УДК 681.32

В. П. Семеренко
А. С. Коробов

РЕАЛІЗАЦІЯ ТЕХНОЛОГІЇ БЛОКЧЕЙНУ НА ОСНОВІ ПОТОКОВИХ ХЕШ-ФУНКЦІЙ

Вінницький національний технічний університет

Анотація

Показано значення блокчейну як однієї з ключових технологій сучасної епохи цифровізації. Запропоновано реалізацію блокчейну на основі потокових хеш-функції і його використання в нефінансових сферах. Доведено, що функції переходів на основі теорії лінійних послідовнісних схем (ЛПС) відповідають всім мінімальним вимогам до потокових хеш-функцій.

Ключові слова: блокчейн, потокові хеш-функції, лінійні послідовнісні схеми (ЛПС)

Abstract

The importance of blockchain as one of the key technologies of the modern era of digitalization is shown. The implementation of blockchain based on stream hash functions and its using in non-financial fields is proposed. It is proved that the transition functions based on the theory of linear finite-state machine (LFSM) correspond to all the minimum requirements for stream hash functions

Keywords: blockchain, stream hash functions, linear finite-state machine (LFSM)

Вступ

Головною тенденцією сучасного розвитку світового господарства є цифровізація, тобто перехід до діяльності, в якій основними засобами виробництва є цифрові дані [1]. До цифрових технологій належать хмарні та мобільні технології, штучний інтелект, біометричні засоби ідентифікації, технології віртуалізації та доповненої реальності.

До цього переліку можна віднести і блокчейн, який представляє собою розподілену у глобальній мережі спеціальну базу даних для запису і перевірки операцій. Головна особливість цієї бази даних полягає в її організації у вигляді ланцюжка блоків. Кожний блок складається з хеша та корисної інформації. Хеш кожного блоку обчислюється із цілого попереднього блоку (рис.1). Будь-які зміни в блоці приведуть до інших значень хешів, в результаті буде порушена цілісность ланцюжка блоків.

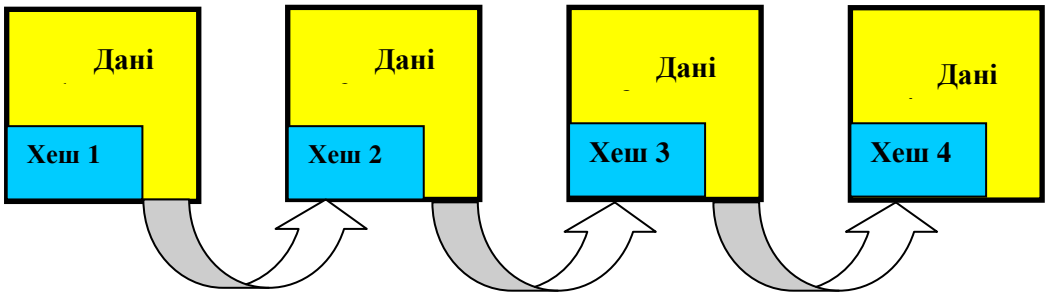

Рис. 1. – Ланцюжок блоків у блокчейні

Основна перевага блокчейну полягає у великій надійності в збереженні даних при усуненні потреби в різних адміністраторах та посередниках. Саме така вимога є найважливішою для фінансових розрахунків, тому блокчейн і зміг забезпечити появу цифрової криптовалюти [2].

Однак, надійність, простота і конфіденційність є також необхідними характеристиками в інших, нефінансових, сферах. Як приклади можна навести операції завірення юридичних і медичних документів, смарт-контрактів. Важливим є також є забезпечення цілісності різноманітних документів у сфері освіти: атестатів, дипломів, екзаменаційних відомостей тощо.

Блокчейн і потокові хеш-функції

В традиційному блокчейні використовуються блокові хеш-функції типу SHA-256 [3]. Такі функції високонадійні і тому цілком виправданим є їх використання у найбільш відповідальних сферах, зокрема у фінансах. Перевагою потокових хеш-функцій є їх дуже проста програмна реалізація [4]. Покажемо, що потокові хеш-функції на основі теорії лінійних послідовнісних схем (ЛПС) [5] відповідають всім мінімальним вимогам, і тому можуть знайти широке застосування в нефінансових сферах.

Будь-яка хеш-функція повинна задовольняти таким вимогам [6]:

– бути придатною до блоку даних довільної довжини;
– давати на виході значення фіксованої довжини;
– бути зручною при програмній та апаратній реалізації;
– забезпечувати високий спротив колізіям;
– бути односторонньою.

Для хеш-функцій на основі теорії ЛПС перші три вимоги задовольняються із самого означення ЛПС. Проаналізуємо решту вимог.

Для 2^w-1 різних ненулевих вхідних послідовностей довжини w r-вимірна ЛПС може сформувати 2^r-1 різних хеш-функцій довжини n. Кожній хеш-функції, таким чином, відповідає $2^{w-r}-1$ однакових вхідних послідовностей. Звідси, при умові рівноймовірності вхідних послідовностей, ймовірність виникнення колізії дорівнює

$$p_0=\frac{2^{w-r}-1}{2^w-1}\approx 2^{-r}.$$

При значеннях $r\geq 32$ при відсутності навмисного спотворення вхідного повідомлення ймовірність виникнення колізій для зазначених хеш-функцій на практиці дуже мала.

За визначенням, одностороння функція – це функція, що ефективно обчислюється, для задачі інвертування якої не існує швидких алгоритмів. В [7] доведено, що криптостійкі псевдовипадкові генератори існують тоді і тільки тоді, коли існують односторонні функції. Відомо також, що r-вимірна ЛПС, яка реалізує функції автоматних переходів, буде генератором псевдовипадкових чисел, якщо відповідний їй породжувальний поліном є примітивним. Така ЛПС буде генерувати послідовність символів періоду 2^r-1 (M-послідовність), яка при великих r ($r\geq 32$) практично не відрізняється від випадкової послідовності. Отже, функція автоматних переходів ЛПС, для примітивного породжувального полінома є односторонньою функцією.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. https://m.day.kyiv.ua/uk/article/ekonomika/didzhytalizaciya-ce-lyshe-pochatok
2. Лоран Лелу. Блокчейн от А до Я. Все о технологии десятилетия. — М.: Эксмо, 2018. — 256 с.
3. https://ru.bitcoinwiki.org/wiki/SHA-256.
4. Поточные шифры / [А. В. Асосков, М. А. Иванов, А. А. Мирский и др.]. – М. : КУДИЦ-ОБРАЗ, 2003. – 336 с.
5. Семеренко В. П. Теорія циклічних кодів на основі автоматних моделей : монографія. Вінниця : ВНТУ, 2015. – 444 с.
6. Ємець В., МельникА., Попович Р. Сучасна криптографія. Основні поняття. – Львів: БаК, 2003. – 144 с.
7. Impagliazzo R. Pseudo-random generation from one-way functions / R. Impagliazzo, L. Levin, M. Luby // Proc. 21st Annu. ACM Symp. on Theory of Computing. – 1989. – P. 12–24.

Василь Петрович Семеренко – канд. техн. наук, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця, e-mail: *vasilsemerenko@gmail.com*

Артур Сергійович Коробов – студент групи 2КІ-16б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця. e-mail: *gigabyte4gb@gmail.com*

Vasyl P. Semerenko – PhD, Associate Professor, Department of computer technique, Vinnytsia National Technical University, Vinnytsia, e-mail: *vasilsemerenko@gmail.com*

Artur S. Korobov – student, Department of computer technique, Vinnytsia National Technical University, Vinnytsia. e-mail: *gigabyte4gb@gmail.com*