ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

DOI: 10.18372/2225-5036.25.13745

КРИПТОГРАФІЧНІ АЛГОРИТМИ ТА ОСОБЛИВОСТІ ЇХ ВИКОРИСТАННЯ В БЛОКЧЕЙН-СИСТЕМАХ

Ірина Миронець, Андрій Шкребтій

Черкаський державний технологічний університет

МИРОНЕЦЬ Ірина Валеріївна, *к.т.н., доцент*

Рік та місце народження: 1982 рік, с. Скородистик, Чорнобаївський район, Черкаська область, Україна.
Освіта: Черкаський національний університет ім. Б.Хмельницького, 2004 рік.
Посада: доцент кафедри інформаційної безпеки та комп'ютерної інженерії з 2015 року.
Наукові інтереси: підвищення оперативності доступу до конфіденційних інформаційних ресурсів, розробка методів та засобів оцінки ефективності соціоінжинірингу.
Публікації: більше 70 наукових публікацій, серед яких монографії, навчальні посібники, наукові статті, матеріали та тези доповідей на конференціях, а також патенти на винаходи.
E-mail: irenmir30@gmail.com.
Orcid ID: 0000-0003-2007-9943.

ШКРЕБТІЙ Андрій Володимирович

Рік та місце народження: 1991 рік, м. Сміла, Черкаська область, Україна.
Освіта: Черкаський державний технологічний університет, 2017 рік.
Посада: аспірант кафедри інформаційної безпеки та комп'ютерної інженерії з 2017 року.
Наукові інтереси: захист віртуальної валюти на основі вдосконалених блокчейнів.
Публікації: наукові статті, матеріали та тези доповідей на конференціях.
E-mail: jimmy.wilson11@gmail.com.
Orcid ID: 0000-0002-7494-3760.

Анотація. *Сучасна економіка є повністю електронною не тільки через те, що сучасний обіг інформації включно з банківськими транзакціями та економічними відносинами здійснюється через електронні засоби комунікації. Тотальне переведення всіх економічних розрахунків у віртуальну площину викликало появу нових явищ, таких, як криптовалюта, що у свою чергу поступово змінює саме поняття валюти та забезпечує можливість абсолютно точно відслідковувати всі тенденції у розвитку суспільства. Створення програмних додатків на базі технології блокчейн є перспективним напрямком сучасних досліджень по децентралізації сховищ даних. У даній статті проведено огляд та дослідження алгоритмів, які використовуються для створення хеш-функцій в технології блокчейн. Блокчейн - це надійний спосіб зберігання даних про угоди, контракти, транзакціях, про все, що необхідно записати і перевірити. Сьогодні блокчейн проник практично в усі сфери життєдіяльності, готовий змінити фінансову систему держави і в декілька разів спростити роботу середнього і великого бізнесу. Блокчейн – не таємна технологія, знаходиться у вільному доступі, причому існує величезна кількість статей про те, як він влаштований і за яким принципом працює. У статті розглянуто основні криптоалгоритми, які використовуються в криптовалютах для створення хешів. Визначено переваги та недоліки існуючих криптоалгоритмів, принципи та специфіку функціонування технології блокчейн в цілому, а також схему її роботи. Особливу увагу приділено дослідженню проблеми безпеки та конфіденційності при її використанні. При детальному розгляді алгоритмів, які використовуються для отримання криптовалют варто відзначити алгоритми групи X. У цьому випадку розробники нехтують швидкодією заради стійкості, що майже унеможливлює знаходження кількості раундів для злому. Кожен з описаних алгоритмів в подальшому має потенціал для покращення його характеристик, за рахунок чого можливе збільшення криптостійкості кожного з них, що забезпечить зростання безпеки у криптовалюті в цілому.*

Ключові слова: *захист інформації, віртуальна валюта, блокчейн, майнінг, альткоін, хеш-функція, Secure Hash Algorithm, BLAKE, Hash Iterative Framework, X11, X13, X15, X17.*

Вступ

Блокчейн – це надійний спосіб зберігання даних про угоди, контракти, транзакціях, про все, що необхідно записати і перевірити. Сьогодні блокчейн проник практично в усі сфери життєдіяльності, готовий змінити фінансову систему держави і в декілька разів спростити роботу середнього і великого бізнесу. Блокчейн – не таємна технологія, знаходиться у вільному доступі, причому існує величезна кількість статей про

те, як він влаштований і за яким принципом працює. Сьогодні блокчейн перестає асоціюватися з біткоіном і стає самостійною технологією, яка є основою нових додатків і систем. Експерти впевнені: блокчейн стає логічним еволюційним продовженням традиційних інструментів обліку. До того ж, якщо раніше про блокчейн говорили, як про сховище даних, то тепер його можливості стають набагато ширше, тому що він також може виконувати програми. Деякі блокчейни дозволяють кожному факту містити міні-програму. В основі блокчейну лише математика, але ця властивість не обмежує сферу реалізації даної технології.

Аналіз існуючих досліджень

Суть роботи блокчейну, як ланцюжка блоків, можна порівняти з пазлом. Блок – масив даних, в нього вноситься інформація про транзакції, які потрапили в мережу після створення попереднього блоку (приблизно за останні 10 хвилин). Кожен новий блок даних кріпиться до попереднього за допомогою складних математичних алгоритмів, що дозволяє скріпити ці блоки. Щоб створити новий блок, необхідно обчислити його криптографічний відбиток (хеш), що задовольняє певним умовам.

Цей процес проводиться за допомогою великої кількісті комп'ютерів, що працюють в одній мережі і вирішують певну складну криптозадачу, в ході якої необхідно розрахувати хеш (вихідні дані) заголовка блоку в блокчейні. Іншими словами, підібрати особливий код, який дозволить отримати хеш, що містить певну кількість нулів на своєму початку. Процес пошуку блоків називається майнінгом. Коли завдання виконане, формується новий блок, який не можна ні видалити, ні змінити. Проте кожен користувач мережі може побачити всю інформацію, що знаходиться в блокчейні. На криптографічних хешах тримається вся надійність і захищеність блокчейна. Хеш видається системою в форматі величезного числа. Для заданого набору даних хеш-функція дає один хеш, який володіє двома важливими властивостями:

– перша полягає в тому, що, навіть володіючи ключем, можна дізнатися вихідний набір даних;

– друга властивість – практично неможливо знайти інший набір даних, що дає такий же хеш.

Одне з головних правил даної технології: всі дані блокчейн-блоків відкриті для всіх і завжди. Їх легко перевірити, легко відстежити будь-яку зміну інформації. Проблемою створення нових алгоритмів шифрування даних в блокчейн системах є відсутність уніфікованого алгоритму. Майнери та люди, які створюють нові криптовалюти прагнуть створити алгоритми, які було б важко перевести на спеціалізоване обладнання, ASIC. Для розуміння будови будь-якого алгоритму шифрування потрібно знати, що було основою. Для прикладу: хеш-функції сімейства SHA, побудовані на основі структури Меркла-Демгарда.

Метою даної роботи є дослідження та аналіз алгоритмів, які використовуються для створення хеш-функцій в технології блокчейн.

Основна частина дослідження

З 2007 року творці криптографічних алгоритмів беруть участь у спеціальному конкурсі, який організовує Американський Національний Інститут Стандартів і Технологій (NIST). На конкурсі представляються криптографічні хеш-функції, призначені для "стиснення" довільного повідомлення або набору даних, записаного, як правило, в двійковому алфавіті, в деяку бітову комбінацію фіксованої довжини.

У ньому всі пропозиції оцінюються за чотирма критеріями:

– продуктивність;
– безпека;
– аналіз;
– різноманітність хешів для різних режимів роботи.

Для того, щоб хеш-функція вважалася криптографічно стійкою, вона повинна задовольняти трьом основним вимогам, на яких засновано основне використання їх в криптографії:

– незворотність або стійкість до відновлення прообразу: для заданого значення хеш-функції m повинно бути обчислювально неможливо знайти блок даних X, для якого H(X) = m;

– стійкість до колізій першого роду або відновленню других прообразів: для заданого повідомлення M має бути обчислювально неможливо підібрати інше повідомлення N, для якого H(N) = H(M);

– стійкість до колізій другого роду: має бути обчислювально неможливо підібрати пару повідомлень *(M, M')*, що мають однаковий хеш.

Алгоритм отримання хешу для майнінгу SHA 2 на основі SHA 256

Алгоритм безпечного хешування (Secure Hash Algorithm SHA) - стандарт, який був розроблений національним Інститутом Стандартів і Технології (NIST – National Institute of Standards and Technology) і виданий як Федеральний Стандарт Обробки Інформації (FIP 180). В даний час це сімейство криптографічних хеш-функцій, які включають в себе такі алгоритми як SHA-0, SHA-1, SHA-2, SHA-3.

Алгоритм SHA 2 на основі SHA 256 - той самий алгоритм, за рахунок якого існує майнінг Bitcoin і багатьох альткоінів. Знати про цей алгоритмі, так само як і про його ключовий компонент, хеш-функцію SHA 256 повинен кожен, хто працює з технологією блокчейн. Для початку потрібно розшифрувати скорочення SHA та цифри за ними. Отже, SHA 2 або Secure Hash Algorithm 2 (алгоритм безпечного хешування) - це набір криптографічних хеш-функцій, що ставить перед собою завдання шифрувати дані. Цей алгоритм - не щось абстрактне, а має реальне застосування в сучасному і звичному для нас світі: протоколи захищеної передачі даних TLS, SSH, PGP – всі базуються на цьому алгоритмі.

SHA 256, в свою чергу – це одна з хеш-функцій, що використовує алгоритм SHA 2. Словосполучення «хеш-функція» означає функції, призначені для "стиснення" довільного повідомлення або набору даних, записаного, як правило, в двійковому алфавіті, в деяку бітову комбінацію фіксованої довжини. SHA 256

являє собою односпрямовану функцію для створення цифрових відбитків фіксованої довжини (256 біт, 32 байт) з вхідних даних розміром до 2,31 екзабайти (2^{64} біт) [1].

Основою функції є структура Меркла-Демгарда. Конструкція була описана Ральфом Мерклом в його кандидатській дисертації у 1979 році. Суть конструкції полягає в ітеративному процесі послідовних перетворень, коли на вхід кожної ітерації надходить блок вихідного тексту і вихід попередньої ітерації. Вхідний рядок x розбивається на t однакових по довжині блоків, довжина блоку x_i рівна r. Довжина блоку r повинна відповідати довжині вхідного блоку функції стиснення f. Загальний вигляд схеми зображено на рисунку 1.

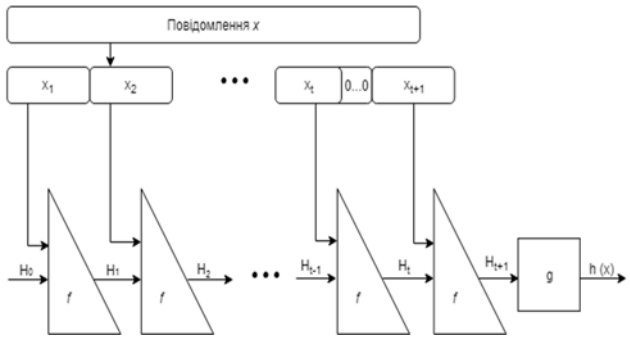

Рис. 1. Конструкція Меркла-Демгарда

Оригінал тексту після доповнення розбивається на блоки, кожен блок - на 16 слів. Алгоритм пропускає кожен блок повідомлення через цикл з 64 ітераціями. На кожній ітерації два слова перетворюються, функцію перетворення задають інші слова. Результати обробки кожного блоку складаються, сума є значенням хеш-функції. Так як ініціалізація внутрішнього стану проводиться результатом обробки попереднього блоку, то немає можливості обробляти блоки паралельно [2]. Графічне представлення однієї ітерації обробки блоку даних зображено на рисунку 2.

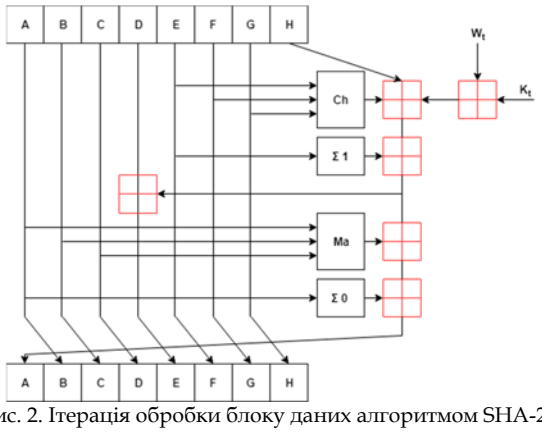

Рис. 2. Ітерація обробки блоку даних алгоритмом SHA-256

Алгоритм відмінно шифрував дані, і був стійкий до колізій. Колізії (англ. *collision* – зіткнення, конфліктна ситуація) – це не що інше, як конфлікт в роботі хеш-функцій, і виникає він через рівності значень на різних блоках інформації. На даний момент відомі методи для конструювання колізій до 31 ітерації. Криптографічні функції, на зразок SHA 256, повинні генерувати унікальних хеш - свідоцтво про унікальність контенту або інформації, а також її приналежність до чогось конкретного. Таким чином, інформація отримує унікальний «цифровий підпис». Якщо алгоритм не стійкий до колізій, то підробити цифровий підпис, виявиться реальним завданням. Виходячи з цього були описані чотири основні вимоги для роботи алгоритму:

1. Залишок від хеш-функції повинен змінюватися при зміні вихідних даних. Якщо ж залишок (хеш) не змінюватиметься в залежності від оригіналу, значить функції хешування працюють некоректно.

2. Кожен образ повинен бути унікальним. Імовірність їх збігу вкрай мала, хоча і існує. SHA 2 є досить надійним алгоритмом, тому проблем на цьому етапі не виникає (захист від колізій).

3. Функції хешування повинні бути односпрямованим. Це означає, що до вихідних даних можна працювати лише в одному напрямку: шифрувати, перемішувати, розсіювати біти інформації. Розшифрувати ж ці дані, використовуючи зворотний алгоритм, не вийде.

4. Підбір необхідного хеш-значення (ключа) повинен бути дуже складним. Саме таким чином виключається можливість підробки даних.

Для алгоритму SHA-256 при стандартних параметрах маємо:

Таблиця 1

Розмір входу	Розмір внутрішнього стану	Розмір блоку	Довжина блоку	Розмір слова	Кількість раундів
256	256	512	64	32	64

В теорії існують значення кінцевих ітерацій, при яких цей алгоритм можливо зламати:

Таблиця 2

Атаки (складність кількість раундів/ітерацій)	
Знаходження прообразу	Знаходження другого прообразу
$2^{284.4}$	$2^{284.4}$

Такі високі параметри складності атаки на алгоритм в даний час (2018/2019 рр.) дозволяють ефективно використовувати його в наступних технологіях:

– Bitcoin – криптовалюта через пошук відбитків з певними рамками значень;
– DNSSEC – дайджести DNSKEY;
– DSA – використовується для створення електронного цифрового підпису;
– IPSec – в протоколах ESP і IKE;
– OpenLDAP – хеші паролів;
– PGP - використовуються для створення електронного цифрового підпису;
– S/MIME - дайджести повідомлень;
– SHACAL-2 – блоковий алгоритм шифрування;
– X.509 – використовуються для створення електронного цифрового підпису сертифікату.

Алгоритм BLAKE

Алгоритм розроблений командою з чотирьох криптографів зі Швейцарії. BLAKE256-512 відрізняється дуже простою розробкою для застосування і спирається на структуру HAIFA (HAsh Iterative FrAmework) – ітеративний метод побудови хеш-функцій, близький за своєю структурою до класичного побудованого на схемі Меркла-Демгарда. Творцями алгоритму є вчені Елі Біхам і Ор Дункельман - ізраїльські криптографи, які працювали в Хайфському університеті. Конструкція HAIFA, запропонована в 2007 році, має ряд конструктивних особливостей. Крім нулів і інформації про довжину вхідного повідомлення, вхідні дані доповнюються *r* бітами, що кодують довжину хеш-суми. В якості аргументів функції стиснення, яка базується на модифікованій схемі Девіса-Мейєра, крім внутрішнього стану і чергового блоку повідомлення, використовується кількість біт, які вже надходили на вхід функції стиснення на попередніх ітераціях, і «сіль» - використання кількості біт, які вже надходили на вхід функції стиснення на попередніх ітераціях, як аргумент функції стиснення – міра протидії атаці з використанням рухомих точок. Додавання «солі» дозволяє розглядати дану конструкцію як екземпляр сімейства рандомізованих хеш-функцій і забезпечує наступні переваги:

– можливість оцінити стійкість хеш-функції на теоретичному рівні;

– виключення атак, заснованих на попередніх обчисленнях;

– підвищення стійкості цифрових підписів до атак знаходження другого прообразу.

Дана конструкція дозволяє отримувати хеш-суми різних довжин в рамках одного додатку. Використовується універсальний вектор ініціалізації, передбачений розробником додатку, а вторинний вектор ініціалізації (довжина якого відповідає бажаній довжині хеш-суми) виходить як результат функції стиснення від універсального вектора і значень інших параметрів.

Найбільш характерні риси BLAKE - це високий запас надійності і високопродуктивна універсальність (дуже важливо для майнерів). Що потрібно запам'ятати про BLAKE, так це те, що він може і буде працювати швидше, ніж SHA- 2(56) на ряді платформ.

Блочний шифр оперує внутрішніми станами, які можуть бути представлені квадратною матрицею слів порядку 4. BLAKE-224 і BLAKE-256 використовують 512-бітний блочний шифр, в якому блок представляється 32-бітними словами, а BLAKE-384 і BLAKE-512 використовують 1024-бітну версію шифру з 64-бітними словами. Функція стиснення *G*, яка зображена на рисунку 3, основана на поточному шифрі ChaCha, вона оновлює стовпці, використовуючи ARX-операції. Слова вхідних даних і константи вибираються за допомогою фіксованих перестановок або в залежності від номера раунду *r*. В останньому раунді кількість ітерацій функції стиснення було збільшено авторами з 10 до 14 для BLAKE-224 і BLAKE-256 і з 14 до 16 для BLAKE-384 і BLAKE-512.

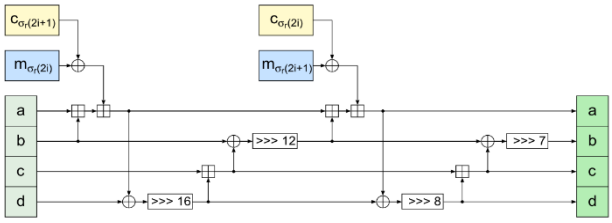

Рис. 3. Функція стиснення алгоритму BLAKE

В 2013 році, з'явився BLAKE2. Нова версія алгоритму має швидкість, близьку до швидкості MD5 на 64-бітних платформах (в 2.53 рази швидше, ніж SHA-2), і вимагає на 33% менше оперативної пам'яті, ніж SHA-2, на пристроях з обмеженими ресурсами. Автори досягли таких результатів, не сильно змінивши конструкцію BLAKE. Зокрема, були змінені початкові установки для функції стиснення, оптимізовані під апаратні платформи константи циклічних зрушень, виключені константи раундової функції. Ці оптимізації привели до зниження теоретичної стійкості. Успішна атака на всі 12 раундів версії BLAKE2b має вкрай високу складність 2^{876}. Аналіз показав, що виключення констант з раундової функції зробило стійкість хеш-функції сильно залежною від правильного вибору вектора ініціалізації. У 2014 році з'явилися теоретичні атаки відразу на обидві версії BLAKE2: BLAKE2s (7.5 раундів, складність 2^{184}) і BLAKE2b (8.5 раундів, складність 2^{474}). Такі показники, як і раніше залишають за BLAKE2 право вважатися легким, швидким та надійним алгоритмом для отримання хеш-функцій. Основною відмінністю від попереднього алгоритму є його швидкодія: початкова кількість раундів SHA-2 була 10 раундів для 256- бітної версії та 14 раундів для 512-бітної версії, а для BLAKE це значення 8 та 10 раундів відповідно. Завдяки збільшеній швидкодії алгоритм використовується для майнінгу монет DCR (Decred), а також як один з раундів хешування у алгоритмах групи X.

Алгоритми групи X

Алгоритми групи X – це передова технологія програмування коінів. На даний момент існують такі алгоритми, як «X11», «X13», а також «X15» і «X17». Вони є вдосконаленими версіями алгоритму доведення виконаної роботи PoW (Proof-of-Work). Що ж стосується числа, яке розташоване після «X», то воно означає кількість функцій, які використовуються для обчислень в блоці.

Подібні алгоритми застосовують математичні формули обчислень. З їх допомогою можна здійснювати ефективний майнінг коінів з використанням ресурсів відеокарт. При цьому певний відсоток користі з пулів отримують не тільки самі майнери, а й власники основних мережевих вузлів.

Найбільш ефективним для більшості майнерів на момент написання роботи є майнінг альткоїнів на алгоритмах групи X.

В X11 використовує 11 раундів хешування з 11-ма різними хеш-функціями:

- BLAKE;
- KECCAK;
- BMW;
- GROESTL;
- JH;
- SKEIN;
- LUFFA;
- CUBEHASH;
- SHAVITE;
- SIMD;
- ECHO, що робить його одним з найбільш надійних в світі криптовалют.

Алгоритм X11 був представлений світу у 2014 році, з роками структура алгоритму змінювалася на більш покращену і світ побачив оновлені версії X13, X15 ті X17. З кожною новою версією алгоритму до попередніх функцій по створенню хешу додавалися дві нові: у X13 це HAMSI та FUGUE, у X15 – SHABAL та WHIRPOOL та у X17 - LOSELOSE і DJB-2 відповідно [6].

Для того, щоб запобігти використанню ASIC-майнерів з метою видобутку токенів, творці Dash розробили алгоритм, який набагато складніше, ніж SHA-256 в Bitcoin. Розробники об'єднали 11 різних алгоритмів хешування в один. Таке рішення дозволило понизити швидкодію, але збільшити складність злому. Тому що на кожному раунді, починаючи з версії X11, додавалися нові алгоритми зі своїми параметрами. Тобто в даний чай алгоритм X17 являє собою сукупність криптостійких 17-ти алгоритмів і є найнадійнішим для використання в криптовалюті. Криптовалюта, яка може бути здобута за алгоритмом X17 включає в себе Verge (XVG), MKTCoin (MLM), SHIELD (XSH), Bitmark (BTM), Volvox (VVX) and GlobalToken (GLT).

Висновки

В статті було розглянуто основні крипто-алгоритми, які використовуються в криптовалютах для створення хешів. Але більшість з описаних алгоритмів в даний час (2019 рік) використовуються не тільки при створенні криптовалюти, але і в інтернет-протоколах.

Один з перших алгоритмів був SHA (Secure Hash Algorithm), який за час від створення до даного часу розвився до третьої версії та зазнав суттєвих покращень. Наступний алгоритм це – BLAKE побудований лише з трьох раніше вивчених компонентів: режим ітерації HAIFA, внутрішня структура local wide-pipe, алгоритм стиснення, які були детально описані.

Останні алгоритми, які використовуються в створенні криптовалюти це X-алгоритми. Вони були створені спеціально для роботи на графічних процесорах, де забезпечують якісну рентабельність і низьке енергоспоживання. Кожен результат під-функції потім передається в наступний під-алгоритм і так відбувається X раз. Щоб зламати останню версію X17, потрібно знайти вразливість всіх 17 хешів, що набагато складніше, ніж на SHA-256/512.

При детальному розгляді алгоритмів, які використовуються для отримання криптовалют варто відзначити алгоритми групи X. У цьому випадку розробники нехтують швидкодією заради стійкості, що майже унеможливлює знаходження кількості раундів для злому.

Кожен з описаних алгоритмів в подальшому має потенціал для покращення його характеристик, за рахунок чого можливе збільшення криптостійкості кожного з них, що забезпечить зростання безпеки у криптовалюті в цілому.

Література

[1]. SHA (Secure Hash Algorithm). [Електронний ресурс]. Режим доступу: https:// ru.bmstu.wiki / SHA-1_(Secure_Hash_Algorithm_1).

[2]. Структура Меркла-Демгарда. [Електронний ресурс]. Режим доступ: http://wiki-org.ru/wiki/ Структура_Меркла_—_Демгарда.

[3]. Д. Лукьяненко, Алгоритм хеширования для майнинга sha 256 и SHA 2. [Електронний ресурс]. Режим доступу: https://profitgid.ru/algoritm-heshirovanija-dlja-majninga-sha-256-i-sha-2.html.

[4]. А. Марков, Обзор алгоритма BLAKE2b на основе поточного шифра ChaCha. [Електронний ресурс]. Режим доступу: https://miningbitcoinguide. com/mining/sposoby/blake2b.

[5]. M.J. Dworkin, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions.

[6]. А. Марков, Алгоритм X13 для майнинга на графических процессорах. [Електронний ресурс]. Режим доступу: https:// miningbitcoinguide. com/ mining/ sposoby/x13.

УДК 004.056.5

Миронец И., Шкребтий А. Криптографические алгоритмы и особенности их использования в блокчейн-системах

Аннотация. *Современная экономика есть полностью электронной не только из-за того, что современный оборот информации, включая банковские транзакции и экономические отношения, осуществляются через электронные средства коммуникации. Тотальный перевод всех экономических расчетов в виртуальную плоскость вызвало появление новых явлений, таких, как криптовалюта, что в свою очередь постепенно меняет само понятие валюты и обеспечивает возможность абсолютно точно отслеживать все тенденции в развитии общества. Создание приложений на базе технологии блокчейн является перспективным направлением современных исследований по децентрализации хранилищ данных. В данной статье проведен обзор и исследование алгоритмов, которые используются для создания хэш-функций в технологии блокчейн. Блокчейн - это надежный способ хранения данных о сделках, контракты, транзакциях, обо всем, что необходимо записать и*

проверить. Сегодня блокчейн проник практически во все сферы жизнедеятельности, готов изменить финансовую систему государства и в несколько раз упростить работу среднего и крупного бизнеса. Блокчейн - не тайная технология, она находится в свободном доступе, причем существует огромное количество статей о том, как она устроена и по какому принципу работает. В статье рассмотрены основные криптоалгоритмы, которые используются в криптовалюте для создания хэшей. Определены преимущества и недостатки существующих криптоалгоритмов, принципы и специфика функционирования технологии блокчейн в целом, а также схему ее работы. Особое внимание уделено исследованию проблемы безопасности и конфиденциальности при ее использовании. При детальном рассмотрении алгоритмов, которые используются для получения криптовалюты стоит отметить алгоритмы группы X. В этом случае разработчики пренебрегают быстродействием ради устойчивости, что почти исключает нахождения количества раундов для взлома. Каждый из описанных алгоритмов в дальнейшем имеет потенциал для улучшения его характеристик, за счет чего возможно увеличение криптостойкости каждого из них, что обеспечит рост безопасности криптовалюты в целом.
Ключевые слова: *защита информации, виртуальная валюта, блокчейн, майнинг, альткоин, хэш-функция, Secure Hash Algorithm, BLAKE, Hash Iterative Framework, X11, X13, X15, X17.*

Myronets I., Shkrebtii A. Cryptographic algorithms and features of their use in blockchain systems

Annotation. *The modern economy is completely electronic, not only because the current information circulation, including banking transactions and economic relations, is carried out through electronic communications. The total transfer of all economic calculations to the virtual plane caused the emergence of new phenomena such as cryptocurrency, which in turn gradually changes the concept of currency and provides an opportunity to accurately track all trends in the development of society. The creation of software applications based on the blockchain technology is a promising direction of modern research on the decentralization of data storages. This article reviews and studies the algorithms used to create hash functions in the blockchain technology. Blockchain is a reliable way to store data about transactions, contracts, everything that needs to be written and checked. Today blockchain has penetrated practically all spheres of life, is ready to change the financial system of the state and simplify the work of medium and large businesses. Blockchain is not a secret technology, it is freely available, and there is a huge amount of articles on how it is organized and on what principle it works. The article deals with the main cryptographic algorithms used in cryptography for creating hashes. The advantages and disadvantages of existing cryptographic algorithms, principles and specifics of the operation of the blockchain system as a whole, as well as the scheme of its work, are determined. Particular attention is paid to the study of security and privacy issues with its use. In a detailed consideration of the algorithms used to obtain cryptographic values, it's worth noting the algorithms of group X. In this case, developers ignore the speed for stability, which makes it almost impossible to find the number of rounds for hacking. Each of the described algorithms in the future has the potential to improve its characteristics, due to it is possible to increase in cryptostability of each of them, which will increase the security of the cryptocurrency in general.*
Keywords: *information security, virtual currency, blockchain, mining, altcoin, hash function, Secure Hash Algorithm, BLAKE, Hash Iterative Framework, X11, X13, X15, X17.*

Отримано *27 червня 2019 року*, затверджено редколегією *21 липня 2019 року*