УДК 004.031.43:004.056

РОЗРОБКА ПРОГРАМИ ДЛЯ ДЕМОНСТРАЦІЇ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Якушко Максим

Науковий керівник: канд. пед. наук, доцент Лупан І.В.

Центральноукраїнський державний педагогічний університет

імені Володимира Винниченка, м. Кропивницький, Україна

У статті розглянуто додаток, розроблений для демонстрації та вивчення технології блокчей, за допомогою інтегрованого середовища Visual Studio 2019 а саме за допомогою додатку Windows forms(.NET framework) та за допомогою мови програмування C#(Сі Шарп). У додатку, реалізованому у вигляді багатовіконної програми, змодельовано введення нових блоків даних, шифрування даних в блокчейні та поширення хеш-коду нововведеного блоку у розподіленій базі, вилучення блоків, тощо. Розроблений додаток можна використовувати при вивченні дисциплін, пов'язаних з використанням технології розподіленого зберігання даних.

Ключові слова: блокчейн, хеш, біткоін, дані.

DEVELOPMENT OF THE PROGRAM FOR BLOCKCHAIN TECHNOLOGY DEMONSTRATION

Yakushko Maxim

Scientific supervisor: Candidate of Pedagogical Sciences, Docent Lupan I.V.

Volodymyr Vynnychenko Central Ukrainian State Pedagogical University,

Kropyvnytsky, Ukraine

Abstract. The article discusses an application designed to demonstrate and study blockchain technology using the Visual Studio 2019 integrated environment. The application, implemented as a multi-window program, simulates the entry of new data blocks, data encryption in the blockchain and the distribution of the hash code of the newly entered block in the distributed database, the removal of blocks, and so on. The developed application can be used in the study of disciplines related to the use of distributed storage technology.

Keywords: blockchein, hash, bitcoin, data.

Технологія блокчейн виникла у 1991 році, але серйозного розвитку набула лише на початку двохтисячних. На сьогоднішній день вона отримала стрімкий стрибок розвитку в різних додатках, не тільки у тих, що пов'язані з криптовалютами. В основу технології покладено розподілену між великою кількістю користувачів базу даних, що зберігає впорядкований ланцюжок даних, який постійно нарощується. Ці дані захищено від підробки шляхом посилання на попередній блок, застосування принципів дзеркального зберігання даних та контрольних сум. Кожен блок включає в себе власний хеш-код, часову мітку, хеш попереднього блоку та дані транзакцій, подані у вигляді хеш-дерева. Така база даних покладена, зокрема, в основу криптовалюти Bitcoin, де технологія блокчейн слугує контейнером для зберігання інформації щодо всіх проведених операцій. На сьогоднішній день найбільш активно технологію блокчейн застосовують для здійснення фінансових транзакції на основі роботи криптовалют (наприклад, цифрових платежів на основі біткоіна); забезпечення контрактів (використання технології в сферах економіки, фінансів, робота з акціями компаній, облігаціями, активами та контрактами); використання в сфері державного управління, науки, освіти та охорони здоров'я).

На сьогоднішній день блокчейн є передовою технологією для обміну інформації між користувачами, а її вивчення та дослідження особливостей застосування у різних сферах діяльності є актуальною задачею.

Мета нашої роботи полягає у створенні комп'ютерної програми, яка дозволить демонструвати роботу технології блокчейн в різних сферах діяльності з метою навчання.

Постановка задачі. Технічне завдання полягало у створенні в середовищі Visual Studio 2019 програми для моделювання роботи технології блокчейн. Програма повинна дозволяти користувачеві вводити та змінювати дані в системі; обраховувати хеш-код нововведених блоків даних; обраховувати хеш, який починається префіксом "0000" для підтвердження транзакції і передачі

нового блоку до загального ланцюжку блоків; наочно представляти роботу технології. Також програма повинна бути зрозумілою у використанні та мати графічний інтерфейс.

Підготовка до проектування та розробки демонстраційної програми за вищевказаними вимогами починалася з грунтовного вивчення засад, покладених в основу технології. Блокчейн – це послідовність розташованих один за одним блоків з інформацією про транзакції [1]. При цьому кожен блок містить вказівник (хеш) попереднього блоку. На Рис. 1 схематично показано розподілену базу даних, що має впорядкований ланцюжок транзакцій (так званих блоків), що постійно збільшує свою довжину.

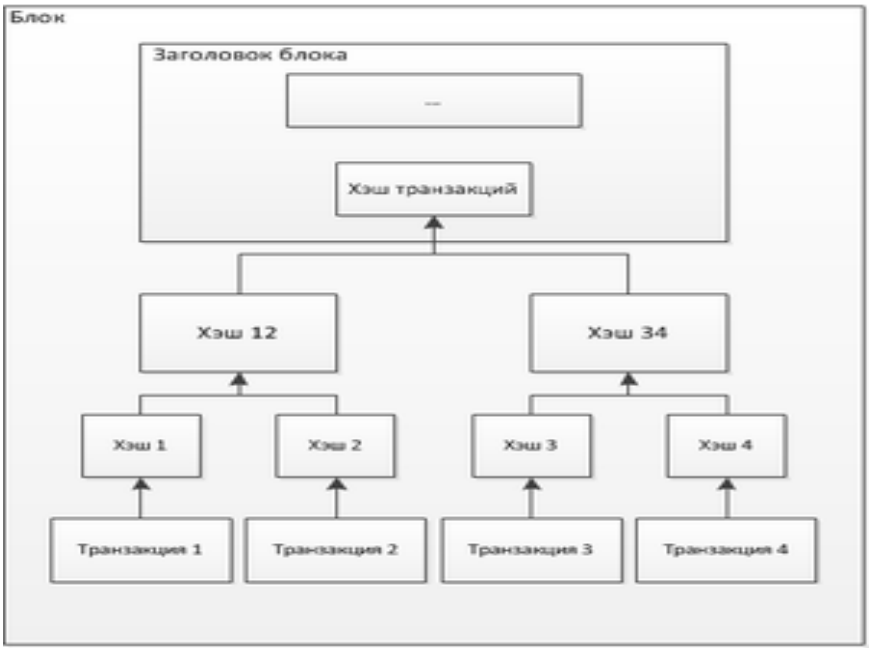

Рис.1 Архітектура технології блокчейн [2]

Блок – елемент даних, що містить в собі заголовок та тіло для відокремлених даних. Заголовок містить деяку форму хешованих посилань на довільні дані та хеш-вказівник на один існуючий заголовок блоку. Особливий випадок блоку, що не посилається на попередній існуючий блок, називається блоком генезису, який означає початок структури даних [3, 4].

Хеш-вказівник – це вказівник, який зберігає в собі деякий набір даних і обчислюється за допомогою криптографічного хешу. Це дає змогу знаходити та перевіряти дані на предмет захищеності.

Головною проблемою технології блокчейн є достовірність даних. Отже з'являється необхідність застосовувати ефективні алгоритми шифрування. Ці алгоритми повинні забезпечувати криптографічну стійкість даних та інформації в мережі та мати реалізацію цифрового підпису.

Кожен блок у блокчейні складається з двох головних частин – заголовку (Head) і тіла (Payload). Payload містить список всіх транзакцій, які повинні бути збережені в даному блоці і потрапити в Blockchain. Head містить інформацію, яка відповідає за стабільність мережі.

У блокчейні Head містить такі поля:

- Номер версії (Version);
- Хеш попереднього блоку (prev_block);
- Хеш всіх транзакцій в поточному блоці (mrkl_root);
- Мітку часу коли цей блок був створений (Time);
- Bits і Nonce, які використовують в майнінгу.

Хешування – процес перетворення інформації у бітовий рядок. Ці перетворення називаються хеш-функціями (згортка), а їхніми результатами є хеш-код. Хеш-код є унікальним. Якщо в послідовності змінити хоча б один байт, то хеш-код змінить своє значення. Отже дані будь-якого розміру, закодовані за допомогою хеш-функцій, перетворюються в бітову послідовність, яка має фіксовану довжину [5].

Для отримання хешів будь-якого виду використовують хеш-функції. Для отримання хешу всіх транзакцій в блоці використовують спеціальний алгоритм Меркла. Прикладом є алгоритм SHA 256, в основу якого покладена структура Меркла.

Алгоритм SHA 2, побудований на основі SHA 256, – це той самий алгоритм, за рахунок якого існує майнінг Bitcoin і багатьох альткоінів. Скорочення SHA 2 або Secure Hash Algorithm 2 (алгоритм безпечного хешування) – це набір криптографічних хеш-функцій, що шифрують дані. Цей алгоритм має реальне застосування, зокрема, у протоколах захищеної передачі даних. Протоколи TLS, SSH, PGP – всі вони базуються на цьому алгоритмі.

SHA 256 – це однонапрямлена функція для створення цифрових відбитків фіксованої довжини в 256 біт з вхідних даних розміром максимум 2^{60}-1 біт (що дорівнює 2 ексабайтам), яка використовує алгоритм SHA 2

Інформація, що передається в системі, має унікальний підпис (хеш). Якщо алгоритм шифрування не стійкий до колізій (тобто обчислень однакового хешу для різної інформації), тоді підробити хеш буде досить реально.

Створення додатку. При побудові додатку були використані наступні елементи керування форми:

- ✓ Label – являє стандартну мітку Windows.
- ✓ Panel – використовується для групування колекцій елементів управління.
- ✓ Button – представляє елемент керування кнопки Windows.
- ✓ pictureBox – представляє елемент керування Windows Picture Box для відображення зображення.
- ✓ textbox – представляє елемент керування текстового поля Windows.
- ✓ toolTip – представляє невелике прямокутне спливаюче вікно, в якому відображається короткий опис призначення елемента управління, коли користувач кладе покажчик на елемент управління.

Демонстраційний додаток має бути наочним, тому було прийнято рішення створити декілька вікон, кожне з яких буде емулювати роботу технології блокчейн в деякій мірі. Для виклику кожного вікна було створено головне вікно (Рис.2):

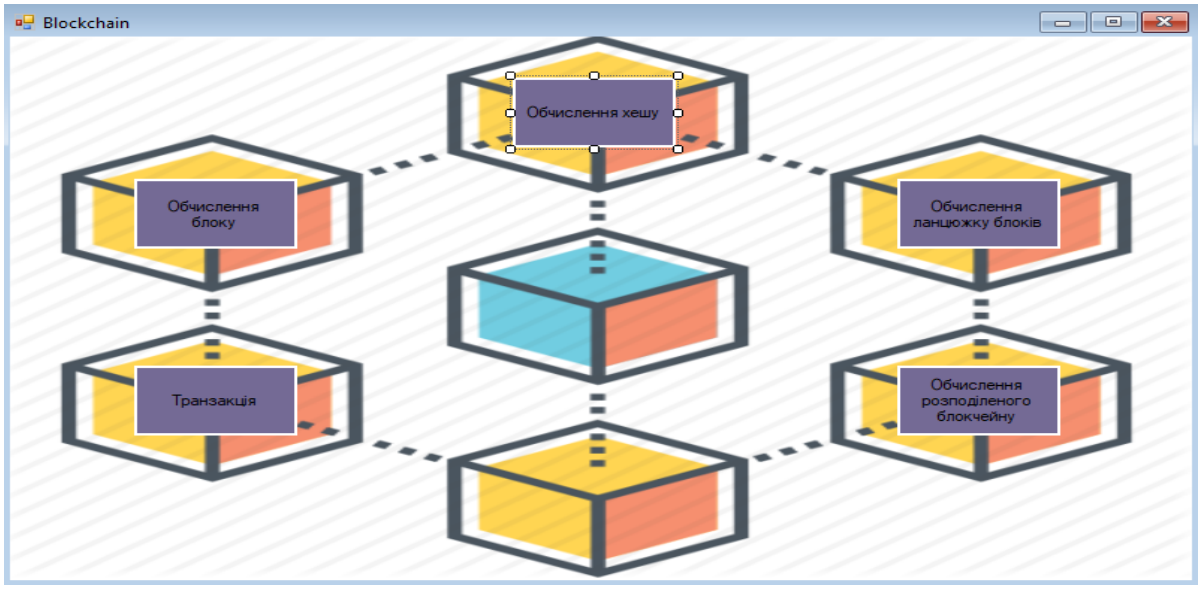

Рис. 2. Головне вікно для вибору наступної дії.

Дане вікно представляє собою меню для обрання дії, яку бажає здійснити користувач. Кожна з кнопок (Рис.3.) викликає відповідне вікно, кнопка «_» згортає вікно, кнопка «▭» розгортає вікно на весь екран, а кнопка «X» завершує роботу програми. Код для однієї з кнопок представлено на Лістінгу 1:

Лістінг 1. Кнопка переходу в вікно «Обчислення хешу»:

```
private void calchash_Click(object sender, EventArgs e)
        {
            this.Hide();
            HashForm hashForm = new HashForm();
            hashForm.Show();
        }
```

На Рис. 3 зображено вікно програми для знаходження хешу через змінення даних, введених в поле «DATA»:

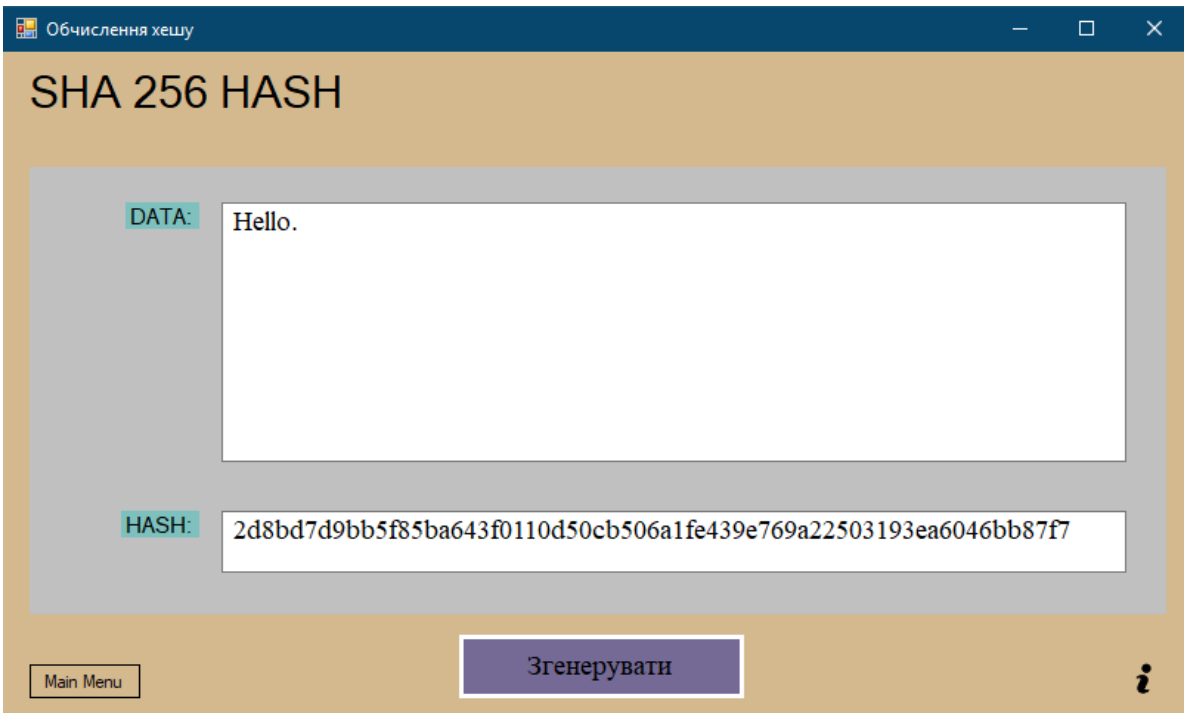

Рис. 3. Вікно для обрахування хешу в залежності від введених даних.

При побудові цього вікна було використано 3 елемента Label(), 2 елемента Button(), 1 елемент pictureBox(), 2 елементи textBox() та 1 елемент Panel(). Нижче наведено код для кнопки «Згенерувати» (Лістінги 2):

Лістінг 2: «Згенерувати»:

```
private void generate_Click(object sender, EventArgs e)
    {
        String data = textBox1.Text;

        using (SHA256 sha256Hash = SHA256.Create())
        {
            string hash = GetHash(sha256Hash, data);

            textBox2.Text = hash;

        }
    }
```

На Рис. 4 зображено вікно, яке показує ланцюжок блоків. Тут до поля з даними додається поле, що містить хеш попереднього блоку (поле prev). Тобто кожен наступний блок має хеш попереднього блоку. Тепер, якщо змінити дані в попередньому блоці, то наступний блок стане неправильним, тому що зміниться хеш попереднього блоку, а також зміниться хеш наступного блоку.

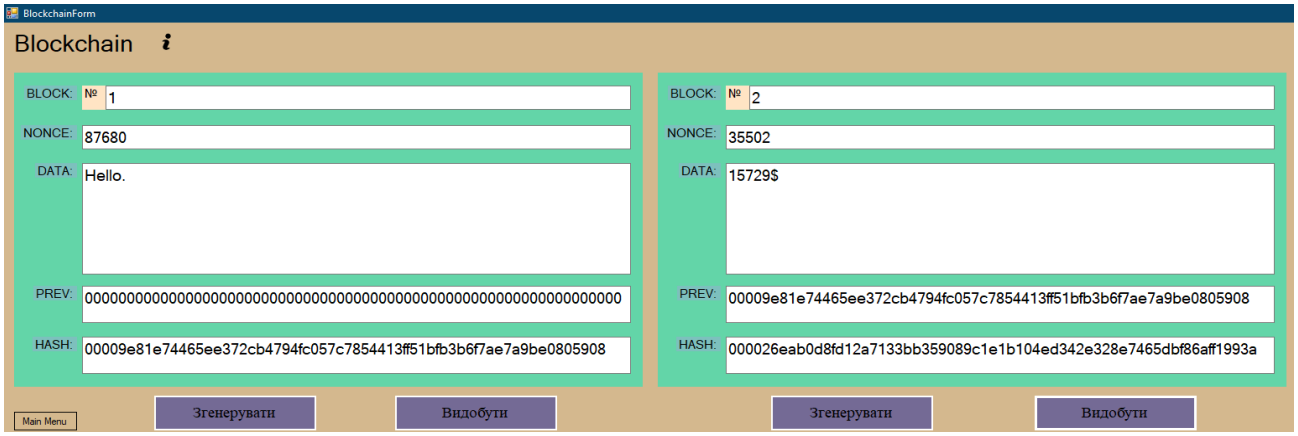

Рис. 4. Вікно для дослідження обрахування ланцюжку блоків.

В процесі виконання поставлених завдань було досліджено особливості функціонування технології блокчейн, а саме те що блоки даних доступні всім користувачам системи та захищені від неправомірних дій, саме це дозволяє технології блокчейн бути прозорою та водночас зберігати важливі дані, які не можливо підробити. Також децентралізована мережа потребує більшої кількості пристроїв, що означає більше технічного обслуговування та потенційних проблем, що, в свою чергу, накладає додаткове навантаження на IT-ресурси. Розподілена мережева система складається з процесів, потоків, агентів та розподілених об'єктів. Лише розподілених фізичних компонентів недостатньо для розподілу в мережі; зазвичай розподілена мережа використовує паралельне виконання програм. Оскільки технологія блокчейн може записувати кожну транзакцію за допомогою конкретного алгоритму, кожна наступна зміна у транзакції, створює інший блок даних в ланцюжку, що зв’язаний та простежується в кожній частині транзакції копіюючи транзакції за певний період часу в режимі реального часу, що робить дані транзакції більш безпечними, унеможливлюючи підробку або знищення даних.

Програмний продукт, що моделює роботу технології блокчейн, розроблено в середовищі Visual Studio 2019. Результати дослідження, а саме створений програмний додаток, можуть бути використані при викладанні дисциплін, пов’язаних з використанням та розробкою розподілених систем та систем захисту інформації. У подальшому планується удосконалити додаток та розробити його розподілену версію для запуску на локальному кластері.

Список літератури

1. Спасітєлєва С. О., Бурячок В. Л. Перспективи розвитку додатків блокчейн в Україні. *Кібербезпека: освіта, наука, техніка.* 2018. №1 (1). С.35-48. URL: http://oaji.net/articles/2020/8096-1594978172.pdf

2. Схема получения хеша транзакций (рисунок). [Електронний ресурс]. URL: https://ru.wikipedia.org/wiki/Блокчейн

3. Блокчейн (blockchain, цепочка блоков). [Електронний ресурс]. URL: https://alpari.com/ru/beginner/glossary/blockchain/

4. Wright Aaron, De Filippi Primavera. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. 2015. [Електронний ресурс]. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664

5. Технології захисту інформації. Мультимедійне інтерактивне електронне видання комбінованого використання / уклад. Євсеєв С. П., Король О. Г., Остапов С. Е., Коц Г. П. Х.: ХНЕУ ім. С. Кузнеця, 2016. 1013 Мб. ISBN 978-966-676-624- 6