Технічні науки

УДК 004.4

Андрющенко Ірина Ігорівна

студентка кафедри ПІ

Харківського національного університету радіоелектроніки

Андрющенко Ирина Игоревна

студентка кафедры ПИ

Харьковского национального университета радиоэлектроники

Andriushchenko Iryna

Student of the Software Engineering Department

Kharkiv National University of Radioelectronics

ВИКОРИСТАННЯ ХЕШ-ФУНКЦІЇ У КРИПТОВАЛЮТАХ
ИСПОЛЬЗОВАНИЕ ХЕШ-ФУНКЦИИ В КРИПТОВАЛЮТАХ
HASH FUNCTION FOR USING IN CRYPTOCURRENCIES

Анотація. *Хеш-функції мають безліч властивостей, які роблять їх актуальними для використання в багатьох сучасних алгоритмах. У тому числі в основі роботи криптовалют є застосування хешування. У цій статті ми розглянемо аналіз роботи алгоритму SHA-256. А також цілі майнінгу та використання хеш-функцій для вирішення цього завдання.*

Ключові слова: *хеш-функція, блокчейн, криптовалюта, bitcoin, колізія.*

Аннотация. *Хеш-функции имеют множество свойств, которые делают их актуальные для использования во многих современных алгоритмов. В том числе в основе работы криптовалют лежит применение хеширования. В этой статье мы рассмотрим разбор работы алгоритма SHA-256. А также цели майнинга и использование хеш-функций для решения этой задачи.*

Ключевые слова: *хеш-функция, блокчейн, криптовалюта, bitcoin, коллизия.*

Summary. *Hash functions have many properties that make them relevant for use in many modern algorithms. In particular, the operation of cryptocurrencies is based on the use of hashing. In this article, we'll take a look at how the SHA-256 algorithm works. As well as the goals of mining and the use of hash functions to solve this problem.*

Key words: *hash-function, blockchain, cryptocurrency, bitcoin, collision.*

Кожен, хто цікавиться блокчейн або криптовалютами, напевно, чув термін хеш-функція, але не всі розуміють, як вони працюють і чому такі важливі. Тому в цій статті я спробую пояснити основи хеш-функцій і чому вони так широко використовуються в блокчейн.

Хеш-функція — це будь-яка детермінована функція, яка приймає вхідні дані довільної довжини, застосовують до цього входу математичну функцію та видає вихідні дані фіксованої довжини. Вихід хеш-функції називається дайджестом хешування. Блокчейни багато в чому покладаються на хеш-функції для генерації криптографічних ключів і хешування блоків транзакцій. Ми можемо краще зрозуміти хеш-функції, розуміючи їх властивості.

Загальні властивості:

- Відображення фіксованої довжини
- Детермінованість
- Ефективне обчислення

Криптографічні властивості:

- Стійкість прообразу
- Стійкість до колізій
- Ефект лавини

- Дружелюбність до головоломок

Після отримання вхідного параметра будь-якої довжини функція завжди генеруватиме вихід фіксованої довжини. Ця властивість дозволяє нам хешувати будь-який файл, будь то текстовий документ, зображення або навіть відеофайл, і отримати вихід такої ж довжини.

Для заданого входу вихід завжди буде однаковим. Отже, якщо передати хешу фразу «hello, world» за допомогою хеш-функції SHA-256, то скільки би разів ми не перераховували хеш, завжди отримуємо той самий вихід.

Хеш-функція має властивий лавинний ефект - важлива криптографічна властивість для шифрування, яка полягає в тому, що зміна значення малої кількості бітів у вхідному тексті або ключі веде до «лавинної» зміни значень вихідних бітів шифрованого тексту. Іншими словами, це залежність всіх вихідних бітів від кожного вхідного біта.

Хеші дружелюбні до головоломок, що в основному означає, що навіть якщо ви отримаєте початкові 200 байт із хешу довжиною 256 байтів, ви не зможете визначити наступні 56 байт з нього.

Для пояснення як працює найпоширеніший хеш-алгоритм SHA-256 можливо розділити весь процес на п'ять різних сегментів, як зазначено нижче:

Використання заповнювачів:

Додаємо деякі додаткові біти до повідомлення, так щоб довжина була точно на 64 біти менше кратної 512. Під час додавання перший біт має бути одиниця, а решта його має бути заповнена нулями.

Регулюємо довжина прокладки:

Можемо додати 64 біти даних зараз, щоб зробити кінцевий відкритий текст кратним 512. Ви можете обчислити ці 64 біти символів, застосувавши модуль до вихідного відкритого тексту без заповнення.

Ініціалізація буферів:

Вам потрібно ініціалізувати значення за замовчуванням для восьми буферів, які будуть використовуватися в раундах. Також потрібно зберігати 64 різні ключі в масиві від K[0] до K[63].

Функції стиснення:

Усе повідомлення розбивається на кілька блоків по 512 біт кожен. Кожен блок проводить 64 раундів операцій, причому вихідні дані кожного блоку служать вхідними для наступного. Хоча значення K[i] у всіх цих раундах попередньо ініціалізовано, W[i] — це ще один вхід, який розраховується окремо для кожного блоку, залежно від кількості ітерацій, що обробляються на даний момент.

Вихід:

З кожною ітерацією кінцевий вихід блоку служить входом для наступного блоку. Весь цикл повторюється, поки ви не досягнете останнього 512-бітового блоку, а потім ви вважаєте його результат остаточним дайджестом хешування. Цей дайджест буде мати довжину 256 біт відповідно до назви цього алгоритму.

Хеш-функції не були розроблені для криптовалют, але вони дуже широко використовуються у провідних криптовалютах, насамперед через властивості, про які я згадував вище. Ці властивості забезпечують безпечні транзакції через блокчейн.

Блокчейн спочатку був розроблений для інформаційної безпеки. Найпростішим варіантом використання для цього є зберігання паролів, для входу на будь-який веб-сайт, ми вводимо своє ім'я користувача та пароль, але пароль ніколи не зберігається на сервері, тому цікаве завдання полягає в тому, як ми перевіряємо, чи введений пароль правильний, чи ні, ось тут і з'являються хеш-функції. Ми хешуємо пароль і зберігаємо хеш-дайджест і перевіряємо його замість оригінального пароля.

Bitcoin використовує SHA-256 і RIPEMD160, тоді як Ethereum використовує хеш-функцію Keccak-256. В основному вони використовуються для генерації відкритих ключів і блокування хешування.

Хешування блоків є основною концепцією майнінгу біткойнів. У цьому процесі блок непідтверджених транзакцій передається до хеш-функції і створюється дайджест хешування. Майнер використовує цей хеш-дайджест і додає деякі вхідні дані зі свого боку, щоб створити вихід, який містить певну кількість провідних нулів, наразі кількість провідних нулів становить 20. Генерування цих провідних нулів вимагає величезної обчислювальної потужності і, отже, видобуток біткойнів за допомогою доказу виконаної роботи (Proof-Of-Work) дуже дорогий спосіб і споживає велику кількість електроенергії.

Майнери використовують потужні комп'ютери, обчислювальна потужність яких використовується для рішення складних математичних головоломок. Майнінг також забезпечує проходження транзакцій, в обмін отримаючи можливість карбування нових біткоїнів, як винагороду за невелику частину транзакцій біткойнів.

Майнінг одного біткоіна займає близько 10 хвилин. Однак це передбачає ідеальне обладнання та програмне забезпечення, яке може дозволити собі не багато користувачів. Більш розумна оцінка для більшості користувачів, які мають системи з продуктивними відеокартами, — це 30 днів.

Оскільки майнінг може забезпечити солідний потік доходу, кількість людей – також майнерів – бажаючих керувати потужними машинами, щоб отримати невеликий прибуток від кожної транзакції біткойн, яку вони допомагають схвалити, різко зросла.

Література

1. Криптографическая защита информации : учебное пособие / А.В. Яковлев, А.А. Безбогов, В.В. Родин, В.Н. Шамкин. Тамбов : Изд-во Тамб. гос. техн. ун-та, 2006. 140 с.
2. Аграновский А. В., Хади Р. А. Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р. А. Хади. 2002. ("СОЛОН-Р").
3. Paul C. van Oorschot. Handbook of Applied Cryptography / Paul C. van Oorschot. 780 с.
4. Поппер Н.. Цифровое золото: невероятная история Биткойна, или как идеалисты и бизнесмены изобретают деньги заново / Н. Поппер. 2016. 368 с.
5. Винья П. Эпоха криптовалют Как биткоин и блокчейн меняют мировой экономический порядок / П. Винья. М.: Кейси., 2017. 432 с.