Using Lotka-Volterra Equations and Lightweight Post-Quantum Algorithm to Develop Lightweight Blockchain Security

Rasha Hani Salman[1,*], **Hala Bahjat Abdul Wahab**[2]

[1]Informatics Institute for Graduate Studies, University of Information Technology and Communications, Baghdad, Iraq

[2]Computer Sciences Department, University of Technology, Baghdad, Iraq

Email; rsalman@uowasit.edu.iq; Hala.B.AbdulWahab@uotechology.edu.iq

Abstract

Blockchain technology is now widely used in data sharing, cryptocurrency industry, Internet of Things and other fields. However, despite its increasing use, security and privacy concerns remain important issues. Blockchain security is enhanced by the use of hashing algorithms that ensure data integrity and provide a solution to security problems, but hashing algorithms usually have limitations in terms of resource consumption, memory and speed. To overcome these obstacles, the efficiency and security of the hashing algorithm used in blockchain must be increased. This paper presents a proposal to improve the hashing process in blockchain by leveraging the lightweight quantum algorithm Ascon, which has been improved after integrating it with nonlinear Lotka-Volterra equations. This integration can improve performance and security by combining the mathematical principles of these nonlinear equations to study the interactions between systems. Through this integration, it is possible to improve power management and work on intelligent resource allocation, as well as make the system more robust against attacks by complicating the random number generation process. The performance of the proposed system was tested in terms of throughput, elapsed time, amount of memory used, and time required to process data. The results showed that the proposed algorithm outperforms the original Ascon algorithm in terms of providing faster processing while maintaining a high level of performance and security, reducing time, and increasing the amount of data processed with less memory required for storage. These improvements are of great importance in developing blockchain technology and enabling its multiple uses in many applications.

Keywords: Lightweight blockchain; Cryptographic hashing; Post-quantum algorithm; Ascon algorithm; Lotka–Volterraequation; Performance optimization

1. Introduction

With the development of blockchain technology, it has become very important and has a strong impact on many industries, including financial services and e-government. It is very important for data management and information security due to its transparency and decentralized design, which is difficult to penetrate. Blockchain supports e-government, which creates a new approach to increasing performance efficiency, transparency and accountability in developing countries, where governments suffer from problems in education systems, high crime rates and lack of public services. The message patterns that are cryptographic hash functions are the basic components of blockchain functions. They transform variable-length inputs into fixed-length outputs. Data verification, transaction authentication, and secure communication protocols are all derived from hash functions. Blockchain technology has many advantages, but traditional hashing operations prevent its expansion, especially in resource-limited environments such as IoT and low-power devices. The security and integrity of blockchain-based systems are at risk due to the recent increase in quantum computing. Some algorithms have been shown to

DOI: https://doi.org/10.54216/FPA.190112
Received: November 10, 2024 Revised: January 17, 2025 Accepted: February 14, 2025

be able to break publi[2]c-key encryption and reduce the computational resistance of hash functions, such as Shor and Grover's algorithm [7][8] . With the recent increase in interest in post-quantum cryptography, the blockchain community has become interested in this type of cryptography, which is a modern field of study dedicated to creating robust systems that can repel quantum attacks. In order to provide appropriate solutions to this problem, lightweight encryption methods were used to find a balance between performance efficiency and security. These algorithms have become a focus of interest, especially in resource-limited environments. The blockchain technology, which relies on traditional hashing algorithms such as SHA-256, is not suitable for environments that require saving battery life, low memory consumption, and low computing power. In addition, it is not secure against quantum attacks.

Combining a lightweight algorithm like Ascon with Lotka-Volterraequations improves blockchain performance in many areas such as efficiency, security, and dynamic analysis. The main important contributions made by this paper are:

- Improving the consensus mechanism: The use of Lotka-Volterraequations allows describing the dynamic interactions between nodes, which helps improve the efficiency of consensus processes and increase the speed of reaching accurate collective decisions.
- Enhancing network security: Introducing dynamics inspired by the Lotka-Volterraequations adds new complexity that makes it difficult for attackers to predict systemic behaviour, enhancing the network's resistance to attacks.
- Reducing transaction delays: By optimizing node interaction and effectively managing resources, delays associated with hashing and transaction processing can be reduced, improving overall network performance.
- Intelligent resource management: Combining these equations provides an efficient mathematical method for analyzing the distribution of resources, such as computing power, based on network dynamics and node interaction.
- Introducing an innovative mathematical model: Using the Lotka-Volterra equations in a blockchain environment is an unconventional approach that opens up new horizons for understanding and analyzing complex interactive processes in decentralized networks.

2. Related work

The basis of crucial technologies like blockchain, cryptography, and data verification, hashing became important in recent years for the safe processing of data. Despite the fact that research has been devoted to developing and improving hashing methods, issues regarding effectiveness, safety, and resistance to new threats still exist.. This section examines earlier research that demonstrates hashing algorithms with a blockchain focus.

A new optimization method for blockchain hashing algorithms based on Proactive Reconfigurable Computing Architecture (PRCA) was suggested in [11]. By integrating blockchain technology with mimic computers, this method seeks to optimize communication infrastructure and network data transfer while improving the computation performance of hashing functions with a pipeline-hashing algorithm. The authors additionally choose lightweight hashing algorithms for numerous hashing processes and change the hash algorithm's structure to ensure data security.

A hash generation algorithm for block chain based on novel Merkle-Damgård construction and logistic maps (1D and 2D) from chaos theory was proposed in [12]. Time, complexity, and collision tests are performed on the hash outputs. When the suggested approach is assessed using a variety of transaction metrics and Jaccard similarity, it is discovered that the input and output similarity is less than 0.1932 percent. Every outcome point to a successful performance. The suggested technique takes only a few milliseconds to run and uses fewer resources than other hash algorithms (such SHA1, SHA2, and MD5) when it is implemented on a blockchain-based transaction flow system.

The researcher in [13] proposes a lightweight cryptography system that uses logistic maps to generate a hash algorithm for a block chain based on a chaotic key (hamming bird 2). The time and difficulty of guessing hash outputs are evaluated using cryptanalysis techniques. To test the suggested technique, cryptanalysis site-based brute attack using force. The outcome demonstrates that under all cryptanalysis settings, the updated hash cannot be recognized by site, demonstrating the strong generated hash to thwart attacks.

A genetic-based hashing algorithm in blockchain for data security has been proposed in [14] for strong collapse effect, lower computational cost, low space coverage, increased security and integrity. The simulation will demonstrate the integrity, authenticity and immunity of the data record. This secure decentralized network uses a modified 512-bit cryptographic hashing method. The key required to encrypt and decrypt medical data is generated

DOI: https://doi.org/10.54216/FPA.190112
Received: November 10, 2024 Revised: January 17, 2025 Accepted: February 14, 2025

using a genetic algorithm (GA). A genetic algorithm is a metaheuristic method that is commonly used to produce excellent solutions to difficult problems. It is inspired by the rules of genetics. In the medical fields of radiology, cancer, cardiology, endocrinology, surgery, oncology and radiation.

Improved Iterations of Conventional Hashing Algorithms, the researcher in [15] suggested SHA-288, a 288-bit variation that lowered the number of rounds from 64 to 44 in order to overcome the drawbacks of SHA-256. The method maintained strong data dispersion in spite of this decrease, providing faster execution, increased security, and more energy economy.

The authors are creating a local blockchain application using a novel hashing algorithm (SHA-512)in [16], The highly secure SHA-512 algorithm works with 1024-bit blocks and 64-bit words. Using a few mathematical models, they are demonstrating that SHA-512 is more resistant to collisions than its predecessor is. Used sophisticated mathematical modelling to show the promise of SHA-512 in blockchain systems, emphasizing its strong cryptographic security and improved resilience to collisions.

An optimized encryption-hashing scheme is introduced in [17] to generate a hash value, which prevents the hash value from being the same and provides double data protection. In this system, an improved advanced encryption algorithm is used that determines the key value based on the input data using the cuckoo search algorithm. The improved approach produces different cryptographic hash values. The hash value indicates the file path and is stored in the blockchain. The authors use IPFS to encrypt and store files across a decentralized network, enhancing data availability and helping to ensure its immutability.

3. Research gap

These studies highlight the important developments in blockchain hashing algorithms, but they also point out the on-going difficulties faced in using many traditional hashing algorithms such as SHA-256 and others, most notably their high resource consumption. They require high computing power to encrypt and distribute data, in addition to their need to store duplicate copies of data to ensure resilience, which leads to a significant drain on energy and storage resources, making them unsuitable for lightweight blockchains used in resource-constrained environments such as Etc. These algorithms also suffer from poor distribution efficiency, as it is difficult to balance between nodes with different capabilities. Moreover, they lack sufficient security to address post-quantum technologies, as they were not designed to address the challenges posed by quantum computing. Thus, a clear research gap emerges between the limited performance of these algorithms and the need of modern blockchain networks for less resource-intensive solutions that are more flexible in dealing with changing environments and nodes with limited capabilities, in addition to the need to improve security against advanced threats that quantum computing will impose in the future.

4. Motivation of this work

The proposed research describes the utilization of the lightweight post-quantum algorithm "Ascon" in conjunction with dynamic Lotka-Volterraequations in the blockchain environment in order to achieve high effectiveness and superior security, specifically in environments that are resource limited, such as IoT. Ascon is recognized by its lightweight nature and high efficiency, both of which contribute to the reduction of energy consumption, in addition to reducing the need to store duplicate copies via dynamic hashing methods supported by Lotka-Volterraequations. In addition, Ascon is compatible with post-quantum security requirements, which makes it resistant to quantum attacks, additionally; Lotka-Volterraequations augment the analysis of interactions between nodes, which increases the network's capacity to recognize malicious behavior. Additionally, the combination of the two approaches allows for the analysis of network dynamics in real time, this contributes to the efficient distribution of resources based on changes in demand and load, and improves the fair distribution of data between nodes, which reduces the stress on nodes with limited capabilities, and creates an optimal balance that produces a lightweight and safe blockchain that can be employed in various applications..

5. Blockchain security and threats

Blockchain functions as a distributed, decentralized ledger that includes network participants that collaborate to maintain a precise record of all transactions. By creating blocks and utilizing global consensus methods to rectify and approve transactions, this collective effort ensures that all participants remain in agreement [18][19]. The utilization of cryptographic hashing methods to ensure data authenticity, secrecy, and anonymity is integral to blockchain technology. In Proof-of-work (PoW) systems, which are crucial to preserving equality and avoiding malevolent attacks, hashing decreases the overhead of processing while still allowing for a quick verification. SHA-256 is one of the most commonly employed hashing methods in blockchain-based systems, particularly in Bitcoin. SHA-256 is a powerful method of encryption that is effective, but it has several problems, including high computational requirements, ineffective utilization of resources, and susceptibility to quantum computing attacks. These imperfections negatively impact the fundamental principles of blockchain technology safety, decentralization, and transparency, which leads to lower confidence, less innovation, financial losses, and a

DOI: https://doi.org/10.54216/FPA.190112
Received: November 10, 2024 Revised: January 17, 2025 Accepted: February 14, 2025

decrease in trust between users of the system, developers, and investors.. Strong security protocols, proactive governance, and ongoing technological development are essential for preserving blockchain's integrity and long-term sustainability.

Double-spending attacks, which take advantage of the same cash in several transactions, are one of the biggest risks to blockchain systems. Double-spending attack variations include:

Race Attack: This is a easy attack on PoW-based blockchains in which a hacker quickly transmits two contradicting transactions to the network. As a result, retailers may accept a payment that is subsequently cancelled [25][26][27].

Finney Attack: In this attack, the attacker spends the same money after pre-mining a block that contains a transaction. Usually involving coordination with a miner, the attack needs at least one confirmation to be successful [28][29].

Attack by Vector76: This technique, which combines aspects of double-spending and privately mined blocks, is often referred to as a one-confirmation attack. It targets cryptocurrency exchanges that directly receive incoming connections, leaving them open to abuse by using static IP addresses [28].

Alternative History Attack: This attack creates a different blockchain history and requires a high hash rate. It becomes possible in networks that need several confirmations, but it exposes the attacker to the dangers of excessive electricity usage [30].

When one person or organization controls more than 50% of the network's hashing power, it is known as a 51% attack. By removing transactions, reversing transactions, or permitting double-spending, the offender might manipulate the network and cause blockchain instability [31][32].

These attack methods highlight the intrinsic weaknesses in blockchain technology, particularly in proof-of-work (PoW) systems. They jeopardize the secure and decentralized character of blockchain, endangering its use and acceptance across a range of industries. To improve blockchain security, scalability, and sustainability, these issues must be addressed by creating quantum-resistant cryptographical algorithms and using more energy-efficient consensus techniques.

By incorporating the post-quantum, lightweight Ascon algorithm into blockchain systems, this work seeks to overcome these issues. The suggested method improves security while using less computing power by improving Ascon using the dynamic features of nonlinear Lotka-Volterraequations. This development helps create a more resilient, effective, and quantum-resistant blockchain architecture that can handle today's security issues [33].

6. Lightweight post quantum encryption algorithm.

Asymmetric key encryption and hashing, or Ascon, is a suitable technique for resource-constrained applications. The goal of the CAESAR competition was to find new, portable electronics-appropriate authenticated encryption methods. As one of the finalists, Ascon received recognition for its effectiveness, security, and flexibility. During the NIST competition, Ascon garnered attention as a possible standardizing option after winning the lightweight competition [34].

6.1 Ascon Hashing onstruction

The sponge construction is the hashing mode of operation. The same hashing algorithm $X_{h,,r,a}$ (see Table 1), which is described in Algorithm1 and shown in Fig. 2, is internally used by variable output size, is used internally by the hash function Ascon -Hash with fixed output size[35].

Table 1: parameter for encrypted methods with authentication [35]

Name	Algorithm	Bit size of			Round	
		Key tag	Nonce	Datablock	p^a	p^b
ASCON-128	$\mathcal{E}\ D_{128,64,12,6}$	128	128	64	12	6

DOI: https://doi.org/10.54216/FPA.190112
Received: November 10, 2024 Revised: January 17, 2025 Accepted: February 14, 2025

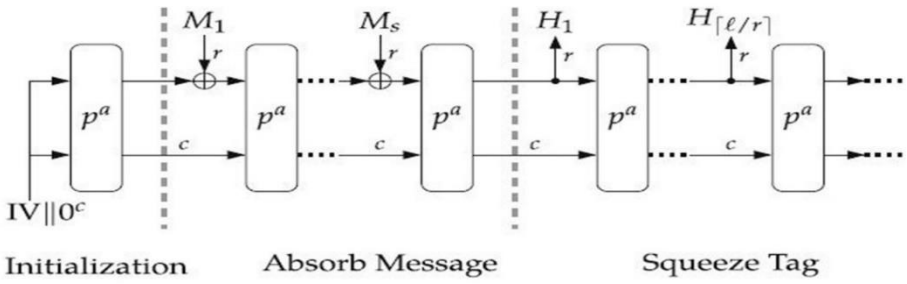

Figure 2. Ascon -Hash X h, r, a [35]

Ascon algorithm consist of many steps: Step1: Starting up the 320-bit initial state of Ascon -Hash is defined by a constant IV that describes the algorithm parameters in a manner similar to that of Ascon (including k = 0, the rate r, and round numbers a and b = 0, each written as an 8-bit integer). This is followed by a 256-bit zero value and the maximum output length of h bits, ich is a 32-bit integer (h = 256 for Ascon-Hash). To initialize the state S, the a-round permutation p^a is used: $IV_{h,r,a} \leftarrow O^8 \parallel r \parallel a \parallel O^8 \parallel h = \{00400c0000000100 \text{ for Ascon} - \text{Hash}\}$

$S \leftarrow p^a$ (IV $h, r, a \parallel 0^{256}$)

Each instance's initial 320-bit state S can be precomputed, and we obtain the Ascon -Hash

$$S \leftarrow ee9398aadb67fo3d$$
$$8bb21831c6of1oo2$$
$$b48a92db98d5da62$$
$$43189921b8fe3e8$$
$$348fa5cd525e140$$

Step2: Absorbing Message

Blocks of r bits are used by Ascon -Hash to process message M. In the same way as with Ascon 's plaintext, the padding procedure adds a single 1 and the fewest possible 0s to M so that the padded message's length is more than r bits. The padded text that is produced is divided into s blocks of r bits.

$$M_1 \parallel \cdots \parallel M_s$$
$$M_{1,\ldots,}M_s \leftarrow r - bit\ block\ of\ M \parallel 1 \parallel 0^{r-1-(\backslash M \backslash mod\ r)}$$

The following is the processing of the message blocks Mi with i = 1..., s. After applying the a-round permutation p^a on S, each block Mi is xored to the state S's first r bits, Sr:

$S \leftarrow P^a((S_r \oplus M_i) \parallel S_c \quad 1 \leq i \leq S$

Step3: Squeezing

Squeezing The state in r-bit blocks yield the hash output. till the output length requested. Blocks t = [ℓ/r] are completed after ℓ ≤ h. The a-round permutation p^a modifies the internal state S following each extraction

$$H_i \leftarrow S_r$$
$$S \leftarrow P^a(S) \qquad 1 \leq i \leq t = [\ell/r]$$

Unless r divides ℓ, the final output block Ht is trimmed to ℓ mod r bits, and H= H_1ll …ll H't returned:

$$H_t \leftarrow [H_t]_{\ell\ mod\ r}$$

The two 320-bit permutations, p^a and p^b, are the fundamental parts of the Ascon -Hash algorithms. Three phases, PC, PS, and PL, make up the SPN-based round transformation p, which is iteratively applied by the permutations:

$$P = PL \circ PS \circ PC$$

DOI: https://doi.org/10.54216/FPA.190112
Received: November 10, 2024 Revised: January 17, 2025 Accepted: February 14, 2025

All that separates p^a and p^b is the quantity of rounds. Two configurable security parameters are the number of rounds (a) and (b). The 320-bit state S is divided into five 64-bit registers, or words xi, for the purpose of describing and applying the round transformations:

$$S = X_0 \parallel X_1 \parallel X_2 \parallel X_3 \parallel X_4$$

As shown in figure 3. Constants are added in round i, the round constant Cr is added by the constant addition step PC to the register word x_2 of the state S as shown in figure 3. The indices r and i both begin at zero, and for p^a and p^b, we utilize r = i and r = a − b, respectively [34]. The pseudo code for Ascon hashing can be express in algorthim1

	Algorithm1: Ascon Hashing Process	
	Input:	**message**
	Output:	**hash output**

Begin	**Step1: states initialize** $S = [IV, rate_{bits}, message_{len_{bits}}, constant1, constant2]$ **Step2: The message absorbs into state** m_ padding = pad_ message(message)
	for block in m_ padding:
	S [0] ^= block **Step 3: Permutation Process (s)** for r in range (12):
	Round constant addition:
	S [2] ^= round_ constants[r]
	Substitution layer (S-box)
	S [0] ^= S [4]
	S [4] ^= S [3]
	S [2] ^= S [1]
	Linear diffusion layer
	for i in range (5):
	S[i] = rotr(S[i], rotation_ values[i]) **Step 4: Squeeze the state to get the hash**
	hash_ output = ""
	while Len (hash_ output) < hash length:
	hash_ output += squeeze(S)
	permutation process (S) **step5: hash_ output [: hash length]**
	extract S0 and add to hash result
	permutation process (S).	

End		

DOI: https://doi.org/10.54216/FPA.190112
Received: November 10, 2024 Revised: January 17, 2025 Accepted: February 14, 2025

	Squeeze the output until the necessary hash length (hash length) is reached. Provide the completed hash result with the desired hash length truncated. **tep6: Output's Finalize** Provide the finished hash result, truncated to the hash length that was requested.

7. Lotka–VolterraEquations:

The dynamics of biological systems including competition or predator-prey relationships are typically modeled using the Lotka-Volterraequations, a collection of first-order nonlinear differential equations. An extension to a three-variable system adds a third interacting component, such as an environmental factor or an additional species, whereas the classical equations only include two interacting variables (predator and prey). The following is a mathematical expression for the three-variable Lotka-Volterramodel [36]:

$$\frac{dx}{dt} = x(\,a - by - cz)$$

$$\frac{dy}{dt} = y(d - ex - fz)$$

$$\frac{dz}{dt} = \mathrm{z}(\mathrm{g} - \mathrm{hx} - \mathrm{iy})$$

In this case, the populations (or levels) of the three interacting variables are denoted by x, y, and z. The interaction rates between the variables are defined by the constants a, b, c, d, e, f, g, h, and i. Depending on the parameter values, this extended model can account for complex interaction patterns such as equilibrium states, chaotic behavior, and cyclic dynamics [37, 38]. The three-variable Lotka-Volterraequations' nonlinearity results in complex interactions, such as predation, competition, and, in certain situations, chaotic dynamics. These chaotic dynamics demonstrate how sensitive the system is to initial settings, where even little changes can have radically different results. In other cases, the equations are Hamiltonian systems with energy-conserving characteristics and are prone to bifurcations, in which changes in the parameters lead to either periodic oscillations or chaos [39].

Important Lotka-VolterraEquation Properties Associated with Hashing Algorithms

The Lotka-Volterraequations' inherent qualities make them highly useful for cryptographic applications, particularly when creating safe hashing algorithms. Important characteristics include:

- Behavior of chaotic: High output variability is ensured via sensitivity to beginning conditions. Because it prevents predictability and improves security, this is an essential feature for safe hashing [40].

Nonlinearity

- Resilience against attacks that take advantage of predictable patterns, such linear cryptanalysis, is increased by the nonlinear interactions between variables. As a result, the hashing mechanism is more resilient.
- Deterministic Disorder: When given identical initial conditions, the equations' determinism ensures consistency of outputs despite their chaotic nature.
- The sensitivity of parameters Significant output variations result from slight adjustments to the initial conditions or input parameters. A sought after attribute of hashing algorithms, this property guarantees the avalanche effect, which is significant and random in its output [38].
- Systems of Adaptive Feedback: Dynamic changes in state are facilitated by the dependent variables in the equations. This facilitates increased dispersal and confusion when combined with cryptographic algorithms; this is essential for strong encryption and hashing.
- Because of their random and predetermined nature, the Lotka–Volterraequations are ideal for hashing that is both secure and efficient. Because of their large variability and lack of predictability, chaotic systems are resistant to a variety of decryption methods. The complex nature of the equations' dynamics causes them to have a greater degree of diffusion and confusion, and to have a more robust performance that is guaranteed by their sensitivity to initial conditions. Cryptographic methods, especially hash functions, have a higher degree of security, efficiency, and resilience when used with the Lotka– Volterra equations. Because of their properties, they are uniquely suited to the contemporary cryptographic issues, such as the threat of quantum computing.

DOI: https://doi.org/10.54216/FPA.190112
Received: November 10, 2024 Revised: January 17, 2025 Accepted: February 14, 2025

8. Proposed System

The resource limitations of traditional devices with limited resources and capabilities to use blockchain technology, such as wireless transmitters, medical implants, and wearable technology, are due to their poor processing, memory, and power capabilities, and thus are unable to handle the computational demands of typical blockchains. Due to this limitation, we have to design a lightweight, secure, and efficient blockchain for such devices. The Ascon hashing algorithm emerged and became famous for its doubt, efficient design, and lightweight, and it is particularly suitable for applications with limited resources, especially blockchain-based platforms for the Internet of Things (IoT) and mobile devices. Ascon's ability to withstand quantum attacks ensures that it will remain relevant in future blockchain networks. Its flexibility enhances the ability to adapt to the increasing performance of blockchain-based applications by providing fast and honest hashing tools. In addition, the Ascon design is inherently resistant to adversarial attacks, especially those seeking to marginalize data as well as transactions, which ensures the integrity of all private information in the data. This provides a robust security system in its basic structure and thus does not burden the network with its low resource demands, which in turn allows it to work with any lightweight security protocols. Combining the lightweight Ascon post-quantum algorithm (Algorithm 1) with the Lotka-Volterra equations (Algorithm 2), is the core of our proposed system, changing the traditional methods of blockchain hashing. This combination provides increased security, sustainability, and its ability to address the inefficiencies of the current and traditional blockchain by increasing its efficiency even in a resource-constrained environment, and providing a comprehensive and efficient transaction management system. Figure 3 illustrates the main stages of the proposed system using critical steps and provides a broad understanding with a focus on creativity, especially scientific ones.

(1) The process of transferring data across a contract or by a prior user in blockchain transactions is to publish information on the network as part of the transaction information such as the monetary value of the sender and receiver information, and this stage is called creation and construction.

(2) Verification stage: In the proposed system, it is derived from the Lotka-Volterraequations of the lightweight post-quantum hashing method; this hybrid integration enhances efficiency and design with dynamics adapting to the data properties. The security of the system as well as its flexibility are greatly increased by using Lotka-Volterradynamics, which shows a lack of predictability and resistance to large attacks. This stage ensures the integrity of the data and prevents change and theft.

(3) Collecting transactions into a single block through the blockchain organizes and verifies transactions via the Merkle tree and hashes each transaction in a separate block, which gives each transaction a unique digital signature. In addition, all layers are paired with their hashing by increasing the total number until the top of the tree has only one hash called the Merkle root. Ultimately, verification is done without the need for authentication of the transaction in each block, which in turn allows the Merkle tree structure to be effective in its investigations through a cryptographic summary that securely links the block to the blockchain, which is added to the block header after its creation.

(4) The proposed system is used to authenticate blocks using the block strength mechanism (PoW), by finding a random number that helps when combined with the block header and hashing it and gives a result that helps reduce the complexity conditions (such as a certain amount of initial zeros) is the method of solving the cryptographic challenge and this stage is called the consensus mechanism. This method includes:

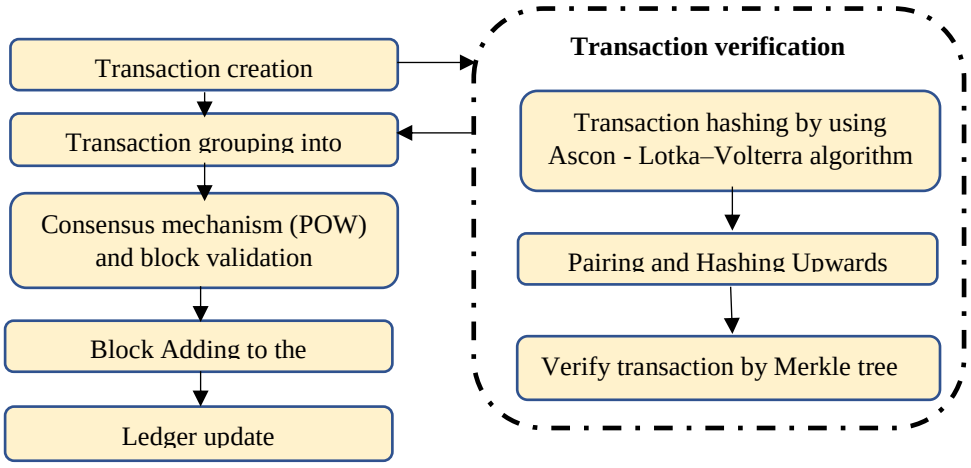

Figure 3. Lightweight block chain proposed system

DOI: https://doi.org/10.54216/FPA.190112
Received: November 10, 2024 Revised: January 17, 2025 Accepted: February 14, 2025

-Block Header Components: The header provides a succinct overview of the block's metadata by containing the timestamp, previous block hash, and Merkle Root.

-Computational Security: PoW's high computational complexity makes it necessary to make several hashing attempts, which makes the system safe from malevolent manipulation.

Phase five: Block Adding to the Blockchain

After being validated, the block is appended to the series of blocks that have already been verified, creating an unchangeable, continuous ledger. To ensure the chain's integrity, the new block is cryptographically hashed to the prior block.

Phase six: Updates to ledger

all the updates are sent to all nodes to reach the consistency of ledger files. The entire node will have the latest copy of the distributed ledger. The transactions in the block are regarded as final once it is uploaded to the blockchain. Multiple confirmations, or fresh blocks put on top of the block, further protect the transaction in the majority of blockchains.

By combining nonlinear dynamics (Lotka-Volterraequations) with a lightweight, post-quantum hashing algorithm (Ascon), this suggested solution significantly improves on conventional blockchain procedures. These developments tackle the security flaws and computational inefficiencies of current systems, especially in settings with limited resources. Together with the strong Proof-of-Work consensus mechanism, the implementation of a Merkle Tree structure guarantees effective transaction validation, scalability, and resistance to new computational threats.

	Algorithm2: Ascon Lotka–Volterra	
	Input:	**message**
	Output:	**hash output**

Begin	**Step1**: states' initialize
	s=bytes _to_state(to_bytes([0, rate*8,a,a-b])+ tagspec + zero_bytes(32))
	Step2 : the message absorb into state
	m _ padding =to _bytes ([0x80]) +zero _byte(rate-(len(message)%rate)-1
	m_padded =message +m_padding
	for block in range (0,len (m_padding)-rate ,rate):
	s[0] ^=byte _to_int (m_padded [block: block +8])
	Ascon _ permutation (s,split,0,b).
	step3: permutation process(s)
	for r in range(12):
	1- Round constant addition
	S[2]^=(0xf0-r*0x10+r*0x1+xround [r%9])
	2- Substitution layer (s-box)
	T = [xround [i%9] ^0_xFFFFFFFFFFFFFFFF) for i in range (5)]
	for i in range (5)
	s[i]^=T[(i+1)%5]
	3- Linear diffusion layer
	For i in range (5) :
	S[i] ^= rotr (s[i] ,xround [i]) ^ rotr (s[i],xround [1+4]	

DOI: https://doi.org/10.54216/FPA.190112
Received: November 10, 2024 Revised: January 17, 2025 Accepted: February 14, 2025

End	**Step4**: Squeeze the state to get the hash hash _output ="" while Len (hash_output)<hash length: hash _output +=squeeze (s) permutation process(s) **step5**: hash_output[:hash length] extract s0 and add to hash result permutation process (s) squeeze the output until the necessary hash length (hash length) is reached. Provide the complete hash result, truncated to the hash length that was requested **Step6**: outputs finalize Give the completed hash result, truncated to the specified hash length.

9. A contrast of the proposed Ascon - Lotka Volterra and original Ascon in the environment of blockchain

Table 2: The main distinctions between the suggested Ascon and the original Ascon can be summed up as follows:

Feature	**Ascon**	**Ascon -Lotka–Volterra**
Initialization	Has constants hardcoded for every circumstance and initializes using preset parameters.	Presents the dynamic parameters a and b, which enable flexibility and adaptability to message sizes and security specifications.
Message Absorption	uses fixed padding with 0x80 for message protection and XOR to incorporate the message into the state S.	Improves message padding by dynamically changing the size of the padding to reduce computational effort and increase memory efficiency.
Target Systems	Although it is not specifically optimized for resource-constrained contexts, it is appropriate for typical cryptography workloads.	Provides settings tailored for systems with high performance or devices with limited resources (e.g., low power and memory utilization).
Round Constant Addition	During each permutation round, a periodic, fixed 64-bit constant is added to the state matrix S[2].	Adds variability and pseudo-randomness by introducing dynamic round constants that are derived from the Lotka-Volterraequations.
Permutation Function	Uses 12 fixed rounds with hardcoded constants for internal state updates.	Uses xround values produced by Lotka-Volterraequations to develop a dynamic approach to constants.
Substitution Layer	Fixed complexity is achieved by performing direct XOR and replacement operations between state elements.	adds complexity by distributing data more widely and nonlinearly among state pieces through the use of XOR operations and dynamic rotations.

DOI: https://doi.org/10.54216/FPA.190112
Received: November 10, 2024 Revised: January 17, 2025 Accepted: February 14, 2025

Linear Diffusion Layer	The state elements S[i] are directly XORed and permuted.	Creates a new list T with elements from xround using modulo-based circular access to account for dynamic complexity.
Bit-Level Complexity	XOR operations lack dynamic depth but propagate bit changes within state elements.	Bit changes are dispersed deeper and wider by rotational XOR and dynamic updates, which improves the security of encryption.
Adaptability	Reliance on constants and static parameters limits flexibility.	High flexibility with dynamic parameter adjustment to meet different performance and security needs.
Security	Depends on permanent structures, which could make it more vulnerable to assaults based on patterns.	Enhances defense against pattern-based attacks by increasing nonlinearity and dynamically adjusting parameters.
Efficiency for Large Messages	enhances defense against pattern-based attacks by increasing nonlinearity and dynamically adjusting parameters.	For large messages, performance is increased and computational overhead is decreased by optimized padding and parameter changes.

This comparison shows how the proposed Ascon Lotka–Volterramodel outperforms the original Ascon, adding efficiency, flexibility, and security to the model while maintaining its computational power.

10. Data set

The proposed system was implemented using a set of tax data to verify the usefulness of the proposed system. It can be located at:
Dataset URL https //www.statista.com/statistics/454876/electronic-tax-declaration-germany/
The tax dataset contains a comprehensive mix of information regarding income and taxes. It's organized according to the ZIP Code, state, and the gross income after adjustments. The information is important because it determines the taxable income of individuals who file income tax forms with the IRS. To maximize the blockchain's performance, complex encryption methods and mathematical models are employed.

11. Execution of the suggested system

The proposed system's implementation is demonstrated in this section, the form is contrasted with the original blockchain via the Ascon algorithm, the post-quantum algorithm. This comparison highlights the importance of variables like processing speed and power that have an effect on blockchain functionality. The contrasts between the original standard blockchain system and the proposed lightweight blockchain system, which combines aspects of Ascon and the Ascon-Lotka-Volterramodel, are listed in Table 2 and Figure 4. Additionally, a comprehensive analysis of the differences in time and capacity for processing between the proposed and original blockchain implementations is documented in Table 3 and Figure 5.

Table 3. Light a weight metric measure for hashing algorithm testing on tax dataset

Metric measure	**Standard block chain**	**Lightweight blockchain (Ascon)**	**Light weight block (Ascon Lotka-Volterra)**
Time	0:01:20.427012	0:00:55.205786	0:00:53.199106
Memory usage	11.7720	8.6520	3.6600
Elapsed time	80.4290	55.2057	53.2021
Throughput	62.1977	90.6155	94.0282
Latency	0.00803888	0.005502444	0.005317551

DOI: https://doi.org/10.54216/FPA.190112
Received: November 10, 2024 Revised: January 17, 2025 Accepted: February 14, 2025

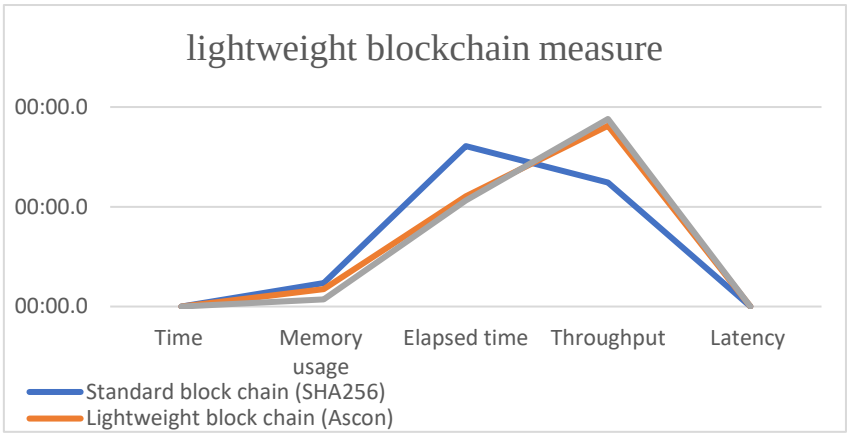

Figure 4. lightweight metric measure base on tax data set

Table 4: A comparison between the original system and the suggested system

Evaluation metric	Standard block chain	Lightweight block chain (Ascon)	Lightweight block chain (Ascon lotka volttera)
Transaction per second (TPS)	0.5	0.5	0.5
Traction's size	149.0 B	149.0 B	149.0 B
Block size	957.11 MB	957.11 MB	957.11 kB
Generation block	80.472	55.2058	53.1991
Verification time	160.8560	135.6327	133.6291
Final time (time generation + verification time	241.2830	190.8386	188.8348
Average CPU usage	12054528	4888596	3747800
Average idle time	19754546	193802812	188469843
Average interrupt time	10.0468	10.0156	9.96875
Average RAM	260.4726	250.4960	240.1523

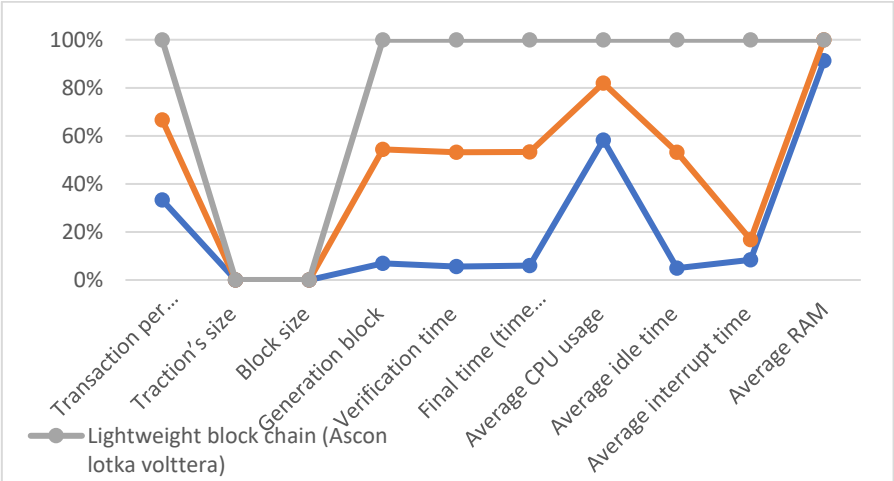

Figure 5. Time and processing power differences between the original and proposed system

DOI: https://doi.org/10.54216/FPA.190112
Received: November 10, 2024 Revised: January 17, 2025 Accepted: February 14, 2025

Significant performance benefits are obtained by integrating the Ascon algorithm into lightweight blockchain systems, as indicated by the results in Table 2 and Figure 4. Additional gains are noted when integrating Lotka-Volterraequations. There was a 33.8% reduction in processing time from 80 seconds with SHA-256 to 55 seconds with Ascon and 53 seconds with Lotka-Volterra. Memory use was greatly reduced, going from 11.7720 MB with SHA-256 to 8.6520 MB with Ascon and then to 3.6600 MB with Lotka-Volterra, resulting in a 68.9% decrease overall. Additionally, scalability significantly increased, as seen by a 51.1% increase in throughput from 62.1977 transactions per second (SHA-256) to 90.6155 with Ascon and 94.0282 with Lotka-Volterra. Due to the large reduction in latency, this method is especially well suited for real-time applications with constrained resources. These results highlight the possibility of improving the effectiveness and scalability of blockchain technology by fusing sophisticated cryptography methods with mathematical models.

The evaluation results, which are shown in Table 3 and Figure 5, show significant performance gains across three blockchain implementations: a standard blockchain, a lightweight blockchain that uses the Ascon algorithm, and an optimized lightweight blockchain that combines Ascon with Lotka-Volterraequations. With a block size of 957.11 kB, the improved Ascon-Lotka-Volterrablockchain drastically reduces storage needs. In terms of block creation and verification times, it likewise outperforms the standard and Ascon-only models. The Ascon-Lotka-Volterra, and RAM consumption. Lastly, this search examines implementation also shows improved resource efficiency, with significant decreases in interrupt time, CPU utilization input-output inconsistencies, output unpredictability, input independence, and data uniformity by evaluating the suggested systems using statistical and similarity measurements.. These criteria, which are shown in Table 4 and show how robust and resilient they are against attacks, emphasize the enhanced security of the suggested system by utilizing the Ascon and Ascon-Lotka-Volterraalgorithms.

Table 5: Statistical and similarity measures the input and output of Ascon and Ascon Lotka Volterra

Metric measure	**Standard block chain**	**Light weight block chain (Ascon Lotka Volterra)**
Correlation coefficient	-0.0017	-0.00245
Mean square error	1049.6530	1050.8802
Cosine similarity	-0.3292	-0.3287
Levenshtein_ Distance	523901	523898
RMSE-coefficient determination	32.3983	32.4160
Hamming distance	1693450	1692707
Bray Curtis dissimilarity	0.16848	0.1685

According to the evaluation metrics, both the Ascon and Ascon-Lotka-Volterrasystems improve blockchain security. Increased independence between input and output data is indicated by lower correlation coefficients (-0.0017 for the standard block chain and -0.00245 for light weight proposed system). With a minor increase in the RMSE-coefficient determination, 32.4160 consistent mean square error (MSE) and root mean square error (RMSE) results show improved variability control. Better output differentiation and divergence are also shown by decreases in the Levenshtein and Hamming distances. The robust cryptographic security is ensured by the Bray-Curtis dissimilarity, which stays high between 0.16848 and 0.1685. The aforementioned findings demonstrate how the Ascon-Lotka-Volterramethod improves robustness, independence, and randomness while fortifying the system's security.

11. Conclusion

The Ascon algorithm is an efficient and lightweight design specifically designed for resource-constrained environments, such as mobile devices and the Internet of Things. Our proposed approach is an ASCON algorithm, a type of cryptanalysis rather than a traditional blockchain hashing method, but it is improved by incorporating Lotka-Volterra equations. The ASCON algorithm is efficient in its design and lightweight, especially for resource-constrained environments, such as mobile devices and the Internet of Things. Therefore, it enhances strong security against quantum threats while also being able to hash and authenticate very quickly. The investigation examines three different blockchain configurations: a standard blockchain (SHA-256), a lightweight blockchain (ASCON), and a lightweight blockchain with added Lotka-Volterra equations. Moving from SHA-256 to Ascon increases throughput while reducing latency, processing time, and memory usage, which is ideal for resource-constrained

DOI: https://doi.org/10.54216/FPA.190112
Received: November 10, 2024 Revised: January 17, 2025 Accepted: February 14, 2025

applications. Additional advantages are produced when Lotka-Volterraequations are combined with Ascon, specifically:The lightweight blockchain is further improved by adding Lotka-Volterraequations, which further increases memory efficiency, more reduces latency and elapsed time, and greatly enhances throughput. Safety and Randomness: The Ascon with Lotka-Volterraalgorithm possesses increased randomness and a more powerful avalanche (higher Hamming distance), these properties are crucial to the security of cryptographic systems due to a lower correlation coefficient. Structural Distinctiveness: Levinstein distance and Bray–Curtis dissimilarity are structural measures. Both of these algorithms perform similarly. However, Ascon's algorithm with Lotka–Volterrahas good improvements, which is why it outperforms the hash output. Efficiency: Metrics like cosine similarity, RMSE, and MSE show that Ascon's Lotka – Volterra maintains comparable computing efficiency. Improved cryptographic principles: Combining Ascon with Lotka -Volterra equations increases the cryptographic stability of Ascon, which is beneficial for blockchain systems that require a high degree of flexibility and security. Combining the Lotka –Volterraand the Ascon hashing method. These improvements make this system a superior choice for blockchain-based applications, providing greater security and reliability. Future studies are recommended that combine AI techniques to analyze blockchain data. Advanced features such as predictions, data analysis, and anomaly detection may be facilitated, leading to more resilient, secure, and intelligent blockchain systems.

References

[1] Y. Zou, T. Meng, P. Zhang, W. Zhang, and A. Li, "Focus on blockchain: A comprehensive survey on academic and application," *IEEE Access*, vol. 8, pp. 187182–187201, 2020.

[2] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in *European Conference on Technology Enhanced Learning*, 2016, pp. 490-496: Springer.

[3] D. A. Dawar, "Enhancing Wireless Security and Privacy: A 2-Way Identity Authentication Method for 5G Networks," *Int. J. Math., Stat. Comput. Sci.*, vol. 2, pp. 183–198, 2024. [Online]. Available: https://doi.org/10.59543/ijmscs.v2i.9073.

[4] V. Morabito, "Business innovation through blockchain," Cham: Springer International Publishing, 2017.

[5] Z. H. Noori and S. K. Ebis, "An information security engineering framework for modeling packet filtering firewall using neutrosophic petri nets," *Computers*, vol. 12, no. 10, 2023.

[6] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," *IEEE Access*, vol. 7, pp. 36500–36515, 2019.

[7] B. Marr, "A very brief history of blockchain technology everyone should read," *Forbes*, New York, NY, USA, 2018.

[8] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in IoT: Challenges and solutions," *Blockchain: Res. Appl.*, p. 100006, 2021.

[9] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. Ann. IEEE Symp. Found. Comput. Sci. (FOCS)*, 1994, pp. 124–134. doi: 10.1109/SFCS.1994.365700.

[10] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. Ann. ACM Symp. Theory Comput.*, vol. Part F1294, pp. 212–219, 1996. doi: 10.1145/237814.237866.

[11] J. Fu, S. Qiao, Y. Huang, X. Si, B. Li, and C. Yuan, "A Study on the Optimization of Blockchain Hashing Algorithm Based on PRCA," *Security Commun. Netw.*, vol. 2020, pp. 1–12, 2020. doi: 10.1155/2020/8876317.

[12] Z. A. Kamal and R. Fareed, "A proposed hash algorithm to use for blockchain base transaction flow system," *Periodicals Eng. Nat. Sci. (PEN)*, vol. 9, no. 4, pp. 657–673, 2021.

[13] A. A. M. A. Ali, M. J. Hazar, M. Mabrouk, and M. Zrigui, "Proposal of a Modified Hash Algorithm to Increase Blockchain Security," *Procedia Comput. Sci.*, vol. 225, pp. 3265–3275, 2023.

[14] Z. A. Othman, S. Tiun, and Y. A. Lotfy, "Towards a secure signature scheme based on multimodal biometric technology: application for IoT Blockchain network," *Symmetry*, vol. 12, no. 10, p. 1699, 2020.

DOI: https://doi.org/10.54216/FPA.190112
Received: November 10, 2024 Revised: January 17, 2025 Accepted: February 14, 2025

[15] F. Hanif, U. Waheed, R. Shams, and A. Shareef, "GAHBT: genetic-based hashing algorithm for managing and validating health data integrity in blockchain technology," *Blockchain Healthc. Today*, vol. 6, 2023.

[16] G. Subathra, N. Jeyakkannan, A. Lavanya, R. Karthika, D. Nancykirupanithi, "A Double Security Hashing Algorithm for Storing Data in Blockchain Technology," *IEEE Access*, vol. 1528–1535, 2023. doi: 10.1109/iceca58529.2023.10395158.

[17] R. K. Salih and A. H. Kashmar, "Enhancing Blockchain Security by Developing the SHA256 Algorithm," *Iraqi J. Sci.*, 2024.

[18] Y. Davda, "Design of Hash Algorithm for Blockchain Security," in *Blockchain Applications in Cryptocurrency for Technological Evolution*, pp. 118–135, IGI Global, 2023.

[19] R. F. Ghani, A. A. Salman, A. B. Khudhair, and L. Aljobouri, "Blockchain-based student certificate management and system sharing using Hyperledger Fabric platform," *Periodicals Eng. Nat. Sci.*, vol. 10, no. 2, pp. 207–218, 2022.

[20] I. M. Hasan and R. F. Ghani, "Blockchain for authorized access of health insurance IoT system," *IRAQI J. Comput. Commun. Control Syst. Eng.*, vol. 21, no. 3, pp. 76–88, 2021.

[21] M. A. Mohammed and H. B. Abdul Wahab, "Enhancing IoT Data Security with Lightweight Blockchain and Okamoto Uchiyama Homomorphic Encryption," *CMES-Comput. Model. Eng. Sci.*, vol. 138, no. 2, 2024.

[22] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies*, Princeton, NJ, USA: Princeton Univ. Press, 2016.

[23] J. Sedlmeir, H. U. Buhl, G. Fridgen, and R. Keller, "The energy consumption of blockchain technology: Beyond myth," *Bus. Inf. Syst. Eng.*, vol. 62, no. 6, pp. 599–608, 2020.

[24] N. Rathod and D. Motwani, "Security threats on blockchain and its countermeasures," *Int. Res. J. Eng. Technol.*, vol. 5, no. 11, pp. 1636–1642, 2018.

[25] K. C. Chaudhary, V. Chand, and A. Fehnker, "Double-spending analysis of bitcoin," in *Pacific Asia Conf. Inf. Syst.*, 2020, June.

[26] A. Dabholkar and V. Saraswat, "Ripping the Fabric: Attacks and Mitigations on Hyperledger Fabric," in *Applications and Techniques in Information Security*, V. S. Shankar Sriram et al., Eds., Singapore: Springer Singapore, 2019, pp. 300–311.

[27] B. Putz and G. Pernul, "Trust Factors and Insider Threats in Permissioned Distributed Ledgers," *Trans. Large-Scale Data Knowledge-Centered Syst.*, vol. XLII, pp. 25–50, 2019.

[28] Y. Cai, Y. Tang, H. Li, L. Yu, H. Zhou, X. Luo, and P. Su, "Resource race attacks on android," in *2020 IEEE 27th Int. Conf. Softw. Anal., Evol. Reeng. (SANER)*, pp. 47–58, 2020.

[29] J. Joshi and R. Mathew, "A survey on attacks of bitcoin," in *Proceeding Int. Conf. Comput. Networks, Big Data IoT (ICCBI-2018)*, pp. 953–959, 2020.

[30] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon MAC, PRF, and Short-Input PRF: Lightweight, Fast, and Efficient Pseudorandom Functions," *Cryptographers Track at RSA Conf.*, Cham: Springer Nature Switzerland, 2024.

[31] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1.2: Lightweight authenticated encryption and hashing," *J. Cryptol.*, vol. 34, pp. 1–42, 2021.

[32] U. V. Johnson, O. S. Adesina, O. O. Agboola, and A. F. Adedotun, "A Lotka-Volterra nonlinear differential equation model for evaluating tick parasitism in canine populations," *Math. Model. Eng. Problems*, vol. 10, no. 4, 2023.

[33] S. H. Strogatz, *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*, 2nd ed., Cambridge, MA, USA: Perseus Books, 2018.

DOI: https://doi.org/10.54216/FPA.190112
Received: November 10, 2024 Revised: January 17, 2025 Accepted: February 14, 2025

[34] D. Hawashin, M. Nemer, S. A. Gebreab, K. Salah, R. Jayaraman, M. K. Khan, and E. Damiani, "Blockchain applications in UAV industry: Review, opportunities, and challenges," *J. Netw. Comput. Appl.*, vol. 230, p. 103932, 2024.

[35] J. K. Madhloom and H. N. Abd Ali, "A quantum-inspired ant colony optimization approach for exploring routing gateways in mobile ad hoc networks," *Electronics*, vol. 12, no. 5, p. 1171, 2023.

[36] Z. A. Othman, S. Tiun, and Y. A. Lotfy, "Towards a secure signature scheme based on multimodal biometric technology: application for IoT Blockchain network," *Symmetry*, vol. 12, no. 10, p. 1699, 2020.

[37] S. Nakaoka, Y. Saito, and Y. Takeuchi, "Stability, delay, and chaotic behavior in a Lotka-Volterra predator-prey system," *Math. Biosci. Eng.*, vol. 3, no. 1, pp. 173–187, 2005.

[38] L. Sidhom and T. Galla, "Ecological communities from random generalized Lotka-Volterra dynamics with nonlinear feedback," *Phys. Rev. E*, vol. 101, no. 3, p. 032101, 2020.

[39] A. A. Elsadany, A. E. Matouk, A. G. Abdelwahab, and H. S. Abdallah, "Dynamical analysis, linear feedback control and synchronization of a generalized Lotka-Volterra system," *Int. J. Dyn. Control*, vol. 6, pp. 328–338, 2018.

[40] H. Ibrahim, "A review on the mechanism mitigating and eliminating internet crimes using modern technologies," *Wasit J. Comput. Math. Sci.*, vol. 1, no. 3, pp. 50–68, 2022.

DOI: https://doi.org/10.54216/FPA.190112
Received: November 10, 2024 Revised: January 17, 2025 Accepted: February 14, 2025