Technology adoption and integration

In 2026, technology is central to national economic strength. Artificial intelligence, digital assets, and infrastructure are now key tools of power and influence. Governments are linking technology with economic resilience, integrating it into policy for security autonomy and foreign investment. In return, there is an expectation of private sector alignment with national priorities.

Against this backdrop, policymakers have grappled with three key questions:

- To regulate or accommodate: within their own markets, how can authorities foster innovation without sacrificing stability and/or security (a question sharpened by the release of Mythos and the growing ability of AI systems to defend or exploit critical infrastructure at unprecedented speed)?
- To co-opt or to leave to private sector: Debates about unfettered use by government and sharing in the wealth generation of AI companies are blurring the line between private sector corporations that have developed the technologies and national authorities that use the technologies.
- To collaborate or to compete: should national policymakers collaborate with one another or compete – sometimes even impeding rivals?

Overview

Technology-led advancement brings recognised benefits, notably through digital assets, AI capabilities, and critical infrastructure. However, some of the market players – and the capabilities they are creating – are now 'too important to fail', i.e., sufficiently important that regulatory or government control and/or oversight is viewed as needed. But exactly what form that oversight takes is still an open question. More pointedly, rapid progress is creating direct challenges to governments' business models, with major policy concerns revolving around political, social, market, financial, and infrastructure implications. As these effects come into sharper focus, tech companies' reputations are shifting from celebrated innovators to instruments of national and international growth, defence, and stability.

Proposals on how best to harness tech's strengths while also exerting some level of control are beginning to emerge and will likely persist. Many of these initiatives directly affect tech companies, but some also focus on products and capabilities, impacting non-tech industries. Importantly, the emerging approaches are fragmented within and across major centres. Internationally, that amounts to a somewhat uneven approach on:

- the policy tools used – e.g., litigation versus legislation/regulation versus executive orders;
- the extent of control and alignment with national priorities; and,
- the tone of competition – merely outdoing the other or also obstructing.

Observation

Key trend

Mainstream acceptance and increased adoption

The evolving tech landscape centres on three key areas, each shaping regulation around national goals:

1. **Digital assets as regulated infrastructure**
   Digital assets are transitioning from speculative uses to regulated platforms, with stablecoins leading this shift. Policy responses include the US's Guiding and Establishing National Innovation for US Stablecoins (GENIUS) Act, UK's Financial Conduct Authority (FCA) regime, the EU's Markets in Crypto-Assets (MiCA) regulation, and Hong Kong frameworks, all supporting stablecoin integration and real-world application. Global competition is driving diverse models for digital-money ecosystems including central bank digital currencies (CBDCs) and tokenised deposits – with licensing frameworks and tokenisation sandboxes from Singapore to the UAE – resulting in rapid but uneven integration and adoption driven as much by competition as by regulation.

2. **Beyond Generative AI (Gen-AI)**
   Gen-AI and Large Language Models (LLMs) are pushing policy towards accountability (e.g., traceability explainability, human oversight, incident reporting). Competing standards from major centres (US, Europe, China) remain voluntary and lack global coherence. Advances in agentic AI offer new opportunities, yet AI is also central to global tech competition and national security strategies. As such, policy currently lacks internal consistency.

3. **Tech's resilience:**
   As 'foundational' financial technologies embed into traditional financial ecosystems, they are being put to the test by emerging innovations, notably the potential of quantum computing's impact on cryptography. Data localisation rules and cross-border restrictions challenge cloud infrastructure and analytics, with over 75 per cent of state actors enforcing such regulations.[5] System outages and dependencies highlight the importance of operational resilience. Data centres are now deemed critical infrastructure alongside undersea cables.

The issues in the balance for policymakers

Policymakers and regulators are examining various areas of focus, both old and new, to encourage innovation while minimising risks. Regions use legislation, regulation, supervision, and litigation to varying degrees. Given tech's ubiquity, traditional sector-based regulation is often unsuitable. Policy responses now target specific tech firms or products (such as digital assets and AI), resulting in a mix of entity-level and activity-level regulations. The specific areas that are of relevance are:

- **Competition/anti-trust:** Increasing scrutiny of mergers, restricting tech companies' preferential treatment, and opening datasets to new entrants; industrial policy tools are also used to address global imbalances.
- **Data management:** Privacy and data rules govern access and transfer.
- **Consumer protection:** Regulations on ethical AI, illegal content removal, and consumer redress.
- **Stability standards:** Prudential rules ensure operational resilience across industries.
- **Safety standards:** Guardrails for human-out-of-the-loop, agent-to-agent interactions.

What policymakers are doing

From a policy perspective, nations' approaches to technology frameworks fall along a continuum anchored by three main poles, each reflecting regional interests and priorities to be protected or promoted in distinct ways.

- The **US** – which emphasises tech development and market interests of companies and investors.
- **China** – which emphasises technology use.
- **Europe** – which emphasises consumer protection and technology sovereignty as an instrument of strategic autonomy.

Other important markets, who array themselves across this spectrum include:

- **UK** – the UK's FCA rules (and EU's MiCA framework) seek to embed digital assets within existing national prudential frameworks.
- **UAE** – the Central Bank's Payment Token Services Regulation established a framework for AED-backed stablecoins with licensed issuers.
- **The Kingdom of Saudi Arabia** – announced plans to introduce stablecoins under national regulation, though frameworks remain under development.
- **India** – is positioning itself as a hub for affordable and scalable AI, using its large skilled workforce, digital user base and growing private investment to advance domestic innovation.

Expectations

Policy trajectory

In the US, a business-focused growth model aligned with government is likely to persist but could face backlash if seen as exploitative or partisan. China may strengthen its tech-industrial policies for self-reliance and global reach. The EU aims to simplify digital rules and boost funding but may struggle with slow legislation and drift toward protectionism. Middle and emerging powers seek balance between major players, with groups like ASEAN pursuing shared governance. Despite fragmented regulations, mutual regime recognition – especially between the UK and US – may become more likely.

5. McKinsey & Company, Localization of data privacy regulations creates competitive opportunities. 2022.

The rise of stablecoin: Stablecoins are set to lead private digital currencies, driven by US innovation and supportive policies, especially as CBDCs lag. Adoption will likely accelerate in emerging markets, while developed markets may enforce tighter controls. Improved licensing and interoperability are likely to increase financial access by linking tokenised deposits to public payment systems. Institutions are working to expand stablecoin use, potentially growing the market up to USD2 trillion by the end of 2028 – a ten-fold increase over three years.[6] Regulators are expected to apply Basel standards to clarify which activities remain regulated or shift to unregulated exchanges, while debates on the role of the dollar often miss key shifts in global payment networks.

Modernising payments infrastructure: ISO 20022 and CBDC pilots, progressing unevenly by region, are driving payment upgrades through bank-fintech-blockchain partnerships for cross-border transactions.[7] Increased competition from non-banks is pushing banks to team up with embedded finance firms. Notable areas to watch include US sanctions prompting alternative payment rails, G20 aiming to reduce retail payment costs below one per cent by 2027, and machine learning plus digital tools easing Anti-Money Laundering (AML)/Know Your Customer (KYC) for high-volume payments.[8]

AI is adopted but rules diverge: Enterprises are set to expand AI integration in areas like credit, compliance, and customer analytics, while regional regulations and policy will differ, prioritising competitiveness, innovation, sovereignty, and/or safety. Without coherent legislative framework, courts will likely increasingly resolve legal disputes related to AI, while organisations focus on more immediate practical issues, such as management of cybersecurity threats and workforce changes.

Progress towards quantum readiness: While the technology for large scale quantum computing remains hindered, AI-accelerated advances in cryptanalysis are bringing forward the timeline for cryptographic risk. Regulators are seeking to prioritise post-quantum cryptography and partnering with financial institutions to develop expertise and set up quantum excellence centres.

First order effect

Data centres as the next battleground

The expansion and location of data centres are becoming key elements in strategic competition. Building a sovereign AI stack – which integrates compute, models, data, and infrastructure – requires sustained spending of at least one per cent of GDP, a level achievable by only a few state actors.[9] Nations like India, Canada, Australia, and Japan are adopting versions of sovereign AI cloud strategies to increase control over computing resources, data localisation, and connectivity, while recognising the limits to complete independence. More broadly, access to abundant, affordable renewable energy is emerging as a structural differentiator in attracting AI investment, with implications for economic and geopolitical strength. At the same time, local backlash to the energy demands of data centres may place limits on their expansion in some markets.

Second order effect

Who decides: responsible autonomous AI

Legal frameworks have struggled to keep up with AI advancements. While most legal and regulatory systems allow broad access to public information, human capacity has historically constrained its use, forcing attention onto top priorities. AI is removing this structural constraint, raising questions about whether all accessible data should be used, and for what purpose. Where rapid and fairly accurate AI-driven predictions apply to or influence users at scale, this may cause widespread and potentially destabilising actions. Moreover, as autonomous AI-to-AI agent interactions become routine, finance, commerce, defence, and labour markets among other aspects of life will be transformed, prompting questions about human involvement and control over AI decisions. These issues underscore the urgent calls for discussions about responsible AI use as technology approaches a point where humans might be neither "in the loop" nor "on the loop".

Questions

In assessing the trajectory of this trend over the next two years, we will be considering the following questions:

1. Will tokenisation displace conventional money as a dominant store of value and, if so, will token-based systems remain subject to monetary authority or fragment beyond the reach of any single jurisdiction?

2. Will diverging regulatory regimes in digital assets converge around meaningful interoperability? If so, how much friction should remain by design, given that seamless, always-on transferability may enhance access but amplify contagion risks?

3. As AI governance frameworks take shape, who retains meaningful control over AI as a tool: states, developers or the institutions that deploy it? And what trade-offs between autonomy, efficiency and sustainability will that contest produce?

6. Standard Chartered Global Research, Stablecoins – Implications for EM, 2025.
7. ISO 20022: a global standard for financial messaging, i.e., the structured data exchanged between institutions to execute and record transactions."
8. FSB, G20 Roadmap for Enhancing Cross-border Payments, 2025.
9. Gartner, Gartner Predicts 35 per cent of Countries Will Be Locked Into Region-Specific AI Platforms by 2027, 2026.

Disclaimer

This communication has been prepared by Standard Chartered ("SC") Group Public and Regulatory Affairs team. It is general and data-driven in nature and has been provided solely for information/educational purposes. It may not be reproduced or be used to create derivative works, redistributed, or transmitted, whole or in part, without attribution and the prior written consent of SC.

This is not research, nor a product of SC's Global Research Department. Any views and opinions expressed herein belong to the author(s) and may differ from those of SC's Global Research and other departments or affiliates of SC.

This communication does not contain or constitute investment advice, a recommendation to enter into any product or service, nor does it market any product or service provided by SC or constitute solicitation. It is not intended for distribution, publication, or use in any jurisdiction where such distribution, publication, or use would be unlawful, nor is it aimed at any person or entity to whom it would be unlawful for them to access.

SC does not provide, and has not provided, any strategic or specialist advice, including legal, regulatory, accounting, model, auditing or taxation advice or services. Laws, rules, regulations, standards, and other guidelines will differ in different countries and/or may change at any time without notice. You are advised to make your own independent judgment (with the advice of your professional advisers as necessary) with respect to the risks and consequences of any matter contained herein.

Predictions, projections, or forecasts contained herein are not necessarily indicative of actual future events and are subject to change without notice. All opinions and information are given as of the date of this material and are subject to change without notice SC assumes no duty to update any information in this material in the event that such information changes.

While all reasonable care has been taken in preparing this communication, SC makes no representation or warranty as to its accuracy or completeness, including of any information/research obtained from third parties used in its production. It does not purport to identify or suggest all the risks (direct or indirect) that may be associated with conducting business. Any liability (including in respect of direct, indirect, or consequential loss or damage) is expressly disclaimed.

Standard Chartered Bank is incorporated in England with limited liability by Royal Charter 1853 Reference Number ZC18. The Principal Office of the Company is situated in England at 1 Basinghall Avenue, London, EC2V 5DD. Standard Chartered Bank is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority.