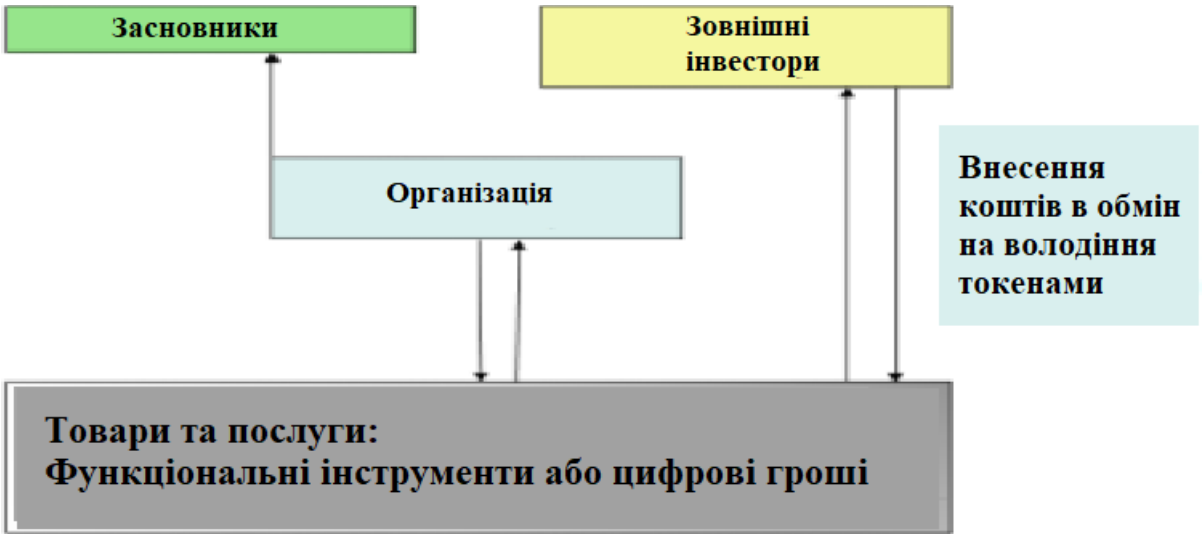

Рисунок 3.3 – Схема інвестицій у токени

Так як на ICO зазвичай виходять маловідомі проекти, потрібно, перш за все, привернути увагу інвесторів. Для цього в криптовалютних спільнотах, наприклад, Reddit або Bitcoin Talk, розміщується презентація компанії з описом її бізнес-моделі. В ході обговорень в співтоваристві модель може кілька разів змінюватися, щоб стати цікавою для фінансування. Як тільки угода між проектом і інвесторами досягнута, проект готує оферту [44].

В оферті вже докладно описуються всі подробиці проекту, вказується бажана сума інвестицій. Також вказується фінансовий еквівалент продаваних токенів і права, якими вони володіють. Після підготовки оферти, компанія готує документи і оголошує день початку продажу токенів. Для проведення ICO компанія може створити власний блокчейн або використовувати вже готову ICO-платформу. Плюси і мінуси готової ICO-платформи:

- Більш високий рівень довіри до проекту з боку інвесторів;
- Просте управління;
- Потрібно менше інвестицій на початковому етапі;
- Захист коштів від зловмисників;
- Платформа бере комісію.

Найвідоміша платформа для проведення ICO - це Ethereum.

Платформа не тільки лідирує по числу користувачів, але і за сумою грошей в обігу. Створена на основі цього блокчейна криптовалюта ефір є в обігу практично на всіх біржах, Ethereum-токени легко додати на торговельні майданчики, існує більше пов'язаних з системою гаманців.

При наявності гаманця з криптовалютою і вмінням проводити транзакції можна взяти участь в краудсейлі на сайті проекту. Також є спеціальні інформаційні ресурси, де можна знайти проекти, які проводять ICO, наприклад, ICO Alert.

Так як ICO не регулюється законами, і проведення операції засновано лише на довірі до засновників проекту, перед тим як інвестувати гроші, слід звернути увагу на наявність:

- Всіх необхідних угод і правил, опублікованих на веб-сайті в якості публічної оферти;
- Робочого прототипу проекту;
- Необхідної документації;
- Escrow (спеціальний умовний рахунок, на якому враховуються майно, документи або грошові кошти до настання певнихобставин чи виконання певних зобов'язань) ;
- Реєстрації самої компанії;
- Інформації про репутацію людей, які започаткували проект.

Для того, щоб система працювала стабільно, важливо, щоб вона була фінансово стійкою. Новий спосіб залучення інвестицій дозволяє залучити не тільки кошти, а й більшу кількість зацікавлених осіб, які можуть сприяти розвитку організації. В системі може бути створена власна криптовалюта організації – токени.

За допомогою них, завдяки наявності зв'язків у системі (рисунок 3.5), можливо проводити наступні операції:

- оплата навчання з боку учнів;
- виплата заробітної плати викладачам з боку освітньої установи;
- виплата стипендій учням з боку освітнього установи;
- інші види виплат всередині організації;
- придбання токенів освітнього закладу з метою його інвестування

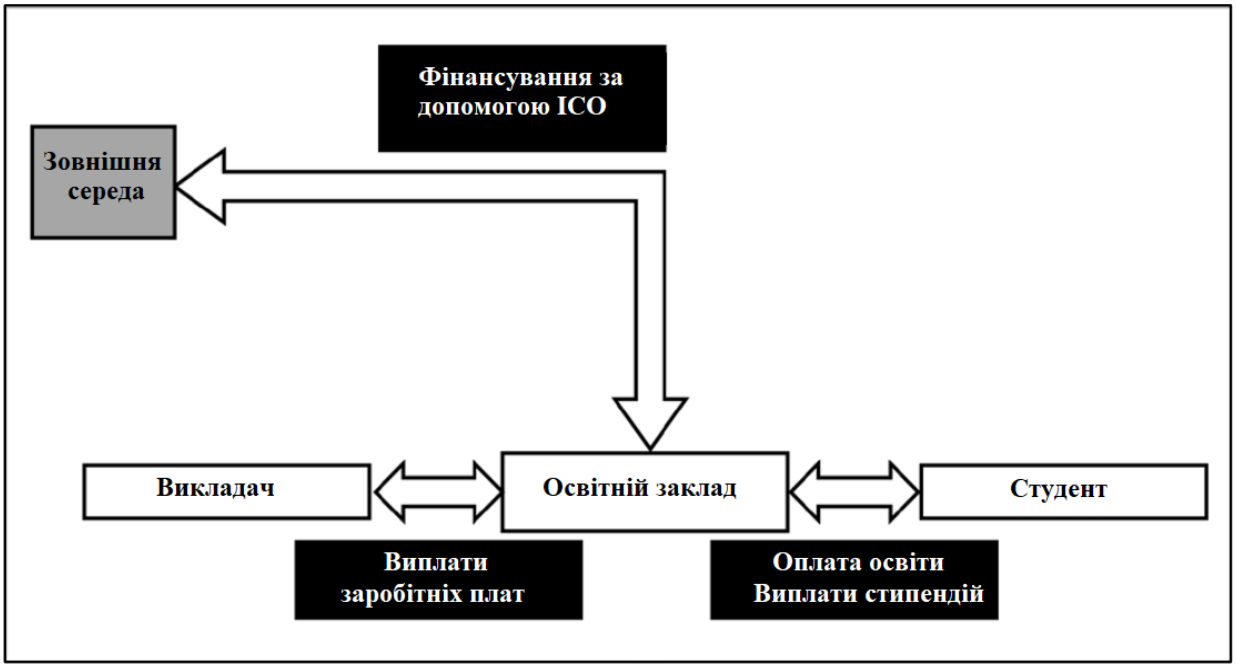

Рисунок 3.5 – Схема шляхів залучення фінансів до освітньоїсистеми

Таким чином, в освітній системі будуть власні активи, що залежать від показників їх власної діяльності, роблячи систему самодостатньою. Освітні установи зацікавлені в тому, щоб вести освітню діяльність ефективно, оскільки від цього буде залежати попит, безпосередньо виражений в ціні на їхтокени.

3.3 Метод видачі цифрових сертифікатів та дипломів

Більшість навчальних закладів ведуть записи у паперовій формі або зберігають їх у ексклюзивних базах даних, структурованих для доступу лише працівникам навчальних закладів. В основному ці установи мають свої спеціалізовані системи для зберігання повних даних студентів. Щоб забезпечити безпроблемну інформацію про записи студентів на всіх рівнях, тобто студент, заклад та роботодавці, організації працюють над розробкою системи управління сертифікатами на основі блокчейну. Це призводить до автоматизації процесів видачі паперового сертифікату та надсилання запиту на перевірку сертифіката через різні вузли блокчейну [47].

Облікові дані на паперовій основі видача передбачає час і схильність до помилок та шахрайства. Ця автоматизація може призвести до завершення робо-

ти в режимі реального часу, а дані зберігаються в незмінній інфраструктурі. Для студентів це просто зберігання облікових даних протягом усього життя з можливістю контролювати право власності. З іншого боку, роботодавці можуть зменшити вимогу верифікації третьою стороною та мінімальний ризик отримання фальшивих заявок на сертифікацію.

У дослідженні «Блокчейн в освіті» [48] Об'єднаного дослідницького центру Європейської комісії є попередній огляд технології і її потенційних застосувань в Європі. Це демонструє, наскільки серйозно технологія сприймається в освітньому просторі. Одним із застосувань технології блокчейн описаних у статті є видача цифрових сертифікатів та дипломів.

Наприкінці захисту, оголошується оцінка всіх робіт. Диплом підписується ректором навчального закладу, головою комісії, деканом і секретарем. Всі документи повинні бути завірені печаткою навчального закладу. Диплом видається студенту особисто або за заявою висилаєтьсяпоштою, рекомендованим відправленням. Ця заява зберігається в особовій справі випускника, а також там зберігається і копія виданого диплома. Всі документи, є бланками суворої звітності і враховуються за спеціальним реєстром. Для обліку всіх виданих дипломів, в освітньому закладі ведеться книга реєстрації, листи якої нумеруються, а сама книга прошнуровується і на ній ставиться печатка навчального закладу та зазначається кількість аркушів. Книга так само зберігається як документ суворої звітності.

Для вирішення проблем з шахрайством у сфері підробки документів, і проблемою зберігання документів, було запропоновало впровадити технологію блокчейн. Модель роботи блокчейн представлена на рисунку 3.6

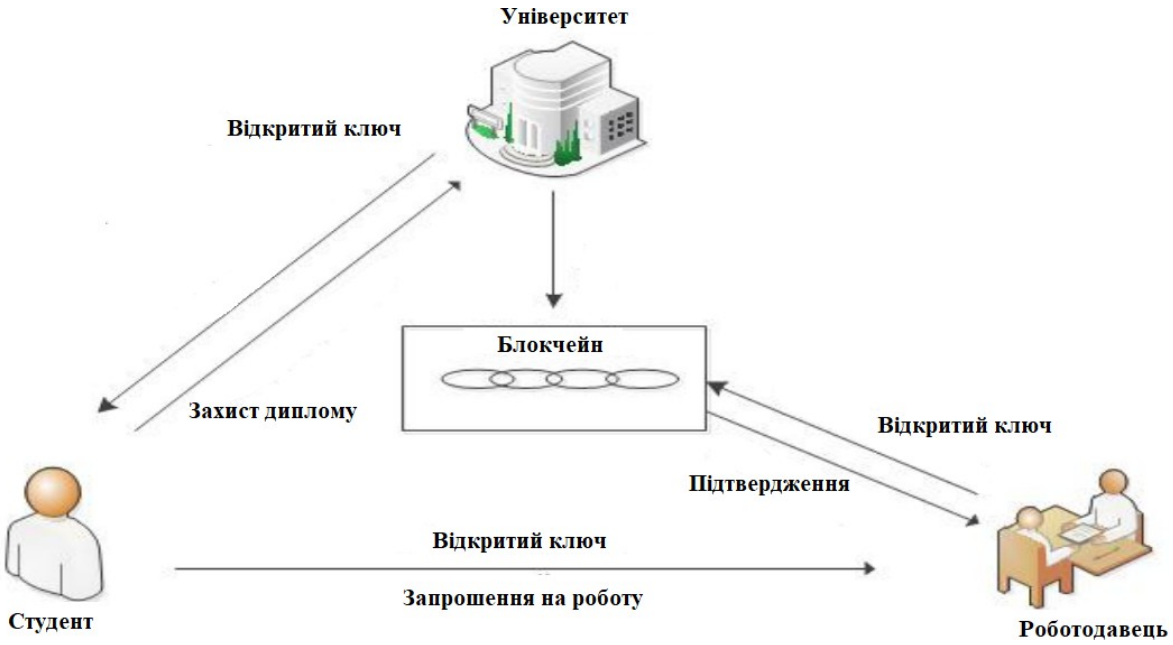

Рисунок 3.6 – Модель видачі диплому
з використаннямблокчейну

В даній моделі, вищі навчальні заклади, що випускають цифрові дипломи, будуть використовувати єдиний блокчейн для їх зберігання. Унікальні дипломи, підписані приватним ключем, будуть надаватися безпосередньо роботодавцям. Таким чином, перевірка справжності диплома вимагає тільки порівняння з хешем, що зберігаються в ланцюжку блоків. Це вирішить проблему з шахрайством у сфері підробки документів і проблему збереження документів.

В першу чергу, створюється цифровий файл, який містить основнуінформацію, такі як назва університету і одержувача диплома, дату видачі, посвідчення. Потім, університет підписує вміст диплома з використанням закритого ключа, до якого має доступ тільки освітня організація. Дані підтверджуються мережевим вузлом і передаються в мережу. Запис
приєднується до блоку. Університет створює хеш файл облікових даних - коротку рядок букв і цифр, які можуть використовуватися для перевірки того, щоб ніхто не порушив зміст диплома. Існує тільки одна можлива комбінація букв і цифр, яка відповідає цифровому файлу, і будь-яка зміна файлу призведедо іншого хешу. Потім, університет знову використовує свій приватний ключдля створення запису в блокчейне, в якій говориться, що освітня організація видала

певний сертифікат певній особі на певну дату. Після чого, випускнику передається відкритий ключ. Таким чином, користувач може перевірити, комубув виданий диплом, ким і для перевірки вмісту самого диплома [49].

Переваги перед поточним станом – докази сертифікатів будуть зберігатися повністю, надійно і в постійному блокчейні. Таким чином, навіть якщо установи, що видали сертифікати, повинні були закрити або якщо вся система освіти звалилася, ці сертифікати все ще перевіряються щодо записів, що зберігаються в блокчейні.

Крім того, як тільки установи видають диплом, їм не потрібно витрачати додаткові ресурси, щоб підтвердити дійсність цього документа третім особам, так як вони зможуть безпосередньо перевіряти дипломи у вигляді ідентифікації ланцюжка блокчейн.

Рисунок 3.7 – Механізм роботи технології блокчейн для видачідипломів

4 ДОСЛІДЖЕННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН З ВИКОРИСТАННЯМ МАСШТАБОВАНОГО ПРОТОКОЛУ КОНСЕНСУСУ І УДОСКОНАЛЕНОГО МЕТОДУ ШАРДІНГУ

4.1 Недоліки існуючої системи

Розглянуті у попередньому різділі методи реалізації технології блокчейнзасновані на можливостях вже створених блокчейнах Ethereum та Bitcoin, які мають низку недоліків для їх використання у будь-яких сферах, у тому числі всфері навчання. Деякі методи функціонування блокчейну потребують удосконалення.

Оригінальний блокчейн Bitcoin був розроблений як однорангова платіжна система, яка дозволяє людям переказувати кошти без посередників, таких як банки або платіжні системи. Однак, коли Bitcoin набув популярності, його недоліки в роботі стали очевидними через обмежену пропускну здатність близько 7 транзакцій в секунду, а вартість його як платіжної системи стала надмірно дорогою. Невдовзі Віталій Бутерін запропонував нову інфраструктуру блокчейну під назвою Ethereum, яка дозволила розробникам створювати різні типи блокчейн-додатків за допомогою «розумних контрактів». Однак Ethereum не вирішив проблему масштабованості і, маючи близько 15 транзакцій в секунду, не зміг підтримати високопродуктивні додатки, такі як ігри або децентралізовані біржі [50].

Враховуючи обмеження продуктивності Ethereum та Bitcoin, багато проектів блокчейну пропонували різні рішення, які намагалися збільшити пропускну спроможність транзакцій. Різні блокчейни пропонували замінити консенсус Proof-of-Work на консенсус Proof-of-Stake . Інші блокчейни, такі як EOS, використовують делегований доказ ставки (DPoS), де пропозиція блоків обирається голосуванням, а не за допомогою ланцюгового алгоритмічного процесу. Такі проекти, як IOTA, замінили структуру даних ланцюжків блоків структурою даних DAG (Directed Acyclic Graph), що порушує обмеження послідовної обробки транзакцій. Однак ці запропоновані рішення не можуть суттєво збіль-

шити продуктивність, не жертвуючи іншими важливими аспектами, такими як безпека та децентралізація [60].

4.1.1Механізм консенсусу

Протокол консенсусу є ключовим компонентом будь-якого блокчейну. Він визначає, наскільки надійно та швидко перевіряється блокчейн, щоб досягти консенсусу щодо наступного блоку.

Першим протоколом консенсусу блокчейнів, який забезпечує Bitcoin, є консенсус Proof-of-Work. PoW – це процес, за допомогою якого майнери знаходять рішення криптографічної головоломки – переможець отримує право запропонувати наступний блок і отримує деякі символічні винагороди. Понад 50% потужності хешування контролюється чесними вузлами. Правило консенсусу полягає в тому, що найдовшим ланцюгом буде єдиний правильний і, таким чином, консенсус PoW також називається консенсус на основі ланцюга. Головний недолік такого консенсусу: Якщо у когось буде знаходитися потужності більше, ніж у решти мережі мінімум на 1 %, тобто 51% і більше, свого роду «контрольний пакет» генеруючих потужностей – в такому разі він може одноосібно контролювати всі операції по системі, генерувати блоки, підтверджувати або блокувати транзакції.

Хеш в такому протоколі представляє собою набір з 64-рьох буквених і числових символів, а складність регулює кількість нулів на його початку.. Основний процес доказу роботу – майнинг. Він полягає в переборі числовогозначення до тих пір, поки заголовок блоку не буде виглядати належним чином.Після виконання всіх необхідних умов, майнер публікує блок із зазначенням всіх необхідних атрибутів, включаючи знайдене значення. Знаючи всі атрибути, повні в автоматичному режимі перевіряють, чи дійсно при таких вхідних даних і такому знайденому значенні, хеш заголовка буде виглядати саме так, а не інакше. Після підтвердження майнер переключаються на генерацію нового блоку, а автор щойно створеного блоку отримує на свою Bitcoin гаманець нагороду [51].

У підході Proof-of-Stake ноди також намагаються хешувати дані в пошуках результату менше певного значення, але складність в даному випадку розподіляється пропорційно і відповідно до балансу даного вузла відповідно до кількості монет (токенів) на рахунку користувача.

Таким чином, більше шансів згенерувати наступний блок має вузол з великим балансом. Навідміну віж Proof-of-Stake цей алгорит витрачає набагато менше потужності.

Інший тип консенсусного протоколу PBFT (Practical Byzantine Fault Tolerance). Названий на честь математичної загадки «Завдання візантійських генералів». Кілька візантійських генералів оточили місто своїми арміями – вони повинні домовитися про дії при атаці або відступі. Якщо рішення не будепогоджено генералами, то операція призведе до катастрофи. У PBFT один вузол обирається "лідером", тоді як решта вузлів є "валідаторами". Кожен раунд консенсусу щодо PBFT включає дві основні фази: фазу підготовки та фазу фіксації. На етапі підготовки лідер передає свою пропозицію всім валідаторам, які, в свою чергу, передають свої голоси за пропозицію всім іншим. Причиною ретрансляції для всіх валідаторів є те, що голоси кожного валідатора повинні підраховуватися всіма іншими валідаторами. Підготовча фаза закінчується, коли більше ніж $2f + 1$спостерігають послідовні голоси, де f- кількість зловмисних валідаторів та загальна кількість валідаторів плюслідер$3f + 1$. Етап комітування передбачає подібний процес підрахунку голосів, і консенсус досягається, коли $2f + 1$ спостерігаються послідовні голоси. Через ретрансляцію голосів серед валідаторів PBFT $O(N)^2$складність зв'язку, яка не є масштабованою для системи блокчейнів із сотнями або тисячами вузлів.

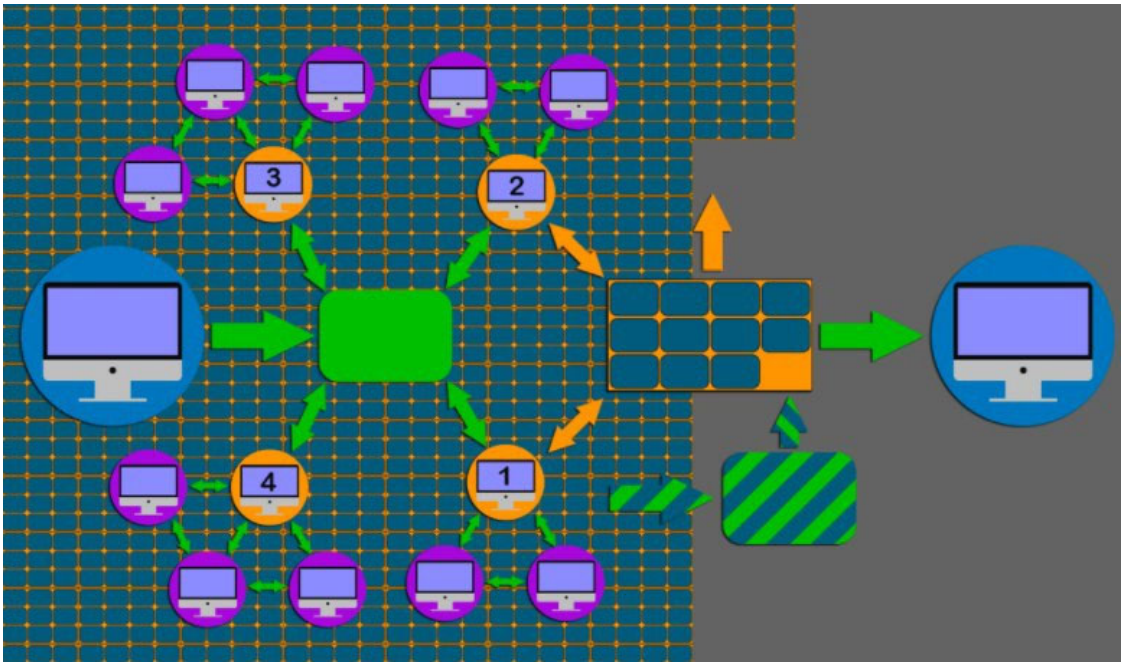

Рисунок 4.1 – Механізм Practical Byzantine Fault Tolerance

4.1.2 Метод шардінгу

Рішення для масштабованості, яке одночасно зберігає безпеку та децентралізацію – це шардінг, який створює кілька груп валідаторів і дозволяєїм одночасно обробляти транзакції. В результаті загальна пропускна здатність транзакцій лінійно зростає зі збільшенням кількості учасників.

Блокчейн Zilliqa був першим публічним блокчейном, який запропонував вирішити проблему масштабованості за допомогою шардингу. Однак , цей блокчейн не відповідає двом напрямкам. По-перше, він не розділяє зберігання даних блокчейну (шордування стану). Це заважає машинам з обмеженими ресурсами брати участь у мережі, тим самим обмежуючи децентралізацію.

Консенсусні алгоритми, засновані на PoW блокчейні, споживають багато обчислювальних ресурсів. У багатьох сценаріях застосування, користувачі не можуть отримати потужну обчислювальну потужність, і всі алгоритми консенсусу на основі майнінгу стикаються з малою швидкістю транзакцій. Якщо масштабованість системи блокчейн не буде вирішена, то її не можна буде застосовувати у різних сферах [52].

Деякими розробниками пропонується паралельно розподілена архітектура розподіленої хмарної системи зберігання даних та системи децентралізації блокчейну для вирішення проблеми масштабованості, великомасштабного зберігання та обміну даними. Запропонований метод представляє новий гібридний консенсус-протокол для широкомасштабного публічного блокчейну, заснований на спільній оптимізаційній розробці.

Запобігання атаці Sybil є ключовим фактором безпеки в публічних блокчейнах. Атака Sybil – це тип однорангової атаки, яка лише з'єднує жертву з вузлами, контрольованими зловмисником. У однорангових мережах, де ні один вузел не є надійним, кожен запит дублюється для кількох одержувачів, так що немає єдиного вузла, якому можна буде повністю довіряти. У той же час користувачі мережі можуть мати декілька ідентифікаторів, які фізично пов'язані з різними вузлами. Ці ідентифікатори можуть бути використані для спільного використання ресурсів або мати кілька їх копій. Останнє створить резервування, яке перевірить цілісність даних, взятих з мережі самостійно. Зворотна сторона такого підходу полягає в тому, що в якийсь момент всі доступні сайти, які повинні представляти різних одержувачів певного запиту, можуть контролюватися тим самим користувачем. Таким чином, якщо цей користувач виявиться порушником, він матиме на цій сесії всі можливості посередника, невиправдано отримав при цьому повну довіру ініціатора сесії. Чим більше ідентифікаторів зловмисник має, тим більша ймовірність того, щонаступний сеанс користувача буде закрито. Зловмиснику важливо, щоб новий ідентифікатор був досить легким для створення [53].

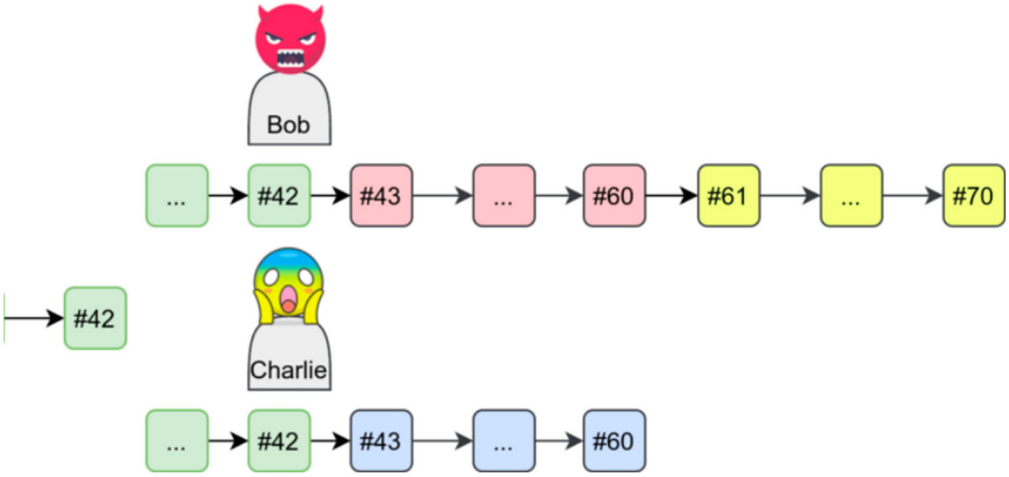

Рисунок 4.2 – Блокчейн, який розділяється на два, тому що шкідливівузли хочуть створити блоки, які не відповідають консенсусу

Bitcoin та Etherium вимагають від майнерів обчислення криптографічної головоломки (PoW), перш ніж вони зможуть запропонувати блок. Подібним чином, блокчейни на основі шардингу, такі як Zilliqa [54] або Quarkchain [55], також використовують PoW для запобігання атакам Sybil.

Шардінг – метод поділу та зберігання єдиного логічного набору даних у вигляді безлічі баз даних. Інше визначення шардінга – горизонтальний поділ даних. Стосовно до блокчейну, шардінг передбачає поділ мережі блокчейна на індивідуальні сегменти (шарди). Кожен шард містить унікальний набір смарт-контрактів і балансів рахунків. За кожним шардом закріплюється нода, верифікуються транзакції і операції, на відміну від методу, в якому кожна нода відповідає за верифікацію кожної транзакції у всій мережі. Поділ блокчейна на більш керовані сегменти дозволяє збільшити пропускну здатність транзакцій і тим самим вирішити проблему масштабованості, з якою стикається більшість сучасних блокчейнів.

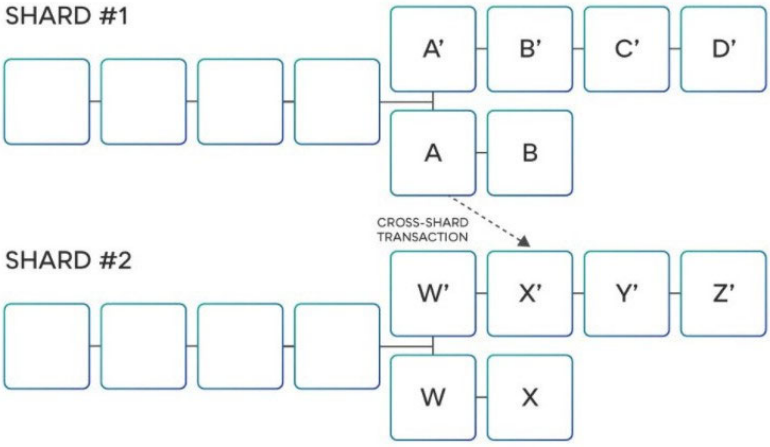

Рисунок 4.3 – Шарди у блокчейні Zilliqa

У цьому блокчейні є два шарди, обидва вони мають розгалуження саме тоді, коли транзакція включена у блок A в шарді №1 і блок X у шарді № 2. Коли відбувається розгалуження, шарди повинні відкинути один ланцюжок і прийняти інший. У цьому випадку, якщо шард №1 приймає ланцюжок A, B і так далі, і шард №2 – ланцюжок W, X і так далі, консенсус буде підтверджений. Якщо шард №1 приймає ланцюжок A, B і так далі, а шард №1 – ланцюжок W`, X` і т.д., угода буде відхилена і може бути відправлена знову. Якщо шард №1 приймає ланцюжок A`, B` і т.д., і шард №2 – ланцюжок W, X і т.д, тоді одна частина угоди буде підтверджена (A`, B` і т.д.), а інша частина не буде (W, X і т.д.).

Різні рішення для шардінгу пропонуються як у промисловості, так і в науці. У промисловості Zilliqa був першим публічним блокчейном на базі шардингу, який заявив про пропускну здатність 2800 транзакцій в секунду. Zilliqa використовує PoW як процес реєстрації особи (тобто запобігання атаці Sybil. Мережа Zilliqa містить єдиний комітет з обслуговування каталогів та декілька комітетів з шардів (тобто мережеве шардування), кожен з яких містить сотні вузлів. Транзакції присвоюються різним шардам та обробляються окремо. Отримані блоки з усіх осколків збираються та об'єднуються в комітеті служб довідників. В академічних колах такі публікації, як Omniledger [56] та RapidChain [57], пропонують такі рішення, де кожен шардінг містить підмножи-

ну стану блокчейну. Omniledger використовує багатосторонній обчислювальну схему під назвою RandHound [25], щоб сформувати безпечне випадкове число, яке використовується для випадкового розподілу вузлів на шарди. Omniledger припускає адаптивний модель, в такому разі зловмисники з часом можуть пошкодити все більшу частину вузлів. Згідно з такою моделлю безпеки, один фрагмент може врешті-решт бути пошкоджений. Omniledger запобігає пошкодженню осколків шляхом перестановки всіх вузлів в осколках за встановлений часовий інтервал, що називається епоха (фаза). RapidChain будується на вершині Omniledger і пропонує використовувати правило обмеження для перестановки вузлів без перерв [58].

4.1.3 Генерація розподіленої випадковості

На поточний момент запропоновано різні підходи для розподілу вузлів в шарди, такі як розподіл на основі випадковості [56] розподіл на основі розташування [59] та централізоване управління [60]. З усіх підходів найбільш надійним рішенням було визнано шардування на основі випадковості. У заснованому на випадковості шардінгу для кожного вузла використовується взаємоузгоджене випадкове число.

Випадкове число повинно мати такі властивості:

1. Непередбачуване: ніхто не повинен мати змоги передбачити випадкове число до його створення.
2. Необ'єктивне: процес генерації випадкового числа не повинен бути упередженим будь-яким учасником.
3. Повинно перевірятися: дійсність сформованого випадкового числа повинно перевірятися будь-яким спостерігачем.
4. Масштабоване: алгоритм генерації випадковості повинен масштабуватися до великої кількості учасників.

Блокчейн Omniledger [56] використовує протокол RandHound [61], який є процесом генерації розподілених випадкових випадків, керованим лідером, який включає PVSS (Public Public Verified Secret Sharing) та візантійську угоду. RandHound – це протокол, який ділить вузли учасників на кілька груп розміру. Він досягає перших трьох властивостей описаних вище, але повільно кваліфікується як масштабований.

RapidChain застосовує більш простий підхід, дозволяючи кожному учаснику виконувати VSS (Verifiedble Secret Sharing) [62] і використовуючи комбіновані секретні обміни як результуючу випадковість. Даний протокол не захищений, оскільки шкідливі вузли можуть надсилати несумісні спільні ресурси на різні вузли [61]. Крім того, RapidChain не описує, як вузли досягають консенсусу щодо багатьох можливих версій відновленоївипадковості.

Ethereum 2.0 пропонує використання перевірки функції затримки, для затримки розкриття фактичного випадкового числа, щоб запобігти хакерськоїатаки [63]. Перевірка функції затримки являє собою криптографічний примітив, для обчислення потрібно регульована мінімальна кількість часу, і результат можна негайно перевірити.

4.2 Огляд методу

В даній роботі для створення повністю масштабованого, доказово безпечного та енергоефективного блокчейну, досліджено функціональні можливості і особливості системи блокчейн на основі шардингу наступного покоління, який вирішує низку проблем існуючих блокчейнів.

Підхід вдосконалює існуючі методи. Завдяки масштабованості та енергоефективності метод підходить для створення блокчейну для використанні його у сфері навчання.

4.2.1 Масштабований протокол консенсусу

Як вдосконалення PBFT у даній роботі запропоновано лінійно масштабований з точки зору складності комунікації механізм консенсусу. Замість того, щоб просити всіх валідаторів опублікувати свої голоси, лідер запускає процес підписання з декількома підписами для збору голосів валідаторів у $O(1)$ – мульти-підпис, а потім транслюйте його. Тому замість отримання $O(N)$ підписів, кожен валідатор отримує лише один мульти- підпис, тим самим зменшуючи складність зв'язку з $O(N)^2$ до $O(N)$.

Ідея використання $O(1)$ – багатофункціонального підпису це покращення методу BFT від блокчейну ByzCoin [64], який використовує схемупідпису Шнорра для агрегування багатозначних сигналів постійного розміру та формує дерево багатоадресної розсилки серед валідаторів для полегшення доставки повідомлення. Однак багатозначний підпис Шнорра вимагає таємного раунду зобов'язань, що призводить до загальної кількості двох запитів в обидва кінці для одного мультипідпису.

Запропонований у роботі метод вдосконалює вже інуючий завдяки використанню мультипідпису BLS (Boneh – Lynn – Shacham) [65], який вимагає лише одного запиту туди-назад. Тому запропонований методпринаймні на 50% швидший, ніж метод BFT ByzCoin.

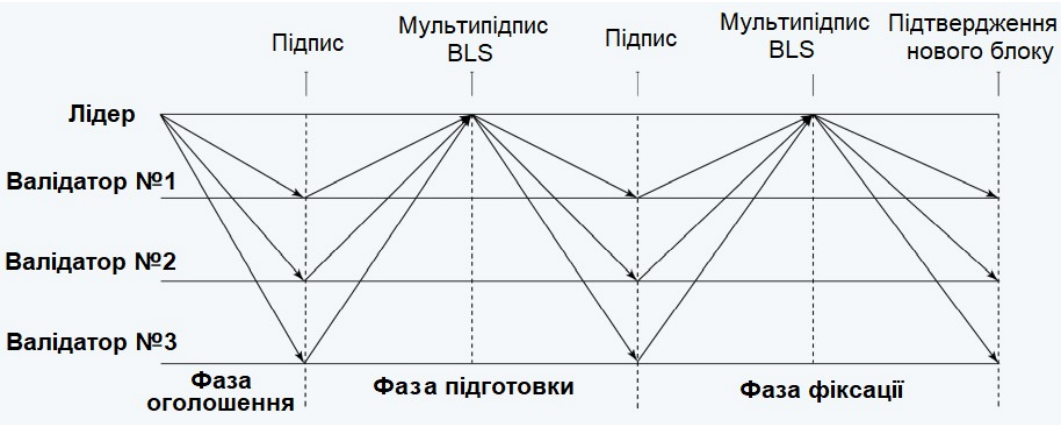

Рисунок 4.4 – Мережева комунікація під час одного раунду консенсусу

Запропонований консенсус передбачає такі кроки:

1. Лідер конструює новий блок і передає заголовок блоку усім валідаторам. Тим часом лідер транслює вміст блоку із кодуванням стирання. Це називається фазою "оголошення".
2. Валідатори перевіряють дійсність заголовка блоку, підписують заголовок блоку підписом BLS і відправляють підпис назад лідеру.
3. Лідер чекає принаймні $2f + 1$ дійсних підписів від валідаторів (включаючи підпису самого лідера) і об'єднує їх у BLS мульти-підпис. Потім лідер транслює агрегований мульти-підпис разом із растровим малюнком зі змінами, які підписали валідатори. Разом із кроком 3 завершується етап "підготовки" PBFT.
4. Валідатори перевіряють, чи має мульти-підпис хоча б $2f + 1$ підписувачив, перевіряє транзакції з блоковим вмістом, що транслюються від лідера на кроці 1, підписують отримане повідомлення з кроку 3 і надсилають його назад лідеру.
5. Лідер чекає принаймні $2f + 1$ дійсних підписів і починаючи з кроку 4, об'єднує їх разом у BLS-мульти-підпис і створює растрове зображення, що реєструє всіх, хто підписував. Після чого лідер фіксує новий блок із усіма підписаними, мульти-підписами та растровими зображеннями та передає новий блок для всіх валідаторів. Разом із кроком 5 завершується фаза "фіксації" PBFT.

Валідатори консенсусу обираються на основі Proof-of-Stake. Запропонований протокол відрізняється від існуючого PBFT тим, що валідатор із більшою кількістю голосуючих акцій має більше голосів, ніж інші, а не один підпис-один голос. Замість того, щоб чекати хоча б $2f + 1$ підписи від валідаторів, лідер чекає підписів від валідаторів, які колективно володіють принаймні $2f + 1$ голосуючих акцій.

Традиційна процедура завантаження історії блокчейнів і реконструкція поточного стану занадто повільна, щоб не було можливе повторне внесення

змін (на повну синхронізацію історії блокчейну Ethereum потрібно декілька днів), враховуючи те, що поточний стан значно менший за всю історію блокчейну. Завантаження поточного стану за часовий проміжок епохи можливий порівняно із завантаженням усієї історії. Для того, щоб оптимізувати процес синхронізації стану запропоновано зробити стан блокчейну якомога меншим.

У Ethereum багато рахунків порожні і витрачають простір стану блокчейну. Порожні рахунки не можна видалити через можливі помилки відтворення, коли старі транзакції повторно подаються на видалений рахунок[66]. Дану проблему можна вирішити уникненням атак повтору, дозволивши транзакціям вказати хеш поточного блоку: транзакція дійсна лише до певної кількості (наприклад, 300) блоків, що слідують за блоком зазначеного хешу. Таким чином, старі облікові записи можна безпечно видалити, це значно прискорить перевірку стану блокчейну.

Таким чином нові валідатори, які приєднуються до шарду, спочатку завантажують поточний стан цього осколка, щоб вони могли швидко розпочати перевірку транзакцій. Щоб переконатись, що поточний завантажений стан є дійсним, новий вузол повинен зробити належну перевірку. Замість того, щоб завантажувати всю історію блокчейнів і відтворювати всі транзакції для перевірки поточного стану, новий вузол завантажує історичні заголовки блоків і перевіряє заголовки, перевіряючи їх підписи. Поки існує криптографічний слід (наприклад, хеш-вказівники та підписи) від поточного стану до блоку генезису, стан є дійсним. Перевірка підписів не є незатратною обчислювальною і це займає значну кількість часу на те, щоб перевірити всі підписи, починаючи з блоку генезису. Щоб пом'якшити цю проблему, перший блок кожної епохи запропоновано включати додатковий хеш-вказівник на перший блок останньої епохи. Таким чином, новий вузол може переходити через блоки протягом епохи, коли відстежує хеш-вказівники до блоку генезису. Це значно пришвидшить перевірку поточного стану блокчейну.

4.2.2 Механізму вибору, що підтверджує шард

В запропонованому консенсусі застосовується підхід, котрий відрізняється від раніше розглянутих – із доказом частки (PoS) як механізмом реєстрації валідатора або механізму запобігання атакам Sybil. Для того, щоб стати валідатором майбутні учасники (або зацікавлені особи) повинні зробитиставку на певну кількість жетонів, щоб отримати право на участь. Кількість закладених токенів визначатиме кількість голосуючих акцій, призначених валідатору. Такий метод містить основний ланцюг і безліч шардів. Основний ланцюг служить реєстром ідентичності, тоді як ланцюжки шардів зберігають окремі стани блокчейну і одночасно обробляють транзакції. Даний алгоритм використовує генерацію випадковості, поєднуючи функцію перевірки випадкової функції (VRF) і функцію перевірки затримки (VDF) і включає PoS у процес шардінгу, який зміщує питання захисту фрагмента з мінімальної кількості вузлів на мінімальну кількість голосуючих акцій.

Кожна частка, що має право голосу, відповідає одному голосу в консенсусі BFT. Стакери отримують акції з правом голосу, пропорційні їх жетонам. Потім голосуючі частки випадковим чином призначаються шардінгу. Токени стають валідаторами для тих фрагментів, за які вони голосують.

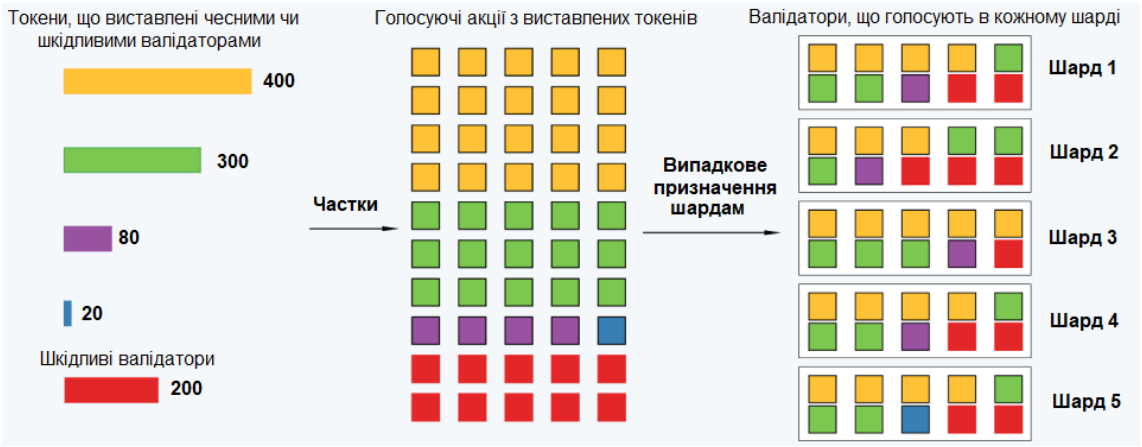

Рисунок 4.5 – Шардінг шляхом голосування акцій

Частка для голосування – це віртуальний квиток, який дозволяє валідатору віддати один голос за консенсус. Валідатори можуть придбати акції з правом голосу, ставлячи токени. Кількість токенів, необхідна для участі в голосуванні,

алгоритмічно коригується. На початку кожної фази нові акції з правом голосу валідаторів будуть випадковим чином присвоюватися шарду. Нові валідатори приєднуються до шарду, де їм призначаються акції з правом голосу. Консенсус у певному фрагменті досягається валідаторами, які, як мінімум, мають спільно $2f + 1$ голосуючих акцій для підписання блоку. Щобгарантувати безпеку одного шарду, кількість голосуючих акцій у шкідливих валідаторів потрібно, щоб було нижче $\frac{1}{3}$ усіх голосуючих акцій цього шарду. Адаптивний PoS запропонованого методу консенсусу гарантує вимоги добезпеки шляхом адаптивного регулювання ціни акції, що має право голосу, і присвоєння окремих акцій, що мають право голосу, шардам, а не окремимперевіряючим.

Безпека шардінгу шляхом голосування акцій полягає в тому, що навіть якщо для всіх закладених токенів $\frac{1}{4}$ являються шкідливими валідаторами, то одному валідатору призначається один шард. В такому разі, в гіршому випадку коли єдиний зловмисний валідатор тримає всі токени (голосуючі акції), він має менше, ніж $\frac{1}{3}$ голосуючих токенів у цьому шарді. Причина в тому, що ставки на кожен шард в m разів менше, ніж ставки всієї мережі, де m – кількість шардів. Таким чином запобігання атаки шкідливих валідаторів замість шардінгу валідаторами, голосуючі акції розділяються (одній акції, що має право голосу, присвоюється один шард).

В такому методі ціна акції, що має право голосу, встановлюється алгоритмічно, так що вона досить мала, щоб шкідливі учасники не могли зосередити свою силу голосу в одному шарді.

Враховуючи достовірне джерело випадковості та процес шардінгу на основі випадковісті, розподіл ймовірності кількості шкідливих голосуючих акцій у кожному фрагменті може бути змодельований як гіпергеометричний розподіл (тобто випадкова вибірка без заміни).

$$P(X = k) = \frac{C_K^k C_{N-K}^{n-k}}{C_N^n} \quad (4.3)$$

де N – загальна кількість голосуючих акцій;

$K = \frac{N}{4}$ – максимальна кількість шкідливих голосуючих акцій;

$n = \frac{N}{N_{\text{ш}}}$ – кількість голосуючих акцій у кожному шарді;

k – кількість шкідливих акцій з правом голосу в шарді.

Фактична частота відмов шарду $P(X \leq k)$ випливає з кумулятивного гіпергеометричного розподілу (N, K, n, k), який, коли N велике, погіршуєтьсядо біноміального розподілу (тобто довільної вибірки із заміною):

$$P(X \leq k) = \sum_{i=0}^{k} (n_i)\, p^i (1-p)^{(n-i)} \quad (4.4)$$

Коли n достатньо великий, ймовірність того, що шард містить більше ніж $\frac{1}{3}$,шкідливих токенів, незначна.

Коли n = 600 ймовірність того, що шард містить менше ніж $\frac{1}{3}$ шкідливих акцій з правом голосу $P(X \leq 200) = 0{,}999997$, це вказує на невдачу такого шарду, тобто консенсус не може бути досягнутий.

Щоб гарантувати високу безпеку шардів λ = 600. λ регулює мінімальну кількість голосуючих акцій, яку повинен містити один шард.

Дане рішення функціонально подібне до мінімальної кількості вузлів в осколку, які описано в інших рішеннях на основі PoW [56,57].

Цей підхід стійкий до коливань кількості валідаторів. В ньому не встановлено нижню межу кількості валідаторів у кожному фрагменті, як в інших рішеннях, таких як Zilliqa. Натомість прийнято адаптивну модель на

основі PoS, щоб зловмисники ніколи не могли займати більше ніж $\frac{1}{3}$ голосуючих акцій в одному шарді, що і робить його надійним.

4.2.3Масштабована генерація випадковості за допомогою VRF та VDF

Підхід запропонованого блокчейну поєднує в собі переваги розглянутих рішень. Verifiable Random Function (VRF) – функція випадкової перевірки. Verifiable Delay Function (VDF) – функція перевірки затримки. Даний підхід використовує консенсус BFT для забезпечення остаточності випадкового числа. Зокрема, протокол включає такі етапи:

1. Лідер посилає повідомлення з хешем останнього блоку $H(B_{n-1})$ для всіх валідаторів.
2. Для кожного валідатора i, після отримання повідомлення, VRF обчислюється для створення випадкового числа r_i і доказуp_i:$(r_i, p_i) = VRF\big(sk_i, H(B_{n-1})\big), v$, v, де sk_i це секретний ключ валідатора i, v– це поточний номер консенсусу. Тоді кожен валідатор відправляє назад (r_i, p_i)до лідера.
3. Лідер чекає, поки не отримає принаймні $f + 1$дійсних випадкових чисел і поєднує їх за допомогою операції, щоб отримати прообразостаточної випадковості $pRnd$.
4. Лідер проводить BFT серед усіх валідаторів для досягнення консенсусу щодо $pRnd$ зафіксуйте це блоціB_n
5. Після того, як $pRnd$ виконується, лідер починає обчислювати фактичну випадковість $Rnd = VDF(pRnd, T)$, де T є складністю VDF і встановлюється алгоритмічно таким чином, що випадковість можна обчислити лише після kблоків. Коли йде обчислення Rnd, лідер ініціює BFT серед усіх валідаторів для узгодження дійсностіRndі згенерувати випадковісті у блокчейні.

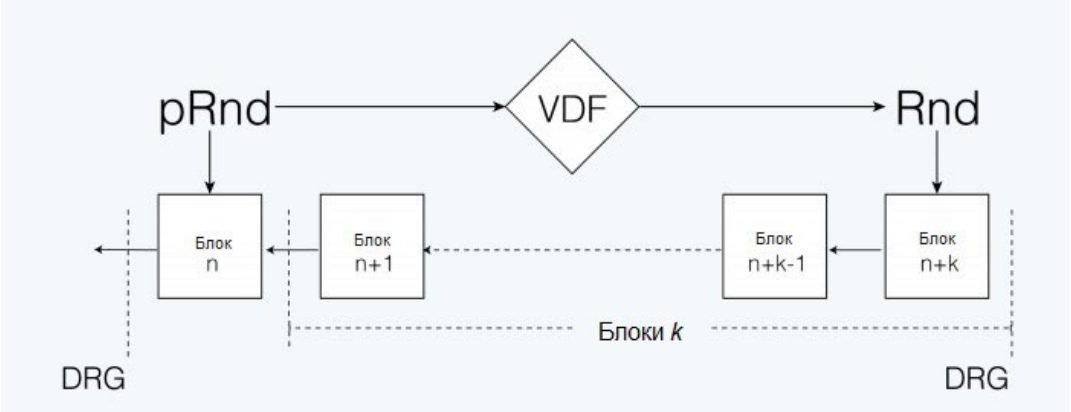

Рисунок 4.6 – Затримка виявлення остаточної випадковості Verifiable DelayFunction

VDF використовується для доказової затримки розкриття Rndі для того, щоб запобігти шкідливому лідеру упереджувати випадковість, вибираючи значення підмножини випадкових чисел VRF.

Завдяки VDF лідер не зможе дізнатися фактичну остаточну випадковість$pRnd$поки вона не додана до блокчейну. Поки Rndобчислюється за допомогою VDF, $pRnd$вже додано у попередній блок, тому лідер більше не може ним маніпулювати.

Найгірше, що може зробити шкідливий лідер це або додати випадковість$pRnd$або зупинити протокол, не фіксуючи $pRnd$. Це не завдасть великої шкоди, оскільки той механізм очікування буде використаний для перемикання лідера та перезапуску протоколу. В майбутньому в довгостроковій перспективі можуть бути винайдені ASIC (інтегрована схема для вирішення конкретних задач) для обчислень VDF, яка зможе знайти вразливі вузли і обчислити результат перед іншими чесними вузлами. Але на даний час настільки потужні схеми ще не винайдені.

Висновки до розділу

У цьому розділі запропонована нова система блокчейн, яка працює на лінійно масштабованого механізмі консенсусу, методу вибору, що підтверджує шард шляхом голосування акцій та має масштабовану генерація випадковості за

допомогою VRF та VDF. Система заснована на аналізі існуючих механізмів консенсусів, шардінгу та генерації розподіленої випадковості. Вона повністю маштабована, безпечна, енергоефективна та маєшвидкий консенсус.

Порівняно з методами, наведеними у на початку розділу, покращений метод шардів виконує не тільки мережевий зв'язок та перевірку транзакцій, але також розкриває стан блокчейну і виконує не тільки мережевий зв'язок та перевірку транзакцій, але також розкриває стан блокчейну. Поріг досить низький, щоб маленькі валідатори могли брати участь у мережі та отримуативинагороди. Запропонований процес шардінгу є безпечним завдяки процесу розподіленої випадковості (DRG), який є непередбачуваним, неупередженим та перевіреним. Мережа перевантажується безперервно, щоб запобігти повільним адаптивним візантійським шкідникам. На відміну від інших блокчейнів на основі шардингу, які вимагають PoW для вибору валідаторів, запропоновани консенсус базується на PoS і, отже, енергоефективний. Консенсус досягається за допомогою лінійно масштабованого алгоритму BFT, який швидше за PBFT. Впроваджуючи інновації на протокольному і на мережевому рівнях, надають масштабовану та безпечну систему блокчейн, яка здатна підтримувати децентралізовану економіку децентралізацію.

ВИСНОВКИ

У даній кваліфікаційній роботі була запропонована нова система блокчейн, яка працює на лінійно масштабованому механізмі консенсусу, методу вибору, що підтверджує шард шляхом голосування акцій, та має масштабовану генерацію випадковості за допомогою функції випадкового перевірки та функції перевірки затримки.

Методи створення такого блокчейну покращують вже існуючі механізми функціонування блокчейну і мають практичну цінність використання розподільної бази даних блокчейн для навчальних потреб, зокрема, ідентифікації та обліку успішності студента, автоматичної видачі дипломів і сертифікатів, проведення тестувань, залучення інвестицій.

В рамках магістерської дисертації проведено дослідження розподіленої бази даних блокчейн. На основі проведених досліджень отримано наступні результати:

1 Проаналізовано теоретичні засади основних принципів роботи технології розподіленого реєстру та їх відмінності від традиційних баз даних. Проведено огляд технології блокчейн, вивчено можливість і доцільність її використання у різних сферах, у тому числі для створення освітнього середовища.

2 Досліджено та описано алгоритми створення блокчейну, наведено приклади готових рішень для реалізації технології у навчанні. Розглянуто програмні засоби і особливості розробки та функціонування технології блокчейн.

3 Розглянуто особливості застосування чотирьох методів реалізації технології блокчейн у сферу навчання. Наведено опис методів та детально описані їх алгоритми на основі проведеного теоретичного аналізу, в ході якогобув розібраний принцип використання технології блокчейн.

4 Запропонований метод створення повністю масштабованого, доказово безпечного та енергоефективного блокчейну, завдяки використанню нового протоколу консенсусу, шардінгу та генерації розподіленої випадковості.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1 Vasin, P. (2014) Blackcoin’s Proof-of-Stake Protocol v2, URL: https://blackcoin.co/blackcoin-pos-protocolv2-whitepaper.pdf

2 Генкин А. С. Блокчейн: Как это работает и что ждет нас завтра [Текст] / А.С. Генкин, А. А. Михеев. — Москва: Альпина Паблишер, 2018. — 592 с.

3 Holmberg A. The Theatre of Robert Wilson. Cambridge University Press, 1996. – Vol. E77 – D. – No.20, October. – P. 899-902

4 Муравьева, Г.Е. Проектирование технологий обучения / Г.Е. Муравьева // Вестник Брянского государственного технического университета. - 2008. - №4. - С.149-155.

5 Meunier S. Blockchain technology — a very special kind of DistributedDatabase//Medium.com. 2016. URL:

6 https://medium.com/@sbmeunier/blockchaintechnology-a-very-special-kind-of-distributed-database-e63d00781118

7 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

8 Ассоциация Финтех. Децентрализованная сеть обмена и хранения информации "Мастерчейн". White paper, версия 1.1 2017. URL: http://fintechru.org/documents/Masterchain_whitepaper_11_08.pdf

9 DeCenter. Смарт-контракты и платформы для их реализации [Электронный ресурс] [2018]. URL: https://decenter.org/ru/smart-kontrakty-i-platformy-dlya-ikh-realizatsii

10 Як влаштований блокчейн і навіщо він потрібен / Афіша - медійно-сервісна платформа Rambler & Co, URL: https://daily.afisha.ru/brain/6058-kak-ustroen-blokcheyn-i-zachem-on-nuzhen/

11 A. Kumar, C. Fischer, S. Tople, and P. Saxena, "A Traceability Analysis of Monero's Blockchain,"IACR Cryptology ePrint Archive, vol. 2017, p. 338, 2017.
12.Исаев М. Д. Проблемы образования в государственных федеральных учреждениях высшего образования [Текст] / М. Д. Исаев // Молодой ученый. — 2017. — №2. — С. 676–678.
12 Стаття «Blockchain Technology Applications in Education», URL: https://www.researchgate.net/publication/337670514_Blockchain_Technology_Applications_in_Education
13 Стаття «Blockchain in education research», URL: https://journals.uic.edu/ojs/index.php/fm/article/view/10654/9726
14 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.
15 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.
16 Стаття «The Blockchain Revolution and Higher Education», URL: https://er.educause.edu/articles/2017/3/the-blockchain-revolution-and-higher-education
17 Стаття «Using blockchain to re-imagine learning», URL: https://medium.com/@KnowledgeWorks/using-blockchain-to-re-imaginelearning-fb3bf2717b09
18 Стаття «Use Cases for Blockchain for Higher Ed», URL: https://www.ibm.com/blogs/blockchain/2019/02/how-blockchain-could-change-higher-education/
19 Стаття «Smart Contracts for Effective Curriculum», URL: https://medium.com/@benblair_34530/smart-contracts-for-effective- curriculum-30c610067c51

20 Стаття «Authenticating academic certificates on the Bitcoin» blockchain, URL: https://bravenewcoin.com/insights/authenticating-academic-certificates-on-thebitcoin-blockchain

21 Стаття «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

22 Стаття «Blockchain Technology Needs to Be Changing Education», URL: https://medium.com/age-of-awareness/blockchain-technology-needs-to-be-changing-education-2739324281e2

23 On the (Im)possibility of Obfuscating Programs, URL:https://www.iacr.org/archive/crypto2001/21390001.pdf

24 Febin, J. How Can Blockchain Technology Innovate Your EducationHackernoon, URL: https://hackernoon.com/how-can-blockchain technology- innovate-your-educationd1cd80c26f08

25 Поляков Н. Е. Впровадження технології блокчейн в освіту: зарубіжний досвід / Н. Є. Поляков, А. В. Солодов // Управління соціально- економічними системами: теорія, методологія, практика: збірник статей III Міжнародної науково-практичної конференції. - Пенза: МЦНС «Наука і Просвещение», 2017. - Ч. 2. -С. 100-104

26 Sony впроваджує блокчейн в сферу освіти, URL: https://cryptorussia.ru/news/sony-vnedryaet-blokcheynv-sferu-obrazovaniya

27 Sony Details Blockchain Use for Education Data / CoinDesk - компанія, що спеціалізується на цифрових медіа, події та інформаційних послугах для спільноти кріптоактівов і блокчейн технологій, URL: https://www.coindesk.com/sony-patentfiling-details-blockchain-use-managing-education-data/Watters, A. The Blockchain for Education: An Introduction / Hack Education - особистий блог Одрі Уоттерс. http://hackeducation.com/2016/04/07/blockchain-education-guide

28 Grech, A., Gamilleri, AF Blockchain in Education, URL: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education(1).pdf

29 Indistinguishability Code Obfuscation research, URL: https://eprint.iacr.org/2013/451.pdf

30 Intel Software Guard Extensions, URL: https://software.intel.com/sgx

31 Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contract Execution, URL: https://arxiv.org/abs/1804.05141

32 S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system,"2008, URL: https://bitcoin.org/bitcoin.pdf.

33 A. Miller, M. M¨oser, K. Lee, and A. Narayanan, "An Empirical Analysis of Linkability in the Monero Blockchain,"arXiv preprintarXiv:1704.04299, 2017

34 Солодов А. В. Внедрение технологии блокчейн в образование: зарубежный опыт [Текст] / А. В. Солодов // Инновационные научныеисследования: теория, методология, практика: теория, методология, практика: сбор- 93 ник статей XII Международной научно-практической конференции. — Пенза: МЦНС «Наука и Просвещение», 2018. — Ч. 1. — С. 215–218.

37 Солодов А. В. Массовые открытые онлайн-курсы – альтернатива традиционному образованию / А. В. Солодов // Актуальные проблемы развития вертикальной интеграции системы образования, науки и бизнеса: экономические, правовые и социальные аспекты: материалы V Международной научно-практической конференции. — Воронеж: АНОО ВО ВЭПИ, 2016. — Т. 3. — С. 218–221

38 Сорокина Н. В. Система образования в Волгоградской области: современное состояние и тенденции развития / Н. В. Сорокина, Л. А. Григорьева // Научный вестник Южного института менеджмента. — 2016. — № 4. — С. 56–59.

39 Тапскотт Д. Технология блокчейн: то, что движет финансовой революцией сегодня / Д. Тапскотт, А. Тапскотт; пер. К. Шашковой, Е. Ряхиной. — Москва: Эксмо, 2017. — 448 с

40 Цветкова Л. А. Перспективы развития технологии блокчейн: конкурентные преимущества и барьеры / Л. А. Цветкова // Экономика науки. — 2017. — Т. 3. — № 4. — С. 275–296.

41 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

42 Поляков, Н. Е. Внедрение технологии блокчейн в образование: зарубежный опыт / Н. Е. Поляков, А. В. Солодов // Управление социально- экономическими системами: теория, методология, практика: сб. ст. III Междунар. науч.-практ. конф. – Пенза: МЦНС «Наука и Просвещение», 2017. – Ч. 2. – С. 100–104.

43 Ковалев, М. М. Образование для цифровой экономики / М. М. Ковалев // Цифровая трансформация. – 2018. – № 1(2) . – С. 37-

44 Солодов, А. В. Массовые открытые онлайн-курсы – особенности и перспективы / А. В. Солодов, А. О. Прокубовская, Е. В. Чубаркова // Наука. Информатизация. Технологии. Образование: материалы XI Междунар. науч.-практ. конф. – Екатеринбург: ФГАОУ ВО РГППУ, 2018. – С. 434–440

45 Grech, A. Camilleri, A. F. (2017) Blockchain in Education. Inamorato Santos, A. Luxembourg: Publications Office of the European Union, 2017. – 132p.

46 Солодов, А. В. Codecademy как средство обучения программированию / А.В. Солодов // Фундаментальные и прикладные исследования: от теории к практике:материалы Междунар. науч.-практ. конф., приуроченной ко Дню

российской науки. – Воронеж; КызылКия: АНОО ВО ВЭПИ, 2017. – Т. 1. –С. 225–228

47 Свон, М. Блокчейн: схема новой экономики / М. Свон. – М.: Олимп-Бизнес, 2017. – 240 с

48 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

49 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.

50 Кирилова, Д.А. Перспективы внедрения технологии блокчейн в современную систему образования / Д.А. Кирилова, Н.С. Маслов, Т.Н. Астахова // International Journal of Open Information Technologies. – 2018. –№ 6. – С. 31-37

51 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

52 Dan Boneh, Joseph Bonneau, Benedikt Bünz, and Ben Fisch. Verifiable delay functions. In CRYPTO 2018, 2018.

53 J.R. Douceur, The Sybil attack, in: 1st International Workshop on Peer-to-Peer Systems (IPTPS 02), 2002.

54 The Zilliqa Team. The zilliqa technical whitepaper, URL: whitepaper.pdf (zilliqa.com)

55 The QuarkChain Team. Cross Shard Transaction, URL: https://github.com/QuarkChain/pyquarkchain/wiki/Cross-Shard-Transaction

56 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.

57 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.

58 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.

59 M. F. Nowlan, J. Faleiro, and B. Ford. Crux: Locality-preserving distributed systems. CoRR, abs/1405.0637, 2014.

60 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.

61 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.

62 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.

63 Paul Dworzanski. A note on committee random number generation, commit-reveal, and last-revealer attacks. ,
URL: http://paul.oemm.org/commit_reveal_subcommittees.pdf.

64 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.

65 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

66 Derek Leung, Adam Suhl, Yossi Gilad, and Nickolai Zeldovich. Vault: Fast bootstrapping for cryptocurrencies. Cryptology ePrint Archive, Report 2018/269, 2018.