Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи)

магістр
(освітній рівень)

на тему: *«Дослідження та розробка програмних компонентів для токенізації активів на основі блокчейн технологій»*

Виконав: студент (ка) *VI* курсу, групи *СБм-61*
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Фіголь В.Я.
підпис (прізвище та ініціали)

Керівник *Карпінський М.П.*
підпис (прізвище та ініціали)

Нормоконтроль *Лобур Т.Б.*
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 20*20*

АНОТАЦІЯ

Дослідження та розробка програмних компонентів для токенізації активів на основі блокчейн технологій // Дипломна робота ОР «Магістр» // Фіголь Валерій Ярославович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2020 // С. , рис. – 111, табл. – , кресл. – , додат. – .

Ключові слова: ТОКЕНІЗАЦІЯ АКТИВІВ, БЛОКЧЕЙН, АЛГОРИТМИ КОНСЕНСУСУ, ДЕЦЕНТРАЛІЗОВАНИЙ РЕЄСТР.

Дана магістерська кваліфікаційна робота присвячена дослідженню методів та технологій токенізації активів, пов'язаних з навчальним процессом. Проведено дослідження засобів і механізмів забезпечення підтвердження справжності документів про освіту, конфеденційності особових карток студентів, , ідентифікації студентів.

Для створення децентралізованого розподіленого реєстру для токенізації освітніх активів, запропоновано застосування технології блокчейн та смарт-контрактів. В роботі запропоновано розподілений реєстр даних, який містить інформацію про студентів у вигляді цифрових токенів.

У першому розділі наведено основні теоретичні відомості щодо тематики роботи. У другому розділі проведено аналіз протоколів забезпечення конфіденційності, цілісності та автентичності даних у технологіях блокчейн та смарт-контрактах. У третьому розділі наведено приклад розробки програмного забезпечення для токенізації освітніх активів (дипломів про освіту) га основі технології блокчейн. В четвертому розділі описано приклад використання розробленого програмного забезпечення.

У підрозділі "Охорона праці" розглянуто правила охорони праці під час експлуатації електронно-обчислювальних машин У підрозділі "Безпека життєдіяльності" описано окремі питання безпеки у виробничих приміщеннях.

ANNOTATION

Study and development of program components for the assets tokenization based on blockchain technologies // Thesis of "Master" Degree// Fihol Valerii Yaroslavovych // Ternopil National Technical University named after Ivan Pulyuy, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group SBm-61 // Ternopil, 2020 // S., fig. - 111, table. -, chair. -, added. -.

Keywords: TOKENIZATION OF ASSETS, BLOCKCHAIN, CONSENSUS ALGORITHMS, DECENTRALIZED REGISTER.

This master's thesis is devoted to the study of methods and technologies of tokenization of assets related to the educational process. The research of means and mechanisms of ensuring confirmation of authenticity of documents on education, confidentiality of identity cards of students,, identification of students is carried out.

To create a decentralized distributed registry for tokenization of educational assets, the use of blockchain technology and smart contracts is proposed.

The paper proposes a distributed data register, which contains information about students in the form of digital tokens.

The first chapter provides basic theoretical information on the subject of the work.

The second chapter analyzes the protocols for ensuring the confidentiality, integrity and authenticity of data in blockchain technologies and smart contracts.

The third chapter gives an example of software development for tokenization of educational assets (diplomas of education) based on blockchain technology.

The forth chapter describes an example of using the developed software.

The fifth section calculates the main indicators of economic efficiency from the development and implementation of the proposed algorithm.

In the subsection "Occupational safety" the rules of occupational safety during operation of electronic computers are considered. In the subsection "Safety of life" separate questions of safety in industrial premises are described.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

PI – Application programming interface;

BTC – Bitcoin;

ECDSA – Elliptic Curve Digital Signature Algorithm;

ETH - Ethereum

ICO – Initial coin offering;

IOTA – Internet of Things;

NIST – National Institute of Standards and Technology;

P2P – Person to Person;

PoS – Proof of Stake;

PoW – Proof of Work;

SEC – The United States Securities and Exchange Commission;

SHA – Secure Hash Algorithm;

XRP – Ripple;

ВСТУП

Сьогодні в світі відбувається революційний перехід від інформатизації основних сфер людської діяльності до їх цифровізації.

Якщо інформатизація передбачає, по суті, модернізацію тих чи інших видів людської діяльності на основі використання інформаційно-комунікаційних технологій, то цифрова трансформація (або цифровізація) передбачає їх якісне перетворення, відхід від звичних видів і форм діяльності до нових, заснованих на цифрових моделях і технологіях [1].

Розвиток цифрового середовища вимагає підтримки і розвитку як вже існуючих умов для виникнення перспективних наскрізних цифрових платформ і технологій, так і створення умов для виникнення нових платформ і технологій.

Основними наскрізними цифровими технологіями є:

- великі дані;
- нейротехнології і штучний інтелект;
- системи розподіленого реєстру (blockchain / блокчейн);
- квантові технології;
- нові виробничі технології;
- промисловий інтернет;
- компоненти робототехніки та сенсорика;
- технології бездротового зв'язку;
- технології віртуальної і доповненої реальностей.

Продовжуючи цикл робіт по цифровій трансформації освіти [2-7], в роботі проовдяться дослідження щодо використання технології блокчейн (ланцюжків блоків / blockchain) для токенізації освітніх активів і перспективні напрямки її використання в сфері освіти.

Метою даної роботи є моделювання процесів токенізації освітніх активів за допомогою технологій блокчейн та смарт-контрактів.

Для досягнення поставленої мети необхідно вирішити наступні *завдання*:

1. Аналіз основних напрямків розвитку та застосування технологій блокченй в освіті.

2. Аналіз методів забезпечення конфеденційності та цілісності даних в розподіленому реєстрі на основі блокченй.

3. Аналіз алгоритмів хешування технології блокчейн.

4. Дослідження засобів і механізмів забезпечення конфеденційності даних в децентралізованому реєстрі.

5. Моделювання процесів токенізації освітніх активів на основі технології блокчейн.

Об'єктом досліджень є процес забезпечення конфеденційності та цілісності даних в деценралізованому реєстрі.

Предметом дослідження є моделі та алгоритми забезпечення конфедеційності зберігання та обробки даних в децентралізованому реєстрі на основі блокчейн.

Наукова новизна дисертаційного дослідження:

- проведено аналіз напрямків розвитку технології блокчейн у сфері освіти;

- розроблені теоретичні пропозиції щодо впровадження технології блокчейн і організації роботи децентралізованих систем нового виду для токенізації освітніх активів.

Теоретична значимість дослідження обумовлюється актуальністю поставлених завдань і полягає в тому, що отримані в результаті дослідження висновки і пропозиції доповнюють і розвивають ряд аспектів в застосуванні технології блокченй в різних областях і в подальшому можуть послужити теоретичним і практичним фундаментом для концептуального обґрунтування і оптимізації процесів управління організаційними інноваціями в діяльності освітніх організації.

Практична значимість проведеного дослідження полягає в тому, що положення і висновки, викладені в роботі, можуть бути використані вищими навчальнними закладами України при визначенні напрямків розвитку систем електроного навчання.

Апробація результатів роботи. Окремі результати роботи доповідались на VIII науково-технічній конференції «Інформаційні моделі, системи та технології», Тернопіль, ТНТУ, 9 – 10 грудня 2020 р.

1 ТЕОРЕТИЧНА ЧАСТИНА

1.1 Аналіз основних напрямків розвитку технологій блокчейн в освіті

Згідно з книгою Мелані Свон «Блокчейн: Схема нової економіки», можна виділити три умовні області застосування даної технології: Блокчейн 1.0 - це валюта. Криптовалюта застосовуються в різних додатках, що мають відношення до грошей, наприклад системи переказів і цифрових платежів.

Блокчейн 2.0 - це контракти. Цілі класи економічних, ринкових і фінансових додатків, в основі яких лежить блокчейн, працюють з різними типами фінансових інструментів - з акціями, облігаціями, ф'ючерсами, заставними, правовими титулами, розумними активами і розумними контрактами.

Блокчейн 3.0 - додатки, область яких виходить за рамки фінансових транзакцій і ринків [1]. До цієї області і буде відноситися блокчейн в освіті.

Блокчейн дає можливість всьому людству оптимізувати найрізноманітніші сфери життя. Однією із переваг цієї технології є те, що її практично неможливо зламати і немає необхідності в залучення третіх осіб. Весь принцип роботи блокчейна заснований на математиці і криптографії. Згодом, блокчейн вселиться в усі сфери діяльності, в тому числі і в освіту. В даний час існує ряд проблем в освіті. Однією з важливих проблем є шахрайство в сфері підробки документів і проблема збереження документів.

Освітні організації в даний час видають і зберігають дипломи на паперових носіях, у вигляді бланків суворої звітності. Ці дипломи є дорогими для випуску, обслуговування та перевірки.

Інфраструктура відкритих ключів таких як друк та підписи, вимагає використання центру сертифікації як посередника для видачі сертифікатів, створення залежності, яка може бути порушена. У разі стихійних лих або воєн також можуть бути знищені дані документи.

В даний час процес видачі і зберігання дипломів, є вельми довгим і трудомістким. На рисунку 1.1 представлений даний процес.

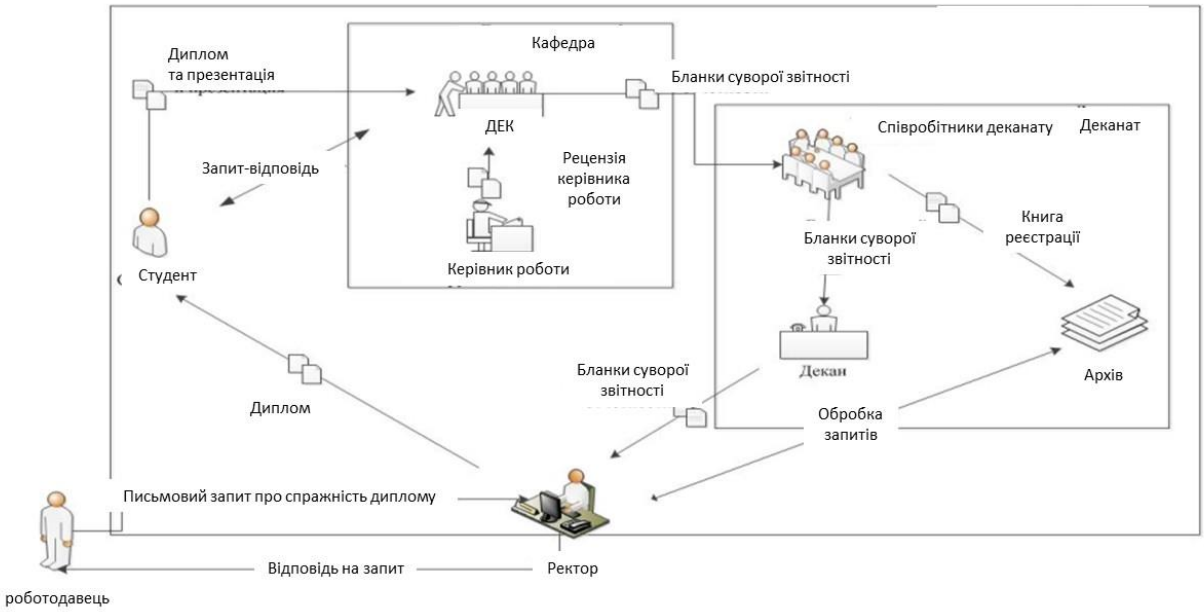

Рисунок 1.1 – Порядок видачі та зберігання дипломів

Захист диплома проводиться на закритому засіданні Екзаменаційної комісії (ЕК). Наприкінці захисту, оголошується оцінка всіх робіт.

Диплом підписується ректором навчального закладу. Всі документи повинні бути завірені печаткою навчального закладу, печатка повинна бути чіткою.

Після того як бланк заповнять його потрібно ретельно перевірити.

Документ, в якому є помилки, вважається зіпсованим і його знищують по спеціально відведеному порядку.

Диплом видається студенту особисто або за заявою висилається поштою, 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.

1.2 Аналіз предметної області дослідження

Для вирішення проблем з шахрайством у сфері підробки документів, і проблемою зберігання документів, в роботі пропонується впровадити токенізацію освітніх активів за допомогою технології блокчейн.

Модель токенізації освітніх активів представлена на рисунку 1.2.

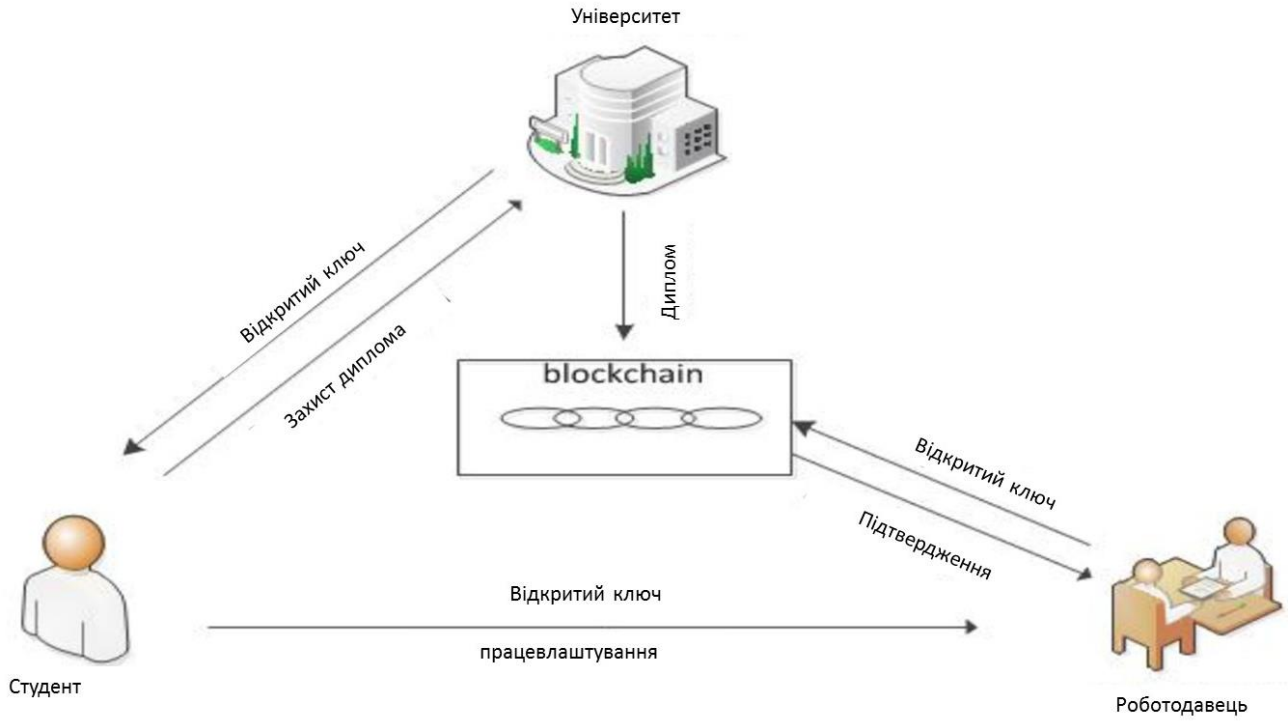

Рисунок 1.2 – Модель токенізації освітніх активів

В цьому випадку, вищі навчальні заклади, що випускають цифрові дипломи (освітні активи), будуть використовувати єдиний децентралізований реєстр 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 в сфері підробки документів і проблему збереження конфіденціальних документів.

Навіть, якщо установа, яка видала диплом, закрилася, дипломи залишаються в розподіленої базі блокчейна. Крім цього, не потрібно витрачати додаткові ресурси, щоб перевірити справжність документа через треті особи, роботодавець може безпосередньо перевірити диплом в ланцюжку блоків.

Щоб детально розібратися в послідовності дій в блокчейн, необхідно розглянути його механізм роботи (рисунок 1.3).

Рисунок 1.3 – Механізм роботи технології блокчейн

В першу чергу, створюється цифровий токен, який містить основну інформацію, такі як назва університету і одержувача диплома, дату видачі, посвідчення і т.ін.

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 - короткий 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 токену диплома, і будь-яка зміна призведе до іншого хешу.

Потім, університет знову використовує свій приватний ключ для створення запису в блокчейн, в якій говориться, що освітня організація видала певний сертифікат певній особі на певну дату.

І нарешті, випускнику передається відкритий ключ. Таким чином, користувач може перевірити, кому був виданий диплом, ким і для перевірки вмісту самого диплома.

Переваги перед поточним станом - докази сертифікатів будуть зберігатися повністю, надійно і в постійному блокчейн реєстрі. Таким чином, навіть якщо установи, що видали сертифікати, закрилися ці сертифікати все ще перевіряються щодо записів, що зберігаються в блокчейн-реєстрі. 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.

Єдиною умовою, необхідною для включення цього сценарію, є програмне забезпечення, яке дасть змогу видавати сертифікати з підписом, розміщеними на блокчейн, а також програмне забезпечення перевірки для підтвердження цих сертифікатів.

1.3 Аналіз перспектив впровадження технології блокчейн для токенізації освітніх активів

Подальшими перспективами впровадження блокчейн в освіту можуть бути такі проекти як:

1) особова картка студента;

2) підтвердження акредитації ВНЗ;

3) інтелектуальна власність;

4) ідентифікація студентів.

Розглянемо їх докладніше.

1. Використання блокчейн в якості особистої картки студента.

Поточний стан: багато різних соціальних мереж, електронні щоденники та інші сервіси, вже надають користувачам можливість записувати свої досягнення. Однак, жоден з них не надає способи перевірки досвіду і облікових даних, описаних і включених в ці системи, тому ці системи працюють як цифровий

аналог коробки, повної паперових сертифікатів, які не отримують, практично ніяких додаткових переваг або ефективності від процесу оцифровки.

У відповідність з даним напрямком в особистій картці студента буде зберігатися успішність, досягнення в навчання і особисті досягнення цього студента. Перевага цього в тому, що кожен студент зможе мати резюме, що містить записи та докази всіх отриманих ним знань, навичок і умінь, що значно скоротить шахрайство пов'язане з підробкою резюме, а також в залежності від форми реалізації, значно скоротить навантаження організацій і приватних осіб, яким необхідно перевіряти це резюме.

З технічної точки зору найпростішим способом реалізації, є створення перевіреного цифрового смарт-контракту. Коли люди завантажують свої досягнення, вони додаються в ланцюжок блоків, які потім перевіряються іншими вузлами блокчейн, за допомогою перевірки фактів досягнення. Як тільки певна кількість користувачів підтвердить вимогу як справжн і в залежності від репутації користувачів, які перевіряють, досягнення отримує оцінку довіри, яка є оцінкою її достовірності. Вже є компанії, що тестують цей вид програмного забезпечення і послуг.

Якщо використовується стандарт метаданих, щоб описати різні типи резюме, наприклад, досвід наукової роботи, зайнятість, навчальні курси. То це буде пов'язано з програмним забезпеченням і системами набору, які дозволять установі автоматично перевіряти, чи мають люди необхідними навичками для різних посад.

2. Використання блокчейна для перевірки акредитації.

Поточний стан: В даний час в Європі існує буквально сотні шляхів акредитації. Що стосується публічної акредитації, то в кожній країні існує своя система акредитаційних організацій і агентств, які їх акредитують, а також різноманітні системи для різних організацій.

Роботодавці часто повинні перевіряти не тільки організацію, що навчає студентів, а й організацію, котра проводить акредитацію. В цьому випадку дипломи, видані державними чи приватними освітніми організаціями, мають значну вагу при визначенні якості кваліфікації.

Щоб дізнатися, виданий диплом законним установою, фізичній особі необхідно буде перевірити:

- що установа дійсно випустила конкретний, диплом. Ніяких підтверджень щодо якості освіти, представленого таким дипломом, не пред'являється.

- акредитаційний орган, чи дійсно він акредитував установу;

- повноваження, чи дійсно акредитуючі органи уповноважені діяти.

Вищевказаний процес, надзвичайно трудомісткий і технічно складний.

Відповідно до цих напрямків, не тільки освітні установи використовують цифрові дипломи (описані в напрямку 1), а й організації, що акредитують їх, так само будуть розміщувати свої цифрові підписи в блокчейн. Це дозволить перевірити не тільки те, що студент X дійсно отримав диплом установи Y, але також, що установа Y було сертифіковане організацією акредитації Z.

Така система може бути використана для забезпечення того, щоб освітня організація, що видає дипломи, була ліцензована урядом, або щоб переконатися, що освітня організація має спеціальні сертифікати якості.

Перевагою даного напрямку є те, що, використовуючи блокчейн, замість того, щоб відправляти запити в усі організації, установи, які повинні перевірити «родовід» диплома, можуть легко зробити це одним клацанням миші. Повністю автоматизований процес міг би візуалізувати ланцюжок акредитації та перевірити, чи дійсно видані дипломи, і що вони все ще дійсні для кожного кроку ланцюга.

Існує цілий ряд різних способів створення такого сценарію, кожен з яких передбачає, що акредитаційні організації публікують свої акредитаційні сертифікати, або підписи цих сертифікатів, на блокчейн, а саме:

- акредитовані організації можуть створювати і публікувати «верифікатори» на своїх власних веб-сайтах, які дозволять будь-якому користувачеві завантажити свій диплом і перевірити, чи дійсно він був випущений акредитованою організацією;

- акредитовані організації можуть публікувати видані дипломи в публічний реєстр. Це дозволило б іншій третій стороні перевірити:

а) диплом, виданий вишем студенту;

б) чи має цей виш акредитацію в публічному реєстрі;

в) справжність вищевказаного.

Ця реалізація вимагає, щоб незалежна довірена сторона створила публічний реєстр.

3. Блокчейн для відстеження інтелектуальної власності.

Поточний стан: в даний час відстеження інтелектуальної власності є дорогою справою, що здійснюється спеціалізованими організаціями, як правило, коли для цього є істотне справу. Таким чином, колекторські агентства відстежують використання інтелектуальної власності музики і відео, щоб збирати «роялті», в той час як журнальні компанії відстежують цитати статей, оскільки ці данні по-перше цінні через його використання для академічного просування. Через складності відстеження інтелектуальної власності людям, які самостійно публікують інформацію, важко відслідковувати і рекламувати повторне використання їх інтелектуальної власності.

Наприклад, повторне застосування відкритих освітніх ресурсів зазвичай не відстежується або відстежується з надзвичайно простими метриками з обмеженою кількістю прав використання.

Застосовуючи технологію блокчейн в майбутньому, вчені публікуватимуть свої роботи у відкритих освітніх ресурсах і записувати посилання, які вони використовували. Це дозволить нотаріально засвідчити дату публікації та авторські права, а також дозволить відстежувати рівень повторного використання будь-якого конкретного ресурсу.

Перевагою такого підходу, із структурної точки зору є те, що цей сценарій дуже схожий на існуючу систему, яка використовується для відстеження цитат для журнальних статей. Однак відстеження цитат досі вимагає посередників, які обмежують використання цих статей, часто у вигляді високих витрат на доступ і обмеження на спільне використання, і використання інтелектуальної власності. Це обмежує використання моделі відкритих освітніх ресурсів.

Використовуючи блокчейн, виключається посередник, дозволяючи будь-кому відкрито публікувати і точно відстежувати повторне використання без обмежень на вихідний матеріал.

Якби така система була впроваджена, це дозволило б вченим одержувати винагороди в залежності від рівня фактичного використання та повторного використання їх інтелектуальних матеріалів, подібно тому, як вони отримують винагороду на основі посилань на дослідні документи.

У цьому сценарії блокчейн буде використовуватися для:

а) оголошення публікації своїх ресурсів і посилання на ці ресурси;

б) оголошення, інших ресурсів, використаних при створенні матеріалу.

Винагороди будуть присуджуватися ученому відповідно до рівня повторного використання їх відповідних ресурсів. Більш просунута реалізація зможе автоматично сканувати ресурси, щоб визначити, який відсоток інших ресурсів був повторно використаний і автоматично присуджуватися відповідним чином.

4. Використання ідентифікації студентів.

Поточний стан: у великих організаціях навчаються, необхідно регулярно ідентифікувати себе з різними підрозділами організації. У таких випадках кожна частина організації збирає дані студента для себе, або використовує технологію єдиного входу (single-sign-on), за допомогою чого одна загальна копія даних учня використовується всіма сторонами всередині організації. У двох цих моделях, десятки, якщо не сотні людей, можуть мати доступ до особистої інформації, тих хто навчається. Для забезпечення безпеки даних потрібно керувати правами доступу для всіх цих людей, а також забезпечення їх безпеки і захисту від злому.

Використовуючи блокчейн, після того, як особи, що навчаються передають свої персональні дані до приймальної комісії в рамках освітньої організації, вони отримують посвідчення своєї особистості - ключ. Використовуючи біометричну ідентифікацію, наприклад, на смартфоні в поєднанні з цим ключем, особи, які навчаються зможуть ідентифікувати себе з будь-якою іншою частиною організації, яка повинна була ідентифікувати їх, наприклад, бібліотеку, факультет, їдальню, студентські гуртожитки, студентські спільноти і т.ін. Кожний з цих підрозділів зможуть ідентифікувати того, хто навчається без необхідності запитувати або зберігати будь-які особисті дані.

Перевагами даного підходу, є те, що при використанні блокчейн в процесі ідентифікації, тільки особи, відповідальні за перевірку особистості студента, матимуть доступ до даних. Крім цього, єдиною людиною, яка володіє даними, є сам студент. Це означає, що організації більше не потрібно управляти складними системами для прав доступу і потрібно тільки захищати пристрій або мережу, де відбувається верифікація. Це дозволить заощадити значні ресурси, що витрачаються на посилення мережі, на боротьбу з порушеннями даних, навчання персоналу щодо захисту даних і управління правами доступу. Крім того, особи, які взаємодіють зі студентами в організації, не повинні брати на себе відповідальність за конфіденційність даних, оскільки їм не потрібно буде знати їх.

1.4 Висновки до розділу 1

Кілька компаній в даний час запускають суверенні рішення для самостійної ідентифікації, які можуть бути застосовані до запропонованих сценаріїв. Зараз для цього будуть потрібні освітні та наукові організації, для проведення значної технічної роботи, для прив'язки цих систем до їх студентських інформаційних систем.

В даний час застосування блокчейн технологій в освітніх організаціях знаходяться на експериментальних етапах. Але вже існують такі університети, які запустили пілотні проекти з впровадження технології блокчейн, прикладом є Массачусетський технологічний інститут та університет Нікосії на Кіпрі [7].

2 ДОСЛІДЖЕННЯ ЗАСОБІВ І МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ ТОКЕНІЗАЦІЇ ОСВІТНІХ АКТИВІВ НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН І СМАРТ-КОНТРАКТІВ ETHEREUM

2.1 Поняття блокчейну

«Блокчейн (Blockchain) - це вічний цифровий розподілений журнал економічних транзакцій, який може бути запрограмований для запису не тільки фінансових операцій, але і практично всього, що має цінність», - Дон і Алекс Тепскотт, «Революція блокчейна» (2016р). [9]

Базова система блокчейна являє собою постійно зростаючою послідовністю блоків, які розділяються між учасниками за допомогою пірінгових мереж. В результаті формується база даних, яка управляється автономно, без єдиного центру. Це робить ланцюжка блоків дуже зручними для реєстрації подій і операцій з даними, управління ідентифікацією та перевірки походження.

У кожен блок додається тимчасова відмітка (хеш-сума). Ці блоки строго в певному порядку складаються в ланцюжки («blockchain» – буквально «ланцюг блоків»). Якщо спробувати переставити послідовність блоків, то система відкине ланцюг через невідповідність структури і хеш-суми. Кожен блок зберігає в собі свій хеш-код підсумований з хеш-кодом попереднього блоку, що вибудовує однозв'язного залежність між блоками в ланцюзі. Схематично це можна представити як на Рисунку 2.1.

Щоб неможливо було змінити тимчасову позначку і перерахувати хеш-суму, яка буде правильною з точки зору системи, блокчейн використовує кілька способів захисту: Proof of Work (PoW, доказ роботи) і Proof of Stake (PoS, доказ володіння).

Якщо говорити простими словами, механізм PoW забезпечує здатність вузла мережі перевірити, що майнер фактично виконав розрахунки. Даний процес включає в себе спробу знайти хеш заголовка блоку, який буде за своїм значенням відповідати цьому рівню складності.

У підході Proof-of-Stake ноди також намагаються хешировать дані в пошуках результату менше певного значення, але складність в даному випадку розподіляється пропорційно і відповідно до балансу даного вузла. Іншими словами - відповідно до кількості токенов на рахунку користувача.

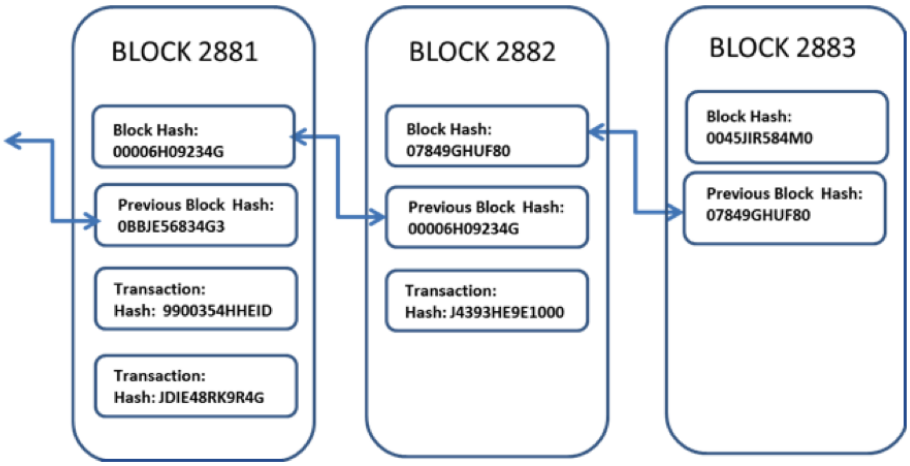

Рисунок 2.1 – Типова структура блокчейн

Узагальнюючи всі факти, не складно зробити висновок що блокчейн дуже надійний і децентралізований одночасно. Всі учасники, які підтримують послугу ланцюжка, рівні між собою. Тут відсутній сервер або будь-який процесинговий центр.

Головним моментом у всій технології є формування і закриття блоків. Як вже говорилося вище, кожна ланка ланцюжка (блок) містить певний ключ. Поки він не буде розшифрований, блок не закриється. За розшифровку в криптовалюта відповідає Майнінг. Майнер, що займаються видобутком криптовалюта, роблять це за допомогою потужностей відеокарт і процесорів. Ті, в свою чергу, виконують обчислювальні операції, головна мета яких – пошук криптографічного підпису до блоку у вигляді хешу. Як тільки вона підібрана – блок закривається, а майнер за це отримує винагороду у вигляді криптовалюта.

Функціонування блокчейна і його безпека забезпечується майнерами і іншими учасниками блокчейна. Їх ще називають нодамі або вузлами. Під повними нодамі маються на увазі майнер і прості користувачі повновагих гаманців. Це означає, що вони на своєму комп'ютері або іншому пристрої мають

повну версію блокчейна. Чим більше в блокчейн активних повних нод – тим швидше обробляється інформація про транзакції.

Підводячи проміжні підсумки, нижче надані ключові особливості Blockchain:

1 Децентралізація – в ланцюжку немає сервера. Кожен учасник – це і є сервер. Він підтримує роботу всього блокчейна;

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

3 Теоретична необмеженість – теоретично блокчейн можна доповнювати записами до нескінченності. Тому його часто порівнюють з суперкомп'ютером;

4 Надійність – для запису нових даних необхідний консенсус вузлів блокчейна. Це дозволяє фільтрувати операції і записувати тільки легітимні транзакції, тому здійснити підміну хеша неможливо.

2.2 Хешування в основі технології

2.2.1 Криптографія в блокчейн

В основі технології блокчейн лежить криптографія– наука про методи забезпечення конфіденційності інформації та збереження її автентичності.

Простими словами, хешування означає введення інформації будь-якої довжини і розміру в заданій стрічці і видачу результату фіксованої довжини заданої алгоритмом функції хешування.

Щоб блокчейн працював, має весь час відбуватися його оновлення – додавання записів про нові транзакціях в мережі. Саме в процесі додавання в систему нової інформації вона стає найбільш вразливою для атак. Але завдяки суворій ієрархії в блокчейне гарантується справжність всіх записів і їх захист від несанкціонованого зміни.

Використання хеш-функції гарантує незмінність вже існуючої ланцюжка транзакцій. Новий блок посилається на хеш попереднього.

Завдяки хеш загальний стан блокчейна (все коли-небудь проведені операції в мережі) можна виразити всього одним числом – хешем нового блоку. За рахунок цього забезпечується незмінність і стабільність роботи.

Криптографічний хеш-функція – це спеціальний клас хеш-функцій, який має різні властивості, необхідні для криптографії.

Очевидно, що алгоритмів шифрування існує безліч і кожна криптовалюта використовує свій алгоритм шифрування. Однак кількість монет значно перевищує кількість алгоритмів криптовалюта, тому деякі криптовалюта використовують один і той же алгоритм хешування даних. [15]

Алгоритм шифрування або алгоритм хешування (алгоритм криптовалюта) – це набір специфічних криптографічних механізмів і правил, які шифрують цифрову валюту.

Сьогодні налічується кілька десятків алгоритмів криптовалюта, однак користуються популярністю лише кілька з них. Серед затребуваних можна назвати наступні: SHA-256, EtHash, Scrypt, X11, CryptoNight, X13. [14]

2.2.2 SHA-256

Абревіатура SHA – це Secure Hash Algorithm, а 256 означає, що алгоритм криптовалюта генерує 256-бітний хеш, тобто рядок (дайджест) розміром 256 біт. На алгоритмі SHA-256 працює Bitcoin, а також ряд інших криптовалюта. Хеш-функції сімейства SHA-2 побудовані на основі структури Меркле - Дамгарда.

Оригінал тексту після доповнення розбивається на блоки, кожен блок – на 16 слів. Алгоритм пропускає кожен блок повідомлення через цикл з 64 ітераціями. На кожній ітерації 2 слова перетворюються, функцію перетворення задають інші слова. Результати обробки кожного блоку складаються, сума є значенням хеш-функції. Так як ініціалізація внутрішнього стану проводиться результатом обробки попереднього блоку, то немає можливості обробляти блоки паралельно. Графічне представлення однієї ітерації обробки блоку даних продемонстровано на Рисунку 2.2.

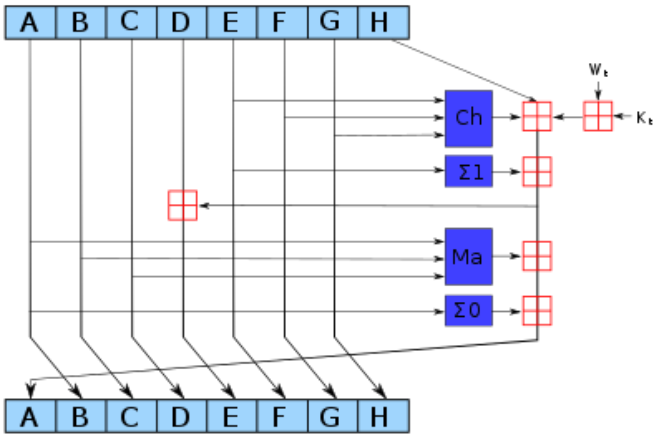

Рисунок 2.2 – Ітерація обробка блоку даних в SHA-256 [12]

Хешрейт для криптовалют, работающих на основе SHA-256, вычисляется в единицах Gigahash в секунду (GH/s). На создание блока уходит от шести до десяти минут.

2.2.3 Ethash

Ethash – це алгоритм криптовалюта, розроблений спеціально для Ethereum. Алгоритм спирається на псевдовипадковий набір даних, ініціалізований поточної довжиною ланцюжка блоків (DAG - файли, які відновлюються кожні 30 000 блоків ~ 5 днів.

Хід виконання алгоритму хешування Ethash можна узагальнити як показано на Рисунку 2.3.

Заголовок, отриманий з останнього блоку і Поточне число в поєднанні з використанням SHA-3-подібного алгоритму, створюють первинні 128 байти міксу. Mix використовується для обчислення того, яка 128-байтовую сторінка з групи DAG витягується.

Mix поєднується з отриманої сторінкою DAG. Це робиться за допомогою функції змішування для генерації наступного міксу. Кроки повторюються 64 рази, в результаті виходить Мікс 64, який піддається постобробці з отриманням більш короткого 32-байтового Mix Digest.

Mix Digest порівнюється з визначеним 32-байтовим цільовим порогом. Якщо Mix Digest менше або дорівнює Target Threshold, то поточний

одноразовий номер вважається успішним і буде транслюватися в мережу Ethereum. Інакше, алгоритм перезапускается з іншим одноразовим номером (або шляхом збільшення поточного одноразового номера, або шляхом вибору нового випадковим чином).

Хейшрейт алгоритму Ethash вимірюється в Megahash в секунду (MH / s).

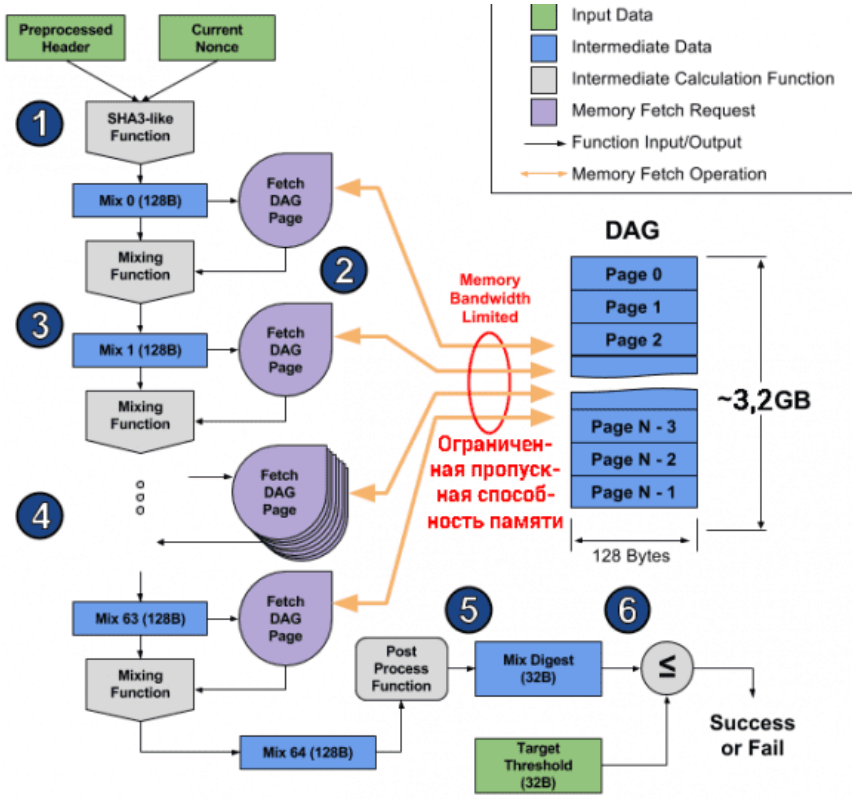

Рисунок 2.3 – Хід виконання алгоритму хешування Ethash [11]

2.3 Ethereum

Ethereum (ефіріум, ефір) – це одночасно і криптовалюта, і функціональна децентралізована середовище, яке по-справжньому революционизировала всю IT-сферу. Ethereum щільно захопив статус другої найпопулярнішою криптовалюта в світі і найбільш революційною. [6]

Якщо дотримуватися догматичної термінології, платформа Ethereum розроблена для створення і функціонування децентралізованих додатків на базі blockchain з використанням smart-контрактів.

Внутрішня валюта платформи – це ether або ефір. Скорочене позначення - ETH. Ефіри застосовуються не тільки в якості розрахункової одиниці. Також вони гарантують виконання розумних контрактів, виконуючи роль такого собі «палива» для мережі.

Хоча Ethereum і порівнюють з Bitcoin, але вони сильно відрізняються за своїм призначенням. Так Ефір став не тільки криптовалюта, але також окремою платформою і мовою програмування. Його можна використовувати для створення нових додатків і їх запуску. [7]

Тут кожна з транзакцій відбувається через дію комп'ютерної програми, яка перевіряє всі умови угоди і якщо зобов'язання між відправником та одержувачем коштів не виконані, то і вона не буде проведена. Таким чином, всі угоди залишаються чесними від початку і до кінця. Обійти або скасувати розумний контракт аж ніяк не можна.

Ефіріум має як сильні, так і слабкі сторони. Серед достоїнств даної платформи можна вказати такі:

1 Мережа Ethereum може служити для передачі інформації і реєстром для її реструктуризації і зберігання.

2 Платіжна система універсальна і дозволяє створювати власні цифрові види валют.

3 Умови договору залишаються незмінними з моменту підписання контракту і до його завершення, якщо самі учасники не включили таку умову в угоду. При цьому всі вимоги прописуються на внутрішньому мовою «Solidity».

4 Тут використовуються безпечні смарт-контракти, угоди укладаються без наявності інших осіб. Система самостійно оцінює статуси кожного з учасників угоди щодо рівня виконання його умов і виробляє транзакцію, коли підтверджені виконання їх зобов'язань.

5 Швидкість проведення транзакцій набагато перевищує систему біткоіни, а комісія за переказ грошей менше.

6 Немає необхідності в посередниках, що дає значну економію в часі і засобах.

7 На рахунку замовника відразу після укладення угоди буде заблокована сума для оплати замовлення, як тільки буде підтверджено його виконання.

8 У операції не можна втрутитися, оскільки вся інформація про неї заноситься в блокчейн.

9 Система підтримує практично будь-яку мову програмування, а простий і доступний її код дозволяє практично необмежено з ним експериментувати.

Існує і головний недолік – система Ethereum не масштабована, а це значить, що транзакція здійсниться тільки після повного виконання всіма учасниками своїх зобов'язань, сам Бутерін вважає даний недолік найістотнішим.

2.4 Протоколи консенсусу

Ключовим аспектом технології блокчейн є визначення того, який користувач публікує наступний блок. Це вирішується шляхом реалізації однієї з багатьох можливих моделей консенсусу. У мережах з невирішеними ланцюжками зазвичай існує багато вузлів публікації, конкуруючих одночасно за публікацію наступного блоку. Вони зазвичай роблять це, щоб виграти плату за криптовалюту і / або транзакцію. Як правило, вони не довіряють користувачам, які можуть знати один одного тільки по їх публічним адресами. Кожен видавничий вузол, швидше за все, мотивований бажанням отримати фінансову вигоду, а не благополуччям інших видавничих вузлів або навіть самої мережі.

У такій ситуації навіщо користувачеві поширювати блок, який інший користувач намагається опублікувати? Крім того, хто вирішує конфлікти, коли кілька вузлів публікують блок приблизно в один і той же час? Щоб зробити це, технології блокчейн використовують консенсусні моделі, щоб дозволити групі взаємно хто не довіряє користувачів працювати разом.

Коли користувач приєднується до мережі блокчейна, він погоджується з початковим станом системи. Це записано в єдиному попередньо сконфігуровані блоці, блоці генезису. Кожна мережа блокчейнов має опублікований блок генезису, і кожен блок повинен бути доданий в блокчейн після нього на основі узгодженої моделі консенсусу. Незалежно від моделі, однак, кожен блок

повинен бути дійсним і, отже, може бути перевірений незалежно кожним користувачем мережі ланцюжка блоків. Комбінуючи початковий стан і можливість перевірки кожного блоку з тих пір, користувачі можуть незалежно узгодити поточний стан ланцюжка блоків. Зверніть увагу, що якщо коли-небудь було дві дійсні ланцюжка, представлені для повного вузла, механізм за замовчуванням в більшості мереж ланцюжка блоків полягає в тому, що «більш довга» ланцюжок розглядається як правильна і буде прийнята; це тому, що в нього було вкладено найбільше роботи. Це часто трапляється з деякими узгодженими моделями і буде обговорюватися детально.

Наступні властивості тоді на місці:

• Початковий стан системи узгоджується (наприклад, блок генезису).

• Користувачі погоджуються з консенсусної моделлю, за допомогою якої блоки додаються в систему.

• Кожен блок пов'язаний з попереднім блоком шляхом включення дайджесту хешу попереднього заголовка блоку (за винятком першого блоку «генезису», який не має попереднього блоку і для якого хеш попереднього заголовка блоку зазвичай встановлюється на всі нулі).

• Користувачі можуть перевірити кожен блок незалежно.

На практиці програмне забезпечення обробляє всі, і користувачам не потрібно знати про ці деталі. Ключовою особливістю технології блокчейн є те, що немає необхідності в тому, щоб довірена третя сторона надавала стан системи - кожен користувач в системі може перевірити цілісність системи.

Щоб додати новий блок в ланцюжок блоків, всі вузли повинні прийти до спільної згоди з часом; проте деякі тимчасові розбіжності дозволені. Для мереж з невирішеною ланцюжком блоків узгоджена модель повинна працювати навіть в присутності, можливо, зловмисних користувачів, оскільки ці користувачі можуть спробувати порушити або захопити ланцюжок блоків. Зверніть увагу, що для дозволених мереж блокчейна можуть бути використані засоби правового захисту, якщо користувач діє зловмисно.

У деяких мережах блокчейн, може існувати певний рівень довіри між вузлами публікації. В цьому випадку може не знадобитися узгоджена модель

ресурсномістких (час обчислень, інвестиції і т.д.), щоб визначити, який учасник додає наступний блок в ланцюжок. Як правило, з ростом рівня довіри зменшується потреба у використанні ресурсів в якості запобіжного генерації довіри. Для деяких дозволених реалізацій ланцюжка блоків уявлення про консенсус виходить за рамки забезпечення достовірності і автентичності блоків, але охоплює всі системи перевірок і перевірок від пропозиції транзакції до її остаточного включення в блок.

У моделі «Доказ роботи» (PoW) користувач публікує наступний блок, першим вирішуючи складну криптографічний завдання. Рішенням цього завдання є «доказ» того, що вони виконали роботу. Завдання розроблена таким чином, що вирішити головоломку складно, але перевірити, що рішення дійсно, легко. Це дозволяє всім іншим повним вузлів легко перевіряти будь-які запропоновані наступні блоки, і будь-який запропонований блок, який не задовольняє завданню, буде відхилений.

Поширеним методом крипто-завдання є вимога, щоб хеш-дайджест заголовка блоку був менше цільового значення. Вузли публікації вносять безліч невеликих змін в заголовок свого блоку (наприклад, змінюючи одноразовий номер), намагаючись знайти хеш-дайджест, який відповідає вимозі. Для кожної спроби вузол публікації повинен обчислювати хеш для всього заголовка блоку. многократне хешування заголовка блоку стає обчислювальним процесом. Цільове значення може бути змінено з часом, щоб відрегулювати складність (вгору або вниз), щоб впливати на частоту публікації блоків.

Наприклад, біткоін, який використовує модель перевірки працездатності, коригує складність головоломки з 2016 року, щоб впливати на частоту публікації блоків приблизно один раз в десять хвилин. Коригування рівня складності завдання, і, по суті, або збільшує, або зменшує кількість необхідних початкових нулів. Збільшуючи число провідних нулів, збільшується складність завдання, тому що будь-яке рішення повинно бути менше, ніж рівень складності - тобто, існує менше можливих рішень. Зменшуючи кількість провідних нулів, знижується рівень складності, тому що є більше можливих рішень. Ця установка призначена для підтримки обчислювальної складності задачі і, отже, для

підтримки основного механізму безпеки мережі біткойнов. Доступна обчислювальна потужність з часом збільшується, так само як і кількість публікованих вузлів, тому складність завдання зазвичай зростає. Коригування до мети складності спрямовані на те, щоб гарантувати, що жоден об'єкт не зможе взяти на себе виробництво блоків, але в результаті обчислення для вирішення завдань вимагають значного споживання ресурсів. У зв'язку зі значним споживанням ресурсів деяких доказів роботи мереж ланцюжка блоків, існує тенденція до додавання вузлів публікації в області, де є надлишок дешевої електроенергії.

Важливим аспектом цієї моделі є те, що робота, закладена в задачу, не впливає на ймовірність вирішення поточних або майбутніх завдань, тому що завдання незалежні. Це означає, що коли користувач отримує заповнений і дійсний блок від іншого користувача, він мотивований відмовитися від своєї поточної роботи і замість цього почати будувати тільки що отриманий блок, тому що вони знають, що інші вузли публікації будуватимуть його.

Модель докази частки володіння (PoS) заснована на ідеї, що чим більше частки користувач вклав в систему, тим більша ймовірність того, що система буде успішною, і тим менш імовірно, що він захоче зруйнувати її. Ставка - це кількість криптовалюта, яку користувач мережі блокчейн вклав в систему (за допомогою різних засобів, таких як блокування через спеціальний тип транзакції, відправка за певною адресою або зберігання в спеціальному програмному забезпеченні гаманця). Одного разу поставлена криптовалюта більше не може бути витрачена. У доказі ставок блокчейн-мережі використовують суму ставки, яку користувач має як визначального фактора для публікації нових блоків. Таким чином, ймовірність того, що користувач мережі з блокчейном публікує новий блок, пов'язана зі ставленням його частки до загальної кількості криптовалюта мережі блокчейн.

При використанні цієї моделі консенсусу немає необхідності виконувати ресурсомісткі обчислення (включаючи час, електроенергію і обчислювальну потужність), як показано в доказі роботи. Оскільки ця консенсусна модель використовує менше ресурсів, деякі мережі блокчейнов вирішили відмовитися

від винагороди за створення блоків; Ці системи спроектовані таким чином, що вся криптовалюта вже розподілена серед користувачів, а не нова криптовалюта генерується в постійному темпі.

У таких системах винагороду за блокову публікацію зазвичай являє собою винагороду за транзакції, що надаються користувачем.

Round Robin - це консенсусна модель, яка використовується деякими дозволеними блокчейн мережами. В рамках цієї моделі консенсусу вузли по черзі створюють блоки. Round Robin Consensus має довгу історію, засновану на архітектурі розподілених систем. Для обробки ситуацій, коли вузол публікації недоступний для публікації блоку в свою чергу, ці системи можуть включати обмеження по часу, що дозволяє доступним вузлам публікувати блоки, щоб недоступні вузли не приводили до зупинки публікації блоку. Ця модель гарантує, що жоден вузол не створить більшість блоків. Він виграє від простого підходу, не має криптографічних завдань і має низькі вимоги до енергоспоживання.

Оскільки існує необхідність в довірі між вузлами, циклічний перебір не працює належним чином в мережах з невирішеними ланцюжками блоків, використовуваних більшістю криптовалюта. Це пов'язано з тим, що шкідливі вузли можуть безперервно додавати додаткові вузли, щоб збільшити свої шанси на публікацію нових блоків. У гіршому випадку вони могли б використовувати це, щоб порушити правильну роботу мережі блокчейна.

Консенсус-модель «Підтвердження достовірності» (також звана «доказом ідентичності») спирається на часткову довіру вузлів публікації через їх відому зв'язок з ідентичностями реального світу. Публікують вузли повинні мати свої посвідчення, доведені і перевіряються в мережі блокчейна (наприклад, ідентифікують документи, які були переєни і завірені нотаріально і включені в блокчейн). Ідея полягає в тому, що видавничий вузол ставить свою ідентичність / репутацію для публікації нових блоків. Користувачі мережі Blockchain безпосередньо впливають на репутацію видавничого вузла, грунтуючись на його поведінці. Вузли публікації можуть втратити репутацію, діючи таким чином, з яким користувачі мережі блокчейнов не згодні, точно так же, як вони можуть

отримати репутацію, діючи таким чином, з яким згодні користувачі мережі блокчейнов. Чим нижче репутація, тим менше ймовірність публікації блоку. Отже, в інтересах видавничого вузла підтримувати високу репутацію. Цей алгоритм застосовується тільки до дозволених мереж ланцюжка блоків з високим рівнем довіри.

В рамках моделі консенсусу докази колишніх часів (PoET) кожен вузол публікації запитує час очікування у безпечного апаратного джерела часу в своїй комп'ютерній системі. Безпечний апаратний джерело часу згенерує випадкове час очікування і поверне його програмному забезпеченню вузла публікації.

Вузли публікації беруть випадкове час, яке їм дають, і протягом цього часу простоюють. Як тільки вузол публікації виходить зі стану очікування, він створює і публікує блок в мережі ланцюжка блоків, сповіщаючи інші вузли про новий блоці; Будь-вузол публікації, який все ще не використовується, перестане чекати, і весь процес почнеться заново.

2.5 Смарт контракти

Смарт-контракти – це по суті програми, які створюються на основі комп'ютерної логіки і передаються у вигляді коду. Саме тому учасники угоди або договору можуть бути впевнені, що всі умови контракту будуть дотримані, і ніхто з учасників не зможе змінити умови або інтерпретувати під себе.

В смарт-контрактах виділяють такі основні об'єкти:

– Підписанти – сторони договору, які взяли обумовлені умови (для цього використовується електронний підпис або мультіподпісь);

– Предмет договору – власне, ресурси для обміну. При цьому вони повинні знаходитися всередині системи, в рамках якої реалізується контракт;

– Умови договору – точніше, математично підтверджене опис умов, при яких договір вважатиметься виконаним;

Очевидно, що головна перевага смарт-контрактів - проведення угод без залучення третіх осіб (в звичайних умовах вони виступають гарантами виконання договору).

Друга перевага смарт-контрактів – безпека і конфіденційність угод. Всі контракти зберігаються в блокчейне в зашифрованому вигляді. Про умови і об'єкт договору знають тільки сторони договору, а внести зміни в програмний код не може ніхто.

Третя перевага – зниження витрат на проведення операції. Якщо умови договору дотримані, користувачі обмінюються активами миттєво. Ніяких додаткових підтверджень чекати не потрібно.

Не можна забувати, що смарт-контракт – це, перш за все, програма. І, як будь-яка програма, він не позбавлений недоліків:

1 Складність самостійного складання смарт-контрактів.

2 Висока залежність від людського фактора (помилки, які були допущені при написанні програмного коду).

3 Недостатня гнучкість (дані в блокчейне не змінні).

4 Погана масштабованість (при одночасному запуску кількох контрактів пропускна здатність системи знижується).

Якщо привести короткий алгоритм роботи, то: клієнт у себе на комп'ютері генерує пару довгих простих чисел – публічний і приватний ключ. Приватний ключ вважається секретним, тому що може розшифрувати те, що зашифровано публічним, також працює і в зворотному порядку.

Якщо публічний ключ є в доступності в іншого користувача блокчейн, то він зможе зашифрувати їм будь-яке повідомлення так, що прочитати його зможе тільки конкретний користувач, так як володіє приватним. Ще одна особливості публічного ключа - за допомогою нього можна перевірити, що дані були зашифровані саме приватним ключем клієнта, що не розшифровуючи при цьому самі дані.

Цим досягається відкритість і безпеку мережі. Якщо раніше за це відповідали банки, то в блокчейне за це відповідає математика. Весь процес описаний вище можна представити у вигляді такої схеми, представленої на Рисунку 2.4, на прикладі деякої ситуації переказу грошей.

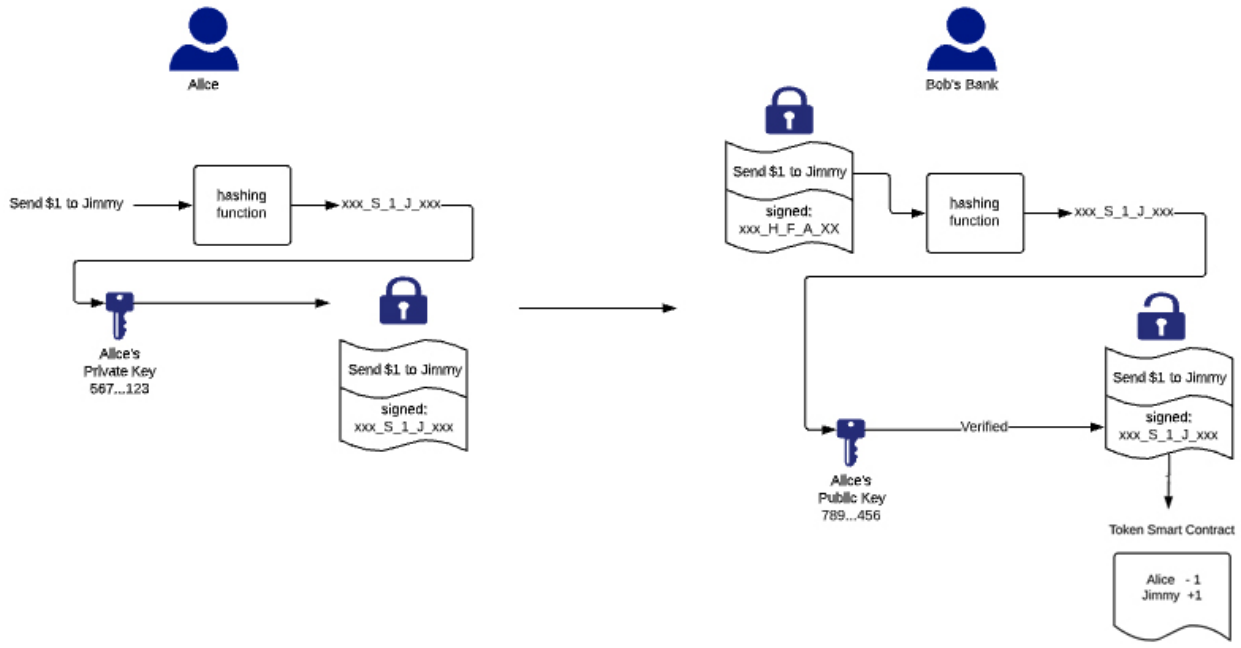

Рисунок 2.4 – Стандартна транзакція в середовищі Ethereum [14]

2.6 Висновки до розділу 2

У другому розділі розглянуто основні поняття блокчен. Проведено аналіз існуючих методів хешування, які використовуються в технології блокчейн. Наведено порівняння основних криптографічних функцій: SHA256, Ethash та їх використання для створення цифрових токенів. Розглянуто платформу Ethereum та смарт-контракти, що можуть створюватися на цій платформі.

Проведний аналіз дозволяє зробити висновок, що технологія блокчейн є достатньо захищеною для створенння та зберігання освітніх активів за допомогою цифрових токенів.

.

3 ПРАКТИЧНА ЧАСТИНА. РОЗРОБКА ПРОГРАМНОЇ РЕАЛІЗАЦІЇ ДЕЦЕНТРАЛІЗОВАНОГО РЕЄСТРУ ДЛЯ ТОКЕНІЗАЦІЇ ОСВІТНІХ АКТИВІВ

3.1 Вибір програмних засобів для реалізації блокчейн для токенізації освітніх активів

У просторі блокчейн повно людей і підприємств, що прагнуть втілити в життя нові ідеї. Визначення того, яка мова використовувати в процесі розробки, необхідно для знаходження найкращого способу створення цифрових токенів.

Розглянемо список деяких з найбільш популярних мов програмування для розробки блокчейн.

C++ є потужною мовою програмування та був вихідним мовою, на якому був побудований біткойн. Він об'єктно-орієнтований, що дозволяє йому методично пов'язувати фрагменти даних і робить його придатним мовою для створення блокчейнов. C ++ допомагає розробникам керувати ресурсами, краще контролювати пам'ять і швидко обробляти взаємодії. Один із способів побачити це - безліч з'єднань між користувачами і Майнером, перевірка транзакцій і будівельні блоки.

Python був створений, щоб бути простим, легким у використанні. Таким чином, він став однією з кращих мов програмування в світі. Простота Python дозволяє розробникам швидко створювати і тестувати нові ідеї, а його підтримка з відкритим вихідним кодом включає в себе безліч інструментів, які можуть допомогти розробникам вирішувати проблеми при їх виникненні.

Solidity був побудований для написання розумних контрактів на основі Ефіріума. Спочатку він був розроблений командою Ethereum, дозволяючи розробникам писати високорівневий, розумний контрактно-орієнтований код, який потім можна було б перекласти і використовувати на мовах програмування нижчого рівня. Solidity покликаний підвищити зручність використання і технології, що лежать в основі блокчейн, і, хоча він є новим, він продовжує рости в популярності серед спільноти розробників.

Java є надзвичайно популярною мовою кодування в співтоваристві блокчейн, завдяки своєму об'єктно-орієнтованому підходу, який також зустрічається в C ++. Його головна привабливість для розробників блокчейн - його мобільність. Завдяки віртуальній машині Java, Java не обмежена архітектурою пристрою і відома своєю здатністю одночасно обробляти велику кількість користувачів в мережі блокчейна.

Інша мова, популярність якого зростає в просторі блокчейн, - це Go. Go, розроблений в 2007 році, є мовою програмування, створеним розробниками Google. У світі блокчейна він використовується головним чином для створення децентралізованих систем. Він відомий своєю простотою використання і масштабованість, допомагаючи вирішувати проблеми завдяки своїй простоті.

3.2 Програмна реалізація цифрових токенів

Для створення блокчейн необхідно попередньо виконати налаштування середовища розробки та додаткового програмного забезпечення. На самому початку встановлюється Python 3.6, Flask і бібліотеки Requests (рис.3.1). Крім цього необхідно встановити HTTP-клієнт, наприклад Postman.

```
Shell
1  pip install Flask==0.12.2 requests==2.18.4
```

Рисунок 3.1 - Установка і настройка середовища розробки

На самому початку клас для реалізації блокчейн, який містить початковий порожній лист для зберігання блокчейн і для зберігання транзакцій (рис.2.2).

Даний клас забезпечує роботу з блокчейном, відповідає за зберігання транзакцій і містить методи для внесення нових блоків в ланцюжок блоків.

```python
class Blockchain(object):
    def __init__(self):
        self.chain = []
        self.current_transactions = []

    def new_block(self):
        # Создает новый блок и вносит его в цепь
        pass

    def new_transaction(self):
        # Вносит новую транзакцию в список транзакций
        pass

    @staticmethod
    def hash(block):
        # Хеширует блок
        pass

    @property
    def last_block(self):
        # Возвращает последний блок в цепочке
        pass
```

Рисунок 3.2 - Шаблон класу для реалізації блокчейна

Розглянемо докладніше програмний код і його реалізацію. Відповідно до опису блокчейн в кожному блоці необхідно зберігати такі дані: індекс блоку, тимчасову мітку (час Unix), список транзакцій, доказ консенсусу і хеш попереднього блоку (рис.3.3).

```python
block = {
    'index': 1,
    'timestamp': 1506057125.900785,
    'transactions': [
        {
            'sender': "8527147fe1f5426f9dd545de4b27ee00",
            'recipient': "a77f5cdfa2934df3954a5c7c7da5df1f",
            'amount': 5,
        }
    ],
    'proof': 324984774000,
    'previous_hash': "2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e730433
}
```

Рисунок 3.3 - Опис блоку блокчейна

Метод new_transaction (рис.3.4) відповідає за внесення нових транзакцій в блок. Метод заносить транзакцію в список і повертає індекс блоку в який буде заноситися транзакція.

```python
class Blockchain(object):
    ...

    def new_transaction(self, sender, recipient, amount):
        """
        Направляет новую транзакцию в следующий блок

        :param sender: <str> Адрес отправителя
        :param recipient: <str> Адрес получателя
        :param amount: <int> Сумма
        :return: <int> Индекс блока, который будет хранить эту транзакцию
        """

        self.current_transactions.append({
            'sender': sender,
            'recipient': recipient,
            'amount': amount,
        })

        return self.last_block['index'] + 1
```

Рисунок 3.4 - Метод new_transaction ()

```python
import hashlib
import json
from time import time


class Blockchain(object):
    def __init__(self):
        self.current_transactions = []
        self.chain = []

        # Создание блока генезиса
        self.new_block(previous_hash=1, proof=100)

    def new_block(self, proof, previous_hash=None):
        """
        Создание нового блока в блокчейне

        :param proof: <int> Доказательства проведенной работы
        :param previous_hash: (Опционально) хеш предыдущего блока
        :return: <dict> Новый блок
        """

        block = {
            'index': len(self.chain) + 1,
            'timestamp': time(),
            'transactions': self.current_transactions,
            'proof': proof,
            'previous_hash': previous_hash or self.hash(self.chain[-1]),
        }
```

Рисунок 3.5 - Метод для створення нового блоку new_block ()

Для створення першого блоку генезису - першого блоку без попередника використовується фрагмент коду:

Створення блоку генезису

self.new_block (previous_hash = 1, proof = 100)

Також в блоці має бути доказ консенсусу, яке представляє результат Майнінгу (рис.3.5).

Метод def proof_of_work (self, last_proof) - реалізує алгоритм докази роботи (рис.3.6), який схожий на алгоритм Hashcash в біткоін. Даний алгоритм шукає таке число p, яке при хешування з попереднім хешем блоку містить 4 заголовних нуля.

```python
import hashlib
import json

from time import time
from uuid import uuid4


class Blockchain(object):
    ...

    def proof_of_work(self, last_proof):
        """
        Простая проверка алгоритма:
         - Поиска числа p`, так как hash(pp`) содержит 4 заглавных нуля, где
         - p является предыдущим доказательством, а p` - новым

        :param last_proof: <int>
        :return: <int>
        """

        proof = 0
        while self.valid_proof(last_proof, proof) is False:
            proof += 1

        return proof

```

Рисунок 3.6 - Метод proof_of_work

Для організації роботи блокчейн використовуємо фреймворк Flask, який дозволяє зіставити кінцеві вузли мережі з функціями блокчейн. Взаємодія з блокчейн виконується за допомогою HTTP-запитів. Для цього необхідно створити три додаткові методи:

- / transactions / new для створення нової транзакції в блоці;

- / mine, дає завдання сервера на початок Майнінгу нового блоку;

- / chain для повернення всього блокчейн

Розглянемо шаблонний код для сервера вузла мережі блокчейн (рис.2.7).

```
from flask import Flask


class Blockchain(object):
    ...


# Создаем экземпляр узла
app = Flask(__name__)

# Генерируем уникальный на глобальном уровне адрес для этого узла
node_identifier = str(uuid4()).replace('-', '')

# Создаем экземпляр блокчейна
blockchain = Blockchain()


@app.route('/mine', methods=['GET'])
def mine():
    return "We'll mine a new Block"

@app.route('/transactions/new', methods=['POST'])
def new_transaction():
    return "We'll add a new transaction"

@app.route('/chain', methods=['GET'])
def full_chain():
    response = {
        'chain': blockchain.chain,
        'length': len(blockchain.chain),
    }
    return jsonify(response), 200

if __name__ == '__main__':
    app.run(host='0.0.0.0', port=5000)
```

Рисунок 3.7 - Шаблон коду для вузла мережі блокчейн

Також необхідно розробити функцію, яка відповідає за внесення транзакцій на вузлі мережі блокчейн (рис.3.8).

```python
import hashlib
import json
from textwrap import dedent
from time import time
from uuid import uuid4

from flask import Flask, jsonify, request

...

@app.route('/transactions/new', methods=['POST'])
def new_transaction():
    values = request.get_json()

    # Убедитесь в том, что необходимые поля находятся среди POST-данных
    required = ['sender', 'recipient', 'amount']
    if not all(k in values for k in required):
        return 'Missing values', 400

    # Создание новой транзакции
    index = blockchain.new_transaction(values['sender'], values['recipient']

    response = {'message': f'Transaction will be added to Block {index}'}
    return jsonify(response), 201
```

Рисунок 3.8 - Функція внесення нових транзакцій на вузли мережі

Також на вузлі необхідно виконувати Майнінг нового блоку. Для цього необхідно вирішити задачу для алгоритму доказу роботи (PoW), видати нагороду Майнеру за рішення крипто-завдання (1 коін) і створити новий блок з занесенням його ланцюжок блоків. Програмний код для вирішення цих завдань представлений на рисунку 3.9.

```python
@app.route('/mine', methods=['GET'])
def mine():
    # Мы запускаем алгоритм подтверждения работы, чтобы получить следующее
    last_block = blockchain.last_block
    last_proof = last_block['proof']
    proof = blockchain.proof_of_work(last_proof)

    # Мы должны получить вознаграждение за найденное подтверждение
    # Отправитель "0" означает, что узел заработал крипто-монету
    blockchain.new_transaction(
        sender="0",
        recipient=node_identifier,
        amount=1,
    )

    # Создаем новый блок, путем внесения его в цепь
    previous_hash = blockchain.hash(last_block)
    block = blockchain.new_block(proof, previous_hash)

    response = {
        'message': "New Block Forged",
        'index': block['index'],
        'transactions': block['transactions'],
        'proof': block['proof'],
        'previous_hash': block['previous_hash'],
    }
    return jsonify(response), 200
```

Рисунок 3.9 -Програмний код для реалізації Майнінгу на вузлі мережі

3.3 Висновки до розділу 3

В розділі розглянуто основні засоби розробки програмного забезпечення для блокчейн. В якості мови програмування обрано Python. Розглянуто основні функції для створення блокчейн реєстру: функція створення вузла мережі блокчейн, функція майнінгу блоків, функція перевірки консенсусу, функція запису транзакції до блоку та функція запису блоку до блокчейн реєстру. Наведено програмний код на мові програмування Python, що реалізує запропоновані функції.

4 ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ БЛОКЧЕЙНІВ

4.1 Взаємодія з розробленим блокчейн

Для взаємодії з блокчейном можна використовувати клієнт HTTP-запитів cURL або Postman. Для початку необхідно запустити сервер вузла мережі блокчейн (рис.4.1)

```
Shell
1  $ python blockchain.py
2  * Running on http://127.0.0.1:5000/ (Press CTRL+C to quit)
```

Рисунок 4.1 - Запуск сервера вузла мережі блокчейн

Для запуску процес Майнінгу блоку необхідно відправити GET-запит серверу вузла (рисунок 4.2).

```
Python
1  curl http://localhost:5000/mine
```

Рисунок 4.2 - Запит на Майнінг блоку

Результат виконання запиту на Майнінг блоку представлений на рисунку 4.3.

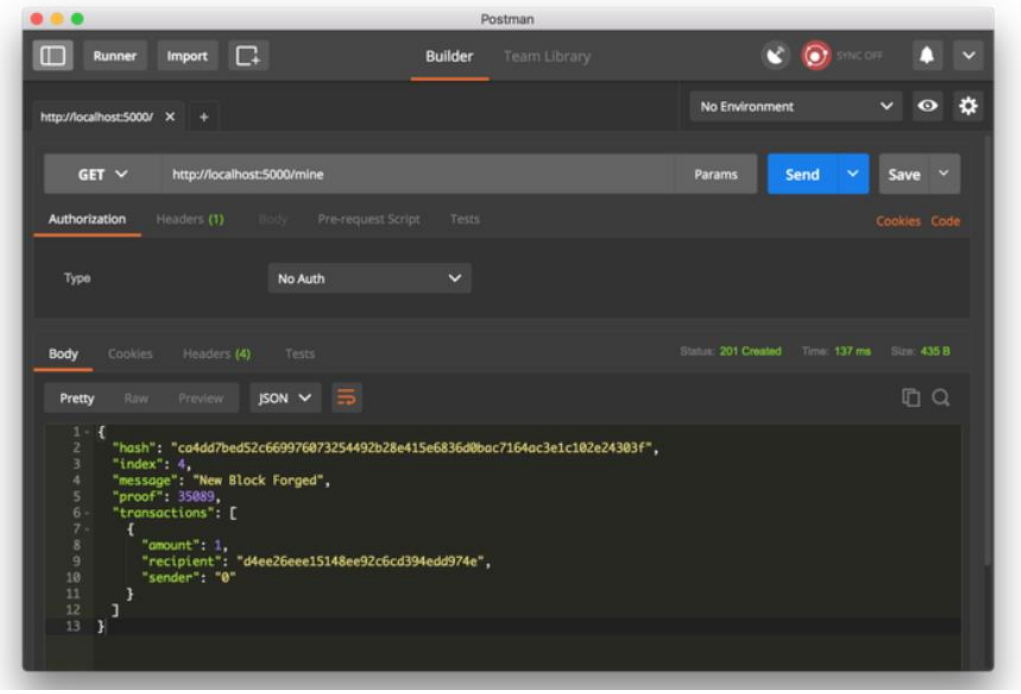

Рисунок 4.3 - Результат виконання запиту Майнінг

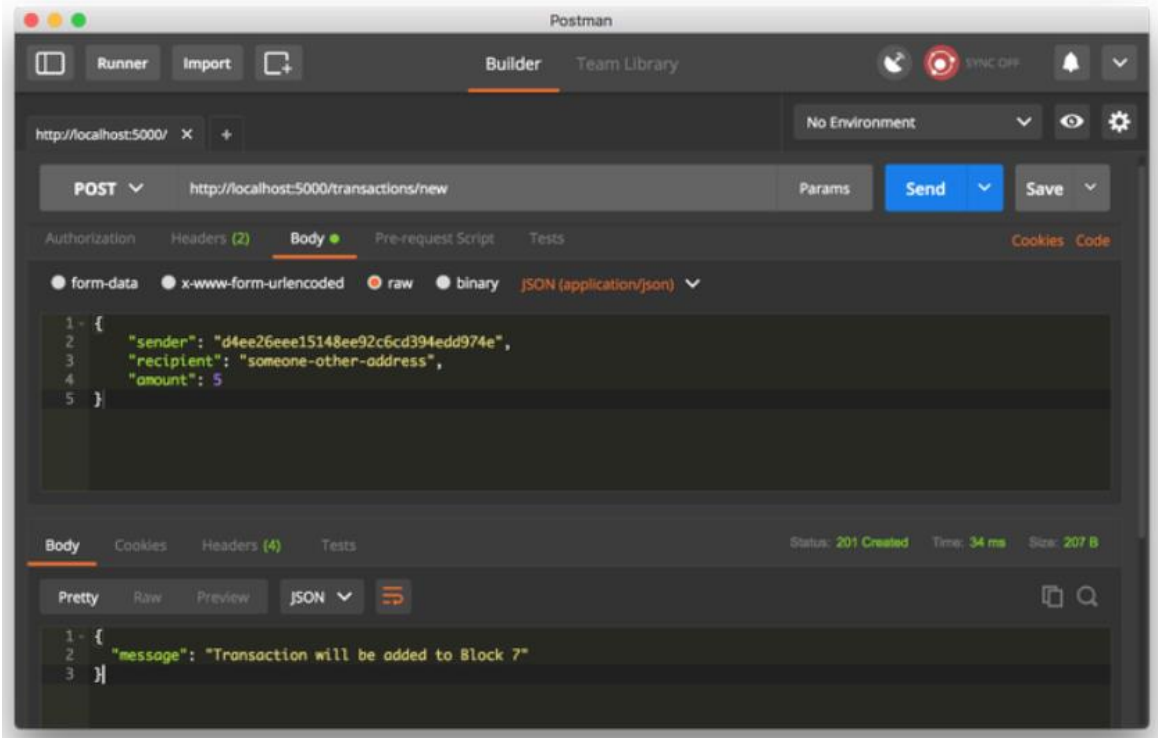

Рисунок 4.4 - Запит на виконання транзакції

Для створення нової транзакції необхідно відправити POST-запит до вузла мережі з тілом, яке містить параметри транзакції (рис.4.4).

4.2 Реалізація транзакцій в розробленому блокчейн

Для реалізації децентралізованої мережі вузлів необхідно реалізувати програмний код для реєстрації нових вузлів мережі і реалізації алгоритмів консенсусу. Програмний код для реалізації даних кінцевих точок представлений на малюнках (4.5 - 4.7).

```python
...
from urllib.parse import urlparse
...


class Blockchain(object):
    def __init__(self):
        ...
        self.nodes = set()
        ...

    def register_node(self, address):
        """
        Вносим новый узел в список узлов

        :param address: <str> адрес узла , другими словами: 'http://192.168.
        :return: None
        """

        parsed_url = urlparse(address)
        self.nodes.add(parsed_url.netloc)
```

Рисунок 4.5 - Реалізація кінцевої точки для реєстрації нових вузлів мережі блокчейн

Згідно алгоритму консенсусу PoW валидной ланцюжком є найдовший ланцюжок. Цей ланцюжок є авторитетним на даному вузол. Метод resolve_conflicts вирішує конфлікти і замінює ланцюг на найдовшу ланцюжок (рис.4.6).

```python
def resolve_conflicts(self):
    """
    Это наш алгоритм Консенсуса, он разрешает конфликты,
    заменяя нашу цепь на самую длинную в цепи

    :return: <bool> True, если бы наша цепь была заменена, False, если н
    """

    neighbours = self.nodes
    new_chain = None

    # Ищем только цепи, длиннее нашей
    max_length = len(self.chain)

    # Захватываем и проверяем все цепи из всех узлов сети
    for node in neighbours:
        response = requests.get(f'http://{node}/chain')

        if response.status_code == 200:
            length = response.json()['length']
            chain = response.json()['chain']

            # Проверяем, является ли длина самой длинной, а цепь - валид
            if length > max_length and self.valid_chain(chain):
                max_length = length
                new_chain = chain

    # Заменяем нашу цепь, если найдем другую валидную и более длинную
    if new_chain:
        self.chain = new_chain
        return True

    return False
```

Рисунок 4.6 - Метод resolve_conflicts

Далі реєструються кінцеві точки для API для додавання нових вузлів і вирішення конфліктів (рис.4.7).

```python
@app.route('/nodes/register', methods=['POST'])
def register_nodes():
    values = request.get_json()

    nodes = values.get('nodes')
    if nodes is None:
        return "Error: Please supply a valid list of nodes", 400

    for node in nodes:
        blockchain.register_node(node)

    response = {
        'message': 'New nodes have been added',
        'total_nodes': list(blockchain.nodes),
    }
    return jsonify(response), 201


@app.route('/nodes/resolve', methods=['GET'])
def consensus():
    replaced = blockchain.resolve_conflicts()

    if replaced:
        response = {
            'message': 'Our chain was replaced',
            'new_chain': blockchain.chain
        }
    else:
        response = {
            'message': 'Our chain is authoritative',
            'chain': blockchain.chain
        }

    return jsonify(response), 200
```

Рисунок 4.7 - Кінцеві струми для API

Для проведення транзакцій і перевірки роботи алгоритмів консенсусу необхідно запустити два нових вузла на комп'ютерах мережі і виконати їх реєстрацію (рис. 4.8).

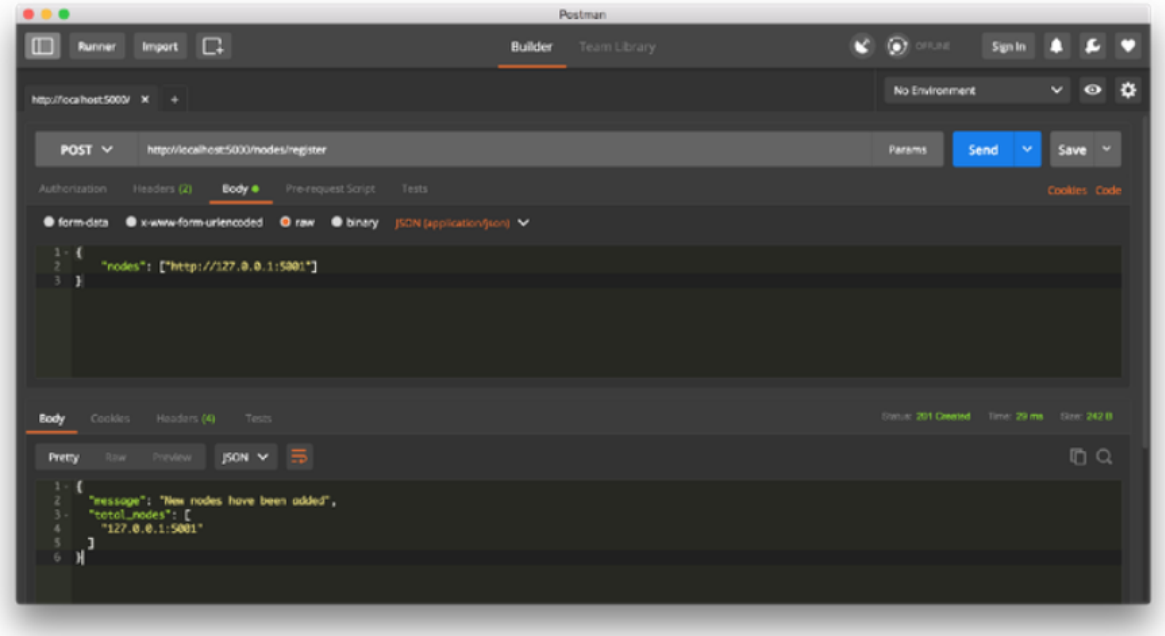

Рисунок 4.8 - Реєстрація нового вузла мережі

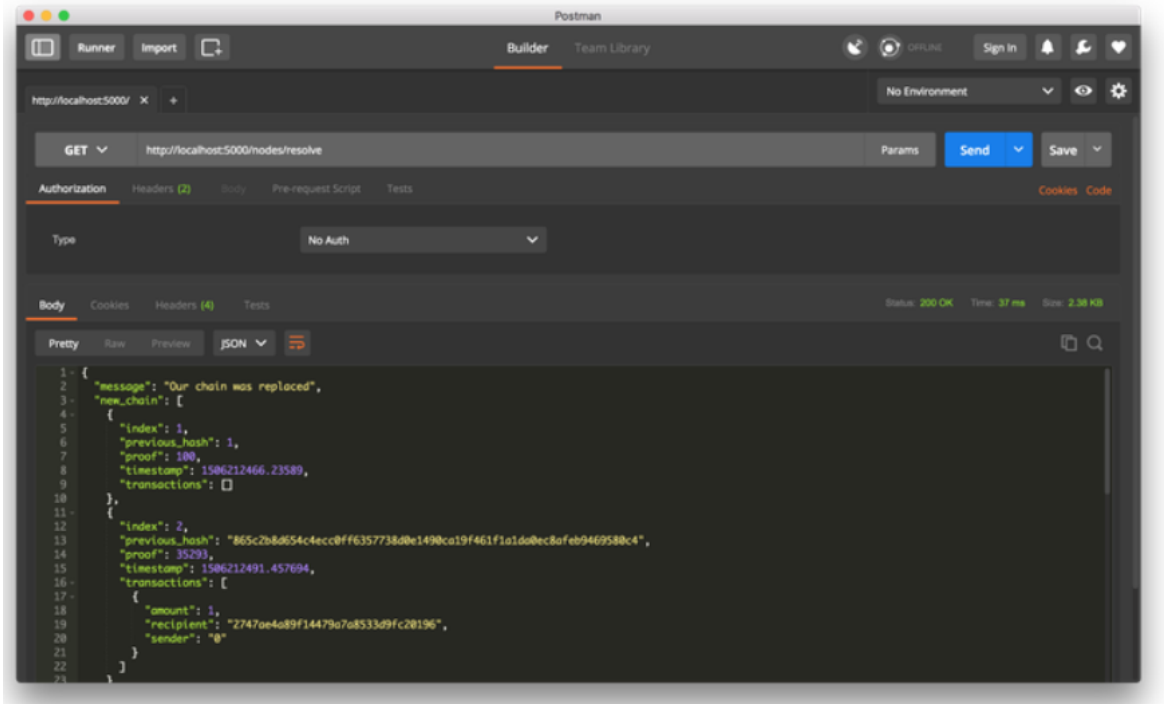

Рисунок 4.9 - Виконання транзакції і перевірка алгоритму консенсусу

4.3 Висновки до розділу 4

У роботі представлено блокчейн, як нова форма механізму збереження даних про цифрові дипломи здобувачів вищої освіти на основі децентралізованого реєстру. Наведено приклад програмної реалізації цифрових токенів на основі технології блокчейн на мові програмування Python.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

5.1 Охорона праці

Сьогодні, напевно, важко уявити компанію, господарська діяльність в якій здійснювалась би без використання комп'ютерної техніки. Через масовий характер робіт, що виконуються працівниками за допомогою комп'ютера, законодавством України чітко врегульовано норми та вимоги до використання комп'ютерної техніки на підприємстві, безпосередньо й охорона праці при роботі з комп'ютером.

Охорона праці всіх підрозділів підприємства, де виконують роботи з персональним комп'ютером супроводжується інструкцією з охорони праці, яка повинна бути розроблена відповідно до:

– положення про розробку інструкцій з охорони праці, затвердженого наказом Держнаглядохоронпраці від 29.01.1998 № 9;

– типового положення про порядок проведення навчання і перевірки знань з питань охорони праці, затвердженого наказом Держнаглядохоронпраці від 26.01.2005 № 15;

– Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями, затверджені наказом Мінсоцполітики від 14.02.2018 р. №207;

– Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПіН 3.3.2.007-98, затверджених постановою Головного державного санітарного лікаря України від 10.12.1998 № 7;

– Загальних вимог стосовно забезпечення роботодавцями охорони праці працівників, затверджених наказом Міністерства надзвичайних ситуацій України від 25.01.2012 № 67 (НПАОП 0.00-7.11-12).

Розглянемо детальніше види інструктажів з охорони праці.

Інструктажі з охорони праці на підприємстві, в організаціях

За характером і часом проведення інструктажі з питань охорони праці поділяються на вступний, первинний, повторний, позаплановий та цільовий.

Вступний інструктаж проводиться:

– з усіма працівниками, яких приймають на постійну або тимчасову роботу, незалежно від освіти, стажу роботи та посади;

– з працівниками інших організацій, які прибули на підприємство і беруть безпосередню участь у виробничому процесі або виконують інші роботи для підприємства;

– з учнями та студентами, які прибули на підприємство для проходження виробничої практики;

– у разі екскурсії на підприємство;

– з усіма вихованцями, учнями, студентами та іншими особами, які навчаються в середніх, позашкільних, професійно-технічних, вищих закладах освіти при оформленні або зарахуванні до закладу освіти.

Первинний інструктаж проводиться до початку роботи безпосередньо на робочому місці з працівником:

– новоприйнятим (постійно чи тимчасово) на підприємство;

– який переводиться з одного цеху виробництва до іншого;

– який буде виконувати нову для нього роботу;

– з відрядженим працівником, який бере безпосередню участь у виробничому процесі на підприємстві.

Проводиться з вихованцями, учнями та студентами середніх, позашкільних, професійно-технічних, вищих закладів освіти:

– на початку занять у кожному кабінеті, лабораторії, де навчальний процес пов'язаний з небезпечними або шкідливими хімічними, фізичними, біологічними факторами, у гуртках, перед уроками трудового навчання, фізкультури, перед спортивними змаганнями, вправами на спортивних снарядах, при проведенні заходів за межами території закладів освіти;

– перед виконанням кожного навчального завдання, пов'язаного з використанням різних механізмів, інструментів, матеріалів;

– на початку вивчення кожного нового предмета (розділу, теми) навчального плану (програми) – із загальних вимог безпеки, пов'язаних з тематикою і особливостями проведення цих занять.

Повторний інструктаж проводиться з працівниками на робочому місці б терміни, визначені відповідними чинними галузевими нормативними актами або керівником підприємства з урахуванням конкретних умов праці, але не рідше:

– на роботах з підвищеною небезпекою – 1 раз на три місяці;

– для решти робіт – 1 раз на шість місяців.

Позаплановий інструктаж проводиться:

– при введенні в дію нових або переглянутих нормативних актів про охорону праці, а також при внесенні змін та доповнень до них;

– при зміні технологічного процесу, заміні або модернізації устаткування, приладів та інструментів, вихідної сировини, матеріалів та інших факторів, що впливають на стан охорони праці;

– при порушеннях працівниками вимог нормативних актів про охорону праці, що можуть призвести або призвели до травм, аварій, пожеж;

– при виявленні особами, які здійснюють державний нагляд і контроль за охороною праці, незнання вимог безпеки стосовно робіт, що виконуються працівником.

Всі вище наведені інструктажі проводяться згідно з документом «Типове положення про порядок проведення навчання та перевірки знань з питань охорони праці, від 26.01.2015 р., №15 (Зм. Від 16.11.2011 р.,№273)»

5.2 Безпека в надзвичайних ситуаціях

Приміщення для роботи з ВДТ повинні мати природне та штучне освітлення відповідно до ДБН В.2.5-28-2018.

Природне освітлення має здійснюватись через світлові прорізи, орієнтовані переважно на північ чи північний схід і забезпечувати коефіцієнт природною освітленості (КПО) не нижче ніж 1,5%. Розраховується КПО за методикою, викладеною в ДБН В.2.5-28-2006.

За виробничої потреби дозволяється експлуатувати ЕОМ у приміщеннях без природного освітлення за узгодженням з органами державного нагляду за охороною праці та органами і установами санітарно-епідеміологічної служби.

Вікна приміщень з ВДТ повинні мати регулювальні пристрої для відкривання, а також жалюзі, штори, зовнішні козирки тощо.

Штучне освітлення приміщення з робочими місцями, обладнаними ВДТ ЕОМ загального та персонального користування, має бути обладнане системою загального рівномірного освітлення. У виробничих та адміністративно-громадських приміщеннях, де переважають роботи з документами, допускається вживати систему комбінованого освітлення (додатково до загального освітлення встановлюються світильники місцевого освітлення).

Загальне освітлення має бути виконане у вигляді суцільних або переривчатих ліній світильників, що розміщуються збоку від робочих місць (переважно зліва) паралельно лінії зору працівників. Допускається застосовувати світильники таких класів світлорозподілу:

– світильники прямого світла – П;

– переважно прямого світла – Н;

– переважно відбитого світла – В.

При розташуванні відеотерміналів ЕОМ за периметром приміщення лінії світильників штучного освітлення повинні розміщуватися локально над робочими місцями.

Для загального освітлення необхідно застосовувати світильники із розсіювачами та дзеркальними екранними сітками або віддзеркалювачами, укомплектовані високочастотними пускорегулювальними аппаратами. Застосування світильників без розсіювачів та екранних сіток забороняється.

Як джерело світла при штучному освітленні повинні застосовуватися, як правило, люмінесцентні лампи типу ЛБ. При обладнанні відбивного освітлення у виробничих та адміністративно-громадських приміщеннях можуть застосовуватися металогалогенні лампи потужністю до 250 Вт. Допускається у світильниках місцевого освітлення застосовувати лампи розжарювання.

Яскравість світильників загального освітлення в зоні кутів випромінювання від 50º до 90º відносно вертикалі в подовжній і поперечній площинах повинна складати не більше 200 кд/м2, а захисний кут світильників повинен бути не більшим за 40º.

Коефіцієнт запасу (Кз) відповідно до ДБН В.2.5-28-2006 для освітлювальної установки загального освітлення слід приймати рівним 1,4.

Коефіцієнт пульсації повинен не перевищувати 5 % і забезпечуватися застосуванням газорозрядних ламп у світильниках загального і місцевого освітлення.

За відсутності світильників без розсіювачів та екранних сіток лампи багатолампових світильників або розташовані поруч світильники загального освітлення необхідно підключати до різних фаз трифазної мережі.

Рівень освітленості на робочому столі в зоні розташування документів має бути в межах 300…500 лк. У разі неможливості забезпечити даний рівень освітленості системою загального освітлення допускається застосування світильників місцевого освітлення, але при цьому не повинно бути відблисків на поверхні екрану та збільшення освітленості екрану більше ніж до 300 лк.

Світильники місцевого освітлення повинні мати напівпрозорий відбивач світла з захисним кутом не меншим за 40º.

Необхідно передбачити обмеження прямої блискості від джерела природного та штучного освітлення, при цьому яскравість поверхонь, що світяться (вікна, джерела штучного світла) і перебувають у полі зору, повинна бути не більшою за 200 кд/м2.

Необхідно обмежувати відбиту блискість шляхом правильного вибору типів світильників та розміщенням робочих місць відносно джерел природного та штучного освітлення. При цьому яскравість відблисків на екрані відеотерміналу не повинна перевищувати 40 кд/м2, яскравість стелі при застосуванні системи відбивного освітлення не повинна перевищувати 200 кд/м2.

Необхідно обмежувати нерівномірність розподілу яскравості в полі зору осіб, що працюють з відеотерміналом, при цьому відношення значень яскравості

робочих поверхонь не повинно перевищувати 3:1, а робочих поверхонь і навколишніх предметів (стіни, обладнання) – 5:1.

Необхідно використовувати систему вимикачів, що дозволяє регулювати інтенсивність штучного освітлення залежно від інтенсивності природного, а також дозволяє освітлювати тільки потрібні для роботи зони приміщення.

Для забезпечення нормованих значень освітлення в приміщеннях з відеотерміналами ЕОМ загального та персонального користування необхідно очищати віконне скло та світильники не рідше ніж 2 рази на рік, та своєчасно проводити заміну ламп, що перегоріли.

ВИСНОВКИ

Ентузіасти впровадження цифрових технологій в освіту вже багато раз переживали піки надій і спади розчарувань. Нині вони перебувають на черговій хвилю оптимізму. І цей оптимізм пов'язаний не з технологіями завтрашнього дня, а з тим, що стало загальнодоступним сьогодні. Дешеві мікропроцесорні набори, компоненти для аматорського конструювання різних програмованих пристроїв, включаючи роботів, приклади, на які мало звертають увагу освітні політики. Але фундаментальна зміна пов'язано з формуванням цифрового освітнього середовища сучасного освітнього закладу, де всі освітні заходи розглядаються як складові частини єдиного освітнього процесу, а освітні результати - як очікувані результати цих заходів (навчальних, навчально-виробничих, виробничих). Поява у кожного учасника освітнього процесу особистого цифрового пристрою (Ноутбука, планшета або смартфона) дозволяє працювати в цифровому освітньому середовищі через інтернет.

Сучасний розвиток цифрової економіки призвело до практичної реалізації цифрової трансформації всіх аспектів людської діяльності, включаючи як виробничу, так і соціальну сферу.

В даний час технології розвиваються дуже швидко і постійно збільшується обсяг одержуваної, переданої і збереженої інформації. У зв'язку з чим, затребуваною стає технологія Big Data, яка дозволяє працювати з великими обсягами даних, внаслідок чого, популярності набуває нова технологія blokchain.

Відповідно до існуючої категоризації можна виділити три умовні області застосування зазначеної технології: блокчейн 1.0 - це валюта; блокчейн 2.0 - це контракти; блокчейн 3.0 - додатки, область яких виходить за рамки фінансових транзакцій і ринків. До останньої категорії і відноситься блокчейн в освіті.

У роботі описаний існуючий процес видачі дипломів і, альтернативний, запропонований в роботі, сучасний підхід із застосуванням цифрових токенів на основі технології блокчейн. Представлена модель роботи блокчейн-технології в освіті і механізм її застосування.

Пропонуються кілька напрямків розвитку освіти на основі технології блокчейн такі, як: підтвердження достовірності документів про освіту, особова картка студента, підтвердження акредитації освітньої організації, інтелектуальна власність, ідентифікація студентів.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Fenn J., Raskino M., Mastering the HypeCycle, Harvard Business Press, 2008, 339 p.
2. Grech A., Camilleri A.F., Blockchain in education, ed. A. Inamorato dos Santos, 2017, [Электронный ресурс]. URL: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education(1).pdf (Дата обращения 05.11.2020).
3. Greenspan G., Avoiding the pointless blockchain project, 2015, [Электронный ресурс]. URL: https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/ (Дата обращения 05.11.2020).
4. Hicken A., 2018 eLearning Predictions Updated Hype Curve, Web Courseworks, December 29, 2017, [Электронный ресурс]. URL: https://webcourseworks. com/2018-elearning-predictions-updatedhype-curve (Дата обращения 05.11.2020)
5. Университеты соперничают за Blockchain Доминирование [Электронный ресурс]: Университетская сеть Copyright © 2018г. URL:https://www.tun.com/ru/блог/университеты-и-правительствакоторые-соперничают-для-blockchain-доминирования/ (Дата обращения 05.11.2020)
6. Грошева Е. К., Невмержицкий П. И., Блокчейн - новая революция // Бизнес-образование в экономике знаний, 2018. №1. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/blokcheyn-novaya-revolyutsiya (Дата обращения 05.11.2020)
7. Заславский А. А. Перспективы использования алгоритмов блокчейн для обеспечения безопасности при управлении образовательной организацией // Вестник РУДН. Серия: Информатизация образования, 2018. №1.
8. Алексей Михеев. Блокчейн: Как это работает и что ждет нас завтра [Текст]. – М.: Бизнес-книги, 2017. – 586 с

9. Пирогов Владислав Юрьевич. Информационные системы и базы данных: организация и проектирование : навч. посібник [Текст]. / Пирогов В.Ю. – М.: БХВ-Петербург, 2009. – 528с.

10. Ethash алгоритм майнинга: как он работает для Ethereum [Электронный ресурс]. URL: https://bytwork.com //, (Дата обращения 03.11.2020).

11. Алгоритмы Хэш-функция SHA-256 [Электронный ресурс]. URL: https://medium.com. (Дата обращения 05.11.2020)

12. Asymmetric Cryptography On The Ethereum Blockchain [Электронный ресурс]. URL: https://medium.com, (Дата обращения 05.11.2020)

13. Алгоритмы криптовалют — как работает биткоин и альткоины [Электронный ресурс]. URL: https://coinpost.ru, (Дата обращения 05.11.2020)

14. Что такое криптография и хэш-функция в системе блокчейна [Электронный ресурс]. URL: https://cryptocartel.club, (Дата обращения 05.11.2020)

15. Проектирование информационных систем: уч. пособие [Текст]. / Н.Н. Заботина. – М.: ИНФРА-М, 2011. – 331 с.

ДОДАТКИ