FUTUREMATTERS™
CENTRE OF EXCELLENCE

GFTN
GLOBAL FINANCE & TECHNOLOGY NETWORK

Discovering the Edge of Tomorrow

Sept 2025

Agenda

Foreword

The Black Swan Summit 2025 served as a forum where bold ideas, new perspectives, and often unconventional solutions confronted the novel challenges of digital transformation. While many pivotal themes were broadly highlighted during the main stage panels, some of the most valuable insights were revealed during the Chatham House rule debates at the roundtables. Here, industry leaders, academics, and policymakers openly addressed critical pain points and creatively explored audacious solutions, offering a glimpse into the very fabric of tomorrow's financial and industrial landscapes.

This volume compiles select summaries from these exclusive roundtables, distilling their core arguments, key takeaways, and the groundbreaking ideas that were freshly discussed and critically examined. These reports are not substitutes for the dynamic, in-depth conversations that transpired, but rather offer a potent distillation of impactful content, designed to provide strategic value to executives, policymakers, founders, and academics.

For those who wish to be first at the edge of tomorrow, to be right at the table when these ideas are fresh, debated, and applied—not merely when they are published—we extend an exclusive invitation to the next edition of the Black Swan Summit. Join us to actively shape the future of finance and technology.

1 Defragging Sustainable AI Innovation in a Fragmented Financial System

This Black Swan Summit roundtable convened experts from diverse fields to address the intricate challenges of integrating sustainable AI innovation within an increasingly fragmented global financial system. The discussions provided invaluable insights for executives, policymakers, founders, and academics seeking to navigate this complex landscape.

a. The Rise of Agentic AI and the Question of Human Agency

A central theme was the imminent proliferation of personalized AI agents. Within the next two to three years, individuals are expected to widely adopt AI for administrative tasks and small-ticket purchases, eventually extending to high-value financial decisions. This raises critical questions about human agency: will individuals be empowered or diminished by increasingly autonomous AI? The panel highlighted the potential for AI agents to act as significant defences against scams and predatory lending, yet also warned of new risks, such as herd behaviour and liquidity challenges, if AI agents, acting on similar logical optimization, trigger correlated market movements.

A crucial and immediate challenge for financial institutions, corporations, and governments is the authentication and oversight of AI agents. How do organizations verify an AI agent's legitimacy when it attempts transactions, and how do they ensure it operates within delegated parameters and fiduciary duties? The complexity of managing these "digital powers of attorney" far surpasses current challenges in the analogue world, underscoring a pressing need for robust new frameworks.

b. The Double-Edged Sword of AI: Fraud, Crime, and Societal Impact

The discussion brought to light the escalating "arms race" between "good bots" and "bad bots." While AI holds immense promise in combating large-scale scam and fraud operations by actively disrupting malicious actors and detecting subtle patterns beyond human perception, bad actors are equally leveraging AI. The rapid pace of AI development is outpacing existing regulatory frameworks, creating an environment where proactive measures are essential.

A critical societal concern raised was **the impact of AI on the labour force**. While some forecast major disruption over the next 10–20 years, others argue the shift is already under way. With roughly 60% of jobs in advanced economies exposed to AI, some firms are trimming entry-level white-collar roles and pausing hiring, while autonomy pilots—such as robotaxi services in selected U.S. cities—signal early effects in blue-collar work, albeit still limited and tightly regulated. This necessitates urgent discussions around economic adjustments, including the potential for universal basic income and its funding mechanisms, for which society is currently ill-prepared.

The ethical implications of AI algorithms, particularly in areas like predatory lending, were a key point of concern. The panel questioned how to ensure AI algorithms promote ethical behaviour and prevent enticement to borrow beyond means, especially in unregulated platforms. The inherent profitability for malicious actors, who incur no compliance costs, creates a strong incentive for the development of "better" (more manipulative) algorithms, highlighting the struggle for regulated entities to keep pace. .

c. Navigating Fragmentation: Regulation, Infrastructure, and Global Equity

The fragmentation of financial systems, with different payment rails and geopolitical "blocks," presents a significant challenge for AI integration. The lack of uniform global laws on AI and data, coupled with difficulties in tracing liability across borders, exacerbates this complexity. The panel debated whether regulating access to hardware or focusing on the ethical design of algorithms is the answer, acknowledging the balance between control and stifling innovation.

A poignant question emerged regarding financial inclusion in underdeveloped countries. With a significant portion of the global population lacking digital footprints, smartphones, or understanding of AI, how can this

rapidly advancing technology benefit them? While AI offers opportunities for "leapfrogging" development and combating corruption, there's a risk of exacerbating inequalities if access and responsible implementation are not prioritized. The consensus was on the importance of ethical AI algorithms and robust education to prevent "gambling inclusion" or "scam inclusion" rather than genuine financial empowerment.

d. Towards Sustainable and Responsible AI Innovation

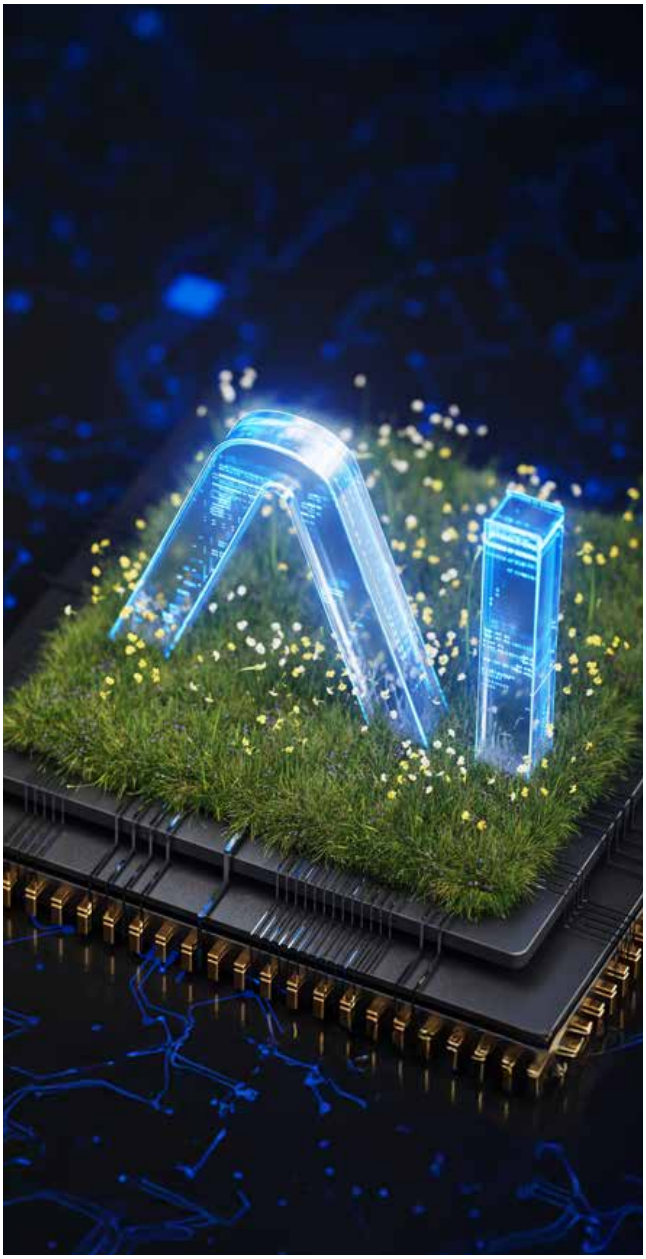
The roundtable underscored that for AI to be truly sustainable, it must do more good than harm, with a single negative incident having the potential to set back progress significantly. This encompasses not just environmental sustainability (e.g., energy consumption of AI) but also social and governance aspects. The concept of human-AI symbiotic intelligence was proposed as a future direction, fostering a mutual reinforcement that solves problems previously unattainable.

The discussion critically examined the traditional commercial model, advocating for a shift towards impact investment where financial markets bear significant responsibility for channelling money towards positive AI development. The fundamental flaw in current governance approaches was highlighted: an overreliance on regulation and law that struggles to keep pace with ever-evolving, "digitally organic" AI systems that can self-modify and replicate.

The legal and regulatory frameworks are fundamentally unprepared for agentic AI. Current intellectual property laws, for instance, struggle with the concept of AI authorship and originality. This calls for a radical rethinking of legal systems to adapt to a world where AI can act autonomously and deceptively.

Ultimately, the powerful message from the roundtable was a call to action for collective, proactive, and responsible innovation. The participants acknowledged that governments, given their historical limitations in adapting to rapid technological change, may not be the primary drivers of solutions. Instead, a new cadre of leaders and innovators must emerge, willing to "move fast and fix things for good," begging forgiveness rather than asking for permission, to harness AI for the benefit of humanity. This requires a fundamental shift in mindset, from reactive control to proactive, ethically designed systems and a commitment to ensuring AI serves a collective, positive purpose.

Key takeaway: The future of finance, humanity, and technology is converging at an unprecedented speed. While the challenges posed by advanced AI are immense, including ethical dilemmas, workforce disruption, and systemic risks, the potential for positive impact, particularly in areas like financial inclusion and fraud prevention, is equally vast. The critical determinant of this future lies in collective action, responsible innovation, and a willingness to rethink fundamental governance and business models. Missing future Black Swan Summit discussions means missing the vital, candid dialogues shaping these crucial developments.



2 From Security to Continuity: Cyber & Resilience at the Cusp of Quantum

This Black Swan Summit roundtable convened experts to dissect the rapidly evolving landscape of cyber threats, emphasizing the critical interplay between human vulnerabilities, advanced AI, and the looming spectre of quantum computing. The dialogue illuminated urgent needs for a paradigm shift in cybersecurity, impacting executives, policymakers, founders, and academics.

a. The Evolving Threat Landscape: Beyond Traditional Cybersecurity

Key Insight: Cybersecurity must move beyond protecting mere data to safeguarding cognitive assets, as AI weaponizes human vulnerabilities and creates a new "machine versus machine" battleground.

The discussion opened by highlighting the escalating nature of digital threats. While traditional cybersecurity focused on data (like credit card details with a finite lifespan), the new frontier targets health data (permanent and exploitable for fraud) and even human cognition. The rise of AI-powered social engineering has dramatically increased the sophistication of attacks. Deepfake AI, for instance, has already been used to execute multi-million dollar frauds, with one notable case in Hong Kong leading to a $20 million loss. Phishing simulations show high failure rates, even among senior leadership, demonstrating the effectiveness of AI in creating highly convincing scams. The recent "deepseek" development, which significantly reduced the computing power needed for complex AI models and impacted Nvidia's market cap by $1.3 trillion, further underscores the unpredictable and disruptive nature of evolving computational paradigms.

Blockchain, despite its inherent security features, presents a uniquely adversarial environment where human operational security (SecOps) around private key management remains a critical vulnerability. State-sponsored actors, particularly those from Pyongyang, are responsible for a significant portion of digital asset losses, with a single recent Bybit hack accounting for $1.5 billion. Annually, global losses to fraud and scams now represent a GDP comparable to a major nation, growing at an alarming rate exceeding 30% per year.

This arms race necessitates an understanding that AI is being leveraged by both good and bad actors, making the battle increasingly a "machine versus machine" contest.

b. Digital Assets: A Broad and Vulnerable Frontier

Key Insight: Any piece of digital information, from a picture to geolocation, can be a valuable digital asset for criminals, underscoring the vast and expanding attack surface.

The definition of "digital asset" was expanded beyond cryptocurrencies to encompass any valuable data that can be exploited. This includes personal likeness (voice, video), sensitive health records, and corporate data, all susceptible to exploitation by criminals. The challenge is immense, as the maturity of protection mechanisms has not kept pace with the rapid proliferation and adoption of these digital assets.

c. The Quantum Horizon: Urgency and Ethical Imperatives

Key Insight: While the full impact of quantum computing is not yet realized, proactive preparation is crucial to prevent the wholesale breaking of current cryptographic foundations.

Quantum computing presents both a powerful opportunity and a profound threat. Experts noted that while the exact timeline for its ability to break current cryptography (a "quantum-safe" world) is debated, the underlying research and development are advancing rapidly. A significant barrier to quantum readiness is the scarcity of professionals with expertise in both cybersecurity and quantum. Australia's national quantum strategy uniquely emphasizes an ethical, trusted, and inclusive quantum ecosystem, recognizing that the power of quantum applications (from drug discovery to payments and defence) must be developed responsibly. Preparing today means embedding quantum-resilient cryptography into critical systems before adversaries can exploit the gap. Cybersecurity readiness must move in lockstep with quantum progress, or society risks a sudden collapse of trust in digital infrastructure.

d. Forging Continuity: Leadership, Policy, and Human Behaviour

Key Insight: Building resilience in a volatile digital world demands a fundamental shift in leadership, a willingness to rethink governance, and a proactive approach to human cybersecurity hygiene.

The roundtable concluded with a strong call for systemic change in organizational and governmental approaches to cybersecurity:

- **Boardroom Imperative:** Cybersecurity must be elevated to the boardroom level, with technology experts actively participating in strategic decision-making, moving beyond mere compliance checklists.
- **Government's Role**: The "free market has failed cybersecurity" due to misaligned incentives. Governments have a critical role to play in setting clear regulatory "guide rails" and taking a more interventionist approach where necessary, ensuring security is not an afterthought. Concerns about "militarization of cyberspace" were raised, underscoring the need for careful balance between national defence and public interest.
- **Rethinking Human Nature and Machine Nature:** As AI systems learn and evolve in "digitally organic" ways, the concept of "machine nature" must be understood and addressed alongside human behaviour. The ultimate battle is between good and bad actors, and the good guys must leverage AI more effectively.
- **Prioritizing Digital Hygiene:** Despite advanced systems, human actions (e.g., using public Wi-Fi, oversharing personal data) remain the weakest link. Cybersecurity training needs to be continuous, interactive, and integrated into daily operations, rather than a periodic tick-box exercise. A critical question was posed: Do we truly need every "smart" technology if it creates new attack vectors, or should we question the human drive for convenience at the cost of security?

This roundtable made it clear that "security is not a department; it's a mindset." For leaders, policymakers, and innovators, the imperative is to embrace responsible innovation, proactively address technical and ethical risks, and foster a collective culture of cybersecurity from the ground up, ensuring resilience and continuity in a future increasingly defined by intelligent machines. Attending future Black Swan Summit discussions will be crucial for staying ahead of these rapidly evolving dynamics and influencing a secure digital future.

3 There's a Token for That: Exchanging Value in Modern Times

This Black Swan Summit roundtable focused on tokenization, exploring its current state, vast potential, and the significant hurdles preventing its mass adoption. The discussion offered critical insights for executives, policymakers, founders, and academics on how digital tokens are poised to redefine value exchange in modern times.

a. Tokenization: Defining the Opportunity

Key Insight: Tokenization represents an asset digitally, from real-world and financial assets to non-tangibles, promising market efficiencies, increased liquidity, faster price discovery, and enhanced financial inclusion.

The discussion clarified that tokenization, in this context, refers to using cryptographic technology to represent assets digitally on a Distributed Ledger Technology (DLT), whether as "digitally native" assets to the DLT or digital representation of a real world asset (RWA). While the concept has been discussed for years, its full potential remains untapped. Key benefits highlighted include:

- **Market Efficiencies:** Streamlining processes, reducing costs, and enabling faster transactions.
- **Increased Liquidity:** Unlocking value in illiquid assets, such as real estate.
- **Facilitated Price Discovery:** Enabling more dynamic and transparent pricing.
- **Financial Inclusion:** Providing access to financial services and investment opportunities for underserved populations.

b. Current Applications and Challenges in Adoption

Key Insight: While early, successful use cases demonstrate tokenization's power, widespread adoption is hindered by the disconnect between digital and physical assets, interoperability issues, and a lack of regulatory clarity.

Several practical use cases were presented:

- **Stablecoins:** Identified as a "gateway drug" to asset tokenization, stablecoins already surpassed Visa and Mastercard in total transaction volume last year by 7.7%, representing 1% of the entire USD circulation supply. They offer significant benefits for cross-border payments, reducing FX costs and risks for individuals and multinational corporations.
- **Real Estate Tokenization (RWA):** Early attempts in 2018 were costly and complex. However, advancements in white-label solutions and KYC/AML providers have drastically reduced setup costs. A pioneering innovation by a Slovenian firm, Blocksquare, allowed to tokenize a parking space, proving fractional, borderless ownership of real estate. Legal innovations, such as notarized token issuance recorded on land registries with automated enforcement, are enhancing security and trust, as seen in pilot programs in Europe and the US. This enables "fractional ownership" of properties that would otherwise be inaccessible.
- **Trade Receivables Financing:** Tokenizing loan receivables has allowed SMEs to access liquidity more efficiently, reducing bad debt rates to as low as 0.1% for some platforms.

Despite these advancements, significant challenges persist:

- **Physical-Digital Disconnect:** Ensuring the "truthfulness" of the digital twin by maintaining a reliable connection between the on-chain token and its real-world asset (e.g., verifying a carbon credit is still backed by standing trees, or whiskey remains in a cask) is crucial for trust.
- **Interoperability:** Seamless integration between blockchain (web3) and traditional finance (TradFi), as well as between different blockchain networks, remains a hurdle.
- **Regulatory Uncertainty:** A lack of clear, consistent, and cost-effective regulatory frameworks across jurisdictions prompts founders to "vote with their feet," seeking friendlier environments. Japan, for instance, has

classified tokens into stablecoins, security tokens, and crypto assets, with a nascent secondary market for real-world asset tokens.

- **Education and User Experience:** The public lacks understanding of basic crypto concepts like wallets, hindering mass adoption. Success requires simple, safe, and intuitive user interfaces that hide the underlying technical complexity.
- **Liquidity Fragmentation:** New tokenized markets need sufficient liquidity, which requires significant capital deployment across numerous platforms.
- **Taxation and Compliance:** Clear guidance on how to account for and audit tokenized transactions is essential for widespread commercial adoption.

c. The Problem Tokenization Solves: Efficiency, Access, and Redefining Capital Flow

Key Insight: Tokenization is fundamentally about enabling more efficient, accessible, and fluid exchange of resources and capital, potentially leading to unprecedented price discovery and breaking down traditional financial silos.

The core problem tokenization solves is the inefficient transfer of resources and capital. It promises to facilitate this flow more quickly, cheaply, and verifiably. While "fractionalization" existed before, tokenization enhances it by:

- **Democratizing Access:** Allowing individuals to own very small, affordable portions of assets previously exclusive to large investors (e.g., Hilton Hotels).
- **Lowering Friction:** Reducing the cost and inertia associated with traditional asset transfer.
- **Enhancing Portability:** Enabling seamless custody and transfer of assets across borders, addressing challenges faced by global citizens with multiple bank accounts.
- **Facilitating New Markets:** Creating opportunities for investment in local economies that are currently overlooked by major global funds, fostering more equitable distribution of capital.

The panel acknowledged the "incremental" nature of these benefits, but emphasized that across trillions of dollars of assets, even small improvements in efficiency translate to massive value. The potential for "radical price discovery" was highlighted, as tokenization could remove the existing silos and frictions that currently obscure true market value.

d. Trade-offs and the Future Outlook

Key Insight: While tokenization offers immense benefits, it introduces new operational and liquidity risks, and its disintermediating effect may reshape, rather than eliminate, financial service providers.

The discussion did not shy away from the trade-offs:

- **New Risks:** While mitigating settlement and counterparty risks, tokenization introduces operational risks (e.g., smart contract vulnerabilities, bridge attacks) and new forms of liquidity risk (e.g., susceptibility to "toxic flow" in automated market makers).
- **Custody and Responsibility:** Empowering individuals with direct asset custody demands greater personal responsibility for safeguarding.
- **Disintermediation vs. Reshaping Intermediaries:** The rise of agentic AI, which could manage individual investments with the "brain power of the best investment fund," threatens traditional financial intermediaries. However, new types of intermediaries (e.g., bridging partners, token wrappers) are emerging, suggesting a reshaping of the financial services industry rather than its complete elimination. The goal is for a larger, better-distributed financial "pie," with intermediaries making less profit per transaction.

The roundtable concluded that the future of tokenization is not just about clever technology, but about its utility in solving real-world problems for end-users, from daily payments to long-term wealth creation. Mass adoption will come when consumers no longer need to understand the underlying technology but can simply enjoy easy, safe, and accessible financial services. This journey requires ongoing collaboration between innovators, regulators, and users to overcome obstacles and realize tokenization's full, transformative potential.

Authors

Dr. Andrzej Gwizdalski
Global Finance & Technology Network (GFTN)

Contributor

Akanksha Rath
Head of Capacity Building and Learning Initiatives
Global Finance & Technology Network (GFTN)

Production

Carol Ann Christy
Graphic Designer

**Global Finance &
Technology Network (GFTN)**

6 Battery Road, #28-01, Singapore 049909
gftn.co | hello@gftn.com