The Future of Cryptocurrency Blockchains in the Quantum Era

Sarah Alghamdi and Sultan Almuhammadi
College of Computer Science and Mathematics
King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia
Emails: saraalghamdi497@gmail.com, sultan@almuhammadi.com

***Abstract*—Cryptocurrency are decentralized digital money systems built on blockchain technology. The transactions are secured in these system using digital signatures based on public-key cryptography. Public-key cryptographic algorithms used for digital signatures, such as ECDSA, are vulnerable to quantum attacks. With over 2 trillion dollars market capitalization, the cryptocurrency industry will be at high risk in the Quantum Era. This paper evaluates the security of today's cryptocurrency blockchains under quantum attacks. It also reviews some of the proposed solutions to protect blockchains in the Quantum Era. Moreover, it presents a number of post-quantum digital signature schemes used to build quantum-safe blockchains. The result of this study shows that only a small portion of cryptocurrency can resist quantum attacks, while most of the cryptocurrencies used today are vulnerable to quantum attacks, with more than 99.8% of the total cryptocurrency market cap remains at risk. Useful recommendations are provided as a result of this study.**

***Keywords*—Cryptocurrency, Blockchain, Quantum Attack, Digital Signature, ECDSA, Hash Function.**

I. Introduction

Recent years have witnessed a significant evolvement of blockchain and distributed ledger technologies. A blockchain has many desired features, such as privacy, security, immutability, redundancy, accountability and transparency. Therefore, it has been employed in cryptocurrency and other various cryptographic applications, such as healthcare, digital voting systems, financial smart contracts, supply-chain control management, and automotive services.

A blockchain acts as a peer-to-peer distributed ledger based on a growing list of records (called blocks) linked cryptographically using secure hashing. It was born with the creation of Bitcoin in 2008 [1]. As of today, more than 5000 cryptocurrencies have been created on blockchain technology. The cryptocurrencies are secure due to the security of the blockchain, which in turn depends on secure cryptographic algorithms such as digital signatures and hash functions. For example, Bitcoin uses SHA-256 for hashing and elliptic curve digital signature. Other blockchains may use more cryptographic tools to provide additional features, such as anonymity and untraceability.

The cryptocurrency market capitalization exceeded 2.5 trillion dollars in May 12, 2021 [2]. With the rapid advances in quantum computing technology, potential quantum attacks are considered serious threats to both hash functions and public-keys cryptography, which may put most of today's cryptocurrencies at a high risk. Therefore, several studies have been recently devoted towards developing quantum-safe blockchains to protect the cryptocurrency industry against quantum attacks.

In the light of the post-quantum transition plans announced by the National Security Agency (NSA) in 2015, it has been observed that the growth of elliptic curve usage has coincided with ongoing development in quantum computing research. Therefore, the elliptic curve cryptography cannot be considered as a desirable long-term solution [3]. There are five main types of post-quantum cryptography (PQC) that can be used to secure blockhains in the Quantum Era, namely: lattice-based, hash-based, code-based, supersingular elliptic curve isogeny-based, and multivariat. These five types are used for post-quantum digital signature schemes. The lattice-based post-quantum digital signature schemes are the most common among these types. Hash-based signature schemes offer a viable post-quantum safe alternative but not practical due to their performance characteristics. Therefore, they are used with modification to suit the blockchain application. For example, the eXtended Merkle Signature Scheme (XMSS) is used as a single path instead of a tree [4].

In this paper, we review existing blockchains used for today's cryptocurrencies. We discuss the vulnerability of these blockchains under quantum attacks. This includes attacks on digital signatures and hash functions. We give an estimate on how soon a potential quantum attack may occur.

The remainder of this paper is structured as follows. Section II gives a brief background on blockchain technology for cryptocurrency and highlights its structure and security features. In Section III, we discuss the security of cryptocurreny blockchains under quantum attacks. In Section IV, we review a number of quantum-safe digital signatures that can be used to protect blockchains in the Quantum Era. The analysis and the discussion of the results are given in Section V. Finally, the conclusion is given in Section VI with recommendations and future work.

II. Background

Users interact with the blockchain in a secure manner by using public-key cryptosystems for digital signatures to authenticate transactions. Hash functions are also essential in a blockchain for linking the blocks. A public-key cryptosystem assigns a pair of keys to each user. The public-key is used for encryption and the private-key is used for decryption. Digital signature systems are also built on public-key cryptography, where the private-key is used to securely sign a message in a

978-1-6654-1760-0/21/$31.00 ©2021 IEEE
DOI 10.1109/Blockchain53845.2021.00082

way that the signature can be verified publicly using the public-key. Digital signatures are essential cryptographic algorithms that secure the cryptocurrency transactions in a blockchain. The public-key is considered the address of the payee, while the private key is used to authorize the payment.

The elliptic-curve digital signatures algorithm (ECDSA) is commonly used to secure transactions in most of the cryptocurrency blockchains. It requires a shorter key than RSA of the same security level. For example, the security of a 256-bit ECDSA is equivalent to a 2048-bit RSA signature [5]. The security of RSA is based on the difficulty of integer factorization, while ECDSA is based on the discrete logarithm problem over elliptic curves (ECDLP). However, both integer factorization and the discrete logarithm problem (DLP) can be solved in polynomial time using a quantum computer with a sufficient number of qubits. Other elliptic-curve based tools are also used in blockchains to reduce the key size, such as the elliptic-curve zero-knowledge proofs [6]. Using an elliptic-curve tool does not prevent quantum attacks on the system unless it is based on one of the five PQC types.

Another important component in blockchains is the hash function. A secure hash function is a one-way function that hashes a message of an arbitrary length and generates a fixed-length output string called a hash code. It is an essential component to ensure the immutability of the blockchain since each block contains a hash code of the previous block as shown in Figure 1. These hash links in the blockchain make it computationally infeasible to modify a block once it is added to the chain and linked to other blocks.

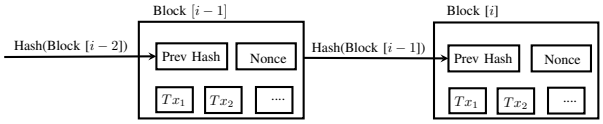

Figure 1. Hash links in a blockchain

Blockchain technology is notably vulnerable to quantum attacks. Quantum computers exploit quantum physics to reduce the time needed to tackle some computational problems. Two main types of quantum algorithms are applicable to attack blockchain security. The first type is represented by Shor's algorithm which can both factor large integers and solve the discrete logarithm in polynomial time [7]. The second type is based on generalizations of the Grover search algorithm [8], which allows searching for hash codes and solving any NP-complete problem quadratically faster than any known classical algorithm. It is worth noting that the speedup of Shor's algorithm is exponential, which implies that any cryptosystem based on integer factorization or DLP is completely vulnerable to quantum attack. On the other hand, the impact of Grover's algorithm on hash functions is quadratic, which implies that a hash-based cryptosystem can resist quantum attack by doubling the size of the key. Further discussion is given in Section V-B with a detail example on attacking bitcoin blockchain.

III. Cryptocurrency in the Quantum Era

Blockchains can be protected from potential quantum attacks by using quantum-resistant cryptography. Post-quantum cryptography represents all algorithms that have the ability to resist quantum attacks. These cryptosystems are based on the generation of asymmetric keys that are secure in the presence of quantum computers.

In this paper, we study a number of today's cryptocurrency blockchains and we classify them into three categories. In the first category, we have those blockchains which are vulnerable to quantum attacks. In the second category, we discussed blockchains that resist quantum attacks. While the third category includes unimplemented post-quantum blockchains found in the literature but not implemented yet. In the following three subsections, we discuss the security of the cryptocurrencies in these categories under quantum attacks.

A. Cryptocurrency Vulnerable to Quantum Attacks

The digital signatures used in the blockchains in this category are mainly based on ECDLP, which can be solve by quantum computers in polynomial time [9]. Examples of blockchains in this category include: Bitcoin, Ethereum, Tether, Binance, Litecoin, Zcash, and many others. Table I shows the digital signaures used in these cryptocurrencies. Notice that some cryptocurrencies, like Monero, Beam and Grin, use more than one signature scheme, but they all are based on elliptic curve discrete logarithm and hence they are vulnerable to quantum attacks.

Table I. Signatures used in cryptocurrencies vulnerable to quantum attacks

Signature	Cryptocurrencies
ECDSA	Bitcoin, Ethereum, Litecoin, Tether, Zcash, Beam, Grin
EdDSA	Monero, Binance
RingCT	Monero, Beam, Grin

1) Bitcoin (BTC): is the first peer-to-peer digital cash system introduced by Satoshi Nakamoto in 2008 [1]. It is the first decentralized system that solves the double spending problem using a distributed timestamp server. It is based on blockchain technology where each block is securely linked using secure hashing. The block contains permanent record of transactions and the hash values make it tamper evident. The block time of Bitcoin is 10 minutes, which means one block is created and linked to the blockchain every 10 minutes on average. This time duration is maintained by the difficulty level imposed by the Proof-of-Work (PoW). It requires the miners to compute a hash value using SHA-256 hashing with a random number (nonce) to ensure that the hash value is less than a specified target value. This is a programmable parameter in the Bitcoin network that is updated roughly every two weeks to maintain the difficulty level needed for the 10 minute block time.

To show ownership of a coin in a transaction, the owner of the coin should sign the transaction using the corresponding private key. Signing the transaction nullifies the value of the spent coin and creates a new coin in same the amount assigned to the payee's public-key who will be the owner of the newly created coin. Bitcoin's transaction mechanism employs the ECDSA signature technique to secure the transaction. Secp256-k1 is the elliptic curve used for ECDSA in Bitcoin. Bitcoin considered to be vulnerable to quantum attack since

Shor's algorithm can be used to break ECDSA in polynomial time $O(n^3)$ on a quantum computer of appropriate scale [9].

2) Ethereum (ETH): is the first cryptocurrency that supports smart contracts. Ethereum utilizes a secp256-k1 elliptic curve-based version of the ECDSA method. The primary public key K linked with an account is not explicitly exposed in an Ethereum transaction since there is no "from" field. In Ethereum 2.0, Proof-of-Stack (PoS) is being used instead of Proof-of-Work (PoW) that was initially introduced for Ethereum original version back in 2015. The new system's security is based on the notion that the more significant the stake, the more voting power a miner will gain. By staking more coins, users are more motivated to act honestly because they stand to lose more if they are caught. The signature scheme of Ethereum 2.0 is still vulnerable to quantum attacks using Shor's algorithm since it is based on the discrete logarithm problem [10].

3) Litecoin (LTC): is a fork of the Bitcoin blockchain sharing many similarities with Bitcoin. Litecoin is a light version of bitcoin with a quarter of block time and less power consumption, which makes it faster and more practical for everyday transactions than Bitcoin. It reduces block time from 10 minutes in Bitcoin to 2.5 minutes, and improves the storage efficiency. Litecoin uses a different PoW method than Bitcoin known as Scrypt. Its objective is to employ computational resources to solve a problem that will allow a user to construct the next block in the blockchain. Scrypt is a password-based key derivation function. It is meant to utilize much less hashing power. This can be seen in comparison with Bitcoin where the hashing rate is approximately $46,000,000$ TH/s compared to 298 TH/s for Lightcoin [9]. To sign transactions, Litecoin employs the ECDSA method. Therefore, it is vulnerable to quantum attacks.

4) Monero (XMR): uses an obfuscated public ledger, where the transactions are untraceable. Monero uses Ring Confidential Transaction (RingCT) to obfuscate the amount sent in a transaction and the sender public-key. Transactions can be broadcasted or sent by all peers, while an outside observer cannot tell the source. The ring digital signature scheme allows a number of peers sign a transaction. When sending the transaction, the sender signs the transaction with an owned key and 10 other keys to give a total of 11 input keys that might have been used to generate a signed transaction. This obfuscates the transaction, and makes it untraceable. Monero uses a modified Edwards curve digital signature algorithm (EdDSA), which is based on the discrete logarithm problem. Like ECDSA, the EdDSA signature is vulnerable to quantum attacks using Shor's algorithm.

However, because RingCT is utilized, the quantum attacker will have to solve several Pedersen commitments to locate the correct public key used in the transaction. Although the Bulletproof protocol used by Monero to obfuscate transacted amounts is vulnerable to quantum attacks, an attacker would have to rely on chance to choose a transaction of substantial value. Furthermore, according to a recent update in Monero's consensus protocol, where RandomX was added, it would be more resistant to quantum assaults attempting to use Grover's method to conduct a 51% attack [9].

5) Grin: is similar to Monero in a way that it employs Pedersen commitments to hide transaction details. The amount represented by the unspent transaction output (UTXO) is hidden by this blinding factor, giving the blockchain an extra layer of anonymity. Like Monero, Grin is vulnerable to quantum attacks against both its obfuscation and signature schemes. While a quantum attacker can remove the obfuscation, the attacker has no way of knowing if the transactions are important enough to merit a quantum attack. The signature scheme is vulnerable to quantum attacks since it is based on ECDSA. However, the concealing of transaction and account values, like with Monero, reduces some of the motivation for a quantum attacker [11].

6) Beam: is similar to Grin in many aspects. First, it employs Pedersen commitments to hide transaction details. The amount represented by the unspent transaction output (UTXO) is hidden by this blinding factor, giving the blockchain an extra layer of anonymity. However, allows optional tracking of transactions and user identifiers as needed. Both Beam and Grin, like Monero, are vulnerable to quantum attacks against their ECDSA based signature schemes. As discussed in Grin, the concealing of transaction and account values reduces the attacking motivation [9]. Unlike Grin and Monero, the goal of Beam is to create a coin that is more regulator-friendly, but can offer additional privacy without conflict with the law.

7) Zcash (ZEC): ensures that the transactions are completely private using Zero-knowledge proofs, which are powerful tools to prove the validity of a secret without revealing any knowledge about it [12]. This allows transactions to be verified without revealing the sender, receiver or the amount in the transaction. Selective disclosure features within Zcash allow a user to share some transaction details, for purpose of compliance or audit. As of 2020, a synthetic version of Zcash is made available on Ethereum through a process known as *wrapping*. This makes Zcash compatible with all of the major wallets and applications. Zcash uses ECDSA with zk-SNARKs (Zero-Knowledge Succinct Non-interactive ARgument of Knowledge) which are vulnerable to quantum attacks [9].

The global public parameter used to create zk-SNARKs is a public-key with no matching private-key, and it is based on the discrete logarithm problem's difficulty. An attacker might utilize Shor's algorithm to figure out the global private key and break the signature scheme. Moreover, the quantum attack on the consensus process is the major concern regarding the integrity of the system. This opens the door to a quantum attack on the consensus mechanism, resulting in a quantum 51% attack on the network.

B. Quantum-safe Cryptocurrency

In the second category we have have blockchains that can resist quantum attacks. The digital signatures used in these blockchains are built on computationally hard problems that cannot be solved by known quantum algorithms in polynomial time. Examples of such blockchains include: IOTA, Nexus, Cellframe, HyperCash, Mochimo, and Quantum Resistant Ledger. Table II shows the signatures used in these quantum-safe cryptocurrencies.

Table II. QUANUTUM-SAFE SIGNATURES USED FOR CRYPTOCURRENCIES

Signature	Cryptocurrency
WOTS	IOTA
WOTS+	Mochimo, Quantum Resistant Ledger
CURL-P	IOTA (Future Plan)
XMSS	Quantum Resistant Ledger
XMSS+	Mochimo
Signature Chains	Nexus
Ring LWE	HyperCash
Multi-Signature	Cellframe

1) IOTA (MIOTA): is a cryptocurrency built on directed acyclic graph (DAG) technology. Like blockchain, DAG allows the creation of a peer-to-peer digital money system without the need for a mint or a third trusted party. In IOTA DAG structure, each transaction is linked to two previously unconfirmed transactions using Proof-of-Stack (PoS) to reduce the confirmation waiting time. The resultant structure is a directed graph with no cycle (DAG), known as *tangle*.

IOTA uses a hash-based digital signature, known as Winternitz One-Time Signature (WOTS). It is considered quantum-safe since there is no known quantum algorithm that breaks hash-based digital signature in polynomial time. However, Grover's algorithm reduces the search-space for the hash-based signature, which implies reducing the security level by half. A longer key might be used in the future to reduce the risk of quantum attacks. IOTA future plan includes an implementation in which a new hash function called CURL-P which uses a ternary hardware instead of binary which add additional security to the system [4].

2) Cellframe (CELL): Several quantum resistant signatures have been successfully developed in Cellframe, particularly the NIST-PQC standardization process second round finalists. A 2-byte ID was introduced at the beginning of each location for encryption to preserve the variability principle. Using the 2-byte ID, Cellframe can support up to $2^{16} = 65{,}536$ digital signature algorithms. The most promising post-quantum algorithms, such as Frodo, SIDH, NewHope, and NTRU, were first selected. The default digital signature was Crystal-Dilithium, which is based on Lattice. Besides, a user might use a mix of algorithms; for example, multi-algorithm signatures could be employed to close all of the deposits in the wallet using more than one key [13].

3) HyperCash (HC): is used as a medium for value exchange of cross-platform, while the platform serves as a carrier for data interflow of cross-platform. In order to achieve the free flow of value and information between blockless and blockchain-based systems, HC platform is being developed to serve as a sidechain for both systems. In light of these design characteristics, HC has considered the data reading from blockchain-based and DAG-based distributed ledger at the earliest level of system design. The blockchain-based distribute ledger includes both Account-Based and UTXO public ledgers. HC is compliant with regular ECDSA signatures and supports post-quantum signature approaches like Ring learning with error (Ring LWE), providing users in a future quantum computing environment with a high-level essential security solution [14].

4) Mochimo (MCM): The eXtended Merkle Signature Scheme (XMSS+) is employed in Mochimo with the WOTS+ which is a digital signature variant of the Winternitz One-Time Signature. Both MXSS+ and WOTS+ make the scheme quantum-resistant. A number of security features are included in MCM, such as transaction mirroring and three-way handshake. The transaction mirroring ensures the validity of the transactions and the peers to leverage the random network model. If the transaction is invalid, it will be rejected and the peer made the request will be blacklisted. The three-way handshake protocol protects the MCM blockchain from denial of service attacks, spoofing, and man-in-the-middle attacks. MCM blockchain provides scalability using the ChainCrunch algorithm. It allows full node operation mode using only a small percentage of the blockchain data. The algorithm uses HASH256 which makes it quantum resistant [15].

5) Nexus (NXS): has taken precautions by incorporating numerous cryptographic schemes that enable higher degrees of quantum resistance. Falcon, Argon2, and Keccak are among the cryptographic functions included in Nexus. The security of existing digital signature algorithms benefits from signature chains. With each transaction, the public-key is kept hashed until it is used, and the key pair is changed for the output coins generated by the transaction. The signature chains mainly employ the public-key cryptography. However, the hash value of these credentials is stored on the blockchain for future use rather than storing the keys on a disc or in the cloud. Consequently, the private key falls outdated whenever the next transaction is created. This results in higher levels of security compared to other blockchain systems wherein the private key is permanently reused [16].

6) Quantum Resistant Ledger (QRL): uses a hash-based signature scheme, which employs chained XMSS trees to establish an extensible stateful asymmetrical hypertree signature methodology. This offers the combined benefit of allowing creation of ledger addresses with the ability to sign transactions without the significant pre-computation delay found with large XMSS structures. WOTS+ was chosen as the scheme's hash-based one-time signature for both performance and security considerations. QRL is the first commercial version of the Internet Research Task Force (IETF) employing XMSS, a hash-based, secure signature scheme with minimum security restrictions and reusable addresses that are approved by the National Institute of Standards and Technology (NIST) [17].

C. Unimplemented Quantum-safe Cryptocurrency

The third category includes recently designed quantum-safe cryptocurrency blockchains but not implemented yet. Examples of cryptocurrencies in this category include: Bitcoin PostQuantum, Ethereum 3.0, and Corda. Table III shows the digital signatures proposed in these cryptocurrencies. We review the security issue of each cryptocurrency in this category.

Table III. QUANTUM-SAFE SIGNATURES OF UNIMPLEMENTED CRYPTOCURRENCIES

Signature	Cryptocurrencies
SPHINCS-256	Corda
XMSS, WOTS+	Bitcoin PostQuantum
Multi-Signature	Ethereum 3.0

1) Corda: uses Sequential Photon Interrogation and Neutron Counting Signatures (SPHINCS), which is a quantum-safe digital signature, in addition to a number of public-key signatures schemes. It is cryptographically agile wherein the available set of signature schemes is carefully chosen based on a variety of aspects. These aspects may include: the security level, cryptographic strength, business demand, algorithm standardization, and the solution for post-quantum resistance method. There are currently five signature schemes supported by Corda, which are:

- Pure EdDSA (utilizing ed25519 curve and SHA-512)
- ECDSA (utilizing Koblitz k1 curve (secp256-k1) and SHA-256)
- ECDSA (utilizing NIST P-256 curve (secp256-r1) and SHA-256)
- RSA (3072 bit) PKCS#1 and SHA-256
- SPHINCS-256 and SHA-512 (experimental)

Among these five signatures, SPHINCS-256 is the only safe post-quantum scheme that exclusively uses hash functions. It is employed as a safety net in case a hostile attacker gets hands on a quantum computer capable of performing Shor's algorithm in the future. SPHINCS is basically based on a sophisticated utilization of Merkle hash tree [18].

Our analysis of the scheme shows that SPHINCS utilizes relatively large public keys, and it is slower and produces larger signatures than RSA, ECDSA and EdDSA. However, hash function cryptography is a well-known approach extensively studied in literature. As a result, significant quantum attacks on the mathematical bases of hashing are thought to be far less likely than on RSA and ECDSA signatures.

2) Bitcoin PostQuantum (BPQ): uses the hash-based XMSS scheme, which combines reasonable key generation time, signature size, and strong security. The XMSS signature contains the W-OTS+ signature and the authentication path to denote the sequence of tree nodes required to calculate the root of the Merkle tree. In addition, BPQ adopts a robust post-quantum zero-knowledge framework for transaction to provide privacy via anonymity for both classical and post-quantum signature. To achieve the minimum security level of 128-bits, BPQ uses a hash function of size 256 bit [19].

We conclude that BPQ is one of the best suggested solutions to secure cryptocurrencies in the Quantum Era. It addresses many desired security issues such as: secure transactions against quantum attacks, anonymity and untraceability of transactions using zero-knowledge proofs, and a secure migration plan from classical to post-quantum blockchain using a hard-fork of the main blockchain.

3) Ethereum 3.0: supports multi-signatures that are post quantum. Quantum-resistant components, such as zk-STARKs (Zero-Knowledge Scalable Trans-parent ARguments of Knowledge), are planned to be integrated in the future. The zk-SNARKs is also used in Ethereum 3.0, and it relies on a reliable setup that demands the pre-creation of a greater public-key [20]. The global public-key must be devoid of a private-key as discussed in Zcash. Otherwise, the key holder might generate Zcash coins as will. Moreover, this greater public-key is generated by several users working together to create tiny pieces of a larger public-key from their private keys. In case of destroying the private-key by at least one individual after the public ceremony, then identifying the greater public-key's conforming private-key on a traditional computer will become computationally intractable. This is due to the fact that computing this private-key requires either solving the discrete logarithm or providing access to all of the private-keys needed to produce the greater public-key.

It is worth mentioning that, with all of the newly added features, Ethereum 3.0 will be a very important quantum-safe platform that support smart contracts in the Quantum Era. This also will provide quantum-resistance to many of today's cryptocurrencies that run on Ethereum ERC-20 platform.

IV. A Review on Quantum-Safe Digital Signatures

In Section III-A, we discussed the vulnerability of some existing blockchains, such as Bitcoin and Ethereum, under quantum attacks. The total market cap of these two cryptocurrencies alone is over 1.06 trillion dollars as of August 1, 2021 [2], which is about 65% of the total market cap. Therefore, many researchers work on protecting these vulnerable blockchains, and design post-quantum cryptographic digital signatures to replace ECDSA. Moreover, researchers work on the transition protocol from pre-quantum (classical) to post-quantum blockchains. This protocol guarantees the safe and smooth transition without potential loss of assets. In this section, we review a number of quantum-safe digital signatures suitable for cryptocurrency blockchains in the Quantum Era.

Gao et al. [21] proposed a signature based on lattices. The short lattice delegation algorithm is employed to create secret keys with a random value. The message is then signed with a trapdoor one-way function using the preimage sampling algorithm. To decrease the correlation between the signature and the message, the first and last signatures are designed and defined as double-signature in the presented scheme. The post-quantum blockchain (PQB) is then constructed by integrating the proposed signature with the blockchain in which the security is reduced to the lattice short integer solution problem (SIS). The proposed scheme resists quantum attacks and the signature is claimed to fulfill correctness as well as unforgeability under the SIS assumption. Relative to existing signature schemes, the size of the signature and secret keys in the proposed scheme are comparatively shorter than that of the other schemes, which is claimed to reduce the computational complexity. Therefore, the proposed cryptocurrency scheme is both efficient and secure.

Yin et al. [22] proposed a signature scheme on lattice based using Bonsai Trees technology. They proposed a new authentication scheme extending the lattice space to multiple lattice spaces accompanied by the corresponding key. Each signature in a transaction uses a lattice space to ensure the randomness and increase the security of the whole scheme.

Lattice based signature scheme is also used in [23]. In this work, the authors also use Bonsai Trees technology with random basis algorithm. Their goal is construct a secure lightweight non-deterministic wallets.

Noel et al. [24] provided analysis of stateful hash-based signature schemes for the Bitcoin blockchain. In their study, they presented Lamport One-Time Signature Scheme, Merkle Signature Scheme, and WOTS. These three schemes are stateful hash-based signature schemes and, therefore, have common features as show in there analysis.

Zhang et al. [25] proposed a lattice based cryptosystem scheme to reduce the size of the public key and signature. A qTESLA lattice-based blockchain system is developed to resist quantum attacks. To deal with the block capacity challenge, they proposed an algorithm that keeps only the hash values of signatures and public keys on the blockchain, while the complete content are saved on interplanetary file system. Consequently, the number of bytes required for each transaction will be significantly reduced. The proposed scheme is tested and the stability and feasibility are verified.

Torres et al. [26] introduced one-time Lattice-based Linkable Ring Signature scheme (L2RS). This L2RS scheme grants unconditional anonymity and security with respect to the ring short integer solution (Ring-SIS) under the lattice hardness assumption. The proposed scheme is used to build a lattice ring confidential transaction scheme (Lattice RingCT) that provides the privacy-preserving protocol for any post-quantum secure cryptocurrency, such as Hcash and Monero.

Sun et al. [27] proposed a new version of lattice based on ring confidential transaction protocol (RingCT 2.0) for Monero. RingCT 2.0 is based on the Pedersen commitment for secret sharing [28]. The proposed scheme is proved to be efficient and able to meet the security requirements. They investigated the (RingCT 1.0) in [26], and found that the transaction size in the original RingCT suffers from a linear growth in terms of the number of groups included in the ring. They make the transaction size in RingCT 2.0 independent of the number of groups in the ring. Relative to the original protocol, the proposed RingCT 2.0 protocol contributes to significant space saving allowing each block to perform multiple transactions.

Liu et al [29] a cryptographic primitive scheme known as linkable ring signature scheme with stealth addresses (SALRS) is proposed. The security and privacy requirements of hiding the transaction's payee and payer are completely guaranteed. A lattice-based SALRS construction is also proposed for which the security and privacy of the proposed construction in proved in random oracle model. It is observed that the proposed lattice-based SALRS scheme is quantum safe and suitable for practical implementations.

V. Analysis and Discussion

As of August 1, 2021, the total cryptocurrency market capitalization is 1.65 trillion dollar[1] according to CoinMarketCap website [2]. About 71% of the market cap (1.18 trillion dollar) is in the top four cyptocurrencies, namely: Bitcoin, Ethereum, Tether, and Binance, with signatures based on DLP, as shown in Table IV. This puts the cryptocurrency market at high risk when a sufficiently large scale quantum computer exist.

[1]The total market cap was fluctuating between 1.2 and 2.5 trillion dollars during the period between May and August 2021.

Table IV. Cryptocurrency market cap and signatures [2]

Cryptocurrency	Market Cap	Signature
Bitcoin (BTC)	$780,913,407,401	(ECDSA)
Ethereum (ETH)	$285,002,633,143	(ECDSA)
Tether (USDT)	$61,816,134,107	(ECDSA)
Binance (BNB)	$56,716,831,371	(EdDSA)
Others	$482,020,827,080	–
Total market cap	$\mathbf{\$1,647,359,772,538}$	–

A. Amount of Cryptocurrency Protected Against Quantum Attack

In Section III-B, a number of quantum-safe cryptocurrency blockchains are discussed, such as: IOTA, Cellframe, Nexus, HyperCash, Quantum Resistant Ledger, and Mochimo. These are the top quantum-safe cryptocurrencies in terms of their market capitalization according to CoinMarketCap website [2]. We would like to estimate the amount of cryptocurrency that will remain secure in the Quantum Era. Table V shows the digital signatures used in these coins as well as their market cap. Other quantum-safe cryptocurrencies have much smaller caps and, therefore, can be safely neglected in our discussion. The total market cap of the quantum-safe cryptocurrency in Table V is about $2.68 billion. This means that less than 0.2% of the total market cap is quantum-safe as of today, while the remaining 99.8% is at risk of quantum-attacks.

Table V. Top quantum-safe cryptocurrencies [2]

Cryptocurrency	Market Cap	Signature
IOTA (MIOTA)	$2,564,086,687	WOTS, CURL-P
Nexus (NXS)	$38,356,070	Signature Chains
HyperCash (HC)	$33,738,125	Ring LWE
Cellframe (CELL)	$19,655,700	Multi-Signature
Quantum Res. Ledger (QRL)	$18,426,400	XMSS, WOTS+
Mochimo (MCM)	$2,170,139	XMSS+, WOTS+
Total	$\mathbf{\$2,676,433,121}$	-

In spite of the clear risk of quantum attacks on the existed cryptocurrency blockchains, yet we see many cryptocurrnceys launched this year that are not quantum-safe. Table VI shows examples of new cryptocurrencies appeared this year but not quantum-safe. Although post-quantum digital signatures are efficient, the main reason for not implementing quantum-safe in the newly launched cryptocurrencies given in Table VI is because they are built as tokens on Ethereum (ERC-20) or Binance Smart Chain (BSC BEP-20) for an easy startup. Therefore, it will be highly recommended to build a quantum-safe blockchain that supports smart contracts like in Ethereum ERC-20 and Binance BSC BEP-20. This will provide a platform for easy startups of quantum-safe cryptocurrencies in the future.

Table VI. Non-quantum-safe cryptocurrencies in 2021

Cryptocurrency	Date	Market Cap	Signature
Alpha Impact (IMPACT)	May 30, 2021	$19,222,208	ECDSA
BlackPool (BPT)	June 11, 2021	$4,125,943	ECDSA
Fluity USD (FLUSD)	May 20, 2021	$3,603,294	EdDSA
Kuma Inu (KUMA)	June 14, 2021	$2,028,645	ECDSA
Star Foxx (FOXX)	May 16, 2021	$353,443	ECDSA

B. The 51% Attack on Blockchain Using Quantum Computers

The security of Bitcoin and other cryptocurrencies depends on the honesty of the majority of the peers in the network.

If a dishonest node tries to deviate from the protocol to gain advantage, the majority will eventually reject the block. However, a peer with high computational power might approve an invalid transaction with a double-spent coin successfully without being detected if it can outrun the majority. This could be done by generating a transaction with a double-spent coin, adding it to the block, and linking it to the blockchain, then adding several blocks so that the block with the double-spent coin ends up in the longest chain eventually. Since other peers only consider the longest chain and append to it, the transaction with double-spent coin will remain accepted by consensus in "the blockchain" (i.e. the longest chain). The previous transaction where the coin was first spent will no longer be valid, and the new owner of that coin will not be able to claim it any more. As a result, if the attacker can out the majority, the same coin can be spent twice, however only the second time is considered valid. This is known as a 51% attack where the attacker should possess more than half of a computational power in the network.

Quantum computers are superior compared to classical ones. A quantum computer with sufficient qubits can theoretically outrun all the classical computer in the world. Suppose Eve has a quantum computer, and she wants to attack the bitcoin blockchain. The current hash rate in Bitcoin is about 97 exahash per second (Eh/s) [2], which is 97×10^{18} hash/s. Grover's algorithm gives a quadratic speedup for the search problem [8]. Therefore, the search space can be reduced to $\sqrt{97 \times 10^{18}} = 9.8 \times 10^9$. This emphasis that an attacker with a quantum machine can do $\frac{97\times10^{18}}{9.8\times10^9} \approx 10^{10}$ times faster than the classical machines. This is equivalent to 970 Mega hash/s, which is much smaller than the actual 97 Eh/s. Therefore, an attacker with a quantum computer can easily perform the 51% attack in general. According to Satoshi Nakamoto [1], this might not be a serious problem since the attacker in this case is ought to play by the rules and obtain the mining incentive rather than break the system. However, we should not ignore the fact that the blockchain system is vulnerable to quantum search attack.

C. When to Expect a Potential Quantum Attack?

According to Aggrawal et al. [30], ECDSA used by Bitcoin could be completely broken by a quantum computer as early as 2027. Mosca [31] estimated that there will exist a quantum computer capable of breaking the RSA with 2048 bits security in year 2031 with a 50% chance. On the other hand, Kearney et al. [9] estimated that breaking the 2048-bit RSA bit will be possible by year 2035.

We give an argument based on Moore's law to estimate the year in which quantum attack will be probable. According to Moor's law, the number of transistors that can be put in an integrated circuit (IC) is doubled every two years [32]. This law is based on the observation of the advances in technology over three decays. If we apply Moore's law in quantum computing technology, we may assume that the number of qubits in quantum computers is doubled every two years. For simplicity, we may also ignore the noise associated with the increasing number of qubits. Based on this assumption, we may estimate the expected year for a potential quantum attack on RSA 2048 bit. According to Sparkes [33], a Chinese team developed a quantum computer featuring 66 qubits in July 2021. By Moore's law, in 12 years from now, the number of qubits will be doubled 6 times. Therefore, in year 2033 we will have a quantum computer with $66 \times 2^6 = 4224$ qubits. This will be sufficient to break a 2048-bit RSA scheme since the number of qubits needed by Shor's algorithm to factorize a 2048 integer is $2 \times 2048 + 3 = 4099$ using implementation in [34]. Our estimated year is closed to the years of 2031 and 2035 obtained by Mosca [31] and Kearney [9], respectively.

VI. Concluding Remarks and Recommendations

Despite blockchains are usually safe and utilize asymmetric and symmetric cryptography as required throughout the blockchain network, they are essentially vulnerable to quantum attacks. In principle, quantum computers can solve hard mathematical problems used to secure many cryptocurrency blockchains. Therefore, these blockchains will not be secure in the Quantum Era. Other blockchains are built on different problems for which no know quantum algorithm can solve in reasonable time. These blockchains may resist quantum attacks in the future as long as their underlying mathematical problem remains intractable even when large scale quantum computer exist.

Due to their high market cap, and the high risk associated with it, the cryptocurrency blockchains should be protected from potential quantum attacks in the near future by switching to post-quantum blockchains cryptography. As a result of this study, we provide the following recommendations:

1) The cryptocurrency industry is urged to migrate from classical blockchains to post-quantum blockchains. Based on our study, potential quantum attacks might occur as early as 2033.
2) Blockchains for new cryptocurrency should be built on post-quantum cryptography. ECDSA should no longer be used in newly created blockchains (like the ones in Table VI) since they will be vulnerable to quantum attacks.
3) Post-quantum blockchain solutions should not depend on specific post-quantum signature scheme (like in Cellframe [13]). Although there is no known algorithm that can solve the underlying mathematical problem of the specified scheme today, such an algorithm might be built in the future. Therefore, it is recommended to design scheme-independent post-quantum solutions for blockchains.
4) It is highly recommended to have a quantum-safe blockchain supporting smart contracts to provide a platform for easy startups of quantum-safe cryptocurrencies in the future.
5) For IOTA and other post-quantum blockchains using hash-based digital signatures, we recommend increasing the key size in the signature schemes by at least the double to cope with the quadratic speedup achieved by Grover's algorithm.
6) To reduce the potential risk of the 51% attack by quantum computers, we recommend that new post-quantum blockchains should avoid using PoW in the their consensus algorithms. We recommend using PoS or any other alternatives that are not based on hash searching.

Regarding the future work, the post-quantum digital signatures presented in this work can be tested and their performance can be compared experimentally. In addition, the migration process from classical blockchain to post-quantum blockchain should be discussed to ensure secure and safe transition. The solutions discussed in this paper for quantum-safe cryptocurrency blockchains can be applied to other blockchain applications, such as healthcare, digital voting, financial smart contracts, supply-chain management, and automotive services.

ACKNOWLEDGMENT

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

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Available: https://bitcoin.org/bitcoin.pdf, 2008, [Online]. Accessed 1 August 2021.

[2] "Coinmarketcap: Cryptocurrency prices, charts and market capitalization," Available: https://coinmarketcap.com/, [Online]. Accessed 1 August 2021.

[3] National Cryptographic Solutions Management Office (NCSMO), "Cryptography today," Available: https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml, [Online]. Accessed 1 August 2021.

[4] T. M. Fernández-Carames and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE access*, vol. 8, pp. 21 091–21 116, 2020.

[5] E. Barker, W. Burr, A. Jones, T. Polk, S. Rose, M. Smid, Q. Dang *et al.*, "Recommendation for key management part 3: Application-specific key management guidance," *NIST Special Publication*, vol. 800, p. 57, 2009.

[6] S. Almuhammadi, N. T. Sui, and D. McLeod, "Better privacy and security in e-commerce: using elliptic curve-based zero knowledge proofs," in *Proceedings. IEEE International Conference on e-Commerce Technology, 2004. CEC 2004.* IEEE, 2004, pp. 299–302.

[7] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*. IEEE, 1994, pp. 124–134.

[8] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 1996, pp. 212–219.

[9] J. J. Kearney and C. A. Perez-Delgado, "Vulnerability of blockchain technologies to quantum attacks," *Array*, vol. 10, p. 100065, 2021.

[10] V. Buterin, "Ethereum whitepaper," Available: https://ethereum.org/en/whitepaper/, 2013, [Online]. Accessed 1 August 2021.

[11] T. E. Jedusor, "Grin: Mimblewimble," Available: https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.txt, 2016, [Online]. Accessed 1 August 2021.

[12] S. Almuhammadi and C. Neuman, "Security and privacy using one-round zero-knowledge proofs," in *Seventh IEEE International Conference on E-Commerce Technology (CEC'05)*. IEEE, 2005, pp. 435–438.

[13] "Cellframe: Service oriented blockchain network, whitepaper ver 2.0 beta," Available: https://cellframe.net/ files/CllfrmWPbeta20(1).pdf, [Online]. Accessed 1 August 2021.

[14] "Hcash: The new standard of value, whitepaper v.0.8.5," Available: https://h.cash/themes/en/images/Hcash+Whitepaper+V0.8.5.pdf, [Online]. Accessed 1 August 2021.

[15] M. Zweil, "Mochimo: Post-quantum currency," Available: https://mochimo.org/wp-content/uploads/dlm_uploads/2018/04/mochimo_wp_EN.pdf, 2018, [Online]. Accessed 1 August 2021.

[16] "Nexus: The tritium protocol," Available: https://tech.nexus.io/files/tritium/Nexus-Tritium-White-Paper.pdf, 2018, [Online]. Accessed 1 August 2021.

[17] "Quantum resistant ledger (qrl)," Available: https://raw. githubusercontent.com/theQRL/Whitepaper/master/QRL_whitepaper. pdf, 2016, [Online]. Accessed 1 August 2021.

[18] R. Gendal Brown, J. Carlyle, G. Ian, and H. Mike, "Corda: An introduction," Available: https://docs.corda.net/en/pdf/corda-introductory-whitepaper.pdf, 2016, [Online]. Accessed 1 August 2021.

[19] N. Anhao, "Bitcoin post-quantum," Available: https://bitcoinpq.org/download/bitcoinpq-whitepaper-english.pdf, 2018, [Online]. Accessed 1 August 2021.

[20] "Ethereum's official roadmap," Available: https://github.com/ethereum/wiki/wiki/Sharding-roadmap, [Online]. Accessed 1 August 2021.

[21] Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu, and Y.-X. Yang, "A secure cryptocurrency scheme based on post-quantum blockchain," *IEEE Access*, vol. 6, pp. 27 205–27 213, 2018.

[22] W. Yin, Q. Wen, W. Li, H. Zhang, and Z. Jin, "An anti-quantum transaction authentication approach in blockchain," *IEEE Access*, vol. 6, pp. 5393–5401, 2018.

[23] C.-Y. Li, X.-B. Chen, Y.-L. Chen, Y.-Y. Hou, and J. Li, "A new lattice-based signature scheme in post-quantum blockchain network," *IEEE Access*, vol. 7, pp. 2026–2033, 2018.

[24] M. D. Noel, O. V. Waziri, M. S. Abdulhamid, and A. J. Ojeniyi, "Stateful hash-based digital signature schemes for bitcoin cryptocurrency," in *2019 15th International Conference on Electronics, Computer and Computation (ICECCO)*. IEEE, 2019, pp. 1–6.

[25] P. Zhang, L. Wang, W. Wang, K. Fu, and J. Wang, "A blockchain system based on quantum-resistant digital signature," *Security and Communication Networks*, vol. 2021, 2021.

[26] W. A. A. Torres, R. Steinfeld, A. Sakzad, J. K. Liu, V. Kuchta, N. Bhattacharjee, M. H. Au, and J. Cheng, "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*. Springer, 2018, pp. 558–576.

[27] S.-F. Sun, M. H. Au, J. K. Liu, and T. H. Yuen, "Ringct 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero," in *European Symposium on Research in Computer Security*. Springer, 2017, pp. 456–474.

[28] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Advances in Cryptology — CRYPTO '91*, J. Feigenbaum, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1992, pp. 129–140.

[29] Z. Liu, K. Nguyen, G. Yang, H. Wang, and D. S. Wong, "A lattice-based linkable ring signature supporting stealth addresses," in *European Symposium on Research in Computer Security*. Springer, 2019, pp. 726–746.

[30] D. Aggarwal, G. K. Brennen, T. Lee, M. Santha, and M. Tomamichel, "Quantum attacks on bitcoin, and how to protect against them," *arXiv preprint arXiv:1710.10377*, 2017.

[31] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?" *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, 2018.

[32] G. E. Moore *et al.*, "Cramming more components onto integrated circuits," 1965.

[33] M. Sparkes, "China beats google to claim the worlds most powerful quantum computer," Available:https://www.newscientist.com/article/2282961-china-beats-google-to-claim-the-worlds-most-powerful-quantum-computer/, 2021, [Online]. Accessed 1 August 2021.

[34] S. Beauregard, "Circuit for shorś algorithm using 2n + 3 qubits," *arXiv preprint quant-ph/0205095*, 2002.