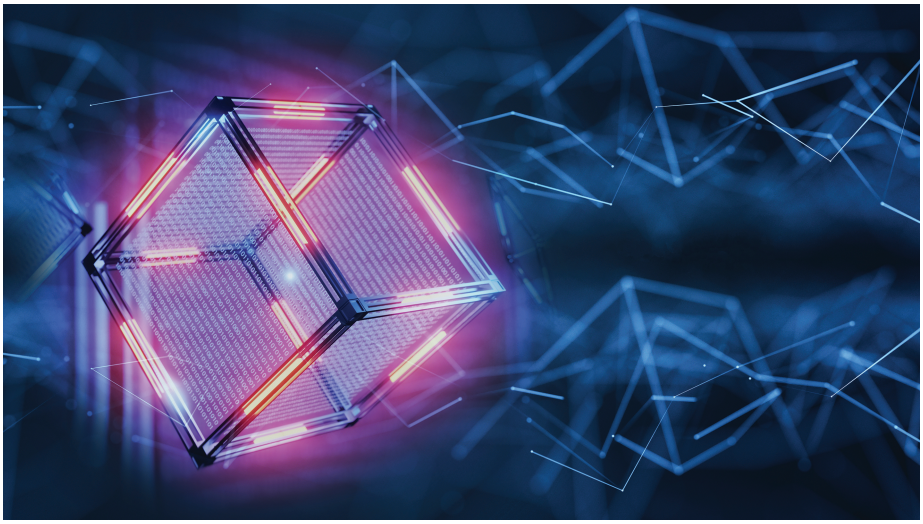

Chapter 7

Towards Post-Quantum Blockchain Platforms

By S. Brotsis[1,*]*, N. Kolokotronis*[1,†] *and K. Limniotis*[2,‡]

[1] *University of the Peloponnese*
[2] *Hellenic Data Protection Authority*
[*] *brotsis@uop.gr*
[†] *nkolok@uop.gr*
[‡] *klimniotis@dpa.gr*

DOI: 10.1561/9781680838350.ch7

Published in *Security Technologies and Methods for Advanced Cyber Threat Intelligence, Detection and Mitigation* by Gohar Sargsyan, Dimitrios Kavallieros and Nicholas E. Kolokotronis (eds.). 2022. ISBN 978-1-68083-834-3. E-ISBN 978-1-68083-835-0.

Suggested citation: S. Brotsis, N. Kolokotronis and K. Limniotis. 2022. "Towards Post-Quantum Blockchain Platforms" in *Security Technologies and Methods for Advanced Cyber Threat Intelligence, Detection and Mitigation*. Edited by Gohar Sargsyan, Dimitrios Kavallieros and Nicholas E. Kolokotronis. pp. 106–130. Now Publishers. DOI: 10.1561/9781680838350.ch7.

now
the essence of knowledge

Two of the most significant arising technological advancements currently underway that are showing an ever-increasing spread both in industrial and academic areas, are the blockchains and the advent of quantum computing. Since, blockchains have dramatically advanced in the recent years and have found numerous applications in many fields with the expectation to significantly enhance their security, the conundrum related to the quantum threat and the implementation of post-quantum signatures in blockchains is a trending topic in nowadays scientific community. As any product that is based on cryptographic primitives, this technology is influenced by the advent of quantum computing, since they are not essentially different from other resilient and secure applications in such regard. This chapter provides the theoretical support of the recent developments in the area of post-quantum cryptography (PQC) aiming at the incorporation of secure cryptographic primitives

to the blockchain technology. For this reason, the chapter assesses contemporary PQC algorithms and presents the current situation of the NIST's 3rd round PQC candidates. In addition, it demonstrates the impact of quantum-computing on blockchains and it investigates the incorporation of PQC primitives to the various blockchain platforms. Therefore, this chapter aims to provide guidelines and demonstrate the challenges to both researchers and industry regarding the implementation of post-quantum algorithms in blockchain applications.

7.1 Introduction

Since the evolution of Bitcoin, the blockchain technology has met growing interest in the last years as a novel technology facilitating the degree of decentralisation required by modern applications and services in an efficient and robust way. Blockchain is a distributed database of records, or shared ledger of all the transactions or digital events having been executed and exchanged among a number of parties. Blockchains have already adopted the basic cryptographic primitives, such as the hash functions and the digital signatures, which are used to achieve consensus and authenticate transactions. Most of the most popular blockchain platforms use a linked list of blocks, in which each block pertains a hash pointer of the previous, while the data of each block is organized using Merkle trees. However, such schemes and algorithms cannot guarantee the security requirements that might occur in the future. While, the modern computer society tends to globalization, the goals for security are not only basic requirements, such as tamper resistance and trust, but also compelling security demands for privacy preservation mechanisms and needs for enforcing accountability in many applications [1]. Since, the blockchain technology has been adopted not only to the financial industry, but to many other areas as well [2–4]; its security and business architecture cannot be easily modified. Therefore, the security of blockchains should acknowledge not only the ongoing means of attacks, but also security issues that might surface in the future.

Essentially, for the transaction's authentication, the blockchains are based on the elliptic curve digital signature algorithm (ECDSA), which is not adequate enough to deal with the quantum threat. The Shor algorithm has been proven to demonstrate quantum supremacy over classical computing. If this algorithm is used by an attacker, then the victim's private key can be derived from the public key and the system's security to be compromised. Similarly, if the attacker forges the user's signature, then all the user's assets and privacy will be lost. Therefore, considering the cryptographic underpinnings of blockchains, this chapter underlines the post-quantum security aspects that can be adopted in blockchain technology and enable it to resist quantum attacks based on the Shor's and Grover's algorithms.

More precisely, this chapter presents the impact of quantum-computing attacks on blockchains and it investigates the incorporation of PQC primitives in the various blockchain platforms. Particularly, the most appropriate post-quantum cryptosystems for blockchains are examined along with their main challenges. Therefore, this chapter can be used as a guide for the development of post-quantum blockchains, since it is necessary that both researchers and industry to be aware to the quantum computing area and its advances.

The chapter consists of six sections, including the current introductory section. More precisely, the structure of the document is as follows: Section 7.2 describes the state-of-the-art in post-quantum cryptography (PQC), in which the public key PQC cryptosystems, the PQC signing algorithms and the the current situation of NIST are presented. Section 7.3 deals with the advances of the PQC in the blockchain technology and presents the blockchain platforms that support PQC primitives. Section 7.4 performs a comparison of the performance of PQC primitives that passed to the third round of the NIST call and describes the resistance of PQC algorithms on various cryptographic attacks. Finally, the main conclusions obtained are summarized in Section 7.5.

7.2 State-of-the-Art in PQC

7.2.1 Public-Key Post-Quantum Cryptosystems

Post-quantum cryptography (PQC) refers to cryptographic systems that will provide security even in case that quantum computers become a reality. More precisely, quantum computing makes use of quantum-mechanical phenomena, thus being more powerful than classical computers. In simple words, classical computers operate on bits, which can have one of two values (states), i.e. 0 or 1, whereas quantum computers operate on qubits, which are in a superposition of states, i.e. 0, 1, or (a little bit of) both. Due to this, quantum algorithms can leverage this superposition of states to provide efficient solutions to several mathematical problems in which classical computers practically fail to provide a solution. Although not every problem can be efficiently solved; there exist though several problems which are being considered difficult today, but they are efficiently solvable by a quantum computer. Some of these problems constitute building blocks for contemporary cryptographic algorithms, thus rendering them fully insecure in the post quantum era.

The most famous quantum algorithms, which have direct impact on the security of cryptographic systems, are the Shor's integer factorisation algorithm, which is a quantum algorithm that factors an integer N in polynomial time with respect to the length of N and the Grover's algorithm, which is a quantum algorithm for searching an unstructured database.

Current symmetric ciphers with 256-bit keys such as AES-256, are believed to be quantum-resistant. Similarly, hash functions with proper parameters (i.e., length of the hashed value) are also considered post-quantum secure, in terms of collision resistance. Therefore, post-quantum cryptography research focuses on asymmetric algorithms, so as to replace RSA, (EC)DH and (EC)DSA. These post-quantum secure algorithms are based on mathematical problems that are believed to be difficult in the classical and quantum cases. Moreover, since hash functions are also post-quantum secure, several post-quantum digital signature schemes whose security relie on the security of hash functions also exist.

More precisely, the post-quantum cryptographic algorithms are mainly classified into one of the following categories, whilst each of them rests its security with one specific difficult mathematical problem:

- Code-based cryptography,
- Lattice-based cryptography,
- Multivariate cryptography,
- Hash-based cryptography,
- Supersingular elliptic curve isogeny cryptography.

whereas hybrid approaches are also considered. In addition, a few algorithms are based on the security of zero-knowledge proofs, which are described next.

Code-based cryptography

The security of the cryptographic algorithms included in this class is based on coding theory – i.e., with the inherently different problem of decoding an erroneous codeword which has been produced through an unknown error correcting code. The most classical such system is the McEliece's cryptosystem, whose security is based on the syndrome decoding problem. McEliece's cryptosystem provides fast encryption and relatively fast decryption, which is an advantage for performing rapid blockchain transactions. However, McEliece's cryptosystem requires large matrices that act as public and private keys, which may be a restriction in constrained environments.

Lattice-based cryptography

This class includes cryptographic algorithms whose construction is based on lattices, which are sets of points in n-dimensional spaces with a periodic structure. These algorithms rest their security on the known difficulty of specific mathematical problems in the field of lattices, like the Shortest Vector Problem (SVP), being NP-hard, which is related with the finding of the shortest non-zero vector within a lattice. Other similar lattice-based difficult problems also exist, such as the Closest

Vector Problem (CVP), the Shortest Integer Solution (SIS) or the Shortest Independent Vectors Problem (SIVP). An important lattice-based problem, which is being "present" in several lattice-based cryptographic system, is the "learning with errors" (LWE) problem, which has security reductions to variants of SVP.

Multivariate cryptography

Multivariate cryptography relies on the complexity of solving systems of multivariate equations, which have been demonstrated to be either NP-hard or NP-complete. In general, it is known that such cryptographic schemes have some limitations into their decryption speeds (due to the involved "guess work". Currently, some of the most promising multivariate-based schemes are based on Hidden Field Equations (HFE) for a generic survey of mathematical problems in the field of multivariate cryptography.

Hash-based cryptography

This scheme includes cryptographic digital signatures schemes whose security relies on the security of the underlying hash function instead of on the hardness of a mathematical problem. This kind of schemes was initiated since the late 70s, when Lamport proposed a signature scheme based on a one-way function.

Supersingular elliptic curve isogeny cryptography

This scheme includes cryptographic algorithms whose security relies on the isogeny protocol for ordinary elliptic curves but enhanced to withstand the quantum attack. Such cryptosystems usually employ key sizes in the order of a few thousand bits.

Other approaches

Post-quantum cryptography based on zero-knowledge proofs: Based on the classical concept of zero-knowledge proofs, these cryptographic algorithms are generalizations of hash-based cryptographic schemes, enriched by nice cryptographic properties of symmetric ciphers towards constructing zero-knowledge proofs.

Hybrid approaches: The hybrid schemes seem to be the immediate next step towards post-quantum security, since they appropriately merge pre-quantum and post-quantum cryptosystems, aiming to protect the exchanged data both from quantum attacks and from attacks against the used post-quantum schemes. However, such schemes involve implementing two complex cryptosystems, which require significant computational resources and more energy consumption. Therefore, future developers of hybrid post-quantum cryptosystems for blockchains will have to look for a trade-off between security, computational complexity and resource consumption.

7.2.2 Post-Quantum Signing Algorithms

In real-world applications today, the most widely used cryptographic schemes for digital signatures are RSA, Digital Signature Algorithm (DSA), and Elliptic Curve Digital Signature Algorithm (ECDSA. However, as it is already mentioned, such digital signature schemes are not post-quantum secure. Therefore, it is essential, for blockchain applications to provide a long-term security and ensure that the digital signatures are secure against post-quantum computers. To this end, we subsequently focus explicitly on post-quantum signing algorithms.

Hash-based digital signatures

The hash-based signature (HBS) algorithms are schemes with minimal security requirements, reasonably fast, providing small size signatures and having strong security guarantees (their security proofs are relative to plausible properties of the cryptographic hash functions).

HBS schemes can be classified as stateless and stateful schemes which can be further categorized as One-Time Signature (OTS), Few-Time Signature (FTS), Multi-Time Signature (MTS), and Hierarchical Signature (HS), depending on key and signature generation. A nice taxonomy of these schemes can be seen in Figure 7.1.

Stateful one-time signature (OTS) schemes: The Lamport scheme, the Winternitz scheme, and its variants WOTS+, WOTS^{PRF} are characteristic algorithms lying in in this class. To sign a message with OTS schemes, the private key is uniformly generated at random, whereas the public key is derived by the private key, by appropriately involving a hash function; the irreversibility of the hash function, as well its collision resistance, ensure that knowledge of the public key does not allow the computation of the private key. The Lamport scheme, even if it possesses great security properties, it is actually practically inappropriate due to several limitations; first is the one-time signature scheme (i.e., each signature can be used only once), whereas it requires extremely large sizes of keys; the derived signatures are also large (see Table 7.1). The fact that it is an OTS scheme implies that each secret key is being used only once for signing; otherwise, an attacker may be capable to derive useful information for imitating the user via setting valid signatures (since the attacker will be able to learn part of the secret key). The drawbacks that are related with the efficiency of the Lamport scheme are being alleviated by the Winternitz One Time signature (WOTS) scheme, which utilizes a so-called Winternitz parameter that controls a time/memory trade-off. Therefore, in principle, reducing the space required for keys and signatures makes WOTS a good choice for memory-constrained embedded devices, but at the cost of slower signing and verifying process.

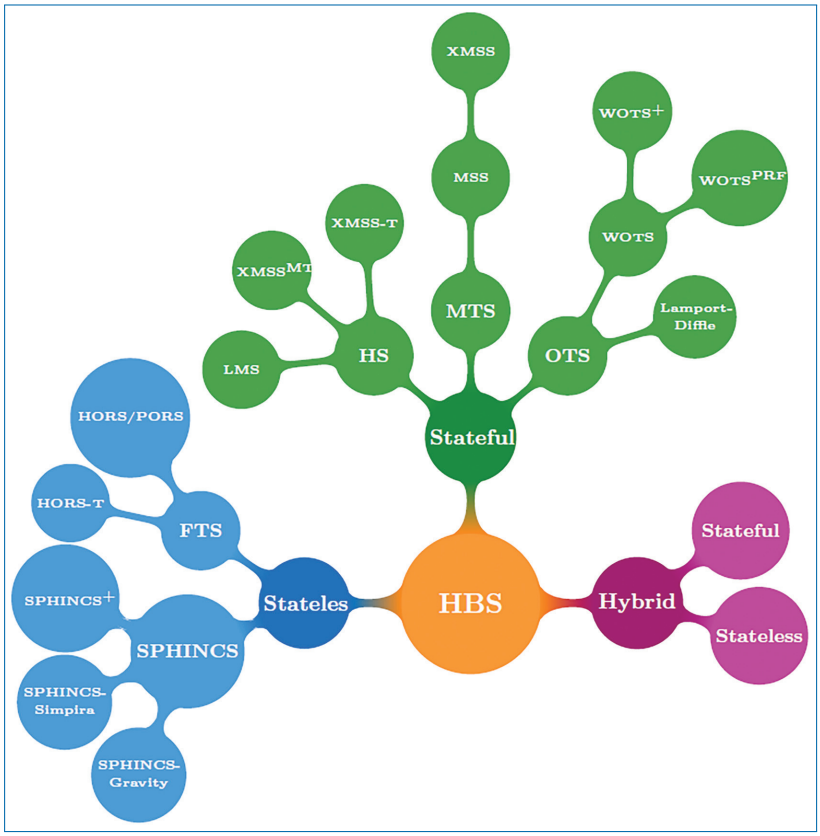

Figure 7.1. A taxonomy of HBS cryptographic scheme [9].

Table 7.1. OTS and FTS schemes for 384-bit message length and about 128-bit post-quantum security level.

Signature Scheme	Type	Signature Size (Kb)	Key Size (Kb)
Lamport	OTS	18.4	36.9
WOTS	OTS	4.8	4.8
WOTS+	OTS	3.2	3.2
$WOTS^{PRF}$	OTS	3.2	3.7
HORS-T	FTS	17.3	0.05

Stateful Multi-time Signature Schemes (MTS): To tackle with the inherent limitations of OTS schemes, MTS schemes are proposed to construct many-time signatures by using OTS as an underlying primitive. The first such scheme has been proposed by Merkle, being called Merkle Signature Scheme (MSS) [5]. This scheme utilizes a so-called Merkle tree, which suffices to combine a large number of OTS

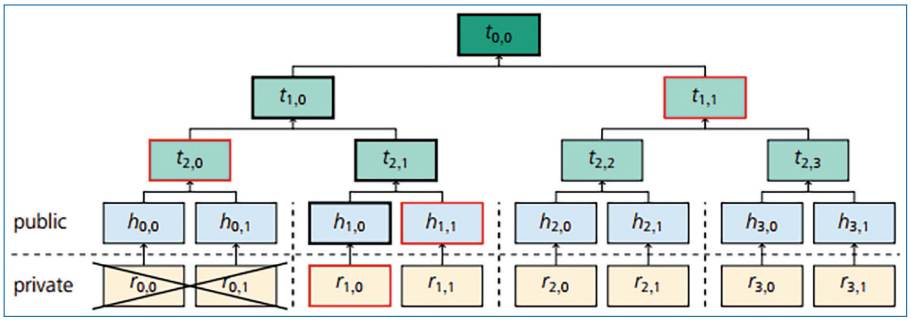

Figure 7.2. A Merkle tree with a verification path for the OTS public key h1,0 [5].

key pairs into a single binary hash tree structure (as shown in Figure 7.2). The root of the tree constitutes a global public key. Due to the properties of the underlying hash functions that are being used to build a Merkle tree, the signer (and nobody else) can easily prove that an one-time public key (e.g. a WOTS+ public key) is associated with a global public key, by revealing appropriate nodes of the tree, determining the authentication path, which allow the validator to reconstruct the path from the relevant one-time public key to the tree's root upon signature verification.

Moreover, there are several other efficient ways to handle Merkle trees, especially the authentication (i.e. appropriately caching the authentication path from the previous signature). Such clever techniques give rise to more efficient signature schemes based on Merkle trees – with the Extended Merkle Signature Scheme (XMSS) being a prominent example [6]. The XMSS scheme is an appropriately modified Merkle hypertree, where the inherent leaves of the tree are based on a WOTS+ scheme. More precisely, the XMSS scheme utilizes a Merkle tree with a major difference being the use of bitmask XOR of the child nodes prior to concatenation of the hashes into the parent node. The use of the bitmask XOR allows the collision resistant hash function family to be replaced. Each leaf of the tree is the root of child trees (also XMSS trees) being called L-trees, which hold the OTS public keys.

Stateful Hierarchical Signature Schemes (HS): Stateless hash-based signature schemes are generally considered slow, since it is necessary to construct a new tree to generate a new key pair. Therefore, hierarchical signature schemes (HS) constitute the next step towards improving efficiency. HS schemes are actually MTS schemes that use other hash-based signatures in its construction. The idea of HS is based on the formation of a hyper-tree that involves tree chaining by using multiple layers of MSS tree. By these means, the upper layers are used to sign the roots of the layers below while only the lowest layer is used to sign messages. Notable examples of HS

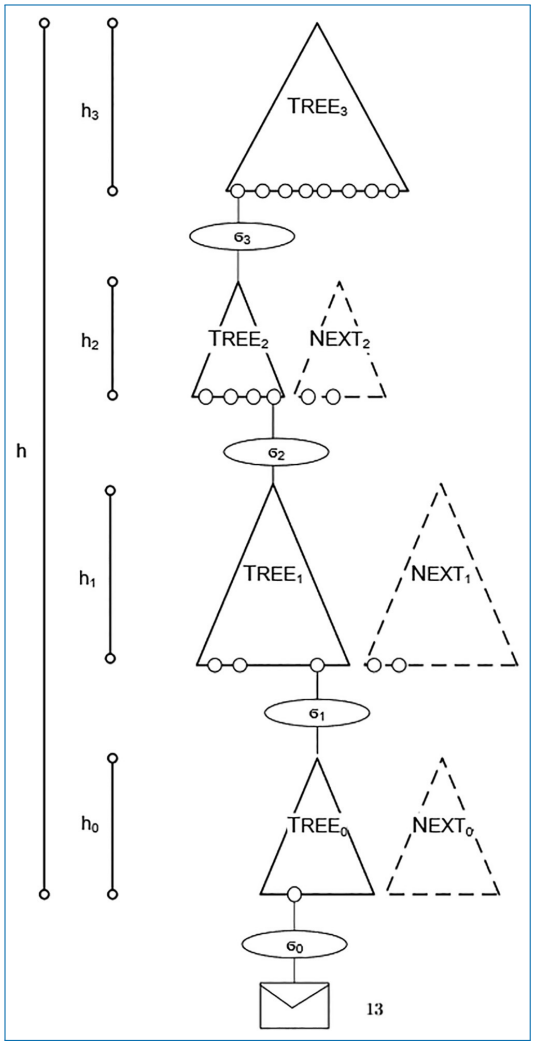

Figure 7.3. XMMS^{MT} with 4 layer [42].

are XMSS-MultiTree (XMSS^{MT}) (see also Figure 7.3), XMSS with tightened security (XMSS-T) and Leighton Micali Scheme (LMS). A XMSS^{MT} is a nice option for applications that require many messages to be signed, provided that the techniques mentioned above for optimization (use of PNRG, caching of authentication path etc.) are still present.

Another, more recent, stateful HBS scheme, which utilizes a blockchain for storing "authentication paths" is the so-called BPQS scheme [7]. BPQS is actually a modified XMSS scheme, using a single authentication path (i.e. a chain and not a tree). The researchers in [7] suggest thar BPQS fits well with blockchains.

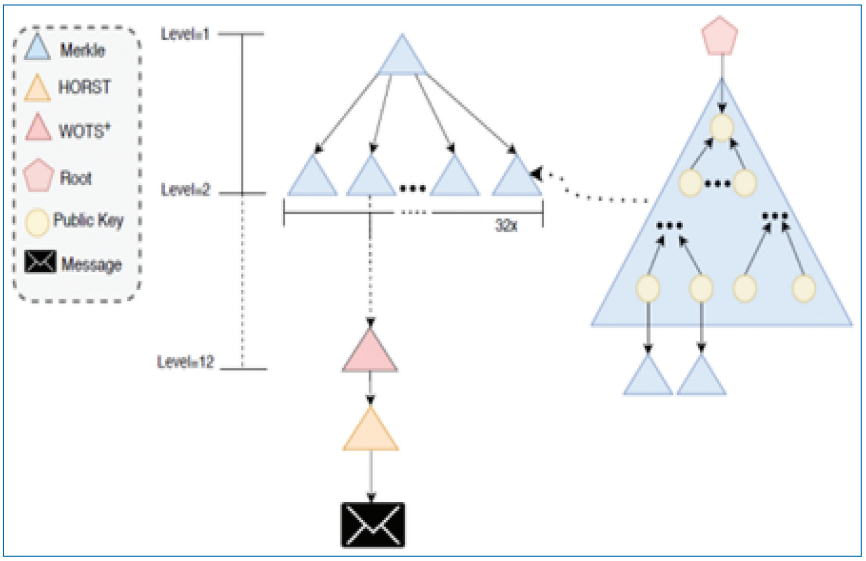

Figure 7.4. Hypertree structure used in SPHINCS [9].

Stateless Hierarchical Signature Schemes (HS): The mail property of stateful hierarchical signature schemes is that the signing process requires the renewal of the secret key. In other words, for stateful signature schemes, signing requires keeping state of the used one-time keys and making sure they are never reused. However, there are also stateless hierarchical signature schemes, with the most prominent example being the SPHINCS [8] and its variants SPHINCS-Simpira, Gravity-SPHINCS and SPHINCS+. Similar to XMSS^{MT}, SPHINCS uses a hypertree such that the upper layers use XMSS with WOTS+ to sign roots of their ancestors, while the lowest layer uses a Merkle tree construction with HORS-T for signing messages (as shown in Figure 7.4). Since the stateless schemes do not keep a record of used key pairs, hence to ensure the correct few-time usage of key pairs, SPHINCS deploys multiple HORS-T key pairs and selects a random one for each signature generation (HORS-T are few times – instead of one time – signature primitives (FTS)). Hence, no path-state tracking is required.

In stateless schemes such as the SPHINCS, generating all private (HORS-T and WOTS+) keys with a PRNG and computing one tree in each layer for signature generation results in an efficient computation. Nevertheless, stateless schemes pose the following performance issues. First, the signature generation is more expensive because the key pairs are used in random order rather than successive order; hence, several optimization algorithms that are being used in stateful schemes are not applicable. Moreover, in contrast to WOTS+, HORS-T signatures are relatively much larger [9]. Note that Table 7.1 also provides relevant information on HORS-T, as an FTS primitive, compared to OTS primitives. A summary between the discussed

Table 7.2. Comparison between stateful and stateless signature schemes in [9].

Signature Scheme	Instantiation	Base Scheme	Key Re-use Capability	Signature Size (Kb)	Key Size (Kb)
MSS	SHA-384	WOTS	2^{60}	7.7	0.05
XMSS	SHA-256	WOTS^{PRF}	2^{60}	4.7	0.03
$XMSS^{MT}$	AES-128	WOTS^{PRF}	2^{80}	10.7	Private key = 26.1 Public key = 1.8
SPHINCS	SHA-256	HORS-T & WOTS+	Unlimited	41.0	1.0

stateless (SPHINCS) and stateful (MSS, XMSS, XMSS^{MT}) HBS schemes is given in Table 7.2, whereas an overall evaluation, is given in Table 7.3.

Even though post-quantum security is considered to be present in HBS schemes, all the potential attack surface should be also examined, mainly stemming from implementation attacks – i.e., side channel attacks and fault attacks. In a side-channel attack, the attacker gains extra critical information (i.e., relative to a secret key) by monitoring and/or measuring quantities such as power consumption, electromagnetic leaks, timing for performing an execution etc. In a fault attack, a fault, which can be either natural or malicious, is misbehavior of a device that causes the computation to deviate from its specification, which could also yield some information on the secret key. HBS schemes are vulnerable to hardware fault attacks both in the presence of natural and malicious faults, so special attention should be given on appropriately implementing such schemes. Moreover, another problem in the stateful signature schemes is the so-called cloning. Such a threat occurs whenever a private key is copied and then used without coordination with execution units (known as non-volatile cloning) or without coordination with storage units, known as volatile cloning.

Some researchers consider XMSS and SPHINCS to be impractical for blockchain applications due to their performance (relatively slow signing speed, whereas the size of the signature in SPHINCS is 41kb), so alternatives have been suggested.

Code-based digital signatures

Several post-quantum code-based signing algorithms have been proposed; probably the most known are the schemes from Niederreiter and CFS (Courtois, Finiasz, Sendrier), which are similar to the McEliece's cryptosystem. The signatures of such schemes are short in length and can be verified really fast, but similarly to

Table 7.3. An overall generic evaluation of stateful and stateless HBS schemes [9].

Type	Pros	Cons	Use Case
Stateful	– Shorter signature size – Faster signature generation time	– State synchronization problem synchronization failure – Face cloning problem	Performance-constrained environment
Stateless	– No state synchronization. problem – No cloning problem	– Longer signature size – Slower signature generation time	Resource-constrained environment

the McEliece's cryptosystems, the use of large key sizes requires significant computational resources and, as a consequence, signature generation may become inefficient [10].

Multivariate digital signature schemes

This class of post-quantum signatures typically yields large public keys, but very small signatures. Some of the most popular multivariate-based schemes rely on Matsumoto-Imai's algorithm or on variants of HFE, which can generate signatures with a size comparable to the currently used RSA or ECC-based signatures. Other relevant multivariate-based digital signature schemes have been proposed, like the Rainbow. In general, it is widely assumed that such cryptosystems need to be further improved in terms of key size.

Lattice-based digital signature schemes

Among the several lattice-based signature schemes described in the literature, the ones based on Short Integer Solution (SIS) seem to be promising due to their reduced key size. For several years, it was assumed that BLISS-B (Bimodal Lattice Signatures B), whose security rests with the hardness of the SIS problem, could be a very nice option due to its good performance. However, it is found out that BLISS is vulnerable to side-channel attacks [10]. Besides BLISS, there are in the literature other lattice-based signature schemes that rely on the SIS problem but that were devised specifically for blockchains [11]. Moreover, lattice-based blind signature schemes have been used to provide anonymity and untraceability in distributed blockchain-based applications for the IoT.

Isogenies digital signature schemes

Although supersingular elliptic curve isogenies can be used for creating post-quantum digital signature schemes, there are not many such schemes known, whereas they also are not efficient. Some schemes of this class indicate though that "it is necessary to address key size issues when implementing isogeny-based cryptosystems and Supersingular Isogeny Diffie-Hellman (SIDH), especially in the case of resource constrained devices".

Zero-knowledge proofs for digital signatures

There is one important post-quantum digital signature scheme, called Picnic, which has a significantly different design principle compared to all the previous. Picnic, which is submitted to the NIST competition, is based on non-interactive zero-knowledge proofs, where the proof of knowledge is instantiated using the MPC-in-the-head approach. The signature is a proof of knowledge of a secret key for a block cipher that encrypts a public plaintext block to a public ciphertext block, which together form the public key of the signature scheme. All the cryptographic building blocks can be instantiated using symmetric-key primitives (block ciphers and hash functions), whereas the MPC (Multi-Party Computation) protocol can be instantiated with information-theoretic security.

7.3 Blockchain and Post Quantum Cryptography

To tackle the quantum threat in the blockchain technology, several researchers have proposed post-quantum-enabled blockchain solutions or even some adjustments to popular distributed leaders. Commercial blockchains have also analyzed and addressed the impact of quantum computers. These include the Quantum Resistant Ledger (QRL) which uses XMSS, the IOTA which uses WOTS and Corda which uses BPQS.

7.3.1 Bitcoin

The platform Bitcoin uses the ECDSA with the Koblitz curve secp256k1 algorithm and the hash function SHA-256 to authorize the transferring of coins and assets. Defined by the Standards for Efficient Cryptography Group (SECG), the Koblitz curve provides several advantages, such as efficiency, reduction of the key size and security, but the main drawback is its weakness against the quantum attack. Therefore, to secure the digital signatures that are included in Bitcoin transactions against the Shor's algorithm, the authors in [13], implemented a signature scheme based on the TESLA# algorithm, which uses the BLAKE2 and the SHA-3 functions,

hence yielding a fast signing and verifying signing scheme. However, qTESLA is not present in the third round of evaluation in the NIST competition.

The research of lattice-based cryptography, which lays the foundation for the design of anti-quantum attack signature scheme, is not only fruitful to resist the quantum threat, but it is also suitable for blockchains. Therefore, the authors in [14] proposed a transparent e-voting blockchain system, which could be applied in Bitcoin. In this scheme the voters that operate maliciously are audited, while code-based cryptography is used to resist quantum threats. More precisely, a certificate-less traceable ring signature algorithm is introduced in the proposed blockchain-enabled e-voting system to solve the problem of verifying public key certificates and the Niederreiter's code-based cryptosystem is adopted to address the quantum threat in the e-voting protocol.

7.3.2 Ethereum

The authors in [15] proposed a framework that encrypts and sensitive industrial data, while the uploader decides with whom this data can be shared with. The architecture is modeled to operate with the popular Ethereum platform and the Inter Planetary File System (IPFS). However, similar and traditional platforms are also able to provide the necessary requirements for the framework's operation. The framework uses the Elliptical-Curve Diffie-Hellman Key Exchange (ECDH) and the SIDH algorithms. Thus, the advantages and drawbacks of each algorithm is discussed in that paper, concluding that SIDH is the most suitable approach because it is post-quantum secure and it ensures security against attackers with quantum computing capabilities. The Ethereum platform is also modified in [16], in which paper, the authors applied a multivariate-based cryptosystem (the Rainbow signature scheme) and compared its efficiency with the current version of Ethereum, which is based on the ECDSA.

7.3.3 IOTA

IOTA is a popular distributed ledger designed for the IoT ecosystem. The platform is considered as a quantum resistant, rather than as a quantum-proof ledger. In particularly, is does not use conventional public key cryptography, but the IOTA Signature Scheme (ISS) that is based on WOTS. In this platform, the users in IOTA sign the message's hash, which means that the security of ISS is based on the cryptographic strength of the hash function. Therefore, IOTA transactions are quantum resistant, but require a new private/public key to be generated each time that a transaction is being signed with the private key, because a part of the private key is revealed in the signature process.

7.3.4 QRL

While designing the QRL, great emphasis has been given to the cryptographic security of its signature scheme, in order to be secure against both classical and quantum attacks, not only at the present day, but also in the future decades. QRL replaces secp256k1 with XMSS, using the hash function SHA-256 and offers 196-bit security with expected security against the brute force attack until the year of 2164. The asymmetrical hypertree signature scheme that is being used in QRL is consisted by chained XMSS trees and provides the dual advantage of using a validated signature scheme and the permission of generating ledger addresses with the capability of signing transactions without a pre-computation delay that is observed in XMSS constructions.

7.3.5 Corda

Corda typically supports conventional public key signature algorithms, such as ECDSA and RSA (the default signature is ECDSA with NIST P-256 curve – i.e., secp256p1). However, at an experimental level, SPHINCS has been employed towards providing post-quantum security. Moreover, very recently, researchers from R3 (i.e. the company supporting Corda) proposed the aforementioned BPQS signature scheme, forming an improvement of the XMSS (and, actually, the blockchain by itself plays such a role, thus comprising a blockchained signature scheme).

7.3.6 Hyperledger Fabric

The Hyperledger Fabric does not provide (by default) post-quantum security. However, it has been announced that achieving post-quantum security is one of the priorities with respect to further advancements of the ledger. To this end, such an approach has been very recently suggested in a research paper [17]. The researchers present the so-called PQFabric, which is the first version of the Hyperledger Fabric enterprise permissioned blockchain whose signatures are secure against both classical and quantum computing threats. In this paper, the researchers implement and analyze hybrid signatures that are configurable with any post-quantum signature algorithm.

The authors redesign the credential-management procedures and specifications of the Fabric network and they created hybrid signatures that are a combination of the classical and quantum-safe digital signatures. The comparative benchmarks of PQ-Fabric are performed with some of the NIST candidates and alternates, namely Falcon-512, Falcon-1024, Dilithium-2, Dilithium-3, Dilithium-4 and qTesla-p-I.

The proposed system is built on-top of Fabric v.1.4 and the LIBOQS v0.4, which is used for the implementation of the post-quantum cryptographic algorithms.

The integration presented in [17], was not straightforward, and therefore three core modules of the Fabric's codebase were modified to allow the incorporation of hybrid quantum signatures, (1) the Blockchain Cryptographic Service Provider (BCCSP) that offers the implementation of a uniform interface. This interface calls the relevant signature scheme based on the key type that is being used; (2) the local Membership Service Provider (MSP) that extracts the cryptographic keys, both public and private – since the hybrid quantum-classical cryptography needs two keys – from the X.509 certificate; and (3) the cryptogen, which is a template used to create the cryptographic material needed to run the Fabric platform from its configuration files. Therefore, the modified MSP obtains the private and public keys from the X.509 certificate, stores them for each node in an internal structure and then provides them to the BCCSP module every time that a message is signed. The signature scheme simple allows the LibOQS to re-hash the already hashed message, but this action has a cost for the platform's performance. Particularly, the speed of the signature algorithm is the key factor that impacts the performance of schemes with larger signature sizes and keys.

7.4 Performance and Resistance of Potential Blockchain Post-Quantum Cryptosystems

7.4.1 Performance Assessment

The performance of post-quantum digital signatures has been extensively studied in the literature. Such a performance evaluation has been considered with respect to several underlying hardware platforms, as well as, in several networking protocols with several assumptions on the underlying communication channel. In the case of FALCON, the authors measured its performance in terms of spent time instead of cycles. For Rainbow, the values indicate the performance of the key-compressed version that require much more computational effort than the regular version due to the involved decompression process. However, most cryptosystems have been evaluated after optimizing them for AVX2, a 256-bit instruction set provided by Intel. The only exception is the performance of SPHINCS for the HARAKA version, whose optimized version was implemented to take advantage of the AES-NI instruction set.

It is interesting to point out that this performance evaluation presented in Table 7.4 is based on appropriate hardware that can be used for running both a regular blockchain node (i.e., a node that only interacts with the blockchain) or a

Table 7.4. An overall performance evaluation on post-quantum signatures being present in the 3rd round of NIST evaluation [19].

Scheme	Algorithm	Execution Time (ms)	Size (Bits)
Dilithium	Dilithium II	$KeyGen = 0.18$ $Sign = 0.82$ $Ver = 0.16$	$K_s = 22,400$ $K_p = 9,472$ $\sigma = 16,352$
Falcon	Falcon-512	$KeyGen = 16.77$ $Sign = 5.22$ $Ver = 0.05$	$K_s = 10,248$ $K_p = 7,176$ $\sigma = 5,52$
Rainbow	Rainbow-Ia-Cyclic	$KeyGen = 0.48$ $Sign = 0.34$ $Ver = 0.83$	$K_s = 743,680$ $K_p = 465,152$ $\sigma = 512$
GeMSS	GeMSS128	$KeyGen = 13.1$ $Sign = 188$ $Ver = 0.03$	$K_s = 107,502$ $K_p = 2,817,504$ $\sigma = 258$
Picnic	Picnic-L1-FS	$KeyGen = 0.005$ $Sign = 4.09$ $Ver = 3.25$	$K_s = 128$ $K_p = 256$ $\sigma = 272,256$
SPHINCS+	SPHINCS+ – SHA256 – 128f – simple	$KeyGen = 2.95$ $Sign = 93.37$ $Ver = 3.92$	$K_s = 512$ $K_p = 256$ $\sigma = 135,808$

full blockchain node (i.e., a node that stores and updates periodically a copy of the blockchain and that is able to validate blockchain transactions).

The conclusions derived can be summarized as follows: first, with respect to multivariate-based cryptosystems, MQDSS provides small keys, its lightest version is quite fast, but the sizes of its signatures are among the largest in the comparison (whereas other multivariate schemes have large sizes. In contrast, the rest of the compared multivariate-based schemes have keys with large sizes, but they generate short signatures; note also that MQDSS does not continue in the third round.

Next, with respect to lattice-based signatures, they generally require smaller keys than the multivariate schemes, but they produce larger signatures. Amongst all of them, FALCON – which continues to the third round of the NIST competition – makes use of the smallest key sizes and signature lengths. qTESLA is also fast, but its major drawback is the large key sizes; qTESLA is not present in the third round of evaluation in the NIST competition. The fastest scheme is Dilithium (amongst all the types of post-quantum signatures – not only amongst lattice-based). DILITHIUM obtains, in terms of performance, very similar results

Table 7.5. Time (ms) of key-pair generation, signing and verification [7].

Scheme	KeyGen	Sign	Verify
BPQS ($w = 4$, *SHA256)*	0.569	0.08	0.10
BPQS ($w = 4$, *SHA384)*	1.107	0.16	0.19
BPQS ($w = 16$, *SHA256)*	0.872	0.19	0.20
BPQS ($w = 16$, *SHA384)*	1.719	0.39	0.38
ECDSA SECP256K1 (SHA256)	0.10	0.34	0.25
Pure EdDSA Ed25519 (SHA512)	0.18	0.08	0.16
RSA3072 (SHA256)	561.1	5.39	0.17
SPHINCS-256 (SHA512)	0.69	144.5	1.76

to ECDSA-256. Unfortunately, DILITHIUM key sizes are much larger than the ones used by ECDSA-256.

However, apart from Dilithium, another option that achieves good performance is the lightest version of the Rainbow. This is also verified, apart from the aforementioned results in [10], in the evaluation over the TLS protocol [18]. Note also that Rainbow necessitates smaller parameters than Dilithium, thus rendering the algorithm a very strong candidate for future (including blockchain) applications. Falcon provides the best verification time, but it is slow in signing. The slowest digital signature algorithms are Picnic, GeMSS and SPHINCS (all of them are alternate algorithms in the NIST competition).

In order to summarise the results (in terms of performance), we illustrate the performance results of the candidates (and the alternates) in the third round of NIST (see Table 7.4). This table is based on the results from [18], which are in fully compliance with the survey presented in [10].

As stated above, SPHINCS is generally a very slow signing algorithm. It is interesting to point out though that the BPQS, being also hash-based (and outside of the NIST competition) suffices to achieve better performance than SPHINCS, whereas it is blockchain oriented. This is illustrated in Table 7.5. It can be seen that, despite the relevant parameters of BPQS, it is much faster than SPHINCS in terms of signing and verifying (with performance actually comparable to traditional public key digital signature schemes). The main drawback is the key generation time, which however is comparable, in some cases, with the SPHINCS. Regarding the signature size, all BPQS modes outperform XMSS for the first number of signatures. However, BPQS signatures grow linearly with the number of times a key is reused and, thus the length of the signature output is dynamic (it starts small and increases per additional signature).

Table 7.6. Time for generating XMSS trees for a QRL wallet [20].

XMSS Tree Height	No. of OTS Signatures	Hash Function/Algorithm	Gen. Time
18	262.144	SHA2_256 / SHA2	1h 10min 49sec
10	1.024	SHAKE_128 / SHA3	11sec
12	4.096	SHA2_256/ SHA2	1h 20sec
12	4.096	SHAKE_128/ SHA3	48sec
12	4.096	SHAKE_256/ SHA3	46sec

Table 7.7. Information on transactions in QRL [20].

Transaction Size (Bytes)	Signing Time	Signature Size (Bytes)	Verification Time	Block #	Block Size (Bytes)
2662	1sec	2500	4min 36sec	81188	2915
2662	1sec	2500	9sec	81168	2915
2662	1sec	2500	3min 0sec	80944	2915
2704	–	2500	–	80939	2958
2662	1sec	2500	1min 2sec	80205	2915
2662	1sec	2500	24sec	66804	2915
2705	–	2500	–	66739	2959

It is also interesting to focus more carefully on XMSS, and especially on the QRL – which is a ledger supporting XMSS for achieving, by default, post-quantum security. It is known that XMSS has several limitations (and that's why SPHINCS and BPQS are considered as improvements of XMSS); however, XMSS is indeed one cryptographic primitive that is currently used in a post-quantum secure commercial blockchain.

We next present recent experimental results on QRL, aiming to see in practice the performance of QRL (implementing XMSS) in a conventional workstation [20]. The experiments have been conducted in an Intel Core2Duo E6750 @ 2,66GHz processor, with 6 Gb RAM (DDR2 @ 400MHz) and Windows 10 Pro, 64 bit, as an operating system. To perform several measurements, the researcher produced several different wallets with different parameters for the XMSS. The results are shown in Table 7.6.

Moreover, the researcher in [20] proceed in performing several transactions in a testing environment (provided by the QRL), with the ultimate goal to see in practice the corresponding signing and verification times. This is shown in Table 7.7, for

the second wallet. As it is shown in this table, the size of the signature is constant, which is expected since the size of the signature is related with the height of the XMSS tree (or, equivalently, with the number of the OTS signatures). More precisely, in QRL the size of the signature is given by the relation $2180 + (height * 32)$ bytes. The variations in verification time are probably due to the load of the miner in the tested blockchain and the experiments tool placed.

7.4.2 Attacks on PQC Primitives

As NIST has stated the importance of side channel attacks (SCA) and countermeasures. More precisely, in the original NIST PQC call for proposals in 2016, it was stated that *"the Schemes that can be resistant to SCA at lower cost are more preferable than those whose performance is severely hampered by any attempt to resist side-channel attacks."* NIST also hopes to see implementations that will have protective mechanisms against side-channel attacks, such as timing attacks, fault attacks, power monitoring attacks, etc. Therefore, in this section, it is presented a number of SCA and ISD attacks against the NIST PQC 3rd round candidates.

These attacks on the NIST's 3rd round candidates are categorized as:

- Classical Cryptanalysis (CC), which mathematically analyses the corresponding cryptosystem.
- Static Timing Analysis (STA), which manipulates variable runtime of an algorithm.
- Fault Attacks (FA), which are semi-invasive techniques to deliberately induce faults and disclose cryptographic internal states.
- Simple Power Analysis (SPA) and Advanced (differential/correlation) Power Analysis (APA), which non-invasively exploits the variations in the cryptographic algorithm's power consumption.
- Electromagnetic attacks (EMA), which exploit the radiation from a cryptographic algorithm.
- Template attacks (TA) that use a sensitive device to obtain access to the secret.
- Cold-boot attacks (CBA), which exploit the memory remanence to read data out of a computer's memory when the computer has been turned off.
- Countermeasures (CM) that protect/hinder attacks through masking or hiding techniques.

Therefore, the next table (Table 7.8) presents which schemes are directly susceptible on the aforementioned attacks.

Table 7.8. A summary of attacks on NIST PQC 3rd round candidates.

			SCA								
		Algorithm	**CC**	**STA**	**FA**	**SPA**	**APA**	**EMA**	**TA**	**CBA**	**CM**
Finalists	KEMs	Classic McEliece,			✓			✓		✓	
		Kyber			✓	✓		✓	✓	✓	
		NTRU				✓				✓	
		Saber						✓			✓
	Signs	Dilithium			✓			✓			✓
		Falcon			✓						
		Rainbow	✓				✓			✓	
Alternatives	KEMs	BIKE		✓	✓						
		FrodoKEM		✓		✓	✓	✓	✓	✓	✓
		HQC		✓			✓				
		NTRU Prime					✓		✓		✓
		SIKE	✓	✓							
	Signs	GeMSS	✓				✓				
		Picnic	✓				✓				
		SPHINC+			✓						

7.5 Conclusions and Future Directions in PQC Blockchains

This chapter considered the post-quantum security aspects in blockchain technology. More precisely, it has assessed contemporary PQC algorithms and the current situation of the NIST's 3rd round PQC candidates. In addition, it has presented the impact of quantum-computing attacks on blockchains and it has investigated the incorporation of PQC primitives in blockchains.

Currently, quantum computing is an area that has gained a lot of interest from both the academia and the industry. Sequentially, new attacks might be developed against the post-quantum cryptosystems. Therefore, it is necessary that both researchers and industry to be aware to the quantum computing area and its advances and for this reason, we present the challenges and the future directions in PQC blockchains.

7.5.1 Transitioning to Post-quantum Blockchains

The transition to post-quantum blockchains necessitates the involved steps to be considered carefully. Therefore, several researchers have discovered new methods for the implementation of post-quantum security to the blockchain technology. For example, in [21] the authors introduced a scheme that extends the validity of the blockchain, if the security of the digital signatures or of the hash functions is imperiled. However, hard forks or smooth-forks might occur and for this case, the authors proposed a soft-fork mechanism [22]. In another work [23], a commit–delay–reveal protocol is proposed that enables the Bitcoin users to move funds from the non-quantum-resistant protocol to a version that adhere to a quantum-resistant signature scheme. This transition protocol can work well even if the ECDSA has been formerly compromised.

7.5.2 Keys – Signature Sizes and Performance Challenges

The key's sizes in post-quantum cryptosystems are among 128 and 4,096 bits, meaning that the post-quantum cryptosystems demand key's sizes much larger than the public key cryptosystems. Some signature cryptosystems, which are based on supersingular isogenies, appear to be auspicious to solve the key size issue, but such schemes generate large signatures and provide pour performance compared to the public key cryptosystems. As one issue is seemingly solved several others are created, since the blockchains store a vast number of signatures. In a similar way, the hashed-based cryptosystems have comparatively small key sizes, which comes to contradiction with the size of their signatures, which is often more than 40 KB. On the other hand, the majority of the multivariate-based cryptosystems generate short signatures, but the keys used for their generation and verification might need several kilobytes. The lattice cryptosystems, which are based on DILITHIUM are very fast, but their signature length is 2701 bytes and their key size is approximately 1500 bytes.

The post-quantum cryptosystems need a considerable amount of (a) execution time, (b) computational and (c) storage resources. To some extent, some schemes reduce the number of the signed messages with the same key. This practice results to the generation of new keys repeatedly and to the dedication of the computational resources for this purpose that could be otherwise used for certain blockchain processes. Nevertheless, the current research in post-quantum cryptosystems is not adequate for having a good trade-off among the size of the keys and the scheme's performance for the blockchains. Therefore, novel approaches are required, which will minimize the cryptosystems' energy consumption and therefore, the performance of the blockchain network.

7.5.3 General Directions

A large distributed network, such as the blockchain, necessitates exceptional consideration when migrating to a post-quantum cryptography, due to the limitations of the downtime and the synchronous update. Such transitions require not only performance assurance and backwards compatibility, but also slow rollouts and rollbacks. Therefore, a post-quantum implementation of a blockchain network requires the following steps:

I. Software rollout: A slow rollout of the software to all the network's peers. This migration should be backwards compatible, with the nodes to be able to continuously sign and verify signatures, as well as, to validate X.509 certificates classically until they change to a post-quantum mode.
II. Key rollover: While the certificate authority will be modified with a post-quantum key, the node certificates should be re-issued following a key rollover method.
III. Slow rollout of the PQC keys: When the key-pairs of post-quantum keys will be generated, the configuration files of each node that belongs to the network should be updated.
IV. The final step will be the rollout of post quantum keys to the client peers.

Therefore, all the above steps should be taken into consideration when implementing post-quantum digital signatures or encryption algorithms to a blockchain platform.

Acknowledgment


This work has received co-funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 786698. The work reflects only the authors' view and the Agency is not responsible for any use that may be made of the information it contains.

References

[1] S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis and S. Shiaeles, "On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance," *Computer Networks*, p. 108005, March 2021.
[2] B. Sotirios, K. Nicholas, L. Konstantinos and S. Stavros, "On the Security of Permissioned Blockchain Solutions for IoT Applications," *2020 6th IEEE Conference on Network Softwarization (NetSoft)*, pp. 465–472, 2020.

[3] S. Brotsis, N. Kolokotronis, K. Limniotis, S. Shiaeles, D. Kavallieros and E. Bellini, "Blockchain Solutions for Forensic Evidence Preservation in IoT Environments," *IEEE Conference on Network Softwarization (NetSoft)*, pp. 110–114, 2019.

[4] N. Kolokotronis, S. Brotsis, G. Germanos, C. Vassilakis and S. Shiaeles, "On Blockchain Architectures for Trust-Based Collaborative Intrusion Detection," *2019 IEEE World Congress on Services (SERVICES)*, pp. 21–28, 2019.

[5] R. C. Merkle, "A certified digital signature," *Conference on the Theory and Application of Cryptology*, pp. 218–238, 1989.

[6] J. Buchmann and E. A. H. A. Dahmen, "XMSS-a practical forward secure signature scheme based on minimal security assumptions," *International Workshop on Post-Quantum Cryptography*, pp. 117–129, 2011.

[7] K. Chalkias, "Blockchained post-quantum signatures," *Cryptology ePrint Archive: Report 2018/658*, 2018.

[8] Bernstein, M. Schneider, P. Schwabe and Z. Wilcox-O'Hearn, "SPHINCS: practical stateless hash-based signatures," *Annual international conference on the theory and applications of cryptographic techniques*, pp. 368–397, 2015.

[9] S. Suhail, R. Hussain, A. Khan and C. S. Hong, "On the role of hash-based signatures in quantum-safe internet of things: Current solutions and future directions," *IEEE Internet of Things Journal*, 2020.

[10] T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21091–21116, 2020.

[11] 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, pp. 27205–27213, 2018.

[12] A. Coladangelo, "Smart contracts meet quantum cryptography," *arXiv preprint arXiv:1902.05214*, 2019.

[13] M. C. Semmouni, A. Nitaj and M. Belkasmi, "Bitcoin Security with Post Quantum Cryptography," *Networked Systems*, pp. 281–288, 2019.

[14] 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, 2018.

[15] J. Preece and J. Easton, "Towards encrypting industrial data on public distributed networks," *2018 IEEE International Conference on Big Data (Big Data)*, pp. 4540–4544, 2018.

[16] R. Shen, H. Xiang, X. Zhang, B. Cai and T. Xiang, "Application and Implementation of Multivariate Public Key Cryptosystem in Blockchain (Short Paper)," *International Conference on Collaborative Computing: Networking, Applications and Worksharing*, pp. 419–428, 2019.

[17] B. Das, A. Holcomb, M. Mosca and G. C. Pereira, "PQ-Fabric: A Permissioned Blockchain Secure from Both Classical and Quantum Attacks," *arXiv preprint arXiv:2010.06571*, 2020.

[18] D. Sikeridis, P. Kampanakis and M. Devetsikiotis, "Post-Quantum Authentication in TLS 1.3: A Performance Study.," *IACR Cryptol. ePrint Arch.*, vol. 2020, p. 71, 2020.

[19] T. G. Tan, P. Szalachowski and J. Zhou, "SoK: Challenges of Post-Quantum Digital Signing in Real-world Applications".*eprint.iacr.*

[20] N. Sakellion, "Post-quantum cryptography in blockhain technologies," Cyprus, 2020.

[21] M. Sato and S. Matsuo, "Long-term public blockchain: Resilience against compromise of underlying cryptography," *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–8, 2017.

[22] F. Chen, Z. Liu, Y. Long, Z. Liu and N. Ding, "Secure scheme against compromised hash in proof-of-work blockchain," *International Conference on Network and System Security*, pp. 1–15, 2018.

[23] I. A. I. D. Stewart, A. Zamyatin, S. Werner, M. Torshizi and W. J. Knottenbelt, "Committing to quantum resistance: a slow defence for Bitcoin against a fast quantum computing attack," *Royal Society open science*, vol. 5, no. 6, p. 180410, 2018.

Contacts

S. Brotsis
University of the Peloponnese
brotsis@uop.gr

N. Kolokotronis
University of the Peloponnese
nkolok@uop.gr

K. Limniotis
Hellenic Data Protection Authority
klimniotis@dpa.gr