Summary: Digitalisation of finance

Overview

This summary provides an overview of the 'Digitalisation of finance' report published by the Basel Committee on Banking Supervision in May 2024. The report delves into the transformative effects of digitalisation on the banking industry, exploring the adoption and implications of emerging technologies, the emergence of new market participants, and the associated risks and challenges. It also discusses the evolving regulatory landscape and the strategic responses of banks and supervisors to the digitalisation of finance.

Section 1: Innovative Technologies and Their Applications in Banking

The ongoing digitalization of finance is characterized by the increasing adoption of innovative technologies within the banking sector. This section of the report examines the use of such technologies, focusing on those that are widely implemented by banks in either development or production stages. It excludes technologies like quantum computing, which may have future implications, and does not address the potential impact of central bank digital currencies. The technologies under consideration are integral to various aspects of the banking value chain, enhancing the efficiency and capabilities of financial services.

Section 1.1: Application programming interfaces

Application programming interfaces (APIs) are increasingly utilized in the financial sector to enable efficient real-time data sharing and execution of financial services between software applications. Banks employ APIs for data exchange within their internal systems, such as mobile banking, and with external partners or unrelated third parties, like sharing transaction data with accounting software or for supervisory reporting. APIs are considered secure and provide banks with control over customer data access. They enable partnerships with third-party firms for integrated services, new business models, and secure outsourcing.

Open banking/finance frameworks, which vary globally in their mandatory or voluntary nature, scope, and regulatory approach, leverage APIs to foster innovation, competition, and financial inclusion. These frameworks differ in the types of data shared, API usage mandates, customer consent, licensing of third parties, and cost arrangements. Open banking/finance is expected to scale up customer-permissioned data sharing, spurring further innovation in products and business models.

The South Korean open banking system, launched in 2019, is a market-led infrastructure that uses standardized APIs to provide banking services through a central hub, the Korea Financial Telecommunications and Clearings Institute (KFTC). Participation is voluntary for licensed institutions, and the system offers both inquiry and transfer APIs, enabling a variety of financial services. With 136 institutions participating and 35 million subscribers, the system benefits from network effects, reducing costs and increasing overall benefits.

Globally, open banking/finance initiatives are being adopted or considered, with the potential to significantly impact the financial services industry by enabling large-scale, customer-permissioned data sharing and fostering innovation.

Section 1.2: Artificial Intelligence and Machine Learning in Banking Operations

Banks are increasingly integrating artificial intelligence and machine learning (AI/ML) across various functions, including credit underwriting, trading, and fraud detection. These technologies enhance operational efficiency, risk management, and customer service by streamlining processes, improving predictive accuracy, and enabling the handling of large, unstructured datasets. In Italy, banks are using ML for credit scoring, which has improved risk assessment accuracy and may facilitate credit access for underserved applicants. These models balance accuracy with explainability and are developed mainly in-house, sometimes with external support. While ML models assist credit analysts, some institutions plan to automate credit lending fully after performance monitoring. Post hoc explainability tools are being developed to understand decision-making variables, although these are not disclosed to customers. Fairness standards to prevent discrimination are not yet widespread.

In Asia, the Monetary Authority of Singapore (MAS) encourages AI use in anti-money laundering (AML) efforts, focusing on explainability and effectiveness. MAS has also co-created COSMIC, a digital platform for sharing high-risk transaction analysis among banks. In Japan, the Japanese Bankers Association's Cooperation Agency for Anti-Money Laundering (CAML) provides AI scoring services to assess the riskiness of transaction alerts. Banks remain cautious in AI adoption due to regulatory uncertainties regarding accountability and ethics, among other factors. Generative AI use in banking is limited but being explored for internal operational efficiency improvements.

Section 1.3: Distributed Ledger Technology in Financial Services

Distributed ledger technology (DLT) offers potential benefits for the financial sector, including the creation of central bank digital currencies, asset tokenization, and enhanced operational management. DLT can reduce costs and increase efficiency through immutable record-keeping, digital identity, atomic settlement, and automation, which may also decrease the need for intermediaries. However, the realization of these benefits faces legal and other challenges, and the current scale of DLT-based products in banking is not systemic due to a fragmented ecosystem and interoperability issues.

Banks are increasingly interested in tokenization, which allows for digital representation of assets on a programmable platform, leading to innovative financial asset usage and new arrangements. Use cases include tokenization of real estate, equity, customer shares, financial instruments, and even art ownership, allowing for fractional investment and trading. Banks are also exploring tokenized liabilities and stablecoins.

DLT applications in banking extend beyond tokenization to include identity verification, settlement, cross-border payments, digital asset custody, and real-time asset management. Despite these diverse applications, DLT's market share remains small.

Most banks prefer private permissioned ledgers for their DLT activities, but some are considering public permissionless ledgers, which could integrate with the crypto ecosystem and reduce costs but require new risk management approaches. For instance, banks are investigating how to manage AML and KYC risks on permissionless blockchains using smart contracts or verifiable credentials.

An example of a bank-issued stablecoin is Société Générale's EUR CoinVertible (EURCV), launched on the Bitstamp exchange. EURCV is a euro-backed stablecoin designed to comply with the EU's Markets in Crypto-Assets Regulation, ensuring transparency and asset segregation. It is available on the Ethereum blockchain and other platforms, with trading accessible to parties that pass compliance checks. The reserve assets for EURCV are cash or certain securities, segregated and managed by a third party, providing direct recourse for stablecoin holders.

Section 1.4: Cloud Computing

Cloud computing is transforming the financial services industry by providing on-demand computing resources that enhance efficiency and reduce costs. It enables easier access to technology and infrastructure, lowering barriers to entry for firms and allowing for scalability. The European Central Bank's survey indicates that distributed ledger technology (DLT) has a low adoption rate among banks, with less than 20% utilizing it. Cloud services are categorized into four main service models and three deployment models: public, private, and hybrid clouds, each with distinct characteristics regarding resource delivery, access control, and data sharing.

Financial institutions, including banks and fintech companies, are increasingly adopting cloud services for a variety of functions. This shift is driven by the need for greater efficiency, improved interoperability, and the ability to handle fluctuating computing demands without the expense of building and maintaining on-premise data centers. Cloud providers can offer robust operational resilience, often at a lower cost due to economies of scale. The trend towards cloud computing has accelerated, partly due to the digitalization push from the Covid-19 pandemic, with banks initially using Software as a Service (SaaS) and gradually moving to Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). Workloads moved to the cloud vary, with some banks migrating low-risk functions and others transitioning core systems. Some banks, especially digital banks, operate entirely on the cloud, while others adopt a cloud-first strategy for new offerings.

Minna Bank in Japan exemplifies a cloud-only bank, utilizing a multi-cloud approach for its core banking systems, contact center, and employee virtual desktops. Targeting digitally native customers, Minna Bank focuses on providing financial services through smartphones. The emergence of new entrants and business models in the financial sector is concurrent with these technological advancements.

Section 2: New competitors and business models

Financial technology advancements have led to the entry of new competitors and the development of innovative business models in the banking sector. These changes have primarily manifested in increased competition, especially in payment services, and the formation of strategic alliances between traditional banks and various firms. The review in this section focuses on the impact of these new entrants and the changing business models of banks, which are part of the broader digital transformation within the industry.

Section 2.1: New entrants

Innovative technologies have enabled new digital-only banks, fintechs, and large technology companies to enter the banking and financial services sector. These entities often possess technological and data advantages over traditional banks, such as the absence of legacy IT systems, and may operate without the same regulatory constraints. Neobanks, which target individuals and small businesses, offer services like accounts, credit cards, and loans, and can often operate more cost-effectively due to their lack of legacy infrastructure. However, they may face challenges such as less stable funding and, in some cases, partner with incumbent banks to access banking licenses.

Fintechs typically focus on specific banking services, using digital channels for customer acquisition and specializing in areas like lending and payments. They are expected to continue growing, particularly in higher-risk financial segments. Big tech companies leverage their extensive user networks and data analytics to provide financial services, especially in payments, and have the potential to become dominant market players.

An example of big tech's expansion in financial services is Mercado Libre in Latin America, which offers an online marketplace, digital payment solutions, and credit products, using data from its platforms for credit assessments. While not regulated as banks, these platforms can enhance financial inclusion and efficiency

for consumers.

Some new entrants may seek bank regulation to access benefits like deposit insurance and central bank accounts, as seen during the Covid-19 pandemic when weaknesses in non-bank funding models were exposed. Others may form partnerships with banks to gain similar advantages. Despite their small size compared to traditional financial institutions, these new entrants are considered more agile and user-friendly, and they continue to expand their presence in the financial services industry.

Section 2.2: Banking Partnerships

Banks are increasingly forming partnerships with non-banks and technology firms to enhance their operational efficiency, expand their offerings, and strengthen customer relationships. These collaborations often utilize APIs, enabling third-party access to banks' systems. Banking as a Service (BaaS) is a model where banks provide services through non-bank intermediaries like fintechs and big techs, which interface directly with clients. The typical roles in these partnerships include banks holding deposits, processing payments, and extending credit; platform providers offering necessary infrastructure; and non-bank intermediaries engaging with customers.

These partnerships leverage the strengths of both banks and non-banks, with banks contributing their infrastructure, expertise, and regulatory framework, and non-banks offering product innovation, data analytics, and enhanced user experiences. Successful partnerships can lead to improved services, increased business for both banks and non-banks, and benefits for consumers and businesses through greater competition, efficiency, lower prices, and innovation.

In the United States, platform providers like Synapse, Synctera, Treasury Prime, and Unit are rapidly evolving, offering comprehensive solutions that facilitate the connection between fintechs, banks, and end users through APIs. These platforms support a range of services, including payments, deposits, lending, identity verification, card issuance, and investments, as well as compliance functions like anti-money laundering and know your customer checks.

While BaaS is not yet a significant portion of banking services and is more common among smaller banks, it offers opportunities for these banks to overcome challenges such as technology upgrade costs and competitive pressures. BaaS enables smaller banks to expand their customer base beyond regional or market limitations and outsource functions to third parties for more efficient operations.

Section 3: Risks

The section of the report acknowledges the numerous benefits that digitalisation brings to banks and consumers, such as innovation, efficiency, enhanced risk management, improved financial inclusion, reduced transaction costs, and increased competition. However, it also highlights that digitalisation can introduce new vulnerabilities and exacerbate existing risks, affecting banks, their customers, and overall financial stability. The report proceeds to examine these potential risks and vulnerabilities in greater detail, clarifying that the sequence of topics does not imply their relative importance.

Section 3.1: Strategic Risks

Banks are grappling with strategic risks as they navigate the digital finance landscape, where they face stiff competition from fintechs and big tech companies. These non-bank entities are challenging traditional banks by offering financial services integrated with other products, and open banking regimes are encouraging customer mobility, potentially diminishing banks' market share and profitability. To stay

competitive, banks may enhance their digital capabilities, form partnerships with tech firms, or diversify their revenue streams, such as collaborating with e-commerce platforms. However, these strategies introduce new risks.

Digital transformation initiatives are fraught with strategic and operational risks, particularly for smaller banks with limited resources to upgrade their technology and expertise. These banks risk falling behind more agile, digital-first competitors. Partnerships with non-banks also present strategic risks, as banks could become dependent on these entities for business origination, losing control over key aspects of their operations and potentially their customer base, which could have severe consequences for their liquidity and financial performance. Such partnerships might lead to narrow banking models, where banks offer a restricted range of services, increasing their reliance on fee income and creating vulnerabilities in their business models and balance sheets.

Section 3.2: Reputational Risks

Banks engaging with new technologies and third-party partnerships face increased reputational risks, which are critical given the reliance on depositor and market confidence. The use of complex AI/ML models, due to their potential for opaque and discriminatory outcomes, can lead to negative publicity and regulatory sanctions. Banks' associations with non-bank entities can also impact their reputation, affecting their business operations and relationships with consumers, investors, and service providers. This may hinder a bank's ability to secure liquidity or professional services. Even with clear liability demarcations, banks can suffer reputational damage from incidents such as customer data breaches. Additionally, banks may encounter "step-in" risks, feeling compelled to intervene in the event of financial distress within non-bank partners to ensure service continuity and protect customer assets.

Section 3.3: Operational Risks

Operational risks in the context of digitalisation encompass a range of potential issues that could lead to losses for banks. These include model risks associated with AI/ML, such as lack of explainability, overfitting, and data biases that could result in unethical outcomes. Technology risks arise from the challenges of integrating new technologies with legacy IT systems, vendor lock-in, and transparency issues. Cyber risks are heightened due to increased interconnectivity and reliance on technologies like APIs and cloud computing, which may expose the banking system to more cyber threats. Legal uncertainties are present as new technologies test existing legal frameworks, raising questions about the legal status of digital assets and accountability for AI-driven decisions. Compliance risks are elevated when banks engage with cryptoassets or rely on non-bank partners for KYC and AML checks, potentially leading to issues with money laundering and terrorism financing. Fraud-related risks are evolving with digitalisation, as fraudsters use sophisticated techniques like deepfakes. Third-party risks are amplified when banks depend on external service providers, which can affect information security and operational resilience. Overall, these operational risks may be intensified by inadequate governance and risk management practices, such as poor technological literacy, oversight of data governance, and reliance on third-party systems. Effective management of these risks is crucial for maintaining operational resilience in the face of digitalisation.

Section 3.4: Data Issues and Related Risks

The section discusses the challenges and risks associated with the increasing use of data in banking due to digitalisation. Banks face data governance issues due to the volume, velocity, variety, quality, and integrity of data. The use of alternative data, such as utilities billing and social media information, presents specific risks including the lack of historical data to confirm its predictive value, privacy concerns, and potential

biases, which are exacerbated when used with AI/ML applications. Integration of new data sources with legacy risk management processes poses additional challenges, such as aligning new underwriting methods with existing credit loss models.

The sharing of data between banks and third parties increases the risk of data breaches and cyber attacks. Partnerships with non-banks introduce complexities in data ownership and accessibility, which can affect a bank's ability to comply with regulatory requirements, such as anti-money laundering and counter-financing of terrorism (AML/CFT) obligations. For instance, banks may need to collect information on end users in bank-fintech arrangements, even without a direct relationship, to understand compliance obligations. Fintechs may view certain data as proprietary, complicating the bank's regulatory compliance efforts.

Section 3.5: Financial Stability Risks

The section on financial stability risks highlights the potential threats to the banking system and overall financial stability posed by the digitalisation of finance. These risks include increased interconnections between banks, fintechs, and technology firms, which add complexity and make it difficult for supervisors to manage risks, especially since these networks have not been tested in an economic downturn. Regulatory arbitrage is another concern, as non-banks providing banking-like services without equivalent regulation could introduce vulnerabilities. The speed of technological transactions and information transmission could accelerate contagion across institutions or markets, with the integration of crypto/DeFi ecosystems and traditional finance increasing spillover risks. Digitalisation may also amplify traditional financial risks, such as liquidity risks, and encourage procyclical behaviors through automated models. New infrastructures like DLT could lead to market fragmentation, and the dominance of private digital currencies could pose risks to financial stability. Concentration risks may arise from reliance on specific infrastructures, models, or third-party service providers, with system-wide impacts from failures or outages.

Generative AI (GenAI) presents unique risks, including model risks like reasoning errors and "hallucinations," challenges in explainability due to model complexity, data governance issues with large data sets, and governance and accountability concerns for banks using GenAI. Third-party risks are also significant, as banks may depend on external providers for GenAI models, raising issues of transparency, privacy, security, and cyber risks. The broad adoption of GenAI could lead to increased interconnectivity and interdependencies, amplification of traditional financial risks, and greater third-party concentration risks.

The document further discusses banks' risk management strategies to address the challenges of digitalisation, which will be elaborated in subsequent sections.

Section 4: Banks' Risk Management Strategies in the Digital Era

Banks have implemented a variety of strategies and practices to address the risks associated with the digitalisation of finance. These measures are diverse and continuously evolving, with their effectiveness yet to be fully proven across different business cycles and stress periods. The effectiveness of these risk mitigation strategies remains to be tested in various market conditions.

Section 4.1: Governance and Risk Management in the Digitalisation of Finance

Banks are enhancing governance and risk management to address the challenges posed by the digitalisation of finance. This includes updating strategic and business planning to account for the impact of new technologies and market entrants, investing in digital capabilities, and improving cost efficiency. Staff development is being prioritized to manage fintech risks, and new product approval and change management processes are being strengthened. Banks are aligning risk management with the Basel

Committee's principles for operational risk and resilience, and ensuring new offerings comply with regulatory requirements, including consumer and data protection, as well as anti-money laundering and counter-financing of terrorism (AML/CFT) standards.

To mitigate risks from application programming interface (API) usage, banks are adapting controls for IT risk management and third-party relationships. This includes due diligence, secure coding, data encryption, access management, and regular security audits. API practices are being implemented to control access and data flow, with measures such as the principle of least privilege, API gateways, certificate pinning, secure storage of API keys, and restrictions on API key usage.

Regarding distributed ledger technology (DLT), banks are applying existing risk frameworks to governance, reporting, monitoring, and business continuity, while adjusting them for DLT-related activities. DLT is mainly used to expand existing business cases, and banks are conducting pilots and proof of concept exercises to identify cybersecurity and legal requirements. Some banks participate in innovation and fintech accelerator programs to support startups and explore DLT use cases. Advanced banks use a phased and risk-based approach for DLT adoption, often within regulatory sandboxes to gain supervisory guidance. Banks must also meet cyber resilience requirements, including secure coding and robust technology risk governance frameworks.

Section 4.2: Model risk management

Banks are enhancing their model risk management frameworks to address the complexities and risks associated with AI/ML, particularly for more material AI applications which require greater human oversight. Understanding model outputs, including potential biases and limitations, is crucial for effective decision-making and risk management. Banks are employing tools like post hoc explainers to aid in understanding AI functions and outputs, while also recognizing the limitations of these tools.

To manage AI risks, banks are updating governance structures and risk management frameworks, with some establishing executive committees focused on AI-specific issues such as ethics and explainability. A risk-based approach is being adopted for generative AI, with controls being built out and various measures implemented that generally extend existing model risk management frameworks. These measures include establishing AI policies, enhancing human oversight, promoting employee education, requiring enhanced validation, formalizing approval processes, and enhancing governance structures to manage data, model, and operational risks.

Specific practices to mitigate generative AI risks involve restricting its use to non-strategic activities, limiting data sharing with external parties, and implementing constraints on model outputs. Technology usage includes grounding models in ethical guidelines, using retrieval augmented generation, and ensuring security through adaptation and checks. For third-party AI models, banks may conduct security scans, restrict personal data use, and apply internal controls. Banks also evaluate vendor models for biases and integrate third-party applications into broader outsourcing frameworks.

Section 4.3: Data Governance in Banking Sector

Banks are implementing various strategies to mitigate data-related risks, including breaches and privacy concerns, which arise from the adoption of innovative technologies. To manage the risks associated with third-party data sharing, banks utilize master service agreements that outline data maintenance, access, rights, ownership, intellectual property, and security requirements. They also perform due diligence on third parties to evaluate their data controls and may conduct ethical reviews to understand data usage intentions. Risk ratings are assigned to data based on its use case, influencing the decision to share data with third parties. Certain jurisdictions mandate more secure data sharing methods, such as tokenized authentication

via APIs, to enhance control and security.

When incorporating new data sources, banks are cautiously applying their existing data governance and risk management frameworks, with additional controls for high-risk scenarios, such as those requiring customer-explainable outcomes. Ethics are increasingly considered in data decision-making, assessing not only the capability but also the appropriateness of data usage. In the context of AI/ML applications, banks are integrating the management of alternative data within their AI/ML governance processes.

Section 4.4: Third parties

Banks are actively managing risks associated with third-party engagements, particularly in outsourcing and cloud computing services. They employ due diligence, operational risk management, continuous monitoring, and enforce contracts that clearly delineate responsibilities and service levels, including audit rights. Regulations often mandate these contracts to ensure banks can inspect and audit third-party services, with some jurisdictions extending these rights to supervisory authorities.

With the growing reliance on cloud technology, banks are conducting comprehensive risk assessments to address cybersecurity concerns, such as data protection and supply chain vulnerabilities. They require cloud service providers (CSPs) to implement robust security measures, including data encryption and access controls, often verified through third-party assessments or certifications. Despite CSPs managing the cloud infrastructure, banks maintain certain responsibilities, such as managing encryption keys.

Banks have varying strategies to manage potential concentration risks from using a single CSP. Some accept the risk for operational efficiency, while others use multiple CSPs or combine cloud services with on-premise systems to distribute their workload. Banks also prepare comprehensive exit strategies to ensure a smooth transition if they need to switch CSPs.

The dominance of a few CSPs presents challenges in terms of switching providers, interoperability, and oversight due to potential limitations on access rights. The complexity of cloud models can obscure operational and concentration risk exposure, especially when involving fourth-party CSPs. While contracts typically include audit clauses, their practical enforcement can be challenging.

To overcome these challenges, banks are engaging in industry initiatives and joint audits, and participating in forums to discuss common issues with supervisors and CSPs, aiming to enhance the industry's resilience in cloud service utilization. These efforts are part of a broader response to the digitalization of finance, which includes evolving regulatory and supervisory frameworks.

Section 5: Regulatory and Supervisory Initiatives

Regulatory and supervisory frameworks have been adapted to address the challenges and risks brought about by the digitalisation of finance. These initiatives aim to ensure the safety and soundness of the banking sector while promoting responsible innovation. The evolving regulations consider the need for a level playing field, guided by the principle of "same risk, same activity, same regulation" to prevent regulatory arbitrage. Additionally, the importance of human judgment in risk management and supervision is underscored, despite the growing reliance on automated processes. International cooperation is highlighted as essential for dealing with the cross-border and cross-sectoral effects of digitalisation.

Section 5.1: Regulatory Frameworks

Regulatory frameworks are adapting to the risks introduced by the digitalization of finance, with

international standard-setting bodies issuing new standards and guidance, such as the Basel Committee on Banking Supervision's (BCBS) standards on cryptoasset exposures and principles on operational resilience and risk. National authorities are also updating their regulations, often adopting a technology-neutral stance that adheres to the principle of "same activity, same risk, same regulation." Legislative frameworks are expanding the regulatory perimeter in some jurisdictions to include oversight of cryptoasset activities and critical ICT third-party service providers.

The European Union is advancing legislative initiatives like the Digital Operational Resilience Act (DORA) and the Markets in Crypto-Assets Regulation (MiCA) to harmonize rules and foster innovation while ensuring financial stability and consumer protection. The Artificial Intelligence Act (AI Act) is another EU initiative aimed at ensuring trustworthy AI, with banking supervisors overseeing compliance for high-risk use cases.

Licensing frameworks for digital-only banks generally follow the same requirements as traditional banks, with some adaptations allowed for digital entrants. Some jurisdictions have distinct licensing processes or criteria for digital-only banks, and may exempt them from certain prudential requirements or remove impediments like the need for a physical main office.

Supervisors are using existing guidance on technology and operational risk management to oversee banks' use of innovative technologies. Some have issued technology-specific guidance, such as for open banking frameworks and APIs, while others have provided principles or guidance on AI/ML, promoting a risk-based approach. For distributed ledger technology (DLT), conservative rules are common, with some supervisors issuing guidelines on DLT-related activities and tokenization initiatives.

Cloud computing risks are being evaluated, with some jurisdictions issuing cloud-specific requirements and considering direct oversight mechanisms for critical third-party service providers. Banks' partnerships and use of third parties are supervised using existing regulations and guidance, with some authorities developing more specific guidelines for new business models.

Overall, regulatory and supervisory frameworks are evolving to address the challenges of digitalization, with a focus on mitigating risks and fostering innovation while ensuring the safety and soundness of the banking system.

Section 5.2: Supervisory approaches and tools

Banking supervisors are adapting their approaches and tools to address the challenges posed by the digitalization of finance. They face issues such as the technical complexity of new technologies, limited oversight of certain activities, uncertainty regarding the legal status of products like tokenized assets, and a lack of standardization. Supervisors are guided by a risk-based approach and are considering how to balance innovation with risk mitigation.

In response, supervisory strategies are being updated to assess digitalization-related risks and strengthen frameworks for early corrective action. Organizational changes include forming specialist teams for cyber and operational risks, and creating fintech hubs for collaboration and research. Training programs are being implemented to upskill supervisors on new technologies and broader topics, and some authorities have established digital finance academies.

Supervisors are also requiring banks to notify or seek approval before adopting new technologies or entering into third-party arrangements. Prudential reviews now emphasize technology and cyber risks, and business model analysis is focusing on new and emerging models.

To enhance oversight, supervisors are increasingly using suptech tools for tasks like text analysis, sentiment analysis, market surveillance, and automating supervisory processes. These tools also help monitor trends in the fintech sector, including crypto and DeFi projects.

Supervisory cooperation is growing, with engagement between public and private sector participants on digitalization-related topics. This includes collaboration with domestic agencies, international standard-setting bodies, and industry experts. Authorities are also working with non-bank firms and have established regulatory sandboxes to test new technologies.

Efforts to promote digital innovation include showcase events, roundtables, and training sessions. Some supervisors have set up support desks for fintech consultations and conducted roadshows to strengthen digital capacity in smaller banks.

Project Guardian is an example of cross-border cooperation, aiming to explore asset tokenization and manage associated risks. It involves industry pilots, policy development, and technology standards, with the Monetary Authority of Singapore (MAS) partnering with international regulators and institutions to develop standards for asset tokenization.

Section 6: Implications for Banks and Supervisors

Advances in digitalization are significantly affecting the banking sector, presenting both opportunities and risks that necessitate effective governance and risk management. Banks and supervisors must address the evolving nature of risks, particularly strategic and operational, and their interplay with traditional financial risks. The Basel Committee on Banking Supervision (BCBS) will continue to monitor these developments and may develop new standards or guidance as needed.

The adoption of innovative technologies and business models offers benefits such as increased efficiency and improved customer experiences. However, it is crucial to ensure that innovation is responsible and does not compromise the safety and soundness of the banking system. Supervisors are actively monitoring these developments and engaging in initiatives to promote responsible innovation.

The digitalization of finance is challenging the traditional supervision paradigm by enabling non-banks to offer banking-like services. To prevent regulatory arbitrage, the principle of "same risk, same activity, same regulation" should be integrated into regulatory frameworks. Supervisors may need to review and adapt their oversight to ensure appropriate regulation of banking activities, even when conducted by non-banks.

Data has become a critical resource, necessitating robust data governance and secure data sharing practices by banks. Supervisors should support effective data governance and address broader public policy issues related to data. The increased use of service providers by banks introduces operational and systemic risks, requiring banks to implement strong risk management practices and supervisors to assess systemic risks from service provider concentration.

Despite the automation benefits of digitalization, human judgment remains essential in bank risk management and supervision. Banks must maintain accountability for decision-making, and supervisors should use technology to augment, not replace, their judgment.

Banks and supervisors need to ensure they have the necessary skills and expertise to manage digital innovations and associated risks. This may involve staff training and hiring specialists. Public/private forums and broader dialogue with various stakeholders can enhance understanding and address digitalization's risks and benefits.

Effective communication and cooperation among bank supervisors and other relevant authorities are vital to address issues beyond prudential supervision, such as data privacy and cyber security. International cooperation is also important to promote effective policy responses and limit risks from regulatory fragmentation. The BCBS provides a global forum for supervisory exchange and cooperation.

Appendix: Glossary of terms

The Appendix of the report serves as a glossary, defining key terms related to the digitalisation of finance. It includes explanations of concepts such as alternative data, application programming interfaces (APIs), artificial intelligence (AI), banking as a service (BaaS), big tech, cloud computing, cryptoassets, data governance, decentralised finance (DeFi), distributed ledger technology (DLT), large language models (LLMs), machine learning (ML), neobanks, open banking/finance, and service providers. These definitions provide clarity on the terminology used throughout the report, facilitating a better understanding of the digital transformation within the banking sector.