THE JBBA

PEER REVIEWED RESEARCH

OPEN ACCESS
ISSN Online: 2516-3957
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-6-1-(1)2023

A Performance Comparison of Post-Quantum Algorithms in Blockchain

Lu Gan and Bakhtiyor Yokubov
Department of Electronic and Electrical Engineering, Brunel University London, UK

Correspondence: lu.gan@brunel.ac.uk
Received: 30 July 2022 **Accepted:** 12 September 2022 **Published:** 23 September 2022

Abstract
Blockchain and other Distributed Ledger Technologies have triggered widespread research and interest. This is due to their ability to create redundant, transparent, and accountable connections in various application domains while utilising asymmetric cryptography, digital signature, and hash functions. However, the current blockchain system exhibits vulnerability to attacks, especially those staged and actualised using quantum computers leveraging Grover's and Shor's algorithms. There is a need to examine the various algorithms of digital signatures, post-quantum generations of public-key cryptography, and their performance to gain insights into the most suitable way to address the issue. In our review, we examine the performance of different post-quantum public-key generation and digital signature algorithms in blockchain and provide a performance comparison of computing time and memory usage. The research presented here includes application domains where post-quantum blockchain may be used.

Keywords: *blockchain, post-quantum blockchain, distributed database, digital signature, public-key cryptography*

JEL Classifications: *C61, C88*

1. Introduction

The Distributed Ledger Technology (DLT) concept provides a distributed peer-to-peer system for value transactions with no central authority mediation. The most widely used form of DLT is blockchain, which originated with the peer-to-peer cryptocurrency Bitcoin [1].

Blockchain is expected to change many domains of our life shortly, with the help of consensus in the trustless environment. The applications of cryptocurrencies such as Bitcoin utilise the protocol of proof-of-work in blockchain as a digital signature scheme and a consensus mechanism in transaction verification.

As a result of the development of rapid quantum computers, the digital signature algorithms in blockchain systems subject them to vulnerability to a quantum adversary [2]. Most public-key cryptosystems utilise mathematical problems that are easily solved using quantum chambers using a finite abelian group. The elliptic curve digital signature algorithm (ECDSA) is used in Bitcoin and enabled by the structure of a finite abelian group. The transformation of quantum Fourier is also used in Shor's algorithm to generate exponential speed-up for the problem of discrete logarithm and integer factorisation. Grover's algorithm is used in quantum computers to speed up hashes' production while allowing for the recreation of the complete blockchain.

Various academic researchers have focused on digital signature systems in the post-quantum era to prevent quantum attacks witnessed in recent years. This has influenced the emphasis of this study in analysing how various signature algorithms can be used to create blockchain systems immune to computer attacks. There is also a comprehensive comparison between digital signatures and schemes of asymmetric encryption in the post-quantum era with respect to their performance and properties.

2. Post-Quantum Blockchain Proposals

Various authors have proposed post-quantum blockchain or modifications to existing blockchain to address the quantum threat.

In 2008, Gentry et al. introduced the first lattice-based signature technique that is probably safe in the random oracle based on the SIS issue [3]. Their core thesis is that lattices allow for natural and inherent "trapdoors" with various valuable cryptographic applications. Yin et al. [4] introduce a new transaction authentication scheme based on lattice-based cryptography that can resist quantum attacks while remaining lightweight in the blockchain system. The signature length on their schema is O(1), which is better suited for storing in a blockchain than other signature lengths. The authors of [5] proposed a safe lattice-based multi-signature system under the ring variant of the short integer solution (Ring-SIS) assumption in the random oracle model. They define a functional lattice-based multi-signature scheme (PLMS), which they extend to allow public key aggregation in a small signer group environment.

Their schemes are based on the practical digital signature scheme and follow the FS-like digital signature structure. In 2019, Esgin at al. [6] provided a post-quantum RingCT protocol based on computational lattice issues such as M-SIS and M-LWE. Their initial contribution to the field is the introduction of the most minor ring signature to date, namely M-SIS and M-LWE, based on conventional lattice assumptions. The authors of Ref. [7] propose a new lattice-based signature scheme for generating sub-private and sub-public keys based on bonsai tree technology. Furthermore, the security of the proposed signature scheme is based on the short integer solution (SIS) problem.

3. Blockchain Overview

In general, blockchain can be considered a decentralised and distributed data structure. Blockchain allows non-trusted members to interact with each other in a verifiable manner without third-party authority. Bitcoin, the first electronic peer-to-peer cryptocurrency in the blockchain context, was introduced in 2008 by Nakamoto [1]. Each block in a blockchain is identified with a cryptographic hash. Each block refers to the previous block's hash, back to the first (genesis) block, thus creating a blockchain or chain of blocks (see Figure 1).

Three types of blockchain are available based on their functioning: private, public, and consortium. In permissioned or private blockchain, only a limited number of users can participate in consensus and have the right to validate transactions. In contrast, anyone can join the network and validate permissionless or public blockchain transactions. Consortium blockchains are permissioned blockchains managed by a group of organisations rather than a single entity, as is the case with private blockchains. As a result, consortium blockchains have more decentralisation than private blockchains, resulting in higher levels of security. Bitcoin, Ethereum, Litecoin, and most cryptocurrencies are well-known implementations of public blockchains. Multichain is considered an open platform for developing and implementing private blockchains.

One of the primary benefits of blockchain technology is its ability to validate transaction trustworthiness in a decentralised environment without the use of intermediaries via consensus algorithms. The different consensus mechanisms can be used depending on the blockchain type. Proof-of-work (PoW), proof-of-stake (PoS), and Byzantine fault tolerance (BFT) are the most common examples of consensus algorithms. PoW protocols require miners to solve challenging computational tasks to create a block. PoS protocols distribute stake blocks to miners in proportion to their current wealth. BFT refers to the process of achieving consensus between two nodes communicating securely over a distributed network in the presence of malicious or misleading nodes.

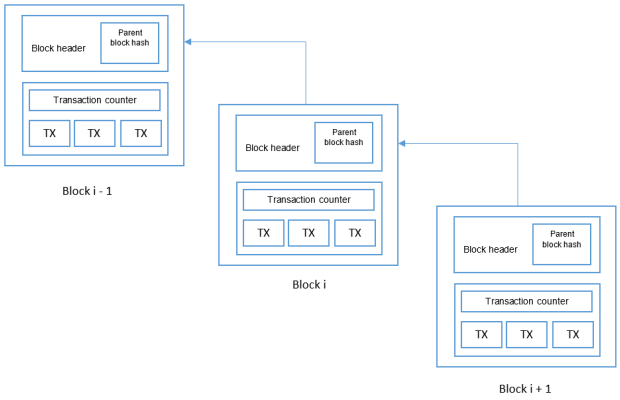


Figure 1. Block structure in a blockchain.

One of the main advantages of blockchain is smart contracts in its applications. In 1994, Nick Szabo proposed the concept of a smart contract [8]. It was described as a computerised transaction protocol that performs a contract's terms. A smart contract satisfies common conditions, minimising the need for trusted intermediaries. It can be considered a digitised form of a legal contract in simple terms. Smart contracts have the following properties: autonomy, trust, backup, and savings.

4. Blockchain Applications

Blockchain technology can be implemented in various applications, including finance, insurance, Internet of Things (IoT), healthcare, voting, supply chain, etc.

4.1 Finance

The global financial system moves trillions of dollars and serves billions of people every day. Nevertheless, the system is riddled with problems, increasing costs through fees and delays, increasing friction through redundant and onerous paperwork, and providing opportunities for fraud and crime. Blockchain technology can ease business operations while still generating a level of security and trustable records of agreements and money transfers in the banking and financial service domains.

4.2 Healthcare

Blockchain is a technology that plays a critical role in the healthcare industry, with numerous applications, such as the traceability of medicine and patients' medical data records. In the pharmaceutical industry, medicine counterfeiting is a significant issue. According to a report by the World Health Organization (WHO), counterfeit or substandard medicines make up about 50% of the global medicine market, with 25% being consumed in developed or developing countries [9]. These medicines can lead to severe problems in a patient's life rather than treating the disease. Blockchain promises to overcome the above challenge by making all the transactions immutable and timestamped. Using blockchain, it is possible to track medicine and make information tamper-proof.

One of the primary healthcare concerns is maintaining patient data integrity. Each patient needs a different treatment strategy for a common disease depending on their physical variability. Their complete medical history needs to be accessible to provide individual treatment. On the other hand, medical data are sensitive and necessitate a secure sharing platform. The current medical record-keeping system lacks both privacy and interoperability. Keeping patients' medical data safe and secure is currently one essential blockchain application. Blockchain can establish a secure and robust framework for storing patients' medical data, resulting in better service while lowering treatment costs.

Compliance requirements for healthcare blockchains depend on things like what sensitive data are stored on the blockchain, what the data usage agreements are, and where the blockchain nodes and decentralised ledgers that store this information are physically located. For example, HIPAA (Health Insurance Portability and Accountability Act of 1996) [10] rules apply when a blockchain stores PHI (Protected Health Information) about US citizens. When blockchains store sensitive information about patients who live in the European Union (EU), the GDPR (General Data Protection Regulation) [11] applies.

4.3 Internet of Things

The Internet of Things (IoT) is crucial in transforming the physical world into a massive information system. IoT can support different applications in industries, such as logistics, food industry, manufacturing, etc. IoT aspires to increase performance and efficiency, decrease machine downtime, and improve product quality. The IoT system currently faces the following challenges: heterogeneity, poor interoperability, resource limitations, and security and privacy vulnerabilities. The distributed architecture of IoT is a critical challenge. In an IoT network, each node is typically a potential point of failure that can be used to launch cyber-attacks, such as distributed denial-of-service (DDoS) [12]. Moreover, the centralised communication of IoT devices may lead to a central point of failure. Data confidentiality, integrity, and authentication need to be addressed in the IoT environment [13].

Blockchain seems to be a perfect complement to IoT, with improved interoperability, privacy, security, reliability, and scalability. Blockchain can be utilised in several domains of IoT, such as "Smart City," "Smart Home," "Smart Industry," and "Smart Grid."

4.4 Electronic Voting

Many studies have been conducted on electronic voting systems to minimise the cost of running an election while ensuring election integrity by meeting security, privacy, and compliance requirements. Replacing the traditional pen-and-paper system with a new election system can reduce fraud while making the voting process traceable and verifiable.

DLTs, such as blockchain, provide a decentralised node for an electronic voting system with the help of an end-to-end verification process [14]. Blockchain is an appealing alternative to traditional voting systems due to decentralisation, non-repudiation, and security protection [15].

4.5 Supply Chain

A supply chain is a network that links a business and its vendors to produce and distribute particular goods to the buyer. Several companies can benefit by utilising blockchain in supply chains to store, monitor, and optimise immutable and reliable data. By storing serial numbers or other product information, such as price, location, date, and quality, on a blockchain, we can obtain a secure and transparent supply chain and eliminate counterfeit products. Moreover, we can check and trace in real-time supply chains, from raw materials to ready goods, speeding up recording and verification operations. The blockchain-based supply chain can enhance trust between involved parties and final consumers by saving all the immutable data on a blockchain.

Blockchain is ideal for establishing a chain of custody. Once written to the record, chain-of-custody transactions are immutable because they constitute a tamper-proof record. This chain of custody is also accessible to all parties on the blockchain, so parties need only read the blockchain to verify it. A chain-of-custody solution promotes the openness, efficiency, and accountability of supply chain processes that are usually unclear.

Through greater transparency and enhanced product traceability, blockchain can help reduce or even prevent fraud in the supply chain. It is extremely challenging to manipulate the blockchain, which is an immutable ledger that can only be updated and validated through network consensus. And if a product is recorded on blockchain, its origin can be easily determined because the data is on a shared, distributed ledger.

5. Post-Quantum Cryptography

According to current knowledge, Shor's and Grover's algorithms do not violate the new generation of public-key algorithms known as post-quantum cryptography. The primary objective of post-quantum cryptography is to create cryptosystems that are secure for both quantum and non-quantum computers while also being able to communicate with existing networks. In this section, the four types of post-quantum cryptosystems are studied.

5.1 Code-based cryptosystem

The algorithmic primitive in a code-based cryptosystem uses error correction codes. An asymmetric encryption mechanism, introduced in 1978 by Robert McEliece [16], was the first of these systems whose security is based on the syndrome decoding problem [17]. The public key is a random generating matrix of a randomly permuted private key version that is an arbitrary binary irreducible Goppa code. The ciphertext is a codeword with certain flaws that can only be removed by the private key owner (the Goppa code). Even though certain

parameter adjustments have been necessary during the last three decades, no attack has been identified as posing a substantial danger to the system, even on a quantum computer. McEliece's system is very fast because both the encryption and decryption procedures are simple, which is beneficial for completing quick blockchain transactions. McEliece's cryptosystem, on the other hand, requires the storage and execution of large matrices that serve as public and private keys that can require between 100 kilobytes and several megabytes, and this may be a constraint for resource-constrained devices.

Harald Niederreiter developed a knapsack-type cryptosystem, a dual variant of the McEliece public key cryptosystem in 1986 [18]. Unlike the McEliece cryptosystem, Niederreiter proposed encoding the message into the error vector instead of representing it as a codeword. The dual variant uses the smaller public key size, while slowing down encryption and decryption. The security of both public key cryptosystems is equivalent.

5.2 Hash-based cryptosystem

Like any other digital signature technique, hash-based digital signature systems rely on a cryptographic hash function. The security of these methods is determined by the hash function's collision resistance rather than the difficulty of a mathematical problem. Collision-resistant hash functions might be considered a prerequisite for a digital signature method that can sign many documents with a single private key. This method dates back to the late 1970s, when Lamport developed a one-way function-based signature scheme [19]. This schema uses a one-way function and the security parameter n is a positive integer number

$$f: \{0,1\}^n \rightarrow \{0,1\}^n, \tag{1}$$

and a cryptographic hash function

$$g: \{0,1\}^* \rightarrow \{0,1\}^n \tag{2}$$

The key and signature generation of Lamport's one-time signature scheme is very efficient, but the signature size is large.

Then, hash-based signature schemes were invented by R. Merkle [20]. Variants of the extended Merkle signature method (XMSS) [21], such as XMSS-T and SPHINCS [22], are now seen to be promising hash-based signature schemes for the post-quantum period, derived from the Merkle tree scheme. Due to their performance, XMSS and SPHINCS may be impractical for blockchain applications. However, several improvements have been made, making hash-based signatures a potential alternative to RSA and elliptic curve signature systems.

5.3 Lattice-based cryptosystem

Lattice-based cryptographic constructs promise post-quantum cryptography since they provide solid security proofs based on worst-case hardness, relatively fast implementations, and considerable simplicity. Furthermore, lattice-based cryptography is resistant to quantum computers. A lattice is a set of points in an n-dimensional space with a periodic structure.

A lattice is a set of points in an n-dimensional space with a periodic structure. Given n linearly-independent vectors $\mathbf{v_1}, \ldots, \mathbf{v_n} \in \mathbb{R}^n$, the lattice generated by $\mathbf{v_1}, \ldots, \mathbf{v_n}$ is given by an integer combination of these vectors in n-dimensional space, with $\mathbf{v_1}, \ldots, \mathbf{v_n}$ forming the basis of the lattice [23]

$$\boldsymbol{\Lambda}(\boldsymbol{v_1}, \ldots, \boldsymbol{v_n}) := \left\{ \sum_{i=1}^{n} \alpha_i \boldsymbol{v_i} \,|\alpha_i \in \mathbb{Z} \right\} \tag{3}$$

The assumed hardness of lattice problems, the most fundamental of which is the shortest vector problem (SVP), underpins lattice-based cryptographic constructs. We were given a lattice represented by an arbitrary basis as input, and we aimed to find the shortest nonzero vector in it. Other analogous lattice-related problems, such as the closest vector problem (CVP) or the shortest independent vectors problem (SIVP) [24], are currently inefficiently handled by quantum computers. The ones based on a short integer solution (SIS) problem [25] appear to be promising among the several lattice-based signature schemes described in the literature due to their decreased key size. According to specific performance evaluations, Bimodal Lattice Signature Scheme B (BLISS-B), which is based on the hardness of the SIS problem, has one of the top performances for lattice-based signature cryptosystems ranked among the RSA and ECDSA [26]. On the other hand, BLISS-B is vulnerable to caching attacks that can retrieve the secret signing key after 6,000 signature generations [27]. Aside from BLISS, other lattice-based signature systems in the literature rely on the SIS problem but were designed to generate secure and efficient blockchains [28].

5.4 Multivariate-based cryptosystem

The multivariate public-key cryptosystem is based on multivariate functions over a finite field instead of single-variable NP-hard or NP-complete functions. This family is regarded as one of the key PKC families capable of withstanding even the most powerful quantum computers in the future. The public is the set of quadratic polynomials:

$$P = (p_1(w_1, \ldots, w_n), \ldots, p_m(w_1, \ldots, w_n)), \tag{4}$$

where each p_i is a nonlinear polynomial in $\mathbf{w} = w_1, \ldots, w_n$:

$$z_k = p_k(\boldsymbol{w}) := \sum_i P_{ik} w_i + \sum_i Q_{ik} w_i^2 + \sum_{i>j} R_{ijk} w_i w_j \quad (5)$$

At any given value, the evaluation of these polynomials corresponds to either the encryption or verification procedure.

The main drawback of multivariate schemes is the large public key size. Further research is needed for better decryption speed and reduced key size [29]. Currently, among the most promising multivariate-based schemes include those based on the usage of square matrices with random quadratic polynomials, Matsumoto algorithm-derived Imai's cryptosystems, and hidden field equation-based schemes (HFE) [30], [31], [32], which can generate signatures size similar to RSA- and ECC-based signatures.

6. Signature Algorithms

This section describes the ECDSA signature scheme and the NIST Round 3 finalist signature schemes Falcon, Dilithium, and Rainbow.

6.1 Elliptic Curve Digital Signature Algorithm

In 1992, Scott Vanstone proposed the ECDSA as a variant of the digital signature algorithm (DSA) that incorporates elliptic curve cryptography [33]. It is a very efficient equation that is based on public-key cryptography. ECDSA is commonly used in several security systems and is widely known in encrypted communication applications, as well as being the foundation of Bitcoin protection.

The following steps are used in ECDSA:

1) Key generation.

The key pair of an entity A is associated with EC domain parameters $D = (q, \mathrm{FR}, a, b, G, n, h)$. The entity A must be confident that the domain specifications are correct before generating keys. The following steps are performed by each entity A:

a) Select an integer number d randomly from the range $[1, n-1]$.
b) Calculate $Q = dG$.
c) Q represents the public key, and d represents the secret key.

2) Signature generation.

An ECDSA signature is built using several domain parameters, a secret key d, and a message m. The outputs are the signature(r, s), where r and s are integer signature components, and continue as follows:

a) Select an integer k randomly from the range $[1, n-1]$.
b) Calculate $kG = (x_1, y_1)$ and $r = x_1 \bmod n$. If $r = 0$ then go to step 1.
c) Evaluate $k^{-1} \bmod n$.
d) Convert the result from SHA-1(m) into an integer number c.
e) Calculate $s = k^{-1}(c + dr) \bmod n$. If $s = 0$ then go to step 1.

3) Signature verification.

B obtains a copy of A's public key and domain parameter to verify A's signature (r, s) on message m, and then performs the following steps:

a) Ensure that r and s are in the range $[1, n-1]$.
b) Convert the result from SHA-1(m) into an integer number c.
c) Calculate $w = s^{-1} \bmod n$.
d) Calculate $l_1 = cw \bmod n$ and $l_2 = rw \bmod n$.
e) Calculate $X = l_1 G + l_2 Q$. if $X = \mathcal{O}$, reject the signature. Else, compute $v = \bar{x}_1 \bmod n$ where, $\bar{x}_1$ is an integer converted from x-coordinate x_1 of X.
f) if $v = r$, verify the signature.

6.2 Falcon Signature Algorithm

Falcon is a lattice-based signature scheme over NTRU that NIST selected as a finalist in NIST PQC contest Round 3. Falcon utilises the GPV framework with NTRU lattices as a post-quantum signature algorithm, and as a trapdoor sampler, it uses a novel technique known as fast Fourier sampling [34].

Gentry, Peikert, and Vaikuntanathan created the GPV framework in 2008 to obtain secure lattice-based signatures.

The following is a high-level description of that framework:

- The public key used to generate q −ary lattice Λ, which contains a full-rank matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ where $m > n$;
- The private key is used to generate $\Lambda_q^{\perp}$, which contains $\mathbf{B} \in \mathbb{Z}_q^{m \times m}$, and is the lattice orthogonal to Λ modulo q. At the same time, the rows of $\mathbf{A}$ and $\mathbf{B}$ needs to be a pairwise orthogonal: $\mathbf{B} \times \mathbf{A}^{\mathbf{t}} = \mathbf{0}$;
- The message m's signature is a short value $\mathbf{s} \in \mathbb{Z}_q^m$ and it should verify $\mathbf{s}\mathbf{A}^{\mathbf{t}} = H(\mathrm{m})$;
- To compute a valid signature, first compute a preimage $\mathbf{c_0} \in \mathbb{Z}_q^m$, which verifies $\mathbf{c_0}\mathbf{A}^{\mathbf{t}} = H(\mathrm{m})$, where c_0 is not necessarily required to be short and $m \geq n$. Then, a vector $\mathbf{v} \in \Lambda_q^{\perp}$ close to $\mathbf{c_0}$ is computed using matrix $\mathbf{B}$. $\mathbf{s} = \mathbf{c_0} - \mathbf{v}$ is a valid signature.

Falcon, like other signature algorithms, has three phases:

1) Key pair generation.

f and g short polynomials are chosen randomly using an appropriate distribution. The matching F and G polynomials are then founded in the solution of the NTRU equation. In this case, the public key is a basis for a $2n$ dimension lattice, where n is typically 512 or 1024.

$$\begin{bmatrix} -h & I_n \\ qI_n & O_n \end{bmatrix} \tag{6}$$

The corresponding private key is another basis for the same lattice.

$$\begin{bmatrix} g & -f \\ G & -F \end{bmatrix} \tag{7}$$

$g, f, G,$ and F need to fulfil the following equations.

$$h = g/f \bmod w \bmod q \tag{8}$$

$$fG - gF = q \bmod w \tag{9}$$

2) Signature generation.

The message and a random nonce are first hashed into polynomial c modulo w. Next, a pair of short polynomials (s_1, s_2) are generated using the knowledge of the secret lattice basis (f, g, F, G) such that $s_1 = c - s_2 h \bmod w \bmod q$, where signature is s_2.

3) Signature verification.

After computing s_1 using the hashed message c and s_2, it should be verified that (s_1, s_2) is a short vector with the process integer computations mod q.

6.3 Dilithium Signature Algorithm

The CRYSTALS-Dilithium lattice-based signature proposed by Ref. [35] is the next finalist in the NIST.

The Dilithium signature algorithm is summarised in the steps below.

1) Key pair generation.

Initially, a matrix $\mathbf{A}$ with polynomial entries in the ring $R_q = \mathbb{Z}_q[X]/(X^n + 1)$ is generated, where n is a power of 2. Then, the two private key samples s_1 and s_2 are generated randomly. Finally, the second part of the public key is calculated from $\mathbf{t} = \mathbf{A}\mathbf{s_1} + \mathbf{s_2}$, where the public key is $(\mathbf{A}, \mathbf{t})$ and the private key is $(\mathbf{s_1}, \mathbf{s_2})$.

2) Signature generation.

The potential signature is calculated as $\mathbf{z} = \mathbf{y} + c\mathbf{s_1}$, where $\mathbf{y}$ is a vector of polynomials and the challenge c is generated using digest and a vector $\mathbf{w_1}$. $\mathbf{y}$ need to be less than the parameter γ_1. $\mathbf{w_1}$ is then high-order bits of the coefficients of vector $\mathbf{Ay}$, and every coefficient w in $\mathbf{Ay}$ can be written as $w = w_1 \cdot 2\gamma_2 + w_2$, where $|w_2| \leq \gamma_2$. Thus, $\mathbf{w_1}$ is the vector, including w_1. Afterwards, the rejection sampling is used to avoid the dependency of $\mathbf{z}$ on the secret key and prevent the leakage of information about the secret key.

3) Signature verification.

The verification process computes $\mathbf{w_1'}$ and accepts if all the coefficients of $\mathbf{z}$ are less than $\gamma_1 - \beta$ from $\mathbf{Az} - c\mathbf{t}$ and if c is the hash of the message and $\mathbf{w_1'}$.

6.4 Rainbow Signature Algorithm (has been broken)

Rainbow's new multivariable polynomial signature scheme was proposed in 2005 [36]. The Rainbow signature algorithm can be defined in the below steps:

1) Key generation.

The private key consists of two randomly chosen invertible affine linear maps, L_1 on k^{n-v_1} and L_2 on k^n, and the map $F = (f_{v1+1}(x), \ldots, f_n(x))$. The number of polynomial components of F is $m = n - v_1$. The public key is the composed map $\bar{F}(x) = L_1 \circ F \circ L_2$.

2) Signature generation.

For signing a document, firstly, it needs to be considered as an element $Y' = (y_1', \ldots, y_{1-v_1}')$ in k^{n-v_1}. The signature of Y' is the inverse of L_2 from this equation.

$$L_1 \circ F \circ L_2 = \bar{F}(x) = Y' \tag{10}$$

The signature is denoted as $X' = (x_1', \ldots, x_n')$.

3) Signature verification.

The following equation needs to be checked to verify the signature.

$$\bar{F}(X') = Y' \tag{11}$$

The Rainbow signature scheme was since proven to be insecure, where the Intersection Attack and the Rectangular MinRank attack proposed by Beullen are shown to break the signature scheme in several days [37].

7. Analysis

Present-day research is focused on post-quantum blockchain. The transition from pre-quantum to post-quantum blockchain necessitates careful consideration of the steps involved. In this section, we compare performance of pre-quantum and the most promising post-quantum public-key encryption and digital signature schemes that can be utilised in blockchain nodes.

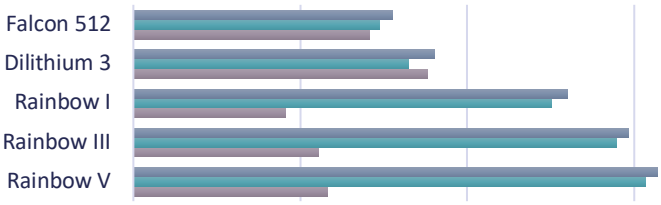
There is no comprehensive answer to the present uncertainties. For instance, varying quantum algorithms are created, bringing forth unprecedented attacks. It is also impossible to evaluate highly secretive projects, thereby presenting a significant loophole that can be used to conduct computer attacks. The performance features are inaccessible, thereby hindering their improvement. Present encryption systems are being rendered obsolete by the continuing advances in quantum computing. The most profound threat of quantum computers has been reported to be targeting the ECDSA systems relied upon by Distributed Ledger, Bitcoin, and other blockchain applications.

The existing public-key cryptography based on the ECDSA is evidently broken. This has subjected AES cryptography to a significant reduction in bit security due to the era of quantum computing. This study evaluated three signature techniques of post-quantum cryptography that could potentially replace the current blockchain signature scheme.

Table 1. ECDSA [38].

Software/ Scheme	Computation Assumption	Bit Security	Key Size (B)	Signature Size(B)
ECDSA (P-256)	Elliptic Curve Discrete Logarithm	128	pk: 64 sk: 96	64

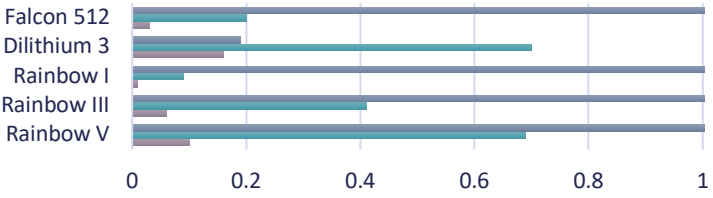
The ECDSA algorithms used in the Distributed Ledger and Bitcoin technologies were examined. Table 1 represents the parameters of ECDSA that were applied as the points of comparison for the secret key, public key amount size, and security bits of the quantum as the variables that can be separately changed. The National Institute of Standards and Technology (NIST) maintains that schemes that have security lower than 112-bit are obsolete and likely to be prohibited from sensitive data handling. The encryption and decryption speeds are crucial factors. An assessment was carried out of the PQC finalists drawn from Round 3 of the NIST for harmonisation and potential replacement in the digital signature algorithms of the blockchain.



	Rainbow V	Rainbow III	Rainbow I	Dilithium 3	Falcon 512
Private Key (B)	1,885,400	861,400	157,800	4,000	1,281
Public Key (B)	1,375,700	611,300	101,200	1,952	897
Signature (B)	212	164	66	3,293	666

Figure 2. Memory usage of post-quantum signature cryptosystems [34]–[36]. The chart is given in logarithmic scale base 10.

Figure 2 compares the post-quantum signature schemes concerning the public key, private key, and size of the signature in bytes. Among all the signatures, Dilithium is the largest. The lattice-based cryptosystems (Dilithium and Falcon) have smaller key sizes than the cryptosystem Rainbow, which is multivariate-based, deriving into large public keys with limited signatures.



	Rainbow V	Rainbow III	Rainbow I	Dilithium 3	Falcon 512
Key Gen. (ms)	121.05	54.59	8.98	0.19	7.49
Signature Gen. (ms)	0.69	0.41	0.09	0.7	0.2
Signature Ver. (ms)	0.1	0.06	0.01	0.16	0.03

Figure 3. Execution time of post-quantum signature cryptosystems [34]–[36].

The speed of the key pair generation, signature execution, and verification process of each post-quantum scheme that passed to the third round of NIST calls are given in Figure 3. All schemes were measured on an Intel(R) Core(TM) i7-1165G7 @ 2.80GHz. Dilithium 3 was the fastest for key generation, while Rainbow I offered the fastest signature generation and verification.

The lattice-based signature schemes are more promising due to their smaller key size, especially those based on the short integer solution (SIS) problem in the literature. Performance evaluations indicated that Falcon is among the best lattice-based performances in cryptosystem signing compared to the

ECDSA and RSA. This has been attributed to its foundation in the hardness of the SIS problem.

Smaller keys are required in the schemes of lattice-based signatures than in the schemes based on a multivariate signature and result in slightly larger signatures. Among the studied lattice-based signatures, Falcon was found to have the shortest signature lengths and shortest key sizes. Dilithium systems were quick but had enormous signatures and key sizes. Based on the outlined analysis, most researchers have deduced that the Falcon signature scheme in blockchain is more promising.

8. Sample Implementation

The sample blockchain implementation was adapted from [39]. The Open Quantum Safe (OQS) library was used in this implementation to integrate the quantum-safe signature into the Hyperledger Fabric blockchain.

Hyperledger Fabric is a well-known and adaptable solution for creating private Distributed Ledger platforms. Fabric achieves high performance and scalability by utilising the execute–order–validate paradigm, which was first proposed to improve the performance of state machine replication [39]. Access control and identity management of Hyperledger Fabric are handled by a membership service provider (MSP) whose cryptographic interface only supports standard PKI authentication methods, such as the RSA and ECDSA classical signatures. Hyperledger Fabric is considered an industry-deployed blockchain, with 20,000 transactions per second [40].

The set of definitions used in Hyperledger Fabric blockchain are as follows:

- **Membership Service Provider (MSP)**. The membership service provider (MSP) is in charge of creating digital identities for the organisation's peers and users. For a new entity to participate in a channel, peers' identities must be configured in an existing network.
- **Fabric CA.** Fabric CA is an MSP implementation that provides a mechanism for registering users and issuing them digital certificates. Fabric CA is typically executed within a Docker container.
- **Peer (endorser).** An endorser peer is designed to simulate transactions and prevent unstable or non-deterministic transactions from passing through the network. In the form of a transaction, a transaction proposal is sent to an endorser. Every peer who endorses it is also a committing peer.
- **Orderer.** An orderer verifies the signatures of all endorsers and uses a consensus protocol to organise the transactions into a block candidate for each set of transactions. Before returning the block candidate to peers for final validation and inclusion in the ledger, orderers sign it.
- **Transaction.** An authorised end-user performs a read/write operation on the ledger. There are three types of transactions: deploy, invoke, and query.

LibOQS [41] is used to implement post-quantum cryptographic signature algorithms in Hyperledger Fabric. LibOQS is an open-source C library used for quantum-resistant cryptographic algorithms and prototype integration into protocols and applications such as OpenSSL. Because LibOQS is written in C and Hyperledger Fabric is written in Go, a CGO wrapper has been written around LibOQS.

Implementation is carried out by a network with one orderer, one client, and two peers. The client sends all the transactions to a single peer, and the second peer plays the role of the endorser.

The chaincode from [40] was used as a simple balance account that allows for sending values between accounts. The standard cryptographic set-up only uses the ECDSA defined over the NIST curve P-256 and provides 128-bit classical security. This was then compared with the hybrid schemes that combined the ECDSA with post-quantum schemes.

Table 2. Public keys and signature sizes of the algorithms [39].

Algorithm	Size* (bytes)	Execution Time** (ms)
ECDSA	96	4
Falcon 512	1563	18
Falcon 1024	3073	28
Dilithium 2	3228	18
Dilithium 3	4173	21
Dilithium 4	5126	25
qTesla p-I	17472	37

* Size of public key and signature.
** Rounded execution time of LibOQS library and hashing that includes key generation, signature generation, signature verification, and hashing times.

Table 2 estimates how much time each signature scheme spent on hashing and LibOQS functions for each block compared to the scheme's public key plus signature size.

Even though qTesla is no longer in the running for NIST, it decided to assess its performance because it was specifically mentioned in recent work on post-quantum Hyperledger Fabric.

9. Conclusion

Recent developments in quantum computing have attracted the interest of blockchain researchers and developers, for which public-key cryptography and hash functions are important. This article examined quantum-computing attacks (based on Grover's and Shor's algorithms) on blockchain and how to use post-quantum cryptosystems to mitigate them. To this end, the most applicable post-quantum methods were studied and their application to blockchain was analysed. Moreover, comprehensive comparisons of the properties and performance of the most promising post-quantum public-key encryption and digital-signature methods were presented.

The largeness of the key sizes was identified as the most significant disadvantage presented by the current signature schemes of the post-quantum era, thereby discouraging their adoption. Many studies are being conducted to refine it into a viable option for key size reduction and facilitating more efficient implementations. Alternatives providing reduced key sizes compared to the present ECDSA algorithms should be encouraged.

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
Lu Gan and Bakhtiyor Yokubov prepared the manuscript in entirety.

Funding:
None declared.

Acknowledgements:
None declared.

References:

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *www.bitcoin.org*, vol. 15, no. 4, pp. 580–596, 2020.

[2] D. Aggarwal, G. Brennen, T. Lee, M. Santha, and M. Tomamichel, "Quantum Attacks on Bitcoin, and How to Protect Against Them," *Ledger*, vol. 3, pp. 1–21, 2018.

[3] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," *Proc. Annu. ACM Symp. Theory Comput.*, pp. 197–206, 2008.

[4] W. Yin, Q. Wen, W. Li, H. Zhang, and Z. Jin, "An anti-quantum transaction authentication approach in blockchain," *IEEE Access*, vol. 6, pp. 5393–5401, 2017.

[5] C. Ma and M. Jiang, "Practical Lattice-Based Multisignature Schemes for Blockchains," *IEEE Access*, vol. 7, pp. 179765–179778, 2019.

[6] M. F. Esgin, R. K. Zhao, R. Steinfeld, and J. K. Liu, "MatRiCT : Efficient, Scalable and Post-Quantum Blockchain Confidential Transactions Protocol *," 2019.

[7] C. Y. Li, X. B. Chen, Y. L. Chen, Y. Y. Hou, and J. Li, "A New Lattice-Based Signature Scheme in Post-Quantum Blockchain Network," *IEEE Access*, vol. 7, pp. 2026–2033, 2019.

[8] N. Szabo, "Smart Contracts," 1994. [Online]. Available: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

[9] B. Glass, "Counterfeit drugs and medical devices in developing countries," *Res. Rep. Trop. Med.*, p. 11, 2014.

[10] U. D. of Health and H. Services, "Summary of the HIPAA Security Rule," 2018. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

[11] "GDPR." [Online]. Available: https://gdpr.eu/.

[12] C. Kolias, G. Kambourakis, A. Stavrou, J. Voas, and I. Fellow, "DDoS in the IoT," *Computer (Long. Beach. Calif).*, vol. 50, no. 7, pp. 80–84, 2017.

[13] S. Sicari, A. Rizzardi, C. Cappiello, D. Miorandi, and A. Coen-Porisini, "Toward data governance in the internet of things," *Stud. Comput. Intell.*, vol. 715, no. May 2018, pp. 59–74, 2018.

[14] A. Ometov *et al.*, "An Overview on Blockchain for Smartphones: State-of-the-Art, Consensus, Implementation, Challenges and Future Trends," *IEEE Access*, vol. 8, pp. 103994–104015, 2020.

[15] S. Gao, D. Zheng, R. Guo, C. Jing, and C. Hu, "An anti-quantum e-voting protocol in blockchain with audit function," *IEEE Access*, vol. 7, pp. 115304–115316, 2019.

[16] R. J. McEliece, "A Public-Key Cryptosystem Based On Algebraic Coding Theory," *The Deep Space Network Progress Report*, vol. 42, no. 44. pp. 114–116, 1978.

[17] E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg, "On the Inherent Intractability of Certain Coding Problems," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 384–386, 1978.

[18] "Knapsack-Type Cryptosystems," vol. 15, pp. 159–165, 1986.

[19] L. Lamport, "Constructing Digital Signatures from a One-Way Function," *SRI Int. Comput. Sci. Lab.*, vol. 94025, no. October, pp. 1–8, 1979.

[20] R. C. Merkle, "Advances in Cryptology — CRYPTO' 89 Proceedings," vol. 435, no. June, pp. 175–185, 1990.

[21] J. Buchmann, E. Dahmen, and A. Hülsing, "XMSS - A practical forward secure signature scheme based on minimal security assumptions," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7071 LNCS, no. November, pp. 117–129, 2011.

[22] D. J. Bernstein *et al.*, "SPHINCS : practical stateless hash-based signatures," vol. 284833, pp. 1–30.

[23] O. Regev, "Lattice-based Cryptography."

[24] J. Bl, "Sampling Methods for Shortest Vectors, Closest Vectors and Successive Minima Sampling Methods for Shortest Vectors, Closest Vectors and Successive Minima," no. August, 2007.

[25] M. Ajtai and S. Jose, "Generating Hard Instances of Lattice Problems," pp. 1–29.

[26] M. Sjöberg, "Post-quantum algorithms for digital signing in Public Key Infrastructures Post-quantum algorithms for digital signing in Public Key Infrastructures," 2017.

[27] L. G. Bruinderink, H. Andreas, T. Lange, and Y. Yarom, "Flush, Gauss, and Reload – A Cache Attack on the BLISS Lattice-Based Signature Scheme," no. 645622, pp. 1–31, 2016.

[28] Y. L. Gao, X. B. Chen, Y. L. Chen, Y. Sun, X. X. Niu, and Y. X. Yang, "A Secure Cryptocurrency Scheme

Based on Post-Quantum Blockchain," *IEEE Access*, vol. 6, no. Part Ii, pp. 27205–27213, 2018.

[29] A. Petzoldt, S. Bulygin, and J. Buchmann, "Selecting Parameters for the Rainbow Signature Scheme - Extended Version -."

[30] J. Ding, A. Petzoldt, and L. Wang, "LNCS 8772 - The Cubic Simple Matrix Encryption Scheme," no. May, 2019.

[31] J. Ding, "A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation," no. March 2004, 2015.

[32] J. Ding and D. Schmidt, "Cryptanalysis of HFEv and internal perturbation of HFE."

[33] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63, 2001.

[34] P.-A. Fouque *et al.*, "Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU Specifications v1.2," pp. 1–65, 2020.

[35] L. Ducas *et al.*, "CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 0, no. 0, pp. 238–268, 2018.

[36] J. Ding and D. Schmidt, "Rainbow, a new multivariable polynomial signature scheme," *Lect. Notes Comput. Sci.*, vol. 3531, no. December 2014, pp. 164–175, 2005.

[37] W. Beullens, "Improved Cryptanalysis of UOV and Rainbow," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 12696 LNCS, pp. 348–373, 2021.

[38] R. Campbell, "Evaluation of Post-Quantum Distributed Ledger Cryptography," *J. Br. Blockchain Assoc.*, vol. 2, no. 1, pp. 1–8, 2019.

[39] A. Holcomb, G. Pereira, B. Das, and M. Mosca, "PQFabric: A permissioned blockchain secure from both classical and quantum attacks," *IEEE Int. Conf. Blockchain Cryptocurrency, ICBC 2021*, 2021.

[40] C. Gorenflo and S. Lee, "FastFabric : Scaling Hyperledger Fabric to 20,000 Transactions per Second."

[41] D. Stebila, "Post-Quantum Key Exchange for the Internet and the Open Quantum Safe Project *," pp. 1–22, 2017.

