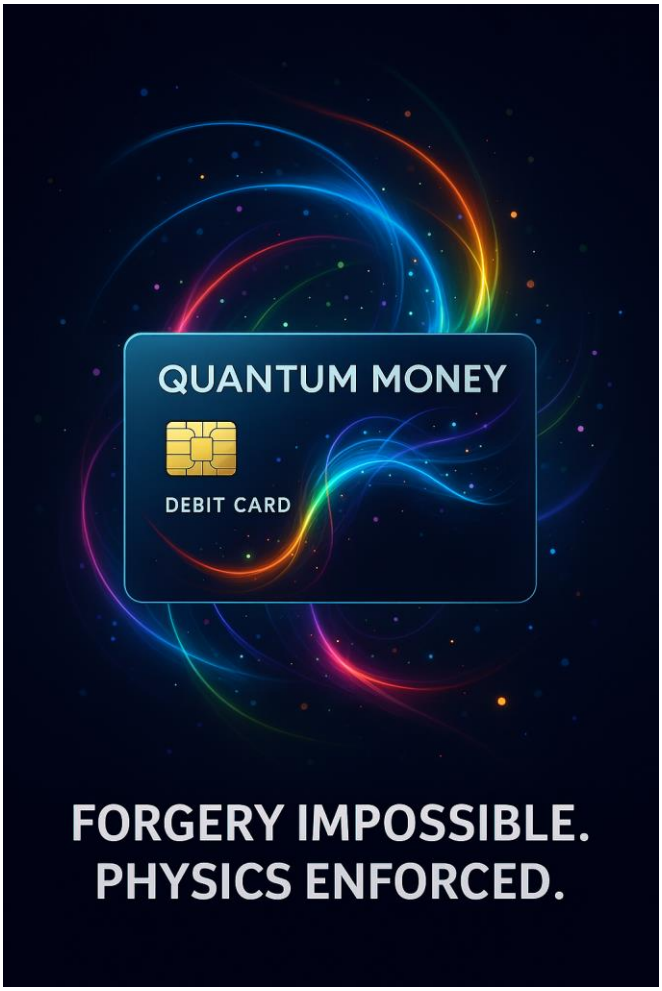
Please visit
www.Qdayready.com

Qday Ready

September-October
2025 Volume 6

Welcome to this month's special edition on Quantum Money & Finance

INSIDE



Quantum Money Unleashed: The Debit Card You Cannot Fake

Quantum money is steadily moving from theory to tangible progress. This month we saw researchers stress-testing cryptographic designs, new schemes that simplify how "banknotes" could be minted, and real-world experiments with quantum tokens over city-scale networks. At the same time, industry voices are sounding the alarm on quantum threats to existing systems, and market studies highlight that the real financial upside will flow to early adopters rather than hardware vendors. Together, these signals suggest a dual reality: the technology is maturing, and so is the urgency for finance to prepare.

Physicists at the Kastler Brossel Laboratory in France have achieved a groundbreaking milestone in quantum information science by demonstrating a quantum debit card capable of storing unforgeable quantum money. This innovation builds on a concept first proposed in 1983 by physicist Stephen Wiesner, who envisioned a protocol for quantum money based on the no-cloning theorem-a fundamental law of quantum mechanics that prohibits the duplication of quantum states. Because quantum states cannot be copied without disturbing them, any attempt to forge such money would be immediately detectable, making counterfeiting not just difficult but physically impossible.

Led by Julien Laurat, the French research team used ultracold atoms and photons to create a rudimentary quantum debit card. In this system, quantum money is encoded in particles of light, each prepared in a unique quantum state that acts as a secure currency. The bank issues these "banknotes" by configuring quantum particles in specific states. If someone tries to copy or alter them, the quantum state collapses or changes, instantly revealing the forgery attempt. What sets this experiment apart is its added capability: the quantum debit card can now store funds for future use, enabling a practical mechanism for loading and retrieving quantum currency.

Unlike traditional banknotes, which rely on detection technologies and the skill of counterfeiters to determine authenticity, quantum money is secured by the immutable laws of physics. This means that the integrity of the currency is not dependent on external safeguards but is inherently protected by quantum mechanics itself.

The implications of this breakthrough are profound. It transforms Wiesner's decades-old theoretical idea into a working prototype, signalling a shift from abstract quantum principles to tangible financial tools. Quantum money could revolutionize secure financial transactions by eliminating the risks of counterfeiting and fraud. Beyond finance, this development showcases the growing maturity of quantum technologies and their potential to reshape trust, security, and the architecture of global commerce.

Source: NewScientist

Breakthrough in Quantum Tech: Polymer Unlocks Room-Temperature Quantum Devices

For decades, quantum technologies have dazzled scientists with their promise of unparalleled computing power, ultra-secure communications, and sensors of extraordinary precision. Yet one stubborn barrier has kept these marvels confined to specialized labs: the need for extreme refrigeration. Quantum states, the delicate building blocks of these technologies, typically collapse unless cooled to near absolute zero. This requirement has made quantum devices bulky, expensive, and impractical for everyday use.

Now, a breakthrough from researchers at Georgia Tech and the University of Alabama could change that narrative. They have developed a novel polymer-based material capable of sustaining quantum states at room temperature. This innovation hinges on a conjugated polymer which comprises a flexible molecular chain engineered with alternating electron-conducting blocks. At its core are two

key components: a donor unit known as dithienosilole and an acceptor unit, which together enable stable quantum interactions without cryogenic support.

Unlike traditional quantum platforms that rely on rigid crystals like diamond or silicon carbide under freezing conditions, this polymer mimics solid-state behaviour while operating comfortably at ambient temperatures. The implications are profound. By eliminating the need for costly refrigeration systems, the material paves the way for scalable, lightweight, and affordable quantum technologies. Applications could span from portable quantum sensors and secure communication devices to more accessible quantum computing modules.

Beyond the technical leap, this development signals a shift in how quantum innovation might unfold. It demonstrates the power of chemistry-driven solutions to solve problems previously tackled only through physics and engineering. By moving quantum capabilities out of ultra-controlled environments and into practical settings, the polymer could accelerate the adoption of quantum technologies across consumer and enterprise domains.

In essence, this room-temperature breakthrough does not just warm up quantum, it could ignite a new era where quantum devices are no longer exotic lab specimens, but everyday tools woven into the fabric of modern life.

Where is the Money in Quantum?

Quantum computing is rapidly evolving from a theoretical concept into a strategic investment frontier, attracting billions in global funding. As Forbes reports, over $55 billion has already been committed by governments and industry leaders worldwide, with the market valued at more than $1 billion in 2024 despite limited current utility. Countries like China, Germany, France, and the United States are leading the charge; Germany plans to invest over $3 billion by 2026; France is allocating nearly $2 billion to train 5,000 quantum engineers and create 30,000 jobs, and the U.S. has authorized $1.2 billion under the National Quantum Initiative Act.

The technology itself promises exponential speedups in solving complex problems across cryptography, optimization, and materials science, leveraging quantum bits (qubits) that operate in superposition for massive parallelism. Although no quantum computer has yet surpassed classical supercomputers in practical tasks, venture capital firms like Quantonation project the sector could reach $850 billion by 2040. Investors are betting on long-term roadmaps, scientific credibility, and ecosystem development, recognizing that quantum's artisanal phase is giving way to scalable innovation. This momentum aligns with our advocacy for quantum-safe governance and crypto agility, reinforcing the urgency for talent pipelines, modular standards, and cross-border collaboration. The financial commitment signals that quantum is no longer just a scientific pursuit-it is a race to define the future of computing, security, and global competitiveness.

Sources:
Quantum Computing Takes Off With $55 Billion In Global Investments – Forbes
Who Is Investing in the $850 Billion Quantum Tech Market and Why – Forbes

Cryptanalysis of Isogeny-Based Quantum Money

Researchers have recently studied a type of quantum money system that uses special mathematical structures called isogenies—connections between elliptic curves. These systems are designed to be extremely secure, relying on quantum physics to prevent forgery. However, the new research found a way to analyze and slightly improve how these systems can be verified and potentially attacked. By using rational points and mathematical tools called division polynomials, the researchers showed that it is possible to speed up the process of checking whether a quantum banknote is valid. This does not mean the system is broken-it is still very hard to forge quantum money-but it does reveal some weaknesses in how the system is built. These insights help scientists better understand the limits of current quantum money designs and guide improvements for future, more secure versions.

Financial Sector Readiness for Q-day

The financial sector is increasingly aware of the transformative potential of quantum technologies, but global preparedness remains uneven and largely inadequate in the face of looming quantum threats.

A recent survey highlighted in the BoF Bulletin reveals that while banks and financial institutions recognize quantum computing's promise for optimization, fraud detection, and secure transactions, most admit they are underprepared to defend against quantum-enabled attacks. This concern is amplified by the anticipated arrival of "Q-Day"-the moment when quantum computers become powerful enough to break widely used public-key cryptographic systems such as RSA and ECC.

Experts warn that Q-Day could compromise the integrity of digital signatures, transaction records, and secure communications across global financial infrastructure.

Despite this, only a handful of financial institutions have begun transitioning to post-quantum cryptographic standards. The U.S. National Institute of Standards and Technology (NIST) has selected several algorithms for post-quantum cryptography, but adoption across the finance sector remains slow.

In Europe, regulators are beginning to nudge institutions toward quantum-safe readiness, while countries like China and France are investing heavily in quantum talent and infrastructure. However, many firms still lack clear migration roadmaps, crypto agility frameworks, and cross-border coordination mechanisms.

The gap between optimism and operational readiness is risky. As quantum computing advances, often in tandem with AI, the threat landscape is evolving faster than institutional defences. Regulators are expected to play a more assertive role in mandating preparedness, especially for systemically important financial institutions. This moment presents both a challenge and an

opportunity: to shape resilient architectures before Q-Day arrives and to ensure that financial systems remain secure, interoperable, and future-proof.

In India, regulatory awareness around quantum risks in the financial sector is beginning to take shape, though formal guidelines remain in early stages. The Reserve Bank of India (RBI), through its 2025 FREE-AI Committee Report, has acknowledged the strategic implications of emerging technologies, including quantum computing on financial services. While the report primarily focuses on artificial intelligence, it emphasizes the need for trust-centric frameworks and anticipates future enhancements to RBI's Master Directions that may incorporate quantum resilience as part of broader digital trust initiatives.

Meanwhile, the Securities and Exchange Board of India (SEBI) has issued a Cybersecurity and Cyber Resilience Framework (CSCRF) for regulated entities, which includes provisions for threat intelligence, incident response, and critical infrastructure audits. Although quantum-specific mandates are not yet codified, SEBI's emphasis on proactive cyber governance and its alignment with RBI's standards suggest that quantum-safe considerations may soon be integrated into India's financial regulatory architecture. These developments reflect a growing recognition that quantum preparedness is essential for safeguarding digital assets and maintaining systemic stability in the years ahead.

Source: BoF Bulletin – Finance Sector Readiness: Survey Insights

Before Q-Day Strikes: The Race to Reinvent Digital Signatures

Digital signatures are essential for securing online communications, verifying identities, and protecting financial transactions. Today, most systems rely on classical cryptographic algorithms like RSA, ECDSA, and DSA, which are vulnerable to quantum attacks.

Once scalable quantum computers become available, algorithms such as Shor's could efficiently break these cryptographic foundations, allowing attackers to forge signatures, impersonate users, and compromise sensitive data. This looming threat, often referred to as Q-Day, has prompted urgent global efforts to develop and adopt quantum-safe digital signatures, also known as post-quantum signatures.

To address this, the U.S. National Institute of Standards and Technology (NIST) has selected several algorithms for standardization, including CRYSTALS-Dilithium and FALCON (both lattice-based), and SPHINCS+ (hash-based). These schemes are designed to resist both classical and quantum attacks, offering robust security for future-proof systems. However, transitioning to these new algorithms presents challenges. Quantum-safe signatures often require larger key sizes and longer processing times, which can impact performance and compatibility with existing infrastructure. This makes crypto agility which involves designing systems that can flexibly switch cryptographic algorithms a critical requirement for smooth migration.

Globally, adoption is gaining momentum. U.S. federal agencies are beginning to implement post-quantum standards, while European and Asian regulators are assessing sectoral readiness. Tech companies and blockchain platforms are also piloting quantum-safe signature schemes in live environments. As quantum computing advances, the shift to quantum-safe digital signatures is becoming a strategic imperative not just a technical upgrade. Institutions that act early will be better positioned to maintain trust, regulatory compliance, and operational resilience in a post-quantum world.

From Classical to Quantum-Safe: Solana Reinvents Signature Security

Solana's unveiling of a quantum-resistant vault marks a pivotal moment in the evolution of digital signatures and cryptographic infrastructure. As quantum computing approaches practical viability, the threat it poses to classical cryptographic systems-particularly those underpinning digital signatures like RSA and ECDSA has become increasingly urgent.

These traditional algorithms rely on mathematical problems that quantum computers, using algorithms like Shor's, could solve exponentially faster than classical machines, potentially enabling attackers to forge signatures, impersonate users, and compromise secure transactions. In response, developers across blockchain and cybersecurity domains are accelerating the adoption of post-quantum cryptography-techniques specifically designed to resist both classical and quantum attacks.

Solana's initiative reflects a broader industry shift toward quantum-safe digital signatures, which are essential for maintaining trust, authenticity, and integrity in a post-Q-Day world. By integrating quantum-resistant algorithms into its infrastructure, Solana is not only future-proofing its ecosystem but also setting a precedent for other platforms and financial institutions.

This move underscores the importance of crypto agility-the ability to upgrade cryptographic systems without disrupting operations and highlights the need for scalable, interoperable solutions that can be adopted across sectors.

As digital signatures are foundational to secure communications, identity verification, and blockchain consensus, transitioning to quantum-safe standards is no longer optional, it is a strategic imperative. Solana's vault serves as a blueprint for the next stage of digital trust, where resilience against quantum threats becomes a baseline requirement for secure digital systems.

Source: [Solana Unveils Quantum-Resistant Vault Amid Rising Cryptographic Threats – BoF Bulletin]

"Digital signatures are the backbone of trust in the digital world. If we do not upgrade them before quantum computers arrive, we risk losing the integrity of everything from financial transactions to national security."

Want to learn more and stay updated about exciting developments in quantum computing?

Subscribe to our monthly newsletter at www.QdayReady.com

OR

Email us at: editor.qdayready@gmail.com