THE kyndryl institute

Trend Topic: **The next frontier of global finance**

By

Carole House

CEO of Penumbra Strategies, Former White House National Security Council Special Advisor

Carole House is a strategic technology executive who has spent her career focusing on leveraging innovative technologies to combat national security threats. She is the founder and CEO of a strategic technology and national security advisory practice, Penumbra Strategies, and serves as a Senior Fellow at the Atlantic Council GeoEconomics Center. Carole recently served two tours on the White House National Security Council, where she architected two Executive Orders and drove critical steps to promote innovation in cybersecurity, digital identity, artificial intelligence, and digital assets. She has held positions in the private sector as an Executive in Residence at Terranet Ventures, Inc., co-founder and interim COO for a stealth fintech startup, and served on advisory boards for three financial regulatory agencies and three non-profits. Carole's prior government experience includes service as a U.S. Army Captain as well as positions leading emerging tech, cybersecurity, and national security initiatives across the White House, Senate Homeland Security Committee, and the U.S. Treasury.

Explore more from The Kyndryl Institute
kyndryl.com/institute

The fintech frontier

Navigating the emerging technology terrain shaping the future of finance

When I was once asked as a regulator to define "fintech," my — admittedly cheeky — answer was: it's just "finance." If you're not leveraging technology in finance today, you're not really competing.

Fintech is advancing across a frontier where competition and convergence across new technologies and geopolitical realities are defining the terrain for financial leadership.

Throughout my career at the nexus of innovative technologies and national security — whether as an Army officer preparing for chemical weapons threats or as a regulator promoting payments innovation — I've witnessed how cutting-edge technology forges competitive advantages for allies and adversaries alike.

The lesson is clear: those who recognize the strategic potential of emerging technologies and harness them thoughtfully will reap competitive benefits. Those who hesitate or chase hype without guardrails risk being left behind, exploited, or facing other existential risk. For example, those companies that use customer analytics feature 19 times for profitability than those which do not, and strong innovation cultures within organizations drive much more successful digital transformations.[1] Failures like Kodak[2], Blockbuster[3], Blackberry[4], or Pets.com[5] have showcased the consequences of not adapting products and business models to technical

innovations, while collapses of once-thought-industry-titans Theranos[6] and FTX[7] underscore that tech adoption without guardrails or governance can kill a company.

Unlike past frontiers, we don't have the luxury of choosing whether to explore this technological frontier. We're already immersed in a digital landscape that undergirds our communications, operations, and — in the case of digital assets — can define the very nature of property, instruments, and services.

Being tech savvy is no longer an option, but a mandate.

The stakes are high. Fintech revenues are projected to grow three times faster than traditional banking and flaunt massive consumer adoption including across emerging markets[8]. Entire blocs like the BRICS nations are pursuing alternatives to traditional financial rails to bypass the U.S.-centric financial system, while the U.S. dollar's share of global foreign exchange reserves has declined to its lowest point since 1994[9]. I have also seen those unprepared to address the radical shifts in risk exposures and digital attack surfaces find themselves stripped of millions, even billions, in intellectual property, sensitive data, and financial assets. The global call to innovate is unmistakable.

Financial executives face unprecedented convergences: advanced computing and AI-driven decision engines enabling real-time analytics, programmable money reshaping cross-border payments, and quantum computing threatening current cryptographic foundations. Simultaneously, aging core systems struggle to keep pace, dynamic cyber threats evolve faster than defenses can adapt, and financial criminals exploit vulnerabilities across expanding digital terrain.

This is the financial frontier — where technological innovation, market disruption, and geopolitical realities converge to create both unprecedented opportunity and existential risk.

To thrive on this frontier, companies will need more than cutting-edge tech. They'll need strategies to manage risk without inadvertently smothering its rewards. Now is the time to survey these frontier technologies and organize approaches to leverage them.

Quantum and edge computing

Advances in computation, such as quantum and edge computing, provide infrastructure to supercharge the speed and complexity of thinking underlying digital applications like artificial intelligence. Where quantum handles the immensely complex, edge makes it immediate and at the point of consumer need.

Quantum systems can assess millions of variables simultaneously to generate unprecedented modeling of complicated scenarios and interdependencies. Companies harnessing quantum can create hyper-personalized services and enhanced fraud detection and stress testing that were previously impossible to model efficiently[10].

> Institutions like JPMorgan Chase, Goldman Sachs, and Turkey's Yapı Kredi Bank are pioneering quantum algorithms for portfolio optimization, options pricing, and risk calculations promising to compress weeks of classical computation into minutes.

These benefits are moving from theoretical to practical applications. Institutions like JPMorgan Chase[11], Goldman Sachs[12], and Turkey's Yapı Kredi Bank[13] are pioneering quantum algorithms for portfolio optimization, options pricing, and risk calculations promising to compress weeks of classical computation into minutes.

Edge computing changes where financial intelligence operates – instead of processing everything in centralized data centers hundreds of miles away, computational power moves to the point of need. Think smart ATMs approving complex loan applications instantly, trading systems executing decisions on the exchange floor without delay, or mobile apps generating investment advice even with poor connectivity.

However, organizations must account for risks threatening security and user privacy. Quantum computing will break many current cryptographic methods, potentially making much of today's encrypted traffic essentially public by potentially 2035[14]. Meanwhile, thousands of edge devices can drastically increase digital attack surfaces while challenging data sovereignty.

Organizations should look now toward quantum-ready infrastructure and secure edge deployments. They can partner with hyperscalers and those piloting quantum-as-a-service platforms on specific use cases like fraud detection, and explore integrating edge computing at high value touchpoints like trading floors and mobile banking while leveraging zero-trust[15] security frameworks to mitigate potential compromises.

Most critically, companies must begin thinking about a years-long post-quantum cryptography migration, beginning with steps similar to those we took in the government[16]: an inventory of cryptographic dependencies and a phased timeline to move to quantum-resistant algorithms before the "cryptographic cliff" arrives.

AI and autonomous finance

In no technological arena is the tension across opportunity and risk more evident than in AI. AI and machine learning has increasingly become a key feature in finance, whether in robo algorithmic trading, chatbots in customer services, or transaction monitoring and compliance. Financial services spending on AI is projected to almost triple to almost $100 billion by 2027.[17]

Advances in generative and agentic AI have unlocked vast potential through democratized access and greater usability. With natural language as the new user interface, compounded by the scale and reach of automation, both employees' and customers' experiences will see new efficiency opportunities. Imagine AI agents that monitor global markets while you sleep and automatically rebalance portfolios to hedge against overnight geopolitical shocks, or that pre-screen mortgage offers and then negotiate the best fit product.

But risks also loom large. The same advanced models that can create vaccines could foster development of biological agents. AI-driven cyber tools supporting code audits and automated vulnerability management could also scale malicious cyber operations, which nations like Iran[18] are already experimenting with. Image and voice generation tools create deepfakes fueling unprecedented fraud campaigns, evident in social manipulation scams and phishing in Europe rising 156% and 77%[19] respectively in 2024.

Autonomy also introduces vulnerability. With current AI systems' significant capability comes also great capacity to be misled[20]. These vulnerabilities are exacerbated by AI's challenges with explainability, bias, and procyclicality[21] that could reinforce erroneous decisions.

Organizations must be deliberate in integrating governance frameworks in their use of AI, which is why the White House directed creation of tools like NIST's AI Risk Management Framework[22]. Otherwise, agentic AI's speed and complexity can create blind spots in compliance and security monitoring and enable cascading impacts that corrupt critical operations.

We must invest in building blocks to better oversee these models, as well as to address the current authenticity crisis. Agentic AI cannot work if we remain rooted in a reality where we cannot trust that individuals, content, transactions, and machines online are real or that sensitive data remains private.

We are past voice and selfie-based verification being reliable. In this digital age, cryptography-grounded systems of digital identity[23] must be the foundation of trust. Companies should invest in using digital identity verification solutions like verifiable credentials and strong access management controls for sensitive operations, as well as in privacy enhancing technologies that permit analysis without compromising data confidentiality.

In a market flooded with AI applications and automation, firms that can prove transparency, security, and ethical AI will win trust and customer loyalty in the long run.

These "trust-tech" primitives needed to ensure approach security, integrity, and accountability against exploitation in the use of technologies like AI have not yet been built or deployed at scale. But there's a business interest in doing so. In a market flooded with AI applications and automation, firms that can prove transparency, security, and ethical AI will win trust and customer loyalty in the long run.

Programmable money and tokenization

Digital assets and blockchain-based innovations form the last major terrain feature on the fintech frontier, presenting a vision to revolutionize how value moves by enabling cross-border transfers with reduced reliance on intermediaries like banks and nearly instant settlement.

Touting a market cap around $4 trillion[24], interest in digital assets continues to climb. Almost 40%[25] of surveyed Chief Financial Officers see cryptocurrency improving cost and time efficiencies compared to traditional finance, and 137 countries[26] are exploring central bank-issued digital currencies.

Some of the more groundbreaking aspects of blockchain involve making money programmable and the development of smart contracts. With programmability, developers can build technological features that can enhance security and compliance with precision and transparency required for counterparties and regulators.

Conditional payments, automated escrow services, and built-in compliance like sanctions screening are all possible with blockchain innovations. Tokenization of real-world assets – like real estate, commodities, bonds, art, and intellectual property – offers potential for enhanced liquidity and access through digital marketplaces.

However, significant challenges remain. Leaders must keep a constant eye on the evolving regulatory landscape as they evaluate digital asset services. With recent stablecoin legislation and capital market legislation under development, I always encourage industry leaders to engage with policymakers on requirements affecting them. Strike while the iron is hot; make sure your voice is heard before policy is finalized.

Organizations must also carefully consider the nascent maturity of much of the digital asset industry. Despite blockchain's risk mitigating features like transparency of the blockchain ledger, cryptocurrency remains a significant risk in areas like money laundering, cybersecurity, and consumer exploitation.[27] This is generally not an inherent fault of "blockchain" but instead of some players across the industry sporting weak compliance and security frameworks.[28]

While compliance is programmable, most developers choose not to build in these features. The largest heist in history just occurred this year when North Korean cyber actors stole $1.5 billion[29] from a cryptocurrency exchange. Romance and investment scams con consumers out of billions[30] using crypto. The lack of serious movement to be able to recover these funds or drive improvements in security across the sector at scale underscore major challenges currently presented by decentralized finance like the lack of clear lines of accountability, inability to recover assets, and regulatory arbitrage across borders.

Let me emphasize that these are solvable problems, which I also think will benefit from more mature institutions and regulators engaging with digital assets. Though I am enheartened to see how conversations and compliance solutions have evolved over the past decade, it needs a kickstart to accelerate investment in the trust-tech solutions needed for greater market transparency and security, like digital identity frameworks and improved standards for blockchain wallets and key management.

The road ahead

The fintech frontier is not a destination to approach leisurely – it is ground we're already standing on. The convergence of advanced computing, AI, programmable money, and shifting geopolitical currents is reshaping finance in real time.

Those who lead successfully will drive competitive edge by pairing technological ambition with deliberate investments in organizational, security, and governance building blocks of trust. This means preparing for post-quantum migration before the cryptographic cliff arrives, integrating zero-trust frameworks into edge deployments, adopting AI risk management frameworks and digital identity solutions as a foundation for secure interactions, and leveraging risk-managed transformation in areas like digital assets.

History teaches us that frontiers reward the bold but punish the reckless. For financial leaders, this means embracing emerging technologies with both vision and vigilance. Those who strike this balance will not just compete in the fintech domain; they will define it.

References

1 https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/five-facts-how-customer-analytics-boosts-corporate-performance; https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/how-innovative-companies-leverage-tech-to-outperform; https://www.bcg.com/publications/2024/most-large-scale-tech-programs-fail-how-to-succeed

2 https://www.forbes.com/sites/chunkamui/2012/01/18/how-kodak-failed/

3 https://hbr.org/2011/04/how-i-did-it-blockbusters-former-ceo-on-sparring-with-an-activist-shareholder

4 https://www.theguardian.com/technology/2023/oct/15/blackberry-smartphone-status-symbol-then-crashed-and-burned

5 https://www.cnet.com/tech/tech-industry/pets-com-latest-high-profile-dot-com-disaster/

6 https://www.nytimes.com/2022/01/03/technology/elizabeth-holmes-theranos.html

7 https://apnews.com/article/ftx-bankruptcy-binance-timeline-c519d50b9059aa8bff0ce8b6cd26c40e

8 https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-fintech

9 https://www.ecb.europa.eu/press/key/date/2025/html/ecb.sp250526~d8d4541ce5.en.html

10 https://www.weforum.org/stories/2025/07/banking-quantum-era-fraud-detection-risk-forecasting-financial-services/?utm_source=chatgpt.com

11 https://thequantuminsider.com/2024/09/19/new-study-from-jpmorgan-chase-and-aws-optimizes-large-scale-portfolio-management-with-quantum-classical-hybrid-solutions/?utm_source=chatgpt.com

12 https://www.goldmansachs.com/careers/blog/possibilities-quantum-computing?utm_source=chatgpt.com

13 https://www.weforum.org/stories/2025/07/banking-quantum-era-fraud-detection-risk-forecasting-financial-services/?utm_source=chatgpt.com

14 https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

15 https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf

16 https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

17 https://reports.weforum.org/docs/WEF_Artificial_Intelligence_in_Financial_Services_2025.pdf

18 https://www.recordedfuture.com/research/irans-ai-ambitions-balancing-economic-isolation-national-security-imperatives

19 https://www.tietoevry.com/en/newsroom/all-news-and-releases/press-releases/2025/04/tietoevry-bankings-new-insight-report-reveals-an-increase-in-digital-payment-fraud-in-europe/

20 https://www.techradar.com/pro/agentic-ais-security-risks-are-challenging-but-the-solutions-are-surprisingly-simple

21 https://www.cftc.gov/media/10626/TAC_AIReport050224/download

22 https://www.nist.gov/itl/ai-risk-management-framework

23 https://pages.nist.gov/800-63-4/sp800-63a.html

24 https://www.reuters.com/business/crypto-sector-breaches-4-trillion-market-value-during-pivotal-week-2025-07-18/

25 https://www.deloitte.com/us/en/insights/topics/business-strategy-growth/2q-2025-cfo-signals-survey.html

26 https://www.atlanticcouncil.org/cbdctracker/

27 https://www.cftc.gov/media/10106/TAC_DeFiReport010824/download

28 https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html

29 https://www.ic3.gov/psa/2025/psa250226

30 https://alert.jamf.com/af718171-4ea2-47f7-b9c2-2f08cff5da80/blocks/BLOCK?classification=Q3J5cHRvY3VycmVuY2Ilcw%3D%3D