frontiers | Frontiers in Computer Science

TYPE Original Research
PUBLISHED 21 May 2025
DOI 10.3389/fcomp.2025.1457000

OPEN ACCESS

EDITED BY
Dileep Kumar Yadav,
Bennett University, India

REVIEWED BY
Ramin Karim,
Luleå University of Technology, Sweden
Arijet Sarker,
Florida Polytechnic University, United States

*CORRESPONDENCE
Sultan Almuhammadi
✉ sultan@almuhammadi.com

RECEIVED 29 June 2024
ACCEPTED 16 April 2025
PUBLISHED 21 May 2025

CITATION
Almuhammadi S and Alghamdi S (2025) A novel transition protocol to post-quantum cryptocurrency blockchains.
Front. Comput. Sci. 7:1457000.
doi: 10.3389/fcomp.2025.1457000

A novel transition protocol to post-quantum cryptocurrency blockchains

Sultan Almuhammadi[1]* and Sarah Alghamdi[2]

[1]College of Computing and Mathematics, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia, [2]College of Engineering and Physics, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia

Blockchain-based public ledgers, known as cryptocurrencies, are used to build peer-to-peer digital payment systems. Cryptocurrency transactions are secured by digital signatures. However, today's public-key cryptography, which is the basis of digital signatures, is vulnerable to quantum attacks. Therefore, there is a significant risk to the 2.7 trillion dollar market capitalization of the cryptocurrency sector in the Quantum Era. In this paper, we review the current risk of quantum attacks on the blockchains of cryptocurrencies. We also discuss the migration of existing cryptocurrencies from classical to quantum-resistant blockchains and review some of the existing transition protocol algorithms. The main contribution of this work is to propose a new transition protocol algorithm that allows smooth and safe migration to post-quantum blockchains without delay. The proposed algorithm requires a soft fork of the original blockchain, which makes it more desirable than other hard-fork solutions. We also prove the soundness and completeness properties of the proposed algorithm and discuss its advantages compared to the existing ones. We conclude by highlighting our recommendations based on this study.

KEYWORDS

blockchain, cryptocurrency, digital signature, post-quantum cryptography, transition protocol

1 Introduction

Blockchain technology has been evolving rapidly in recent years. A blockchain has many features, including security, immutability, reliability, and privacy. It has been used in cryptocurrency and many other applications, such as information systems, supply chains, government services, military, and defense (Krichen et al., 2022). Blockchain technology is also used in secure smart systems (Rawat et al., 2020), applications of the decentralized Internet of Things, and healthcare (Alamri et al., 2022).

The security of blockchains depends on hash functions and public-key cryptographic schemes such as digital signatures. As quantum computing technology develops rapidly, quantum attacks pose significant risks to public-key cryptography and hash functions. The majority of cryptocurrencies in use today will soon be at serious risk when large-scale quantum computers become available. In November 2021, the market capitalization of the cryptocurrency industry exceeded $2.97 trillion dollars. The market capitalization of Bitcoin alone exceeded $1.45 trillion of the $2.78 trillion total market cap achieved on March 14, 2024 (Coinmarketcap, 2024). It should be mentioned that most of the cryptocurrency data used in this research is obtained from the CoinMarketCap website (Coinmarketcap, 2024), which is a highly reliable source of information on the current market of cryptocurrencies. We also use the cryptocurrencies white paper to provide technical details (Nakamoto, 2008; Hcash, 2024; Cellframe, 2024; Kevin and Yuan, 2024).

The security of the cryptocurrency and its blockchain depends on the security of the underlying cryptographic algorithms they are built on, such as hash functions and digital signatures. For instance, Bitcoin uses an elliptic-curve digital signature algorithm (ECDSA) and SHA-256 for hashing. In certain cryptocurrencies, extra features such as anonymity and untraceability are provided by the use of other cryptographic tools. However, elliptic curve cryptography is not a good candidate for long-term solutions based on the National Security Agency (NSA) plans for post-quantum transition published in 2015 [National Cryptographic Solutions Management Office (NCSMO), 2024]. NIST selected a number of post-quantum cryptographic schemes, like: Code-base, hash-based, supersingular elliptic curve isogeny-based, lattice-based, and multivariate to replace the current cryptographic schemes in the Quantum Era. The most well-known of them is the lattice-based digital signature. Although hash-based digital signatures are quantum-safe schemes, their performance limitations make them impractical. However, they can be used in blockchain applications with some modifications. For example, we may use a single path in implementing the eXtended Merkle Signature Scheme (XMSS) rather than the whole tree (Fernández-Carames and Fraga-Lamas, 2020).

In this work, we discuss the security of today's cryptocurrency against quantum attacks on hash functions and digital signatures, and review a number of solutions to secure blockchains against quantum attacks. Moreover, we discuss the migration from classical to post-quantum blockchains using secure transition protocols. We propose a new transition protocol algorithm to safely and smoothly migrate existing blockchains to quantum-resistant blockchains. We discuss the advantages of the proposed protocol and compare it with other transition protocols found in the literature.

The remainder of this paper is organized as follows. Section 2 gives a brief background on blockchain technology and discusses the security of cryptocurrency blockchains under quantum attacks. The migration from classical to quantum-resistant blockchains is discussed in Section 3, where the proposed transition protocol is explained. The results of this work are analyzed and further discussed in Section 4. Finally, the conclusion is given in Section 5 with recommendations and future work.

2 Background

Digital signatures are used for authenticating transactions in cryptocurrencies. Hash functions are also important for securely linking the blocks with each other in the blockchain. The recent development of quantum computers threatens both hash functions and public-key cryptography. Future quantum computers are capable of recovering sensitive transaction data, such as the private key in today's public-key cryptosystems to launch attacks on public-key cryptography. In public-key schemes, each user is assigned a pair of keys. Generally, the public key is used for encryption, while the private key is used for decryption. However, to securely sign a message, the private key is used in the digital signature scheme. The signature can later be verified publicly using the corresponding public key. When a user makes a transaction to spend a digital coin, the public key is used as the address of the payee's wallet, while the private key is used for payment authorization.

Most of today's cryptocurrencies use ECDSA for transaction authorization. The ECDSA is better than the RSA, as it uses a shorter key to achieve the same security level. For instance, a 2048-bit RSA signature has the same level of security as a 256-bit ECDSA signature (Barker et al., 2009). In addition to digital signatures, blockchain technology uses hash functions to securely link blocks to each other, which makes the blockchain immutable. In order to maintain the blockchain's immutability, hash functions are crucial. As shown in Figure 1, each block contains a hash value of the previous block. To add a new block (say Block $[i]$) to the blockchain, the previous block (Block $[i-1]$) is hashed, and the hash value of Block $[i-1]$ is stored in Block $[i]$. Furthermore, Block $[i-1]$ also contains a previous hash that stores the hash value of Block $[i-2]$, and so on. If any part of Block $[i-2]$ is modified, its hash value will change, and therefore the hash value stored in Block $[i-1]$ will no longer be valid and must be updated as well. Therefore, when several blocks are added after a given block, it would be extremely difficult to modify it without being detected. This makes the whole blockchain temper-evident.

2.1 Security of cryptocurrencies in the quantum era

Blockchains based on classical cryptographic algorithms like RSA and ECDSA are vulnerable to quantum attacks because these algorithms rely on mathematical problems–such as integer factorization and the discrete logarithm problem (DLP)–that can be efficiently solved using a quantum computer. Shor's factorization algorithm (Shor, 1994) can break RSA and ECDSA in polynomial time, rendering the cryptographic foundations of most existing blockchains insecure in the quantum era. This threatens the integrity of digital signatures used to authenticate transactions, potentially allowing attackers with quantum capabilities to forge signatures and compromise blockchain security.

The majority of blockchains used today are vulnerable to quantum attacks (Alghamdi and Almuhammadi, 2021). Quantum algorithms threaten blockchain security in two ways. First, quantum algorithms can break most digital signature schemes, such as ECDSA, that are used to authenticate transactions on the blockchain. In principle, it is mathematically proven that DLP can be solved using a polynomial reduction of the integer factorization problem, and hence it can be solved using Shor's algorithm. This makes both RSA and ECDSA digital signature schemes vulnerable to quantum attacks. However, this kind of attack can only take place in the future when a large-scale quantum computer is available (Alghamdi and Almuhammadi, 2021).

Second, the Grover algorithm (Grover, 1996) can be generalized to achieve quadratic speedup of the search for hash codes. This enables attackers equipped with quantum computers to successfully launch the 51% attack on the blockchain (Nakamoto, 2008). However, the effect of such algorithms on hash functions is quadratic. Therefore, we can resist quantum attacks on hash-based systems by doubling the sizes of their keys (Alghamdi and Almuhammadi, 2021).

The blockchains for the existing cryptocurrencies today can be classified into two groups: (1) blockchains vulnerable to quantum

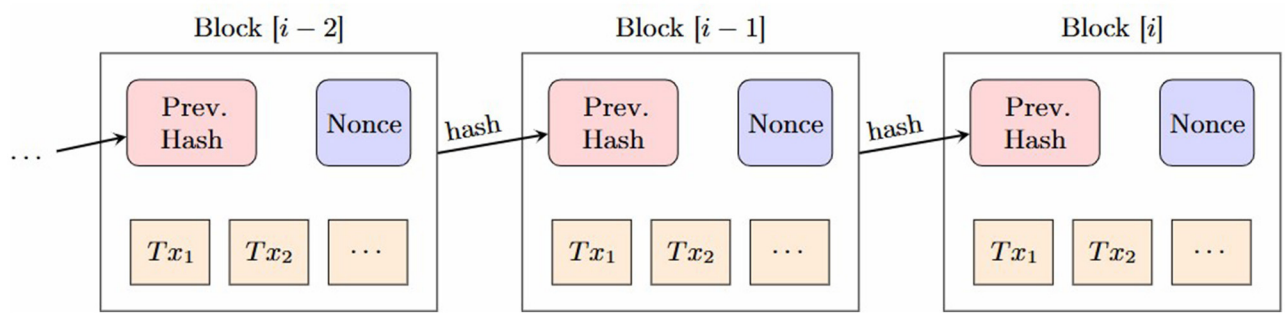

FIGURE 1
Hash links in a blockchain.

attacks, and (2) blockchains that are secure against quantum attacks. First, the blockchains that are vulnerable to quantum attacks include: Ethereum (ETH), Bitcoin (BTC), Tether (USDT), Binance (BNB), Solana (SOL), Litecoin (LTC), and Zcash (ZEC). Most of the blockchains in this group use ECDSA or similar DLP-based digital signatures, which a quantum computer can solve in polynomial time (Kearney and Perez-Delgado, 2021). In this group, several cryptocurrencies, including Beam, Grin, and Monero, employ various signature schemes to achieve additional features. However, they are all vulnerable to quantum attacks because they are all based on elliptic curve DLP. On the other hand, blockchains that can resist quantum attacks include: IOTA (MIOTA), Nexus (NXS), Cellframe (CELL), HyperCash (HC), Mochimo (MCM), and Quantum Resistant Ledger (QRL). These blockchains use lattice-based and hash-based digital signatures which are quantum-resistant.

2.2 Digital signatures used in blockchains

In Section 2.1 we present a number of cryptocurrencies that are vulnerable to quantum attacks and some quantum-safe cryptocurrencies. In this section, we review the digital signatures used in these cryptocurrencies and discuss their security against quantum attacks.

The ECDSA is based on the discrete logarithm problem on elliptic curves, which is tractable by quantum computers (Kearney and Perez-Delgado, 2021). This makes the ECDSA vulnerable to quantum attacks. The ECDSA is used in most of today's cryptocurrencies, such as: Ethereum, Bitcoin, Tether, Litecoin, Zcash, Beam, and Grin. A modified version of ECDSA, known as Edwards-Curve Digital Signature Algorithm (EdDSA) is also based on DLP. Hence, it is not quantum-safe. The EdDSA is used in Binance, Solana, and Monero.

The Ring Confidential Transactions (RingCT) is a digital signature scheme for obfuscating the public ledger and making the transaction untraceable. It hides both the amount sent and the sender's public key. In this scheme, Any peers can broadcast or send transactions, and it is impossible for an outside observer to determine who sent them. This scheme is used in Monero, Beam, and Grin to make the transaction untraceable. It is worth mentioning that Monero, Beam, and Grin are vulnerable to quantum attacks since they are built on EdDSA and RingCT signatures.

WOTS is a hash-based digital signature used in IOTA to secure transactions. Since there is no known quantum algorithm that can break hash-based digital signatures in polynomial time, it is considered to be quantum-safe. Grover's algorithm, on the other hand, speeds up the search space for the hash-based signature, implying a halving of the security level. In the future, a longer key might be employed to reduce the probability of 51% attacks employing quantum computers (Alghamdi and Almuhammadi, 2021). Another variant of WOTS known as WOTS+ is used in Quantum Resistant Ledger and Mochimo to provide extra security features such as transaction mirroring and three-way handshaking. CURL-P is a new hash-based digital signature to be used in IOTA in the future. It uses the new hash function called CURL-P, which employs ternary hardware instead of binary. The ternary hardware will give IOTA additional security to resist quantum attacks.

The XMSS is a hash-based signature scheme, which makes it secure against quantum attacks. It is used to establish an extendable stateful asymmetrical hypertree signature methodology for Quantum Resistant Ledger (QRL), A modified version of this scheme, known as XMSS+, is used in Mochimo to provide extra security like the WOTS+ digital signature. The Signature Chains scheme incorporates many quantum-safe cryptographic schemes to achieve high security against quantum attacks. It is used in Nexus blockchain to provide extra security to the system. Ring Learning with Errors (Ring LWE) is a lattice based signature. There is no known quantum algorithm that solves lattice computational problems in polynomial time (Torres et al., 2018). Therefore, the Ring LWE digital signature provides high security against quantum attacks. It is used in HyperCash (HC) blockchain (Hcash, 2024).

The multi-signatures scheme is proposed to be used in Cellframe and the new Ethereum 3.0 to provide security against quantum attacks (Cellframe, 2024; Kevin and Yuan, 2024). A 2-byte ID is introduced in Cellframe to support up to $2^{16} = 65{,}536$ digital signature algorithms, among which a lattice-based digital signature known as Crystal-Dilithium is selected by default. In addition, a user can use multi-algorithm signatures with more than one key to secure all of the deposits in the wallet Cellframe (2024).

Table 1 summarizes the signatures used in today's most popular cryptocurrencies. It also indicates whether the cryptocurrency is quantum-safe or not based on the digital signature it uses. If

TABLE 1 Digital signatures proposed for cryptocurrencies.

Signature	Cryptocurrencies	Quantum-safe?
ECDSA	Ethereum, Bitcoin, Tether, Zcash, Litecoin, Beam, Grin	No
EdDSA	Binance, Solana, Monero	No
RingCT	Monero, Beam, Grin	No
WOTS	IOTA	Yes
WOTS+	Q. R. Ledger, Mochimo	Yes
CURL-P	IOTA (Future Plan)	Yes
XMSS	Quantum Resistant Ledger	Yes
XMSS+	Mochimo	Yes
Signature Chains	Nexus	Yes
Ring LWE	HyperCash	Yes
Crystal-Dilithium	Cellframe	Yes
Multi-Signature	Cellframe, Ethereum 3.0	Yes

the signature is based on DLP, such as ECDSA, EdDSA, and RingCT, then the cryptocurrency is not quantum-safe. Otherwise, if the signature is based on lattices or hash code, such as WOTS, CURL-P, LWE, Dilithium, and XMSS, then the cryptocurrency is quantum safe.

3 Migration to post-quantum blockchains

A number of post-quantum digital signatures are proposed in Section 2.2 as solutions for quantum-safe blockchains. Once a solution is implemented for a cryptocurrency blockchain, it should include a grace period for the peers to migrate their digital assets from the classical blockchain to the post-quantum blockchain. A transition protocol for each cryptocurrency blockchain should be put in place that guarantees a safe and smooth transition of assets to the new post-quantum blockchains. In this section, we discuss how to migrate quantum-vulnerable cryptocurrencies, such as Bitcoin and Ethereum, from classical to post-quantum blockchain. First, we present existing migration protocols in Section 3.1. Then in Section 3.2 we proposed a new transition protocol that is more practical and secure.

3.1 Existing transition protocols

Stewart et al. (2018) proposed a transition protocol based on a commit-delay-reveal scheme. This scheme has three steps. First, the user marks the commitment of the unspent coins using the public and secret key pair (pk, sk). This commitment is broadcast by creating a special commitment transaction $T_c(pk, pk_{QR})$. T_c contains a hash value of both pk and the quantum-resistant public key pk_{QR} generated by the user. It is worth noting that the user needs quantum-resistant coins to fund the transaction (T_c) in order to publish it. The second step is the delay after publishing the hash commitment. In this step, the user leaves the coins in the commitment untouched for a sufficiently long period of time to ensure the security of the scheme. The duration of the delay depends on many factors, but the authors suggested an initial period of six months subjected to follow-up and further discussion. The third step is the reveal after the security delay. In this step, the user safely reveals the public keys pk and pk_{QR} and claims ownership of the coins in the commitment. This is done by creating a reveal transaction $T_c(sk_{QR})$ signed by the user quantum-resistant secret key, in which the (pk, pk_{QR}) is revealed.

The protocol proposed by Stewart et al. works even if the digital signature is compromised. The authors suggested a soft fork of the Bitcoin blockchain to implement their proposed protocol. The proposed is safe but slow due to the delay in the underlying commit-delay-reveal scheme. This scheme requires waiting for a period of time after the commitment is made, then it reveals the proof of the ownership of assets. This makes the protocol slow and impractical since it requires the possession of quantum-resistant coins to fund the commitment transaction.

Anhao (2018) presented a transition protocol for Bitcoin Post-Quantum (BPQ) that does not depend on commit-delay-scheme, but it requires a hard fork instead of a soft fork of the Bitcoin blockchain. In this protocol, only transactions with ECDSA signatures are allowed in Bitcoin as part of the current consensus before the block height of 555,000. Meanwhile, Bitcoin nodes will reject blocks containing transactions signed by XMSS. The proposed post-quantum consensus in Bitcoin works as follows. The rules of the network are mainly identical to the Bitcoin network before the block height of 555,000. In view of this block, the new rules will be in effect. Based on these rules, the support of quantum-safe XMSS signatures is introduced, and the size of the block is increased. Besides, the mining algorithm is also modified to accommodate these changes.

At the hard fork time, the owners of Bitcoins automatically receive a similar number of coins in the BPQ blockchain. It is worth mentioning that new keys of XMSS are required to be created as well as the transaction from the old addresses of the owners to the new addresses in order to prevent the hacking of their coins with the help of quantum computers. It is to be noted that old-type address transactions are yet to be supported by standard software. Nevertheless, such transactions could be manually created and validated by the network. However, their outputs cannot be spent via ECDSA. In fact, the support for old elliptic curve digital signatures will be completely disabled within a year of launching the main BPQ network. Moreover, there is no transaction malleability problem in BPQ, and it is ready for the Lightning Network (Anhao, 2018).

3.2 The proposed transition protocol algorithm

Transition protocols are done using either a soft or a hard fork of the blockchains. Both hard forks and soft forks are similar in the sense that when an existing code of a cryptocurrency is updated, the old version remains on the network while the new version is created. With a hard fork, both the new and the old

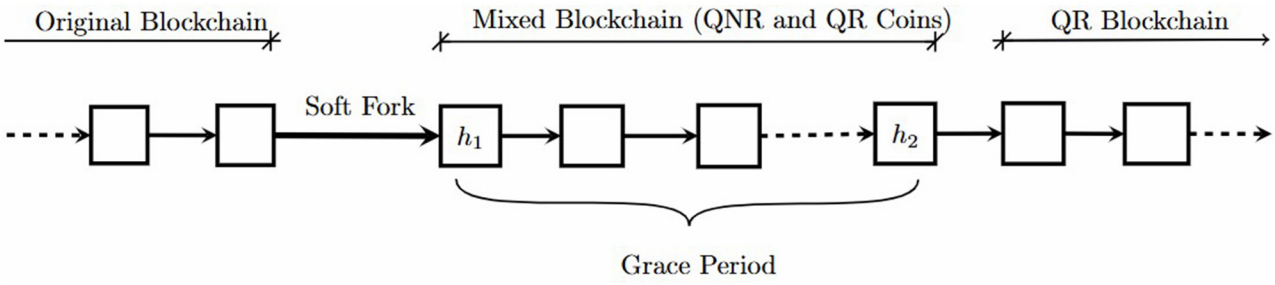

FIGURE 2
The proposed transition protocol.

blockchains coexist at the same time. While in a soft fork, only the new blockchain will remain valid after the update.

The existing transition protocol by Stewart et al. presented in Section 3.1 is based on a commit-delay-scheme using a soft fork of the Bitcoin blockchain. This requires a waiting time (delay) after commitment to ensure the security of the protocol. The delay should be long enough (like 6 months as suggested by the authors) to ensure the security of the systems by all peers before they verify the proof of ownership of assets. During this delay period, the user cannot use the committed coins in anything until the reveal step. This delay is considered the major drawback of this protocol. Moreover, the protocol requires the possession of quantum-resistant coins to fund the committing transaction.

On the other hand, the transition protocol presented by Anhao (2018) does not have a waiting time (delay). However, it requires a hard fork of the Bitcoin blockchain. This means that we will end up having two blockchains running in parallel. The challenge will be to convince the majority of the peers to join the new blockchain. Peers might decline and stay in the old chain, or join both chains to virtually double their assets. This will have undesired effects on the value of Bitcoin in the future.

In this work, we propose a soft fork solution without delay. The soft fork yields a single blockchain and all the peers have to stay on it. Removing the commit-delay scheme will allow the peers to continue processing the transaction without interruption, which makes the proposed transition protocol smooth and secure. The proposed transition protocol can be used with any post-quantum digital signature, and it does not require any waiting time for the hard fork process. We refer to coins that are generated by transactions done before the soft fork in the original blockchain as quantum-non-resistant (QNR) coins. While the coins generated after the soft fork are called quantum-resistant (QR) coins.

Initially, the original blockchain contains only QNR coins. When the soft fork process starts at block height h_1, the blockchain becomes a mixed blockchain that accepts both QNR and QR coins as an input, but only outputs QR coins in any transaction. The mixed blockchain allows a grace period for all peers to either spend their coins or convert them to the quantum-resistant version (QR coins). At the end of the grace period (block height h_2), the blockchain becomes totally quantum-resistant and only accepts QR coins as an input. Figure 2 illustrates the grace period in the proposed transaction protocol.

Thus, transactions done during the grace period may accept both QR and QNR coins as input, and only generate QR coins as output. While transactions done after the grace period should only accept QR coins as input and generate QR output. Algorithm 1 outlines the new rules of the proposed transition protocol. All other rules of the blockchain remain identical to the ones before the soft fork at block h_1.

We suggest that the grace period should last at least two years to allow the peers enough time to spend their coins or convert them to new quantum-resistant coins by paying the coins to themselves in normal transactions. The grace period is also utilized to fix errors or address any critical issue that might appear in the migration process from the classical to the quantum-resistant blockchain. Moreover, coins that are not spent or converted to the QR version during the grace period are neither protected nor supported by the blockchain any longer. Therefore, they can be burned and the mining award is increased accordingly to maintain the total supply of the coin, such as a 21 million cap in the case of Bitcoin.

In order for the transition protocol to make sense, we assume that no quantum attack is possible before or during the grace period. This implies that the QNR coins are safe to use before the end of the grace period. The QNR coins are considered *legitimate* if the user holds the corresponding private key in the digital signature scheme and can successfully sign the transaction. We also assume that the QR coins as secure against quantum attacks and, therefore, they are considered *legitimate* all the time if the user holds the corresponding private key of the coin in the quantum-resistant digital signature scheme. Moreover, we assume that all accessible QNR coins are used or converted to QR coins during the grace period. If a QNR coin is not used or converted to a QR coin during the grace period, it is assumed to be inaccessible and will be counted as burned or expired and no longer legitimate in the blockchain. Therefore, the expiration date of all QNR coins is set to be the expected date of h_2, and it should be announced to all peers when the transaction protocol is started.

3.3 Examples

In this section, we give three examples on Bitcoin blockchain to clarify the proposed transition protocol. The first two examples show transactions occurring during the grace period, while the

Data: B : current blockchain,
b : current block (height, transaction list),
h_1 : block height to begin the fork,
h_2 : height of the last block in the grace period.
Result: Add b to the blockchain if *valid*.
for all $Tx \in b$ **do**:
if $height(b) < h_1$ **then**
  if *all Tx.input are QNR and not spent* **then**
    Mark Tx as *valid*
  else
    Mark Tx as *invalid*
  end
else
  if $height(b) \leq h_2$ **then**
    if *all Tx.input are QR or QNR and not spent* **then**
      Mark Tx as *valid*
    else
      Mark Tx as *invalid*
    end
  else
    if *all Tx.input are QR and not spent* **then**
      Mark Tx as *valid*
    else
      Mark Tx as *invalid*
    end
  end
end
end-for
if *all* $Tx \in b$ *are valid* **then**
  Add b to B
else
  Reject b
end

Algorithm 1. Transition Protocol

third example shows transactions occurring after the grace period. All transactions occurring before the grace period are treated normally as in the original blockchain. As discussed in Section 4.2, the recommended block height to begin the fork for the Bitcoin blockchain is $h_1 = 945{,}000$ which marks the beginning of the grace period. While the recommended height of the last block in the grace period is $h_2 = 1{,}155{,}000$ which gives a four-year grace period.

3.3.1 Example 1

Suppose Alice has BTC 0.9 in three QNR coins of BTC 0.3 each. She obtained these coins in the original blockchain before the fork, which means Alice holds their private keys in ECDSA. Then, after the fork, she wants to pay BTC 0.8 to Bob during the grace period. Figure 3 illustrates this transaction. Since this happens during the grace period, the height of the block (b) that contains this transaction should be between h_1 and h_2, say $height(b) = 945{,}001$. According to Algorithm 1, since $h_1 \leq height(b) \leq h_2$, the system

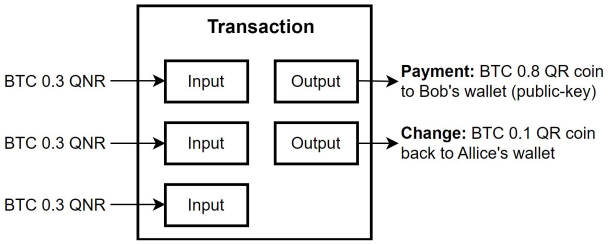

FIGURE 3
Alice pays BTC 0.8 to Bob in Example 1.

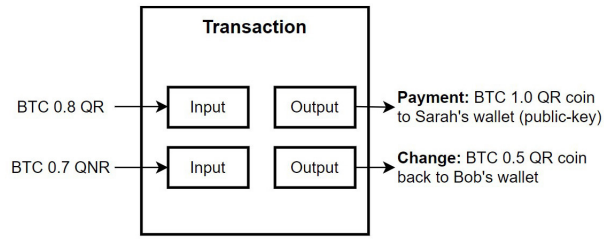

FIGURE 4
Bob pays BTC 1.0 to Sarah in Example 2.

first checks if these three coins are not spent and they are either QR or QNR in order to validate the transaction, and then generates two QR coins. The first coin is for the payment in the amount of BTC 0.8 sent to Bob's wallet (public key generated in the QR system). While the second coin is the change in the amount of BTC 0.1 sent back to Alice's wallet as shown in Figure 3. The algorithm will add the block b to the blockchain after confirming the validity of all transactions in b.

3.3.2 Example 2

Suppose Bob later wants to pay BTC 1.0 to Sarah during the grace period in a transaction included in a block of height 950,008. He uses the BTC 0.8 QR coin received from Alice in addition to a BCT 0.7 QNR coin he already has. Since this transaction occurs during the grace period, the system will accept a mix of QR and QNR coins in one transaction and create two QR coins for the payment and the change as shown in Figure 4.

3.3.3 Example 3

Suppose Sarah wants to pay BTC 1.5 to Alice after the grace period using the BTC 1.0 QR coin from Bob in Example 2 plus BTC 0.6 in two QR coins she has obtained recently. Since this transaction occurs after the grace period, the current block height will be greater than h_2, say $height(b) = 1{,}155{,}001$. Therefore, the algorithm checks that all the input coins in this transaction are QR in order to accept the transaction, and creates two QR coins for the payment and the change as illustrated in Figure 5. Then, the algorithm will add the block containing this transaction to the blockchain after confirming the validity of all other transactions.

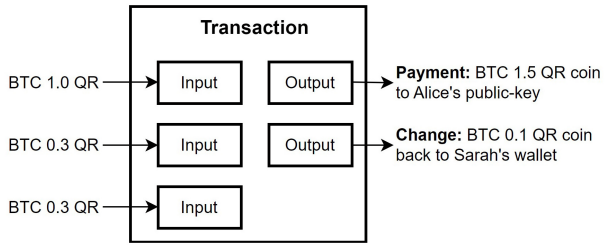

FIGURE 5
Sarah pays BTC 1.5 to Alice in Example 3.

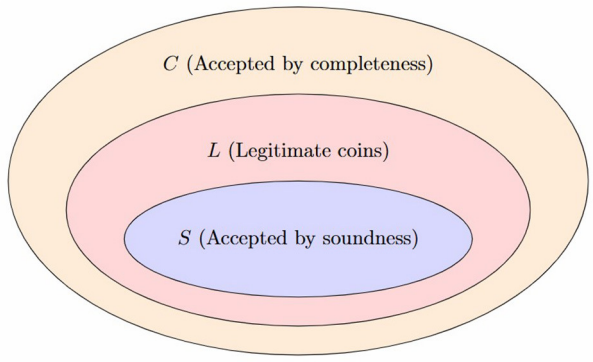

FIGURE 6
Coins accepted due to soundness and completeness properties.

On the other hand, if a user has a BTC 0.5 QNR coin obtained in the original blockchain, and wants to spend it after the grace period, the algorithm will reject this coin and mark the transaction as *invalid*. Only QR coins are accepted if $height(b) > h_2$. Any block containing transactions using QNR coins will be rejected. Consequently, the user can no longer use the BTC 0.5 QNR coin. This coin is assumed to be burned permanently at this point. Therefore, there is a risk of losses to valid users who do not convert their coins to the new QR coins during the grace period when the cryptocurrency migrates to the post-Quantum Blockchain.

3.4 Soundness and completeness properties

In this section, we discuss the soundness and completeness properties of the proposed transition protocol given in Algorithm 1. In general, we say an algorithm is sound if it returns an output, that output is correct. notice that a sound algorithm may not give an output in some cases. On the other hand, We say an algorithm is complete if it always returns an output that is most likely correct but it could be bogus sometime.

The terms soundness and completeness are well defined in the context of computational theory, where computing problems are represented as languages. A language is a set of strings on some alphabet. An algorithm is a function that determines whether a given string x belongs to some language or not by returning true or false respectively.

Definition. Let L be a language on some alphabet Σ, and Σ^* be the set of all strings on Σ. Thus, $L \subseteq \Sigma^*$. Then, the soundness and completeness properties can be formally defined as follows.

Soundness Property: An algorithm A is said to be *sound* if

$$\forall x \in \Sigma^*, A(x, L) = True \longrightarrow x \in L$$

Completeness Property: An algorithm A is said to be *complete* if

$$\forall x \in \Sigma^*, x \in L \longrightarrow A(x, L) = True$$

In the context of transition protocol algorithms, the soundness property means that if the algorithm accepts a coin in any transaction, then this coin is legitimate. The completeness property of the algorithm means that if a user has legitimate coins, then the algorithm will accept them in any transaction that is made with only legitimate coins. In other words, suppose that L is the set of all legitimate coins. Then a sound algorithm accepts a subset S of L. While a complete algorithm accepts a superset C of L. Thus, $S \subseteq L \subseteq C$ as illustrated in Figure 6. We want to show next that Algorithm 1 is sound and complete. Thus, the proposed algorithm accepts the whole set of legitimate coins (by completeness property) and nothing else (by soundness property). Notice that if both legitimate and illegitimate coins are used in a single transaction, then the algorithm should not accept the transaction. This does not violate the completeness property since not all coins in the transaction are legitimate.

3.4.1 Proof of soundness property

Suppose Alice spent a coin c_1 in transaction Tx_1 and the algorithm accepted it in block b_i. Then, we have two cases:

Case 1: $height(b_i) \leq h_2$, which means that the transaction Tx_1 is done before the end of the grace period. This implies that all coins used in Tx_1 are either QR or QNR. If c_1 is a QR coin, then it is produced by the new algorithm with a quantum-safe digital signature, Which implies that $c_1 \in L$. If c_1 is a QNR coin, then it is safe to be used under the assumption of no potential quantum attacks can accur before or during the grace period, which also implies that $c_1 \in L$.

Case 2: $height(b_i) > h_2$, which means that the transaction Tx_1 is done after the grace period. Therefore, c_1 must be a QNR coin. Hence, it is produced by the new algorithm with a quantum-safe digital signature and it is safe to use it even if a large scale quantum computer exists, which implies $c_1 \in L$.

Therefore, if Algorithm 1 accepts c_1 in any a transaction, whether it occurs before, after, or during the grace period, then c_1 is a legitimate coin.

TABLE 2 Top cryptocurrency market cap and their signatures.

Cryptocurrency	Market cap	Signature
Bitcoin (BTC)	1,450 B	(ECDSA)
Ethereum (ETH)	482 B	(ECDSA)
Tether (USDT)	103 B	(ECDSA)
Binance (BNB)	94 B	(EdDSA)
Solana (SOL)	76 B	(EdDSA)
Others	575 B	–
Total market cap	2,780 B	–

TABLE 3 Top 5 quantum-safe cryptocurrencies.

Cryptocurrency	Market cap (million dollars)			
	2020	2021	2022	2023
IOTA (MIOTA)	1110.00	2564.09	786.86	409.19
Q. R. Ledger (QRL)	10.00	18.43	10.98	15.87
Cellframe (CELL)	0.00	19.66	9.22	7.11
Nexus (NXS)	17.57	38.36	3.68	3.28
HyperCash (HC)	75.80	33.74	5.23	2.46
Sum	1213.37	2676.45	816.65	437.91
Total Market Cap	367683	1647360	1028450	1062027
Percentage	0.330%	0.162%	0.079%	0.041%

3.4.2 Proof of completeness property

Suppose Alice has a legitimate coin c_2 and wants to spend it in some transaction, say Tx_2, to be added in block b_j. Then, we have three cases:

Case 1: Suppose Alice wants to spend the coin c_2 before the grace period. Then, c_2 must be a QNR coin since all coins are QNR in the original blockchain. Hence, Tx_2 is added to block b_j with $height(b_j) < h_1$. Therefore, the algorithm will mark Tx_2 as a *valid* transaction and accepts c_2.

Case 2: If she wants to spend it during the grace period, then c_2 can be either QNR or QR. Since $h_1 < height(b_j) \leq h_2$ in this case, the algorithm will mark Tx_2 as a *valid* transaction and accept c_2.

Case 3: If she wants to spend it after the grace period, then c_2 must be a QR coin since all QNR coins are burned and no longer legitimate at this point. Hence, the algorithm accepts c_2 and marks Tx_2 as *valid* accordingly.

Therefore, all legitimate coins are accepted by Algorithm 1 in any transaction occurring before, during, or after the grace period.

4 Discussion

By analyzing the market capitalization of the cryptocurrencies (Coinmarketcap, 2024), we found that about 79% of the total market cap (2.2 trillion dollars) is in the top five cryptocurrencies as shown in Table 2. Bitcoin and Ethereum have been always at the top of the list. While Tether, Binance, and Solana came next as of 2024. All of these cryptocurrencies use elliptic-curve digital signatures, which are vulnerable to quantum attacks.

4.1 Amount of cryptocurrency protected against quantum attacks

By analyzing the quantum-safe digital signatures presented in Section 2.2, Table 3 shows the market capitalization (in millions of dollars) of the top five quantum-safe cryptocurrencies as of August 20, 2023 (Coinmarketcap, 2024). We analyze the market cap of these cryptocurrencies in the last four years.[1] Other quantum-safe cryptocurrencies do exist but they have negligible market capitalization compared to the ones listed here and can be ignored in this analysis. Table 3 also shows the percentage of the protected amounts in each year. We note that the percentage of the protected amounts dropped from 0.330% in 2020 to 0.162% in 2021, then to 0.079% in 2022, and finally to 0.041% in 2023. This implies that the cryptocurrency industry is not taking the quantum threat seriously. Thus, the risk of quantum attacks on cryptocurrencies has been growing during the last four years. Moreover, there are many newly created cryptocurrencies that are not built on quantum-safe blockchains despite the existence of post-quantum digital signatures (Alghamdi and Almuhammadi, 2021).

4.2 Transition protocol parameters analysis

The proposed transition protocol in Section 3.2 has a number of parameters left as input. In this section, we discuss these parameters to make appropriate recommendations on the setup of this protocol. First, according to Alghamdi and Almuhammadi (2021), quantum attacks might be possible in the year 2033. Expectations of other researchers in Aggarwal et al. (2017) and Mosca (2018) are not far from this. We introduce a buffer zone of three years to ensure that we are on the safe side since we may safely assume that there will be no serious quantum attack on blockchains sooner than the year 2030.

The recommended duration for the grace period depends on many factors related to the cryptocurrency in question, like the block time, block reward, maximum supply, etc. For Bitcoin, for example, we recommend a four-year grace period after launching the soft fork by our proposed transition protocol. This is long enough to allow all peers to migrate to the new post-quantum blockchain. The justification for the four-year grace period is based on the history of Bitcoin when Satoshi Nakamoto stayed four years in the Bitcoin community to maintain the system and address any issues that appeared in Bitcoin's early days. The four year grace period gives the developer enough time to solve any problems that may appear while migrating from the classical to the post-quantum blockchain. During this grace period, there could be more than one soft fork or restart of the transition protocol to accommodate different updates. However, the grace period should just start and end once. In addition, the grace period of four years is long enough

1 The readings were taken on 8/20/2020, 8/22/2021, 8/20/2022, and 8/20/2023 (Coinmarketcap, 2024).

TABLE 4 Comparison between existing and proposed transition protocols.

Protocols	(Stewart et al., 2018)	(Anhao, 2018)	Proposed
Fork Type	Soft fork	Hard fork	Soft fork
Delay in transition	Yes	No	No
Blockchain splitting risk	No	Yes (two chains run in parallel)	No
Ease of adoption	Complex (requires commitment transactions)	Difficult (requires consensus on a hard fork)	Easy (grace period allows smooth transition)
Security	High, but slow due to delay	High, but risk of adoption split	High, with seamless transition
Grace Period	No	No	Yes
Need of initial quantum-safe coints	Yes (for commitment transactions)	No	No
Transaction continuity	Paused during commitment phase	Immediate, but requires new keys	Continuous and uninterrupted

to allow all peers to migrate to the new post-quantum blockchain and minimize the loss of assets.

In the following, Bitcoin is considered as an example for analysis. However, these parameters can be easily calculated for other cryptocurrency blockchains. Based on the above discussion, the following parameter settings are recommended for Algorithm 1 in the case that it is applied to Bitcoin.

- The soft fork should start at the block height $h_1 = 945{,}000$ in the Bitcoin blockchain (expected on April 26, 2026). This is the first block number in the mixed blockchain. However, since this is the first block in the mixed blockchain, it will only have to take QNR coins as input and generate QR coins. Later blocks will have both QNR and QR coins as input and only generate QR coins as output.
- At the end of the grace period, the blockchain will be purely quantum-resistant and will accept only QR coins. All unspent QNR coins should be permanently burned, and their values should be returned to the maximum circulation supply of 21 million BTC. This will increase the mining reward in the next half-cycle. In case of Bitcoin, the mining reward is halved every 210,000 blocks (approximately 4 years). Since a four-year grace period is recommended for Bitcoin, the grace period will end at block height $h_2 = h_1 + 210000 = 1{,}155{,}000$ which is expected to occur on April 26, 2030. We suggest that the mining reward is increased by the value of the burned coins with the next halving cycle, which is expected in 2032 at block height 1,260,000. At this point, more than 99% Bitcoin will have been mined and any increase in the reward will be greatly appreciated by the miners.

4.3 Advantages of adopting the proposed transition protocol

The proposed soft fork transition ensures seamless migration to quantum-resistant blockchains without network disruption. Unlike Stewart's protocol, it eliminates delays while avoiding blockchain splits, a risk in Anhao's hard fork approach. Transactions remain uninterrupted during the grace period, allowing gradual adoption. Table 4 highlights the differences between the existing and the proposed protocols.

The proposed transition protocol has the following features:

1. No Transition Delay: Unlike Stewart's protocol, which requires a commit-delay-reveal process, our protocol allows an immediate transition without any waiting period.
2. Avoids Blockchain Splitting: Unlike Anhao's protocol, which results in two chains running in parallel, our protocol ensures that all users remain on the same chain.
3. Simple Adoption: The proposed protocol uses a grace period, where users can transition at their own pace, making it easier to implement.
4. Higher Security Without Complexity: Unlike Stewart's protocol, which requires initial possession of quantum-resistant coins for transactions, our protocol enables a direct transition without special prerequisites.
5. Ensures Continuity: The protocol ensures that transactions remain uninterrupted during migration, making it more practical than the existing approaches.

Moreover, the performance of the proposed transition protocol is highly effective and resilient. It maintains network stability, requires minimal computational overhead, and prevents inflation by burning unspent QNR coins post-transition. It offers high security, efficiency, and flexibility, making it an optimal solution for quantum-safe blockchain migration.

5 Conclusion

Although blockchains are secure with today's cryptographic tools, like hash functions and digital signatures, they are basically vulnerable to quantum attacks. Quantum algorithms are capable of breaking the underlying cryptographic schemes used to secure today's blockchains. Some of today's cryptocurrencies use quantum-safe digital signatures, such as hash-based and lattice-based digital signatures. Therefore, they are expected to resist quantum attacks provided that their cryptographic schemes remain secure against quantum attacks. However, our study shows that the market capitalization percentage of these quantum-safe cryptocurrencies is very small in the last four years. It dropped from 0.330% in 2020 to 0.041% in 2023, leaving over 99.95% of the total market capitalization at risk.

As a result of this study, we summarize our recommendations as follows:

1. There is a notable growing risk of quantum attacks on today's cryptocurrencies' blockchains despite the availability of quantum-safe digital signatures.
2. The migration to post-quantum blockchains should start as soon as possible to have a long enough grace period and a buffer zone before any potential quantum attack.
3. The cryptocurrency industry is urged to use the proposed transition protocol, which guarantees safe and smooth migration to post-quantum blockchains by applying a soft fork to the original blockchain.
4. The recommended duration of the grace period in the proposed protocol should be at least two years to give enough time for peers to migrate to the post-quantum blockchain. This can be easily implemented as tool that pays all coins in a wallet to a newly created Quantum-resistant address within the same wallet. Once the tool is executed, the proposed transition protocol will convert all the coins in the wallet to QR coins and sent them to the newly created address.
5. We recommend that the migration of Bitcoin to the post-quantum blockchain has to be done by 2026. This allows a four-year grace period and a three-year buffer zone before potential quantum attacks.
6. It is worth noting that the expected year of potential quantum attacks and the corresponding buffer zone are just estimates according to what we may observe today. Thus, these parameters should be closely monitored and updated based on the advances achieved in the field of quantum computing.

Regarding future work, we suggest applying the post-quantum digital signatures to other applications that are built on blockchains. Examples include supply chain management, smart contracts, healthcare, and Internet-of-Things. The proposed transition protocol can also be used in these applications with minor modifications, such as the duration of the grace period and the type of signature schemes.

Data availability statement

Requests to access the datasets should be directed to the corresponding author: sultan@almuhammadi.com.

Author contributions

SAlm: Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Supervision, Visualization, Writing – original draft, Writing – review & editing. SAlg: Data curation, Investigation, Software, Validation, Writing – original draft, Writing – review & editing.

Funding

The author(s) declare that financial support was received for the research and/or publication of this article. The research is supported by King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia.

Acknowledgments

The authors would like to thank King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia, for supporting this research.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., and Tomamichel, M. (2017). Quantum attacks on bitcoin, and how to protect against them. arXiv [preprint] arXiv:1710.10377. doi: 10.5195/ledger.2018.127

Alamri, B., Crowley, K., and Richardson, I. (2022). Cybersecurity risk management framework for blockchain identity management systems in health iot. Sensors 23:218. doi: 10.3390/s23010218

Alghamdi, S. and Almuhammadi, S. (2021). "The future of cryptocurrency blockchains in the quantum era," in 2021 IEEE International Conference on Blockchain (Blockchain), 544–551.

Anhao, N. (2018). Bitcoin Post-Quantum.

Barker, E., Burr, W., Jones, A., Polk, T., Rose, S., Smid, M., et al. (2009). Recommendation for key management part 3: application-specific key management guidance. NIST Special Public. 800:57. doi: 10.6028/NIST.SP.800-57p3

Cellframe (2024). Cellframe: Service oriented blockchain network, whitepaper ver 2.0 beta. Available online at: https://cellframe.net/white-paper/ (accessed 14 March, 2024).

Coinmarketcap (2024). Coinmarketcap: Cryptocurrency prices, charts and market capitalization. Available online at: https://coinmarketcap.com/ (accessed 14 March, 2024).

Fernández-Carames, T. M. and Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE Access 8, 21091–21116. doi: 10.1109/ACCESS.2020.2968985

Grover, L. K. (1996). "A fast quantum mechanical algorithm for database search," in Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, 212–219.

Hcash (2024). Hcash: The new standard of value, whitepaper v.0.8.5. Available online at: https://h.cash/themes/en/images/Hcash+Whitepaper+V0.8.5.pdf (accessed 14 March, 2024).

Kearney, J. J. and Perez-Delgado, C. A. (2021). Vulnerability of blockchain technologies to quantum attacks. Array 10:100065. doi: 10.1016/j.array.2021.100065

Kevin and Yuan (2024). What Does Ethereum 3.0 Look Like? Available online at: https://hackernoon.com/what-does-ethereum-30-look-like-yr1134eu (accessed 14 March, 2024).

Krichen, M., Ammi, M., Mihoub, A., and Almutiq, M. (2022). Blockchain for modern applications: a survey. Sensors 22:5274. doi: 10.3390/s22145274

Mosca, M. (2018). Cybersecurity in an era with quantum computers: will we be ready? IEEE Secur. Privacy 16, 38–41. doi: 10.1109/MSP.2018.3761723

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Available online at: https://bitcoin.org/bitcoin.pdf (accessed 14 March, 2024).

National Cryptographic Solutions Management Office (NCSMO) (2024). Cryptography Today. Available online at: https://www.nsa.gov/ (accessed 14 March, 2024).

Rawat, D. B., Chaudhary, V., and Doku, R. (2020). Blockchain technology: emerging applications and use cases for secure and trustworthy smart systems. J. Cybersecur. Privacy 1, 4–18. doi: 10.3390/jcp1010002

Shor, P. W. (1994). "Algorithms for quantum computation: discrete logarithms and factoring," in Proceedings 35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM: IEEE), 124–134.

Stewart, I., Ilie, D., Zamyatin, A., Werner, S., Torshizi, M., and Knottenbelt, W. J. (2018). Committing to quantum resistance: a slow defence for bitcoin against a fast quantum computing attack. Royal Soc. Open Sci. 5:180410. doi: 10.1098/rsos.180410

Torres, W. A. A., Steinfeld, R., Sakzad, A., Liu, J. K., Kuchta, V., Bhattacharjee, N., et al. (2018). "Post-quantum one-time linkable ring signature and application to ring confidential transactions in blockchain (lattice ringct v1. 0)," in Australasian Conference on Information Security and Privacy (Cham: Springer), 558–576.