

БЛОКЧЕЙН ТЕХНОЛОГІЇ ДЛЯ ПРИЙНЯТТЯ КОЛЕКТИВНИХ РІШЕНЬ НА ОСНОВІ ДОКУМЕНТІВ

Вінницький національний технічний університет

Анотація. Виконані дослідження використання технології блокчейн для прийняття рішень на основі консолідованих документів. Запропонована система документообігу, що використовує децентралізовану масосореplikовану базу даних. Безпека системи базується на алгоритмі Кескак–256. Ця функція перетворює документ будь-якого обсягу у фіксований рядок довжиною 256 біт. Сформовані поведінкові моделі роботи системи. Запропоновано використовувати гібридну модель, яка передбачає, що документи розміщуються в децентралізованій мережі, а ідентифікатори зберігаються в смарт-контракті.

Ключові слова: документообіг, блокчейн-голосування, дерева блокчейн, Ethereum, поведінкові моделі, структури даних, смартконтракти.

Abstract. Research has been conducted on the use of blockchain technology for decision-making based on consolidated documents. A document management system using a decentralized mass-replicated database has been proposed. System security is based on the Keccak-256 algorithm. This function converts a document of any size into a fixed string of 256 bits in length. Behavioral models of the system have been formed. It is proposed to use a hybrid model that assumes that documents are placed in a decentralized network and identifiers are stored in a smart contract.

Keywords: document management, blockchain voting, blockchain trees, Ethereum, behavioral models, data structures, smart contracts.

Актуальність використання блокчейн технологій для прийняття колективних рішень не зменшується з часом. Розподілені структури організації, проблеми колективної роботи з документами, прийняттям рішень на їх основі вимагає активного запровадження децентралізованих, масово реплікованих баз даних та знань. Такі бази використовують спеціальні структури даних – дерева, які мають кореневий хеш для позначення всього дерева з неможливістю зміни дерева без зміни кореневого хешу. Кожен обліковий запис в дереві зберігається як чотири пакети даних – параметри акаунту, код хешу, остання транзакція [1]. Сучасні системи колективного управління вимагають переходу до децентралізованих архітектур, де довіра забезпечується криптографічними протоколами. Використання платформи Ethereum дозволяє інтегрувати юридично значущі документи безпосередньо в програмну логіку смарт-контрактів, що унеможливорює ретроспективну зміну умов або фальсифікацію результатів.

Процес ініціації голосування активується функцією, яка приймає хеш документа як константну точку відстеження. Ідентифікація учасників здійснюється через механізми асиметричного шифрування, де право голосу підтверджується володінням специфічними активами або включенням до реєстру через цифрові підписи.

Безпека системи базується на алгоритмі Кескак–256. Ця функція перетворює документ будь-якого обсягу у фіксований рядок довжиною 256 біт. Унікальність цифрового відбитка гарантує, що навіть мінімальна зміна в тексті призведе до повної невідповідності хешу, зафіксованого в мережі. Оскільки зберігання великих файлів безпосередньо в блокчейні є економічно недоцільним, застосовується гібридна модель. Документи розміщуються в децентралізованій мережі, а ідентифікатори зберігаються в смарт-контракті [2].

В таблиці 1 представлені архітектурні параметри системи для прийняття колективних рішень на основі документів.

Таблиця 1 – Архітектурні параметри системи

Параметр системи	Технологічне рішення	Функціональне призначення
Цілісність даних	Алгоритм Кессак–256	Захист документа від несанкціонованих правок
Доступність даних	Протокол IPFS	Децентралізоване зберігання великих файлів
Логіка управління	Смарт-контракти Solidity	Автоматизація підрахунку та виконання рішень
Безпека транзакцій	Рівень 2 (Rollups)	Зниження вартості та збільшення швидкості

Для запобігання зловживанням впроваджуються методи захисту від повторного голосування та механізми фіксації стану мережі. Це дозволяє визначити коло користувачів, що приймають рішення, саме на момент створення пропозиції, нівелюючи ризики маніпуляцій. Докази з нульовим розголошенням додатково забезпечують анонімність волевиявлення, зберігаючи можливість публічного аудиту.

Інтеграція Ethereum із децентралізованими сховищами та надійними хеш-функціями перетворює статичні документи на динамічні об'єкти управління. Такий підхід усуває розрив між етапом погодження та фактичною реалізацією рішення, створюючи прозоре середовище для колективної взаємодії.

Для запровадження блокчейн технологій в система документообігу повинна відповідати таким вимогам:

1. Розмежування прав доступу користувачів та введення ролі адміністратора;
2. Контроль реєстрації користувачів адміністратором;
3. Збереження метаданих кожного документу;
4. Відповідність форматів та параметрів файлів;
5. Можливість оповіщення користувачів;

Поведінкова модель користувача передбачає роботу таких рольових користувачів як адміністратор; визначений співробітник. Така модель передбачає реалізацію загальних процедур – реєстрація, перегляд інформації про файл, видалення файлу, завантаження, перегляд файлу та його версій; перегляд прав доступу до файлу та завдань до файлу; перегляд списку користувачів та груп. Адміністратор може додати користувача, працювати з метаданими; створювати та видаляти групи користувачів; додавати та видаляти завдання; змінювати параметри файлів; відновлювати дані щодо користувачів та документів; переглядати списки та документи, створені іншими учасниками.

Логічна модель передбачає наявність користувача, який відноситься до визначеної групи, має доступ або створив документ з визначеними категорією та завданнями. Вона передбачає роботу сервісів з базою даних та знань; з користувачами, групами, файлами, категоріями та завданнями.

Сервіс для роботи з базою даних забезпечує стійке підключення та формує основні таблиці.

Сервіс для роботи з користувачами і групами відповідає за аутентифікацію користувачів і адміністраторів – перевіряє наявність користувача, його права та надає доступ.

Сервіс для роботи з файлами і каталогами дозволяє додавати та видаляти каталог, відображати його зміст, працювати з файлами.

Сервіс для роботи з блокчейн дозволяє додавати записи в блокчейн, переглядати записи, створювати та верифікувати підписи для документу; верифікувати документ.

Тобто, розподілена інформація серед багатьох користувачів, визначені права доступу та голосу, дозволяють прийняти рішення на основі документів.

Категорії документів передбачають різноманітність параметрів – загальні, спеціалізовані, з використанням підписів та голосування тощо. Роль адміністратора також передбачає контроль керівництва. Процес прийняття рішень автоматизується через призначення завдань до конкретних документів, де статус виконання може підтверджуватися транзакціями в блокчейні. Завдяки використанню структури – дерево та

його властивостям, система не потребує дублювання даних, оскільки вузли нового стану можуть посылатися на ідентичні ділянки пам'яті попередніх блоків, що оптимізує ресурсомісткість. Це дозволяє створити універсальне середовище для документообігу, яке не залежить від спеціалізації організації та забезпечує кросплатформенність.

Визначені методи та моделі дозволяють зробити висновок про доцільність використання технологій блокчейн в процедурах прийняття колективних рішень. Такі технології дозволяють реалізувати прозорі та обгрунтовані процедури прийняття рішень.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. 2024.
2. Benet J. IPFS - Content Addressed, Versioned, P2P File System. 2014.

Шептяков Ігор Олександрович група 122а, Факультет інтелектуальних інформаційних технологій та автоматизації

Белзетський Руслан Станіславович, к.т.н., доцент, доцент кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця, belzetskiy@vntu.edu.ua

Ihor Sheptiakov, group 122a, Vinnytsia National Technical University, Vinnytsia. Faculty of Intelligent Information Technologies and Automation

Ruslan Belzetskyi, Ph.D., Associate Professor, Associate Professor, Department of Computer Science, Vinnytsia National Technical University, Vinnytsia, belzetskiy@vntu.edu.ua