Journal of Information Systems Engineering and Management
2025, 10(28s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Enhancing Blockchain Security and Decentralization Using the ASCON Algorithm for Lightweight Applications

Rasha Hani Salman[1], Hala Bahjat Abdul Wahab[2]
[1]Informatics Institute for Postgraduate studies, Information Technology & Communication University, Baghdad, Iraq.
[2]Computer Sciences Department, University of Technology, Baghdad, Iraq.

ARTICLE INFO

Received: 20 Dec 2024

Revised: 12 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

Blockchain is a decentralized digital ledger technology that records transactions across multiple machines while maintaining security, immutability, and transparency. Due to its decentralized architecture, which remains unaffected by fraud and tampering, one of its main advantages is increased security. Additionally, blockchain technology promotes openness by giving all stakeholders access to the same data, ensuring accountability. Eliminating intermediaries also speeds up and reduces transaction costs and enhances traceability, making tracking the origin and history of assets easier. It is suggested in this paper that a lightweight post-quantum ASCON algorithm is used with blockchain technology to improve decentralization and security in situations where devices are limited. The system aims to increase overall security and provide resilience against quantum attacks by using ASCON instead of the traditional SHA-256 algorithm. ASCON, a component of the National Institute of Standards and Technology's Post-Quantum Cryptography Standardization Process, is ideal for IoT devices because it is small, efficient, and resistant to both classical and quantum attacks. The technology greatly improves the operating environment of resource-limited devices by leveraging blockchain for data management and security and ASCON for privacy.

INTRODUCTION

Organizations need to adopt technological innovations as they challenge their existing knowledge base, strengthen corporate structures, and simplify the process of seizing opportunities. Additionally, it facilitates access to outside financing and expertise, promotes innovative collaboration, and enhances resource accessibility. In a competitive market, blockchain technology offers decentralized platforms where algorithms guarantee confidence instead of centralized bodies [1]. The security of the cryptographic systems that underpin blockchain technology is at risk due to the emergence of quantum computing. Blockchain technology, best known for Bitcoin, has attracted a lot of interest from academic and business communities since it allows for decentralized communication and trust [2]. Blockchain is being used widely; one example of this is decentralized AI platforms. Traditionally, AI algorithms and models have been managed by large tech companies within centralized data centers. However,

blockchain technology can facilitate fully decentralized AI networks. The distributed ledgers and smart contracts in these networks make it possible for participants to work together, share data, and make transactions. This lets the collaborative AI models be trained without having to be defined in the abstract. , provide a maximum need for a central authority [3]. Another example is Bitcoin, which runs without the need for central banks. The increasing demand for Bitcoin investments highlights the necessity of a system that is semi-democratic and decentralized. Blockchain has developed into a widely used technology for building decentralized networks, clouds, and other systems, going beyond just a coin system [4][5]. The security of the cryptographic protocols that now underpin blockchain technology is at risk due to quantum computing. Blockchain has attracted a lot of interest from academia and business because it allows for decentralized trust and communication, with Bitcoin as a prominent example of its widespread use [1][6]. As researchers and developers explore solutions to mitigate the potential threats posed by quantum computing, the future of blockchain technology remains a topic of significant debate and innovation. This ongoing evolution could lead to the development of more resilient cryptographic methods that ensure the integrity and security of decentralized systems in a post-quantum world. Bitcoin, operating without central banks, exemplifies the widespread use of blockchain technology. The increasing interest in Bitcoin investing underscores the need for a decentralized, partially democratic system. Blockchain has developed into a recognized technique for building decentralized networks, clouds, and other systems, going beyond just a coin system [2][4]. It also finds a broad range of applications, such as smart contract-based apps [7], decentralized networks and clouds [5], and reasonably priced distributed platforms like Internet of Things (IoT) systems [8]. We now acknowledge that centralized systems can lead to decentralized systems. Quantum computing, on the other hand, threatens the safety of hash functions and public-key cryptography, which are necessary for blockchains, since Shor's algorithm [9] breaks most public key encryption schemes. The blockchain community is looking into ways to protect against the dangers that quantum computing poses, like Grover's algorithm, which speeds up unstructured searches and could break public key encryption, and Shor's algorithm, which can factorize numbers. Post-quantum cryptography, which uses non-factorization-based encryption, is a key focus, resulting in post-quantum blockchains. Quantum networks and computers are being looked into as ways to make quantum blockchains [10–12]. These blockchains could have fully quantum-based structures or a mix of classical and quantum architectures. The SHA-256 hash algorithm in blockchain technology faces challenges, including vulnerability to quantum computing attacks. Quantum algorithms like Shor's can efficiently solve the underlying mathematical problems of SHA-256, posing a significant threat [13]. The SHA-256 hash algorithm in blockchain systems faces potential security compromises from quantum computing attacks. Additionally, it requires a lot of processing power and is computationally intensive, which makes it less appropriate for contexts with limited hardware, such as IoT devices [14][15]. Blockchain network speed may suffer as a result of SHA-256's processing needs, which can cause delays in transaction processing and verification. SHA-256 is also

inappropriate for IoT devices and other devices with low memory, processing, or battery life.

RELATED WORK

Combining blockchain technology with lightweight cryptography (Ascon) offers significant advantages for resource-limited environments such as embedded systems, mobile applications, and IoT devices. Lightweight cryptography is efficient for low-resource devices due to its reduced memory, processing power, and energy requirements. When integrated with blockchain, it enables secure, decentralized transactions and data integrity without straining hardware. This combination enhances the scalability and performance of blockchain applications while maintaining strict security standards and broadening market adoption. The following highlights recent research on this integration. In [16], the authors suggest using Healthcare 4.0 standards to handle microarray gene expression data securely. By using lightweight cryptography and blockchain technology, this approach improves security features. This method utilizes blockchain, edge layer, fog, and cloud storage technologies to store and retrieve gene data effectively. In addition to providing increased scalability and processing efficiency, this suggested approach drastically cuts down on encryption and decryption times to 325 ms and 20 ms, respectively. In [17], this work introduces a blockchain-based proof-of-authentication system for IoT sensor nodes, utilizing lightweight authenticated encryption. The system generates tags based on sensor data, broadcasts them to the network, and authenticates the cluster head node. The solution can be implemented in software or hardware, achieving high-throughput authentication speeds and resource efficiency. In [18], we present a novel secure blockchain technology. It also incorporates BC-LWCIE technology, creating the ideal LWC-based hash function and key generation. The algorithm known as chicken flock optimization (CSO) is applied. Additionally, the civic society group Algo The rhythm maximizes the signal-to-noise ratio (PSNR) while determining the fitness function. In an IIoT context, BC-LWCIE maintains the encoded pixel values of the encrypted file image in BCT to guarantee confidentiality. This is done to showcase the enhanced security capabilities of BC-LWCIE technology. An Numerous simulations were run, and the outcomes demonstrated how BC-LWCIE technology has improved because it is based on contemporary technologies. The paper in [19] suggests an attribute-based access control scheme for IoT (AAC-IoT) that uses the Hyperledger Fabric (HLF) blockchain and a lightweight hashing algorithm to deal with security issues. Data owners and users are registered using identities, certificates, and signatures, with a credence score for authentication. ABAC uses a fuzzy logic method to determine attribute count, and HLF blockchain manages metadata and security credentials. We develop the model using Java and iFogSim simulators. In [20], the researcher has shown the integration of Internet of Things (IoT) nodes with blockchain networks is the primary focus of this work, particularly for non-real-time IoT nodes without an internal clock mechanism. They are therefore unable to establish real-time communication with blockchain networks. One more important one: the

protection of data entering blockchain networks from Internet of Things devices is a security concern. The data within the blockchain ecosystem can be protected thanks to its maturity. However, data that originates from beyond the globe lacks protection. Make sure the data is secure and intact. The difficulty of leveraging network time to keep blockchain and node synchronizing is first discussed in this paper. The suggested protocol presents a basic cryptographic technique to improve the security of the whole blockchain ecosystem. Combining blockchain technology with lightweight cryptography (Ascon) offers significant advantages for resource-limited environments such as embedded systems, mobile applications, and IoT devices. Lightweight cryptography is efficient for low-resource devices due to its reduced memory, processing power, and energy requirements. When integrated with blockchain, it enables secure, decentralized transactions and data integrity without straining hardware. This combination enhances the scalability and performance of blockchain applications while maintaining strict security standards and broadening market adoption. The following highlights recent research on this integration. In [16], the authors suggest using Healthcare 4.0 standards to handle microarray gene expression data securely. By using lightweight cryptography and blockchain technology, this approach improves security features. This method utilizes blockchain, edge layer, fog, and cloud storage technologies to store and retrieve gene data effectively. In addition to providing increased scalability and processing efficiency, this suggested approach drastically cuts down on encryption and decryption times to 325 ms and 20 ms, respectively. In [17], this work introduces a blockchain-based proof-of-authentication system for IoT sensor nodes, utilizing lightweight authenticated encryption. The system generates tags based on sensor data, broadcasts them to the network, and authenticates the cluster head node. The solution can be implemented in software or hardware, achieving high-throughput authentication speeds and resource efficiency. In [18], we present a novel secure blockchain technology. It also incorporates BC-LWCIE technology, creating the ideal LWC-based hash function and key generation. The algorithm known as chicken flock optimization (CSO) is applied. Additionally, the civic society group Algo The rhythm maximizes the signal-to-noise ratio (PSNR) while determining the fitness function. In an IIoT context, BC-LWCIE maintains the encoded pixel values of the encrypted file image in BCT to guarantee confidentiality. This is done to showcase the enhanced security capabilities of BC-LWCIE technology. An Numerous simulations were run, and the outcomes demonstrated how BC-LWCIE technology has improved because it is based on contemporary technologies. The paper in [19] suggests an attribute-based access control scheme for IoT (AAC-IoT) that uses the Hyperledger Fabric (HLF) blockchain and a lightweight hashing algorithm to deal with security issues. Data owners and users are registered using identities, certificates, and signatures, with a credence score for authentication. ABAC uses a fuzzy logic method to determine attribute count, and HLF blockchain manages metadata and security credentials. We develop the model using Java and iFogSim simulators. In [20], the researcher has shown the integration of Internet of Things (IoT) nodes with blockchain networks is the primary focus of this work, particularly for non-real-time IoT nodes without an internal clock mechanism. They are therefore unable to establish

real-time communication with blockchain networks. One more important one: the protection of data entering blockchain networks from Internet of Things devices is a security concern. The data within the blockchain ecosystem can be protected thanks to its maturity. However, data that originates from beyond the globe lacks protection. Make sure the data is secure and intact. The difficulty of leveraging network time to keep blockchain and node synchronizing is first discussed in this paper. The suggested protocol presents a basic cryptographic technique to improve the security of the whole blockchain ecosystem.

Background

The basis of cryptocurrencies such as Ethereum and Bitcoin is a decentralized peer-to-peer computing paradigm called blockchain technology, which is mostly used to provide security and anonymity in the absence of centralized servers [21]. Blocks make up blockchain structures. Blockchain databases share, distribute, and tolerate faults by storing records in blocks. Blockchain users can access all blocks, but they cannot remove or change them. Blockchain databases are composed of blocks. Every block has a number of validated transactions and the hash value from the preceding block. The genesis block, which is the initial block in a blockchain, has no parent block and, as a result, has no hash value. Blockchains are chronological sequences of blocks that list every transaction, as seen in Figure 1. Linked lists relate to each successive block—also referred to as parental blocks—by using the hash value of the previous block. In a blockchain, the genesis block does not reference any other blocks. A block body (list of transactions) and a block header (information) are present. The metadata contains the following information in addition to block version, parent block hash, Merkle tree root hash, timestamps, and nonce. A random integer called a nonce is used to facilitate cryptographic communication between users. Each participant digitally signs the block body, which is made up of transactions, records, and data [22]. Various fields such as industry, healthcare, real estate, and metaverse security use blockchain technology, popularized by cryptocurrencies. Block verification involves finding the correct nonce, allowing nodes to add blocks, and earning rewards. The proof of work (POW) algorithm used for this is complex and computationally intensive, making blockchain resource-consuming [23]. The POW consensus mechanism prevents tampering and faking by requiring immense computing power to alter every hash in the blockchain and its subsequent blocks, making it mathematically infeasible. Bitcoin's protocol specifies that a block is valid only if its SHA-256 hash falls below a certain threshold, which the network adjusts regularly to control the block generation rate. The nonce in the block header helps vary the required hash value. Each node in the Bitcoin network has voting power proportional to its processing power, making the protocol a type of voting mechanism [24]. A malicious node cannot pose as several voters, preventing what is known as a Sybil attack [25]; voting rights are gained by demonstrating the ability to execute some calculation, and the system is secure as long as the vast majority of the nodes are secure.

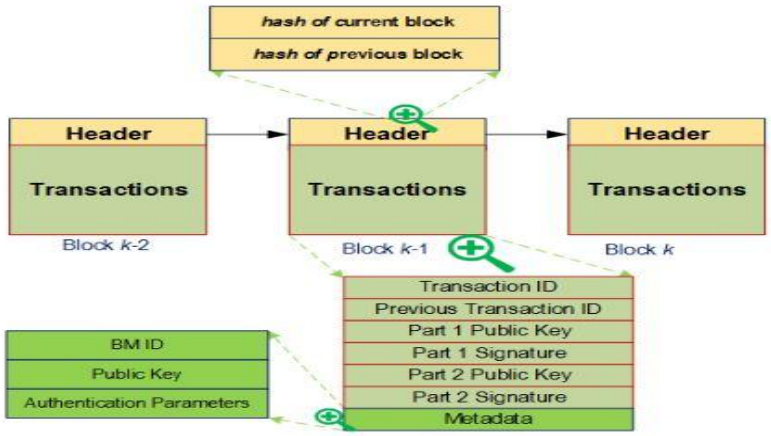

Figure 1: Blockchain Technology Blocks [22]

The SHA-256 Algoritim

As previously mentioned, the SHA-256 hash function plays a crucial role in the security of numerous blockchain technologies. The National Institute of Standards and Technology (NIST) unveiled the SHA-256 function in 2001 [26][27]. Currently, no known weakness exists, leading to its use as a safe hash algorithm [28]. SHA-256 takes arbitrary-length messages (up to 264 bits) and outputs a 256-bit hash value. Processing of the message to be hashed is done in fixed-length 512-bit blocks, with the output from each block serving as the input for the subsequent block. Note that the output of the processing function is half the length of its input. As a result, the building method is known as Merkle-Darmgard, which guarantees collision resistance as long as the underlying compression is present. The compressor function is based on the Davies-Meyer construction, where the output of the compressor function is the keyed function that receives the hash value of the preceding PDB as input. Then, we use the hash value of the preceding block as an XOR to create the hash value for the current PDB. The 64 iterations that make up the keyed function of the SHA-256 compression compute the round function as follows [29].

$$
\begin{aligned}
T_t^1 &= H_t + \sum_1 (E_t) + Ch(E_t, F_t, G_t) + K_t + W_t \\
T_t^1 &= H_t + \sum_1 (E_t) + Ch(E_t, F_t, G_t) + K_t + W_t \\
T_t^2 &= \sum_0 (A_t) + Maj(A_t, B_t, C_t) \\
A_{t+1} &= T_t^1 + T_t^2 \\
B_{t+1} &= A_t \\
C_{t+1} &= B_t \\
D_{t+1} &= C_t \\
E_{t+1} &= D_t + T_t^1 \\
F_{t+1} &= \\
E_t & \qquad \forall t \in [0,63] \\
G_{t+1} &= F_t
\end{aligned}
\tag{1}
$$

Eq. (1) defines the following: Wt is one of the 64 input-dependent words that are explained shortly after; Kt is one of the 64 constants defined in the standard, and the Choose and Majority functions are defined as follows. Variables The hash of the previous block initializes the intermediate state variables At to Ht.

$$ch(E_t, F_t, G_t) = (E_t \wedge G_t) \oplus (\neg E_t \wedge F_t)$$

(2)

$$Maj(A_t, B_t, C_t) = (A_t \wedge B_t) \oplus (A_t \wedge C_t) \oplus (B_t \wedge C_t)$$

To generate the 64 Wt words needed by the round function, the PDB goes through an expansion phase when it calculates the subsequent operation [28].

$$W_t = M_j[32.t + 31 : 32.t] \qquad 0 \le t \le 16$$

(3)

$$\sigma_1(W_{t-2}) + w_{t-7} + \sigma_0(w_{t-15}) + w_{t-16} \qquad t \ge 16$$

$$\sigma_0(x) = x \ggg \tau\ 7 \oplus x \ggg \tau\ 18 \oplus x \ggg 3$$

$$\sigma_1(x) = x \ggg \tau\ 17 \oplus x \ggg \tau\ 19 \oplus x \ggg$$

10 (4)

Lightweight Post-Quantum Encryption Algorithm

Asymmetric key encryption and hashing, or ASCON, is suitable for resource-constrained applications. The CAESAR competition aimed to find new, portable, electronics-appropriate authenticated encryption methods. As one of the finalists, ASCON received recognition for its effectiveness, security, and flexibility. ASCON garnered attention as a possible standardizing option during the NIST competition after winning the lightweight competition. The NIST Lightweight Cryptography Team exhaustively evaluated the finalists by closely reviewing their submission packages, third-party security evaluations, and the progress made through status updates [21].

The Ascon Cipher Suite Algorhim

There are several verified encryption algorithms in the Ascon cipher suite and the Ascon-Hash function, which is based on the Ascon-XOF extendable output function. Confirmed the encryption. The key length k < 160 bits, the rate (data block size) r, and the internal round numbers a and b determine the family members of Ascon's authenticated encryption schemes. For every design, we describe a decryption algorithm D k, r, a, b, and an authorized encryption method E k, r, a, b. The authenticated encryption algorithm E k, r, a, and b will work with any length of associated data A, a nonce (public message number) N of 128 bits, a secret key K of k bits, and plaintext P of any length. The verified ciphertext C, which is the same, is the output [30].

Table 1: Parameter for Recommended Authenticated Encrypted Techniques [21]

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

It has a bit size of 128 and validates the data that goes with the encrypted message [21]. The key K, nonce N, related data A, ciphertext C, and tag T are inputs for the decryption and verification procedure D k, r, a, b. It outputs plaintext P if the tag verification is successful and an error ⊥ if it is not. The parameters that create the extendable output function are an output length, a round number a, a constraint h (h = 0 for unlimited output), and the hash rate (data block size) r. The extensible output function maps an input message M of any length to a hash output H of any length. ℓ < h:X_(h,r,a) (M, ℓ). The Ascon-Xof and Ascon-Hash algorithms employ it. When h = 0, Ascon-Xof uses it for infinite output, and Ascon-Hash uses it with h = ℓ. ℓ=256.The only setting that modifies H's bit length is ℓ. Thus, calls to X h, r, a (M, ℓ'') = H' and X h, r, a (M, ℓ'') = H' provide the same value for the first ℓ' bits for both H' and H'' given the identical parameters and inputs (apart from ℓ < ℓ''). Table 2 lists the parameters of our proposed hashing instance, including the number of rounds (a), the size of the hash output (h), and the rate (r) [21].

Table 2: Specifications for Suggested Hashing Algorithms [20].

Name	Algorithm	Bit size of		Round
ASCON-HASH	x256 ,64, with ℓ=256	Hash 256	Data block 64	p^a 12

the permutation p^a. Ascon-Hash is the first and only recommendation on the list, listed in order of priority. Different contexts and parameter settings can utilize additional structures derived from Ascon's permutation. The sponge architecture is the hashing mechanism. The hash function Ascon-Hash [15] uses the hashing algorithm X (h, r, a), as described in Algorithm 1.

$$IV_{h,r,a} \leftarrow 0^8 \parallel r \parallel a \parallel 0^8 \parallel h = \{00400c0000000000 \text{ for ascon} - XOS\}$$

$$S \leftarrow P^a(IV_{h,r,a} \parallel o^{256}$$

For each instance, we can precompute the first 320-bit state S, which yields the following result for Ascon Hash [31][32]. Absorbing Message, Ascon-Hash processes the message M in blocks of r bits. The padding process is the same as for the Ascon plaintext; it adds a single 1 and the fewest available 0s to M so that the padded message's length is more than or equal to r bits. The resulting padded message is split up into s blocks of r bits each [21][33][35].

S ← ee9398aadb67f03d
8bb21831c60f1002

b48a92db98d5da62
43189921b8fe3e8
348fa5cd525e140

In Ascon-Hash, we process the message M in blocks of r bits. The padding adds a single 1 and the fewest 0s to ensure the message is at least r bits long. The message that has been padded is then divided into blocks of S, each r-bits long, and should have.

$M_1 \parallel \cdots \parallel M_s$

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

The processing of the message blocks Mi with i = 1,...,s is as follows. Prior to applying the a-round permutation p^a on the state S, each block Mi is first XORed to the first r bits Sr of the state S.

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

Compressing Up to the required output length, the state in r-bit blocks produces the hash output. t = [ℓ/r] blocks are finished after ℓ ≤ h. After every extraction, the a-round permutation pa changes the internal state S:

$H_i \leftarrow S_r$

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

The final output block Ht is trimmed to ℓ mod r bits, and H1ll unless r divides ℓ. H2ll H't came back [21][34][36]:

$H_{t \leftarrow} [H_t]_{\ell \bmod r}$

	Algorithm1 [14] **Extendable output function X h, r, a (M, ℓ) = H**	
	Input: **Output:**	message $M \in \{0,1\}^*$, output bitesize ℓ ≤ h or ℓ arbitrary if h = 0 hash $H \in \{0,1\}^{\ell}$

Begin
 	
End
	Step1: Initialization
	$S \leftarrow P^a(IV_{(h,r,a)} \parallel 0^c$
	Step2: Absorbing
	$M_1, \ldots, M_S \leftarrow M \parallel 1 \parallel 0^*$
	For $I = 1, \ldots, S$ do
	$S \leftarrow P^a((S_r \bigoplus M_i) \parallel S_c$
	Step3: Squeezing
	For $I = 1, \ldots, t = [\ell/r]$ do
	$H_i \leftarrow S_r$
	$S \leftarrow P^a(S)$
	Return $[H_1 \parallel \cdots \parallel H_t]_{\ell}$	

RESEARCH METHOD

Servers that are centralized may be vulnerable to the alteration or theft of data, but the proposed blockchain system guarantees that the results are able to offer both verification and authentication. The blockchain saves the data in plain text, enabling authorized users to access and read it on each connected node. Lightweight encryption algorithms ensure privacy and data security. The proposed system integrates lightweight post-quantum cryptography (Ascon) with blockchain technology, utilizing an authentication mechanism. This section details the system's performance regarding hardware utilization, time consumption, and security.

• Resource utilization: The proposed system employs the authentication mechanism using the lightweight cryptographic primitives, which use less memory. The following section provides implementation results that reflect this fact.

• Time consumption: The PoW typically takes around 10 minutes to validate a block, a delay that is unacceptable in environments with constrained devices where real-time monitoring is crucial. The proposed system, however, operates much more quickly, as evidenced by the throughput results provided in this section. • • Security: Security is a top priority in a decentralized solution built on the blockchain. The cryptographic primitives employed make it as secure as lightweight authenticated encryption with associated data (AEAD) techniques. Furthermore, the transaction validation process prevents malicious nodes from transmitting data to the cluster head, while the block validation process ensures the immutability of the blockchain.

Figure 2 illustrates this system. The blockchain will transform centralized data into decentralized data. Moreover, this It helps enhance system safety. and ensures that data cannot be changed using blockchain technology poses a privacy issue. A person with permission can view and utilize blockchain information that reflects issues related to privacy, which may be an issue for data coming from competing manufacturers; at this point, only digital data is used because it is the most crucial component and saves time and effort while using computationally constrained resources. Lightweight Post-Quantum Algorithm (ASCON) The algorithm generates and processes data, then distributes and stores it within the blockchain. Tethered or embedded devices with low computational power rely on nodes in a distributed blockchain network to perform complex calculations. The device representing A proof of secret share consensus algorithm verifies the newly added block node first, where a major distribution center is used to distribute hidden shares, and every node aids in the block's verification. Once a majority approves, the block is authenticated and linked to the chain. The ledger is a distributed text file containing block hashes, previous hashes, and timestamps, ensuring no modifications. In the event of discrepancies, researchers regard the majority of the files as correct. Researchers view blockchain as a consistent, reliable, and safe database, frequently utilizing text files to minimize data storage needs. Proper authentication and verification allow updates across the peer-to-peer network. In a permissioned blockchain system, nodes share proofs of identity rather than competing, reducing computational costs.

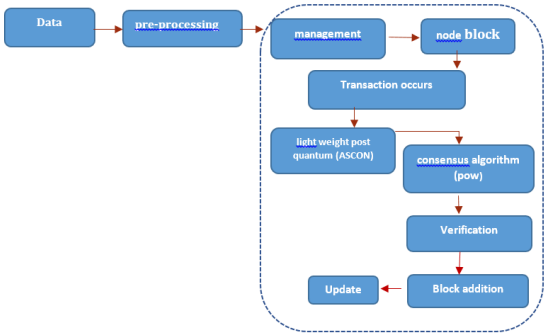

Figure 2: Block Diagram for Proposed System

1. **Management Node**: This node acts as a stand-in for the base station node and is responsible for managing node verification and arranging for the key distribution center to provide each node with the keys it needs. A sensor station must communicate via the peer-to-peer network with the management node in order to submit data to the chain.
2. **Node Block Addition Request**: To add data to the chain, a sensor node must send a request to the blockchain nodes through the management node. This request triggers the authentication, verification, and proof of secret sharing processes, as well as a comparison of the distributed text file that was used.
3. **Hashing**: To ensure that no one can alter the blockchain's content, the standard version of the lightweight post-quantum algorithm (Ascon) is employed to calculate the block's data digest as well as previous data.
4. **Proof of work**: A modified version of secret sharing proof is used, whereby a shared secret produced from the system administrator's initial security and distributed using the proper key distribution technique is assigned to every node wishing to contribute data to the chain.
5. **Verifications**: All nodes involved in the block validation decision will have their text ledger files reviewed and evaluated.
6. **Block addition**: After the data is verified and the nodes validate it, the data is put into the block and added to the chain together with the hashes of the previous and current.
7. **Ledger updated**: To ensure that ledger files are consistent, all modifications are transmitted to every node. The most recent version of the distributed ledger will be available at all base stations. The key components of the suggested system are outlined in algorithm 2.

Algorithm 2 suggested a framework for the proposed system.
Keys and data are input.
Distributed ledger start is the output.
Step 1: Transaction Creation
A user initiates a new transaction by specifying inputs (e.g., sender, recipient, amount) and outputs.
Step 2: Transaction Verification:
Validate the transaction by checking the digital signature for authenticity and ensuring the sender has sufficient balance.
Step 3: Transaction Grouping into a Block:
The ASCON algorithm hashes verified transactions into a block, ensuring adherence to the block size and system constraints.
Step 4: Consensus Mechanism and Block Validation:
Apply the consensus mechanism. Use the Proof of Work method to validate the block. If the block fails validation, reject it and retry with necessary adjustments.
Step 5: Adding the Block to the Blockchain:
Once validated, add the block to the main blockchain.
Step 6: Network Update and Node Synchronization:
Update all nodes in the blockchain network with the latest version of the blockchain, ensuring synchronization**.**
Step 7: Transaction Finalization
Once added to a block, mark the transaction as finalized.

RESULTS AND DISCUSSION

In order to run and validate the algorithms, three transactions are joined in each of the two sets of datasets utilized in this study, producing at least 100 blocks. These are the details of the dataset: The tax dataset: https://www.statista.com/statistics/454876/electronic-tax-declaration-germany/. And the medical dataset is http://filestore.nationalarchives.gov.uk/datasets/records/hospital-records.xls. We designed this system to handle any generated data and interface with devices that have limited resources. Algorithm 1 performs hashing, while Algorithm 2 powers the entire system. We enhance security by hashing data using the lightweight ASCON algorithm instead of SHA-256 and storing it in the blockchain. Evaluation metrics for the standard blockchain and the lightweight post-quantum algorithm in the proposed system include time complexity, elapsed time, throughput, latency, and memory usage, as shown in Table 3 and Table 4.

Table 3: Evaluation Metric for Lightweight Blockchain Metric Based on Tax-Data Set

Metric measure	Lightweight block chain	Standard block chain
Time complexity	0.00.40.473143	0.00.58.327076
Elapsed	40.4731424	58.3280271
Throughput	123.60048425594944	85.7649443795434
Latency	0.004045291594202898	0.005829887766116941
Memory usage	4404	12388

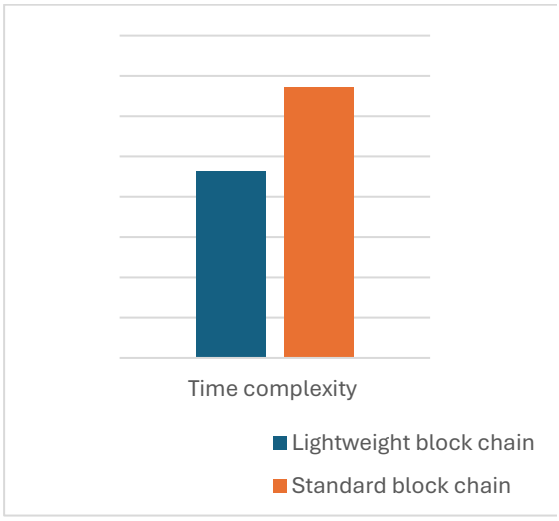

Figure 3: Time Complexity of Blockchain

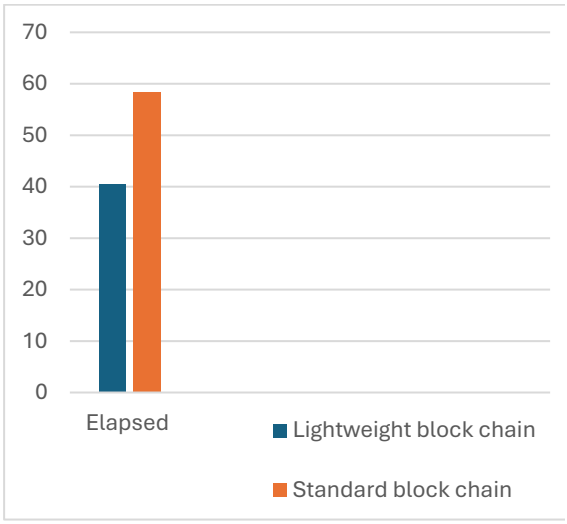

Figure 4: Elapsed of Blockchain

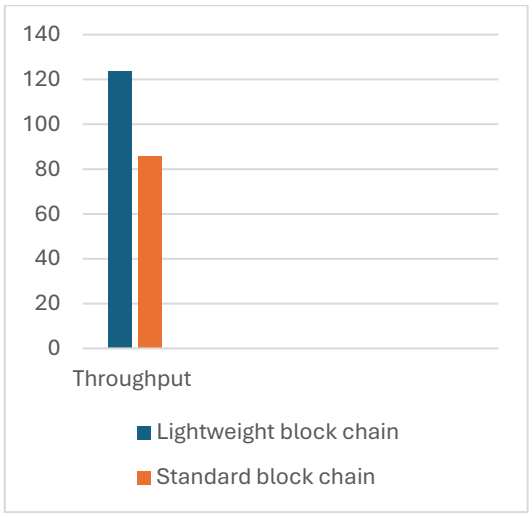

Figure 5: Throughput of Blockchain

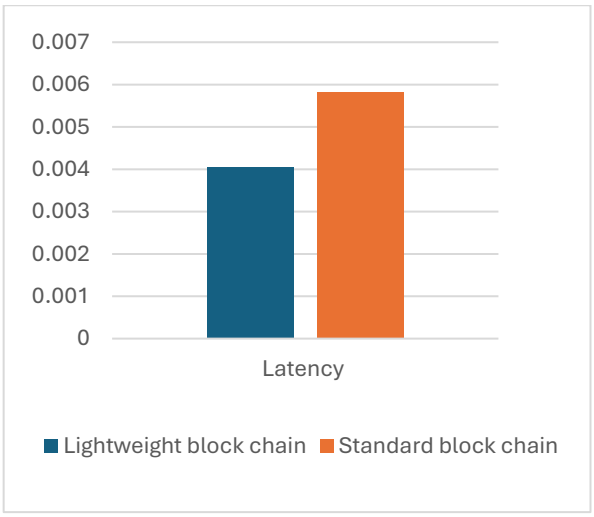

Figure 6: Latency of Blockchain

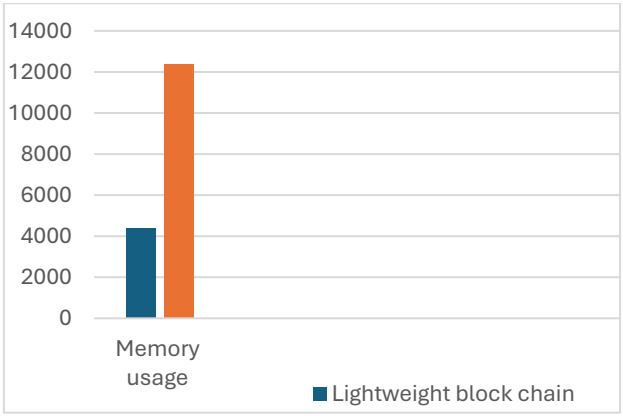

Figure 7: Memory Usage of Hashing Algorthim Blockchain

Table 4: Evaluation Metric for the Lightweight Blockchain Metric Based on A Medical Data Set.

Metric measure	Lightweight block chain	Standard block chain
Time complexity	0.00.13.245758	0.00.19.914988
Elapsed	13.2457575	19.922011899999998
Throughput	121.5106044331553	80.79003305885989
Latency	0.004114867194780988	0.006188882230506368
Memory usage	576	15428

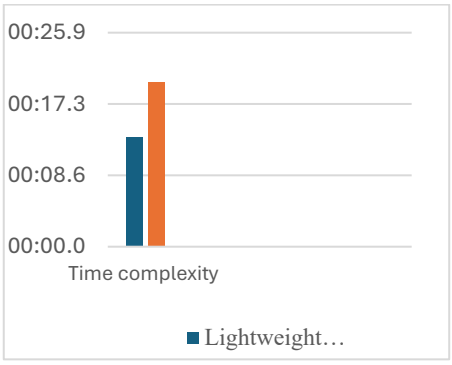

Figure 8: Time Complexity of Hashing

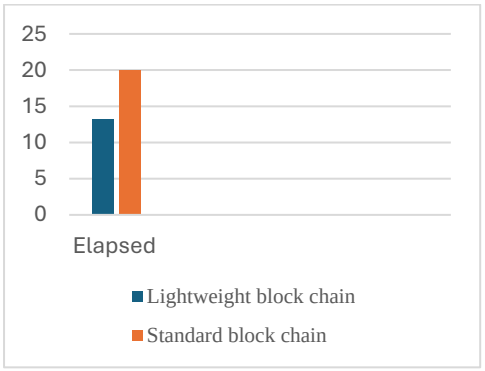

Figure 9: Elapsed Of Hashing Algorithm

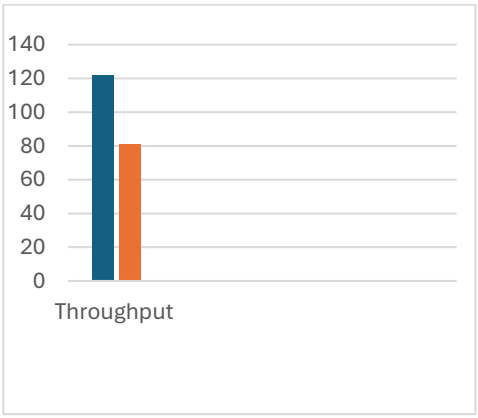

Figure 10: Throughput of Hashing Algorithm

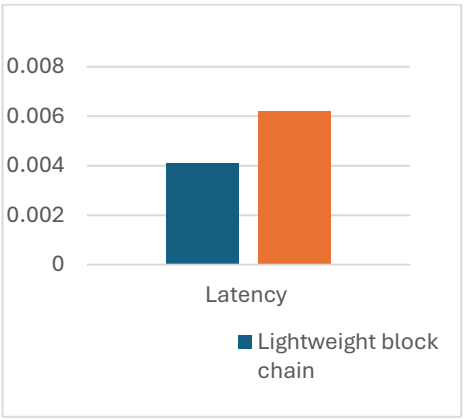

Figure 11: Latency of Hashing Algorithm

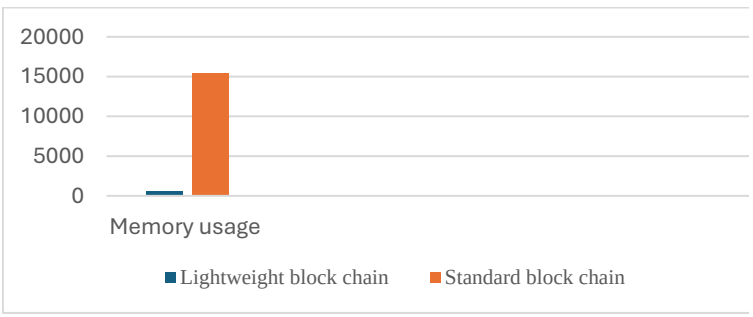

Figure 12: Memory Usage of the Hashing Algorithm

This study also looked at the following metrics to see how well blockchain works: transactions per second (TPS), traction's size, block size, generation block, verification time, final time, average CPU usage, average CPU user time, average CPU system time, average idle time, average interrupt time, and average RAM usage. You can find more information about these metrics in Tables 5 and 6.

Table 5: Evaluation Metric for the Standard Blockchain and Lightweight Blockchain Based on Tax-Data Set

Evaluation metric	**Lightweight block chain**	**Standard block chain**
Transaction per second (TPS)_	0.296580519293953	0.24911913387429817
Traction's size	149.0 B	149.0 B
Block size	957.11 kB	957.11 MB
Generation block	40.473143	58.327067
Verification time	98.8002184	116.65510309999999
Final time (time generation + verification time	139.2733614	174.9821791
Average CPU usage	4509696	12685312
Average CPU user time	60.1	60.2
Average CPU system time	14.9	12.9
Average idle time	3371765625	3399982812499999
Average interrupt time	33.0625	33.109375
Average Ram %	386.02734375	395.640625

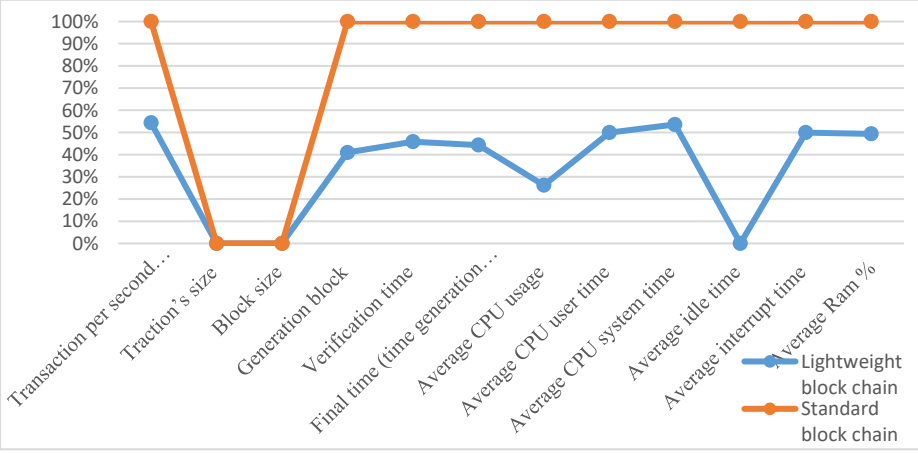

Figure 13. - Evaluation Metric for Standard Block Chain and Light Weight Block Chain Base on Tax -Data S

Table 6. - Evaluation Metric for the Standard Blockchain and Lightweight Blockchain Based on Medical - Data Set.

Evaluation metrics	Lightweight block chain	Standard block chain
Transaction per second (TPS)_	0.5069909983653564	0.4996998865157918
Transaction's size	8.44 KB	8.44 KB
Block size	3.28 MB	3.28 MB
Generation block	13.245758	19.914988
Verification time	33.160745500000004	39.836999899999995
Final time (time generation + verification time	46.40650350000001	59.751987899999996
Average CPU usage	589824	15798272
Average CPU user time	39.5	39.7
Average CPU system time	17.2	12.4
Average idle time	6337.390625	6429.859375
Average interrupt time	11.234375	11.25
Average Ram %	81.2578125	83.984375

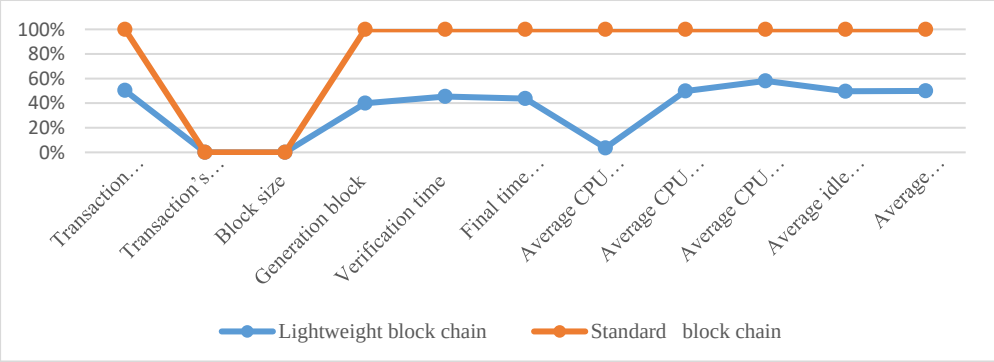

Figure 14: Evaluation Metric for Standard Block Chain and Light Weight Block Chain Base on Medical - Data Set

Table 3 and Figures 3–7 show the results for the tax data set. Table 4 and Figures 8–12 show the results for the medical data set. These show that the proposed system is a better and lighter blockchain solution. Improved metrics like time complexity, elapsed time, throughput, latency, and memory usage reflect this. Additionally, as shown in Figures 13 and 14, along with Tables 5 and 6, the lightweight blockchain outperforms the standard blockchain in several key areas. Specifically, it exhibits superior performance in transactions per second (TPS), block generation time, verification time, final time, average CPU usage, average CPU user time, average idle time, average RAM usage, and average interrupt time. These results suggest that the lightweight blockchain is more efficient and better suited for resource-constrained environments, offering faster processing times and reduced computational load.

CONCLUSION

Blockchain technology plays a pivotal role in ensuring data security and enabling decentralized systems. In a blockchain setting, using the lighter post-quantum ASCON algorithm for hashing instead of the more common SHA-256 algorithm has made a big difference in how well the system works. The ASCON-based approach significantly improves throughput and reduces time complexity, elapsed time, latency, memory usage, and other blockchain metrics like transaction per second (TPS), generation block, verification time, final time, average CPU usage, CPU user time, idle time, interrupt time, and average RAM. These developments highlight the effectiveness and suitability of lightweight blockchain technology in settings with limited resources, enabling quicker processing times and lower computing overhead. This makes lightweight blockchain the go-to option for apps that value effectiveness and low resource use. Stressing the use of cutting-edge cryptographic methods like ASCON improves the security and operational effectiveness of blockchain systems in a variety of industries. However, our investigation has shown that the lightweight ASCON method performs well in the majority of benchmarks, but it is not as efficient in terms of average system CPU time. We plan to further optimize these results by utilizing artificial intelligence approaches in our future study. .

REFRENCES

[1] Valeri, Marco, and Rodolfo Baggio.”A critical reflection on the adoption of blockchain in tourism.”Information Technology and Tourism,vol.23, pp.121–132,June 2020.

[2] Carroll, John M., and Victoria Bellotti. “Creating value together: The emerging design space of peer-to-peer currency and exchange.” Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing , pp.1500-1510. 2015 .

[3] Abed, Saad Abbas."Big Data and Artificial Intelligence on the Blockchain: A Review."Babylonian Journal of Artificial Intelligenc vol.2023,no.2023,pp.1-4.jan.2023.

[4] Keke,Gai,Jinnan Guo, Liehuang Zhu,and Shui Yu."Blockchain meets cloud computing: A survey." IEEE Communications Surveys and Tutorials,vol.3,no.2020,pp.2009-2030.April.2022.

[5] Kaifeng Yue, Yuanyuan Zhang, Yanru Chen and Yang Li, Lian Zhao and Chunming Rong. "A survey of decentralizing applications via blockchain: The 5G and beyond perspective."IEEE Commun. Surv. Tutorials,vol.4,no,4, pp.2191–2217.sep.2021.

[6] Salman, Rasha Hani, Manar Bashar Mortatha, and Riydh Rahef Nuiaa. "Data Mining Technique for Diagnosing Autism Spectrum Disorder." Iraqi Journal of Science vol.65, no. 9, pp: 5239-5253 ,2024.

[7] Mohanta, Bhabendu Kumar, Soumyashree S. Panda, and Debasish Jena. "An overview of smart contract and use cases in blockchain technology."2018 9th

International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2018.

[8] Reyna, A., Martín, C., Chen, J., Soler, E., and Díaz, M. “On blockchain and its integration with IoT. Challenges and opportunitiesn.”Future generation computer systems,vol.88,no.5:pp.173-190,NOV.2018.

[9] Albash, Tameem, and Daniel A. Lidar. "Adiabatic quantum computation" .Reviews of Modern Physics.vol.90,no.1, pp. 015002,jan.2018.

[10] Li, Chun-Tang, Yinsong Xu, Jiahao Tang and Wenjie Liu. “Quantum Blockchain: A Decentralized, Encrypted and Distributed Database Based on Quantum Mechanics.” Journal of Quantum Computing,vol.1,no.2,pp.49-63, 2019.

[11] Soon, JosephNg and Preeta, Nair and Praveen, Kumar and Yew, Kok and Yuen and Phan.”Quantum computing impact of cybersecurity identity verification measures on WhatsApp resilient infrastructureInternational Journal of Advances in Applied Sciences ,vol.13,pp.840-849 ,Dec.2024 .

[12] Fkirin, Alaa, Gamal Attiya, and Ayman El-Sayed. "Steganography literature survey, classification and comparative study."Communications on Applied Electronics,vol.5, no.10, pp. 13-22,sep.2016.

[13] Kearney, Joseph J., and Carlos A. Perez-Delgado. "Vulnerability of blockchain technologies to quantum attacks". Array, vo1.10,no.100065,pp.1-10.Jul.2021.

[14] Pandey, A. A., Fernandez, T. F., Bansal, R., and Tyagi, A. K."Maintaining scalability in blockchain."Springer International Publishing, pp. 34–45. 2021,

[15] Khor, Jing Huey, Michail Sidorov, and Peh Yee Woon. "Public blockchains for resource-constrained IoTdeviceIEEE Internet of Things Journal,vol.8, no.15,pp.11960-11982,Aug.2016, 2021.

[16] Mahajan, Hemant, and K. T. V. Reddy. "Secure gene profile data processing using lightweight cryptography and blockchain." ClusterComputing,vol.27,no.3, pp.2785–2803,Aug.2023,Mar.2022.

[17] Khan, Safiullah, Wai-Kong Lee, and Seong Oun Hwang. "AEchain: A lightweight blockchain for IoT applications". IEEE Consumer Electronics Magazi ne,vol. 11,no. 2, pp.64–76,Mar.2022, 2021.

Bhaskaran, R., Karuppathal, R., Karthick, M., Vijayalakshmi, J., Kadry, S., and Nam, Y.” Blockchain Enabled Optimal Lightweight Cryptography Based Image Encryption Technique for IIoT.” Intelligent Automation & Soft Computing,vol.33, no.3,pp.1593–1606.Dec.2022.

[18] Alshehri, Suhair, and Omaimah Bamasag. "Aac-iot: Attribute access control scheme for iot using lightweight cryptography and hyperledger fabric blockchain".Applied Sciences,vol.12, no.16, pp.1-20.june.2022.

[19] Parmar, Martin, and Parth Shah."Internet of things-blockchain lightweight cryptography to data security and integrity for intelligent application".InternationalJournalofElectrical&ComputerEngineering,vol.3,no.4 ,pp.4422-4431,Aug.2023.

[20] Dobraunig, C., Eichlseder, M., Mendel, F., and Schläffer, M.”Ascon v1.2: Lightweight Authenticated Encryption and Hashing.”Journal of Cryptology,vol. 34,pp.1– 42,june.2022.

[21] Vaigandla,K.K.,Karne, R., Siluveru, M., and Kesoju, M. "Review on blockchain technology: architecture, characteristics, benefits, algorithms, challenges and applications."Mesopotamian Journal of CyberSecurity,vol.2023,no.2023, pp. 73-84, Mar.2023.

[22] Mohd Javaid, Abid Haleem, Ravi Pratap Singh, Shahbaz Khan and Rajiv Suman "Blockchain technology applications for Industry 4.0: A literature-based review".Blockchain: Research and Applications,vol.2,no.4,pp. 1-11,dec.2021.

[23] A. Ravishankar, and Daniel Clarke."Perspectives on emerging directions in using IoT devices in blockchain applications." Internet of Things, vol.10, no. 100079, pp.1-16, june,2020.

[24] John, RincyMedayil, Jacob P. Cherian, and Jubilant J. Kizhakkethottam. "A survey of techniques to prevent sybil attacks."international conference on soft-computing and networks security (ICSNS), IEEE, pp. 1-6. 2015.

[25] Ciulei, Andrada-Teodora, Marian-Codrin Creţu, and Emil Simion. "Preparation for post-quantum era: a survey about blockchain schemes from a post-quantum perspective."Cryptology ePrint Archive, vol.26 ,pp. 0-37, Jan.2022,

[26] Debnath, Santanu, Abir Chattopadhyay, and Subhamoy Dutta. "Brief review on journey of secured hash algorithms.". International Conference on Opto-Electronics and Applied Optics (Optronix), pp.1-5, 2017.

[27] Sharma, Arvind K., and S. K. Mittal."Cryptography & network security hash function applications, attacks and advances: A review".Third International Conference on Inventive Systems and Control (ICISC). IEEE ,pp.177-188. 2019.

[28] Martino, Raffaele, and Alessandro Cilardo. "Designing a SHA-256 processor for blockchain-based IoT applications". Internet of Things,vol.11, no.100254,pp.1-13.Sep.2020.

[29] Neamah, Ali Fahem, and Omar Sadeq Salman. "E-learning as a successful alternative: Proposing an online tests system for iraqi universities." AIP Conference Proceedings. Vol. 2398. No. 1. AIP Publishing, 2022.

[30] Rohit, Raghvendra, and Santanu Sarkar. "Diving deep into the weak keys of round reduced Ascon." IACR Transactions on Symmetric Cryptology, vol.2021,no.2021,pp.74-99,Nov.2021.

[31] Rohit, R., Hu, K., Sarkar, S., and Sun, S. "Misuse-free key-recovery and distinguishing attacks on 7-round ascon". Cryptology ePrint Archive,vol.1,no.1, pp. 0-24, Feb.2021.

[32] Monir Hossain, Momotaz Begum, Bimal Chandra Das and Jia Uddin ."A cost-effective counterfeiting prevention method using hashing, QR code, and website",International Journal of Advances in Applied Sciences, vol.13,no.2 ,pp.351-359,2024.

[33] Salman, R. H., & Wahab, H. B. A. "Using Lotka-Volterra Equations and Lightweight Post-Quantum Algorithm to Develop Lightweight Blockchain Security".vol 19,no.1,pp. 128-143, 2025.

[34] Hani, R. Bahjat, H. "Modify Block Chain Environment based on Post-quantum Algorithms," Journal of Cybersecurity and Information Management, vol.16, no. 1, pp. 151-161, 2025.
[35] Neamah, Ali Fahem, and Asmala Ahmad. "Comparative study in EHR between Iraq and developed countries." Indian Journal of Public Health Research & Development 9.11 (2018): 2023-2029.