A Proposal for the Implementation of a Quantum-Safe Proof-of-Work for Blockchain Technology Utilizing SPHINCS-256

Bryce Weiner
bryce@altsystem.io

Abstract. The greatest existential threat to cryptocurrency networks is quantum computing. A unique implementation of the SPHINCS-256 stateless, hash-based cryptosystem offers a route by which cryptocurrency networks would require an algorithm substitution to preserve network integrity and remain a fungible means of settlement.

Keywords: post-quantum cryptography, one-time signatures, few-time signatures, hypertrees, vectorized implementation, cryptocurrency

Introduction

Prominent Bitcoin developers have noted[2] that the coming onset of consumer quantum computer is a serious threat to the elliptic curve cryptography employed by the Bitcoin network to secure users' funds. However, less attention has been given to the problem that a sufficiently large enough quantum computer can trivialize the proof-of-work system which utilizes an implementation of the SHA-256 hashing algorithm. As proof-of-work is a simple numeric comparison, it is easy to conceive of a scenario where a sufficiently powerful quantum computer could trivialize the generation of the requisite hash value to a "Perfect Nonce": a factorization method which consistently and efficiently produces a golden nonce[3] regardless of the current network difficulty. This paper suggests a quantum-safe alternative which provides identical functionality to the existing system and yet provides the requisite complexity to withstand the application quantum computing into the indefinite future.

SPHINCS-256 based poof-of-work

A SPHINCS-256 based proof-of-work requires some modifications to the existing proof of work process to accommodate the specifics of the SPHINCS methodology existing at the time of this writing.

1. Generating the target nonce

As a one-way SPHINCS-256 hash function does not exist at the time of this writing, a deterministic bare public key[4] (DBPK) is generated upon program execution for the creation of the target proof-of-work hash. As a bare public key is created from a zero-knowledge proof without a corresponding private key, it is possible to then generate a SPHINCS-256 one-way hash of any given value suitable for use as a target hash value for proof-of-work.

2. Searching for the golden nonce

The golden nonce for the generated target hash is computed by first generating a standard 32-bit SHA-256 hash to which is then applied SPHINCS-256 encryption utilizing the network DBPK, identical to the means by which the target hash was created. Following existing standards, if the resulting hash value is lower than that of the target value, the proof-of-work problem is considered "solved" the processing of a block by that miner is permitted.

References

1. Daniel J. Bernstein, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O'Hearn - SPHINCS: practical stateless hash-based signatures (accessed 2015-12-02) http://sphincs.cr.yp.to/sphincs-20150202.pdf
2. Vitalik Bueterin, Bitcoin is not quantum-safe, and how we can fix it when needed (accessed 2015-12-02) https://bitcoinmagazine.com/articles/bitcoin-is-not-quantum-safe-and-how-we-can-fix-1375242150
3. (accessed 2015-12-02) https://en.bitcoin.it/wiki/Nonce
4. Leonid Reyzin, Zero-Knowledge with Public Keys (accessed 2015-12-02) http://groups.csail.mit.edu/cis/theses/reyzin-phd.pdf