Blockchains in the Quantum Era

cloud security alliance®

The permanent and official location for Cloud Security Alliance Internet of Things research is https://cloudsecurityalliance.org/working-groups/quantum-safe-security/

Acknowledgments

Lead Author:

Bruno Huttner

Contributors:

Edward Chiu
John Hooks
Aaron Kent
John Young

Reviewers:

Boulevard Aladetoyinbo
Andrew Brick
Nadia Diakun-Thibault
Ken Huang
Ashish Mehta
Urmila Nagvekar

CSA Staff:

Hillary Baron
AnnMarie Ulskey (Graphic Design)

Table of Contents

1. Introduction

Digital Ledger Technologies (DLT) such as blockchain are being deployed as part of diverse applications spanning multiple market segments. Application developers have successfully leveraged blockchain characteristics of decentralization, immutability, cryptographic security, and transparency to create the benefits of redundancy, non-repudiation and enhanced auditing/compliance. Blockchain infrastructures make extensive use of digital signature algorithms, hashing algorithms, and public-key cryptography. The rapid pace of progress happening within quantum computing technology has made the prospect of quantum computer cyber-attacks a very real possibility. See, for example, the recent review on the quantum threat, which has been published by the CSA.

Initiatives are therefore underway to augment today's DLT/blockchain infrastructures with cryptographic algorithms designed to be resistant to quantum computer attack. These post-quantum algorithms are based on computational problems known to be very difficult for quantum computers to solve by using either Shor's algorithm or Grover's algorithm. This paper provides an introduction to DLT/blockchain technology, some of its representative applications, and an overview of the leading post-quantum algorithm candidates that are actively being pursued.

2. Blockchain Overview

We assume our reader has a working knowledge of Blockchain. If not, we recommend the following links: blockchain introduction from coindesk or an introduction to blockchain technology from NIST. Here we review only briefly the main ideas and tools.

2.1 What is a Blockchain?

The blockchain is a decentralized distributed ledger, on a network of many nodes, with a specific update mechanism, which ensures synchronization between all nodes. This ledger contains linked blocks of transactions. Users can post new transactions, which have to be validated by the network before appending to the ledger. The complete structure is secured by cryptographic processes in order to provide immutability: a transaction validated by the network cannot be altered.

Blockchains are based mainly on two cryptographic primitives, cryptographic hash functions and public key signatures. Signatures have two purposes. They allow users to authenticate their transactions with their private key and enable the blockchain to verify their validity with the public key. Hash functions provide the immutability: once the hash of a transaction block is published on the blockchain, the transaction cannot be modified. This hash is then included in the next transaction block, and on to the next, building a chain of blocks, the blockchain. Any modification in one of the earlier blocks by a rogue node would translate into a modification of all further blocks, which will quickly be discovered by the honest nodes and rejected.

2.2 How it All Started: Bitcoin and Cryptocurrencies

Historically, the first blockchain and still the most used one, is the Bitcoin. With Bitcoin, transactions are exclusively monetary. Bitcoin is the first example of a cryptocurrency. Many other cryptocurrencies have since been invented, based on similar principles. The main advantages of cryptocurrencies decentralization, limited anonymization, and publicly verifiable immutability of transactions.

2.3 A New Paradigm: Smart Contracts

The blockchain structure can also be applied to different types of transactions. In the Ethereum blockchain, for example, transactions can also be supported by pieces of software, which execute when a set of conditions are met. This is the basis of the "smart contracts," which are at the core of new emerging applications.

2.4 Emerging Blockchain Applications

The intrinsic characteristics of blockchain technology position it as a disruptive technology enabling innovative business transformations across multiple market segments. Its decentralized and immutable nature can enable counterparties to conduct transactions, verify them and audit previously completed transactions with an exceptional level of confidence. But it is the functionalities of smart contracts that offer the maximum transformational potential to automate business processes and workflow. Although the primary use of blockchain technology has historically been synonymous with cryptocurrency applications such as bitcoin, a brief review of some emerging use cases within other market segments can help to illustrate the increasing exposure that blockchain applications may have to future quantum computer attacks.

- **Financial Services - Clearing and Settlement.** The use of blockchain technology has the potential to dramatically reduce the time needed to clear and settle the trading or exchange of financial assets. A blockchain-based service that automates database/registry updates and the associated workflow can reduce this time interval from days to minutes. More details can be found in the position paper on blockchains in the finance industry by HP and in a another paper on blockchain use cases published by the CSA.
- **Identity Management Services.** Blockchain technology is particularly well suited for the support of distributed identity management services. A cryptographically secure "digital identity" can be created on the blockchain for each individual. Counterparties can then use the identity "proofs" or attestations from a digital identity to prove that user's identity. This is clearly explained in a recent NIST position paper on identity management.
- **Healthcare.** Blockchain technology can potentially support a wide variety of healthcare use cases (e.g. secure access to patient health records, secure auditing of healthcare transactions, mitigating or preventing the flow of fraudulent prescription drugs). The interested reader may consult a presentation on blockchain in healthcare another position paper on blockchain in healthcare.
- **Smart Homes and IoT.** Blockchain-enabled IoT (Internet of Things) devices that exist within a home environment can be remotely controlled and managed (e.g. home appliances, consumer electronics) in a secure manner. See, for example, a position paper from the BCG and another paper on blockchain for IoT published by the CSA.

- **Supply Chain and Logistics.** Blockchain-enabled IoT devices (e.g. motion sensors, GPS sensors, temperature sensors, vehicle information sensors) can provide granular status updates as shipments traverse complex supply chains. Smart Contracts can also be deployed to automate tasks along the way (e.g. automatically initiating remedial action if the temperature within a refrigerated truck drops too low). This has been addressed by a position paper from the World Economic Forum and a paper published by the CSA.
- **Automotive Industry.** Blockchain technology is being assessed for its applicability in supporting autonomous cars, automated fuel payments, smart parking and automated traffic controls. An example can be found in a position paper from Cube.

Business-critical blockchain applications created within different market segments will likely exhibit the same quantum security vulnerabilities in the form of a common attack surface. Once this attack surface becomes targeted by future quantum computer attacks, the entire industry-wide blockchain security exposure can quickly eclipse the exposure otherwise attributed to Bitcoin cryptocurrency. Potentially, malicious actors may be collecting data, now protected by quantum-vulnerable cryptographic schemes, in order to decrypt it when quantum hardware becomes available. It therefore becomes increasingly imperative to create suitable quantum security countermeasures sooner rather than later.

3. The Quantum Era

The complete blockchain framework relies on the security of the cryptographic processes underlying it. Without trusted hash functions and public key signatures, there are no blockchains. Quantum computers, which perform computations deemed impossible with a classical computer, threaten several of the cryptographic primitives used in blockchains. Universal, scalable quantum computers, which are necessary to attack the mathematical problems behind the cryptographic primitives, are not yet available. However, small scale quantum computers, with a restricted input size and a restricted number of computations, have already been built by several companies and world governments. Some are even accessible on the internet and can be used to test quantum algorithms. Quantum supremacy, which describes the point in time when quantum computers explicitly outperform classical ones, has either been attained or is on the verge of realization. It is therefore of utmost importance to understand the threat posed to blockchains and to outline possible solutions.

4. Main Cryptographic Tools for the Blockchain

Given that future quantum computer attacks will target the building block components of a blockchain, it is imperative to analyze the threat in more detail for each of them.

4.1 Random Number Generation

Random number generation is at the core of most cryptographic processes. As classical computers are deterministic, generating good randomness is not easy. There are many instances in which poor

randomness led to disaster such as in the following recent case. This is especially true for blockchain, where random numbers are applied at various levels of the protocol. The problems are more acute with isolated servers, where most of the computations are performed without any human intervention. Here, quantum technologies can actually help. Quantum theory is indeterministic by essence. Basing random number generation on quantum is therefore a safer way to provide good randomness. Quantum Random Number Generators (QRNGs) now exist in very small form factors. See, for example, the Quantis QRNG chip from ID Quantique. Such small QRNGs can be easily integrated into the servers, maintaining the nodes of the blockchain, and even in the various terminals, such as PCs and smartphones on the user's side.

4.2 Hash Functions

Cryptographic hash functions are truly the workhorse of the cryptographic processes that implement the blockchain. They transform a text input of any length into a fixed length output. The output is deterministically linked to the input, but it is impossible to recover the input from the output, except by brute force, i.e. trying every single input until the correct output is found.

In blockchains, hash functions are used for two purposes. The first one is to guarantee the immutability of the blocks. The most commonly used hash function, SHA256, has a 256 bits output. A brute force attack on this function would require 2^{256} operations, well beyond the capacity of even the largest supercomputer. A quantum attack with the Grover algorithm would reduce this to 2^{128} , which is still unfeasible. The quantum computer will not be able to destroy the immutability of the blockchain, but it may necessitate a doubling of the hash function size.

The second purpose of hash functions for many blockchains is to provide the so-called Proof-of-Work (PoW), which nodes on the network have to complete in order to add a new block. The idea is that, when a new block is ready to be added on the network, miners compete to execute a computation on this block. The first to finish the computation is allowed to add the block and gets a reward. The computation is precisely inverting a hash function with a shorter output. Here again, the Grover algorithm implemented on a quantum computer will allow a much faster calculation.

4.3 Public-key Signatures

Public-key cryptography is used to authenticate the transactions that are completed on a blockchain. The sending party, Alice, will digitally sign a transaction by using her private key. The receiver, and any interested party, can then use Alice's public key to verify that the digital signature is valid. Public-key cryptography is also used to support digital wallet operations on a blockchain. A digital wallet is associated with a public address on the blockchain through some form of hashing conducted on the user's public key. Digital wallets are typically used to securely store a blockchain user's private key along with transaction-related data that may be relevant to the blockchain application. This data might take the form of a user's current cryptocurrency balance in the case of Bitcoin or Ethereum.

[1] This is done by hashing the block, and then hashing a concatenation of this hash with a random number (nonce), until a hash with a given number of leading zeros is obtained. The only known way to achieve this is brute force. This can be easily validated, by sending the value of the random number and asking the other nodes to check.

The public-key signatures used in the blockchain are based on Elliptic Curve Cryptography (ECC), which has a very small key size and is easy to implement in the blockchain environment. Unfortunately it is now known that the current ECC will be destroyed by the Shor algorithm implemented on a quantum computer. This means any public key published on the blockchain will leak the corresponding private key to an adversary equipped with a quantum computer. This is a catastrophe for some blockchains, such as the future and often delayed new release of Ethereum (Ethereum 2.0) based on proof of stake, where publishing the public key is required. It is much less serious for other types of blockchains, such as Bitcoin, where the publicly available address is a hash of the public key, or consortium blockchains which leverage symmetric-key cryptography. See the section below for details.

5. Risk Analysis on a Few Blockchains

Although all blockchains rely on the same cryptographic primitives, the implementation details are distinct. The quantum threat therefore applies at different levels. We exemplify this by briefly analyzing a few existing blockchains. This requires us to explore relatively deeply into the blockchain structure and its technical details. The aim is to show, with a few selected examples, the nature of risk, and how it may be mitigated. A more complete analysis is beyond the scope of this position paper.

5.1 Bitcoin

Bitcoin is the first and still most popular blockchain. For readers who are unfamiliar with the workings of Bitcoin, the best, although a bit outdated, source is the original Book of Satoshi (Satoshi is the pseudonymous inventor of the whole concept). Here, we will simply list the basic issues linked to possible quantum computer attacks.

- Immutability of the chain: This is obtained through hashing, which is understood to be quantum-safe. There is very little risk when sufficiently long hashes are used (i.e. 256 bits and above allows for a factor of two downgrade in view of Grover's algorithm). This is the case for Bitcoin, which uses the SHA 256 algorithm.
- Public address: Transactions are identified by an address, which is a hash of the public key of the receiver. So, if users want to receive bitcoins, they have to create a public/private key pair, and compute an address, which is a hash of their public key. The asymmetric algorithm used by Bitcoin is ECC, which is not quantum-safe. However, as long as the public key is hidden by the hash function, it is well-protected. The public key is published when the user needs to spend the bitcoins associated with the address. This is to ensure the verification of the transaction by the blockchain. However, in a transaction, all the bitcoins linked to this address have to be spent. Any "change" left is sent, in principle, to a new address. If this rule is followed, the only risk from a quantum computer is from an adversary intercepting the transaction, breaking the key and performing another transaction, all within a few minutes. It is rather unlikely that a quantum computer will be fast enough to do this in the near term. This risk is therefore minimal. However for practicality, many users re-use the same address for several transactions. This is not the proper implementation and puts their bitcoins at risk from a quantum computer.

- For PoW: An adversary with a quantum computer may perform PoW much faster than other miners and gain a big advantage. In particular, malevolent users equipped with a quantum computer could attempt a 51% attack and take control of the blockchain. However, this may not be much worse than the initial issues that bitcoin faced, when miners using custom-designed hardware managed to gain a large advantage with respect to others relying on general PCs. This will have to be investigated in more detail.

5.2 Ethereum

Ethereum is the second most popular blockchain platform. It is a global, open-source platform where decentralized applications are built and run and is the underlying platform for the popular Ether token. Many commercial applications are built with Ethereum. Public Ethereum platforms are used for bond issuance and settlement, supply chain automation, credentialing with blockchain certificates, streamlining payment process for utility providers, and so forth. A good guide to Ethereum is the book Mastering Ethereum. In this section, we will simply list the basic issues linked to quantum safety.

- Immutability of the chain: Similar to Bitcoin, immutability in the Ethereum Network is obtained through hashing specifically Keccak-256 (or commonly referred to as SHA-3 in Ethereum circles), which is quantum-resistant.
- Consensus: The consensus mechanism used by Ethereum is currently proof-of-work (PoW), and as in Bitcoin, an adversary with a quantum computer could attempt a 51% attack and take control of the blockchain.
- Ownership of Funds and Contracts: Ethereum uses public key cryptography, which makes use of public-private key pair to represent an Ethereum account with a publicly accessible account handle (the address) and ownership of funds (ether) in the account as well as any authentication the account needs when using smart contracts. The private key controls access by being the unique piece of information needed to create digital signatures, which are required to sign transactions to spend any funds in the account. Digital signatures are also used to authenticate owners or users of contracts.
- The current use of ECDSA by Ethereum to sign transactions is not quantum-resistant.
- Ethereum addresses: These are unique identifiers that are derived from public keys or contracts using the Keccak-256 one-way hash function, which is quantum resistant.
- There is a major upgrade to a new version of Ethereum, Ethereum 2.0, currently underway. Slated to be completed in 2022, it includes upgrades in development features, performance and security. This release will rely on Proof-of-stake (PoS), which is another class of consensus mechanism. In PoS each validating node votes on the addition of a new block. The weight of each validating node depends on the stake it is willing to commit. Advantages of PoS include security improvement, reduced risk of centralization, and energy efficiency. This is described in a FAQ on PoS. In addition, it will include addressing the quantum threat, with quantum-resistant signature schemes such as Lamport, XMSS (eXtended Merkle Signature Scheme) or SPHINCS.

5.3 Hyperledger Fabric (HLF)

Hyperledger Fabric is a permissioned distributed ledger platform, originally developed by IBM and Digital Asset. It is a specific framework within the Hyperledger Project founded by the Linux Foundation in 2015. Hyperledger Fabric is an enterprise-grade platform for the development of modular applications. It provides a scalable and secure platform that supports private transactions and confidential smart contracts. Here, we will identify the basic issues linked to the quantum safety:

- Immutability of the chain: Just like the Bitcoin, immutability in the Fabric is obtained through hashing specifically (SHA-256 algorithm) which is understood to be quantum-safe.
- Transactions: Transaction is a request to the Hyperledger Fabric to modify the state of the ledger. Cryptography ensures integrity of transactions by linking the transaction to previous blocks and ensuring the transactional integrity, if protected, by linking the cryptogram or hash from previously linked blocks. Cryptographic modules within Hyperledger Fabric are pluggable, so modules can be updated to ensure they are quantum safe.
- Identity and Access Management: Since Fabric is a permissioned network, it relies heavily on all members being identified and known to the network. It uses a specialized digital Certificate Authority (CA) for issuing certificates to members of the blockchain network. The Certificate Authority is based on cryptographic function modules that are pluggable within Fabric and can be updated to ensure that they are quantum safe. However, the current signature scheme used in Hyperledger Fabric is not currently quantum-resistant in nature. Research is currently underway to explore the use of a lattice-based digital signature scheme known as qTESLA. This digital signature scheme has been accepted into the NIST Round 2 of digital signature candidates but has not made it into Round 3. It is therefore rather likely that a new signature scheme will be proposed for testing of Hyperledger Fabric against quantum resistant attacks.

5.4 Zcash

Zcash is a fork of Bitcoin that provides the added ability to turn on privacy features related to a transaction. The sender and recipient data, as well as the transaction amount, are protected for privacy but at the same time Zcash provides immutability and verifiability associated with any mainstream blockchain-based system. Privacy features and transaction validity are achieved by means of zero-knowledge proofs and in particular the use of Zero-Knowledge Succinct Non-interactive Arguments of Knowledge (ZK-SNARKs). ZK-SNARKS requires the setup of a trusted party(ies) to enable the zk proof system.

Currently the Zcash encryption mechanism is vulnerable to quantum computer attack. As a consequence, by using a known recipient's address, the amount as well as the encrypted memo associated with the transaction can be discovered. Additionally, the verification process may be manipulated to forge a counterfeit Zcash.

There is currently much research being conducted to develop a post-quantum (PQ) Zcash, such as that based on lattice-based zk-SNARKs. A potential PQ approach may be to incorporate Zero-Knowledge Scalable Transparent Arguments of Knowledge (ZK-STARKs) as part of the Zcash protocol. An added

advantage of ZK-STARKs would be that the requirement for the setup of the trusted entities is not necessary thereby mitigates any potential compromise of privacy by those entities.

6. Future Solutions

6.1 Quantum-Safe Signatures and Encryption

The possibility of a quantum computer breaking all of the secure connections ever recorded, decrypting secure databases, and modifying all the blockchain records ever created could cause large scale damage (both technical and financial) to the security of Internet-connected blockchain networks.

At least one basic cryptographic primitive behind most existing blockchains (i.e. the digital signature scheme) will be broken by the quantum computer. Although, due to their structure, some blockchains, especially those leveraging symmetric-key cryptography, are relatively resilient and others may become so with some simple changes in rules, this primitive will have to be modified.

In addition, in most blockchain implementations, the public/private key pairs are stored by users in digital wallets. Some of these wallets are stored online, for example, at exchanges, and some are stored by the users themselves, typically on portable drives. Since these wallets store the private key, the issue of confidentiality arises. In most instances, confidentiality is also provided by public key infrastructure, with encryption of the keys exchanged over insecure channels. This encryption may also be threatened by the quantum computer. However, since the encrypted wallets can be made quantum resistant independently of the blockchain itself, we will not discuss these further.

Work is currently underway in the NIST process to select suitable candidates for both quantum-resistant signatures and key exchange mechanisms, which can be used to encrypt the private keys. We will review only the signature schemes below.

6.2 Attributes of Post-Quantum Blockchain Signatures

Several industry initiatives to define suitable post-quantum cryptosystems for use with blockchains are currently underway. In addition to providing the necessary level of resistance to future quantum computer attack, these algorithms must be viable from a practical deployment perspective. Some particularly important attributes include the following:

- Small Digital Signatures and Hash Sizes: Since a blockchain represents a continually growing repository of transactions, it is important to minimize the size of digital signatures and hashes being stored.
- Small Public and Private Key Sizes: Suitable post-quantum algorithms must minimize key sizes in order to reduce blockchain storage requirements and to reduce the computational overhead associated with key operations.
- Computationally Fast: Post-quantum algorithms should be computationally fast to execute in order to support high-performance and scalable blockchain infrastructures.

6.3 Post-Quantum Signatures under Standardization

At the present time there are three finalist candidates for standardization of signatures schemes by NIST. Two are based on lattices and one on multivariate cryptography. In addition, there are three alternate candidates, based on hash functions, zero knowledge proofs, and again, multivariate schemes. Many other candidates for the first and the second round have been eliminated. Please refer to the recent assessment of leading post-quantum algorithms as published by the IEEE. A brief summary of these algorithms has been provided below:

6.3.1 Finalist Lattice-Based Cryptosystems

Lattice-based cryptosystems are based upon the geometric construct known as a lattice. Lattices are periodic structures of points that exist within an n-dimensional space. Problems such as the Shortest Vector Problem (SVP) are NP-hard and involve determining the shortest non-zero vector that exists between two points within such a lattice. This and other related problems cannot be solved very efficiently with the use of a quantum computer. Since the implementations of these schemes can be computationally simple to execute, they can be well-suited for use within blockchains. Unfortunately, they all currently incur the storage/use of large keys.

These increased key sizes introduce substantial transmission latency, even if processing times are generally faster than their RSA counterparts. Because consensus mechanisms seek to optimally synchronize validation processing and network communication, the implications of reduced processing time and higher transmission latency vary widely depending on the blockchain/DLT.

Crystals-Dilithium is one such digital signature scheme based on the computational hardness associated with lattice-based cryptosystems. It is recommended by the Crystals (Cryptographic Suite for Algebraic Lattices) organization that the Dilithium-1280x1024 parameter set should be used in order to achieve approximately 128 bits of security against all known classical and quantum attacks. The Crystals-Dilithium digital signature scheme is a NIST Round 3 candidate for digital signature algorithms. Optimized versions of the Dilithium schemes are of considerable interest for blockchain deployments because they represent some of the fastest schemes from an execution perspective. Some additional work is still needed in order to reduce their key sizes.

Falcon is another lattice-based signature scheme selected as a finalist for Round 3. Its digital signatures are shorter in size when compared with other lattice-based schemes. The use of Fast Fourier sampling also results in faster digital signature generation and verification operations as compared with other related schemes. Falcon may also be a promising candidate for use within blockchains.

6.3.2 Finalist Multivariate Cryptosystems

Multivariate cryptosystems are expected to achieve a high-degree of resistance to quantum computer attack because they rely upon the computational hardness associated with solving sets of multivariate polynomial equations. Multivariate-based signature schemes can be implemented in a relatively efficient manner and require only fairly modest computational resources. These attributes are highly desirable from a blockchain perspective. Although these schemes produce relatively short

signatures, they can necessitate the use of relatively large public key sizes. These schemes are, however, not as vetted as their lattice-based counterparts.

Rainbow is the finalist multivariate scheme selected by NIST for Round 3. It is based upon the NP-Hard difficulty of solving random multivariate quadratic systems. The use of Rainbow shows considerable promise from a blockchain perspective due to its very efficient signature generation and verification operations.

6.3.3 Alternate Candidates

SPHINCS+ (hash-based): SPHINCS+ is a stateless, hash-based digital signature scheme and therefore has the advantage of being a "drop-in replacement" for existing digital signature schemes. Improvements were introduced to the original SPHINCS scheme as a way to reduce the size of its digital signatures. This scheme relies on the correlation of a series of one-way hashes. The more secure versions of this scheme may not exhibit the performance characteristics needed for use within a blockchain environment.

Picnic (MPC-in-the-head ZKPoK): Picnic is based on a different approach compared with many other post-quantum digital signature candidates. Rather than being based on the level of computational "hardness" from number theory, it leverages the concept of zero-knowledge proofs in conjunction with symmetric cryptography, hash functions and block ciphers. Although Picnic-based schemes (e.g. Picnic2) present definite security benefits, they may not possess the performance characteristics needed for blockchain deployments.

GeMSS (HEv- Multivariate): GeMSS (Great Multivariate Short Signature) is a multivariate-based signature scheme that produces relatively small signatures. The associated signature verification process is stated to be fast, and it utilizes a medium/large public key. Overall performance of the more secure versions of GeMSS may be a concern for blockchain deployments.

6.3.4 Other Interesting Candidates

qTESLA represents an additional Lattice-based digital signature scheme that was a NIST Round 2 candidate for post-quantum digital signatures, but it was not selected for Round 3. It relies upon the computational hardness of a decisional Ring Learning With Errors (R-LWE) problem. Although qTESLA is relatively simple to implement and is considered to be reasonably fast, the scheme uses relatively large key sizes. It has been one of the schemes under consideration for use in securing Hyperledger Fabric against future quantum computer attacks.

6.4 Quantum Blockchains

In addition to the classical solutions described above, academic research is currently underway to explore the feasibility of leveraging quantum effects to counter the threat of the quantum computer on blockchains. In an interesting twist — "quantum against quantum"— the expectation is that quantum blockchains may provide the ultimate in security. These systems do not incorporate post-quantum algorithms as the means to increase resistance to quantum attack but rather natively adopt quantum effects such as entanglement.

To date, there is no real implementation of quantum blockchains. One proposal, from Kiktenko et al., uses existing quantum key distribution or QKD to protect the blockchain. Another one from Del Rajan and Matt Visser describes a conceptual design for a quantum blockchain that involves encoding a blockchain into a temporal GHZ (Greenberger-Horne-Zeilinger) state of photons that do not co-exist in space. Fast Quantum Byzantine Agreements have been mathematically demonstrated to be able to reach consensus in constant time.

These leveraged quantum effects present further opportunities for time complexity reduction for DLT systems. Much like entanglement-driven BFT consensus, the Merkle tree which defines the data structure for storing on-chain transactions, may no longer have to be decrypted in a sequential fashion. Somewhat analogous to popular cryptographic "rollup" solutions, quantum blockchains will be able to leverage higher dimensional matrices to parallelize this process and batch Merkle tree validation. Similarly, quantum properties enable alternate mechanisms to achieve the properties of zero knowledge proofs, like those necessary for ZCash. These are still mainly theoretical areas. We are definitely many years away from real world use cases and implementations of such blockchains. A more detailed discussion of quantum blockchains is beyond the scope of this paper.

7. Conclusion: Transition from Pre-Quantum to Post-Quantum Blockchain

Advances in quantum computing have triggered a growing sense of urgency within the DLT/blockchain community to identify post-quantum algorithms that are both effective and practical to deploy. The transition from pre-quantum to post-quantum blockchain is necessary to ensure the security of blockchains in the quantum era. The extensive use of digital signatures in support of conducting blockchain transactions represents a prime vulnerability. Much attention is therefore being placed on the development and selection of suitable post-quantum digital signature algorithms, which are suitable for blockchain applications and can be phased in over time. Some of the requirements are outlined below:

First, some computationally intensive post-quantum cryptosystems may not be suitable for certain hardware currently used for implementing blockchain nodes. Therefore, post-quantum schemes should provide a trade-off between security and computational complexity in order to not restrict the potential hardware that may interact with the blockchain. One possibility is having gradations of key strength based on the hardware available.

Second, certain post-quantum cryptosystems generate large overheads that may impact the performance of a blockchain. To tackle this issue, future post-quantum developers will have to minimize ciphertext overhead and consider potential compression techniques.

Finally, in order to increase security, some post-quantum schemes may limit the number of messages signed with the same key. As a consequence, it would be necessary to generate new keys continuously, which involves dedicating computational resources and slowing down certain blockchain processes. Therefore, blockchain developers will have to determine how to adjust such key generation mechanisms to optimize the efficiency of the blockchain from the perspective of both speed and transactions.

In the selection of the right schemes, the NIST Post-Quantum Cryptography Standardization project is widely recognized as the preeminent authority that will drive the selection and adoption of post-quantum algorithms. As of September 2020, Lattice-based cryptosystems known as Crystals-Dilithium and Falcon continue to show promise given that they have been selected as Round 3 digital signature finalists within the competition. The Rainbow multivariate scheme, also selected for round 3, might also be used. However, given the specific requirements of blockchain applications, it is also possible that other signature schemes might need to be applied.