

АПАРАТНЕ ХЕШУВАННЯ ДАНИХ

¹Вінницький національний технічний університет

Анотація

Запропоновано метод обробки велико-розмірних масивів даних на основі оптично-керованих транспарантів та за допомогою створення хеш-функції, яке дозволило збільшити швидкість обробки і відтворення даних.

Ключові слова: хеш-функція, блокчейн, оптично-керовані транспаранти, масив, спеціалізовані комп'ютерні системи.

Abstract

The method of processing large-size arrays of data on the basis of optically controlled banners and by creating a hash function, which allowed to increase the speed of processing and reproduction of data, is proposed.

Keywords: functionality, blockchain, optically controlled transparent, masses, specialized systems

Вступ

Зараз у світі активно розвиваються Blockchain -технології і найбільше поширення вони отримали у фінансово-технологічному секторі. Але ці технології мають набагато більше перспектив, їх можна використати і в інших галузях. Можливо виділити п'ять основних причин, чому підприємствам варто розпочинати використовувати децентралізовані технології.

Blockchain по суті являє собою розподілену базу даних записів або публічної книги всіх транзакцій або цифрових подій, які були виконані і розподілені між сторонами. Кожна транзакція в публічній книзі перевіряється консенсусом більшості учасників системи.

Мета та завдання роботи: підвищення швидкодії та продуктивності, пошук відповідного алгоритму для паралельного обчислення [1]

Результати дослідження

Спеціалізовані обчислювальні системи (КС) - це системи, здатні виконувати складні операції з великомасштабними даними, які подаються на масиви. Для того щоб забезпечити належну швидкість операцій у спеціалізованій КС, необхідно створити для них можливість паралельного введення, обробки і виведення даних. Це можна зробити за допомогою паралельних методів введення, обробки та виведення для спеціалізованих операційних систем. Головними з них є методи, що базуються на шинах з кількома шинами, що базуються на паралельному використанні набору частот і на основі контрольованих банерів.

Оптично-керовані транспаранти (ОКТ) являють собою тонку пластину з електрооптичного матеріалу та нанесеним на нього фотопровідним шаром з напівпровідника. З обох сторін така пластинка має два прозорих електроди [1].

Оптично-керовані транспаранти використовуються для введення, виведення та обробки інформації в спеціалізованих операційних системах. Вони здатні працювати з великими обсягами даних, що є основною умовою їх використання в таких операційних системах.

Зараз в світі активно розвиваються блокадні технології. Вони можуть знайти своє застосування в інших сферах людської діяльності, наприклад: медицина, кібербезпека, освіта, дослідження, правозахисні сфери, продаж і лізинг машин і навіть послуги для прослуховування музики в Інтернеті тощо.

Дану технологію можна розглядати як спеціалізовану обчислювальну систему з методом паралельного введення обробки і виведення даних.

Blockchain - це по суті розподілена база даних записів або загальнодержавна книга всіх транзакцій або цифрових подій, які були виконані та розподілені між учасниками. Кожна транзакція в

державній книзі перевіряється консенсусом більшості учасників системи. І, як тільки введений, інформація ніколи не буде стерта. Blockchain містить певний і перевіряється запис про кожну зроблену операцію.

Хешування - це процес перетворення масиву вхідних даних довільної довжини в (початковий) рядок бітів фіксованої довжини. Наприклад, хеш-функція може приймати рядок з будь-якою кількістю символів (одна літера або ціла літературна робота), а на виході отримувати рядок з суворо визначеним числом символів [2].

Під час обробки даних формується велико-розмірна матриця, в якій кожна комірка перетворюється у хеш-код, який потім формує матрицю з відповідними даними які утворились. В подальшому згідно цих результатів і виконується обробка даних.

Висновки

У роботі проаналізовано основні характеристики технології Blockchain та хешування функції. Охарактеризовано, що однією з основних функцій Blockchain є його паралельна обробка і аналіз даних. З метою підвищення ефективності та швидкості аналізу та обробки даних було запропоновано використовувати оптично контрольовані банери та використовувати хешування при роботі з великими обсягами даних. Подальша робота буде спрямована на вдосконалення раніше описаних функцій, використовуючи спеціалізовану Blockchain -обчислювальну систему з використанням оптично контрольованих банерів.

На сьогоднішній день ми отримали наступні дані: для 512-бітових одиниць, час обробки даних становить 0.325ns, а побудова хеш-функцій за 512-бітовими блоками становить 181,174ns.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Лисенко Г. Л., Тарновський М. Г., Кузьменко Л. В. Сучасні тенденції у вирішенні задач виявлення та розпізнавання об'єктів на зображеннях //Оптико-електронні інформаційно-енергетичні технології. – 2017. – Т. 33. – №. 1. – С. 18-23.
2. Roger Wattenhofer The Science of the Blockchain / Roger Wattenhofer – К. : Information technologies, 2016 – С. 94 – 120.

Науковий керівник: *Лисенко Геннадій Леонідович* – к.т.н., проф. кафедри лазерної та оптикоелектронної техніки, Вінницький національний технічний університет, м. Вінниця, Україна.

Кузьменко Лілія Вікторівна – аспірантка кафедри Лазерної та оптикоелектронної техніки, Вінницький національний технічний університет, м. Вінниця, Україна.

Supervisor: *Lysenko Gennadii L* - candidate of technical sciences, prof. Department of Laser and Optoelectronic Technology, Vinnytsia National Technical University, Vinnytsia, Ukraine.

Kuzmenko Liliia V – Phd student of the Department of Laser and Optoelectronic Technology, Vinnytsia National Technical University, Vinnytsia, Ukraine.