УДК 004.056:004.424.47

Ю. В. Баришев
В. С. Ланова

АНАЛІЗ ГЕШ-ФУНКЦІЙ ДЛЯ ЗАХИСТУ ЦІЛІСНОСТІ ЧУТЛИВИХ ДАНИХ НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Вінницький національний технічний університет;

Анотація *У роботі наведено актуальність захисту чутливих даних із використанням технології блокчейн. Проаналізовано сучасні геш-функції, основну увагу приділено тим геш-функціями, які природним чином реалізовані в найбільших блокчейнах. Наведено результати аналізу та порівняльні оцінки геш-функцій для вибору оптимальної для реалізації смарт-контрактів у технології блокчейн. На основі цих результатів порівняльного аналізу наведено приклад обґрунтування доцільності використання геш-функцій для захисту цілісності на прикладі блокчейну Ethereum.*

Ключові слова: геш-функції, блокчейн, децентралізовані системи, чутливі дані, кібербезпека.

Abstract *The work shows the relevance of protecting sensitive data using blockchain technology. Modern hash functions are analyzed, the main attention is paid to those hash functions that are naturally implemented in the largest blockchains. The results of the analysis and comparative evaluations of hash functions for choosing the optimal one for the implementation of smart contracts in blockchain technology are presented. Based on these results of the comparative analysis, an example of substantiating the feasibility of using hash functions for integrity protection is provided using the example of the Ethereum blockchain.*

Keywords: hash functions, blockchain, decentralized systems, sensitive data, cyber security.

Вступ

На сьогоднішній день постає актуальна задача в забезпеченні захисту чутливих даних. Пошкодження або модифікація цих даних може призвести до серйозних наслідків, таких як втрата розголошення персональних даних чи недоступність критично важливих сервісів.

Застосування традиційних методів захисту часто не гарантує стійкість у сучасних умовах. Технологія блокчейн є інструментом для забезпечення підвищеного рівня цілісності даних завдяки децентралізованій природі системі зберігання даних та їх копіювання [1]. Однією зі складових цієї технології є використання криптографічних функцій гешування, які значно впливають на рівень безпеки, який можна досягти на основі блокчейну.

Геш-функції виконують роль інструментів для забезпечення цілісності даних, перетворюючи інформацію в унікальний геш-код. Цей геш-код служить основою для перевірки автентичності даних. При розробці технологій блокчейн вибір конкретної геш-функції визначається основними критеріями, такими як криптографічна стійкість, швидкодія та інші умови.

Метою цього дослідження є покращення захисту цілісності чутливих даних, шляхом вибору найбільш релевантної геш-функції для реалізації смарт-контрактів, які в подальшому взаємодіятимуть із чутливими даними та захищатимуть їх цілісність та неможливість модифікації.

Для досягнення мети необхідно розв’язати такі задачі:

– проаналізувати геш-функції, які є релевантними для технології блокчейн;
– виконати порівняльний аналіз;
– зробити відповідні висновки.

Результати дослідження

В блокчейні геш-функції використовуються для контролю цілісності повідомлень, що передаються мережею [1]. Для контролю цілісності даних, геш-функція повинна задовольняти таким вимогам:

– стійкість до колізій;
– стійкість до знаходження прообразу;
– стійкість до атаки пошуку другого прообразу;

– висока швидкодія;
– допустимий розмір гешу в межах від 224 до 512 біт;
– незначна ресурсоємність.

Правильний вибір геш-функції забезпечить високий рівень безпеки чутливих даних.

У ході дослідження було проаналізовано геш-функції, які за своїми характеристиками можуть використовуватись в технології блокчейн або вже там використовуються. Серед них такі:

– BLAKE2 [2].
– BLAKE3 [3].
– Gröstl [4, 5].
– Купина [6].
– Keccak [7].
– Skein [8].
– SHA-256 [9].

BLAKE 2 – це набір криптографічних геш-функцій, визначених у RFC 7693.

Сім'я BLAKE2 складається з двох геш-функцій, і обидві з них забезпечують безпеку, яка перевершує SHA-2. BLAKE2B оптимізований для 64-бітних платформ, тоді як BLAKE2S – для платформ від 8-бітних до 32-бітних. Блокчейн Polkadot використовує BLAKE2B, як свій алгоритм гешування. Цей алгоритм гешування є стійким до атак та маловитратним по ресурсам [2].

Геш-функція BLAKE3 [3] є швидшою за BLAKE2. Алгоритм був розроблений відомими криптографами та продовжує розвиток алгоритму BLAKE2, використовуючи механізм Bao для кодування дерева блокчейну. Геш-функція призначена для застосувань, таких як перевірка цілісності файлів, автентифікація повідомлень та генерація даних для криптографічних цифрових підписів. Немає ефективних атак в бік цього алгоритму, тому його можна вважати стійким. Реалізація BLAKE вимагає низьких ресурсів і є швидкою, як в програмному, так і в апаратному середовищі. Одним із недоліків є лише одна розмірність гешу та блоку, на відміну від інших, вживаних в блокчейні, геш-функцій.

Алгоритм Gröstl спеціально розроблений для участі в конкурсі криптографічних функцій SHA-3 командою криптографів з Данського технічного університету [4]. Застосовується в проєкті криптовалюти Verge. Функція ущільнення Gröstl складається з двох фіксованих перестановок P і Q, структура яких запозичена у шифру AES. Зокрема, використовується такий же S-блок. Результат роботи геш-функції може мати довжину від 8 до 512 біт з кроком 8 біт. Варіант, який повертає n біт, називається Gröstl-n [5]. Варто зазначити, що є нестійким до атак «напіввільний початок» та має низьку швидкодію, порівняно з іншими геш-функціями.

Ітеративна геш-функція «Купина», яка представлена в ДСТУ 7564:2014 є сімейством криптографічних геш-функцій, розроблених в Україні в «Інституті інформаційних технологій», який введено в дію від 2 грудня 2014 року, та чинний від 1 квітня 2015 року [6]. Сімейство геш-функцій «Купина» включає в себе декілька різновидів, таких як Купина-256, Купина-384 і Купина-512. Ці різновиди характеризуються вихідною довжиною гешу (256, 384 або 512 біт) і різними параметрами безпеки. Зокрема, функція «Купина-256» рекомендується для більшості сценаріїв застосування, де необхідна висока криптографічна стійкість. На сьогоднішній день не використовується в технології блокчейн, однак за своїми параметрами, в майбутньому, може бути використаною в децентралізованих системах зберігання даних. Серед недоліків можна відзначити малу кількість раундів, у порівнянні, наприклад, з Keccak, який має 24, Купина має 10 або 14 раундів, в залежності від розміру гешу.

Алгоритм Keccak складається з 24 раундів. Використовує конструкцію «губка» і блок-підстановку. Підстановка може бути реалізована на основі 5-бітових S-блоків або на комбінації лінійної і нелінійної операціях змішування. Keccak дозволяє генерувати довільну кількість вихідних бітів. Є стійким до атак: на сьогоднішній день ще не було зареєстровано випадків колізій, які пов’язані з цим алгоритмом. Для захисту від атак, необхідно 18 раундів. Пропускна здатність цього алгоритму є найвищою серед усіх алгоритмів-фіналістів конкурсу. Використовується, як основна геш-функція в блокчейні Ethereum [7].

Геш-функція Skein є універсальним криптографічним примітивом, побудованим на основі блочного шифру Threefish, і використовується в режимі UBI-гешування. Конструкція алгоритму гешування: Matyas–Meyer–Oseas. Основна ідея розробки полягала в оптимізації для мінімального використання пам'яті, забезпеченні криптографічно безпечного гешування невеликих повідомлень, стійкості до всіх відомих атак на геш-функції. Skein захищена від нових видів атак на геш-функції – підбору подовжених повідомлень і псевдоколізій. Має високу швидкодію, значення є в 2,5 рази більшим за раніше

згаданий Keccak [7].

SHA-256 (Безпечний Геш-Алгоритм-256) – це алгоритм видобутку та геш-функція, які використовуються в мережі Bitcoin для підтвердження транзакцій та формування публічних адрес.

Геш-функція SHA-256 забезпечує додатковий рівень безпеки для блокчейну Bitcoin, оскільки вона створює цифрові підписи при ініціації транзакцій. Ці цифрові підписи використовуються для захисту чутливих даних, забезпечуючи можливість перевірки цілісності даних без розголошення вмісту. Вирізняється своєю стійкістю до атак [9].

Доцільно буде побудувати порівняльну таблицю вищезгаданих алгоритмів гешування (табл. 1).

Таблиця 1 – Порівняння алгоритмів гешування

Назва алгоритму	Конструкція	Розмір гешу, біт	К-ть раундів	Стійкість до атак	Швидкодія, Мбіт/с	Вимогливість до ресурсів	Застосування
BLAKE2	Bao tree	128,256	12 (BLAKE2B), 10(BLAKE2S)	Не зафіксовано атак	-	Низька	Використовується в криптовалюті Blakecoin Блокчейн Polkadot використовує BLAKE2B, як свій алгоритм гешування.
BLAKE3	Bao tree	256	12	Не зафіксовані атаки та колізії	264.93	Помірна	Для кодування дерева блокчейну Bitcoin
Gröstl	Wide Trail design strategy	224, 256, 384, 512	10, 14	Нестійкий до атак "напіввільний початок"	118.46, 124.28, 85.65, 85.24	Висока	Застосовується в проєкті криптовалюти Verge
Купина	Davies-Meyer compression function based on Even-Mansour scheme	256, 384, 512	10, 14, 14	Стійка до атак, колізій не зафіксовано	-, 134.85, 81.63	Низька	Є українським стандартом
Keccak	Криптографічна губка Sponge	224, 256, 384, 512	24	Стійкий до атак	274.07, 268.87, 214.70, 149.28	Помірна	В блокчейні Ethereum
Skein	Matyas–Meyer–Oseas	256, 512, 1024	72, 72,80	Захищений від атак підбору подовжених повідомлень і псевдоколізій	643.69, 645.67, -	Невисока	Одна з відомих криптовалют, яка видобувається на алгоритмі Skein через майнінг, є DigiByte (DGB).
SHA-256	Merkle–Damgård	256	64	Є стійкою до колізій, однак був випадок атаки 41 кроку	192.54	Помірна	Використовується, як основна геш-функція блокчейну Bitcoin

Як видно з таблиці 1 певну перевагу на сьогодні для використання при побудові блокчейн мереж мають Skein та Keccak. Зазначені функції гешування є стійкими проти класичного криптоаналізу, в тому числі: до знаходження прообразу; до знаходження другого прообразу, до виникнення чи створення колізій та вирізняються високими показниками швидкодії [1].

Для забезпечення захисту цілісності чутливих даних доцільним є використання блокчейну Ethereum. Ethereum підтримує розробку різноманітних децентралізованих застосунків (DApps) на основі смарт-контрактів, що надає гнучкість для створення різноманітних рішень, що вимагають взаємодії з блокчейном. Стандартом для блокчейну Ethereum є геш-функція Keccak, яка з 2012 року вважається стандартом SHA-3.

Висновки

Таким чином для розв'язання цієї задачі найбільш релевантною геш-функцією буде Keccak, який на противагу іншим алгоритмам гешування є простим в реалізації.

Keccak розроблений так, щоб бути ефективним на різних платформах та в апаратному забезпеченні. Висока швидкість обчислень може бути важливою для застосувань, де важлива продуктивність.

Має гнучкість щодо розміру вихідного гешу та інших параметрів, що дозволяє його налаштовувати під конкретні вимоги застосування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Аналіз застосування фунції гешування у технології blockchain / П. В. Кравчук, І. Д. Горбенко, А. І. Пушкарьов // Прикладна радіоелектроніка – 2018. - Т. 17 - №3, 4. С. 147-151. – Режим доступу: https://nure.ua/wp-content/uploads/2018/Scientific_editions/are_2018_19.pdf (дата звернення: 07.03.2024).
2. BLAKE2 / J. Aumasson [et al.] // Information Security and Cryptography. – Berlin, Heidelberg, 2014. – P. 165–183. – Mode of access: https://doi.org/10.1007/978-3-662-44757-4_9 (accessed: 07.03.2024).
3. BLAKE3 a secure, fast and parallelizable cryptographic hash function.- Mode of access: https://www.linuxadictos.com/en/blake3-a-fast-and-parallelizable-secure-cryptographic-hash-function.html. (accessed: 07.03.2024).
4. Performance Analysis of Cryptographic Hash Functions Suitable for Use in Blockchain / Alexandr Kuznetsov [et al.] // International Journal of Computer Network and Information Security. – 2021. – Vol. 13, № 2. – P. 1–15. – Mode of access: https://doi.org/10.5815/ijcnis.2021.02.01 (accessed: 14.03.2024).
5. The study of cryptographic hashing algorithms used in modern blockchain systems [Electronic resource] / O. O. Кузнецов [et al.] // Radiotekhnika. – 2019. – Vol. 3, № 198. – P. 54–74. – Mode of access: https://doi.org/10.30837/rt.2019.3.198.05 (accessed: 14.03.2024).
6. ДСТУ ISO 7564:2014 Інформаційні технології. Криптографічний захист інформації. Функція гешування [Чинний від 2015-04-01] – Київ – 2015 - 39 с. (дата звернення: 07.03.2024).
7. Keccak / Guido Bertoni [et al.] // Advances in Cryptology – Eurocrypt 2013. – Berlin, Heidelberg, 2013. – P. 313–314. – Mode of access: https://doi.org/10.1007/978-3-642-38348-9_19 (accessed: 14.03.2024).
8. The Skein Hash Function Family. [Electronic resource]. – Access mode : https://www.schneier.com/wp-content/uploads/2015/01/skein.pdf (date of access: 07.03.2024).
9. SHA-256 Meaning. Mode of access: https://csrc.nist.gov/files/pubs/fips/180-2/final/docs/fips180-2.pdf (accessed: 07.03.2024).

Баришев Юрій Володимирович — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: yuriy.baryshev@vntu.edu.ua.

Ланова Владислава Сергіївна — студентка групи 1БС-20б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: lanovaia02y@gmail.com

Yurii Baryshev —PhD (eng), associated professor of information protection department, Vinnytsia National Technical University, Vinnytsia, email: yuriy.baryshev@vntu.edu.ua

Vladyslava Lanova — student of 1БС-20б group, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : lanovaia02y@gmail.com.