EPA ASIA

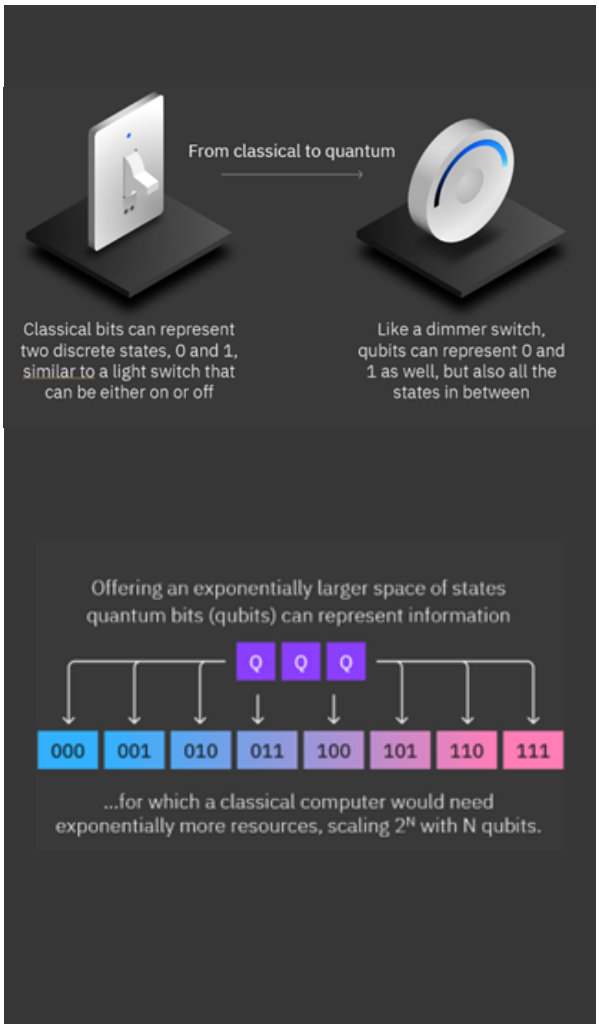
EXECUTIVE LUNCH
QUANTUM SAFE AND PAYMENTS

In collaboration with

OCTOBER 2023

The EPAA recently held a lunchtime roundtable discussion in Sydney regarding the impact of quantum computing on payments and financial services. To both educate the audience and catalyse the discussion, Ray Harishankar, an IBM Fellow leading IBM Quantum Safe[CN1] , made a presentation on the topic, with assistance from Mary Ann Francis, an Industry Advisor to EPAA. This article seeks to capture some of the key points covered in the roundtable.

Ray noted that Quantum computing moves us from the old binary world of 1s and 0s (bits), and into a world where values can exist as 0,1 and states in-between 0 and 1. He provided the great analogy of going from an on/off light switch to a dimmer switch.



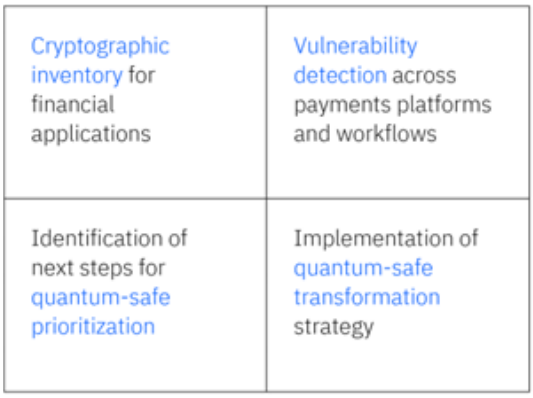
Interestingly, some problems (such as multiplying two numbers) are better solved by the traditional binary computing systems that we all use today, but others, such as factorization of large numbers and problems where optimization across many different parameters and unknowns come into play, are better addressed by the more probability-driven Quantum computing approach. An example would be Monte Carlo simulations, where Quantum computing should offer faster outcomes and allow a significantly increased range of inputs.

But don't expect to be carrying around your own Quantum laptop computer any time soon, as the superconducting qubits in these quantum computers have to be held at temperatures close to zero Kelvin degrees or Absolute Zero to operate. Hence very few of these Quantum computers exist today, but their number, capabilities, and access via the cloud are expanding.

What has any of this got to do with payments and financial services? The issue is security, and particularly the current ubiquitous use of cryptography or encryption. Current encryption methods secure the details of payment credentials and transactions through the fact that traditional binary computing systems are very slow at factorization of very large numbers. Ray suggested that to factor (i.e. $N=p*q$) 2048-bit integers would take about 4.7 billion CPU years - by which time the payment credentials will have expired and the payment will be long gone. But put a Quantum computer (using 6,190 qubits) on the job, the time to crack the factoring problem drops to about 8 hours.

Fortunately this encryption breaking capability is not upon us yet, because the number of qubits available in current quantum computers remains limited and therefore the ability to crack the encryption is yet to be achieved. However, the qubit number and performance [CN1] in these machines is growing, and several studies and US governmental agencies estimate that by the early 2030s new "Quantum-safe" standards will be required for national security systems in order to defend against these threats. Due to the cost and complexity of these encryption cracking machines, the threats are likely to come from nation-state backed organisations - which is not good news.

Even though the threat may be some years away from becoming real, payments and financial services companies need to be taking action now. This is because data records put in place today, which could still have value in the future (such as identity credentials), might be harvested by "bad actors" in the near term and held for decryption in the long term. Ray put forward some ideas from IBM Quantum Safe for financial services, as follows:



The international card schemes (e.g. Visa, Mastercard) are already addressing this future threat. These schemes have used 3DES to encrypt and decrypt payment card data, but are moving to adopt the Advanced Encryption Standard (AES), which was introduced by the National Institute of Standards and Technology (NIST) in 2001 and is used widely throughout the U.S government. This symmetric encryption, or more specifically AES-256, is believed to be quantum-resistant. That means that quantum computers are not expected to be able to reduce the attack time enough to be effective if the key sizes are large enough. In Australia, AusPayNet is leading an AES Migration Program[1], with work already commenced on the first six months of the "Initiation and Mobilisation" phase, focused on the technical blueprint and options to approach the migration.

It should be noted that asymmetric and symmetric cryptography are typically used in conjunction with each other. i.e., a communication using asymmetric cryptography is used to retrieve the symmetric key and then that symmetric key is used to encrypt data. Hence, ensuring that the asymmetric key retrieval mechanism is quantum-safe is critical to ensuring that the eventual symmetric encryption of data is also quantum safe.

The roundtable audience had a number of questions for Ray, including: where vulnerabilities might be? what immediate actions were required? when would the threat become real? and many more.

The key takeaway was that the time to act is now, because your current data could be exposed today to the longer term Quantum threat of Harvest Now Decrypt Later.

The EPAA plans to establish a work grouping on "Quantum Safe" in order to help participants in the payments industry to collaborate and address the ticking clock that is the "bad guys" gaining access to a cryptographically relevant quantum computer and cracking the codes.

EPAA is looking further into the topic of Quantum Safe during 2024. Please express if you have an interest in participating in the Quantum Safe Task force once it's established.

About the author Lance Blockley

Lance Blockley is Managing Director of The Initiatives Group, a consulting firm specialising in payments. He has advised issuers, acquirers, third-party processors, technology providers and payment associations in addressing many of the financial sector's most significant issues. He has over 35 years' experience in senior management and consulting in the UK, USA, Asia and Australia.

We always turn to our members for thought leadership

Thank you