Post Quantum Cryptography Effects On Bitcoin Blockchain

Elsa Velazquez Dr. Daniel Massey Dr. Hunter Albright Dr. Eric Rozner Dr. Jim Curry
University of Colorado, Boulder

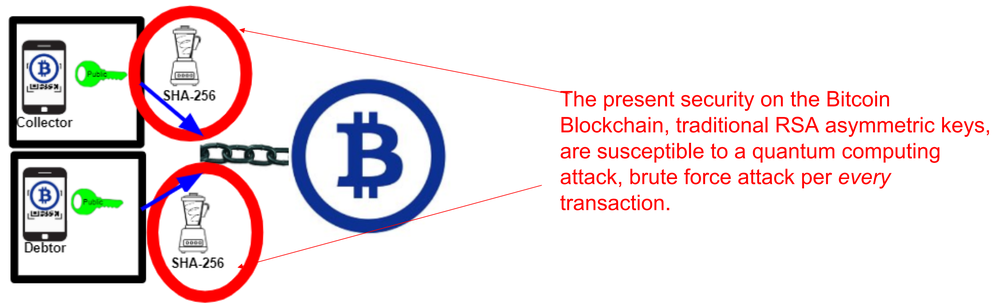
Objectives

- Demonstrate how post-quantum cryptography invalidates Blockchain technology.
- Incorporate quantum-safe cryptography into Blockchain.
- Produce a roadmap for quantum-safe Blockchain.

Challenges

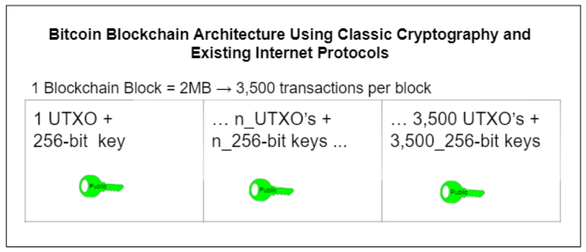
- Architectural limitations within Blockchain
  - ➢ Quantum-safe key sizes exceed the block size limits
  - ➢ There is no mechanism for increasing size limits to fit larger keys
    - Sending keys in multiple blocks will cause a segregation of the transactions from the information in their block, in essence creating the same limitations as failed segWit attempts
- Resource requirements
  - ➢ There is not a fully-vetted, functional internet protocol layer that can handle larger block sizes to include quantum sized keys plus increasing block sizes
- Scaling requirements
  - ➢ Making either smaller or more transactions is at a monetary loss
- Social ramifications
  - ➢ Gaining consensus from the Bitcoin community to change the underlying blockchain architecture has, historically, not been accepted by the entire community
  - ➢ The only way to make an impact in blockchain tech that allows for PQC is by gaining >50% consensus

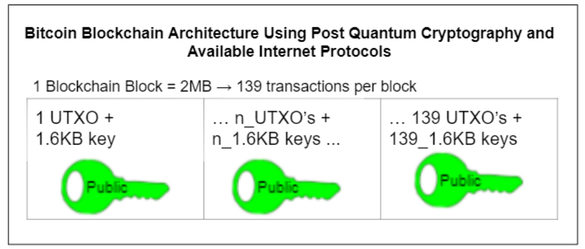
Where are the vulnerabilities in a blockchain?



For every transaction, public addresses are typically available to any node on the network. By leveraging quantum computing, it is possible to quickly determine the very large prime numbers used to create the asymmetric key pair. These prime numbers can then be hashed, which would allow an attacker to determine the private key via a brute force attack on the target's wallet address.

Why not just make the blockchain bigger?





Current internet protocols have already proven difficult when using post-quantum keys, as they exceed bandwidth and have a high drop rate. Segregated witness efforts, where the keys are separated from transactions, have not been shown successful and are not always accepted by the blockchain community because it violates the check for solvent transactions.

Our Results

- A demonstration of how quantum computers break the current blockchain.
  - ➢ Simulated quantum computer and blockchain
  - ➢ Working quantum code at small scale
- Potential Solution 1: Rely on Merkle Roots
  - ➢ Using a one-time, quantum-safe hashing algorithm, will have smaller key sizes
    - Caveat: The user takes responsibility for changing keys every transaction
- Potential Solution 2: Rely on Quantum-Safe Hardware
  - ➢ Store the local Blockchain node on quantum-safe hardware, providing an external firewall
    - Caveat: Quantum-safe hardware is not yet publicly accessible
      - Making the hardware relies on the NIST Quantum-Safe algorithm selection process and updates to internet protocols

Acknowledgements

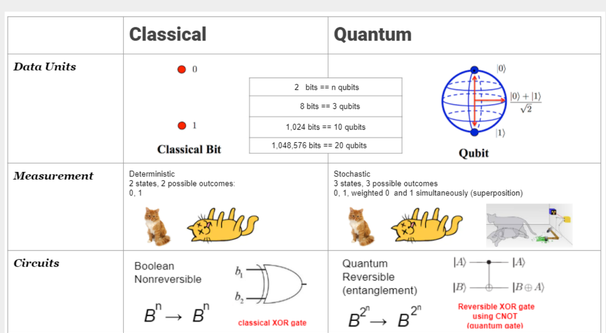
Our research was made possible by the support of Dr. Dan Massey, my thesis committee, CU Boulder, Seagate, the NIST PQC committee, Wajahat Ali, Aung Than, and Meherzad Aga from Seagate, and the CRYSTALS Dilithium developers.

Background

❖ Blockchain Overview

A blockchain is a permanent, digital transactions ledger of inputs and outputs that allows solely for solvent transactions between parties without the need of a bank or other third party. In place of the trust granted to banks, the blockchain architecture relies on peer to peer networks, complex math problems that chain together, and cleverly coded processes to verify all transactions are solvent.

❖ Quantum Computers



❖ Quantum Cryptography