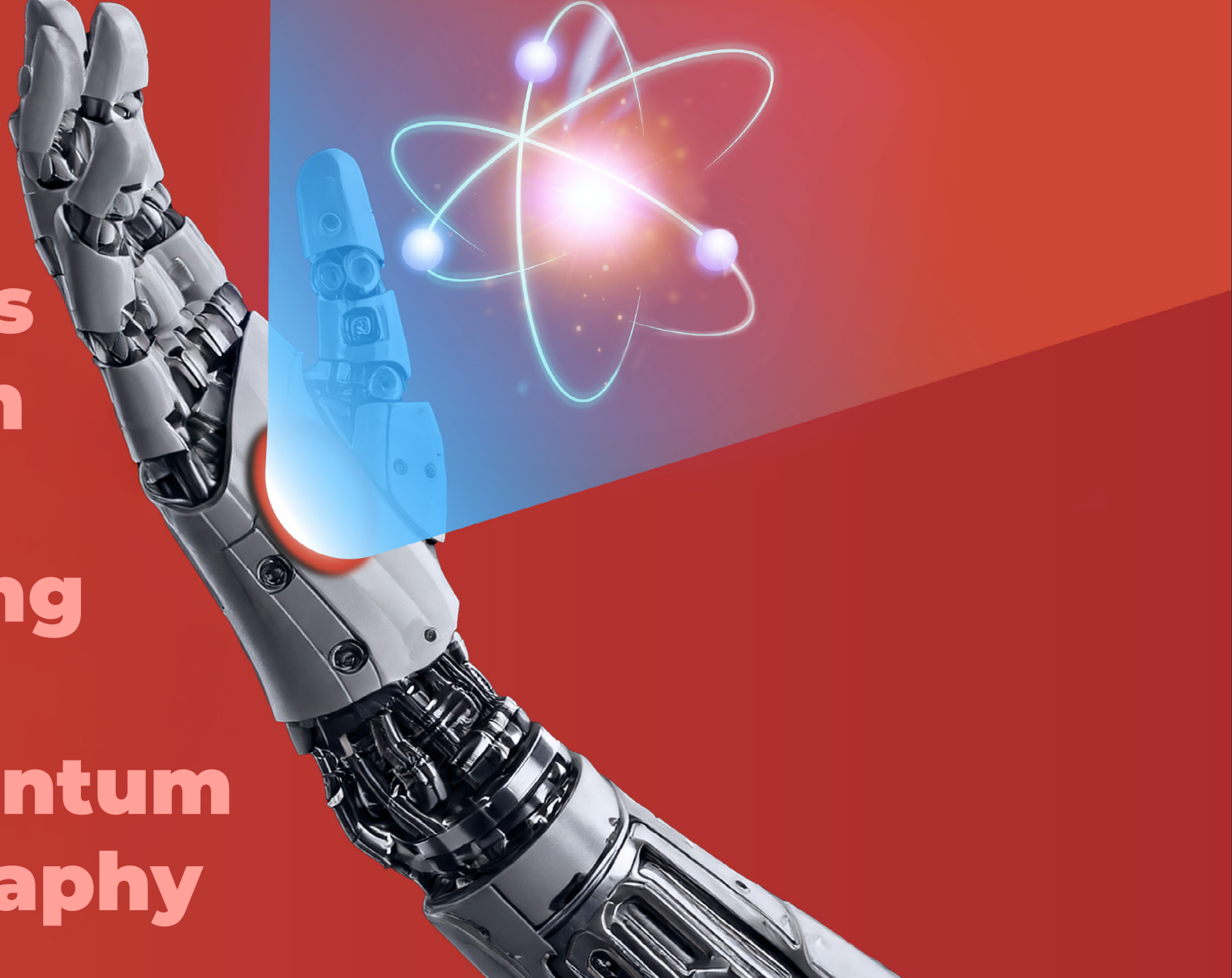
Shaping Banking's Next with Edge Computing and Post-Quantum Cryptography



While the banking industry continues to focus on widely discussed trends like cloud and AI, several nascent technologies are quietly advancing with the potential to reshape the financial ecosystem in the coming years. Edge computing and post-quantum cryptography (PQC) are two such technologies that are not yet mainstream but are gaining momentum. As the demands for faster, more secure, and efficient systems increase, these emerging technologies will address critical challenges in data processing, cybersecurity, and customer experiences. We expect banks to focus more on these technologies in coming years to equip themselves better.

Edge computing will enable banks to process data closer to the source, ensuring real-time insights, reduced latency, and enhanced security—a game-changer for fraud detection and personalized experiences. Meanwhile, post-quantum cryptography will address the imminent threat posed by future quantum computing advancements, which could render today's encryption methods obsolete. By adopting quantum-safe encryption algorithms, banks can safeguard their transactions and customer data against future cyber threats. In 2025 and beyond, banks will progress further in these technology areas, ensuring better preparedness to safeguard their operations, protect customer trust, and drive sustainable growth.

Industry Trendline

Global spending on edge computing to exceed $378 billion by 2028.
IDC

52% of organizations are already assessing their quantum-related vulnerabilities, while another 30% have begun implementing risk mitigation measures

Deloitte

Technologies at gradual pace but strong proposition for banks in 2025 and beyond

Edge Computing to address the need for speed, security, and efficiency

Post-Quantum Cryptography to secure banks in Quantum Era

Edge Computing to Address the Need for Speed, Security, and Efficiency

Most banks today have some form of cloud strategy in place today – moving away from on-site infrastructure. However, the right path forward is to ensure distributed workload storage and management across multiple infrastructure points from scalable remote data centers to on-site points at the edge. Edge computing allows enterprises to process data much closer to where data originates, enabling speed, security, and efficiency. Balancing workloads across cloud and edge infrastructures enables banks to optimize latency, data privacy, and security, tapping into real-time analytics for instant decision-making.

2025 and beyond will see edge computing adoption in the banking sector accelerate, driven by a combination of enhanced customer experiences, real-time analytics, and cost efficiency. Research predicts that over 40% of larger enterprises across industries will integrate edge computing into their core infrastructure by 2025. Furthermore, IDC forecasts global spending on edge computing to exceed $378 billion by 2028. Early use cases emerging in 2025 revolve around fraud detection, risk assessment, high-frequency trading, and hyper-personalized customer engagement. Banks are expected to deploy AI models at the edge to instantly identify suspicious behavior without sending sensitive data to a central repository, mitigating regulatory and compliance challenges.

Most banks, still refining their transition from legacy systems to modernized, cloud-based platforms, should focus on careful workload orchestration between cloud and edge. They will need to establish robust governance frameworks, ensuring consistent security policies across distributed nodes, and develop clear strategies to handle the evolving ethical and regulatory implications of AI. Talent acquisition and executive buy-in will be critical—securing professionals who can design, deploy, and maintain edge architectures is paramount.

Meanwhile, progressive banks are expected to move beyond basic operational improvements, leveraging edge capabilities to deliver hyper-personalized services and near-instant onboarding experiences. These institutions will invest heavily in AI at the edge, allowing advanced ML models to run closer to data origin. Such real-time insights can help streamline everything from risk scoring to product recommendations, ultimately elevating the customer journey. With edge computing becoming central to strategic competitiveness, forward-thinking banks in 2025 will seize this advantage to differentiate themselves through faster innovation and enhanced trust in an increasingly data-driven financial ecosystem.

Case-in-Point

Banco Bradesco enabled a private 5G network capable of supporting surveillance applications with different quality of service requirements. The application will be installed on an edge computing machine with 5G connectivity.

Edge computing enabled HSBC to deploy IoT-based robot “Pepper” which uses AI and ML to deliver unique customer experiences, reduce customer waiting times and present the information as needed.

Securing Banks in Quantum Era with Post-Quantum Cryptography

The gradual advancements in quantum computing are set to fundamentally reshape the cybersecurity landscape. The development of a cryptographically relevant quantum computer (CRQC) while still distant, will render many of today's public-key cryptography protocols obsolete, posing a significant threat to banks' core processes, including secure transactions, user authentication, and data privacy. Once CRQCs materialize, attackers could decrypt sensitive information that was previously considered secure, leaving banks exposed to substantial risks. According to industry surveys, 52% of organizations are already assessing their quantum-related vulnerabilities, while another 30% have begun implementing risk mitigation measures. These figures underscore a growing recognition that proactive preparedness is essential and waiting until quantum threats fully materialize is not an option.

In response to the looming quantum threat, in years to come, post-quantum cryptography (PQC) will emerge as a critical defense mechanism for banks. PQC algorithms are based on mathematical problems that are challenging for both classical and quantum computers to solve, making them inherently resilient to quantum-based attacks. Transitioning to PQC will allow banks to secure sensitive customer data, protect transaction integrity, and ensure long-term privacy. An essential advantage of adopting PQC is that it can safeguard previously intercepted data, ensuring it remains indecipherable even when quantum computers become capable of breaking existing cryptographic methods. For banks, experimenting with quantum-safe algorithms will be crucial to maintaining trust and protecting their digital assets in the years ahead.

While PQC offers a robust solution, the transition to quantum-safe encryption presents several challenges for banks. A lack of preparedness and limited knowledge about post-quantum algorithms pose significant barriers. Unlike traditional cryptographic algorithms, quantum-safe methods often come with different performance characteristics, which may require rewriting existing applications and restructuring cryptographic processes. Additionally, banks must address the operational complexities of transitioning to new algorithms, such as managing data retention policies, replacing legacy cryptographic methods, and updating existing infrastructure. Without a well-defined roadmap, banks risk falling behind in securing their systems against quantum threats.

To ensure a smooth transition to post-quantum cryptography, banks must adopt a structured and forward-looking approach. This begins with establishing a dedicated task force responsible for assessing the scope, impact, and cost of the transition. These teams should coordinate efforts across security operations, IT infrastructure, and software engineering to ensure seamless integration of quantum-safe algorithms. Banks must experiment replacing outdated cryptographic methods with quantum-safe alternatives as part of a long-term risk management strategy. Additionally, banks should begin embedding quantum considerations into their cybersecurity frameworks, ensuring they stay ahead of emerging threats. By proactively embracing post-quantum cryptography and collaborating with industry experts and technology providers, banks can future-proof their digital assets, maintain customer trust, and ensure resilient operations in the quantum era.

The Road Ahead

As banking innovation takes another leap, both edge computing and post-quantum cryptography can emerge as vital areas of investments for banks in coming years. In 2025, banks must accelerate edge adoption to optimize latency-sensitive processes like fraud detection and customer engagement, while also preparing for quantum threats by adopting quantum-safe encryption. By embedding these technologies into long-term strategies and enhancing readiness, banks can future-proof operations, protect customer trust, and maintain competitiveness in an increasingly fast-paced, security-conscious financial landscape.

Why we exist

To inspire better banking so that billions of people and businesses can save, pay, borrow, and invest better.

How we do it

Our solutions and people help banks to engage, innovate, operate and transform better, so that they can improve their customers' financial lives, better.

What we offer

A comprehensive suite of industry-leading digital banking solutions and SaaS services that help banks engage, innovate, operate and transform better.

Infosys® | Finacle

Finacle is an industry leader in digital banking solutions. We are a unit of EdgeVerve Systems, a wholly-owned product subsidiary of Infosys (NYSE: INFY). We partner with emerging and established financial institutions to help inspire better banking. Our cloud-native solution suite and SaaS services help banks engage, innovate, operate, and transform better to scale digital transformation with confidence. Finacle solutions address the core banking, lending, digital engagement, payments, cash management, wealth management, treasury, analytics, AI, and blockchain requirements of financial institutions. Today, banks in over 100 countries rely on Finacle to help more than a billion people and millions of businesses to save, pay, borrow, and invest better.

For more information, contact finacle@edgeverve.com **www.finacle.com**