THE ROAD TO QUANTUM SAFE PAYMENTS

The quantum computing era is unfolding and the need for the development of quantum-safe payment capabilities is immediate.

Scan the QR code to download a digital copy of the Executive Briefing - The Road to Quantum Safe Payments

The global financial system relies on the secure movement of money and data via digital and electronic communication, increasingly shifting real-time, to ensure trust for customers, financial institutions, networks and regulators. Cryptography is commonly used in payments systems, underpinning both virtual and physical rails, to protect the exchange of value and identity from unauthorized access, modification or redirection.

In study after study, payments is recognized as 30-45% of an FI's revenue, requiring consistent and on-going monitoring, investment and strategy in both technology and product solutions. Technology is only part of the solution.

The rapid evolution of quantum computing capabilities has the potential to render widely used public key cryptography schemes, such as RSA, obsolete within the next five to eight years. Business, technology, and security leaders face an urgent need to develop a quantum-safe strategy and post-quantum roadmap now.

The World of Payments

The payments ecosystem is vast and complex. There are five (5) core payment types: cash; cheque; EFT (wire transfer and bulk); card; and crypto currencies. There are numerous rails behind the payments and data movement, delivered via numerous systems or providers in the front, middle and back. All varied by jurisdiction and participants.

To example the complexity, AusPayNet has indicated migration of Australian card payments to a private key cryptography scheme (i.e. AES) will be a significant industry effort requiring an estimated six to seven years to complete[1].

"FI's and clients seek security and solutions for the front-middle-back processes of the complex ecosystem. Quantum (and AI) can address all parts of the dynamic. Focus needs to be on flows, not just the bottom of the triangle."

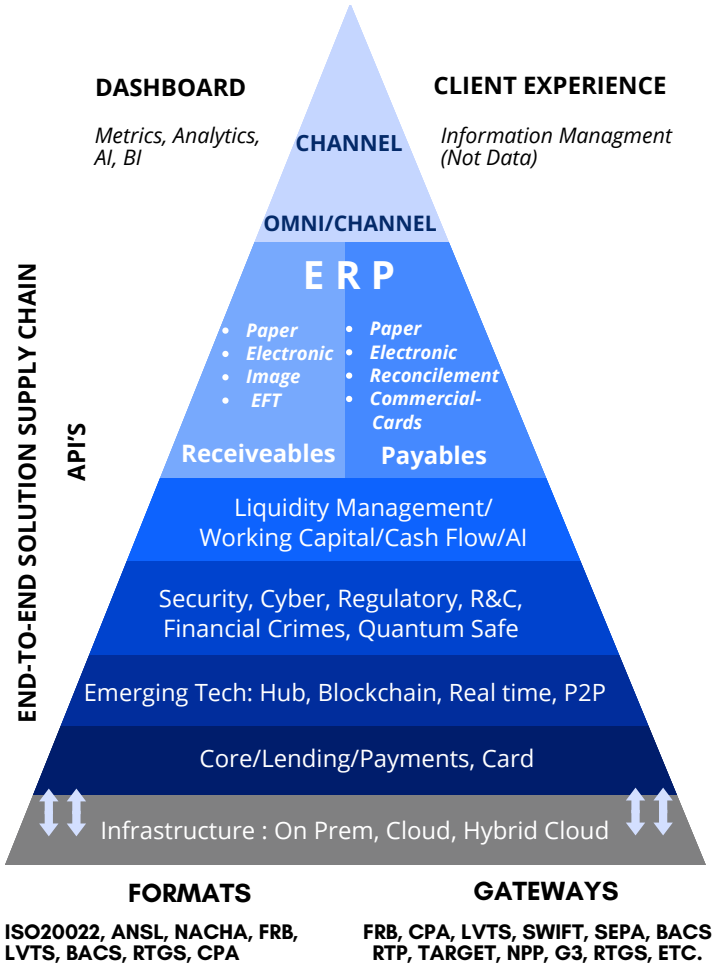

Figure 1. Payment Ecosystem

Figure highlights the complexity that exists upstream and downstream.

The Quantum Era

Quantum computers that harness the laws of quantum mechanics have the potential to solve certain mathematical problems exponentially faster than traditional computers to bring substantive transformation to a diverse range of industries. At the same time, the potential to break some of the commonly used encryption and digital signature algorithms poses a major cybersecurity concern.

The security of financial transaction and sensitive data that financial institutions ("FIs") process could be at risk with the advent of these cryptographically relevant quantum computers ("CRQCs")[2]. Further, Quantum Mechanics and AI, together, have the power to not just compute, but to create.

Significant progress is being made by companies and nations delivering milestones and research breakthroughs in the fields of quantum computing algorithms, performance, error correction and materials science. As quantum computing matures, banking services affected by cryptography concerns include:

- Online Banking, E-wallets
- Cards, Corporate and Consumer
- Clearing and Settlement Systems (SWIFT, Central Banks)
- Commercial Banking, Treasury, Liquidity, Capital Management, Cash flow/cash position, Reporting
- Securities Transactions (stocks, bonds, money markets)
- Custody, Collateral and Document Management Operations

Custodians of Trust and Opportunity

The payments ecosystem has an opportunity to secure the money and identity of consumers and businesses from breaches, fraud and scams, ensuring financial and social well-being, as well as being prepared for "Y2Q".

Forward-leaning companies are preparing for a quantum-safe computing future and positioning themselves to capture benefits including:

- New offerings or solutions – e.g. quantum-safe fraud tools using Ai and Quantum, in a real-time world
- New revenue opportunities – e.g. add-on payments security or data management capabilities
- Reputation as a competitive differentiator [3]

The Time is Now

The threat is today. The impact is in the future.

All data and monies, past, present, and future that is not protected with quantum-safe security will be at risk, and the longer migration to quantum-safe standards is delayed the greater proportion of data will be at risk from "harvest now decrypt later" threats.

The Global Industry is Readying

Governments, regulatory bodies and FI's around the world are already establishing guidelines and offerings for the transition to quantum-safe cryptography:

- In February of 2024, the Monetary Authority of Singapore (MAS) issued an Advisory on Addressing the Cybersecurity Risks Associated with Quantum;
- The US National Security Agency (NSA), US Cybersecurity and Infrastructure Security Agency (CISA), and the US National Institute of Standards and Technology (NIST) have jointly issued a "Quantum-Readiness: Migration to Post-Quantum Cryptography" fact sheet to encourage forward planning for the quantum-safe transition; and,
- NIST has established four new standards for quantum-resistant cryptography, enabling a global security industry technical pathway.

Financial system regulators will be expected to follow national agency recommendations to anticipate quantum security risks in the financial services industry.

Call to Action

- Understand the risks and the opportunities
- Upgrade your encryption
- Monitor your data and offer to support monitoring for your clients
- Include and educate the team: C-suite, LoB, Support, Security, IT and Ops
- Collaborate with experts
- Get involved is spaces, like a Work Group, where info can be shared

EPAA has established a Working Group on Quantum Safe Cryptography to shape the development of the post-quantum payment economy and ensure the payments ecosystem is adequately equipped to act on the topics of post-quantum governance and security, thereby maintaining the integrity of the payment systems and associated liquidity capabilities.

To get involved contact EPAA now for more information info@emeringpaymentsasia.org