УДК 004.056.55
В. Добжанський
(Тернопільський національний технічний університет іменні Івана Пулюя)

БЕЗПЕЧНЕ ПЕРЕДАННЯ ДАНИХ У ВІРТУАЛЬНИХ ДОСЛІДНИЦЬКИХ КОЛЕКТИВАХ ТЕХНОЛОГІЄЮ BLOCKCHAIN

В процесах наукового комуні кування віртуальних дослідницьких колективів достовірність даних та документів є дуже важливою, якщо не критичною. У таких колективах обмін документними потоками повинен відповідати вимогам інтелектуальної власності, а також конфіденційності, що передбачає ефективний захист багатьох документів. Для безпечного передавання даних між членами віртуальних дослідницьких колективів, на нашу думку, слід використовувати технологію blockchain, яка повинна забезпечувати незмінність змісту документу та збереження оригінальних даних від стороннього втручання.

Blockchain – це технологія, яка створює розподілений реєстр для зберігання статичних даних динамічних транзакцій без централізованої координації за допомогою механізму, що базується на принципах перевірки їх дійсності.

Транзакція – це набір команд, що виконується як єдине ціле. У транзакції або всі команди будуть виконані, або жодна з них не виконується. Якщо хоча б одна з команд транзакції не може бути виконана, здійснюється призупинення виконання всієї трансакції. Для транзакцій в блоці використовується деревоподібне хешування, формуванню хеш-суми файлу.

Розглянемо blockchain технологію для передавання даних між членами дослідницького колективу. Дані, файл або документ, що передаються, зберігаються в сховищі, створюючи – хеш для кожного файлу. Хеш – це алгоритм, який перетворює вхідні дані будь - якого розміру в дані фіксованого розміру.

Хеш позначається номером, який формується під час створення і записується в окремі блоки. Блок – це група транзакцій записати в спеціальну структуру. Блок складається із заголовка та списку транзакцій. Заголовок блоку включає в себе свій хеш, хеш попереднього блоку, хеш транзакцій та додаткову службову інформацію. Кожен блок завжди містить інформацію про попередній блок. Усі блоки можна вибудувати в один ланцюжок, який містить інформацію про надісланий файл. Перший блок в ланцюжку – первинний блок – оскільки в нього відсутній материнський блок. При необхідності автентичність даних може бути перевірена шляхом порівняння двох хешів тих самих даних.

Створений блок буде прийнятий іншими користувачами, якщо числове значення хешу заголовка менше або дорівнює певному числу, величина якого періодично коригується учасниками віртуального колективу. Результат хешування непередбачуваний, алгоритму отримання кінцевого результату не створюється, тому формується з допомогою випадкового перебору. Якщо хеш не задовольняє умову, то довільно змінюється блок службової інформації в заголовку - і проводиться повторне звіряння хешу. Після співпадіння варіантів, вузол розсилає отриманий блок іншим підключеним вузлам, які перевіряють блок. Якщо помилок немає, то блок вважається доданим в ланцюжок і наступний блок повинен включити в себе його хеш.

Таким чином, технологія blockchain дозволяє зберігати конфіденційність інформації, якою обмінюються учасники віртуального наукового колективу.

1. What Is Blockchain and What Does It Mean for Data Protection? [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – 2018 Acronis International GmbH. – Режим доступу: https://www.acronis.com/en-us/blog/posts/what-blockchain-and-what-does-it-mean-data-protection – Назва з екрана.