ALTAIR & ALANG

www.altairalang.com
Strategy ➥ Consulting ➥ Redefined

FEATURED INSIGHTS

30 October 2025

TAKEAWAY FROM THE BIS INNOVATION SUMMIT 2025: FUTURE-PROOFING CENTRAL BANKS

Executive-level briefings that provide timely, sector-specific analysis on global market developments. These insights are published to provide high-level insights across the financial services, capital markets, clearing, technology, fintech, cyber, and other sectors.

REF: AA_FEATURED_INSIGHTS_20251015V1F

CONTENTS

1. KEY THEMES ____ 3
2. FUTURE-PROOFING CENTRAL BANKS ____ 3
3. AI IN CENTRAL BANKING: PROMISE MEETS GOVERNANCE DILEMMAS ____ 5
4. QUANTUM THREAT TO FINANCE ____ 6
5. ABOUT US ____ 8

FEATURED INSIGHTS

TAKEAWAY FROM THE BIS INNOVATION SUMMIT 2025: FUTURE-PROOFING CENTRAL BANKS

2025-10-15

Prepared by: Altair & Alang

For any questions regarding this report, please contact: info@altairalang.com

This publication is also available online at the Altair & Alang website: www.altairalang.com/featured-insights

1. KEY THEMES

1. **Future-Proofing Central Banks**
Reimagining how central banks can adapt with agility, fortify institutional resilience, and stay ahead of the curve amid rapidly evolving technologies and shifting global dynamics.

2. **AI in Motion - Expanding the Central Bank Toolkit**
Uncovering the real-world applications of artificial intelligence across central banking; from data-driven monetary policy and regulatory intelligence to risk management and operational efficiency.

3. **Building Bridges Across Borders**
Showcasing how regulators, central banks, and industry leaders are joining forces internationally to spark innovation, enhance resilience, and shape a more secure and interconnected financial ecosystem.

2. FUTURE-PROOFING CENTRAL BANKS

Context: Fireside chat moderated by the BIS, with the Swiss National Bank (SNB), and the Hong Kong Monetary Authority (HKMA).

Theme: how to future-proof central banks while preserving stability, trust, and resilience.

What "Future-Proofing" Means Now

- Dual lens on risk: Innovation creates new risks, but late adoption risk is real in fast tech cycles. Central banks must balance innovation risk vs obsolescence risk.
- Principle-led adoption: Technology should reinforce core mandates (price stability, financial stability, secure payments).
- Three pillars (SNB): Insight (understand tech impact on mandate), Capability (skills, tooling, data), Engagement (stakeholders across public/private/academia).
- Culture shift (HKMA): Encourage measured risk-taking, accept fail-learn-improve cycles, and promote co-creation between policy/oversight teams and technologists.

Trailblazer Case Studies

SNB - Tokenisation in Production

- Project Helvetia (wholesale Central Bank Digital Currency - wCBDC): Explores two designs for settling tokenised assets: (1) wCBDC on the same Distributed-Ledger Technology (DLT) platform as the asset; (2) Real-Time Gross Settlement (RTGS)-link, with DLT platform linked to existing RTGS.

- Prototype → Pilot on SDX: Built prototypes linking banks' core systems and SNB; now piloting settlement of tokenised bonds against tokenised central bank money on SIX Digital Exchange (SDX) - a first for production-grade wCBDC pilots.
- Data & AI: Use Artificial Intelligence (AI) for nowcasting (news sentiment → GDP indicator), financial stability monitoring (social media signals), markets (analyst-report sentiment for CHF), and short-term inflation forecasts via machine learning (ML). Cautious on system-wide payment monitoring to avoid unintended responsibilities.
- Cash still innovates: New banknote series shows the tech "arms race" (counterfeiting vs security features), illustrating insight-capability-engagement in a non-DLT domain.

HKMA: Regulatory Clarity + Build-to-Operate

- Two tracks: (1) Institutional digitisation of HKMA; (2) Five-year fintech strategy for banks (2020–2025).
- Clear guardrails for digital assets:
    - **Crypto-asset trading platforms:** comprehensive regime aligned with **Financial Stability Board (FSB)** standards (regulated by the Securities and Futures Commission; not "light-touch").

Stablecoins: dedicated legislation and licensing with HKMA as regulator.

- Tokenisation at scale: From BIS Project Genesis prototype (tokenised green bond) → real issues (initial small 100m, then HKD 800m benchmark) by interfacing Central Securities Depositories (CSDs) with blockchain; broad investor base.
- Project Ensemble: "Unified ledger"-style architecture: tokenised assets (bonds, money market funds (MMFs), carbon credits, trade docs) + tokenised deposits/stablecoins as private settlement layer + CBDC as final settlement. 20 use cases across capital markets, corporate liquidity, green/ESG, trade finance (e-Bills of Lading, fraud-resistant documentation). Commitment to provide production environments for successful pilots.
- GenAI sandbox: Sector-wide Generative AI (GenAI) environment with Cyberport providing compute for smaller banks; real-time supervisory feedback. Themes: data readiness, model evaluation (accuracy, completeness, reliability, consistency), explainability. Launching an explainable-AI toolkit project with the BIS Innovation Hub. Next cohort adds AI-vs-AI controls (e.g., AI quality-assurance of AI chatbots; detecting defective face/ID recognition).

Governance, Culture & Skills

- Tone from the top: Leadership must articulate the *why*, set risk appetite, and celebrate early wins to drive adoption.
- Talent & literacy: Hire AI/ML/data specialists; upskill economists/supervisors; create tech-champion communities; run Digital Days to showcase use cases.
- Architecture first: Enterprise data lake with robust data governance; modern security posture; enforce standards to avoid tool sprawl.
- Co-creation over ticketing: IT/tech teams act as partners, not service desks.

Collaboration (Domestic & Cross-Border)

- Architecture community (HKMA): Early agreement on interoperability standards across layers (asset platforms ↔ tokenised deposits ↔ CBDC).
- BIS innovation fabric (SNB/HKMA): Multi-centre collaboration (e.g., Project Helvetia; Jura with Banque de France; pilots with Thailand/Brazil/France on Delivery-versus-Payment (DvP)/Payment-versus-Payment (PvP), carbon, and trade-finance).
- Broader ecosystem: Private sector, academia, and other international organisations are integral.

3. AI IN CENTRAL BANKING: PROMISE MEETS GOVERNANCE DILEMMAS

What AI is doing in/for central banks

AI is already embedded in central banking, with use cases spanning real-time inflation forecasting, sentiment monitoring, fraud detection, and AML/KYC pattern recognition. However, scaling it raises structural dilemmas. The Reserve Bank of Australia highlighted efficiency gains across project management, analysis, archives, and communication, while warning of data scarcity and quality constraints that limit model reliability. Concrete use cases are real and growing.

Reserve Bank of Australia (RBA): Internal chatbots (analytics, policy, comms, project support), coding copilots, digitising 200 years of archives, text analytics on 23 years of business-liaison notes; cautious on production use for policy/oversight until data and validation are solid.

Central Bank of the Republic of Türkiye (CBRT): Three-pillar frame-Mind (macro/data): Machine Learning (ML) for credit-risk prediction, model selection, high-frequency inflation (daily food price index from barcode data). "Pulse" (payments oversight): Anomaly detection in real-time instant payments (≈50M msgs/day). Core (operations): a private GenAI "Central Assistant" for summarisation and workflow.

Strategic dilemmas & policy angle

Cost of inaction is real. **South African Reserve Bank (SARB)** flagged that the macro-financial consequences of lagging on AI may outweigh incremental ops gains; central banks must weigh system-wide risks not just internal productivity. Public-policy "sweet spots": AML/financial crime, and real-time payment system oversight are high-impact, central-bank-specific use cases.

Governance & risk management (the core message)

Strong guardrails before scale are vital. **RBA:** clear boundaries for where AI can be used, validation of outputs, "safe sandboxes," alignment with ethical AI guidance, and two committees (strategy oversight; technical assurance). Heavy investment in AI literacy, especially for leaders.
Human accountability stays central. **CBRT** stressed black-box/explicability limits, hallucinations/bias/over-alignment risks, privacy, and the need for **human-in-the-loop** verification. GenAI is not a substitute for judgment in monetary/financial stability decisions.

Data governance is decisive. **"Only as good as the data":** trusted, well-governed datasets and knowledge-management are prerequisites to production use.

Model Risk Management must evolve. Traditional MRM (known inputs/outputs) breaks with GenAI.

Priorities should be:

1. Provenance/Retrieval-Augmented Generation (RAG) to ground answers in verifiable sources.
2. New evaluation regimes for agentic systems (beyond cross-validation).
3. Advance explainability research; do not assume *magical* understanding.

Global coordination is coming but uneven. **SARB/G20 lens:** aim to reduce productivity gaps, share practices, and set standards (aligned with the Financial Stability Board (FSB)/BIS/World Bank workstreams). A "Basel-like framework for AI use in finance" was mooted to protect system integrity.

Practical implications (what to do next?)

- Start with contained, efficiency-oriented pilots (internal assistants, document workflows), while building data quality pipelines and evaluation harnesses.
- Stand up AI governance early (charters, risk appetite, committees, red-teaming, privacy reviews), and train leadership/staff in prompting, validation, and failure modes.
- For supervised firms, expect supervisors to push for traceability, provenance, and outcome testing; plan accordingly.

4. QUANTUM THREAT TO FINANCE

Context: BIS Innovation Hub session on "New frontiers in cybersecurity."
Focus: The quantum-computing threat to today's cryptography and how central banks and financial market infrastructures (FMIs) should respond.

The Problem (Why now?)
Quantum risk: At sufficient scale (≈ order of 10^6 qubits, timing uncertain), quantum computers could break widely used public-key cryptography (e.g., RSA), jeopardising confidentiality, integrity, authentication of financial data and messages.

Harvest-now–decrypt-later (HNDL): Adversaries can intercept and store traffic today and decrypt it once quantum capability arrives → long-lived, sensitive financial data is at risk now.
Non-trivial transition: Financial systems are interconnected; upgrading cryptography requires coordinated, multi-year, multi-stakeholder change, not just a drop-in library swap.

BIS Innovation Hub Projects (What did we learn?)
Polaris - Central Bank Digital Currency (CBDC) & Offline Payments Security
Scope: Cybersecurity for future monetary systems, especially **offline** payments, including CBDC systems.
Outputs:
Offline payments handbook: Tech options, security trade-offs (resilience/inclusion/privacy), new attack surfaces from device proliferation & lack of real-time monitoring.

Baseline 7-step cyber framework: Prepare → Identify → Protect → Detect → Respond → Recover → Adapt (holistic; prevention-heavy).

Threat-modelling gaps: Distributed-ledger technology (DLT) / tokenised systems introduce smart-contract and software supply-chain risks; call for a new baseline threat model.
Design guide & scenarios: Underscores **crypto-agility** systems must swap algorithms later **without heavy redesign** (harder for offline devices).

Fuse: Fully Scalable Settlement Engine

- Architecture: Microservices (modular "Lego" blocks) to balance flexibility & scalability vs. extra interfaces/attack surface and operational discipline.
- Post-quantum cryptography (PQC) experimentation: Lattice-based schemes (e.g., CRYSTALS-Dilithium for signatures; Falcon in specialised uses). Takeaway: crypto-agility is essential; standards are evolving; PQC payloads are larger (keys/signatures) → latency/throughput costs across every service boundary.
-

LEAP - Quantum-Safe Communications & Payments

- **Phase 1:** Quantum-secure **virtual private network (VPN)** between Banque de France (Paris) and Bundesbank (Frankfurt); exchanged payment messages; documented operational/performance issues.
- Phase 2 (with Banca d'Italia, Banque de France, Bundesbank, Nexi, and the Society for Worldwide Interbank Financial Telecommunication (SWIFT)): Implement post-quantum digital signatures in a payments test environment reflecting real operations.

Result snapshot: PQC verify ≈ 210 ms vs ~30 ms classical (≈7× slower). Significant performance, reconfiguration, and coordination implications.
Lesson: Migration is a **major transformation** (payments, cryptography, legal, procurement, change management). **Crypto-agility** and **joint timelines** are critical.

Privacy-Preserving CBDC
Insight: Quantum advances can undermine today's privacy guarantees; new cryptographic approaches are needed to preserve privacy in future designs.

Implications for Central Banks, Financial Market Infrastructures (FMIs), and Supervisors

- **Act early** because of **HNDL** risk and long lead-times for retrofits.
- **Engineer for agility:** *Algorithm-agile* architectures; dual-stack support (classical + PQC); device lifecycle & update channels (especially offline form factors).
- **Expect overheads:** Larger keys/signatures → **performance budgets**; placement of cryptographic boundaries; selective use of PQC (sign vs. encrypt) to manage costs.
- **Coordinated migration:** Interdependent actors; central banks (**CBs**), FMIs, payment service providers (**PSPs**), and vendors; must **align on standards, timelines, and test plans**.
- **Governance:** Enterprise cryptography inventory; risk appetite; red-team & supply-chain security; performance & reliability **service level objectives (SLOs)**; regulator engagement.

5. ABOUT US

Altair & Alang is a boutique UK-based management consulting firm with a global footprint, serving clients across EMEA, APAC, and the Americas. We specialise in business intelligence, financial strategy, and actionable insights tailored to our client's needs. We partner with clients to uncover data-driven opportunities, optimise financial performance, and empower strategic decision-making.

We have worked with over 60 central counterparties (CCPs) worldwide, supporting them on a diverse range of initiatives. Our team has been directly involved in enhancing market transparency standards, advising both CCPs and global regulators. This unique experience positions us as a trusted partner to FMI's seeking to meet international standards while delivering meaningful improvements to governance, resilience, strategies, and stakeholder confidence in the global financial markets.

While our roots are in the financial services and capital markets, our strength lies in data and analytics that translate across all industries. We bring deep functional expertise to a wide range of sectors, including fintech, insurance and cybersecurity. Whether optimising operating models, designing scalable data strategies, or enhancing regulatory insight, we help clients make smarter decisions and deliver measurable results in dynamic environments.

Our deliverables combine deep industry knowledge with advanced analytics to deliver impactful solutions that drive measurable results and long-term success for our clients.

For more information, please contact us: info@altairalang.com

Our website: www.altairalang.com/featured-insights

ALTAIR & ALANG

www.altairalang.com
Strategy ⮡ Consulting ⮡ Redefined