Quantum Resistance in the Doge Protocol Blockchain

Authors: The Doge Protocol Community

Publication Date: October 2021

Table of Content

Contents

Introduction

Public Key Cryptography (also known as 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 popular digital signature schemes are the RSA scheme and Elliptic Curve based schemes such as ECDSA. Bitcoin and Ethereum (PoW) for example, use ECDSA.

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 proportionate 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 are able to do this since it will be too late for them to move to a quantum-resistant cryptographic scheme.

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, 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 widescale 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, nuclear facilities are no longer secure and might have to be shutdown temporarily.

The impact to 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 can no longer be trusted.

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, 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 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 to 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 to become even more centralized than it is now and the network hashrate 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 miners running the network (of which there will only be a few initially), it becomes a pseudo decentralized 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), 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 3 of the NIST PQC standardization effort, for digital signature schemes. However, Classic McEliece is one of the candidates in round 3 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 is a 'round 3' candidate in NIST PQ cryptosystems.

Post Quantum Digital Signature Schemes

The NIST post quantum cryptography program is a process to evaluate and standardize one or more quantum resistant public key algorithms. Standardization is important so that clients, servers, and cryptosystems worldwide including hardware devices adhere to a vetted and battle tested cryptography algorithm. While many candidates were evaluated as part of this ongoing program, three have been shortlisted to be PQ digital signature schemes. There will be further evaluation rounds before one or two of these schemes become the standard.

Dilithium

Dilithium is a lattice-based cryptography system that is based on hard problems over module lattices.

Falcon

Falcon is another lattice-based cryptography system. Falcon uses GPV framework, NTRU lattices and Fast Fourier Sampling.

Rainbow

Rainbow belongs is a multivariate cryptosystem. There have been some proposed attacks based on the “Kipnis-Shamir attack” and “MinRank Attack” that reduce the security of the Rainbow cryptosystem [20].

Limitations

It is preferred for digital signature cryptography schemes to have certain characteristics and functionality, for use 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 time, 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. Ziggy [10] is one such scheme that has been claimed to be quantum resistant but hasn’t been battle tested or standardized.

Recovery Phrases

Recovery Phrases also known as Mnemonic Phrases provides 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 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 Doge Protocol

Doge Protocol will provide quantum resistance in a two-fold manner. First, Doge Protocol will use a hybrid proof-of-stake system that will eliminate the need for Proof-of-Work mining using hashing. This will prevent the category of attacks made possible by Grover's algorithm.

Secondly, Doge Protocol will use one of the round 3 candidates for Digital Signatures, listed in the NIST PQ cryptosystems. This will be used for securing user accounts, validators and other accounts that will play a role in the Doge Protocol blockchain consensus system. Since validator nodes need to be online, the risk of compromising the node with other means 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. Three important criteria are used to evaluate the best PQ digital signature scheme to use.

i) <u>Standardization</u>

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 risks of 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, GPU vendors, if these cryptosystems become standardized.

ii) <u>The size of the public key + signature</u>

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, lets 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 disk space in a full node.

iii) <u>The speed and memory usage for the 'verify' operation</u>

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.

The following table shows a comparison of the 3 candidates from the NIST PQ shortlist for Digital Signature schemes. The reference implementation of these crypto schemes was used for these tests. The hardware and software configuration used for these tests are available under the references section ([8]).

Algorithm	Public Key Size (bytes)	Signature Size (bytes)	verify per sec
Falcon-512	897	666	19389
Falcon-1024	1793	1280	9147
Dilithium3	1952	3293	5333
Rainbow Level 1	161587	66	446

Based on the data from this comparison and evaluating the attack vectors, one of Falcon-512 or Falcon-1024 will be used in the initial release of Doge Protocol.

Multiple Digital Signature Scheme Support

The Doge Protocol 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. 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, its 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 Doge Protocol 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.

As 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.

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 to use for the Doge Protocol 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 Doge Protocol blockchain from quantum computer threats. Overall, the community believes Doge Protocol will be one of the best equipped blockchains to handle security threats from quantum computers.

References

1. Doge Protocol Vision Paper https://github.com/DogeProtocol/Doge-Protocol-Whitepapers/blob/main/Doge-Protocol-Vision-Paper-1.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-3-submissions
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-round3-20210208.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. Ziggy https://github.com/starkware-libs/ethSTARK/tree/ziggy
11. Digital Signature https://en.wikipedia.org/wiki/Digital_signature
12. Public Key Cryptography https://en.wikipedia.org/wiki/Public-key_cryptography
13. Proof of Stake https://en.wikipedia.org/wiki/Proof_of_stake

14. Proof of Work https://en.wikipedia.org/wiki/Proof_of_work
15. EcDSA https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm
16. Qubit https://en.wikipedia.org/wiki/Qubit
17. Assessment of Quantum Threat To Bitcoin and Derived Cryptocurrencies https://eprint.iacr.org/2021/967.pdf
18. Quantum Attacks on Bitcoin https://arxiv.org/pdf/1710.10377.pdf
19. How to achieve a McEliece-based Digital Signature Scheme https://www.iacr.org/archive/asiacrypt2001/22480158.pdf
20. Improved Cryptanalysis of UOV and Rainbow https://eprint.iacr.org/2020/1343