Infotrend

# Blockchain Systems in the Age of Quantum Computers

MARTIAL MICHEL AND IAN MELHORN

# Contents

# Executive Summary

In the digital age, cryptography is the cornerstone of data security, employing mathematical algorithms to prevent unauthorized access or alteration of data. The advent of quantum computing presents a potential threat to many existing cryptographic systems. This poses a significant concern for blockchain technology, which heavily relies on cryptography for its security. Post-quantum cryptography (PQC) is a burgeoning field aimed at developing cryptographic algorithms resistant to quantum computer-based attacks. Within the context of blockchain, several research domains emerge, including post-quantum signature schemes, consensus mechanisms, and privacy-enhancing techniques. This three-part exploration of cryptography, quantum computing, and blockchain technology underscores the need for continued research to secure, maintain integrity, and ensure privacy of blockchain systems in a potentially post-quantum world.

# Cryptography Evolution and Brute Force

Cryptography, in essence, is the art of concealing information within codes. This practice, which dates back millennia, is the bedrock of data security, utilizing mathematical algorithms and protocols to safeguard data from unauthorized interception, modification, or decoding. Before we delve into the intricate relationship between quantum computers and blockchain systems, let's embark on a journey through the evolution of cryptography.

## The Dawn of Cryptography: From Caesar's Cipher to Medieval Complexity

Cryptography initially took form through simple substitution ciphers. A prime example is the Caesar cipher, which Julius Caesar famously used to encrypt military messages. This process involved shifting each letter in a message by a specific number of places down the alphabet, a straightforward yet effective method of concealment.

As we moved into the Middle Ages, cryptography's complexity increased, giving birth to transposition ciphers, which rearrange the letters' order in a message, and more advanced substitution ciphers, which replace letters with other letters or symbols.

The invention of printing and the subsequent rise of literacy in the 16th and 17th centuries spurred further advancements. Cryptographers introduced polyalphabetic ciphers, which utilize multiple alphabets to encrypt messages, and steganography, a technique that cleverly hides messages within other texts or images.

## Cryptography in the 20th Century: A Tool of Warfare and National Security

As we entered the 20th century, cryptography evolved from a practical tool to a critical instrument for military intelligence and national security. The World Wars saw the use of various encryption techniques to protect sensitive information. Techniques such as codebooks, which contained unique codes for words or phrases, the Playfair cipher, a polygraphic substitution cipher encrypting pairs of letters simultaneously, and the ADFGVX cipher, a fractionating transposition cipher using multiple symbols to represent each letter in a 6x6 grid, were prevalent during World War I.

World War II witnessed the ingenious use of Native American code talkers, who transmitted coded messages using their native languages, creating virtually unbreakable codes. The Navajo code talkers, in particular, played an essential role in the Pacific theater of the war. Another technique, the one-time pad, involved using carbon paper to create a series of random letters and numbers.

The Enigma machine, a complex piece of machinery involving rotors, electrical connections, and a keyboard, was another significant advancement in encryption. As a letter was typed on the keyboard, electrical signals were sent through the rotors and reflected, substituting the letter with another. The settings of the rotors and plugboard connections were changed daily, forming the basis of symmetric key cryptography, where the same secret key was used for both the encryption and decryption of messages.

The Data Encryption Standard (DES), a symmetric key algorithm that encrypts data in fixed-size blocks of 64 bits using a 56-bit key, was developed in the 1970s. However, the Advanced Encryption Standard (AES) replaced it in 2001 for its superior security.

## The Advent of Asymmetric Key Cryptography

Asymmetric key cryptography, also known as public key cryptography, revolutionized encryption by introducing the concept of using two different keys - a public key and a private key - for the encryption and decryption process. These keys are mathematically related but not identical. As the name suggests, the public key is available to everyone and is used to encrypt messages. On the other hand, the private key is kept secret by the owner and is used to decrypt messages. This method is widely used to secure sensitive information in the digital world, even without a shared secret between the sender and the receiver. If a hacker intercepts the encrypted message, they will not be able to decrypt it without access to the private key.

Elliptic-Curve Cryptography (ECC) is a type of public key cryptography that uses the algebraic structure of elliptic curves over finite fields to generate a pair of public and private keys. ECC is known for its efficiency: It provides the same level of security as traditional asymmetric key cryptography but with significantly smaller key sizes. This makes it faster and less resource-intensive, making it a popular choice for many cryptographic systems, such as blockchain technology.

## Breaking Encryption Using Brute Force

Breaking encryption refers to bypassing security mechanisms to access encrypted data without authorization. A common method for breaking cryptographic codes is the brute-force attack. This involves trying all possible combinations of a cryptographic key until the correct one is found. The process is time-consuming and resource-intensive, especially when the cryptographic blob (the encrypted data) and the encryption algorithm are unknown. In such cases, an exhaustive search is needed to identify the correct encryption algorithm and key. This involves trying various potential algorithms and keys until the right one is found.

Hashcat is a well-known password-cracking tool that can perform brute-force attacks on encrypted data. It does this by trying every possible password until it finds the correct one. This can be done using a dictionary attack (trying combinations of known or likely words) or a true brute-force attack (trying every possible combination). The time needed to crack a password using brute force depends on several factors, including the length and complexity of the password, the complexity of the encryption algorithm's hash function, the processing power of the machine running Hashcat, and the speed of any graphics processing units (GPUs) used for calculations.

To deter brute-force attacks, some encryption methods use specific strategies. Memory-hard functions, for example, consume large amounts of memory, making it more difficult and resource-intensive for an attacker to perform parallel brute-force attacks. Key derivation functions (KDFs), such as Password-Based Key Derivation Functions (PBKDF), are used to create strong, fixed-length cryptographic keys from user-generated passwords, which can then be used to encrypt or authenticate data.

Strong encryption is essential to protect sensitive data from unauthorized access. For instance, a secret key used by 1Password has over 340 undecillion (10^36) possible combinations. With a single recent GPU, achieving a hash rate to compute about 82KH/s would take about 4 Decillion (10^33) seconds or over 12 septillion (10^24) years to crack the password using brute force. This demonstrates the sheer magnitude of security provided by strong encryption. The more complex the key, the more secure the encryption, and the more difficult it becomes for unauthorized individuals to gain access to the encrypted data.

# Post-Quantum Cryptography

Quantum computers' fundamentally different computation approach allows them to outperform classical computers in solving specific types of problems. These include factoring large numbers and solving discrete logarithm problems.

Quantum computing, although not yet widely available, has advanced significantly with the development of new quantum algorithms, enhancements in the reliability and scalability of quantum hardware, and exploration of potential applications in diverse fields such as chemistry, cryptography, and optimization. Tech giants like IBM, Google, and Microsoft are investing in developing quantum computers and facilitating their accessibility via cloud-based platforms.

Quantum computers threaten several cryptographic algorithms that rely on the difficulty of factoring large numbers or solving discrete logarithm problems. These include:

| | |
|---|---|
| **(Rivest-Shamir-Adleman) RSA** | One of the first public-key cryptosystems widely used for secure data transmission. |
| **Diffie-Hellman** | A method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols. |
| **Elliptic Curve Cryptography (ECC)** | An approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. |
| **Digital Signature Algorithm (DSA)** | This is a Federal Information Processing Standard for digital signatures. |
| **SHA-2 and SHA-3** | Secure Hash Algorithms (SHAs) are cryptographic hash functions designed by the National Security Agency (NSA). |
| **Advanced Encryption Standard (AES)** | While quantum computers could potentially break AES, it would take a significant amount of quantum bits (qubits). |

It is important to note that the development of quantum computers does not automatically mean these algorithms will be broken. Cryptographers are already working on quantum-resistant algorithms to replace the ones potentially threatened by quantum computing.

Post-quantum cryptography (PQC) aims to resist quantum computer attacks. The objective is to maintain the security of information assets even when a large-scale quantum computer exists. The key characteristics of these algorithms include:

**Quantum Resistance**

The mathematical problems these algorithms are based on must not be solvable in polynomial time by any known quantum algorithm.

**Efficiency**

Due to their complexity, PQC algorithms often require larger key sizes or more computational resources than traditional ones. Therefore, they should be designed to not excessively consume CPU time, memory, and bandwidth.

**Security**

PQC algorithms must provide a high level of security against classical attacks, such as brute-force, side-channel, and chosen-ciphertext attacks.

**Interoperability**

The new PQC algorithms should be compatible with the existing infrastructure to ensure a smooth transition. This means they should be designed to work in conjunction with existing protocols and on both new and older hardware systems, including edge or resource-constrained devices.

Several classes of PQC algorithms with these attributes are being considered and researched, with the most common being:

### Lattice-Based Cryptography

Bases its security on mathematical problems related to lattices, which are grids of points in multi-dimensional space. The two most significant problems are the Shortest Vector Problem (SVP), which involves finding the shortest non-zero vector in a lattice, and the Closest Vector Problem (CVP), which involves finding the closest lattice point to a given target point. The NTRU cryptosystem, a public key cryptosystem, uses lattice-based cryptography and is believed to be resistant to quantum attacks.

### Code-Based Cryptography

The security relies on the difficulty of decoding a general linear code, known to be an NP-hard problem (nondeterministic polynomial time). This means that the time to solve this problem grows exponentially with the input size, and there is no known efficient solution. The McEliece cryptosystem, one of the earliest proposed post-quantum encryption schemes, is based on this concept.

### Hash-Based Cryptography

Bases its security on the properties of cryptographic hash functions. These functions take an input and return a fixed-size string of bytes. The security of hash functions comes from their ability to make it computationally infeasible to generate the same hash output from two different input values or to regenerate the original input value from the hash value. Merkle signature schemes, used in blockchain systems, for example, are a hash-based cryptographic system.

### Multivariate Cryptography

Based on multivariate polynomial equations, including both unimodular polynomials and others. The security of these systems is based on the difficulty of solving systems of multivariate polynomial equations, which is computationally difficult.

### Isogeny-Based Cryptography

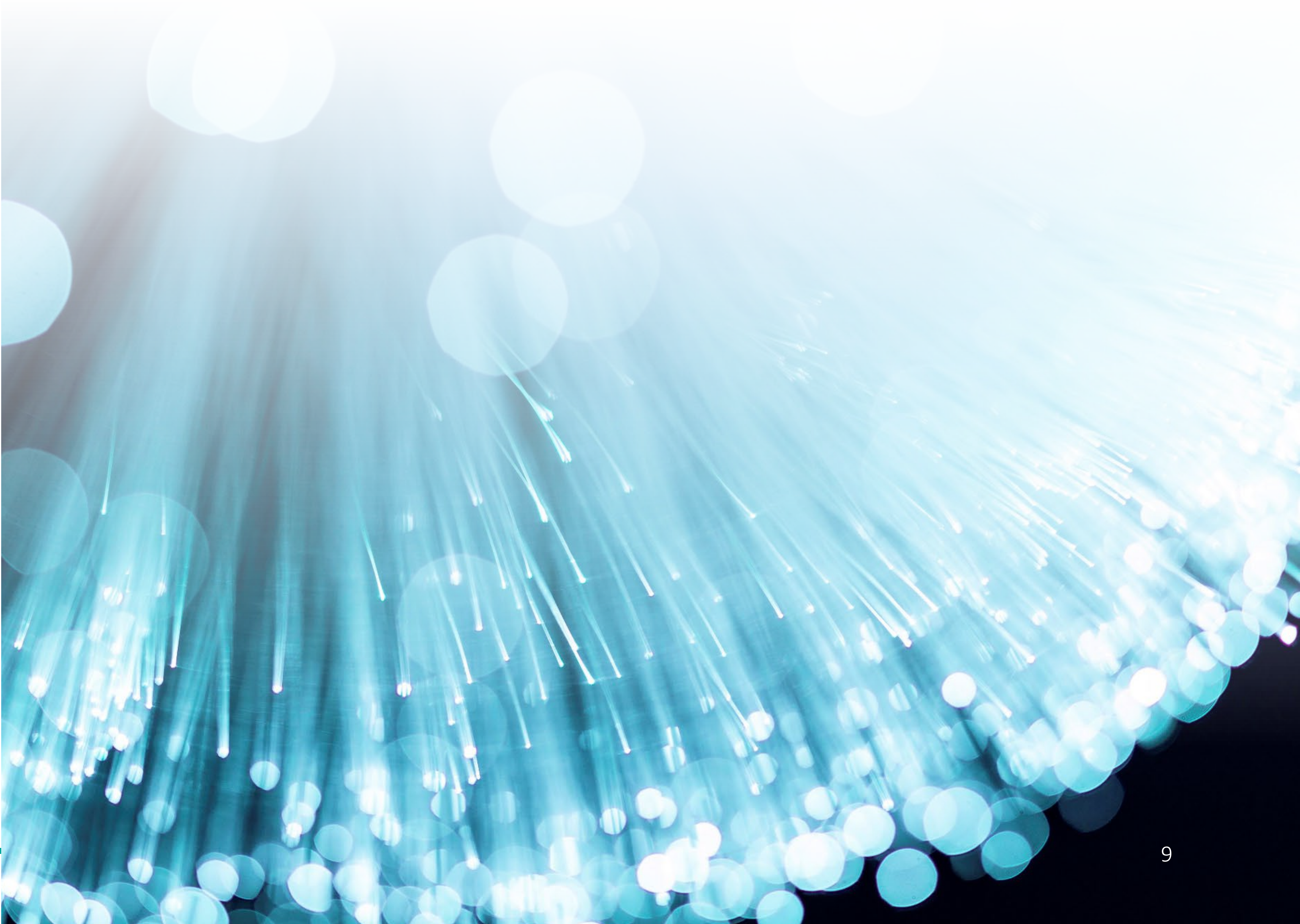
This type of cryptography is based on the supersingular isogeny problem, which involves the mapping between elliptic curves.

The National Institute of Standards and Technology (NIST), which has been studying such algorithms since 2015, is leading an international effort to standardize new post-quantum cryptographic algorithms to replace current public-key algorithms vulnerable to quantum computers. Experts estimate a 10-15% chance of a quantum computer being capable of breaking cryptography within the next 10-15 years. The United States government has set a goal for systems to be transitioned to quantum-resistant cryptography by 2035.

NIST released a list of candidate algorithms in July 2022. CRYSTALS-KYBER (key-establishment, FIPS 203: ML-KEM), CRYSTALS-Dilithium (digital signatures, FIPS 204: ML-DSA), FALCON (FIPS 205: SLH-DSA), and SPHINCS+ (FN-DSA) made it to the list due to their strong security and excellent performance.

CRYSTALS-KYBER is a key encapsulation method (KEM) used to establish a shared secret between two parties. Its application lies with in-transit encryption. It is part of the CRYSTALS (Cryptographic Suite for Algebraic Lattices) suite of algorithms.

A February 2024 presentation by NIST’s Dr. Dustin Moody titled “The First NIST PQC Standards” is available at https://www.youtube.com/watch?v=bU3ml8RXUEo



# Quantum Computers and Blockchain Systems

The advent of quantum computing presents potential threats to the security of many existing cryptographic systems. Notably, this is of immense concern for blockchain technology, which relies extensively on cryptographic primitives for its security. As we delve into PQC within the realm of blockchain, several research domains emerge, including post-quantum signature schemes, consensus mechanisms, and privacy-enhancing techniques.

Blockchain transactions are authenticated through digital signatures, enabling users to verify their transactions without a central authority's intervention. Nodes within the blockchain network verify these transactions by checking the match between the transaction signature and the public key tied to the sender's address. Quantum computers can exploit Shor's algorithm, which is an efficient quantum algorithm for factoring large numbers and solving the discrete logarithm problem, to unravel these schemes and extract the private key from the public key. This could permit an attacker to forge digital signatures and impersonate other users. Proposed post-quantum signature schemes such as hash-based, lattice-based, and code-based signature schemes offer varying security properties and trade-offs, warranting ongoing research to identify the most suitable strategies for blockchain systems.

Consensus mechanisms in blockchain technology ensure a collective agreement on the state of the blockchain across all network nodes, preventing double-spending and other potential attacks. Many consensus mechanisms, like proof of work and proof of stake, employ digital signatures and hash functions. As described above, digital signatures verify transactions and maintain their integrity, while hash functions interlink blocks in a chain (block-chain). A potential attacker with quantum capabilities could manipulate the consensus mechanism and modify the blockchain's state. Proposals for post-quantum consensus mechanisms include quantum-resistant versions of proof of work and proof of stake.

Certain privacy-enhancing techniques integral to blockchain systems, like zero-knowledge proofs and homomorphic encryption, are vulnerable to quantum attacks. Zero-knowledge proofs allow a party to prove the validity of a statement to another party without revealing any additional information. They ensure the validity of a transaction in blockchain systems without disclosing any data about the sender, recipient, or transaction amount. On the other hand, homomorphic encryption, a technique that enables computation on encrypted data without decryption, allows anonymous computations on the blockchain without revealing any underlying data. Both these methods are susceptible to quantum-based attacks using Grover's algorithm, which can expedite searching for solutions to certain cryptographic issues, such as finding pre-images of hash functions. Therefore, developing post-quantum privacy-enhancing techniques resilient to quantum attacks is critical to the continued privacy of blockchain systems.

Despite the concerns raised, it is important to be aware of the large computation gap that must close before real impact. A paper released in 2022 estimated that 1.9 billion qubits would be needed to penetrate a single Bitcoin private key within 10 minutes (block confirmation time). Qubits, or quantum bits, are the analog to "bits" in classical computing. By comparison, most proto-QC computers today can summon 50–100 qubits, though IBM's state-of-the-art Eagle quantum processor can manage 127 qubits. Yes, the computation gap is large but will close over time if blockchain systems do not evolve aggressively.

# Conclusion

As we approach a future where quantum computing may become widely available, the relevance and urgency of post-quantum cryptography cannot be overstated. Quantum computers' ability to solve specific problems faster than classical computers can potentially compromise many existing cryptographic systems. This threat is especially pertinent to blockchain technology, which heavily relies on cryptographic principles for its security and integrity.

Despite these challenges, opportunities arise for developing and refining post-quantum cryptographic methods, such as quantum-resistant digital signatures, consensus mechanisms, and privacy-enhancing techniques. As research progresses in this field, it becomes increasingly clear that securing blockchain systems and other cryptographic-dependent technologies in a potentially post-quantum world will necessitate the successful marriage of quantum computing understanding and cryptographic innovation. Further studies are needed to explore this intersection, but the progress made so far indicates promising avenues for ensuring our digital world's continued security and integrity.