Quantum Resistance in the Quantum Coin Blockchain

Authors: The Quantum Coin Community

Publication Date: October 2021

Revision 3: October 2024

Contents

Introduction

Public Key Cryptography (asymmetric cryptography) is essential for blockchains to secure accounts as well as enable validations in Proof of Stake systems. Digital Signatures are made possible by public key cryptography. Using digital signatures, the authenticity of transactions in blockchains can be verified. Some of the currently popular digital signature schemes are the RSA scheme and Elliptic Curve-based schemes (ECDSA). Bitcoin and Ethereum (PoW) for example, use elliptic curve-based schemes.

Quantum Computer Threat to Blockchains

With current computer hardware (also known as classical computers), it can take millions of years to calculate the private key from a public key. With Quantum Computers, however, it is possible to calculate the private key from the public key rapidly, at a speed that is proportional to the number of qubits of the quantum computer. This is because of the property of quantum computers to be in a superposition of states.

What this means is that anyone with a quantum computer can forge blockchain transactions and send another account's coins to their account, or simply use it to destroy the blockchain, because it is no longer secure. Blockchains like Bitcoin and Ethereum will be broken beyond recovery when quantum computers that are capable of doing this become available; since it will be too late for them to move to a quantum-resistant cryptographic scheme. The time when such quantum computers become available is referred to as Y2Q (years to quantum), an analogy to the Y2K problem.

Likewise, in a Proof-of-Stake blockchain, in addition to forging the signature of account holders, the signature of validators can also be forged, thus causing multiple security problems like double-spending.

Without a post-quantum cryptographic scheme, not only blockchains, but also internet security protocols like TLS will be broken by quantum computers (since the underlying cryptographic schemes used in TLS currently are RSA, and ECDSA). It can take months, if not years, for widespread adoption of TLS that uses quantum-resistant cipher suites, especially in legacy clients and hardware like IoT devices.

If a bad actor manages to get access to such a quantum computer before the wide scale adoption of post-quantum cryptography, it can be catastrophic in unimaginable ways. For example, banks will not be able to process any transactions and have to shutdown their online services because transactions cannot be trusted.

Flight, train or other bookings cannot be made online, because the transactions can be forged. Communication links between power plants, water systems, and nuclear facilities are no longer secure and might have to be shutdown temporarily.

The impact on blockchains is more critical; this is because systems like banks can shutdown temporarily while upgrading to a quantum-resistant TLS cipher suite and re-sign their documents and data (where digital signatures are used) in a phased approach. But blockchains can be rendered invalid without possible recovery because the authenticity of transactions and the blockchain ledger can no longer be trusted.

Inter-Node Communication

Inter-node communication between various blockchain nodes such as validators, data archivers etc. is also at risk due to quantum computers. Quantum Computers that can break communication security in real-time can be used to inspect protocol packets, alter them, delay them, or drop them selectively (man-in-the-middle attacks).

Even though account transactions may be signed before sending over the wire, they won't be enough to safeguard against other protocol parameters that are not part of the signed payload. Furthermore, transactions can be dropped selectively by ISPs, to block a specific account or accounts from a specific IP range or country, for example.

Shor's Algorithm

Peter Shor created an algorithm in 1994 while at Bell Labs, that can solve the problem of integer factorization and extracting discrete logarithms in polynomial time (on a quantum computer). This will break currently known cryptography schemes like RSA, and ECDSA that have so far been successful because no known algorithm can break them in polynomial time with classical computers.

Shor's algorithm is the most important reason why there is a wide effort to come up with new cryptography schemes that are resistant to quantum

computers. Though this algorithm has existed since 1994, recent advances in quantum computer technology have elevated the security risk to a critical level.

Grover's Algorithm

Grover's algorithm can be used to achieve a quadratic speedup of Proof-of-Work hashes on a quantum computer. Though the efficiency over classical computers is only quadratic, a network of powerful quantum computers can break Bitcoin and Ethereum Proof-of-Work systems in two different ways.

One is a 51% attack by creating a longer blockchain that contains forged transactions. This essentially renders these blockchains invalid because the finality gadget of the blockchain is broken. In proof-work-systems, the finality gadget is probabilistic, since, at any point in time, the longest chain becomes the correct chain. The rest of the chains are treated as invalid forks in this case. Because of this reason, the attacker's forged chain will be treated as the correct one, causing a catastrophic impact on these blockchains.

The second attack is a more subtle one; for example, a network of quantum computers can mine most, if not all the newly minted bitcoins, because of their higher hash rate compared to other miners. Depending on the subtlety level, this can impact these blockchains in many ways:

a) Mining may become even more centralized than it is now, and the network hash rate keeps going up, without anyone realizing that a quantum computer network is silently mining many of the Bitcoin rewards.

b) Miners using classical computers might shutdown their mining systems because it is not economical for them to keep running mining operations because they are getting only a few of the newly minted bitcoins. With just the quantum-computer based miners running the network (of which there will only be a few initially), it becomes more or less, a centralized blockchain.

Note that while Grover's algorithm is not considered a significant threat to blockchains in the near term, because it can help achieve only a quadratic speedup over classical computers, it can still become a threat in the longer term.

Classes of Post Quantum Cryptography Schemes

Post Quantum Cryptography (PQ) schemes are those that are resistant to quantum computers breaking the security model, typically by being able to calculate a private key from the public key. Note that the word "quantum-resistant" rather than "quantum proof" is used, since no algorithm should be deemed completely secure to future advances in quantum computer technology. Most of these PQ cryptography schemes fall under the following classes.

Hash-Based Cryptography

Hash based cryptographic schemes rely on the security of hash functions by providing a one-time-signature (OTS) scheme. Leslie Lamport invented this scheme in 1978. The scheme however is impractical for general use, since it can be used only once to sign.

This was extended to provide many times signing support capability using Merkle Trees, by Ralph Merkle. Later, more schemes such as XMSS (eXtended Merkle Signature Scheme) were developed based on this work, but they continued to be stateful in nature. The main disadvantage of stateful schemes is that the key can be used a limited number of times and hence is not helpful for practical purposes.

Newer hash-based crypto schemes like SPHINCS+ worked around this by providing a stateless scheme, by extending the space (of the number of hashes), and by covering every possible signature for that size.

Code Based Cryptography

Code-based cryptography is based on error-correcting codes. Random noise is added as part of the encryption process; this forms the crux of the hardening of the scheme. Decrypting is like correcting these errors. One such popular scheme is Classic McEliece, which was invented in 1978. While this scheme can be extended for use in digital signatures [19], none of the code-based cryptography schemes has made their way into round 4 of the NIST PQC standardization effort ([22]), for digital signature schemes. However, Classic McEliece is one of the candidates in round 4 for "Public-key Encryption and Key-establishment Algorithms".

Lattice-Based Cryptography

Lattice-based cryptography works on basis of the following hard problems that exist in this domain:

a) Shortest Vector Problem (SVP)
b) Closed Vector Problem
c) Bounded Distance Decoding
d) Covering Radius Problem
e) And more

In addition to being conjectured to be quantum resistant, lattice-based cryptography is also used for homomorphic encryption, code obfuscation and attributed-based encryption.

Multivariate Cryptography

This cryptography scheme derives its security from the difficulty of solving systems of multivariate polynomials over finite fields (known to be an NP-hard problem).

Rainbow, one of the digital signature schemes that use this model, was a 'round 3' candidate in NIST PQ cryptosystems. Rainbow was broken ([23]) in 2022, requiring just a classic computer running over a weekend to break it.

Post Quantum Digital Signature Schemes

Dilithium (ML-DSA)

Dilithium is a lattice-based cryptography system that is based on hard problems over module lattices. Dilithium was standardized at the conclusion of Round 3 of the NIST PQ program ([22]).

Falcon

Falcon is another lattice-based cryptography system. Falcon uses the GPV framework, NTRU lattices and Fast Fourier Sampling. Falcon was standardized at the conclusion of Round 3 of the NIST PQ program ([22]).

SPHINCS+ (SLH-DSA)

SPHINCS+ is a stateless hash-based signature scheme. It was standardized at the conclusion of Round 3 of the NIST PQ program ([22]).

Mayo

Mayo ([21]) is a post-quantum oil and vinegar-based signature scheme. Compared to previous UOV signature schemes, Mayo has a smaller public key (614 bytes) and signature size (392 bytes). While Mayo hasn't been submitted to the NIST post-quantum program yet (since it was created only in late 2021), NIST has

called for another smaller program for signature schemes with a smaller signature size.

Mayo was submitted as part of the NIST additional signature ramp program, for evaluation, given its attractive signature and public key size.

There are also other interesting signature schemes like UOV, and SQISign that are submitted and will be evaluated in the forthcoming NIST signature scheme program.

Limitations

It is preferred for digital signature cryptography schemes to have certain characteristics and functionality, for use in blockchains. These systems aren't necessarily a concern for use in other domains like TLS but can become an impediment to either implementation or adoption of blockchains.

Signature Aggregation

Signature aggregation can reduce network and storage requirements in proof-of-stake blockchains, by aggregating many signatures for a common message that needs to be signed. Especially concerning storage, the required space can easily run over many terra-bytes of data over a few years, depending on the consensus algorithm used.

Schemes like BLS signatures make it possible to verify without requiring the original public keys. There is no such scheme yet for post-quantum cryptography that has been standardized by NIST.

Recovery Phrases

Recovery Phrases also known as Mnemonic Phrases provide a human-friendly way to store private keys. While it is less secure compared to hardware wallets or password-encrypted private keys, they do enable wider adoption of blockchain by the masses because of their simplicity. No such method exists (or has been standardized) currently for the post-quantum cryptographic system.

Hardware Wallets

Hardware Wallets are important in protecting user's blockchain accounts from digital theft. However, it would take a while for hardware wallets that support quantum-resistant cryptography schemes, to become available to the general public. This can potentially inhibit the adoption for quantum-resistant blockchains.

Key Recovery

Blockchains like Ethereum use signatures with key-recovery mode so that it makes it possible to calculate the public key from the signature. The typical expectation of the key-recovery mode is that the size of the 'signature-with-key recovery is less than the 'signature-without-key-recovery' plus the length of the public key. While PQ systems like Falcon support key recovery mode, this mode is not part of the formal specification, hence less likely to be well tested and reviewed.

Quantum Resistance in Quantum Coin

Quantum Coin will provide quantum resistance in a three-fold manner.

First, Quantum Coin will use a hybrid proof-of-stake system that will eliminate the need for Proof-of-Work mining. This will prevent the category of attacks made possible by Grover's algorithm.

Secondly, Quantum Coin will use a hybrid digital signature scheme. More details on the hybrid model later in this document. This scheme will be used for securing user accounts, validators and other accounts that will play a role in the Quantum Coin blockchain consensus system.

Since validator nodes need to be online, the risk of the node getting compromised is higher, hence validators will be able to use a different key from the one used for their own user accounts.

Using a quantum-resistant digital signature scheme for these accounts will prevent the category of attacks made possible by Shor's algorithm.

Thirdly, Quantum Coin will use a hybrid public key encryption scheme to protect communication traffic between blockchain nodes.

Important Requirements

The following criteria needs to be satisfied for Quantum Coin to select a specific cryptography scheme for standardization.

i) Standardization

It is important that cryptosystems used in blockchains are standardized. This means that these cryptosystems are thoroughly reviewed by a wider audience including experts from various fields related to cryptography. This reduces security risks either in the cryptosystem design itself or in implementations because standardized systems become well tested and vetted.

There will also be wider support from operating system vendors, hardware wallet vendors, and GPU vendors if these cryptosystems become standardized.

ii) The size of the public key + signature

The size of the publicKey+signature is important because, in typical proof-of-stake systems, validators need to send the signed transactions over the network and need to persist them on the disk. The higher this size, the lower the performance of the blockchain will be, because of higher network and storage requirements.

For example, let's consider a Falcon-512 key; each signature and public key requires 1.5 KB of disk space. In a proof-of-stake system that has 128 validators and 12-second block times, this would mean that just the signature attestation of validators will occupy 1.3GB of disk space in a full node.

iii) The speed and memory usage for the 'verify' operation

In typical proof-of-stake systems, validators might need to sign transactions just once or twice per block but need to verify the signatures of the other validators many times. Depending on the consensus model, this might need to be many hundreds of times per block or epoch. Hence it is important that the verify operation takes

as low a time as possible and is also efficient in memory usage so that the hardware requirement of the validator node is reduced.

iv) Resistance to Side Channel attacks

Blockchain nodes need to be online to send and receive transactions and keep the blockchain running. This opens the possibility of signing operations of the crypto scheme to be timed, opening-up remote side-channel attacks and/or physical proximity side-channel attacks.

For example, in mid-2022, HertzBleed ([24]), a paper that described a remote side-channel attack was published; the dynamic frequency scaling feature of modern x86 processors was used to take advantage to enable remote key extraction. SIKE, a candidate in Round 3 and Round 4 of NIST PQC was one such crypto scheme that was affected, though other cryptography schemes are also likely to be vulnerable to HertzBleed.

Hence, any crypto scheme used in blockchains for scenarios in which a signing operation can be timed, needs to be evaluated for side-channel attack resistance.

Quantum Coin Signature Scheme

While lattice based post-quantum cryptography schemes such as SPHINCS+ and Dilithium have been standardized, they haven't been battle-tested widely over the years like RSA and Elliptic Curve based crypto-schemes. It's possible that newer category of attacks on Lattice based cryptography may come to light.

Because of these reasons, it's preferable to use a hybrid signature scheme that uses two crypto schemes behind the scenes: a PQC scheme and a classical scheme (EdDSA). This hybrid model is required to provide a hedge against Lattice based cryptography schemes such as Dilithium getting broken on classical computers in the interim. In addition, SPHINCS+ which is hash based is also part of the signature scheme, to be used as a breakglass (details below).

When quantum computers capable enough to break EdDSA become available, the hybrid model will still provide protection against quantum computer attacks, since a post quantum crypto scheme is used in the hybrid model.

This hybrid model is abstracted away so that users do not have to worry about managing multiple sets of keys (wallets). To users, it will be just one composite key to manage and use. Likewise, higher-level developers do not have to worry about the hybrid model, since it will be abstracted away.

Some disadvantages of the hybrid model are increased complexity, increased risk of implementation bugs, increased compute time, increased storage, and bandwidth requirements. However, the security benefits of the hybrid model outweigh these disadvantages.

In Quantum Coin Mainnet, Dilithium (ML-DSA), SPHINCS+ (SLH-DSA) and ed25519 are used in a combiner mode. More details on the comment at https://github.com/DogeProtocol/hybrid-pqc/blob/main/hybrid-dilithium-sphincs/hybrid.c

Since SPHINCS+ signatures are large, thye do not fit requirements of many applications. Because of this reason, this hybrid scheme supports two modes of signing:

A compact mode in which a message hashed from the original message, the SPHINCS+ public-key (SPHINCS+-shake-256f-simple) and a 40 byte random nonce is embedded into the signature. If both Dilithium and ed25519 are broken in the future, the SPHINCS+ full signing mode can be required by the verifying applications, like a breakglass.

A full mode in which all the three signature schemes are used to create a signature (including the full SPHINCS+ signature).

State Proof Signing

To strengthen the quantum resistance of Quantum Coin blockchain, validators sign the proposal packet every 4096 blocks, using the full-mode detailed above. This means that SPHINCS+ (SLH-DSA), the strongest known quantum resistant digital signature scheme is leveraged to protect the blockchain. Even if Dilithium and ed25519 are broken in the future, the blockchain is still protected due to this periodic signing of proposal blocks.

Guardrails

Quantum Coin will use constant time implementations of crypto-schemes to provide guardrails against side channel attacks. For example, exchange hot wallet is a scenario in which a lot of signing operations need to be performed; while remote timing attack is not likely a problem in this scenario, physical proximity-based side-channel attacks may be a problem. Adequate documentation and guidelines will be provided for such scenarios, though needless to say relying on documentation alone will not suffice.

Multiple Digital Signature Scheme Support

The Quantum Coin blockchain itself will be extensible so that multiple digital algorithms can be used at any time. The signature will include additional context to indicate the signature algorithm used. This will enable the blockchain to dynamically detect the signature algorithm used for that account or validator. An important reason why this feature is required is that in the future if any vulnerability is found in one of the algorithms, the blockchain can switch to a newer signature scheme with minimal impact.

Key Rotation

Users and Validators will also be able to rotate their keys to a different signature scheme or to a new key in the same signature scheme. The rotation of keys periodically is a general security best practice, but in this case, the added advantage is that if a different algorithm is created in the future that can break current PQ cryptosystems, it’s easier for users of the blockchain to rotate their keys with lesser impact.

Code Checkpoints

In a highly unlikely but non-zero probability event that current PQ algorithms do get compromised in the near future, it becomes a risk to the Quantum Coin blockchain. This is because older blocks can be tampered with to forge signatures, even if validators and users are able to rotate their keys to a different signature scheme. This becomes a problem especially in the event when there isn't any lead time for users to switch to a more secure signature scheme.

To hedge against this unlikely event, the client node software will be periodically updated with hardcoded checkpoint hashes from a few random blocks, so that the integrity of the blockchain can be verified at runtime. While this is not an optimal solution, it is an optimistic hedge as a proactive measure.

Quantum Coin Communication Security

Kyber (ML-KEM) is a public key establishment scheme that was standardized on the conclusion of the NIST PQC program. Quantum Coin mainnet uses Kyber-512 for inter-node communication security and will switch to a hybrid quantum+classical key encapsulation scheme in future updates.

Conclusion

We studied various security risks that quantum computers pose to blockchains with current commonly used cryptosystems. We studied various post-quantum cryptosystems and then finalized on the appropriate digital signature scheme and communication encryption scheme to use for the Quantum Coin blockchain.

We also gave a brief overview of other security features such as signature scheme rotation, key rotation and code checkpoints that improve the security posture of the Quantum Coin blockchain from quantum computer threats. Overall, the community believes Quantum Coin will be one of the best equipped blockchains to handle security threats from quantum computers.

Addendum

"Quantum Coin" and "Quantum Coin Community" were previously known under the monikers "Doge Protocol" and "Doge Protocol Community" respectively.

References

1. Quantum Coin Vision Paper https://quantumcoin.org/whitepapers/Quantum-Coin-Vision-Paper-latest.pdf
2. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer https://arxiv.org/pdf/quant-ph/9508027.pdf
3. Grover's Algorithm https://en.wikipedia.org/wiki/Grover%27s_algorithm
4. NIST Post Quantum Cryptography Round 3 Submissions https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3submissions
5. Falcon https://falcon-sign.info/falcon.pdf
6. Dilithium https://pq-crystals.org/dilithium/index.shtml https://pq-crystals.org/dilithium/data/dilithium-specification-round3202 10208.pdf
7. Rainbow https://www.pqcrainbow.org/
8. Post-Quantum Digital Signature Cryptosystem Performance https://openquantumsafe.org/benchmarking/visualization/speed_sig.html
9. BLS Signature Aggregation https://eprint.iacr.org/2018/483.pdf
10. Digital Signature https://en.wikipedia.org/wiki/Digital_signature

11. Public Key Cryptography https://en.wikipedia.org/wiki/Publickey_cryptography
12. Proof of Stake https://en.wikipedia.org/wiki/Proof_of_stake
13. Proof of Work https://en.wikipedia.org/wiki/Proof_of_work
14. EcDSA https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm
15. Qubit https://en.wikipedia.org/wiki/Qubit
16. Assessment of Quantum Threat To Bitcoin and Derived Cryptocurrencies https://eprint.iacr.org/2021/967.pdf
17. Quantum Attacks on Bitcoin https://arxiv.org/pdf/1710.10377.pdf
18. How to achieve a McEliece-based Digital Signature Scheme https://www.iacr.org/archive/asiacrypt2001/22480158.pdf
19. Improved Cryptanalysis of UOV and Rainbow https://eprint.iacr.org/2020/1343
20. 21. MAYO: Practical Post-Quantum Signatures from Oil-and-Vinegar Maps
21. https://eprint.iacr.org/2021/1144
22. NIST Round 3 status report: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf
23. Breaking Rainbow Takes a Weekend on a Laptop: https://eprint.iacr.org/2022/214
24. Hertzbleed Attack https://www.hertzbleed.com
25. Warnings regarding cryptosystems https://ntruprime.cr.yp.to/warnings.html

26. Data Availability Whitepaper https://QuantumCoin.org/whitepapers/Quantum-Coin-Blockchain-Data-Availability-Whitepaper.pdf

27. SPHINCS+ https://sphincs.org

28.ed25519 https://ed25519.cr.yp.to/

29.Quantum Coin Hybrid PQC https://github.com/DogeProtocol/hybrid-pqc