УДК 004.056.5 **DOI:10.30837/rt.2019.3.198.04**

О.О. КУЗНЕЦОВ, д-р техн. наук, Ю.І. ГОРБЕНКО, канд. техн. наук,
В.В. ОНОПРІЄНКО, канд. техн. наук, І.В. СТЕЛЬНИК, Д.В. МЯЛКОВСЬКИЙ

АЛГОРИТМИ КРИПТОГРАФІЧНОГО ҐЕШУВАННЯ, ЯКІ ЗАСТОСОВУЮТЬСЯ В СУЧАСНИХ БЛОКЧЕЙН-СИСТЕМАХ

Вступ

Сучасні децентралізовані інформаційні системи та мережі, побудовані за новітньою технологією блокчейн, дедалі поширюються та застосовуються у різних додатках, наприклад при побудові криптовалют; для реалізації розподілених та захищених від несанкціонованої зміни реєстрів, кадастрів, списків, тощо; для побудови різних за призначенням та функціональними завданнями децентралізованих систем, які об'єднують, наприклад, центри сертифікації ключів, тощо; при побудові розподілених децентралізованих мереж електронної ідентифікації та електронного голосування; при розбудові інформаційних систем із підтримкою так званих смарт-контрактів, тощо. Отже, аналіз та дослідження всіх складових сучасних систем та мереж, які побудовано за технологією блокчейн, є актуальним та важливим науковим завданням.

За визначенням блокчейн являє собою вибудуваний за певними правилами безперервний послідовний ланцюжок блоків (або зв'язний список), що містить певну інформацію. Найчастіше копії ланцюжків блоків зберігаються на безлічі різних комп'ютерів незалежно один від одного [1]. Вперше цей термін з'явився як назва розподіленої бази даних, реалізованої в системі «біткойнів», через що блокчейн часто відносять до транзакцій в різних криптовалютах, проте технологія ланцюжків блоків може бути поширена на будь-які взаємопов'язані інформаційні блоки [1, 2]. Біткойн став лише першим застосуванням технології блокчейн в жовтні 2008 р. [2].

Для забезпечення захисту інформації від різних загроз безпеці в системах блокчейн застосовуються криптографічні методи, механізми та протоколи. Зокрема одним із головних криптопримітивів в кожній блокчейн-системі є алгоритми криптографічного ґешування [3], які призначені для перетворення вхідного масиву даних довільної довжини у вихідний бітовий рядок фіксованої довжини [4]. Такі перетворення також називаються ґеш-функціями, або функціями згортання, а їхні результати називають ґешем, ґеш-кодом, ґеш-сумою, або дайджестом повідомлення (англ. message digest) [5].

Криптографічні ґеш-функції мають наступні важливі властивості безпеки [6 – 8]:

1. Вони стійкі до знаходження прообразу. Це означає, що вони односторонні, тобто з математичної точки зору неможливо обчислити правильне вхідне значення при відомому вихідному значенні. Наприклад, якщо задане ґеш-значення *y*, тоді обчислювально важко знайти таке *x*, для якого hash(x) = y;

2. Стійкі до знаходження другого прообразу. Це означає, що ніхто не може знайти вхідне значення, яке ґешується у конкретний результат. Більш детально – криптографічні ґеш-функції створені таким чином, що при заданому конкретному вихідному значенні обчислювально неможливо знайти друге вхідне значення, яке дає таке ж вихідне значення. Наприклад, якщо задане *x*, обчислювально важко знайти таке *y*, для якого hash(x) = hash(y). Єдиний доступний підхід полягає у тому, щоб перебирати вихідні значення у всьому просторі, однак з обчислювальної точки зору немає жодного шансу на успіх;

3. Стійкі до колізій. Це означає, що неможливо знайти два вхідних значення, які б ґешувалися до однакового результату. Якщо розглядати більш детально, то з математичної точки зору обчислювально неможливо знайти два вхідні значення, які привели б до одного і того ж вихідного значення. Наприклад, обчислювально важко знайти такі x і y, де hash(x) = hash(y).

В багатьох реалізаціях блокчейну застосовується захищений ґеш-алгоритм (SHA) з розміром вихідного значення 256 біт (SHA-256) [6]. Багато комп'ютерів апаратно підтримують даний алгоритм, що прискорює його обчислення [6].

Втім, слід відмітити, що з появою ASIC стало можливим добувати криптовалюту (наприклад, Bitcoin) набагато швидше, ніж за допомогою відеокарт або десктопних обчислювальних систем [9 – 15]. ASIC – це інтегральна схема, спеціалізована для вирішення конкретного завдання. Ці схеми у багато разів вигідніше відеокарт, тому що при більшій потужності (швидкості розрахунку ґешу) вони споживають набагато менше енергії. Отже почалася, так би мовити, «гонка озброєнь»: розробники блокчейн-протоколів шукають способи протистояти ASIC-Майнінгу, а виробники майнінгового обладнання шукають можливість обійти хитрості розробників за допомогою застосування швидких ASIC-обчислювачів. Таким чином, інвестуючи в придбання ASIC, недобросовісні конкуренти можуть бути поставлені у свідомо більш вигідне становище порівняно з іншими гравцями [16 – 18]. Для захисту від ASIC-майнерів і забезпечення справедливого розподілу прибутку необхідно змінювати алгоритм ґешування або застосовувати принципово нові криптографічні схеми та протоколи консенсусу [15].

В статті проводиться аналіз функцій ґешування, які застосовуються або можуть застосовуватися в різних блокчейн-системах. Зокрема, розглядаються найбільш поширені національні та міжнародні стандарти, в яких наведено специфікацію всесвітньо відомих алгоритмів криптографічного ґешування, та досліджуються різні проекти з побудови децентралізованих блокчейн-систем, де ці функції можуть бути застосовані. В подальших статтях проводяться порівняльні дослідження функцій ґешування за швидкодією та статистичною безпекою.

Аналіз функцій ґешування, які застосовуються або можуть застосовуватися в різних блокчейн-системах

За визначенням, ґешування (або хешування, англ. hashing) є перетворенням вхідного масиву даних довільної довжини у вихідний бітовий рядок фіксованої довжини [5 – 8]. Такі перетворення також називаються ґеш-функціями, або функціями згортання, а їхні результати називають ґешем, ґеш-кодом, ґеш-сумою, або дайджестом повідомлення (англ. message digest) [6]. Отже функція ґешування – це функція, що перетворює вхідні дані будь-якого (як правило, великого) розміру в дані фіксованого розміру. За визначенням з ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція ґешування» під функцією ґешування розуміється криптографічне перетворення повідомлення M довжини від 0 біт (порожній рядок) до $2^{96}-1$ біт у ґеш-значення (ґеш-вектор) $H(M)$, що є двійковим рядком фіксованої довжини n ($n = 8 \cdot s, s \in \{1,2,...,64\}$) [19].

Основним міжнародним нормативним документом, який визначає терміни, основні поняття, класифікацію та специфікацію певних алгоритмів криптографічного ґешування, є міжнародний стандарт ISO/IEC 10118 [20 – 23]:

- в першій частині стандарту ISO/IEC 10118-1:2016 «Information technology – Security techniques – Hash-functions – Part 1: General» наводяться основні поняття та визначення з ґешування інформації, зокрема загальна ітеративна модель ґеш-функції (перша частина стандарту гармонізована в Україні у вигляді ДСТУ ISO/IEC 10118-1:2018 (ISO/IEC 10118-1:2016, IDT) «Інформаційні технології. Методи захисту. Ґеш-функції. Частина 1. Загальні положення» [20]);
- в другій частині ISO/IEC 10118-2:2010/Cor.1:2011 «Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher» визначаються алгоритми ґешування, які застосовують блокові симетричні шифри (ця частина стандарту гармонізована в Україні у вигляді ДСТУ ISO/IEC 10118-2:2015 (ISO/IEC 10118-2:2010; Cor 1:2011, IDT) «Інформаційні технології. Методи захисту. ґеш-функції. Частина 2. ґеш-функції, що використовують n-бітний блоковий шифр» [21]);

- третю частину ISO/IEC 10118-3:2018 «IT Security techniques – Hash-functions – Part 3: Dedicated hash-functions» присвячено розгляду спеціалізованих функцій ґешування (гармонізовано в Україні у вигляді ДСТУ ISO/IEC 10118-3:2005 «Інформаційні технології. Методи захисту. ґеш-функції. Частина 3. Спеціалізовані ґеш-функції» [22]);

- четверта частина ISO/IEC 10118-4:1998/Cor.1:2014 «Information technology – Security techniques – Hash-functions – Part 4: Hash-functions using modular arithmetic» містить опис функцій ґешування, які засновано на модулярній арифметиці (гармонізовано в Україні у вигляді ДСТУ ISO/IEC 10118-4:2015 (ISO/IEC 10118-4:1998; Cor 1:2014; Amd 1:2014, IDT) «Інформаційні технології. Методи захисту. ґеш-функції. Частина 4. ґеш-функції, що використовують модульну арифметику» [23]).

Функції ґешування, які описані у низці стандартів ISO/IEC 10118, не використовують секретного ключа (тобто є безключовими ґеш-функціями), зокрема вони можуть бути використані для формування кодів виявлення маніпуляцій (КВМ) (від англ. manipulation detection code – MDC).

Слід зазначити, що окремі криптографічні функції ґешування можуть також використовувати секретний ключ (тобто бути т.з. ключовими ґеш-функціями). Такі функції ґешування призначені для формування кодів автентифікації повідомлень (КАП) (від англ. message autentifacation code – MAC). Для їхнього опису та стандартизації на міжнародному рівні застосовується інший нормативний документ, а саме ISO/IEC 9797-1:2011 Information technology – Security techniques – Message Authentication Codes (MACs) [24 – 26]:

- перша частина ISO/IEC 9797-1:2011 «Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher» встановлює алгоритми формування КАП із застосуванням блокових симетричних шифрів (гармонізовано в Україні у вигляді ДСТУ ISO/IEC 9797-1:2015 (ISO/IEC 9797-1:2011, IDT) «Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 1. Механізми, що використовують блоковий шифр» [24]);

- друга частина ISO/IEC 9797-2:2011 «Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function» містить специфікацію КАП із застосуванням спеціалізованих функцій ґешування (гармонізовано в Україні у вигляді ДСТУ ISO/IEC 9797-2:2015 (ISO/IEC 9797-2:2011, IDT) «Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 2. Механізми що використовують спеціалізовану ґеш-функцію» [25]);

- третю частину ISO/IEC 9797-3:2011 «Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a universal hash-function» присвячено КАП, які застосовують універсальне ґешування (цей стандарт гармонізовано в Україні у вигляді ДСТУ ISO/IEC 9797-2:2015 (ISO/IEC 9797-2:2011, IDT) «Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 2. Механізми, що використовують універсальну ґеш-функцію» [26]).

Таким чином, відповідно до діючих та гармонізованих в Україні міжнародних нормативно-правових документів загальну класифікацію криптографічних функцій ґешування можна подати у вигляді схеми, яку наведено на рис. 1. На рисунку штриховкою відмічені алгоритми, які не включено до відповідних стандартів, але які можуть бути застосовані для формування ґеш-кодів за відповідною схемою. Наприклад, відповідно до ISO/IEC 10118-2 ґешування може бути реалізоване із застосуванням блокового симетричного шифру. У якості такого шифру може бути застосований і алгоритм Калина (англ. Kalyna) – національний стандарт блокового симетричного криптоперетворення України [27, 28].

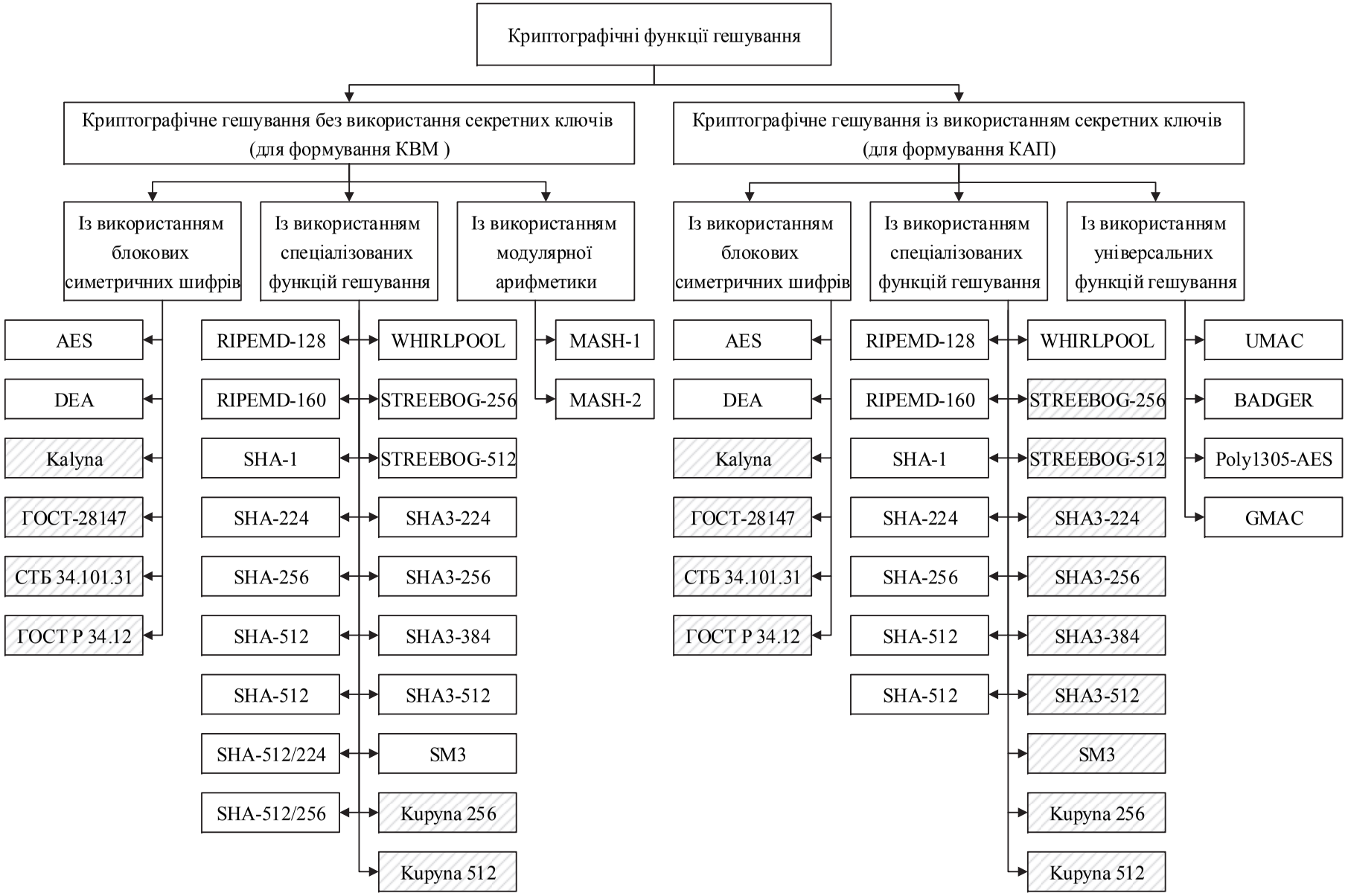

Рис. 1. Загальна класифікація криптографічних функцій гешування
(згідно з міжнародними стандартами ISO/IEC 10118 та ISO/IEC 9797)

Інший приклад – формування КАП. Відповідно до ISO/IEC 9797-1 КАП можуть формуватися із використанням алгоритмів блокового симетричного шифрування. І хоча за специфікацією ISO/IEC 9797-1 не передбачено використання алгоритму Калина, цей шифр може бути застосовано у відповідному режимі для формування КАП (за специфікацією ДСТУ 7624:2014 в алгоритмі Калина передбачена можливість формування КАП [27]).

До загальної класифікації, яку наведено на рис. 1, не входять чисельні алгоритми ґешування, які стандартизовано на національному рівні окремих країн, та алгоритми ґешування, які було подано та розглянуто на різних криптографічних конкурсах. Зокрема, на відкритому конкурсі «SHA-3», який проводився в 2007 – 2012 рр. Національним інститутом стандартів і технологій (NIST) на нову криптографічну ґеш-функцію, призначену для доповнення і заміни SHA-1 і SHA-2, було представлено велику кількість алгоритмів ґешування, з яких 51 алгоритм був допущений до проведення першого туру [29]. У табл. 1 представлені відомі учасники конкурсу «SHA-3» із зазначенням основних атрибутів ґеш-функцій і знайдених атак [30].

У табл. 1 застосовуються такі позначення [30]:

– FN (англ. A Feistel network) – мережа Фейстеля;

– WP (англ. Wide Pipe design) – метод побудови криптографічних ґеш-функцій, схожий на структуру Меркле – Дамгора;

– KEY (англ. Key schedule) – алгоритм, який одержує ключі для кожного раунду ґешування;

– MDS (англ. MDS Matrix) – розмір MDS-матриці;

– OUT (англ. Output Transformation) – криптографічна операція, яка здійснюється в останній вихідний ітерації;

– SBOX (англ. S-box) – S-блоки;

– FSR (англ. Feedback Shift Register) – регістр зсуву з лінійним зворотним зв’язком;

– ARX (англ. Addition Rotation XOR) – складання, циклічний зсув і XOR;

– BOOL (англ. Boolean operations) – булева алгебра;

– COL (англ. Collision Attack) – найкраща з відомих атак на пошук колізій, краще ніж атака «днів народження»;

– PRE (англ. Preimage Attack) – друга найкраща атака на пошук колізій, краще ніж атака подовженням повідомлення.

До переліку алгоритмів ґешування слід добавити спеціально розроблені функції ґешування для застосування в різних криптовалютах та інформаційних системах типу блокчейн. Зокрема, у табл. 2 наведено неповний перелік криптовалют із зазначенням року введення, спеціального позначення (тікера[1]) криптовалюти та алгоритму майнінгу[2].

[1] Тікер, Тікерна назва (англ. ticker symbol) – коротка назва котируваних інструментів (акцій, облігацій, індексів) в біржовій інформації. Є унікальним ідентифікатором в межах однієї біржі або інформаційної системи. Використовується для того, щоб постійно не друкувати в звітах та новинах повне найменування цінних паперів або інших об'єктів торгівлі.

[2] Майнінг, також видобування (від англ. mining – видобуток корисних копалин) – діяльність з підтримки розподіленої платформи і створення нових блоків з можливістю отримати винагороду в формі емітованої валюти і комісійних зборів у різних криптовалютах, зокрема в Біткоїнах. Обчислення потрібні для забезпечення захисту від повторного використання одних і тих же одиниць валюти, а зв'язок майнінгу з емісією стимулює людей витрачати свої обчислювальні потужності і підтримувати роботу мереж.

Таблиця 1

Відомі учасники конкурсу «SHA-3» із зазначенням основних атрибутів геш-функцій і знайдених атак [30]

Алгоритм гешування	FN	WP	KEY	MDS	OUT	SBOX	FSR	ARX	BOOL	COL	PRE
Abacus	-	X	-	4 x 4	X	8 x 8	X	-	-	2^{172}	2^{172}
ARIRANG	X	X	X	4 x 4, 8 x 8	-	8 x 8	-	-	-	-	-
AURORA	-	-	X	4 x 4	X	8 x 8	-	-	-	$2^{234,61}$ / $2^{229,6}$	2^{291} / $2^{31,6}$
BLAKE	X	-	X	-	-	-	-	X —	-	-	-
Blender	-	X	-	-	-	-	-	X	-	$10 \cdot 2^{\frac{n}{4}}$	$10 \cdot 2^{\frac{n}{4}}$
BMW	-	X	X	-	-	-	-	X	-	-	-
Boole	-	-	-	-	X	-	X	-	$\wedge$	2^{34}	$2^{\frac{9n}{r}}$
Cheetah	-	-	X	4 x 4, 8 x 8	-	8 x 8	-	-	-	-	-
Chi	X	X	X	-	-	4 x 3	-			-	-
CRUNCH	X	-	X	-	-	8 x 1016	-	-	-	-	-
CubeHash8/1	-	-	-	-	-	-	-	X	-	-	2^{509}
DHC	-	-	X	-	-	8 x 8	-	-	-	2^{9}	2^{9}
DynamicSHA	X	-	X	-	-	-	-			2^{114}	-
DynamicSHA2	X	-	X	-	-	-	-			-	-
ECHO	-	X	-	4 x 4	-	8 x 8	-	-	-	-	-
ECOH	-	-	X	-	-	-	-	-	-	-	-
Edon-R	-	X	X	-	-	-	-	X	-	-	$2^{\frac{2n}{3}}$
EnRUPT	-	X	-	-	-	-	-	X	-	-	2^{480} / 2^{480}
Essence	-	-	-	-	-	-	X	-	-	-	-
FSB	-	X	-	-	X	-	-	-	-	-	-
Fugue	-	X	-	4 x 4	X	8 x 8	-	-	-	-	-
Gr0stl	-	X	-	8 x 8	X	8 x 8	-	-	-	-	-
Hamsi	-	-	X	-	-	4 x 4	-	-	-	-	-
JH	X	X	-	1.5 x 1.5	-	4 x 4	-		-	-	$2^{510,3}$ / $2^{510,3}$
Keccak	-	X	-	-	-	-	-			-	-
Khichidi-1	-	-	X	-	-	-	X	-	-	1	$1/2^{33}$

Алгоритм гешування	FN	WP	KEY	MDS	OUT	SBOX	FSR	ARX	BOOL	COL	PRE
LANE	-	-	X	4 x 4	X	8 x 8	-	-	-	-	-
Lesamnta	X	-	X	2 x 2, 4 x 4	X	8 x 8	-	-	-	-	-
Luffa	-	-	-	-	X	4 x 4	-	-	-	-	-
Lux	-	X	-	4 x 4 , 8 x 8	X	8 x 8	-	-	-	-	-
MCSSHA-3	-	-	-	-	-	-	X	-	-	$2^{\frac{3n}{8}}$	$2^{\frac{3n}{4}}$
MD6	-	X	-	-	-	-	X			-	-
MeshHash	-	-	-	-	X	8 x 8	-	-	-	-	$2^{323,2} / 2^{\frac{n}{2}}$
NaSHA	X	-	-	-	-	8 x 8	X	-			-
SANDstorm	-	-	X	-	-	8 x 8	-			-	-
Sarmal	X	-	-	8 x 8	-	8 x 8	-	-	-	-	$2^{384} / 2^{128}$
Sgail	-	X	X	8 x 8, 16 x 16	-	8 x 8	-	X	-	-	-
Shabal	-	-	X	-	-	-	X			-	-
SHAMATA	X	X	X	4 x 4	-	8 x 8	-	-	-	$2^{40} / 2^{29}$	$2^{461,7} / 2^{462,7}$
SHAvite-3	X	-	X	4 x 4	-	8 x 8	X	-	-	-	-
SIMD	X	X	X	TRSC+	-	-	-			-	-
Skein	X	X	X	-	X	-	-	X	-	-	-
Spectral Hash	-	-	-	-	X	8 x 8	-	-	-	-	-
StreamHash	-	-	-	-	-	8 x 8	-	-	-	-	$n2^{\frac{n}{2}}$
SWIFFTX	-	-	-	-	-	8 x 8	-	-	-	-	-
Tangle	-	X	X	-	-	8 x 8	-				-
TIB3	U	-	X	-	-	3 x 3	-	-	-	-	-
Twister	-	X	-	8 x 8	X	8 x 8	-	-	-	2^{252}	$2^{448} / 2^{264}$
Vortex	-	-	-	4 x 4	X	8 x 8	-	-	-	$2^{125,5} / 2^{125,5}$	$2^3 / 2^{\frac{n}{4}}$
WAMM	-	X	-	-	X	8 x 8	-	-	-	-	-
Waterfall	-	X	-	-	X	8 x 8	X	-	-	2	-

Таблиця 2

Неповний перелік криптовалют та алгоритмів їхнього майнінгу [31]

Найменування	Рік	Тікер	Алгоритм майнінгу
Bitcoin	2009	BTC	SHA-256
Ethereum	2015	ETH	Dagger- Hashimoto
Steemit	2016	STEEM	SHA-256
Ripple	2013	XRP	ECDSA
DigiByte	2014	DGB	SHA256
Monero	2014	XMR	CryptoNight
Siacoin	2015	SC	blake2b
Litecoin	2011	LTC	Scrypt
EthereumClassic	2015	ETC	Dagger- Hashimoto
Dogecoin	2013	DOGE	Scrypt
NEM	2015	XEM	blockchain
Syscoin	2014	SYS	Scrypt
Augur	2015	REP	Smart contract
Dash	2014	DASH	X11
ByteCoin	2012	BCN	CryptoNight
BelaCoin	2014	BELA	Scrypt
lbryCoin	2016	LBC	LBRY
Radium	2015	RADS	Smartchain
Decred	2015	DCR	Blake256
Einsteinium	2014	EMC2	Scrypt
Gridcoin	2013	GRC	Scrypt
Primecoin	2013	XPM	1CC/2CC/TWN
NEO	2014	NEO	SHA-256 & RIPEMD160
MazaCoin	2014	MZC	SHA-256d
Titcoin	2014	TIT	SHA-256d
Verge	2014	XVG	Scrypt, x17, groestl, blake2s, and lyra2rev2
Stellar	2014	XLM	Stellar Consensus Protocol (SCP)
Tether	2015	USDT	Omnicore
Zcash	2016	ZEC	Equihash
Bitcoin Cash	2017	BCH	SHA-256d
EOS.IO	2017	EOS	–
VertCoin	2014	VTC	Lyra2RE
Dashcoin	2014	DSH	CryptoNight
Potcoin	2014	POT	Scrypt
Peercoin	2012	PPC	SHA-256
Namecoin	2011	NMC	SHA-256
Nxt	2013	NXT	SHA-256d
Nautiluscoin	2014	NAUT	NXT
Auroracoin	2014	AUR	Scrypt
Expanse	2015	EXP	Dagger- Hashimoto
PinkCoin	2014	PINK	X11
FoldingCoin	2014	FLDC	Stanford Folding
Navcoin	2014	NAV	X13
ViaCoin	2014	VIA	Scrypt
DNotes	2014	NOTE	Scrypt
Vcash	2014	XVC	Blake256

Висновки

Аналіз відомих розподілених технологій та блокчейн-мереж показує, що одним із їх головних криптографічних компонентів є ґешування. Саме на використанні криптографічних властивостей необоротності функцій ґешування будуються безперервні послідовні ланцюжки блоків (зв'язні списки), які дозволяють забезпечити надійне зберігання критично важливої інформації. Дійсно, при виконанні певних умов внесення несанкціонованих змін у захищену таким чином інформацію є практично неможливим, бо це порушить безперервність ланцюжка ґеш-значень і стане наявним для всіх користувачів блокчейн-системи. Отже, обрання функції ґешування для побудови зв’язаних списків, вивчення її властивостей та дослідження певних характеристик є дійсно важливою та актуальною науковою задачею.

З урахуванням можливого застосування ASIC-обчислювачів задача обрання надійної криптографічної функції ґешування ще більш ускладнюється. Дійсно, якщо певним гравцям блокчейн-мережі із визначеною криптографічною функцією вдастся першими ввести в дію значну кількість ASIC-майнерів, тоді вони отримують перевагу у формуванні наступних блоків мережі і, таким чином, зможуть нав’язувати свої рішення іншим учасникам системи. Отже в сучасних блокчейн-мережах необхідним є або заміна/модернізація протоколів консенсусу з метою зменшення можливого впливу ASIC-майнерів, або пошук таких алгоритмів ґешування, які б було складно відтворити у ASIC-обчислювачах. Саме тому на сьогодні спостерігається стрімкий зріст кількості різних алгоритмів ґешування, які застосовуються в різних блокчейн-системах.

В роботі розглянуто різні децентралізовані блокчейн-системи та проаналізовано застосовані в них алгоритми криптографічного ґешування. Слід зазначити, що перелік криптовалют та інформаційних систем за технологією блокчейн стрімко зростає. Наприклад, на середину 2018 р. неповний перелік криптовалют містив вже понад 1500 найменувань, і впродовж часу постійно оновлюється та розширюється. Практично неможливо відслідкувати всі діючі проекти з розробки технології блокчейн, але табл. 2 містить найбільш відомі та найпоширеніші криптовалюти світу.

Перспективним напрямком подальших досліджень є аналіз структури та особливостей застосування різних сімейств криптографічних функцій ґешування в блокчейн-системах, проведення порівняльних досліджень їх швидкодії та статистичної безпеки, що буде розглянуто у наступних роботах.

Список літератури:

1. Melanie Swan. Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc., 2015. 152 p.
2. Marco Iansiti and Karim R. Lakhani (2017). The Truth About Blockchain // Harvard Business Review. January–February 2017 issue. Pp. 118-127.
3. Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone. NISTIR 8202 Blockchain Technology Overview // National Institute of Standards and Technology, Internal Report 8202, 66 pages (October 2018). https://doi.org/10.6028/NIST.IR.8202
4. ISO/IEC 10118-1:2016. Information technology – Security techniques – Hash-functions. Part 1: General. (2016-10), 12 p. https://www.iso.org/standard/64213.html
5. Handbook of Applied Cryptography / Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. October 1996, 816 pages, Fifth Printing (August 2001). http://cacr.uwaterloo.ca/hac/
6. Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone. NISTIR 8202. Blockchain Technology Overview. [online] Available at: https://doi.org/10.6028/NIST.IR.8202
7. O. Potii, Y. Gorbenko and K. Isirova. Post quantum hash based digital signatures comparative analysis. Features of their implementation and using in public key infrastructure // 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017. Pp. 105-109.
8. Yu. I. Gorbenko, T. V. Melnik, I. D. Gorbenko. Analysis of Potential Post-Quantum Schemes of Hash-Based Digital Signatur // Telecommunications and Radio Engineering. 2018. Volume 77, Issue 7. Pp. 603-626.
9. M. Khazraee, I. Magaki, L. Vega Gutierrez and M. Taylor. ASIC Clouds: Specializing the Datacenter // IEEE Micro.
10. S. Cheng and S. Lin. A Memory-Hard Blockchain Protocol // 2018 IEEE International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, 2018. Pp. 284-287.

11. M. Bedford Taylor. Bitcoin and the age of Bespoke Silicon // 2013 International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES), Montreal, QC, 2013, pp. 1-10.

12. X. Zhang, R. WU, M. Wang and L. Wang. A High-Performance Parallel Computation Hardware Architecture in ASIC of SHA-256 Hash // 2019 21st International Conference on Advanced Communication Technology (ICACT), PyeongChang Kwangwoon_Do, Korea (South), 2019, pp. 52-55.

13. I. Magaki, M. Khazraee, L. V. Gutierrez and M. B. Taylor. ASIC Clouds: Specializing the Datacenter. 2016 ACM/IEEE 43rd Annual International Symposium on Computer Architecture (ISCA), Seoul, 2016, pp. 178-190.

14. M. Bedford Taylor. The Evolution of Bitcoin Hardware // Computer, vol. 50, no. 9, pp. 58-66, 2017.

15. A. R. Zamanov, V. A. Erokhin and P. S. Fedotov. ASIC-resistant hash functions // 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, 2018, pp. 394-396.

16. N. T. Courtois, P. Emirdag and Z. Wang. On detection of bitcoin mining redirection attacks // 2015 International Conference on Information Systems Security and Privacy (ICISSP), Angers, 2015, pp. 98-105.

17. M. Khazraee, L. V. Gutierrez, I. Magaki and M. B. Taylor. Specializing a Planet's Computation: ASIC Clouds // IEEE Micro, vol. 37, no. 3, pp. 62-69, 2017.

18. Y. Wang, J. Wu, S. Chen, M. C. Chao and C. Yang, "Micro-Architecture Optimization for Low-Power Bitcoin Mining ASICs," 2019 International Symposium on VLSI Design, Automation and Test (VLSI-DAT), Hsinchu, Taiwan, 2019, pp. 1-4.

19. ДСТУ 7564:2014 Інформаційні технології. Криптографічний захист інформації. Функція ґешування. З поправкою. 02.12.2014. Електронний ресурс. Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66229

20. ДСТУ ISO/IEC 10118-1:2003. Інформаційні технології. Методи захисту. ґеш-функції. Частина 1. Загальні положення.

21. ДСТУ ISO/IEC 10118-3:2005 «Інформаційні технології. Методи захисту. ґеш-функції. Частина 3: Спеціалізовані ґеш-функції».

22. ДСТУ ISO/IEC 10118-2:2014. Інформаційні технології. Методи захисту. ґеш функції. Частина 2. ґеш-функції, що використовують n-бітовий блоковий алгоритм шифрування. На заміну ДСТУ ISO/IEC 10118-2:2003.

23. ДСТУ ISO/IEC 10118-4:2014. Інформаційні технології. Методи захисту. ґеш-функції Частина 4. ґеш-функції, що використовують модульну арифметику. Вперше.

24. ДСТУ ISO/IEC 9797-1:2015 (ISO/IEC 9797-1:2011, IDT). Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (macs). Частина 1. Механізми, що використовують блоковий шифр. Електронний ресурс. Режим доступу: http://shop.uas.org.ua/ua/informacijni-tehnologii-metodi-zahistu-kodi-avtentifikacii-povidomlen-macs-chastina-1-mehanizmi-scho-vikoristovujut-blokovij-shifr.html

25. ДСТУ ISO/IEC 9797-2:2015 (ISO/IEC 9797-2:2011, IDT. Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (macs). Частина 2. Механізми що використовують спеціалізовану ґеш-функцію. Електронний ресурс. Режим доступу: http://shop.uas.org.ua/ua/informacijni-tehnologii-metodi-zahistu-kodi-avtentifikacii-povidomlen-macs-chastina-2-mehanizmi-scho-vikoristovujut-specializovanu-gesh-funkciju-31543.html

26. ДСТУ ISO/IEC 9797-3:2015 (ISO/IEC 9797-3:2011, IDT. Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (macs). Частина 3. Механізми, що використовують універсальну ґеш-функцію. Електронний ресурс. Режим доступу: http://shop.uas.org.ua/ua/informacijni-tehnologii-metodi-zahistu-kodi-avtentifikacii-povidomlen-macs-chastina-3-mehanizmi-scho-vikoristovujut-universal-nu-gesh-funkciju.html

27. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення http://uas.org.ua/ua/services/standartizatsiya/109-2/

28. Roman Oliynykov, Ivan Gorbenko, Oleksandr Kazymyrov, Victor Ruzhentsev, Oleksandr Kuznetsov, Yurii Gorbenko, Oleksandr Dyrda, Viktor Dolgov, Andrii Pushkaryov, Ruslan Mordvinov, Dmytro Kaidalov. A New Encryption Standard of Ukraine: The Kalyna Block Cipher. Електронний ресурс. Режим доступу: https://eprint.iacr.org/2015/650.pdf

29. Hash Functions. Created January 04, 2017, Updated May 03, 2019. Електронний ресурс. Режим доступу: https://csrc.nist.gov/projects/hash-functions/sha-3-project

30. Classification of the SHA-3 Candidates. By Ewan Fleischmann, Christian Forler, and Michael Gorski. Version 0.90, April 19, 2009. Електронний ресурс. Режим доступу: https://eprint.iacr.org/2008/511.pdf

31. Алгоритмы майнинга криптовалют – таблица 2019 и краткое описание. Електронний ресурс. Режим доступу: https://mining-cryptocurrency.ru/algoritmy-kriptovalyut/.

Харківський національний
університет імені В.Н. Каразіна;
АТ «Інститут інформаційних технологій»;
Адміністрація Державної служби спеціального зв'язку
та захисту інформації України.

Надійшла до редколегії 02.09.2019