BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2024
http://excel.fit.vutbr.cz

Blockchain Resistant to Quantum Attack

Michal Ľaš*

Abstract

New quantum computers may have the ability to compromise currently used cryptography. This threat significantly impacts blockchain technology, which relies on various cryptographic principles. This paper aims to analyze vulnerabilities, identify solutions to achieve security in the post-quantum (PQ) era, design and implement a PQ blockchain, and test its performance. The key lies in securing the compromised blockchain components and utilizing new PQ cryptography. The proposed design focuses on the utilization of these principles. The important results are the analysis of quantum vulnerabilities for blockchains, solutions to address them, and the analysis of suitable PQ algorithms for blockchains. Finally, the designed implementation presents a performance comparison of new PQ and currently used cryptography algorithms in the blockchain.

*xlasmi00@stud.fit.vutbr.cz, *Faculty of Information Technology, Brno University of Technology*

1. Introduction

[Motivation] To ensure that blockchains can withstand the age of quantum computers, it is necessary to adapt to quantum computer's threats. The main concern lies with the asymmetric cryptography currently in use, although there could be other threats to the blockchain. Fortunately, institutions such as the National Institute of Standards and Technology (NIST) are actively working on establishing new standards for cryptographic algorithms that are secure against both quantum and classical computers. However, these new algorithms are more complex compared to the currently used ones. This raises the question of how implementing these new algorithms will impact the performance of blockchains.

[Problem definition] The problem mainly lies in securing the blockchain against quantum attacks, which are mainly related to current cryptography. Individual threats for blockchains summarize Listing 1. The primary threat to current cryptography arises from Shor's and Grover's algorithms, specifically designed for quantum computers. Shor's algorithm [1] can efficiently solve large number factorization and the Discrete Logarithm problem. This poses a risk to RSA, DSA, and elliptic curve algorithms. In the context of blockchain, such a compromise could threaten the integrity of each transaction, given that each transaction typically involves a digital signature. On the other hand, Grover's algorithm [2] can search an unsorted database with complexity $O(n^{1/2})$ [3]. This algorithm can be used to efficiently search for collisions in currently used hash functions. In blockchains utilizing the Proof-of-Work (PoW) concept, a quantum computer could gain a significant advantage, potentially outperforming classical computers in mining and thus dominating the blockchain network. Additionally, In theory, it would be also possible to exchange a blockchain block for another with the same hash but different content. Such hash collisions can cause a loss of integrity for the entire blockchain.

[Existing solutions] Many current blockchain implementations hesitate to adopt new PQ algorithms due to notable performance drawbacks and the absence of finalized standards. Nevertheless, certain blockchains, such as IOTA or Quantum Resistant Ledger (QRL), have already integrated standardized stateful PQ digital signature algorithms. However, these algorithms, being stateful, bring along their own set of drawbacks.

[Our Solution] The main focus is on integrating new PQ cryptography into blockchain technology also with a quantum-resistant consensus mechanism. The objective is to analyze blockchain components vulnerable to quantum attacks, identify appropriate PQ algorithms, and practically implement them within the blockchain.

2. Cryptography for Blockchains

For a PQ blockchain, it is crucial to select suitable cryptography resistant to the capabilities of quantum computers. Several notable institutions, including NIST, the Czech *Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)*, and the American National Security Agency (NSA), have already provided recommendations for PQ cryptography. Among the most critical aspects of blockchains are hash functions and digital signatures.

When it comes to hash functions, the solution is relatively straightforward. It is generally advised that the hash function possesses an output length of 384 bits or more. There are several well-established and validated algorithms available to choose from.

For asymmetric cryptography, the solution is no longer so simple. These cryptographic processes often rely on mathematically challenging problems that quantum computers can effectively solve. Consequently, ongoing efforts involve the development of new algorithms designed to withstand even the computational power of quantum computers. The earlier mentioned NIST competition is specifically dedicated to advancing solutions in this area.

The most interesting algorithms are the finalists of this competition. In the digital signatures category, these are Dilithium, Falcon, and SPHINCS$^+$. Among these, Falcon and Dilithium stand out as the most promising, offering excellent performance along with optimal key and signature sizes.

3. Post Quantum Blockchain

Considering the threats listed in Listing 1, it is important to secure the following parts of the blockchain:

- *Block hashes* – Each block in a blockchain contains a hash representing data within that block, as well as the hash of the previous block. To ensure PQ resistance it is crucial to employ a hashing function with an output length of at least 384 bits.
- *Transaction signatures* – Each transaction in a blockchain must feature a PQ digital signature to ensure its integrity.
- *Consensus mechanism* – In the case of the PoW consensus mechanism, it is advisable to use a PoW variant that does not grant quantum computers an advantage over classical ones. An Example of such a consensus mechanism can be the Lattice-based Proof-of-Work (LPoW). In the case of Proof-of-Stake (PoS) as well as other consensus mechanisms that use the concept of randomness, it is important to choose a reliable random generator. Theoretically, PQ computers will be able to find the deterministic nature of the pseudo-random generation, as long as this process is based on the phenomenon of classical physics [4]. Some consensus mechanisms also use digital signatures. As for transactions, it is crucial to use PQ digital signature algorithms.

The design of the implemented PQ blockchain is illustrated in Figure 2. The most important components are transactions and the consensus mechanism. Furthermore, the entire implementation employs the SHA-512 hash function. Transactions utilize PQ digital signatures Falcon or Dilithium. For comparison purposes, currently utilized algorithms like ECDSA and Ed25519 are also integrated. The consensus mechanism employed is the XRP Ledger Consensus Protocol, as detailed in [5], which operates as a federated Byzantine agreement consensus. Unlike traditional methods such as PoW, PoS, or randomness, this consensus relies on the cooperation of individual validators. However, it uses digital signatures so there will be used the same PQ algorithms as for transactions.

4. Testing & Results

The primary aim of the testing was to compare the performance of the new PQ algorithms with the current ones. Specifically, all versions of the PQ algorithms Falcon and Dilithium were compared. The testing involved varying numbers of nodes: 3, 5, 10, 15, or 20, with each node generating 20 transactions. The key metrics monitored included the number of processor cycles during program execution Chart 3A, The amount of memory allocated by the program Chart 3B, and the volume of data sent/received by individual nodes Chart 3C.

5. Conclusions

The results obtained align with our expectations. Increased algorithmic security requires higher performance demands. However, the crucial takeaway is that PQ algorithms do not exhibit significant slowdowns compared to the currently employed ones. The primary challenge lies in the size of PQ keys and signatures, particularly in blockchain applications where data is frequently distributed across the network. Nevertheless, further testing with a larger number of nodes and executed transactions is deserved for future assessments.

References

[1] Peter Williston Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, page 124–134, Santa Fe, NM, USA, 8 1994. IEEE Comput. Soc. Press.

[2] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96*, page 212–219, Philadelphia, Pennsylvania, USA: Association for Computing Machinery, 7 1996.

[3] Ritik Bavdekar, Eashan Jayant Chopde, Ankit Agrawal, Ashutosh Bhatia, and Kamlesh Tiwari. Post quantum cryptography: A review of techniques, challenges and standardizations. In *2023 International Conference on Information Networking (ICOIN)*, pages 146–151, Bangkok, Thailand, 2023, 2 2023. IEEE Comput. Soc. Press.

[4] Marcin M. Jacak, Piotr Jóźwiak, Jakub Niemczuk, and Janusz E. Jacak. Quantum generators of random numbers. *Scientific Reports*, 11(16108), 8 2021.

[5] Dave Cohen, David Schwartz, and Arthur Britto. Xrp ledger. online, 05 2019. https://xrpl.org/docs/concepts/consensus-protocol/.