СЕКЦІЯ XVII.
ФІЗИКО-МАТЕМАТИЧНІ НАУКИ

ВИКОРИСТАННЯ ВИЩОЇ МАТЕМАТИКИ, ЯК ОСНОВИ МАЙБУТНЬОЇ ЦИФРОВОЇ ЕКОНОМІКИ, ПОБУДОВАНОЇ НА АВТОМАТІ

Гавриш Кирило Володимирович
здобувач вищої освіти інженерно хімічного факультету
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського", Україна

Науковий керівник: Листопадова Валентина Вікторівна
ORCID ID: 0000-0002-2549-8381
канд. фіз.-мат. наук, доцент,
доцент кафедри математичної фізики та диференціальних рівнянь
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського", Україна

Давно вже не секрет, що вища математика, охоплюючи вищу алгебру та математичний аналіз, формує базис багатьох інших дисциплін. Її використовує розлогий спектр спеціальностей:

– аналітики;
– маркетологи;
– управлінці;
– програмісти;
– інженери;
– архітектори;
– бізнесмени.

Дійсно ж вражає те, що вища математика здатна сформувати принципово новий підхід до економіки, формуючи новий етап її розвитку – цифровий. Ідея цифрової економіки полягає у використанні спеціалізованих технологій, наприклад, технології блокчейн.

Блокчейн (англ. Blockchain) – розподілена система зберігання інформації, що використовує у своїй основі послідовний нерозривний ланцюжок блоків (рис. 1), збудований за певними правилами передачі даних.

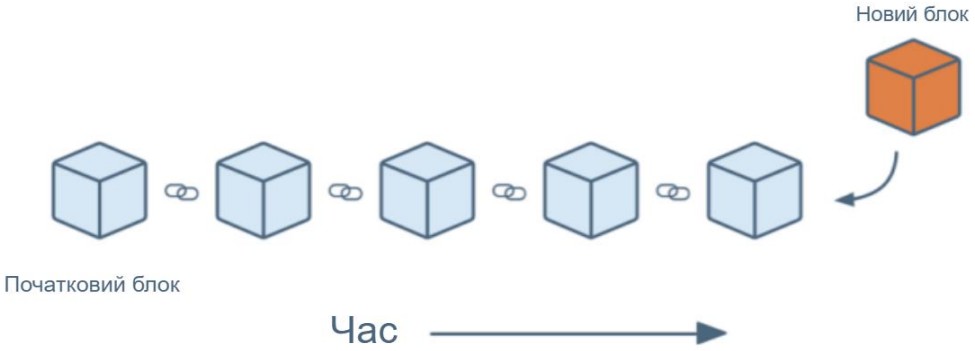

Рис. 1. **Візуалізація послідовного нерозривного ланцюга блоків з плином часу**

Якщо не поринати в технічні деталі, то блокчейн це база даних. На чолі цієї технології стоять безпека, децентралізація та незмінність інформації, що робить блокчейн базою даних нового покоління. На цей час він найкраще проявив себе саме у фінансовій та економічній галузях, створивши перші цифрові активи – криптовалюти, але про них та їх роль згодом. Для визначення ж ролі вищої математики у всьому цьому, варто згадати про теорію автоматів.

Теорія автоматів – розділ дискретної математики, що вивчає абстрактні автомати (обчислювальні машини), представлені у вигляді математичних моделей (задачі, які вони можуть вирішувати).

Автомат можна схарактеризувати як пристрій, що має вхідний та вихідний канали, і що знаходиться у кожний дискретний момент часу в одному із внутрішніх станів [1]. Тобто автоматом можна вважати модель зберігання інформації на одиницю часу. Блокчейн являє собою автомат, де блоки (його складові) відображають внутрішній стан у дискретний момент часу.

Як зазначалося раніше, прикладом використання блокчейну на практиці є новий фінансовий інструмент – криптовалюти, що користуються все більшою популярністю та інтегруються у різні сфери. Вони вже визнаються законним платіжним засобом у різних країнах світу, а в деяких країнах навіть формують значну частину економіки, наприклад у Сальвадорі.

Криптовалюта (англ. Cryptocurrency) – цифрова валюта, побудована на технології блокчейн. В основі криптовалют лежать криптографічні методи шифрування даних та захисту операцій у мережі (цифровий підпис, хешування) – від цього з'явилася приставка "крипто".

Далі дізнаймось, яка роль вищої математики у формуванні нового фінансового активу, що слугує базисом цифрової економіки. Розгляньмо детальніше цифровий підпис та хешування, що використовується у криптовалютах.

Цифрові підписи у блокчейні базуються на криптографії з відкритим ключем. У ньому використовуються два ключі:

– Перший – private key (закритий) – необхідний для формування цифрових підписів (як PIN від банківської карти);

– Другий – public key (відкритий) – використовується для перевірки електронного підпису (як номер банківської карти).

Відкритий ключ можливо обчислити на основі закритого ключа, а ось зворотне перетворення вимагає неможливого на практиці обсягу обчислень. Повертаючись до цифрового підпису, котрий, до речі, використовується для підписання транзакцій в блокчейні, варто звернути увагу на його формування. Непідписана транзакція, що містить (відкритий та закритий ключі адресанта, відкритий ключ адресата, повідомлення про переказ - “адресант X надіслав 100$ адресату Y” та додаткову інформацію про час, розмір і т.д.) математичним чином “зливається” з закритим ключем адресанта і на виході ми отримуємо цифровий підпис. У блокчейні, дані зберігаються в блоках. Щоб ідентифікувати користувача, використовуються блокчейн-адреса, котра з’являється шляхом шифрування конкретного публічного ключа. Існує велике різноманіття схем криптографії з відкритим ключем. Одна з найпопулярніших схем – на основі екліптичної прямої. Наприклад, у Bitcoin – найпопулярнішій криптовалюті світу, використовується стандарт екліптичної криптографії ECDSA разом з екліптичною прямою secp256k1 [2].

Що ж стосується хешування, то:

Хеш-функція (англ. Hash function) – математичний алгоритм, що перетворює вхідні дані в унікальний набір значень (хеш). Розмір хешу фіксований у межах використовуваного алгоритму.

Хеш/хеш-сума/хеш-код (англ. Hash) – набір символів, отриманий в результаті роботи хеш-функції над вхідними даними. Хеш не можна повернути до початкового стану, тобто не можна розшифрувати.

Хеш-функції вирішують безліч проблем, пов'язаних із безпекою інформації. Наведу найпоширеніший варіант використання:

- Перевірка цілісності даних.

Якщо порівняти хеші, обчислені з даних до і після певної дії (наприклад, при передачі між пристроями), можна визначити, чи були внесені зміни до цих даних (рис. 2).

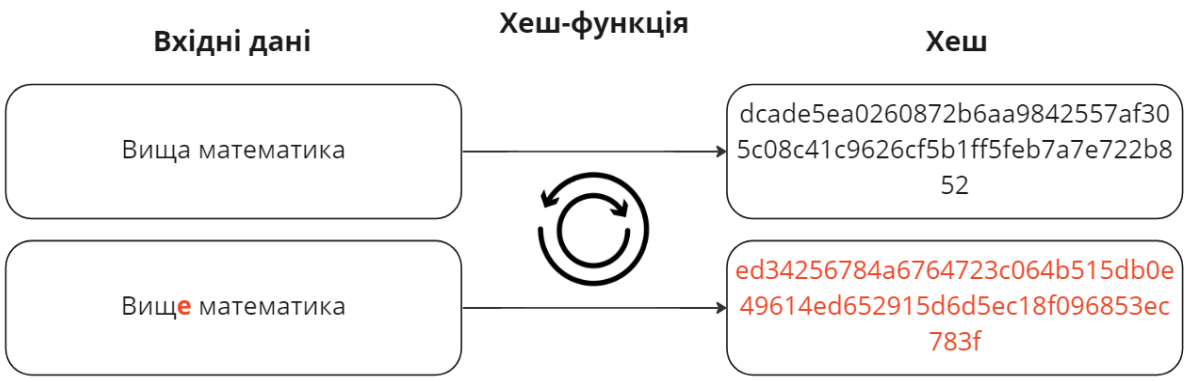

Рис. 2. **Порівняння хешів при зміні вхідних даних**

За допомогою хешування, криптовалюти неможливо підробити, а блокчейн є цілісною системою.

У згаданому вище й полягає роль вищої математики, як основи для забезпечення функціонування елементарних подій, що складають цілісність. Проте як же це все формує нову економіку?

Як пише Мелані Свон у своїй книзі “Блокчейн. Схема нової економіки”: “Цілком імовірно, ми перебуваємо на порозі блокчейн-революції. Ця революція почалася з появою нової економічної реальності в інтернеті – альтернативної валюти під назвою Bitcoin, яка емітується та забезпечується не державою, а користувачами біткойн-мережі при автоматизованому досягненні консенсусу між ними. Унікальність цієї валюти полягає в тому, що її користувачам не обов'язково довіряти один одному. Вбудовані в систему алгоритми саморегулювання запобігають будь-яким зловмисним спробам обману. Якщо бути точним, то з технічної точки зору біткойн - це цифрові гроші, що звертаються в децентралізованої, пірингової електронної платіжної системи, заснованої на публічно доступній книзі обліку, що називається "блокчейном".”[3].

Довіру, безпеку та децентралізоване управління в рамках блокчейну забезпечує вища математика. Саме вона “дала життя” новим цифровим валютам, які з плином часу можуть змінити світ на краще.

Список використаних джерел:

1. Кудрявцев В. Б. (2008) Теорія Автоматів Велика енциклопедія. Вилучено з: https://bigenc.ru/mathematics/text/1850012.
2. BitfuryGroup (2017) Криптографія в блокчейнах: про хеш-функції, ключі та цифрові підписи. Вилучено з: https://habr.com/ru/company/bitfury/blog/327272/.
3. Мелані Свон. (2017) Блокчейн. Схема нової економіки. *1-2.* Вилучено з: http://loveread.ec/read_book.php?id=66268&p=1