Research Article

Asmaa A. Mohammed*, Abdul Monem S. Rahma, and Hala Bahjat AbdulWahab

Improvements in the randomness and security of digital currency using the photon sponge hash function through Maiorana–McFarland S-box replacement

https://doi.org/10.1515/eng-2024-0050
received March 13, 2024; accepted May 01, 2024

Abstract: There is a demand for a digital currency that facilitates remote trading over the Internet and strives to reduce external control, ensuring that transactions are conducted only between authorized persons or parties involved in the transfer. The financial sector has been significantly impacted by cryptocurrency, or digital currency, which brings new potential and challenges. The concept of digital currency is thoroughly examined, as are its complicated implications on various aspects of the economy. Trading digital currencies *via* the Internet may be vulnerable to theft and forgery due to the development of hacker programs. Therefore, we proposed to design a new digital currency and then built a 16 × 16 structure and filled the matrix with random numbers within GF(251). We used the random algorithm (Chun–Hui He's iteration), then generated four directions, and used polynomial equations for the purpose of distributing powers between the parties in our future complete system. The original matrix was encoded with the photon sponge hash function after updating the S box by integrating the algorithms (Chun–Hui He's iteration, Mariorana–McFarland method), and the results were good security measures (correlation coefficient, bijective property, balanced criteria, completeness criteria, and strict avalanche criteria) as well as the encryption and decryption time became faster (0.0005202). The major objective is to design a new digital currency system toward achieving security, scalability, and comprehensive adoption, looking into how it might improve security, promote financial inclusion, and change the present payment systems.

Keywords: electronic currency, types of digital currency, Chun–Hui He's iteration, sponge hash function, Mariorana–McFarland method

*** Corresponding author: Asmaa A. Mohammed**, Department of Computer Science, College of Science, University of Technology, Baghdad, Iraq, e-mail: cs.20.11@grad.uotechnology.edu.iq
Abdul Monem S. Rahma: Department of Computer Science, College of Science, Al-Maarif University College, Al-Anbar, Iraq, e-mail: monem.rahma@uoa.edu.iq
Hala Bahjat AbdulWahab: Department of Computer Science, College of Science, University of Technology, Baghdad, Iraq, e-mail: Hala.b.abdulwahad@uotechnology.edu.iq

1 Introduction

The main introduction of digital currency design refers to the foundational principles and concepts behind creating digital currencies. Digital currencies are virtual or electronic forms of money that use cryptography for secure transactions, decentralization for control, and rely on blockchain technology or other distributed ledger technologies for operation [1,2]. The development of currencies has witnessed significant changes. After the exchange or barter was the first commercial process between individuals and societies, it developed to include bronze in the mining of the first monetary coins. Then, it was followed by the entry of both silver and gold in transactions, which are currently known as currencies. By the end of the second millennium, there was a significant surge in development. This led to the transformation of commercial exchange tools into a digital form, including the emergence of credit cards and specialized applications designed for electronic payments, along with their corresponding digital payment methods. The financial sector experienced significant growth, leading to the emergence of encrypted digital or digital currencies. The trade volume of digital currencies had a significant surge toward the end of the first decade of the twenty-first century, reaching billions of US dollars. This increase in value has made them a destination for electronic hacks and piracy. For instance, the amount of one million US dollars in digital currencies raises concerns about the feasibility of protecting traders involved in this kind of currency [3,4].

It is important to note that designing a new digital currency requires careful consideration of various technical, economic, regulatory, and societal factors [5]. The strengths of our proposed system are as follows: 1. We used Chun–Hui He's iteration and the photon sponge hash function to encrypt digital currency. 2. Direct interaction between users without the need for financial intermediaries, which increases the speed and efficiency of the exchange process between them. 3. Encryption and decryption time is faster. 4. Increased security ratio in our system due to the use of highly complex. The weaknesses facing our proposed system are as follows: 1. Adoption and acceptance: The new digital currency may face challenges in adoption and acceptance by users, institutions, or companies, which may affect its value and use. 2. Security and fraud: The new digital currency may face challenges in terms of security and fraud, especially in its early stages, which can affect customer's trust. Algorithm Research problems: Because of the different aspects of life (commercial, industrial, agricultural, and others) need to exchange wages between people, and the exchange of wages (material) sometimes requires that it be between the two sides only without a third party, such as the bank or a specific supervisory authority, *i.e.,* the exchange is independent, *i.e.,* the currencies are free to exchange through the Internet and that they enjoy the same advantages as paper currencies and coins. That is, they have self-immunity against theft and forgery. Because of these problems, therefore, we proposed designing a digital currency that is electronically unrestricted and independent between people without the need for a third party and, at the same time, has immunity against theft and forgery. In our proposed system, a matrix of size 16 × 16 was designed and filled with numbers within GF(251) and randomly scattered with an algorithm (Chun–Hui He's iteration) to increase randomness and security. Then, we generated from the original matrix four matrices (top, bottom, right, and left) for the purpose of distributing powers in our complete future system. Next, we encoded the random matrix with an algorithm (photon sponge hash function) by updating the S box by merging two algorithms (Chun–Hui He's iteration and Mariorana–McFarland method) for the purpose of increasing randomness and complexity and the proposed method gave higher randomness, as well as the time of encoding and decoding became faster.

The remainder of this article is structured as follows: Related works are explained in Section 2. Section 3 deals with digital currencies with advantages, challenges, and design types of digital currencies. The random algorithm for Chun–Hui He's iteration is highlighted in Section 4. The topic of hash function is explained in Section 5. The Mariorana–McFarland method is explained in Section 6. Finally, the proposal system of digital currency design is discussed in Section 7.

2 Related studies

Technology and finance practitioners, as well as researchers, are interested in the design of digital currencies. Research Gate, Google Scholar, and Google as a large library were searched.

Nakamoto [6] initially created Bitcoin to address the problem of double spending associated with e-accounts since digital currencies could be transferred between users without enabling the user to copy, transfer, and spend electronic currency twice.

Hineman and Blaum [7] presented an approach for accelerating and simplifying the encoding in Shamir's secret-sharing approach by eliminating the need for symbols to be distinguishable at most a predetermined distance apart. Furthermore, this process is accelerated by using array codes based on XOR operations instead of Reed–Solomon codes.

A cryptocurrency wallet (Bitcoin wallet) for Android OS was developed and carried out by Khan *et al.* [8] with the use of a secure private key storage method ("Cold Wallet") and an Android application based on QR codes. Because of its benefits in integrating Blockchain with IoT, Ghalwesh *et al.* [9] depended on the hyperledger project to maximize security in the two monitoring and storage operations. In order to reduce such time complexity, Mbaye *et al.* [10] devised two parallel approaches that rely on distributed systems and GPUs. We were able to reduce time complexity and enhance the algorithms with the aid of the distributed approach.

Garratt *et al.* [11] examined the consequences of utilizing commercial banks of different sizes in the introduction of a central bank digital currency (CBDC). They focused on two aspects of CBDC design: payment simplicity and interest rate. These traits reflect currencies' qualities as a store of value and medium of trade. Payment simplicity is an overlooked aspect of CBDC design that interacts with the financial benefits of interest payments. A sufficiently high convenience value of a CBDC could enhance the transmission of monetary policy.

Kakebayashi [12] concluded that CBDC could address problems with the value-added tax (VAT) system while preserving its efficacy, simplicity, and fairness. According to the report, CBDCs have the potential to significantly alter public financing overall, but their design and acceptance should not be determined solely by how they could impact the tax system, as shown in Table 1.

Table 1: Compression between the related works

Reference and Years	Type of digital currency	Central authority	Technique	Strengths and weaknesses
[6] (2008)	Bitcoin	No	Peer-to-peer principle, digital signatures, and the blockchain	Strengths: Digital currency, like Bitcoin, introduced in 2009, offered decentralized transactions and borderless payments, fostering financial inclusion and reducing reliance on traditional banking systems. Weaknesses: digital currency faced limited adoption and regulatory uncertainty, raising concerns about security, stability, and potential use for illicit activities due to its pseudonymous nature
[7] (2022)	Bitcoin	No	Multi-signature technique based on Shamir's secret sharing	Strengths: digital currencies demonstrated faster and more efficient cross-border transactions, highlighting their potential for reducing fees and transaction times in international remittances. Weaknesses: During this period, digital currencies faced high price volatility and scalability issues, posing challenges to their use as stable stores of value and mainstream payment methods
[8] (2019)	Bitcoin	No	QR code and hot wallet	Strengths: investors searching for alternative assets were more interested in digital currencies for guarding against economic dangers Weaknesses: in various jurisdictions, unclear frameworks, as well as regulatory concerns, have hindered the implementation and broad acceptance of digital currencies in established financial systems
[9] (2020)	Bitcoin	No	Depending on the Hyperledger project	Strengths: digital currencies opened up novel channels to lend, borrow, and yield farming, showcasing their potential for decentralized finance (DeFi) applications. Weakness: the year has shown how easy it is for such currencies to get manipulated in the market, suffer a cyber-attack, or get penalized by governmental rules, resulting in clearer regulations and more robust security measures being demanded
[10] (2021)	Altcoin	Yes	Altcoins can be adopted as a digital currency as they are mainly designed as a means of exchange between two counterparties directly	Strengths: the main historically established financial institutions and multinational corporations showed intention to integrate digital currencies already into their activities alongside quickly rising institutional acceptability. Weaknesses: like a revelation, the year showed that these concerns over environmental and energy implications remain even with respect to proof-of-work-based cryptocurrencies, which brought about the question of whether renewable energies could be the future for this currency
[11] (2022)	Bitcoin, CBDC	No, yes	Blockchain, unified payment interface	Strengths: more state-of-the-art energy-efficient algorithms that are less likely to generate negative environmental effects for digital currencies have been introduced, subsequently ensuring the reliability and sustainability of the network. Weaknesses: however, this period saw regulators worldwide striving to create guidelines for the use of cryptocurrencies, an act that created uncertainty and even business disruptions in the ongoing financial landscape of the emerging world

(Continued)

Table 1: *Continued*

Reference and Years	Type of digital currency	Central authority	Technique	Strengths and weaknesses
[12] (2023)	CBDC	Yes	VAT system	Strengths: digital currencies continued to drive innovation in decentralized applications, smart contracts, and NFTs, expanding their utility beyond traditional financial transactions. Weaknesses: concerns about user privacy and data security remained, prompting discussions around implementing robust privacy solutions in digital currencies

3 Digital currency

Digital currency is issued through private parties and exclusively flows through the Internet instead of government-issued money circulating through traditional banks and financial organizations. While it shares certain characteristics with bank transfers, digital currency transactions are not burdened by high fees, fraudulent chargebacks, or protracted wait times for cleared funds, whereas those involving bank accounts and credit cards [13]. A digital representation of value that could be transferred, stored, or traded electronically is called a digital currency. The public authority or central bank does not issue it. It is not a fiduciary currency-linked payment. The fact that individuals accept it as a form of payment strengthens it [14,15]. Digital currencies are described as a digital representation of a value by the European Banking Committee. It is a form of payment accepted *via* legal and ordinary persons, not issued through a central bank or public authorities, is not always associated with a particular currency, and may be transferred, stored, and traded electronically. Virtual fake currencies made up of digital codes that could be kept on a network or hard drives are called digital currencies. It is challenging to keep track of the selling and buying activities on the Internet or even identify the owners of such currencies because their value depends on demand and supply [16,17].

3.1 Characteristics of electronic currency systems

1. Digital: Electronic currency exists only in digital form and is stored, transferred, and verified electronically.
2. Decentralized: Most electronic currency systems do not have a central authority or intermediary, such as a bank, that controls the system.
3. Cryptographic: Electronic currencies use complex cryptographic algorithms to secure transactions and prevent fraud.
4. Limited supply: Many electronic currencies have a limited supply, meaning that a finite number of units could be created.
5. Peer-to-peer: Users of E-currency systems can frequently and directly interact with one another, bypassing the requirement for a central intermediary [18,19].

3.2 Challenges encountered by electronic currency systems

It is important to consider in relation to some factors before sharing confidential or personal information with

the customer. Similarly, different types of businesses face the same cultural challenges when both cultural adaptation and assimilation are done [20,21].

1. Security: E-currency systems are just as vulnerable to cyberattacks as any other financial system.
2. Scalability: E-currency systems will face inconvenience when they get overwhelmed by the high volume of transactions due to the problems that they encounter while they are growing in popularity.
3. Volatility: the challenges that user experience to determine the value of their digital assets are a result of the magnitude and the rate at which E-currencies value fluctuates.
4. Regulation: Things can be complicated for the authorities as this type of financial system can be difficult to monitor, resulting in profit profiteering by illegal operators who launder and carry out their illegal activities.
5. Integration with traditional financial systems: To collaborate electronic money systems with the standard financial systems may be tedious, as in the exercising of the traditional bank networks and the credit card systems [22].

3.3 Types of digital currency

Many types of digital currencies are available today, and some of the most common variants are listed as follows:

1. Cryptocurrencies: Cryptocurrencies are virtual money systems that primarily use blockchain networks and cryptography technologies as their foundation: Bitcoin, Litecoin, and Ethereum.
2. Stablecoins: Stablecoins are a sort of digital money that ties the price of each coin to one particular item or a basket of related assets, thereby ensuring that the value of each coin remains stable. Ones anchored to a fiat currency, like the United States Dollar or Euro.
3. CBDCs: Digital currencies known as CBDCs are produced and controlled by central banks. CBDCs are centralized and administered by the issuing central bank, in contrast to decentralized cryptocurrencies. The goal of CBDCs is to provide the advantages of digital currencies without sacrificing control over monetary policy and financial stability [23].
4. Utility tokens: Utility tokens are digital assets generated by projects or companies that are used to grant access to their products or services. Such tokens are mainly employed within a given ecosystem to allow for payments, utilization of features, and participation in the system's governance. Here, we have BNB (Binance Coin) and LINK (Chain-link) to cite.
5. Security tokens: Security tokens are used to represent ownership in underlying assets like real estate, stocks, or commodities. These tokens are subject to security regulations and provide investors with rights and benefits, such as dividends or voting rights. Security tokens aim to digitize traditional financial assets, enabling more efficient trading and ownership transfer [24].
6. These are some of the main types of digital currencies available today. Each type serves different purposes and offers distinct features within the digital currency landscape [25,26].

4 Chun–Hui He's iteration

The variant method of He Chun–Hui based on iteration belongs to the class of iterative computing algorithms for solving nonlinear equations and optimization problems. The main purpose of this technique is to solve nonlinear functions and obtain their roots or mains. The method involves an iterative algorithm, which allows the original solution to be updated by small adjustments and consequently leads to a desired precision level.

The main definition of Chun–Hui He's iteration method can be summarized as follows:

Given a nonlinear equation $f(x) = 0$, where x is the variable to be solved for, the iterative update rule for Chun–Hui He's method is as follows:

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}, \tag{1}$$

where x_n is the current estimate of the root or minimum, $F(x_n)$ is the value of the function at (x_n), and $F(x_n)$ is the derivative of the function with respect to (x) evaluated at (x_n).

The main algorithm of Chun–Hui He's iteration method can be summarized as follows:

1. Start with an initial guess (x_0) for the root or minimum.
2. Implement a loop with the update rule $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$ until reaching the minimum (convergence) or maximum number of iterations.
3. To make sure how convergence is attained, one has to check whether the convergence criteria are met (for example, the absolute or relative difference between consecutive iterates is less than some specified threshold value or the function value is close to zero).
4. In the case of convergence, the current iterate (x_n) is taken as the approximate root for the included function. This method operates on the basis of Newton's method and it is particularly eloquent for functions with smooth and well-behaved derivatives. However, it may exhibit convergence issues for functions with complex behavior

or near singularities. Proper initialization and convergence criteria are important aspects to consider when applying Chun–Hui He's iteration method [27–29].

5 Sponge hash function

Megha Mukundan *et al.* created the cryptographic construction known as a sponge [30]. It uses an iterated model, processing r bits regarding a message block to produce n bits of output from a state S of b bits. The width of the permutation, or $b = r + c \geq n$, represents the sponge state's size. In the sponge state, the b bits undergo a permutation αb. The message block size or rate is denoted by the Algorithm 1.

Algorithm 1: Photon sponge structure

Input: data input or message

Output: hash blocks

parameter r, whereas the capacity is denoted by the value c [30,31].

Begin

Step 1: In order to make the input length an integral multiple of r, the data input, or message, is padded by adding a 1 bit and as many zeros as necessary.

Step 2: An internal t-bit state made up of an r-bit rate and a c-bit capacity.

Step 3: The permutation P is applied to the t-bit state after mi is XORed with the rate component of the internal state for each of the i iterations.

Step 4: For the squeezing phase, the internal state is divided into r' and c' sections, which may differ in length from r and c. This phase produces a sequence of I r'-bit hash blocks z0,., zj-1, zi ← P(zi-1)

There are 12 rounds of four stages in the permutation:

1-AddConstants: The first column of the matrix is XORed with round constants.

2-SubCells: An S-box performs the step of mapping each entry in the matrix by a new value.

3-ShiftRows: Each row's cell positions are flipped.

4-MixColumnsSerial: Using this function, each column is individually mixed linearly [32–34].

End.

6 Maiorana–McFarland algorithm

S-boxes can be created using the Maiorana–McFarland algorithm, which is mostly applied to symmetric-key cryptography methods like block ciphers [35]. The algorithm's goal is to produce S-boxes that have advantageous cryptographic characteristics, like strong non-linearity and resilience to cryptanalysis methods [36–38].

Let n be an even positive integer, "f: $Z_p{}^n \to * Z_p{}^m$," a function and denote the m output coordinate functions of f by "$f = (f1,..., fm)$." Assume that every "fi, $i = 1, 2, ..., m$," is a Maiorana function, *i.e.*, has the form "$fi(x) = fi(x1, x2) = \pi i (x1). xz + gi(xl), P$" where πi is a permutation of the space Z,! and g, is a function from $Z_p{}^n$ to $Z_p{}^m$. Then, $f = (f1, f2, ..., fm)$ is perfect nonlinear if every nonzero linear combination of the permutations "xi, $i = 1, 2, ..., m$" is again a permutation of "$Z_{p\frac{n}{2}}$" [39,40].

7 The proposal system for the digital currency design

Algorithm 2: Proposal system for the digital currency design

Input: Array of numbers, size 16 × 16

Output: SHA-256 hash for each cell in the array

Begin

Step 1: Create a 16 × 16 array of numbers.

Step 2: Fill the array with random numbers in the range of GF(251) using the logistic map random algorithm.

Step 3: Determine the interconnections for each cell by specifying the 1-Top, 2-Down, 3-Left, and 4-Right connections.

Step 4: Determine the value of the top (↑) neighbor for the first cell [0, 0] and assign it to the finite set (X^2) as the top value.

Step 5: Determine the value of the down (↓) neighbor for the first cell [0, 0] and assign it to the finite set ($X^2 + 1$) as the down value.

Step 6: Determine the value of the left (←) neighbor for the first cell [0, 0] and assign it to the finite set ($x + 2$) as the left value.

Step 7: Determine the value of the right (→) neighbor for the first cell [0, 0] and assign it to the finite set ($x + 1$) as the right value.

Step 8: Apply the SHA-256 hash algorithm to each cell in all four directions (Top, Down, Left, and Right).

Step 9: Return the hash value after replacing the S box of the photon sponge with the coupled Chun–Hui He's iteration and Maiorana–McFarland S box for each cell.

End

1-Build structure size 16 × 16.

2-Fill the structure with random numbers within the Galois field (GF) 251 using the Chun–Hui He's iteration random algorithm, which can be seen in the next array.

14	10	3	2	11	100	200	209	88	99	12	8	7	0	0	1
2	244	233	230	44	23	97	49	66	65	21	233	23	54	67	78
34	76	89	09	12	56	23	32	45	54	67	90	10	2	9	4
5	4	88	77	45	23	19	200	80	33	67	59	34	76	49	90
41	31	44	51	81	3	2	10	68	99	87	4	3	66	33	12
22	32	24	36	48	5	9	12	22	47	88	98	56	34	23	53
23	97	49	89	09	12	23	97	49	66	12	8	7	0	0	1
56	23	32	88	77	43	56	23	32	45	21	233	23	54	67	78
23	19	200	44	51	66	23	19	200	80	67	90	10	2	9	4
3	2	10	24	36	76	3	2	10	68	67	59	34	76	49	90
12	8	7	0	0	1	23	97	49	66	87	4	3	66	33	12
21	233	23	54	67	78	23	97	89	09	89	98	56	34	23	53
67	90	10	2	9	4	56	23	88	77	88	97	67	90	89	09
67	59	34	76	49	90	23	19	44	51	44	23	67	59	88	77
87	4	3	66	33	12	3	2	24	36	24	19	87	4	44	51
88	98	56	34	23	53	23	97	89	09	89	2	67	90	24	36

3-For each cell, we specify four directions: top, down, right, and left. Then, apply the finite set operations for each direction.

1. top (the top of row 0 is row 15) Top in index 0.0 is 88, then apply finite set operation $x2$

We select five cells to check:

Top [0, 0] = (88*88) mode 251 = 214

Top [0, 15] = (36*36) mode 251 = 41

Top [0, 3] = (34*34) mode 251 = 152

Top [0, 6] = (23*23) mode 251 = 27

Top [0, 8] = (89*89) mode 251 = 140

Then, this operation is applied to all cells.

The resulting array is as follows:

214	66	124	152	27	48	27	122	140	81	140	4	222	68	74	41
196	100	9	4	121	211	91	7	214	12	144	72	49	0	0	1
4	49	73	190	179	27	122	142	89	209	190	73	27	155	222	60
152	3	66	81	144	124	27	27	17	155	222	68	100	4	81	16
25	16	214	156	17	27	110	91	341	85	222	218	152	3	142	68
175	208	179	91	35	9	4	100	106	12	39	16	9	89	85	144
233	20	74	41	45	25	81	144	233	201	214	66	124	152	27	48
27	122	142	140	81	144	27	122	142	89	144	64	49	0	0	1
124	27	20	214	156	92	124	27	27	17	190	73	27	155	222	60
27	110	91	179	91	89	27	110	91	125	222	68	100	4	81	16
9	4	100	74	41	3	9	4	100	106	222	218	152	3	142	68
144	64	49	0	0	1	27	122	142	89	39	16	9	89	85	144
190	73	27	155	222	60	27	122	140	81	140	66	124	152	27	48
222	68	100	4	81	16	124	27	214	156	214	122	222	68	140	81
222	218	152	3	142	68	27	110	179	91	179	27	222	218	214	156
39	16	9	89	85	144	9	4	74	41	74	110	39	16	179	91

2-Down (the down of row 15 is row 0)

Down 14 is 2, then apply finite set operation $x2 + 1$

We select five cells randomly to check:

Down [15, 0] = (14*14) + 1 mode 251 = 197
Down [15, 15] = (1*1) + 1 mode 251 = 2
Down [0, 2] = (233*233) + 1 mode 251 = 74
Down [10, 3] = (0*0) + 1 mode 251 = 1
Down [0, 5] = (23*23) + 1 mode 251 = 28
The resulting array is as follows:

5	50	74	191	180	28	123	143	90	210	191	74	28	156	223	61
153	4	141	82	145	125	28	21	18	156	223	69	101	5	82	17
26	17	215	157	18	28	111	92	126	86	223	219	153	4	143	69
176	209	180	92	36	10	5	101	109	13	40	17	10	90	86	145
234	21	75	42	46	26	82	145	234	202	215	67	125	153	28	49
28	123	143	141	82	145	28	123	143	90	145	65	50	1	1	2
125	28	21	215	157	93	125	28	21	90	191	74	28	156	223	61
28	111	92	180	92	90	28	111	92	126	223	69	101	5	82	17
10	5	101	75	42	4	10	5	101	107	223	219	153	4	143	69
145	65	50	1	1	2	28	123	143	90	40	17	10	90	86	145
191	74	28	156	223	61	28	123	141	82	141	67	125	153	28	49
223	69	101	5	52	17	125	28	215	157	215	123	223	69	141	82
223	219	153	4	143	69	28	111	180	92	180	28	223	69	215	157
40	17	10	90	86	145	10	5	75	42	75	111	40	17	180	92
215	67	125	153	28	49	28	123	143	82	143	5	123	69	75	42
197	101	10	5	122	212	92	8	215	13	145	65	50	1	1	2

3-Left (the left of column 0 is column 15)
Left 14 is 1, then apply finite set operation $x + 2$
Left [0, 0] = (1 + 2) mode 251 = 3
Left [0, 1] = (14 + 2) mode 251 = 16
Left [15, 0] = (36 + 2) mode 251 = 38
Left [6, 0] = (1 + 2) mode 251 = 3
The resulting array is as follows:

3	16	12	5	4	13	102	202	211	90	101	14	10	9	2	2
80	4	246	235	232	46	25	99	51	68	67	23	235	25	56	69
6	36	78	91	11	14	58	25	34	47	56	69	92	12	4	11
92	7	6	90	79	47	25	21	202	82	35	69	61	36	78	51
14	43	33	46	53	83	5	4	12	70	101	89	6	5	68	35
55	24	34	26	38	50	7	11	14	24	49	90	100	58	36	25
3	25	99	51	91	11	14	25	99	51	68	14	10	9	2	2
80	58	25	34	90	79	45	58	25	34	47	23	235	25	56	69
6	25	21	202	46	53	68	25	21	202	82	69	92	12	4	11
11	5	4	12	26	38	78	5	4	12	70	69	61	36	78	51
14	14	10	9	2	2	3	25	99	51	68	89	6	5	68	35
55	23	235	25	56	69	80	25	99	91	11	91	100	58	36	25
11	69	92	12	4	11	6	58	25	90	79	90	99	69	92	91
79	69	61	36	78	51	92	25	21	46	53	46	25	69	61	90
53	89	6	5	68	35	14	5	4	26	38	26	21	89	6	46
38	90	100	58	36	25	55	25	99	91	11	91	4	69	92	26

4-Right (the right of column 15 is column 0)
Right [0, 0] is 10, then apply finite site $x + 1$
Select cells randomly to check:
Right [0, 0] = (10 + 1) mode 251 = 11
Right [0, 1] = (3 + 1) mode 251 = 4
Right [1, 0] = (244 + 1) mode 251 = 245
Right [0, 14] = (1 + 1) mode 251 = 2
Right [0, 15] = (14 + 1) mode 251 = 15
The resulting array is as follows:

11	4	3	12	101	201	210	89	100	13	9	8	1	1	2	15
245	234	231	45	24	98	50	67	66	22	234	24	55	68	79	3
77	90	10	13	57	24	33	46	55	68	91	11	3	10	5	35
5	89	78	46	24	20	201	81	34	68	60	35	77	50	91	6
32	45	52	82	4	3	11	69	100	89	5	4	67	34	13	42
33	25	37	49	6	10	13	23	48	89	99	57	35	24	54	23
98	50	90	10	13	24	98	50	67	13	9	8	1	1	2	24
24	33	89	78	44	57	24	33	46	22	234	24	55	68	79	57
20	201	45	52	67	24	20	201	81	68	91	11	3	10	5	24
3	11	25	37	77	4	3	11	69	68	60	35	77	50	91	4
9	8	1	1	2	24	98	50	67	88	5	4	67	34	13	13
234	24	54	68	79	4	98	90	10	90	99	57	35	24	54	22
91	11	3	10	5	57	24	89	78	89	98	68	91	90	10	68
60	35	477	50	91	24	20	45	52	45	24	68	60	89	78	68
5	4	67	34	13	4	3	25	37	25	20	88	5	45	52	88
99	57	35	24	54	24	98	90	10	90	3	68	91	25	37	89

4-Apply the hash function for each cell after replacing the S-box of the photon sponge hash function with the S-box constructed using the Maiorana–McFarland algorithm. We need to define a new S-box using the Chun–Hui He's iteration and the Maiorana–McFarland method and integrate it into the photon sponge hash function, the result after replacing the S box of photon with the S box of MM.

Hash = f (top, down, left, right)

Cell [0, 15] = (41, 61, 2, 15)

SHA-256(41, 61, 2, 15) = 2ds43d61ccf89b7bb57e3d021b0-da5a1a6e17a8a85b6ce890ae988af5205b940

Cell [15,15] = (91, 36, 26, 89)

SHA-256(91, 36, 26, 89) = 451a3e11a7a4c684758d1c065f-daf737e56b1a2bfc6bfa7c1b92561beeb67d9f

8 Results and discussion

The proposed system is compared with the traditional photon hash function n and photon hash function proposal algorithm according to several evaluation criteria mentioned. Tables 2 and 3 show this comparison.

As shown in Tables 2 and 3, the new method has produced more randomness and security than the standard photon sponge hash function. To enhance security and prevent forgery and replication attempts, the proposed digital currency employed a random (Chun–Hui He's iteration) filling method to populate the matrix structure. We established interconnections from all directions (Top, Down, Left, and Right) and applied equations from the finite set to derive the values. Additionally, we utilized a hash function (SHA-256) that took the four directions as inputs. This approach strengthened the currency's resistance against fraudulent activities and unauthorized duplication. The proposed system gave better results than the traditional photon sponge hash function, and the encryption and decryption time was less.

9 Conclusion and future work

Designing a new digital currency requires addressing various challenges, such as scalability, security, decentralization, user

Table 2: NIST Test Suite comparison between standard photon hash function and modified photon hash function

Test No.	Statistical test name	Standard photon		Modified Photon	
		P-value	Status	*P*-value	Status
1	Approximate entropy	0	Fail	0.421	Pass
2	Block frequency	0.050	Pass	0.556	Pass
3	Cumulative sum	0.876	Pass	0.786	Pass
4	Discrete Fourier transform	0.662	Pass	0.832	Pass
5	Frequency	0.433	Pass	0.671	Pass
6	Linear complexity	0.543	Pass	0.852	Pass
7	Longest run	1.000	Pass	1.000	Pass
8	Non-overlapping template	0.326	Pass	0.474	Pass
9	Overlapping template	0.025	Pass	0.222	Pass
10	Random excursions	0	Fail	0.659	Pass
11	Random excursion variant	0	Fail	0.399	Pass
12	Rank	0	Pass	0.228	Pass
13	Runs	0.132	Pass	0.723	Pass
14	Serial	0	Fail	0.743	Pass
15	Universal	0.044	Pass	0.322	Pass

Table 3: Compression between the standard photon sponge hash function and the modified Photon sponge hash function

Security metrics	Traditional present	Present proposal
1 – correlation coefficient	−0.122251573	−0.30287
2 – entropy of plain text	0.395537806	0.20062288645
3 – entropy of cipher text	0.974489403	0.9936507
4 – bijective property	False	True
5 – balanced criteria	False	True
6 – completeness criteria	False	True
7 – avalanche criteria	60	64
8 – strict avalanche criteria (SAC)	64	64
9 – encryption time	0.000996828	0.000520229339
10 – decryption time	0.001009703	0.001325607299

adoption, and regulatory compliance. We designed a structure size of 16 × 16 and distributed the numbers randomly using an algorithm (Chun–Hui He's iteration) to increase randomness. Then, we generated four matrices, each matrix representing the direction (top, down, right, and left), and then encoded the arrays using the (photon sponge hash function) algorithm. Then, we updated the S-box by merging algorithms (Chun–Hui He's iteration and Maiorana–McFarland) for the purpose of increasing randomness and security so that the theft and forgery process is difficult. A cipher's cryptographic characteristics, especially its non-linearity, diffusion, and resistance to cryptanalysis, can be improved by combining the Maiorana–McFarland and Chun–Hei He's iterations. While Chun–Hei He's iteration can improve the confusion and diffusion qualities through its iterative procedure, the Maiorana–McFarland transformation increases nonlinearity by altering the Boolean function representation. When these two methods are used together, the resulting cipher can function more efficiently and with greater security than when they are used separately. The cipher is also more appropriate for secure data transport and storage applications since the combination of these iterations can offer more resilient protection against different cryptanalytic attacks. Future studies could involve improving technical aspects of digital currency, enhancing privacy and security, investigating user experience and adoption as well as improving regulatory framework.

Funding information: Authors state no funding involved.

Author contributions: All authors have accepted responsibility for the entire content of this manuscript and consented to its submission to the journal, reviewed all the results and approved the final version of the manuscript. AMSR and HBA presented the main problem, analyzed it, and developed a simple preliminary plan. AAM implemented the problem programmatically, analyzed the results, applied security and randomness measures.

Conflict of interest: The authors state no conflict of interest.

Data availability statement: Most datasets generated and analyzed in this study are within the manuscript. The other datasets are available on reasonable request from the corresponding author with the attached information.

References

[1] Mikołajewicz-Woźniak A, Scheibe A. Virtual currency schemes–the future of financial services. Foresight. 2015 Aug;17(4):365–77.

[2] Al-Farhani LH, Varfolomeev AA. Blockchain Fog-based scheme for identity authentication in smart building. Al-Qadisiyah J Eng Sci. 2023;16(3):218–27.

[3] Peters GW, Panayi E, Chapelle A. Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective. arXiv preprint arXiv:1508.04364; 2015 Aug.

[4] Swan M. Blockchain: Blueprint for a new economy. Sebastopol: O'Reilly Media, Inc.; 2015 Jan.

[5] Aftan AO. Design of cofdm system in digital mobile communication. Al-Qadisiyah J Eng Sci. 2010;3(4):414–24.

[6] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. www.bitcoin.org; 2008.

[7] Hineman A, Blaum M. A modified Shamir secret sharing scheme with efficient encoding. IEEE Commun Lett. 2022 Jan;26(4):758–62.

[8] Khan AG, Zahid AH, Hussain M, Riaz U. Security of cryptocurrency using hardware wallet and qr code. In 2019 International Conference on Innovative Computing (ICIC). IEEE; 2019 Nov. p. 1–10.

[9] Ghalwesh A, Ouf S, Sayed A. A proposed system for securing cryptocurrency *via* the integration of internet of things with Blockchain. Int J Econ Financ Issues. 2020;10(3):166.

[10] Mbaye ML, Bodian A, Kimambo ON, Rouamba FI, Gaveta E. Analyses of past extremes precipitation–evapotranspiration indices over Sub-saharan Countries. J Extreme Events. 2021 Dec;8(4):2250002.

[11] Garratt R, Yu J, Zhu H. How central bank digital currency design choices impact monetary policy pass-through and market composition. Available at SSRN 4004341; 2022.

[12] Kakebayashi M. The potential of central bank digital currency for transforming public finance: a focus on VAT systems. Available at SSRN 4449562; 2023 May.

[13] Mullan PC. History of digital currency in the United States. New York: Palgrave Macmillan; 2016.

[14] Frick TA. Virtual and cryptocurrencies – regulatory and anti-money laundering approaches in the European Union and in Switzerland. In Era Forum. Vol. 20, No. 1, Berlin/Heidelberg: Springer Berlin Heidelberg; 2019 Jul. p. 99–112.

[15] Hasan Y, Wijanarko Y, Muslimin S, Maulidda R. The automatic door lock to enhance security in RFID system. In Journal of Physics: Conference Series. Vol. 1500, No. 1, IOP Publishing; 2020 Apr. p. 012132.

[16] Amaral G, Sales TP, Guizzardi G. Towards ontological foundations for central bank digital currencies. In CEUR Workshop Proceedings. Vol. 2835, Rheinisch Westfälische Technische Hochschule; 2021. p. 77–86.

[17] Narayanan A, Bonneau J, Felten E, Miller A, Goldfeder S. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton: Princeton University Press; 2016 Jul.

[18] Yanchao Y. On the legal attributes of digital currency. Soc Sci China. 2021 Apr;42(2):123–41.

[19] Narayanan H. Is future a rule of digital currency. Int J Research-GRANTHAALAYAH. 2020;8(8):96–106.

[20] Bunjaku F, Gjorgieva-Trajkovska O, Miteva-Kacarski E. Cryptocurrencies–advantages and disadvantages. J Econ. 2017 Dec;2(1):31–9.

[21] Abd ZN, Rushdi SA. Investigation of overall mass transfer coefficient of CO_2 absorption in packed Column. Al-Qadisiyah J Eng Sci. 2020 Jun;13(2):153–7.

[22] Nabilou H. Testing the waters of the Rubicon: the European Central Bank and central bank digital currencies. J Bank Regul. 2020 Dec;21(4):299–314.

[23] Gans JS, Halaburda H. Some economics of private digital currency. In: Economic Analysis of the Digital Economy. Chicago: University of Chicago Press; 2015. p. 257–76.

[24] Popescu AD. Non-fungible tokens (nft)–innovation beyond the craze. In 5th International Conference on Innovation in Business, Economics and Marketing Research. Vol. 32; 2021 May.

[25] Tu KV, Meredith MW. Rethinking virtual currency regulation in the Bitcoin age. Wash L Rev. 2015;90:271.

[26] Carstens A. Digital currencies and the soul of money. In Speech as Goethe University's Institute for Law and Finance (ILF) Conference on "Data, Digitalization, the New Finance and Central Bank Digital Currencies: The Future of Banking and Money. Vol. 18; 2022 Jan.

[27] Khan WA. Numerical simulation of Chun-Hui He's iteration method with applications in engineering. Int J Numer Methods Heat Fluid Flow. 2022 Jan;32(3):944–55.

[28] Khan WA, Arif M, Mohammed M, Farooq U, Farooq FB, Elbashir MK, et al. Numerical and theoretical investigation to estimate Darcy friction factor in water network problem based on modified Chun-Hui He's algorithm and applications. Math Probl Eng. 2022 Feb;2022:8116282.

[29] He CH. An introduction to an ancient Chinese algorithm and its modification. Int J Numer Methods Heat Fluid Flow. 2016 Nov;26(8):2486–91.

[30] Megha Mukundan P, Manayankath S, Srinivasan C, Sethumadhavan M. Hash-One: a lightweight cryptographic hash function. IET Inf Secur. 2016 Sep;10(5):225–31.

[31] Stamp M. Information security: principles and practice. Hoboken, New Jersey: John Wiley & Sons; 2011 Nov. p. 452.

[32] Ali NA, Rahma AM, Shaker SH. 3D content encryption using multilevel chaotic maps. Iraqi J Sci. 2023 May;64:2521–32.

[33] Wahab HB, Mohammed MA. Improvement A5/1 encryption algorithm based on sponge techniques. In 2015 World Congress on Information Technology and Computer Applications (WCITCA). Hammamet, Tunisia: IEEE; 2015 Jun. p. 1–5.

[34] Taresh H, Raheema A. AES with chaotic using chebyshev polynomial. Iraqi J Comput Inform. 2018;44(2):35–40.

[35] Maiorana J, McFarland D. Generation of cryptographic s-boxes. In: Proceedings of the international symposium on information theory. Kobe, Japan; 1988. p. 213–7.

[36] Lopes RHC, Franqueira VNL, Hobson PR. Efficient computation of hashes. J Phys: Conf Ser. 2014;513(3):2–5.

[37] Bykov DA, Kolomeec NA. On a lower bound for the number of bent functions at the minimum distance from a bent function in the Maiorana–McFarland class. J Appl Ind Mathematics. 2023 Sep;17(3):507–20.

[38] Bapić A, Pasalic E. Constructions of (vectorial) bent functions outside the completed Maiorana–McFarland class. Discret Appl Mathematics. 2022 Jun;314:197–212.

[39] Iwańczuk-Kaliska A. Potential implications of retail central bank digital currency for banking systems identified in the literature and by central banks. Accounting, Econ, Law: A Conviv. 2023 May;30:271–303.

[40] Chen H. The Maiorana-McFarland structure based cryptanalysis of Simon. Cryptol ePrint Arch. 2021;1–36.