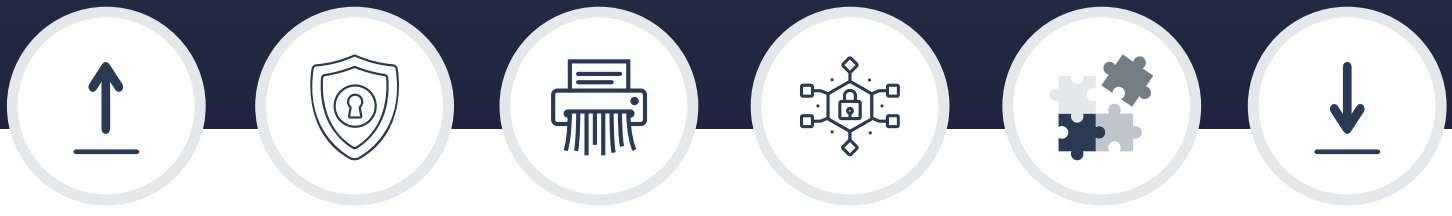
SOLLENSYS™ Making the World Safer, One Block at a Time

The Impending Threat of Quantum Computing on Blockchain Security

Published February 14, 2022



The Impending Threat of Quantum Computing on Blockchain Security

Published February 14, 2022

OVERVIEW

Blockchain technologies provide an open, public, distributed ledger which has many promising applications. However, any new cryptographic application should consider anticipated technological development expected to occur within the lifespan of any potentially deployed systems, especially those of secure data storage and of strategic technical importance. Technological advancements promise the development of computers that process information not according to the rules of classical physics and probability, but according to the governing physics of quantum mechanics. This portends a dramatic increase in computational capacity for specific problems, such as function inversion via Grover's algorithm, and factoring large numbers into prime factors via Shor's algorithm. The computational data structure known as a blockchain provides an open, public (sometimes private), distributed ledger that has many interesting applications, including digital currencies. The security of this ledger depends on the difficulty of solving certain cryptographic problems which are readily undermined by the potential of quantum computation. Specifically, hashes as used in signing the blocks of the ledger can be compromised, as can any public/private key system which relies on the hidden subgroup problem.

THREAT ASSESSMENTS

Sollensys is researching and developing cryptographic standards and tools to counter the threat of quantum computation, primarily to combat two specific threats:

1. The principal threat is a dramatic speed increase in function inversion, for example with Grover's algorithm. This allows the generation of a modified pre-image from a hash collision allowing a signed data block to be modified. This threat voids guarantees of authenticity of the ledger entries undermining and compromising the entire blockchain. The speed-up due to Grover's algorithm is a factor of the square root of the number of possible hashes, meaning that a hash subjected to quantum attack would only be as secure as one with half as many bits subjected to classical, non-quantum attack.
2. The second threat is Shor's algorithm, which applies to any aspect of blockchain that relies on asymmetric key cryptography. The most referenced problem is that of breaking RSA encryption. RSA relies on the ease of multiplying prime numbers in contrast to the difficulty of factoring large numbers into prime factors. Shor's algorithm speeds-up this process exponentially, effectively breaking RSA encryption. Variants of Shor's algorithm do the same for other asymmetric key cryptosystems.

To counter these threats, Sollensys has commenced on developing quantum-resistant (postquantum) cryptographic tools. Post-quantum cryptography is rapidly expanding but has a great deal of uncertainty and no developed uniformly recognized or agreed upon standards. Additional research is needed to develop quantum informational versions of systems like blockchain. The most established quantum application is Quantum Key Distribution (a.k.a. Quantum Cryptography), which promises guaranteed secrecy of a given degree for cryptography, despite potential eavesdropping even if the eavesdropper is equipped with a quantum computer. More exotic developments at Sollensys involve using quantum states to represent information, such as quantum currencies, and would require development of easily used quantum state storage.

SUMMARY

Although quantum computing is not yet developed to a high technology readiness level, neither are the defenses against the algorithms that quantum computation promises. Recent advances in quantum computer hardware capabilities suggest a rapidly shifting landscape in which quantum computing poses a systemic threat to blockchain integrity and security viability. The Sollensys team is currently examining vulnerabilities of blockchain technology manifested by the development of quantum computers and has developed recommendations on how to make blockchain more resistant to such technological advances.

sales@sollensys.com | 1 (866)-438-7657