The development of large-scale quantum computers will threaten the security of computer networks and services that depend on public key encryption, including Smart Ledgers. How real is the threat and how and when should we start preparing for it?

Overview
The post-quantum cryptography (“PQC”) problem will threaten the security of the world’s computer networks when large-scale quantum computers become available. The problem exists because such quantum computers would be able to break the security of widely-used public key cryptography, which allows remote parties to communicate securely and authenticate transactions and data without sharing a secret key in advance. It is uncertain when (and if) such quantum computers will become available - the nearest estimates are 10 to 15 years.

Fortunately, there are good solutions to the PQC problem, and better ones are emerging. The hard questions for individual computer system operators involve when and how to address the PQC problem, given its uncertain timing and the evolving solutions.

The report explains the PQC problem in detail for both non-technical and technical readers, starting with the essentials of cryptography, quantum computing, and how quantum computing threatens public key cryptography. We then consider the available solutions to the PQC problem, and provide frameworks for deciding when and how to respond to it.

Report Extracts

Classical versus Quantum Computers
In a classical computer, eight bits of memory (or one ‘byte’, often corresponding to one character) can hold any of $2^8 = 256$ different values. In a quantum computer, eight entangled qubits (quantum bits) hold all 256 values at the same time, and a program running on the computer could theoretically determine in a single step which of the 256 states is most likely.

<table>
<thead>
<tr>
<th>Risks to Blockchain Architectures from Quantum Computing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transactions</strong></td>
</tr>
<tr>
<td>Read historical records without authorization</td>
</tr>
<tr>
<td>Alter historical records</td>
</tr>
<tr>
<td>Spoof ongoing records</td>
</tr>
</tbody>
</table>
**The Mosca Inequality**

For each system:
- If $X + Y < Z$, there is time to act
- If $X + Y > Z$, it may already be too late to entirely avoid the post-quantum cryptography problem

Some systems may fall into the second category—a particular issue for Blockchain/Smart Ledgers, where $X$ is very large.

**Conclusions**

The sky is not falling. However, action may be appropriate now for Smart Ledgers and other computer systems that (i) are new (to avoid later redesign), (ii) have large consequences associated with insecurity and/or (iii) require security of long duration.

**Framework for Addressing the PQC Problem**

- **Resource**
  - Identify and acquire skills and resources

- **Monitor**
  - Monitor quantum computing and PQC solutions

- **Assess**
  - Assess quantum risks to systems

- **Plan**
  - Plan solution to identified risks

- **Implement**
  - Implement planned solution

Risk assessment affects resource and monitoring requirements. Plan feeds back to ongoing assessment and affects resource requirements.

To learn more about this and other Distributed Futures projects

- www.distributedfutures.net
- www.longfinance.net/Publications.html

You can contact us at hub@zyen.com