УДК 004.056
DOI https://doi.org/10.32838/TNU-2663-5941/2020.6-1/11

Довжик Д.В.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Потапова К.Р.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

ВИКОРИСТАННЯ НАЦІОНАЛЬНИХ ЗАСОБІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ШИФРУВАННЯ БЛОКІВ БЛОКЧЕЙНУ

Стаття присвячена аналізу національних стандартів шифрування даних для використання у технології блокчейн. Blockchain (chain of block) – це розподілена база даних, у якій пристрої зберігання даних не підключені до загального сервера. Вона зберігає постійно зростаючий список упорядкованих записів, званих блоками, що спеціальним чином шифруються і зберігаються на всіх вузлах мережі в одному і тому самому вигляді. Ця технологія була винайдена і розроблена Сатоші Накамото у 2008 р. Спочатку блокчейн існував як основна частина цифрової валюти – Bitcoin, але згодом цю технологію почали використовувати і в інших галузях. Позитивні якості системи сприяли її подальшому проникненню в економіку, і зараз блокчейн застосовують у банківській сфері, державному управлінні, юриспруденції та інших сферах. Дедалі популярнішим стає використання технології блокчейн для задач, у яких надійність і захищеність даних є основними критеріями. У роботі розглянута структура блоку блокчейну та поняття електронно-цифрового підпису, що використовується для криптографічного перетворення даних блоку і забезпечує їхню цілісність та ідентифікацію автора. Електронно-цифровий підпис ґрунтується на використанні алгоритму шифрування даних і функції гешування. Будь-яке програмне забезпечення, котре займається шифруванням інформації (особливо користувацької), повинне відповідати державним стандартам. Тому в роботі розглянута функція гешування Купина, визначена у національному стандарті криптографічного захисту інформації ДСТУ 7564:2014, та алгоритм симетричного блокового перетворення Калина, визначений у стандарті ДСТУ 7624:2014. Разом вони можуть використовуватися для гешування блоку у блокчейн-технологіях із метою розробки державних блокчейн-систем, придатних для захисту інформації у межах нашої країни.

Ключові слова: *блокчейн, захист інформації, функція гешування, шифрування, криптографічне перетворення, електронний цифровий підпис, блочний симетричний шифр.*

Постановка проблеми. Нині в усьому світі активно досліджується технологія блокчейн (Blockchain), а саме переведення на систему блокчейну державних реєстрів (зокрема державної реєстрації прав на нерухоме майно), нотаріальної діяльності, зберігання державних даних, проведення земельних аукціонів, електронного майданчика торгівлі арештованим майном (СЕТАМ), Державного земельного кадастру, банківської сфери, проведення голосування та ін. Серед галузей, де насамперед планується використання системи блокчейн, – держреєстри, ЖКГ, соціальне страхування, охорона здоров'я й енергетика.

Водночас відсутність чіткого закріплення цієї категорії в національному законодавстві свідчить про необхідність її дослідження. Відсутність законодавчої бази також тягне за собою безліч сумнівів учасників ринку. Для того, щоб компанії довіряли новим технологіям, вони повинні відповідати стандартам, як мінімум державним.

Блокчейн (chain of block) – це розподілена база даних, у якій пристрої зберігання даних не підключені до загального сервера. Вона зберігає постійно зростаючий список упорядкованих записів, званих блоками, що спеціальним чином шифруються і зберігаються на всіх вузлах мережі в одному і тому самому вигляді. Кожен блок містить мітку часу та посилання на попередній блок геш-дерева. Така розподілена база даних закладена в основу крипто-валюти Біткоїн та інших, де слугує бухгалтерською книгою для всіх операцій [1].

Саме етап шифрування блоків вимагає використання криптографічних алгоритмів, які можуть вирішити такі проблеми, як безпека, висока доступність і швидкість виконання транзакцій. Ці криптографічні алгоритми повинні відповідати стандартам криптографічного захисту інформації в Україні для можливості використання у державних структурах.

Аналіз останніх досліджень і публікацій. Концепція першого блокчейну була розроблена

у 2008 р. людиною (або групою людей), відомою як Сатоши Накамото. Було описано Біткоїн – протокол електронних платежів для однорангової мережі (peer-to-peer network, P2P). Цей протокол базується на функції гешування SHA-256 (Secure Hash Algorithm), що є розробкою Агентства національної безпеки США й увійшла у стандарт RFC 4634 [2] «Безпечні геш-алгоритми США (SHA і HMAC-SHA)», що з'явився у 2006 р. Нині геш-функція SHA-256 є найпоширенішою у використанні для реалізації блокчейн-технології. Також відомим алгоритмом гешування є MD5 (Message Digest 5), розроблений у 1991 р. та описаний в американському стандарті RFC 1321 [3]. У 2009 р. підрозділ Національного управління кібербезпеки США рекомендував відмовитися від застосування цього алгоритму через виявлені властивості. Відповідний документ RFC 6151 «Зауваження щодо безпеки MD5 Message-Digest та HMAC-MD5 алгоритмів» було опубліковано в березні 2011 р., що визнає алгоритм гешування MD5 небезпечним і рекомендує відмовитися від його використання [4]. У 2020 р. MD5 все ще широко використовується, незважаючи на свої вразливості.

В Україні майже двадцять років як основна криптографічна геш-функція використовувався міждержавний стандарт ДСТУ ГОСТ 34.311-95 (російський ГОСТ Р 34.11-94) [5]. Однак у 2008 р. стали відомі теоретичні криптоаналітичні атаки [6], що унеможливило його подальше використання попри забезпечення практичної стійкості. До того ж ДСТУ ГОСТ 34.311-95 не відповідає сучасним вимогам із погляду швидкодії реалізації на сучасних програмних платформах загального призначення. На заміну застарілому стандарту розроблена геш-функція Купина, яка введена у дію у 2014 р. та широко використовується для забезпечення криптографічного захисту на національному рівні.

Купина є криптографічною геш-функцією, визначеною національним стандартом ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування» [7]. Цей стандарт прийнятий наказом Мінекономрозвитку від 2 грудня 2014 р. № 1431.

Постановка завдання. Метою статті є розгляд теоретичних основ технології блокчейн та аналіз можливості застосування національних стандартів криптографічного захисту інформації для основних компонентів блокчейну: алгоритму шифрування даних у блоці та функції гешування блоку.

Виклад основного матеріалу дослідження. Блокчейн – це один із видів розподіленого зберігання даних, що використовує три раніше відомі технології: однорангові мережі, шифрування і бази даних. База даних є ланцюжком блоків, який спеціальним чином шифрується і зберігається на всіх вузлах мережі в одному і тому самому вигляді. Одним із базисів блокчейну є зв'язки між блоками за рахунок криптографії, тому, як наслідок, практично неможливо підробити інформацію у блоках.

Технологія блокчейн включає в себе 5 етапів:

1) Запит на здійснення транзакції в мережу. Користувач, котрий бажає відправити дані іншому користувачеві, формує транзакцію і відправляє її в мережу. Система створює унікальний ключ для доступу до відправлених даних. Цей ключ відправник передає отримувачу.

2) Обробка транзакції та складання з неї нового блоку. Дані про транзакції обробляються системою і формуються у блок, що містить зашифровану від інших користувачів інформацію.

3) Розсилка нового блоку всім учасникам. Система знаходиться одночасно у всіх користувачів, причому копії постійно перевіряються на відповідність раніше внесеній у базу інформації. Нові дані одночасно передаються в усі екземпляри бази для перевірки.

4) Внесення нового блоку в усі екземпляри блокчейну. Якщо в ході перевірки блок буде визнаний відповідним, він внесеться в усі копії та доповнить вже наявний ланцюжок. Система дасть унікальний цифровий підпис, за яким новий блок можна буде відстежити. Якщо система визнає блок неправильним, то він не вноситься в інші копії, тож транзакція не відбудеться.

5) Завершення операції. Після того, як новий блок буде створено, одержувач зможе отримати відправлену інформацію, скориставшись переданим платником унікальним ключем.

У найпростішому вигляді база даних (БД) є ланцюжком блоків, яка може бути представлена у вигляді файлу формату JSON.

Структура блоку:

– кожен блок складається з адреси, дати та часу створення, гешу і списку транзакцій (рис. 1);

– адреса – публічний ключ, що генерується алгоритмом шифрування на основі вигаданого користувачем приватного ключа;

– дата і час – час створення транзакції (блоку);

– геш (сполучний) – обчислюється за допомогою функції гешування від адреси попереднього блоку і суми гешів всіх транзакцій поточного блоку. Геш є сполучним, тому що при його обчисленні враховується адреса попереднього блоку;

– інформація – повідомлення, сума грошей (криптовалюта), документи, історія хвороб, програмний код (смарт контракти) та ін.

Електронний цифровий підпис. Щоб інформацію всередині транзакцій неможливо було підробити, кожна транзакція всередині блоку підписується електронним цифровим підписом (ЕЦП).

Електронно-цифровий підпис – це послідовність байтів, яка формується шляхом перетворення інформації за криптографічним алгоритмом і призначена для перевірки авторства електронного документа.

ЕЦП ґрунтується на використанні блочного шифрування та геш-функціях.

Алгоритм створення підпису інформації (документа). Для створення підпису необхідні:

– алгоритм шифрування (блочний симетричний шифр Калина);

– геш-функція (криптографічна геш-функція Купина);

– інформація, що повинна бути передана.

Стандарт ДСТУ 7624:2014 [8] визначає сучасний блоковий шифр Калина та режими його роботи для приховування смислового вмісту і запобігання несанкціонованої модифікації повідомлень. Шифр є гнучким і підтримує розмір блоку і довжину ключа аж до 512 бітів. Це єдиний у світі стандарт блочного шифрування, що підтримує такий рівень безпеки. Для порівняння, широко поширений AES забезпечує максимальну довжину ключа 256 біт. Водночас у програмній реалізації на більшості сучасних 64-бітових настільних і серверних платформ за однакових довжин ключів Калина має більш високу продуктивність, ніж AES.

ДСТУ 7624:2014 задає десять режимів роботи блокового шифру. Міжнародний стандарт ISO/IEC10116 має тільки шість режимів (вони є і в національному стандарті України). Додаткові режими надають більше можливостей українським розробникам засобів криптографічного захисту інформації порівняно з колегами із країн регіону та всієї Європи загалом.

Шифр Калина – високостійкий і швидкий симетричний шифр, орієнтований на сучасні продуктивні апаратні платформи.

У стандарті ДСТУ 7564:2014 визначена функція гешування Купина, що забезпечує високостійке і гнучке криптографічне перетворення. Вона використовується і як незалежний стандарт при забезпеченні цілісності, і як додаткове перетворення у складі цифрового підпису.

Геш-функція Купина має ключову властивість, яка відрізняє її від інших алгоритмів формування гешу. Купина може бути використана в технологіях блокчейн, що враховують динамічність геш-функції, і динамічною є не тільки сама функція, а й довжина виходу геш-функції.

Динамічність виходу геш-функції не впливає на кількість транзакцій, які входять у блок, у разі використання динамічного розміру блоку, але покращує криптографічні властивості блокчейну, такі як криптостійкість.

Для прикладу, довжина виходу геш-функції SHA-2, що зараз використовується у Bitcoin, передбачає тільки 4 можливі значення довжини виходу, а саме 224, 256, 384 або 512 біт, тоді як Купина передбачає 64 можливі довжини виходу: {8, 16, ... , 256, 264, ... , 504, 512}.

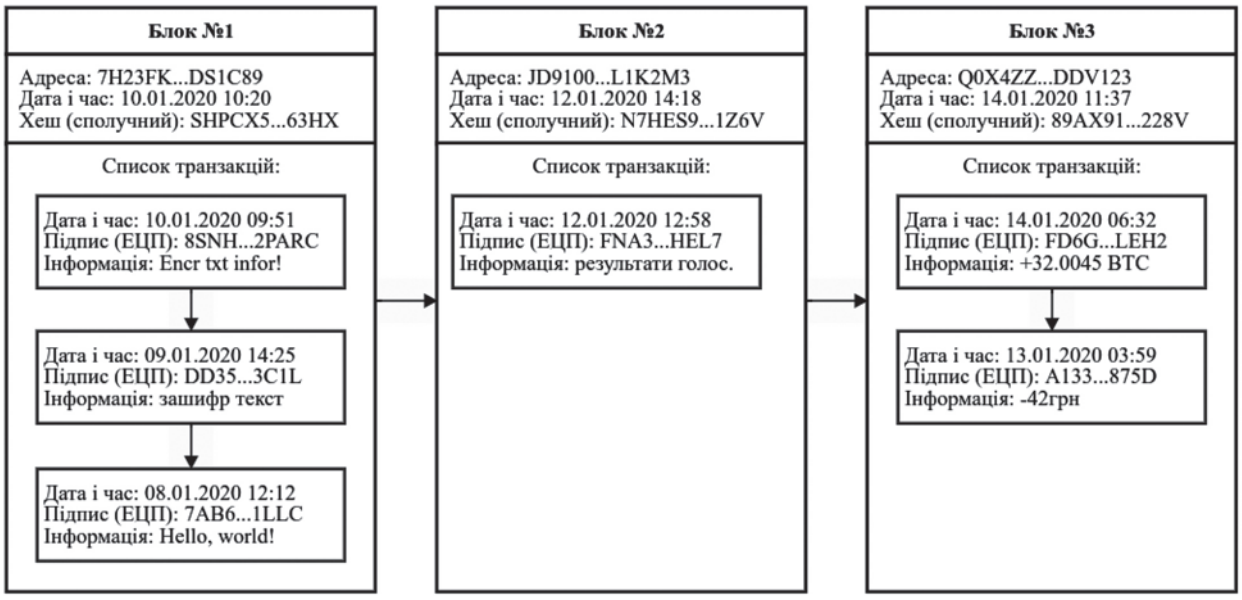

Рис. 1. Приклад системи блокчейн із трьох блоків

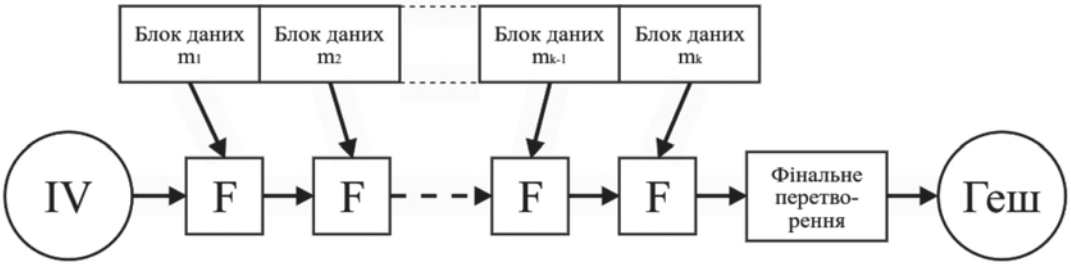

Рис. 2. Загальна структурна схема геш-функції

Функція Купина – це ітеративна геш-функція, заснована на архітектурі Меркле-Дамгора [9]. Вона використовує функцію стиснення Девіса-Мейєра, побудовану на основі конструкції блокового шифру Івена-Мансура [10]. Геш-функція Купина побудована на функції стиснення, що складається із двох фіксованих перестановок, структура яких запозичена у шифру «Калина», та за структурою є підстановлювально-перестановочною мережею, яка відповідає стратегії дизайну AES. Результатом роботи геш-функції є бітова послідовність від 8 до 512 біт. Варіант, що повертає n біт, позначається як Купина-n. Основними режимами роботи функції гешування, рекомендованими до застосування, є Купина-256, Купина-384 і Купина-512.

Основні характеристики конструкції геш-функції Купина. На вхід функції гешування подається повідомлення M як бітова послідовність довжини N. Далі повідомлення завжди доповнюється за певними правилами до довжини, кратної розміру блоку, та поділяється на блоки $m_1, m_2, \ldots, m_k$ довжиною l біт кожен, де l визначається відповідно до розміру геш-значення n, $n \in \{8 \cdot s \mid s = 1, 2, \ldots, 64\}$:

$$l = \begin{cases} 512 \text{ для } 8 \leqslant n \leqslant 256, \\ 1024 \text{ для } 256 < n \leqslant 512. \end{cases}$$

Максимальна довжина повідомлення, що може бути оброблене, становить $(2^{96} – 1)$ біт.

Обчислення геш-значення відбувається за такою ітеративною процедурою [11]:

$$h_0 = IV,$$
$$h_v = T_l^{\oplus}(h_{v-1} \oplus m_v) \oplus T_l^{+}(m_v) \oplus h_{v-1}, \; v = 1, 2, \ldots, k,$$
$$H(IV, M) = R_{l,n}(T_l^{\oplus}(h_k) \oplus h_k),$$

де IV – вектор ініціалізації довжиною l біт, $T_l^{\oplus}$, T_l^{+} – бієктивні перетворення, що виконують відображення вхідного блоку довжиною l біт у вихідний такої самої довжини, $R_{l,n}(x)$ – функція, що повертає n старших біт із вхідного блоку x довжиною l біт ($n < 1$), де результат записується в молодші n біт обчисленого значення. На рис. 2 наведена структурна схема геш-функції Купина у загальному вигляді.

Як видно, функція стиснення F використовує дві перестановки $T_l^{\oplus}$ та T_l^{+} і обчислюється таким чином:

$F(m, h) = T_1^{\oplus}(h \oplus \mathrm{m}) \oplus T_1^{+}(m) \oplus h$.

Тоді на k-му кроці $h_k = F(m_k, h_{k-1})$, причому $h_0 = IV$. Графічне представлення структури функції стиснення наведено на рис. 3.

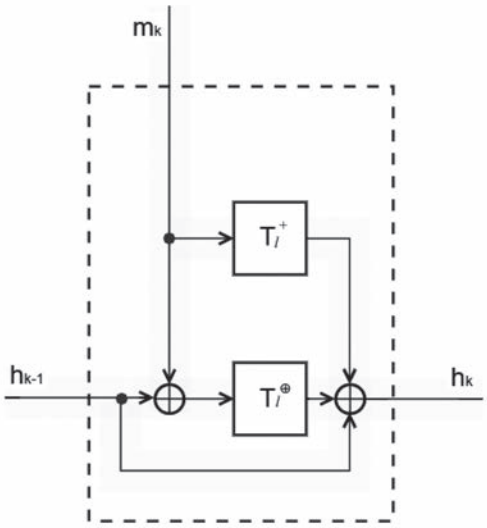

Рис. 3. Структура функції стиснення геш-функції Купина

Купина та Калина уніфіковані, тобто використовують єдиний набір підстановок і матриць лінійного перетворення, що додатково збільшує ефективність систем криптографічного захисту на їх основі. Купина, як і Калина використовує підхід доказової стійкості (*provable security*) при обґрунтуванні властивостей, що є додатковою перевагою ДСТУ 7564 над SHA-256, де така властивість відсутня. Водночас забезпечення доказової стійкості призводить до зниження швидкості перетворень Купини порівняно із SHA-256.

Висновки. Відразу після введення в дію стандартів Купина і Калина були опубліковані англійською мовою і представлені на міжна-

родних конференціях за межами України. Були отримані незалежні результати дослідників із Канади, США, Австрії, Індії та інших країн, що підтверджують стійкість криптографічних перетворень. ДСТУ 7624 і ДСТУ 7564 були включені до складу програмних бібліотек, які розробляються за межами України, наприклад, Crypto++. Тому можна розглянути питання впровадження блочного симетричного шифру Калина та геш-функції Купина, описані у національних стандартах криптографічного захисту інформації, у блокчейн-технологіях, з метою розробки державних блокчейн-систем, придатних для захисту інформації у межах нашої країни.

Список літератури:

1. Dovzhyk D., Potapova K., Online-voting system based on blockchain technology. *Priority directions of science and technology development* : Abstract of the 2-nd International scientific and practical conference. SPC "Sci-conf.com.ua". Kyiv, Ukraine. 2020. P. 248–249.
2. Стандарт RFC-4634 «Безпечні геш-алгоритми США (SHA і HMAC-SHA)». URL: https://tools.ietf.org/html/rfc4634.
3. The MD5 Message-Digest Algorithm. URL: https://tools.ietf.org/html/rfc1321.
4. Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms. URL: https://tools.ietf.org/html/rfc6151.
5. ГОСТ Р 34.11–94. Информационная технология. Криптографическая защита информации. Функция хэширования. Введ. 01–01–1995. Москва, 1994. 20 с.
6. Mendel F., Pramstaller N., Rechberger Ch., et.al. Cryptanalysis of GOST hash function: report. *Advances in Cryptology*. 2008. URL: https://iacr.org/archive/crypto2008/51570163/51570163.pdf.
7. Держспецзв'язку впроваджує нові стандарти криптографічного захисту інформації. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=120158&cat_id=119123.
8. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. Введ. 01–07–2015. Київ : Мінекономрозвитку України, 2015.
9. Merkle R.C. Secrecy, authentication, and public key systems, Department of Electrical Engineering, Stanford University, 1979. P. 13–15.
10. Black J., Rogaway P., Shrimpton T. Blak-box analysis of the block-cipher-based hash-function constructions from pgv. *Advances in Cryptology*. August 18–22, 2002. Proceedings. Vol. 2442. *Lecture Notes in Computer Science*. 2002. P. 320–335.
11. ДСТУ 7564:2014. Інформаційні технології. Криптографічний захист інформації. Функція гешування. Введ. 01–04–2015. Київ : Мінекономрозвитку України, 2015.

Dovzhyk D.V., Potapova K.R. USE OF NATIONAL FACILITIES OF CRYPTOGRAPHIC PROTECTION OF INFORMATION FOR ENCRYPTION OF BLOCKCHAIN BLOCKS

The article is devoted to the analysis of national data encryption standards for use in blockchain technology. Blockchain (chain of block) it is a distributed database in which storage devices are not connected to a shared server. This database maintains an ever-growing list of ordered records, called blocks, that are specially encrypted and stored on all network nodes in the same form. This technology was invented and developed by Satoshi Nakamoto in 2008. Initially, the blockchain existed as the main part of the digital currency – Bitcoin, but later this technology began to be used in other industries. The positive qualities of the system contributed to its further penetration into the economy and now the blockchain is used in banking, public administration, jurisprudence and other areas. The use of blockchain technology for tasks in which reliability and data security are the main criteria is becoming increasingly popular. The paper considers the structure of the blockchain block and the concept of electronic-digital signature, which is used for cryptographic transformation of block data and ensures their integrity and author identification. The electronic digital signature is based on the use of a data encryption algorithm and a hashing function. Any software that encrypts information (especially user information) must comply with national standards. Therefore, the paper considers the Kupyna hashing function, which is defined in the national standard of cryptographic information protection NSTU 7564:2014, and the Kalyna symmetric block transformation algorithm, defined in the standard NSTU 7624:2014. Together, they can be used for blockchain block hashing, in order to develop state blockchain systems suitable for information protection within our country.

Key words: *blockchain, information protection, hashing function, encryption, cryptographic transformation, electronic digital signature, symmetric block cipher.*