Financial Innovation and Digitalisation: Impact on Deposit Insurance Systems

IADI Report

January 2026

This publication is available on the IADI website (www.iadi.org).

Contents

Abbreviations

AI	Artificial intelligence
APIs	Application programming interfaces
BaaS	Banking as a service
BCBS	Basel Committee on Banking Supervision
BIS	Bank for International Settlements
CBDC	Central bank digital currency
CPMI	Committee on Payments and Market Infrastructures
DLT	Distributed ledger technology
EBA	European Banking Authority
ECB	European Central Bank
EMT	E-money token
EU	European Union
FSB	Financial Stability Board
FATF	Financial Action Task Force
GENIUS Act	Guiding and Establishing National Innovation for U.S. Stablecoins Act
GSC	Global Stablecoin
HKD	Hong Kong dollar
IDTI	Insured deposit-taking institution
IMF	International Monetary Fund
IaaS	Infrastructure as a service
IADI	International Association of Deposit Insurers
IOSCO	International Organization of Securities Commissions
MICA	EU Regulation on Markets in Crypto Assets
NBFI	Non-bank financial intermediary
PaaS	Platform as a service
PSD2	Revised Payment Services Directive (European Union)
SaaS	Software as a service
USDT	Tether (cryptocurrency)
USDC	USD Coin (cryptocurrency)

Executive summary

The International Association of Deposit Insurers (IADI) has identified the impact of financial innovation and digitalisation on deposit insurance systems as a key work priority.

Digitalisation and emerging technologies are fundamentally transforming both the financial sector and deposit insurance systems, creating new efficiencies as well as risks. The rapid evolution of digital technologies – including tokenisation, artificial intelligence (AI), cloud computing, and quantum computing – is reshaping the financial landscape and the operations of deposit insurers worldwide. These advancements present significant opportunities for improving efficiency but also introduce new risks and challenges for deposit insurance systems.

Growing demand for digital financial products including e-money, stablecoins, tokenised deposits, and central bank digital currencies (CBDCs) may challenge the conventional definition and role of deposits. These innovations blur the boundaries of conventional deposit-taking activities, raising questions about their treatment under deposit insurance frameworks. While e-money and stablecoins are primarily used for payments, their growing adoption in some markets raises concerns regarding user protection and financial stability. Similarly, while CBDCs have the potential to contribute to enhancing financial inclusion and payment efficiency, it is important to address the risk that they could exacerbate deposit outflows during times of crisis.

Technological innovation within insured deposit-taking institutions (IDTIs), along with the rise of new market entrants, is reshaping traditional banking models and may lead to increased deposit volatility. Neobanks, fintechs and BigTechs are at the forefront of financial innovation and may not be fully integrated in traditional regulatory frameworks for financial services. This creates challenges for oversight, user protection, and financial stability. At the same time, technological advancements are changing depositor behaviour, with digital-savvy consumers increasingly demanding instant access to funds and diversifying their assets beyond traditional deposits. This behavioural shift has the potential to reduce deposit stickiness and heighten deposit volatility, particularly during periods of financial stress.

Technological advancements such as automation, social media, cloud computing, AI, and quantum computing bring opportunities for deposit insurers, but also introduce risks that must be managed. Digital data access and automation can enhance efficiency in premium assessments, risk monitoring, and payout processes, but require robust safeguards against operational and cybersecurity risks. Social media can serve as both an early warning tool for financial distress and a channel for public awareness. It also presents risks of misinformation and accelerated deposit withdrawals. Cloud computing offers scalability and cost efficiency but introduces vulnerabilities such as operational risks, vendor concentration, and cybersecurity threats. AI can transform risk assessment, fraud detection, and resolution planning. Quantum computing offers opportunities for advanced analytics but poses a significant threat to encryption and data security.

Deposit insurers need to adapt their frameworks, build technological capacity, and enhance public awareness in order to protect depositors and safeguard financial stability in an increasingly digital environment. This includes clarifying the coverage of new digital products, investing in operational capacity and technological expertise, and enhancing public awareness to prevent confusion about the scope of protection. Collaboration with other financial safety-net participants and regulators is essential for managing cross-border activities and harmonising standards.

The revised IADI Core Principles of Effective Deposit Insurance Systems emphasise the importance of robust business continuity management and operational resilience to withstand technological disruptions. Deposit insurers are urged to integrate digitalisation-related risks into their strategic planning, ensure compliance with evolving regulations, and prepare for emerging threats such as quantum-enabled cyber-attacks.

Ongoing research and dialogue are essential for equipping deposit insurers to respond effectively to innovation and to uphold both depositor protection and financial stability in the years ahead. This report marks the start of a continuing process to examine how digitalisation and financial innovation are reshaping deposit insurance systems. Each chapter of this report presents open questions for further analysis. These questions aim to provide a foundation for deposit insurers to adapt to these developments while continuing to protect depositors and support financial stability.

Feedback on these questions is welcome and can be shared with IADI at consultation@iadi.org by 16 March 2026.

Introduction

The International Association of Deposit Insurers (IADI) identified the analysis of the impact of financial innovation and digitalisation on deposit insurance systems as a critical work priority. The rapid evolution of digital technologies is transforming the financial landscape, creating both new opportunities and risks for depositors, deposit-taking institutions, and deposit insurance systems. In recognition of these profound changes, IADI organised a series of webinars throughout the year, engaging public and private sector experts, as well as academics, to explore these developments and their impacts on deposit insurance systems.

Digitalisation, alongside specific technologies such as tokenisation, AI, and cloud computing, is enabling deposit-taking institutions, fintech firms, and central banks to streamline operations, enhance user experiences, and expand financial inclusion. These advancements have led to an increasing number of alternatives for payments and value storage that may serve the same purposes as traditional deposits. However, these innovations also pose challenges, including potential impacts on the financial stability and risk profiles of deposit-taking institutions, and the introduction of novel risks that deposit insurers must address.

The emergence of digital deposit-taking institutions and fintech platforms accepting funds from the public further blurs the boundaries of traditional deposit-taking activities, raising critical questions about coverage under existing deposit insurance frameworks. Moreover, the rapid pace of innovation often outstrips regulatory adaptation, potentially undermining consumer protection and financial stability. For deposit insurers, this calls for a thorough review of their mandates to assess what can be achieved within their current scope. It also necessitates evolving risk assessment practices and, where required, considering an expansion of their mandates to effectively address the challenges and implications posed by digital finance on their systems.

This report examines these issues through three interconnected lenses:

- first, it explores the products emerging from innovation that relate to deposits, including digital alternatives such as tokenised deposits, stablecoins, and e-money
- second, it investigates the nature of the actors supplying these services, including digital deposit-taking institutions, fintech platforms, and other intermediaries, and of depositors and others that make up the demand side
- finally, it considers the technology, such as AI, cloud computing, and quantum computing, that underpin these changes.

While these topics are addressed in separate chapters, they are deeply interrelated and should not be viewed in isolation. The findings presented in this report are not conclusive but serve as a starting point for ongoing analysis. They are intended to lay the foundation for further exploration and dialogue, helping deposit insurers adapt to the rapidly evolving financial landscape. To support this objective, the report includes open questions regarding the challenges and opportunities that digitalisation and financial innovation present for deposit insurance systems.

Input for this report was drawn from a series of webinars under the Digitalisation Webinar Series, as well as written contributions from external experts who shared their invaluable insights and perspectives, helping to identify key issues and deepen understanding of the subject matter. These contributors included Art Wilmarth (George Washington University), Tony McLaughlin (Ubyx), Diane Ellis (IntraFi), Carlos Eduardo de Almeida (Central Bank of Brazil), Iñaki Aldasoro (BIS Monetary and Economic Department), Ajit Desai and Priscilla Koo Wilkens (BIS Innovation Hub), Luca Conti and Danny Chau (Hong Kong Monetary Authority), Ralph Croissant and Hubert d'Étigny (BNP Paribas), Linda Jeng (DigitalSelfLabs), Miriam Eggen (University of Berne), and Yueh-Ping Yang (National Taiwan University, Chinese Taipei. The report also benefited from contributions by IADI members, the IADI Fintech Technical Committee, representatives from the Institute of International Finance (IIF), and comments from IMF staff. However, none of the statements in this report should be attributed to these contributors or experts.

1. The Product: Deposits and their Digital Alternatives

This section covers e-money, stablecoins, tokenised deposits, and central bank digital currencies (CBDCs) as key financial products emerging from digital innovation. It assesses their economic significance, examines trends, and defines relevant concepts. While many of these products currently align more closely with the payment function of deposits than their value storage role, this dynamic may evolve over time. Additionally, many of these products do not legally qualify as deposits, which typically require a deposit-taking licence under applicable legislation.

1.1. E-Money

1.1.1. What is e-money?

The concept of e-money, or electronic money, lacks a uniform global definition. Some jurisdictions define e-money as a legal concept which refers to a digital representation of fiat currency used for payments, while in other jurisdictions, absent a legal definition, it may encompass a broader range of digital financial instruments.[1]

E-money is a digital representation of monetary value. E-money generally shares common technical characteristics. It is typically stored electronically (eg on cards, mobile devices, or online platforms), denominated in fiat currency, representing a claim redeemable at par against the e-money issuer, and multipurpose, meaning it is accepted as means of payment by entities other than the e-money issuer.

1.1.2. Economic relevance

E-money's economic relevance differs across jurisdictions. In advanced economies, e-money is primarily a supplementary payment tool, enhancing the efficiency and convenience of established financial systems. It is often used alongside traditional banking services for digital payments. In contrast, in many emerging economies, e-money plays a more critical role as an alternative to deposits. It enables essential financial services to unbanked or underbanked populations, enabling access to payments, savings, and other financial activities in regions where formal banking infrastructure may be limited.

The share of e-money transactions in GDP remains low in advanced economies whereas emerging economies report higher shares. Over the past decade, the value of e-money transactions as a share of GDP has grown steadily but remains low in advanced economies, typically below 1%. In contrast, emerging economies report much higher shares, such as Ghana (over twice GDP) and Kenya (about 50% of GDP).[2]

E-money adoption is significant in underbanked economies. In jurisdictions with limited access to banking services, e-money serves as a cost-effective solution, enhancing financial

[1] See IADI (2026) referring to "mobile money" in Ghana, "small-balance deposits" issued by specialised companies (SEDPES) in Colombia, or "prepaid payment instruments" in Japan.
[2] IADI (2026).

inclusion and providing unbanked populations with access to payment services. Its widespread use in these economies can reach levels that impact financial stability.

1.1.3. Risks and regulation

E-money issuers can fail. The potential failure of an E-money issuer or its inability to allow the redemption of e-money funds can stem from:

- liquidity risks, which arise if the e-money issuer has invested the float in insufficiently liquid assets
- counterparty credit risks, which occur if the e-money issuer incurs losses due to the default of issuers of assets in which the float is invested which includes scenarios where an insured deposit-taking institution (IDTI), holding the float, fails
- market risk which may materialise when e-money issuers suffer losses from changes in market prices, such as fluctuations in interest rates or security prices, during asset liquidation; and
- operational risks, including business continuity risks, cyber risks, fraud, and the mishandling of user records.

Jurisdictions employ converging approaches to address risks associated with e-money issuers. Across jurisdictions, regulatory approaches to e-money issuers commonly include licensing and capital requirements, often calculated as a percentage of the e-money float. To ensure the protection of user funds, regulations typically mandate 100% backing of e-money with segregated, liquid assets such as deposits, high-quality securities, or trusts. Some jurisdictions require the e-money float to be placed at the central bank. Users must be able to redeem e-money at par value, and e-money issuers are generally prohibited from offering interest payments or engaging in lending activities, thereby reducing risk exposure. Anti-money laundering and counter-terrorism financing measures form a universal regulatory requirement, including customer due diligence, transaction monitoring, and the reporting of suspicious activities. Some jurisdictions apply a holding or transaction cap to e-money to mitigate these risks.[3]

1.1.4. Relevance for deposit insurers

Deposit insurance coverage for e-money is a potential policy option to protect e-money users. Despite the implementation of prudential requirements and supervisory measures, the possibility of e-money issuer failures remains, potentially leading to financial losses for users. Additional protection through deposit insurance could provide an extra layer of security to e-money users. However, deposit insurance frameworks for e-money vary in scope and levels of protection they offer.

The default deposit insurance framework for e-money provides limited protection to individual users, focusing primarily on the default risk of the deposit-taking institution (IDTI) holding the e-money issuer's segregated float. Under this framework, the deposit insurer classifies the e-money issuer's float account at the failing IDTI as a single depositor, applying

[3] See IADI (2026) for a more details and references of how prudential regulation and supervision act as first lines of defence in protecting users of e-money.

the coverage limit to this aggregated account. As a result, this approach offers minimal direct safeguards for individual e-money users. It does not address the broader risks posed by the potential failure of the e-money issuer itself, particularly in scenarios where the collapse of the IDTI triggers cascading disruptions.

The pass-through approach enhances protection for e-money users but presents operational challenges. Under this approach, the deposit insurer protects individual e-money users as the ultimate beneficiaries of the e-money issuer's float, up to the coverage limit, in the event of an IDTI's failure. This offers greater protection compared to the default approach but requires the e-money issuer to maintain accurate and detailed records on the identity, eligibility, and balances of e-money users. Additionally, this approach supports the continuity of the e-money issuer's services by facilitating direct reimbursement to the e-money issuer or enabling the transfer of the e-float to another IDTI. However, the technical and administrative demands on deposit insurers are significant.

The direct approach ensures e-money users' claims against failure of the e-money issuer. In this approach, e-money issuers must be members of the deposit insurance system, and users' claims are insured up to the coverage limit regardless of the cause of the e-money issuer's failure. This mechanism requires robust prudential regulation and supervision of the e-money issuer, as well as appropriate pricing of associated risks. The direct approach offers more straightforward and transparent protection to e-money users.

The combined approach combines the direct approach with either the default or pass-through approach and offers additional protection to e-money users. This combination covers both the failure of the IDTI holding the e-money float, and the failure of the e-money issuer itself. It offers some advantage as to the speed of intervention but also comes with financial risks and technical challenges for the deposit insurer.

Financial stability benefits of extending deposit insurance directly to e-money are limited. Credit risks associated with e-money are less significant than those in the conventional deposit-taking businesses, as prudential regulations typically prohibit e-money issuers from engaging in credit intermediation. Moreover, the risks of e-money runs and the financial losses they might impose on users are generally much smaller compared to those triggered by runs on insured deposit taking institutions, reducing the necessity for deposit insurance from a financial stability perspective.

Deposit insurance for e-money can enhance confidence and promote financial inclusion in cases where a significant portion of the population relies on e-money as their primary payment and value storage tool. In highly concentrated e-money markets where the failure of a single provider could have widespread consequences, deposit insurance could provide a valuable mechanism to safeguard public trust and financial inclusion.

1.1.5. Further questions

1. **Are deposit insurers equipped with the necessary powers and tools to protect e-money, where deemed appropriate?**

The different coverage models, including pass-through (indirect) and direct coverage, give rise to operational challenges and legal challenges. The deposit insurer needs to have access to beneficiary information, either indirectly through IDTIs or directly from e-money issuers, and in a form that enables the deposit insurer to meet any reimbursement obligations expeditiously.[4]

2. **What are the potential risks to financial stability and for depositors posed by fragmented regulatory approaches to instruments that are economically and functionally similar? How could these risks be addressed?**

Users may perceive e-money as economically and functionally similar to other products such as tokenised e-money or stablecoins, which may however be subject to different regulatory regimes. Protection by deposit insurance of e-money, but not of other products deemed similar, may cause confusion and rapid reallocations of funds in crisis times, if users suddenly are made aware of differential treatments.

1.2. Stablecoins

1.2.1. What are stablecoins?

There is no universally agreed legal or regulatory definition of stablecoins. Stablecoins are commonly understood to refer to digital assets that aim to maintain a stable value relative to a reference asset or a pool thereof.[5] Stablecoins make use of cryptography and distributed ledger or similar technology to store balances, validate transactions, and prevent tampering.[6] They offer potential for wider adoption as a means of payment and/or store of value, including for cross-border use. The Financial Stability Board (FSB) defines "global stablecoins" (GSCs) as those with potential for significant scale and cross-jurisdictional reach, which could become systemically important in one or more jurisdictions.

The mechanisms that stablecoins apply to stabilise their value differ. Stablecoins can be categorised into four types based on their mechanisms for maintaining stability: [7]

- Fiat-backed stablecoins, which are collateralised by traditional financial assets (eg cash, deposits, and government bonds) and are typically pegged to a fiat currency (eg USD or EUR) or to a basket of fiat currencies

[4] IADI (2014), Core Principle 2, Essential Criteria 3.

[5] BIS (2025b) characterises stablecoins as "designed as a gateway to the crypto ecosystem, promising stable value relative to fiat currencies while operating on public blockchains". Adrian et al (2025) more narrowly characterises stablecoins as "a form of digital asset backed by currencies or government bonds".

[6] See FSB (2023).

[7] For taxonomy, see for instance, ECB (2020), BIS (2024a), Crisanto et al (2024) and US Department of Treasury (2025).

- Crypto-backed stablecoins, which are collateralised by other cryptocurrencies and pegged to a fiat currency or another asset. To account for the volatility of these backing assets and mitigate the risk of insufficient backing, they are often over-collateralised
- Commodity-backed stablecoins are backed by assets like gold or silver and pegged to their value
- Algorithmic stablecoins rely on supply adjustment mechanisms without direct asset backing and can be pegged to a variety of assets, including fiat currency.

Fiat-backed stablecoins are the dominant category in the stablecoin ecosystem, driven by their reliance on traditional financial assets and their direct pegging to fiat currencies. This trend reflects their perceived stability and trustworthiness, which make them more suitable for integration into the broader financial system. Many issuers are actively focusing on fiat-backed models to attract users and meet regulatory expectations, as these stablecoins align more closely with existing financial infrastructure and regulatory frameworks.

Stablecoins are not deposits. Unlike deposits, which represent enforceable claims against licensed financial institutions and are protected if eligible by deposit insurance, stablecoins are digital assets issued on blockchains. Many stablecoins provide holders with a legal or contractual right to redeem tokens at par value (1:1) in fiat currency or the underlying asset. However, these rights may be subject to the issuer's terms and conditions, which may vary in strength and enforceability. The strength of this redemption right depends not only on the legal structure, but also the quality and liquidity of reserve assets, and the regulatory framework.

Stablecoins are bearer instruments. Stablecoins are typically structured as bearer instruments, meaning ownership is determined by control of the private keys associated with a digital wallet. Transfers occur peer-to-peer on the blockchain, without requiring updates to the issuer's records. Ownership is recorded based on blockchain-based wallets and transferring stablecoins between users does not impact the issuer.[8]

In many jurisdictions, stablecoin issuers are prohibited from paying interest, positioning them primarily as payment instruments rather than investment vehicles. However, if such prohibition addresses stablecoin issuers only, fee bonus to facilitate payments on stablecoin holdings or interest-like rewards on lending may still take place.[9] Fiat-backed stablecoins may show some similarity with money market funds, as they are backed with low-risk and highly liquid assets and attempt to maintain a fixed net asset value but may experience valuation discrepancies under market stress, potentially leading to de-pegging.

1.2.2. Economic relevance

The market for stablecoins is dominated by fiat-backed stablecoins. It continues to grow and shows a high degree of concentration both as regards issuers and fiat currency it is pegged to. The total market capitalisation reached USD 300 billion by September 2025, representing

[8] See BIS (2025b), pp 79 and 85.

[9] See Garcia Ocampo (2025). The EU MICA regulation precludes both stablecoin issuers and cryptocurrency exchanges to pay interest. In the US GENIUS Act, this applies to stablecoin issuers only. The brief discusses the competitive pressure on conventional financial products including deposits.

around 7.5% of total crypto-asset market capitalisation.[10] Transaction volume in stablecoins also shows strong growth and rose from USD 87.22 billion in December 2020 to USD 1.03 trillion in September 2025. About 200 million stablecoin transactions are taking place monthly.[11] Two fiat-backed stablecoin issuers, USDT and USDC, both backed by USD, account for more than 82% of the market.[12] About 70% of stablecoins and 99% of total capitalisation are denominated in USD.[13]

Currently, stablecoins are primarily used in transactions and for storage of value relating to crypto assets, but they may also offer benefits in terms of lowering costs of cross-border transactions, programmability and easy access to foreign currency. Stablecoin use for retail and wholesale payments remains low.[14, 15] Stablecoins are primarily used as an on-chain proxy to transact and withhold value for crypto-assets. At the same time, stablecoin demand may be motivated by its use as a digital, cross-border medium of exchange (potentially outside current regulatory perimeter) or as a means to access assets, particularly in contexts where economic conditions are less stable.[16] Their capabilities to incorporate smart contracts could enable stablecoins to serve as interoperable collateral for tokenised trading, lending, settlement activities on a broader scale in the future.[17]

Stablecoin issuers can be both insured deposit-taking institutions (IDTIs) and other institutions subject to varying degrees of oversight depending on jurisdiction. IDTIs are regulated and licensed financial institutions, such as banks, that are subject to sound prudential regulation and supervision and an effective resolution regime. In some jurisdiction IDTIs can issue stablecoins directly, such as in the EU, Hong Kong SAR, Singapore and Japan, whereas in others, such as in the US under the US Genius Act of 2025, banks may issue stablecoins through a subsidiary that is approved as permitted payment stablecoin issuer. A number of IDTIs across various regions are issuing or have announced plans to issue stablecoins, either independently, as part of a consortium, or through subsidiaries.[18] Non-bank stablecoin issuers, on the other

[10] Coinmarketcap (2025).

[11] After addresses associated with high-frequency trading and botting activities are excluded. These transactions are about four fifth of all transactions in both volume and count.

[12] According to Coinmarketcap, tracking 254 stablecoins including non-fiat varieties.

[13] See Aldasoro et al (2025).

[14] Visa Onchain Analytics Dashboard reports that about 60% of stablecoin transactions are identified to be retail-sised below USD 250, collectively amounting to about USD 6 billion or 0.6% of all transaction volume. According to the 93 central banks surveyed by the BIS in 2024, only about 10% of respondents indicated that stablecoins are used beyond particular user groups or beyond small share of wholesale payments. See Illes et al (2025).

[15] According to the 93 central banks surveyed by the BIS in 2024, only about 10% of respondents indicated that stablecoins are used by more than particular user groups or beyond small share of wholesale payments. See Illes et al (2025).

1.1. [16] For a description of recent regional trends, see Chainalysis (2025). Initial estimates of cross-border stablecoin flows are provided by Reuter (2025). An analysis of underlying drivers is provided by Auer, R., U. Lewrick and J. Paulick (2025).

[17] US Department of Treasury (2025).

[18] Eg in the US, JP Morgan Chase issues a stablecoin (JPM Coin) for institutional payments and settlements. In Europe, Societe Generale issued EURCV which is likewise a stablecoin for institutional settlements. Banking Circle, issues EURI, a stablecoin used for cross-border transactions. In September 2025, a consortium of major European banks (Qivalis) announced the launch of a Euro Stablecoin.

hand, include specialised corporations, trust companies, or payment service providers.[19] These issuers range from specialised corporations (eg Tether), centralised cryptocurrency exchanges (Binance) and licensed non-bank financial intermediaries (NBFIs) such as trust companies (Paxos) and payment service providers (eg Circle, Paypal, Stripe). Some major corporations both from within and outside the tech-sphere (eg Meta, SAP, Amazon, Walmart) are actively pursuing initiatives to enter this fast-evolving space. Their efforts are often motivated by the potential to reduce payment costs and broaden their influence within the financial sector.

Most stablecoins today are issued from a single jurisdiction, but multijurisdictional stablecoins – of which the affiliated issuers operate across multiple countries – are becoming increasingly relevant as issuers expand globally. These arrangements feature fungible tokens, distributed reserves, and redemption mechanisms spanning several jurisdictions, and are expected to become more common as stablecoin adoption grows.

1.2.3. Risks and regulation

Stablecoins can pose significant risks to financial stability by affecting traditional banking systems, government securities markets, and monetary policy. Outflows from deposits into stablecoins or rapid changes in stablecoin asset prices can destabilise IDTIs and shift liquidity away from some traditional financial institutions. The growing presence of stablecoins may also impact the structure of short-term government securities markets.[20] As demand for fiat-backed stablecoins increases, so does the demand for high-quality reserve assets, including on a cross-border basis. In some economies, especially where foreign currency denominated stablecoins are used as substitutes for domestic currency, this can lead to capital flight and reduced effectiveness of domestic monetary policy. These risks are particularly acute in countries with less stable economic conditions, where widespread stablecoin adoption may transmit economic and financial shocks and constrain the ability of authorities to respond effectively in a crisis.

The potential for stablecoins to achieve large-scale cross-border adoption introduces significant challenges. Global stablecoins (GSCs) could disrupt existing payment systems, weaken the transmission of monetary policy, and amplify destabilising cross-border capital flows. Furthermore, inconsistent legal definitions and fragmented regulatory approaches increase the risk of regulatory arbitrage, enabling issuers to exploit jurisdictional gaps and undermining effective supervision. As stablecoins become more embedded within the financial system, risks such as operational failures, cyber incidents, or issues with redemption could have wide-ranging consequences. Ultimately, the failure or loss of confidence in a widely adopted stablecoin could trigger systemic disruptions, affecting payment systems, financial institutions, and users on a global scale.

Multijurisdictional stablecoins, which are issued and managed across multiple countries, pose a complex set of potential risks for financial stability and regulatory oversight. A key

[19] For example, in the EU, the MICA regulation allows for the issuance of e-money tokens (EMTs) by IDTIs and licenced e-money issuers (E-money Institutions 'EMI') only. EMTs are essentially stablecoins pegged to a single fiat currency.

[20] On the role of stablecoins in treasury markets, see Ahmed and Aldasoro (2025) and Adrian et al (2025) pp 24.

concern is regulatory arbitrage, where issuers exploit differences in national rules – such as reserve requirements or redemption obligations – by operating in jurisdictions with weaker oversight. This practice can undermine the effectiveness of supervision and leave gaps in user protection. The management of reserves and redemption mechanisms across several jurisdictions also introduces liquidity and redemption risks. In times of stress, users may seek to redeem their stablecoins from the jurisdiction offering the most favourable or fastest terms, which can trigger destabilising runs and strain the system's liquidity. Supervisory and enforcement challenges are compounded by the cross-border structure, making it difficult for any single authority to monitor the full scope of the stablecoin's activities, coordinate enforcement, or respond swiftly to emerging risks. As a result, stablecoin users may be facing varying or unclear rights depending on the jurisdiction in which they interact with the stablecoin. Limited transparency and inconsistent reporting on global operations and reserves can further obscure risk exposures and delay timely intervention.[21]

Even with prudential regulation and supervision in place, the issuers of stablecoins may fail or stablecoins may not be redeemable at par. Stablecoins are exposed to credit, market, and liquidity risks relating to reserve assets, in addition to operational risks specific to underlying technologies and business models. Regulatory requirement on backing stablecoins with high quality liquid assets can mitigate but not eliminate these risks. Stablecoins are therefore subject to run risks, similar to deposits and money market mutual fund shares. Such run risks, under stress scenarios, will be exacerbated by the lack of legal certainty for at par redemption, unsecured creditor status, and absence of policy backstops for stablecoins.

International standard-setters have set out high-level guidance for managing stablecoin-related risks. In 2023, the FSB issued recommendations for the regulation, supervision and oversight of GSC arrangements.[22] The Basel Committee on Banking Supervision (BCBS) developed policies on the prudential treatments of bank exposures to crypto-assets, including stablecoins, in terms of classifications, accounting rules, capital and liquidity requirements, exposure limits, risk management, and supervisory review processes. CPMI and IOSCO issued guidance on applying the Principles for Financial Market Infrastructure in the stablecoin context, in particular with respect to governance, risk management, and settlements.[23] FATF addressed the application of its standards to counter illicit stablecoin-based financing in an G20 Report.[24]

Although a number of jurisdictions have established prudential regulation and supervision frameworks for the issuance of stablecoins, significant gaps and inconsistencies in implementing a global framework remain. Jurisdictions that established stablecoin regulation include the Bahamas, Bermuda, EU, Hong Kong SAR, Japan and the US.[25] Regulations focus on the nature of institutions (mostly both IDTIs and non-IDTIs) that may issue stablecoins and on

[21] On the financial stability risks of stablecoins issued by issuers in multiple jurisdictions, see European Systemic Risk Board (2025).
[22] See FSB (2023).
[23] BIS (2021a).
[24] FATF (2020).
[25] FSB (2025) Table 1.

the requirements for backing stablecoins with assets. They also include rules on redemption rights and whether interest payments are allowed. A 2025 FSB Peer Review points to critical gaps in existing frameworks including insufficient requirements for risk management framework, recovery and resolution planning practices, and capital buffers. Difference across jurisdictions as regards disclosures, reserve collateralisation requirements and custody and redemption rules pose regulatory and supervisory challenges for stablecoin issuers that offer services in multiple jurisdictions.[26] The report highlights the need for strong international cooperation, harmonised regulatory standards, and robust information sharing, notably to mitigate the risks associated with multijurisdictional stablecoin arrangements.

1.2.4. Relevance for deposit insurers

Even when not covered by deposit insurance, stablecoins may affect deposit insurers. Stablecoins are generally not deposits and hence deposit insurance does not extend to stablecoins. As such, the failure of a stablecoin issuer is not a risk that is insured by the deposit insurer. Instead, user protection needs to be addressed through targeted regulation, robust reserve management, and clear legal frameworks specific to stablecoin arrangements. However, distinct from insuring stablecoin issuers, the client funds that back stablecoins may be deposits covered by deposit insurance. In consequence, the failure of the IDTI holding such deposits may trigger action by the deposit insurer that relates to users of stablecoins. The scope of any such action depends on the presence and nature of the coverage of such client funds.

As stablecoins gain popularity, public awareness of the scope of deposit insurance coverage has become increasingly important. Stablecoins may be perceived by users as e-money or deposit-like instruments, despite fundamental regulatory differences. A clear understanding of applicable coverage is essential to mitigate the risk that runs on stablecoins could lead to broader runs on deposits, thereby threatening financial stability.

1.2.5. Further questions

3. **Are stablecoin users adequately protected in the event of failure of the stablecoin issuer?**

If stablecoins become widely used as alternatives to traditional deposits, there is a real risk that, in the event of a failure of the issuer or of the IDTI holding parts of the assets backing the stablecoin, users may not be able to quickly access their funds. This can create a situation where the public expects protections similar to those provided by deposit insurance, even though stablecoins are fundamentally different from deposits. While regulations that require stablecoins to be fully backed by reserve assets – and that enforce segregation and ring-fencing of customer funds from issuer balance sheets – are intended to safeguard users, these measures may not be sufficient to prevent loss of confidence or runs if users begin to doubt the adequacy or accessibility of the reserves. In such scenarios, the absence of deposit insurance could lead to confusion and undermine trust, especially if stablecoin users perceive

[26] FSB (2025). See also IOSCO (2025).

themselves as being in a position similar to insured depositors. Therefore, it is crucial that robust and transparent safeguards are in place for stablecoin users and that public expectations are managed.

4. **What deposit insurance coverage applies to stablecoin reserve assets held as deposits in IDTIs?**

Regulatory frameworks may allow or require stablecoin issuers to hold reserve assets as deposits in IDTIs.[27] If the IDTI fails, deposit insurance would typically cover the issuer's account only up to the standard coverage limit, which is often much less than the total value of reserves. As a result, stablecoin users could face losses. Alternatives like pass-through or direct coverage for individual users are technically challenging – especially since stablecoins are bearer instruments and holders are hard to identify – and raise broader questions about the appropriate role of deposit insurance for these arrangements.

5. **What is the impact of stablecoin growth on deposit-taking? Could stablecoins reduce overall deposits through direct substitution?**

Stablecoin growth may reduce overall deposits by serving as a direct substitute for traditional deposits. At the same time, stablecoin issuers' need to hold reserves could increase deposits at select IDTIs, particularly those acting as custodians. This shift may influence funding costs, interest rates, and credit intermediation, with the effects varying across jurisdictions. In markets with significant adoption of foreign currency stablecoins, deposit outflows from IDTIs could be more pronounced. Increased deposit volatility may require enhanced monitoring, closer cooperation, and better information-sharing among financial safety-net participants. Banks issuing stablecoins may also face distinct risk profiles, including greater contagion risks for their traditional activities.

6. **What does the rising demand for stablecoins mean for public awareness of deposit insurance?**

The increasing popularity of stablecoins could challenge deposit insurers in meeting public policy objectives. To protect depositors and ensure financial stability, clear and effective communication about the scope of protection is essential. This is particularly important as stablecoins may be perceived as e-money or deposit-like instruments by the general public, despite fundamental regulatory differences. Misunderstandings about what is covered could heighten risks, potentially triggering runs on stablecoins that spill over into traditional deposit runs. IADI Core Principle 10 clearly states that the law must prohibit misleading or deceptive statements regarding who is a member institution of the deposit insurer and what constitutes an insured deposit. This means that non-insured deposit-taking institutions (non-IDTIs)—such

[27] See for example the EU MICA framework that requires issuers of asset-referenced tokens and e-money-tokens to hold a share of their reserve of assets as deposits with IDTI. See EBA (2024a) for more details.

as electronic money institutions, stablecoin issuers, or crypto-asset exchanges—must not use terminology that implies they are IDTIs or that their products are insured deposits.

1.3. Tokenisation and Deposits

1.3.1. What is tokenisation?

Tokenisation allows for financial assets to be represented digitally on programmable platforms. Tokenisation refers to the process of digitally representing financial assets, claims, or obligations on platforms that typically use distributed ledger technology (DLT), such as blockchains.[28] This involves generating a digital token that embodies rights to an underlying asset (eg securities, commodities, real estate, or deposits) or obligations to honour claims. In the future, on unified ledgers[29] that combine tokenised central bank money, tokenised commercial bank money and tokenised claims on (financial) assets, such transactions may be executed via smart contracts, offering potential for atomic settlement, where messaging, reconciliation, asset transfer, and cash settlement are integrated into a single seamless operation. This offers potential for efficiency gains through lower complexity, reconciliation costs, and risks.[30]

Deposits in tokenised form are digital representations of IDTI liabilities, but they may come in different designs, which are subject to change given rapid innovation and the evolving regulatory landscape. Current initiatives indicate that there are two main options for their digital representation. Digital currencies can be account-based, where ownership and transactions are verified through user identity and account balances, or token-based, where ownership is determined by possession of cryptographic tokens.[31]

- As a non-bearer instrument, "tokenised deposits" are account-based instruments and tied to specific deposit accounts at the issuing IDTI. Transactions trigger updates to the underlying accounts. Settlement occurs over a common asset such as tokenised central bank money. This model mirrors conventional banking practices.
- As a bearer instrument, "deposit tokens" are token-based instruments and function as transferable claims against the issuing IDTI, circulating freely on blockchains. Transfer do not require updates to the issuer's records. This allows for peer-to-peer settlements and flexibility for use in decentralised finance (DeFi) or programmable payment systems.

The design choice impacts not only the applicable settlement mechanism but also the operation of the deposit insurance system. Account-based instruments typically rely on intermediaries (eg IDTIs or central authorities) for settlement and can conceptually integrate with existing deposit insurance systems. On the other hand, token-based instruments enable direct peer-to-peer settlement without intermediaries, and bearer instrument tokens may not necessarily be settled against central bank money, potentially undermining their credibility. Additionally, in the absence of proper settlement mechanisms, deposit tokens may fail to

[28] BIS (2024b), FSB (2024d)
[29] BIS (2025b) sets out in detail the concept of the unified ledger.
[30] See for example the BIS Innovation Hub's Projects Agora, Meridian FX and Rialto.
[31] Garrett and Shin (2023).

uphold the principle of "singleness of money"[32] and could trade at varying prices, raising concerns about whether these claims can always be settled at par.[33] Token-based instruments also present significant challenges to traditional deposit insurance reimbursement mechanisms as ownership in these instruments is tied to the possession of digital tokens rather than accounts held with intermediaries like IDTIs.

1.3.2. Economic relevance

Tokenisation offers potential for innovation within the regulated banking sector. Potential benefits of tokenised deposits include programmability, atomic settlement, and cost-effectiveness through the integration of blockchain into traditional financial systems. As digital representations of IDTI liabilities, they may enhance existing payment systems. Tokenised deposits may add particular value for corporate users, particularly in scenarios involving large-value and low-number cross-border payments settings. In such cases, the ability to enable simultaneous payment settlements and asset transfers helps to minimise counterparty risk.[34]

Deposit tokenisation presents challenges but also offers opportunities for integration within the two-tiered monetary and financial system revolving around the central bank and deposit-taking institutions. Unlike stablecoins, tokenised deposits are fully integrated into the traditional credit intermediation process. This integration allows them to generate interest through lending activities undertaken by institutions operating under the fractional reserve banking model. As a result, tokenised deposits are more closely aligned with conventional banking operations, offering a seamless extension of existing financial frameworks. These tokenised deposits are issued by IDTIs, and central banks could facilitate their settlement in central bank money, for instance, by leveraging a wholesale CBDC. Some IDTIs have initiated pilot projects for deposit tokenisation, primarily focusing on wholesale deposits to assess scalability with institutional clients.

Interoperability remains a key barrier to the widespread adoption of tokenised deposits. Currently, banks operate their tokenised platforms independently, creating a "multiple-fragmented" model. To overcome this, two pathways to interoperability are being explored:

- making individual tokenised deposit platforms interoperable across institutions (multiple-interoperable model)

---

[32] A receiver of a bearer instrument assumes two counterparty risks. The first is the possibility that the issuer is unable to redeem the instrument at par, which can be resolved if the issuer has access to central bank settlement facilities, subject to prudential rules. The second is the possibility that the previous holder is under restriction due to financial integrity or other reasons. In a permissionless framework, the second risk element is unmitigated, whereas in a permissioned framework, there will need to be confidence by the receiver that the issuer's KYC perimeter is sufficient (ie including all previous holders of the token so that the claim represented is valid). This affects the singleness of money quality. See Garratt and Shin (2023).

[33] BIS (2025b).

[34] Blockchain-based ledgers face a trilemma between scalability (i.e., how many actors can propose transactions), decentralisation (how many actors can be authorised to process transactions), and security (how difficult to gain rights to process transactions) subject to computing power constraints. While a ledger may be public or private, depending on the access to view blockchain records, the permission to process records on the other hand relates to the decentralisation aspect as set out in the governance rules of a blockchain. In this sense, tokenised deposit usage for corporate business, intermediated solely by banks, prioritise the security aspect over scalability. See Bains (2025).

- developing a common programmable platform where banks issue and settle tokenised deposits (common-combined model).

To ensure the singleness of money at scale, tokenised deposits will require a tokenised risk-free settlement asset, such as tokenised central bank reserves. This can be achieved by linking DLT-based platforms with traditional real-time gross settlement (RTGS) systems or by issuing tokenised central bank reserves directly on the programmable platform.[35] In 2025, several institutions launched blockchain-based tokenisation initiatives aimed at enabling real-time cross-border payments, instant settlements, and transaction cost reductions. These initiatives encompass major currencies such as USD, EUR, GBP, HKD, and SGD.[36]

Cross-border standards for tokenised deposits are currently under exploration. BIS Project Agorá is a public-private collaborative initiative that examines the integration of tokenised deposits with tokenised central bank money on programmable platforms. The project aims to enhance the efficiency of correspondent banking processes and mitigate settlement risks. Additionally, Project Agorá is testing the programmability and atomic settlements across different form of tokenised money to enable seamless cross-border transactions. As their core, tokenised deposits remain deposits, preserving the essential characteristics of today's deposits.

1.3.3. Risks and regulation

The tokenisation of deposits introduces unique operational risks that extend beyond those associated with traditional deposits. A key challenge in distributed ledger systems is addressing the double-spend problem, which occurs when the same digital asset (eg a tokenised deposit) is simultaneously used in multiple transactions. This issue can arise because, without a centralised ledger, different processors may validate conflicting transactions in parallel within a block's processing time, leading to irrevocable forks on the blockchain. To mitigate this, distributed ledger systems need to rely on consensus and penalty mechanisms to mitigate inconsistencies, ensure the accuracy of records, and provide transaction finality. However, these mechanisms introduce further complexities and scalability issues.[37] Additionally, the integration of tokenised deposits into interoperable systems will require re-engineering infrastructures and operational processes. For instance, linking decentralised ledger environments with traditional real-time gross settlement (RTGS) systems is a critical step to ensure seamless integration between tokenised and non-tokenised assets. Such efforts are already being explored by central banks in the context of BIS Innovation Hub projects.

The programmability of tokenised deposits has the potential to influence behavioural patterns across interoperable financial systems. Smart contracts embedded within tokenised deposits enable transactions to be executed automatically when specific, predefined conditions are met. For instance, tokenised deposits could seamlessly move across interoperable systems to optimise economic benefits, such as earning higher interest rates, while still benefiting from

[35] See Maechler (2025).

[36] Several examples of tokenised deposit service include those by JPMorgan (JPM Coin), HSBC (Tokenised Deposit Service), Mastercard (Multi-Token Network), Japan Post Bank (in FY 2026), and Standard Chartered (as part of the UK Regulated Liability Network).

[37] See Bains (2025) for a detailed description of the challenges and constraints of consensus mechanisms.

deposit insurance coverage where applicable. Conversely, uninsured tokenised deposits may exhibit higher velocity due to the flexibility offered by smart contract functionalities, such as automated transfers or conditional payments. This increased velocity could alter the funding risk profile of IDTIs, potentially impacting their liquidity management and stability.

1.3.4. Relevance for deposit insurers

The prevailing policy approach tends to view tokenised deposits as digital equivalents of traditional deposits, provided they meet specific regulatory and operational conditions. This perspective assumes that tokenised deposits retain the core attributes of traditional deposits, such as being redeemable at par value, and operating within the existing regulatory framework for IDTIs. This approach aims to ensure that tokenised deposits maintain the same level of trust, stability, and protection as conventional deposits, while accommodating the technological innovations introduced by tokenisation. For instance:

- The European Banking Authority (EBA) regards account-based tokenised deposits as a traditional deposit eligible for deposit insurance under the existing legal framework. The EBA recognises that the tokenisation of a deposit does not by itself alter the fundamental nature of the claim by the depositor on the IDTI[38]
- The US GENIUS Act does not limit the ability of banking institutions to issue digital assets representing deposits or to utilise digital ledgers for books and records and to effect intrabank transfers[39]
- In Japan, the regulatory approach classifies digital money and tokenised deposits issued by IDTIs as deposits subject to prudential regulations and deposit insurance.

Deposit insurers may need to clarify whether tokenised deposits are recognised as eligible for deposit insurance coverage. The functional similarities between tokenised deposits issued by IDTIs and other digital instruments such as stablecoins, deposit tokens, or e-money tokens may create confusion among the public. This overlap underscores the importance of targeted public awareness efforts to clearly delineate the scope of deposit insurance coverage and ensure that users understand which instruments are protected under what conditions.

Without proper guardrails, the tokenisation of deposits may come with significant challenges. In times of financial distress, the rapid and automated migration of tokenised deposits enabled by smart contracts and programmable features could complicate early intervention and crisis management efforts, potentially accelerating liquidity outflows and destabilising institutions. Furthermore, resolution frameworks will need to address complex issues such freezing or suspending blockchain transactions, managing and processing smart contract-based collateral arrangements, and remapping tokenised deposit ledgers as part of transfer strategies. Additionally, deposit insurers may need to establish mechanisms to ensure the consistent and equitable treatment of both traditional and tokenised deposits, where protections apply to both forms.

[38] See EBA (2024). The treatment contrasts with that for electronic money tokens, which lies within the scope of Markets in Crypto-Assets Regulation (MiCA).
[39] 12 USC 5915(a) (2).

1.3.5. Further questions

7. **Are deposit insurance systems adequately prepared to address potential public confusion between tokenised deposits and other types of tokens?**

The functional similarities between tokenised deposits issued by IDTI and other digital instruments such as stablecoins, deposit tokens, or e-money tokens could lead to significant misunderstandings regarding the scope of deposit insurance coverage. Such confusion may result in misplaced trust or unwarranted concerns, ultimately impacting public confidence in the financial system. To mitigate these risks, deposit insurers and regulators must thoroughly assess whether existing regulatory frameworks, public awareness campaigns, and financial literacy initiatives effectively and clearly communicate the distinctions between these instruments. This includes ensuring that consumers understand which instruments are eligible for deposit insurance coverage, the conditions for such coverage, and the associated protections, as well as clarifying the risks and limitations of non-insured tokens.

8. **What infrastructure and expertise are required for deposit insurers to effectively monitor and manage tokenised deposits?**

Deposit insurers may encounter significant operational challenges in reassessing their contingent liabilities, both during normal conditions and in times of financial distress. The complexities introduced by tokenised deposits through the use of smart contracts and programmable features, demand specialised expertise and advanced technological capabilities. Deposit insurers may need to develop or acquire new toolkits to integrate and analyse on- and off-chain data according to legal finality rules and monitor tokenised deposit activities and associated risks. Furthermore, the involvement of crypto-asset service providers, such as wallet providers and blockchain infrastructure operators, introduces additional layers of operational and cybersecurity risks that deposit insurers must account for in their oversight and management processes.

To address these challenges, deposit insurers may need to build expertise in blockchain technology, distributed ledger systems, and smart contract operations, as well as establish robust frameworks to manage the risks associated with third-party dependencies. Insights from ongoing discussions about wallet insurance for stablecoins and CBDCs could provide valuable guidance in shaping policies and practices. Additionally, close collaboration with financial safety net participants, financial institutions, and technology providers will be essential to ensure that deposit insurers can adapt to the evolving landscape of tokenised deposits while maintaining the trust and stability of the financial system.

9. **Do programmable features in tokenised deposits increase the volatility of deposits, and what are the implications for the design of deposit insurance systems?**

Programmable features of tokenised deposits such as the ability to execute automated and instantaneous transfers between IDTIs may increase the velocity and "flightiness" of deposits. This heightened mobility poses challenges for deposit insurance systems, particularly in times of financial stress or crisis. The risk of pre-programmed "deposit runs", where smart contracts automatically trigger large-scale withdrawals or transfers in response to specific conditions, could exacerbate liquidity pressures on vulnerable institutions. Such dynamics could

undermine the ability of deposit insurers to stabilise the financial system and protect depositors. To address these risks, deposit insurance systems may need to consider adjustments to their design, such as enhanced monitoring mechanisms for tokenised deposit flows, real-time data integration capabilities, and operational stress test frameworks that account for the unique characteristics of programmable deposits.

10. **How would the failure of an IDTI with tokenised deposits impact resolution and reimbursement processes?**

The failure of an IDTI holding tokenised deposits would introduce significant complexities to resolution and reimbursement processes. Deposit insurers would need to establish mechanisms to reimburse tokenised deposits, particularly addressing challenges posed by programmable features. The involvement of third-party wallet providers or custodians adds further complications, as deposit insurers would need to ensure the accurate identification and verification of ownership, as well as to secure access to the wallets holding tokenised deposits. Furthermore, deposit insurers would need to assess whether existing legal and regulatory frameworks adequately recognise tokenised deposits as equivalent to traditional deposits in resolution scenarios. This includes ensuring that tokenised deposits are covered by deposit insurance, clarifying the treatment of programmable features during resolution, and addressing the equal treatment of tokenised and traditional deposits.

11. **How can regulators adapt to the evolving landscape of digital financial instruments and ensure appropriate oversight across jurisdictions?**

E-money's definitions and roles as well as applicable regulatory frameworks vary across jurisdictions. With the emergence of digital financial instruments such as stablecoins and tokenised deposits, overlaps with e-money are becoming increasingly apparent. These innovations blur the traditional lines between e-money and other digital financial assets, creating challenges for regulators in defining their scope and ensuring appropriate oversight. Further international work could help to promote convergence of regulatory approaches across instruments that serve the same economic function.

1.4. Central Bank Digital Currency

1.4.1. What is a CBDC?

A CBDC is a form of central bank liability offered in digital format and denominated in the national unit of account. A CBDC is a digital version of a jurisdiction's official currency and are issued and managed exclusively by the central bank. CBDCs are generally free of default risks, as they are fully backed by the central bank, and depending on their design, they can also incorporate programmability features. As a central bank liability, CBDCs can serve as a digital, programmable alternative for physical cash, offering the convenience of digital money. Additionally, they can act as alternative to conventional deposits, in the form of digital central bank money for depositors, and function in a manner akin to central bank reserves for IDTIs.

CBDCs can broadly be categorised into two main types: retail and wholesale. Retail CBDCs are accessible to the general public and are designed for everyday transactions by individuals and businesses. They serve as a default risk-free, digital alternative to physical cash. Wholesale

CBDCs, on the other hand, are restricted to financial institutions and are intended for large-scale transactions between financial intermediaries. For decades IDTIs have had the ability to settle wholesale transactions in central bank money via real-time gross settlement systems. Wholesale CBDCs may leverage distributed ledger technology, enabling a decentralised approach to transaction settlement for other instruments.[40]

Central banks are exploring the introduction of both retail and wholesale CBDCs to achieve distinct policy goals. For retail CBDCs, commonly cited objectives include maintaining the role of central bank money, promoting financial inclusion, enhancing payment efficiency, safeguarding monetary policy transmission, strengthening monetary sovereignty, and addressing risks of currency substitution. Wholesale CBDCs, on the other hand, are primarily motivated by the aim to improve cross-border payment systems.[41]

Retail CBDCs address domestic financial and payment challenges. In jurisdictions with declining cash usage, retail CBDCs can sustain demand for fiat money while providing unbanked populations with access to payment systems. Additionally, they can contribute to the development of efficient domestic payment systems and strengthen monetary sovereignty by preserving the central bank's control over monetary policy and mitigating risks of substitution by alternative currencies, whether public or private. [42]

Wholesale CBDCs focus on enhancing cross-border payment efficiency. Wholesale CBDCs can contribute to real-time settlements, uninterrupted 24/7 operations, lower transaction costs by minimising the reliance on intermediaries, and thereby help to address inefficiencies in the current cross-border payment landscape.

Policy motivations influence the design of CBDCs. The development of CBDCs is shaped by policy objectives which in turn determine three critical design attributes: access, remuneration, and holding limits. Access defines who can transact with the CBDC, remuneration pertains to the potential returns from holding it, and holding limits establish the maximum allowable holdings.

Wholesale CBDCs are tailored for institutional use. When access to a CBDC is limited to IDTIs and financial institutions, it may serve as a substitute for central bank reserves. Such CBDCs can be either remunerated or non-remunerated and may feature high or no limits on transactions.

Retail CBDCs are designed to serve the needs of individuals and businesses. Retail CBDCs are designed to function as substitutes for physical cash or deposits, depending on their configuration. When access is restricted to individuals and businesses, the CBDC is non-remunerated, and strict holding limits are imposed, it operates as a substitute for physical cash. On the other hand, if the CBDC is widely accessible across various sectors, offers remuneration (such as interest), and permits higher holding limits, it may serve as a substitute for bank deposits. This latter configuration of retail CBDCs carries particular significance for deposit

[40] Panetta (2022).
[41] Illes et al (2025).
[42] IADI (2021).

insurers, as it could have implications for financial stability and the structure of the banking system.

1.4.2. Market relevance

Central banks worldwide are actively exploring CBDCs. Despite being implemented in only a few jurisdictions, central banks globally are dedicating significant resources to the development of CBDCs. According to the latest survey of the BIS, 91% of central banks are engaged in exploring either retail or wholesale CBDCs.[43]

Globally, three live CBDCs have been launched, all in emerging economies, but the adoption rates have been modest. To date, they include the Sand Dollar by the Central Bank of The Bahamas (2020), the eNaira by the Central Bank of Nigeria (2021), and JAM-DEX by the Bank of Jamaica (2022).[44] Despite their implementation, the uptake of these CBDCs has been limited. Three years after its launch, the Sand Dollar accounted for less than 0.2% of the total Bahamian dollars in circulation, indicating slow adoption. Similarly, the eNaira has faced challenges, with approximately 98.5% of wallets remaining inactive one year after its introduction[45, 46].

Pilot programmes in other jurisdictions are progressing.[47] Beyond the three live CBDCs, a number of central banks globally are advancing their pilot tests for retail CBDCs. These pilots aim to explore the technical, operational, and policy implications of CBDC implementation, with a focus on addressing specific needs within their respective economies.[48, 49]

1.4.3. Risks and regulation

Global policy principles for CBDCs aim to minimise harmful spillovers and promote collaboration. The BIS and a group of central banks[50] have established a set of foundational principles to guide the exploration of CBDCs. These principles are for CBDCs to (1) "do no harm" to monetary and financial stability; (2) coexist with other types of money, such as cash and private money; and (3) to promote broader innovation and efficiency.[51]

The G7 and G20 have reinforced the key principles and underscored the need for multilateral collaboration. The G7, while endorsing the BIS "do no harm" principle, has further highlighted

---

[43] Illes et al (2025). This is based on responses from 93 central banks globally.

[44] Those central banks have highlighted financial inclusion as one of the primary benefits of CBDCs. See Bank of Jamaica, Central Bank of Bahamas, Central Bank of Nigeria.

[45] Ree (2023).

[46] For a more detailed review of the adoption rates of the Sand Dollar and the JAM-DEX, refer to Branch et al (2025).

[47] Among advanced economies, the United States has taken a different stance. In January 2025, an executive order was signed to prohibit federal agencies from issuing any type of CBDCs (except to the extent required by law).

[48] The Chinese e-CNY has been in a pilot program since 2019. The pilot program has been gradually extended to different cities over the years and includes the use by public entities and companies of the e-CNY to make payroll payments to workers and increase transactions with e-CNY, see, Bai et al (2025).

[49] In India, the digital rupee is also undergoing pilot programs. Currently, 15 banks in India are offering CBDC wallets, and they have also integrated the system with a QR code to enable interoperability with other payment methods (see Reserve Bank of India).

[50] These included the Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, and the Board of Governors of the Federal Reserve.

[51] BIS (2020).

the importance of data privacy and protection, cyber resilience, and cross-border interoperability in the design and implementation of CBDCs.[52] The G20 has similarly underscored the need for multilateral collaboration to ensure CBDCs support global financial stability and enable seamless cross-border transactions.[53]

As a liability of the central bank, CBDCs possess a default-free nature, making them uniquely relevant from a financial stability perspective. This risk-free nature, shared only with physical cash and unmatched by any other digital product, plays an important role in shaping their design. However, despite their advantages, CBDCs also pose financial stability risks to the broader financial sector that require careful consideration.

Design decisions must balance demand and risk mitigation. Key design features, such as caps on holdings or transactions, remuneration through interest payments (or the absence thereof), and reverse waterfalls[54] play a crucial role in managing the risk of runs out of deposits and into default risk-free CBDCs. The central challenge lies in striking a balance between ensuring sufficient demand to achieve CBDC policy objectives and mitigating the risks associated with excessive demand.[55]

1.4.4. Relevance for deposit insurers

Demand for CBDCs may to a certain degree substitute for deposits and impact traditional banking functions. As deposits are a key funding source for IDTIs, this may constrain the ability of IDTIs to intermediate credit.

Bank deposit conversions to CBDCs could exacerbate financial instability during crises. A critical risk involves depositors converting deposits into CBDCs during periods of uncertainty, which could aggravate deposit runs and even trigger failures of IDTIs. This behaviour underscores the importance of addressing the potential destabilising effects of CBDCs when used as a store of value.[56]

1.4.5. Further questions

12. **To which extent can CBDCs complement or substitute deposits, and how does this impact deposit insurers' capacity to achieve public policy objectives?**

Close collaboration among financial safety-net participants – including central banks, supervisors and deposit insurers – will help understand how, to what degree and under what conditions CBDCs substitute for deposits and what the consequences might be during a crisis

---

[52] G7 Finance Ministers and Central Bank Governors (2021).
[53] FSB (2024b).
[54] Reverse waterfalls allow for automatic conversion of deposits into CBDC to the amount necessary for making a CBDC payment. They facilitate funds remaining on IDTI balances sheets.
[55] For a discussion of these, and other, CBDC issues, see Gross et al. (2025).
[56] ECB (2025) analysed the financial stability impact under different assumptions of digital euro holding limits. This included the impact on deposits, bank liquidity and profitability. Impact on deposits, under the highest assumed holding limit of €3,000 per individual, was limited in the "business-as-usual scenario", in which the digital euro is used as a means of payments for day-to-day expenditures. Aggregated outflows of deposits in this scenario were estimated at approximately 1.3% of total retail sight deposits. However, in a crisis or "flight-to-safety" scenario, with system-wide outflows due to a loss of confidence in the banking system, outflows under the same holding limit could reach €700 billion (8% of retail sight deposits).

when depositors run from traditional deposits to CBDCs. A question for deposit insurers is whether such behaviour could accelerate a crisis and necessitate faster action by deposit insurers and resolution authorities.

13. How do CBDC wallet offerings by IDTIs impact resolution?

In the event of the failure of an IDTI offering CBDC wallet services, ensuring continuity of access to retail CBDCs may require transferring the storage of user claims on the central bank to another CBDC wallet provider. This would require the identification of a suitable alternative provider and raises questions about the economic and technical conditions of the transfer, and the respective roles of safety-net participants.

14. Are CBDC users adequately protected against risks associated with the failure of wallet service providers?

The nature of CBDC, as a direct claim on the central bank, eliminates the default risk of CBDC issuers and generally avoids run risks on CBDC. Consequently, there is no need for deposit insurance coverage of CBDC itself. However, risks may arise in relation to ancillary services, such as the provision of digital wallets, which could face disruptions or failures due to operational risks, including cyber-attacks or theft, preventing users from accessing their CBDCs. The question of how users should be protected against those risks may require further investigation. It is not clear whether deposit insurers could or should have a role in protection users against such risks.

15. Could retail CBDCs be used to expedite depositor reimbursements?

Deposit insurers may explore the possibility of leveraging existing CBDC wallets as a tool for reimbursing insured depositors. This could accelerate the reimbursement process but involves several considerations, including CBDC holding limits and the coexistence of CBDCs with traditional accounts held with IDTIs in cases of deposit transfers.

2. The Market Actors: Financial Institutions and Depositors in a Digital Environment

This section explores the evolving landscape of financial institutions and depositors against the backdrop of rapid digital transformation. It examines how technological advancement and the market entry of actors which are not deposit taking institutions are reshaping the traditional banking value chain and the dynamics of deposit-taking. It analyses the relevance of increasing mobility of deposits, and the shifting expectations of digital-savvy depositors.

2.1. Technology, Deposit-taking Institutions and Other Actors

2.1.1. Market developments

Deposit taking institutions are actively pursuing initiatives to modernise their products, interfaces, internal systems, and processes to keep pace with rapid technological advancements and evolving customer expectations. Notable innovations include online-only IDTIs that operate without physical branches, 24/7 digital banking through internet and mobile platforms, and near-instantaneous transfers between accounts, which have significantly enhanced customer convenience. The adoption of cloud platforms has enabled centralised data storage and advanced analytics, allowing IDTIs to gain deeper insights into customer behaviour, improve risk management, and enhance decision-making. Automation technologies are streamlining routine operations, such as loan approvals and payment processing, boosting efficiency and enabling IDTIs to allocate resources to more strategic activities. Moreover, machine learning and artificial intelligence are revolutionising key areas like regulatory compliance, fraud detection, and personalised customer service. To further expand their offerings, IDTIs are increasingly collaborating with tech companies to deliver innovative, value-added solutions, such as advanced financial analytics, tailored financial products, and enhanced customer experiences.

Technological advancements and the rise of new market entrants are reshaping the traditional banking value chain, challenging incumbent IDTIs to adapt to a rapidly evolving landscape. While new entrants such as neobanks, fintechs, or BigTechs may not always hold banking licenses to accept deposits directly – and are therefore not subject to the same prudential and supervisory regulations as licensed deposit-taking institutions (IDTIs) – they often possess competitive advantages in areas such as technology, data analytics, and user experience. Technological innovations such as application programming interfaces (APIs) ease the connection between the traditional banking sector and non-bank service suppliers and foster greater competition, innovation, and efficiency in financial services. Such APIs may be part of open banking regulatory requirements, such as by the PSD2 in the EU, which require IDTIs to share customer data securely with third-party providers through application programming interfaces (APIs). This enables non-bank service providers to offer alternative solutions. As a result, traditional revenue streams for IDTIs, such as fees from payment processing and lending, are facing increasing pressure from these competitive offerings. Moreover, some fintech firms are leveraging their ability to build broad, cross-border customer bases and are climbing the value chain by offering innovative services, with some obtaining

banking licences to compete directly with traditional financial institutions. This shift is driving IDTIs to rethink their business models and focus on customer-centric, technology-driven solutions to maintain their competitive edge.

Technological innovation facilitates the partnering of IDTIs with new actors. Banking-as-a-service (Baas) occurs when IDTIs provide their infrastructure (often through APIs) to third-party non-bank business, enabling these to offer financial products to end-users. IDTIs monetise their infrastructure by offering it as service to non-IDTI actors. As "embedded finance", this combines non-financial products such as offerings on retail online marketplaces with financial offerings including payments, credit, insurance, and wealth management on platforms which are capable of reaching new customers.[57]

As NBFIs play an increasingly significant role in credit provision, the reliance on traditional deposits as a primary source of financing economic activities is gradually diminishing. NBFIs, including asset managers, fintech lenders, private equity firms, and securitisation vehicles, are increasingly facilitating credit flows through market-based instruments and wholesale funding mechanisms, bypassing traditional banking channels. By 2023, non-banks accounted for approximately one-third of total global credit assets, with the growth of the NBFI sector consistently outpacing that of traditional banks.[58] In many jurisdictions, private non-bank credit is expanding rapidly, penetrating a diverse range of industries and reshaping the financial landscape. [59]

2.1.2. Relevance for deposit insurers

The growing activity of new market participants may affect the allocation of deposits to IDTIs. Neobanks and fintechs, leveraging technology such as APIs, help reduce transaction costs and increase competition for deposits. As an example, deposit intermediators – third-party entities or platforms that facilitate the allocation of deposits across multiple IDTIs – reduce information and transaction costs for depositors by facilitating the placement of funds across multiple IDTIs. This benefits depositors by offering higher yields or enhanced effective deposit insurance protection through diversification, while also benefiting IDTIs by offering access to a wider set of depositors, stabilising the depositor base, or lowering funding costs. [60]

New market participants may give rise to new challenges for deposit insurers. Financial stability risks may arise if innovation leads to sudden, large-scale deposit inflows or reallocations in the banking system. This may require an increase in the frequency of evaluating the risks the deposit insurer is exposed to as it could amplify its liabilities. Operational and reputational risks for the deposit insurer may also arise. However, the relevance of these risks depends on the respective business models in deposit-placing markets. These may differ

[57] See BCBS (2024).
[58] See FSB (2024d).
[59] See BIS (2025a). Global total outstanding private loan volumes have increased from around $100 billion in 2010 to over $1.2 trillion today. Almost 90% of private credit is originated in the United States.
[60] Providers such as IntraFi have innovated in the deposit-taking landscape by creating a reciprocal deposit network for banks. De facto, this provides depositors with higher insurance coverage. It does so by splitting large deposits into smaller amounts, which ensures that the deposits stay below coverage limits. Participating banks profit from cheaper access to deposit-funding or from fees in making such funding available to other banks.

significantly. Whereas in some cases, deposit intermediation or banking-as-a-service business models lead to deposits being placed in person-specific accounts at an IDTI, in others, it leads to deposits of multiple depositors being held in omnibus or pooled accounts at IDTIs. In the latter case, the deposit insurer may be faced with complexities in obtaining accurate and timely depositor information. Pooled accounts can obscure the identities of individual depositors, making it difficult for deposit insurers to determine beneficial ownership and accurately calculate deposit insurance coverage during payout or resolution processes. As the role of such joint activities of bank and non-bank actors grows, deposit insurers may need to enhance their regulatory frameworks, data sharing agreements, and technological capabilities to address these challenges and ensure the continued effectiveness of deposit insurance systems.

2.1.3. Further questions

16. How do activities of market entrants that are not insured deposit-taking institutions (non-IDTIs) impact the ability of deposit insurers to meet their public policy objectives?

New, non-IDTI market entrants are reshaping the financial landscape by offering innovative services and deposit-like products that often operate outside the traditional banking system and regulatory frameworks. These developments pose significant challenges to deposit insurers, as such entities are not typically subject to the same regulatory scrutiny or deposit insurance coverage as IDTIs. This creates critical concerns regarding oversight, depositor protection, and financial stability, as customers may mistakenly assume that these new deposit-like products are insured, potentially undermining trust in the broader financial system. Addressing these challenges may require adapting existing regulatory frameworks to clarify the scope of deposit insurance coverage, enhancing public awareness to prevent misconceptions, and coordinating with other regulators to ensure that risks posed by these entities are effectively managed.

17. Does innovation in deposit-placing markets enhance financial efficiency or introduce new risks and complexities?

Innovation in deposit-placing markets, driven by new technologies and market participants, has the potential to enhance financial efficiency by improving the alignment of supply and demand for deposits, reducing transaction costs, and increasing competition. However, these advancements also introduce significant new risks and complexities. Deposit insurers may need to assess whether the risks associated with these innovations are adequately identified and appropriately priced, either through market mechanisms or by employing regulatory tools such as differential premium pricing models. This may involve evaluating the impact of increased deposit mobility, reliance on third-party intermediaries, and the emergence of non-traditional financial actors offering deposit-like products.

18. How can deposit insurers navigate the challenges arising from increasing cross-border activities? How can IADI help?

The increasing ease of cross-border deposits, facilitated by digital innovation and reduced transaction costs, is creating significant challenges for deposit insurers. Many financial service providers now operate across multiple jurisdictions, often without having a formal legal presence in every country where their services are offered. This can result in regulatory and

supervisory gaps, making it difficult to ensure consistent depositor protection and financial stability across borders. Furthermore, the cross-border nature of innovative financial products, such as tokenised deposits and digital wallets, complicates the ability of deposit insurers to identify and protect beneficiaries in the event of failure of an IDTI.

2.2. Digital Depositors: Are They different?

2.2.1. Market developments

Consumers are increasingly expecting financial services to be delivered with speed and convenience, a shift driven by rapid advancements in digital innovation. In recent years, there has been a significant rise in demand for instant or real-time payment services, a trend observed across both advanced and developing economies. Fast payment systems are characterised by instant payment message transmission and immediate beneficiary fund availability, operating on a 24/7/365 basis. This growing preference reflects the evolving expectations of consumers for seamless, efficient, and immediate financial transactions.[61] Such services are currently available to households and businesses in over 100 jurisdictions, with further launches planned in the years ahead.[62, 63] For example, 92% of businesses in the US use some form of fast or instant payment.[64] Brazil's PIX system, a fast payment platform launched by the central bank, has achieved widespread adoption. Within five years, PIX had reached over 90% of Brazilian adults and now handles more than half of all electronic payments in the country.[65]

Digital innovation has significantly reduced transaction and information costs, enabling depositors to transfer funds more easily both within the banking sector and to alternative financial service providers. The rapid digitalisation of financial services has also lowered barriers for individuals, particularly in advanced economies, to diversify their assets across a broader range of financial products and institutions. Using a single app, depositors may easily compare offerings and move deposits to another IDTI, to deposit-like money market funds or to equity markets.

2.2.2. Relevance for deposit insurers

Technological innovation may increase price sensitivity of depositors and lower the stickiness of deposits. Increased competition for deposits and available access to alternatives such as money market funds may increase the speed and frequency of deposit flows. The impact on the availability of deposit funding, however, may vary significantly across IDTIs.[66]

---

[61] For a discussion on changing user preferences in the financial sector, see Petralia et al (2019).
[62] World Bank (2021).
[63] CPMI (2021).
[64] Federal Reserve Financial Services (2024).
[65] Banco Central Do Brasil, PIX Statistics. Accessed on 15 October 2025.
[66] While part of the deposits used for investments are recycled into the banking system, this generally benefits larger institutions (eg entering repo transactions with NBFIs) and creates funding stress for smaller banks, see Bindseil and Senner (2024).

Shifting depositor time preferences, combined with technological advancements enabling instant transfers, have the potential to reshape the dynamics of run risks. The increasing expectation among customers for immediate and seamless access to their funds heightens the speed at which withdrawals can occur, particularly during periods of financial stress. This poses significant challenges for deposit insurance systems, raising critical questions about their ability to respond promptly and effectively to protect depositors and maintain financial stability in times of crisis. The FSB points out that the median speed of 2023 deposit runs was 7% per day, much higher than the 1% per day median of past deposit runs.[67] A recent study by the ECB found that increased use of online banking services amplifies extreme deposit outflows during periods of stress only slightly. The availability of mobile banking apps does not exacerbate this effect. Importantly, neither online banking nor mobile app usage has a causal effect on deposit volatility during normal times. The findings suggest that increased digitalisation has only little effect on extreme deposit outflow events.[68]

2.2.3. Further questions

19. **How can deposit insurers enhance their understanding of depositor behaviour in an increasingly digital environment, particularly in light of heightened competition for depositors' funds and the role of technology in increasing deposit volatility?**

The digital transformation of financial services has affected depositor behaviour, making it easier for individuals to move funds across institutions and even outside the traditional banking sector. Deposit insurers must develop a deeper understanding of how technology, such as mobile banking, online platforms, and real-time payment systems, impacts depositor decision-making and the stability of deposits. Heightened competition from non-IDTI financial institutions, such as fintech companies and providers of digital wallets, has introduced new challenges, as these entities often offer attractive alternatives to traditional deposits, such as higher yields or innovative financial products.

Deposit insurers could enhance their understanding of these trends by leveraging advanced data analytics and behavioural studies to monitor deposit flows, identify patterns in depositor activity, and assess the factors influencing depositors' decisions to move funds.

20. **How can deposit insurers adapt their procedures and operations to address depositor expectations for instant access to funds and mitigate the risk of runs during periods of financial stress, while maintaining public confidence and achieving their public policy objectives?**

The growing expectation for instant access to funds, driven by digital innovation, poses challenges for deposit insurers, particularly in times of financial stress. During a crisis, the ability of depositors to withdraw or transfer funds instantly may accelerate liquidity outflows from vulnerable institutions, increasing the risk of runs on IDTIs. Additionally, deposit insurers must address depositor concerns about the speed and reliability of insurance payouts, as delays or

[67] FSB (2024a).
[68] Fascione et al (2025).

inefficiencies in accessing insured deposits could further erode public confidence in the financial system.

To adapt, deposit insurers may need to modernise their operational capabilities, including investing in real-time data integration and monitoring systems to track deposit flows and identify early warning signs of stress. They may need to explore the feasibility of implementing faster payout mechanisms to meet depositor expectations for immediate access to insured funds in crisis situations. Furthermore, deposit insurers may need to engage in public education campaigns to clarify the scope and limitations of deposit insurance coverage.

3. Digital Technology – Opportunities and Risks for Deposit Insurance Systems

This section highlights the transformative potential and associated risks of emerging technologies – digital data access and automation, social media, cloud computing, artificial intelligence (AI), and quantum computing – on the financial sector, particularly for deposit insurers.

3.1. Digital Data Access and Automation

3.1.1. What is digital data access and automation?

Digital data access and automation involve the use of technologies and processes that enable seamless, standardised retrieval, exchange, and analysis of data to drive efficient, accurate, and data-driven decision-making. Data access is often facilitated through APIs, which serve as secure and structured channels for real-time sharing of data between systems or organisations. These APIs ensure that data is collected, transmitted, and integrated accurately and efficiently, reducing manual intervention and the risk of errors. Once data is retrieved in standardised formats, automation technologies, such as algorithms and machine learning models, apply predefined computational rules to analyse the data. This automated analysis enables organisations to process large volumes of information quickly and extract actionable insights for decisions. By streamlining workflows, digital data access and automation enhance operational efficiency, improve accuracy, and enable faster responses to dynamic business and regulatory needs in an increasingly digitalised environment.

3.1.2. Market relevance

Digital data access and automation have become integral to the financial services industry, transforming how institutions operate and interact with customers. By leveraging financial, transactional and non-structural data, IDTIs can offer tailored products and services such as customised loan options, personalised investment advice, and spending analytics. Automation technologies are also being deployed to optimise some critical processes including credit risk assessment, fraud detection, regulatory compliance monitoring, and supervisory reporting. These advancements position IDTIs to better meet the evolving needs of their customers in a highly competitive digital landscape.

3.1.3. Risks and regulation

While digital data access and automation offer substantial efficiency gains, they also introduce new risks that must be carefully managed to ensure the soundness and resilience of financial systems. Errors or biases can arise and propagate if the underlying data is inaccurate or incomplete or if the automated analysis processes are flawed. Additionally, reliance on third-party services for data storage and processing increases exposure to operational disruptions such as system failures or service outages. The growing dependence on interconnected platforms also heightens the risk of unauthorised access and cyberattacks. Furthermore, the handling of sensitive personal and business information is subject to increasingly stringent data protection regulations, requiring institutions to ensure compliance

with legal and ethical standards. To address these challenges, a robust framework for identifying, managing, and responding to information and communication technology (ICT)-related risks is essential for ensuring resilience and accountability across institutions and their service providers.[69]

The new IADI Core Principles underscore the critical importance of operational resilience for deposit insurers. Recognising the heightened exposure to risks such as system failures, cyberattacks, and data breaches, a new Core Principle 4 was introduced to encourage deposit insurers to establish an effective business continuity management framework. This framework is designed to guide deposit insurers to withstand, adapt to, and recover from severe operational risk-related disruptions, ensuring that critical functions such as depositor reimbursement, public communication and risk monitoring are not compromised. To achieve this, the framework necessitates the implementation of business continuity plans that minimise disruptions, which involves periodic reviews, testing, training, coordination, and communication exercises.

3.1.4. Relevance for deposit insurers

Data process automation offers significant opportunities to improve the efficiency, accuracy, and effectiveness of deposit insurers in fulfilling their mandates. One of the most impactful applications is the modernisation of information systems that support critical deposit insurance functions, including premium assessments, reimbursements, resolution planning, and resolution execution. Automation has the potential to transform several key areas, such as:

- **Early detection of anomalies in deposit dynamics**: Automated monitoring systems can identify unusual patterns in deposit flows, serving as early warning indicators of potential financial stress or instability. By enabling early intervention, automation may enhance abilities to prevent bank failures
- **Calculating risk-based premiums:** Leveraging comprehensive and real-time data, automation can enable deposit insurers to design and implement risk-based premium frameworks that calculate premiums based on current risk profiles, rather than relying on outdated period reports. This strengthens incentives for sound risk management within IDTIs
- **Supporting resolution planning:** Advanced analytical tools and dashboards can enhance resolution scenario analysis, allowing deposit insurers to develop, test, and execute effective resolution strategies with greater precision and speed
- **Determining eligibility and payout readiness:** Automation can streamline the assessment of depositor eligibility for insurance coverage and expedite the preparation of payout processes by accurately linking depositor accounts to IDTIs, significantly reducing response times during financial crises.

[69] See for example the BCBS Principles for the sound risk-management of third-party risk (December 2025).

3.1.5. Further questions

21. How can deposit insurers enhance their operational capacity to leverage automation?

To fully exploit the potential of automation, deposit insurers could explore the development of standardised and interoperable data structures and communication protocols to facilitate seamless and efficient data management. Upgrading legacy systems to accommodate automation and integrating advanced technologies such as AI and machine learning (ML) could enhance capabilities in areas like risk assessment, anomaly detection, and payout readiness.

22. Where might cooperation with other financial safety-net participants be necessary?

Effective collaboration with other financial safety-net participants, such as supervisory authorities, central banks, and resolution authorities could help to unlock synergies, enabling a more comprehensive and coordinated approach to the standardisation of data structures and communication protocols.

3.2. Social Media

3.2.1. What is social media?

Social media refers to digital platforms and networks that facilitate the creation, sharing, and exchange of information, opinions, and multimedia content in real time. These platforms enable users to connect and communicate on a global scale, fostering rapid dissemination of information. In the banking sector, social media plays a dual role: when leveraged effectively, it can enhance depositors' awareness of their IDTI's financial health and developments, while also increasing their responsiveness to news or events that may influence their confidence. Social media can also act as a conduit for misinformation or unverified claims, which may amplify market uncertainty, trigger panic, and influence depositor behaviour, potentially impacting financial stability.

3.2.2. Relevance for deposit insurers

Social media increases the likelihood and speed of deposit withdrawals. Social media enables the rapid and low-cost dissemination of information or misinformation to a vast audience within a short timeframe. Unlike other communication technologies, social media amplifies the credibility of information through peer-to-peer sharing within social networks, which can influence depositor behaviour significantly. The ease with which information or misinformation can spread on these platforms poses risks, as even sound IDTIs may face unwarranted depositor panic. Understanding these dynamics is critical for deposit insurers to improve crisis planning and develop effective response mechanisms to mitigate potential disruptions.

The rapid spread of information via social media reduces the time for deposit insurers to respond. The speed at which information circulates on social media can significantly shorten the timeframe available for deposit insurers to react during a financial crisis. Rapid deposit withdrawals, driven by social media-fuelled concerns, can accelerate the point at which an institution is deemed non-viable, triggering resolution actions. Deposit insurers must be prepared to implement non-payout resolution strategies that minimise disruptions to depositors' access to their insured funds. The reduced response time necessitates faster and

more efficient operational procedures by authorities, including deposit insurers, to maintain confidence and financial stability during such events.

Social media can serve as both a source of insights and a communication tool for deposit insurers. Social media can provide deposit insurers with a valuable resource for monitoring public sentiment and enhancing communication strategies. By leveraging social media analytics and sentiment analysis tools, deposit insurers and other financial safety-net participants can track institution-specific or deposit insurance-related discussions, identifying signs of declining confidence that may precede deposit outflows. Some deposit insurers have established dedicated social media monitoring teams or require IDTIs to monitor social media activity. Additionally, social media can be an effective platform for deposit insurers to conduct public awareness campaigns, providing accurate information and addressing concerns to strengthen depositor confidence and counter misinformation.

Social media use by the Indonesia Deposit Insurance Corporation (IDIC)

IDIC collaborates with influencers and key opinion leaders to amplify messaging and build trust. In a jurisdiction with over 210 million internet users and a social media penetration exceeding 60% of the population, IDIC strategically partners with individuals who have a strong follower base and credibility. As an example, IDIC engages social media personalities to create engaging content about deposit insurance and financial literacy, and partners with community leaders to disseminate information to specific target groups.

IDIC also has a comprehensive approach to tracking social network influence on digital transactions. This includes tracking through monitoring of social media sentiment toward the banking system. This may facilitate the early detection of critical events.

3.2.3. Further questions

23. How relevant is social media in explaining deposit volatility?

Social media has the potential to shape depositor sentiment and rapidly disseminate both accurate and inaccurate information that can influence deposit volatility. Its role in amplifying concerns, whether valid or based on misinformation, could exacerbate deposit outflows during periods of financial uncertainty. However, evidence regarding the extent of social media's impact on depositor behaviour remains inconclusive. It is unclear whether social media serves primarily as an amplifier of pre-existing concerns or as an independent driver of depositor actions.[70]

24. How can financial safety-net participants effectively monitor social media activities? Who is best positioned to monitor social media activities and assess their potential impact on IDTIs?

The responsibility for monitoring social media activities and assessing their potential impact on IDTIs depends on the structure and mandates of financial safety-net participants in a given

[70] FSB (2024a).

jurisdiction. Deposit insurers, financial supervisory authorities, and IDTIs themselves all have roles to play, with their responsibilities varying based on their expertise and regulatory remit. Deposit insurers may focus on monitoring depositor sentiment and identifying early warning signals of potential runs, while supervisory authorities can assess broader systemic risks and ensure institutions are prepared to address social media-driven challenges. IDTIs, as the entities directly impacted, may be best positioned to track institution-specific social media activity and respond to concerns in real time. Effective collaboration and coordination among these actors may help to ensure a comprehensive approach to managing the risks posed by social media to financial stability.

3.3. Cloud Computing

3.3.1. What is cloud computing?

Cloud computing enables the on-demand use of IT resources without the need for local or physical ownership of such infrastructure. This includes the remote and scalable use of infrastructure, such as servers and storage capacity (Infrastructure as a Service, IaaS). On a more sophisticated level, and building on IaaS, it also covers the provision of platforms that allow for easier development of applications (Platform as a Service, PaaS) and software (Software as a Service, SaaS). The latter presents a vertical integration of cloud computing by offering fully functional, ready-to-use applications on an infrastructure and platform managed by the provider.

Cloud computing offers significant opportunities for the financial sector by enhancing cost efficiency, scalability, and innovation. Cost benefits come from the reduced need for on-premises infrastructure. The inherent scalability of cloud services allows users to increase their consumption quickly when demand raises, without the need to change on-premise physical infrastructure. More advanced use of cloud computing (PaaS, Saas) offers access to applications and technologies such as artificial intelligence, machine learning, and big data analytics that users in the financial sector may not hold sufficient expertise in developing.

The adoption of cloud computing in the financial services sector is growing rapidly. KPMG[71] reports that cloud services for non-core systems, i.e. collaboration platforms and business relationship management, are seeing broader growing by banking and insurance companies. At the same time, core functions such as payments and transaction processing, credit underwriting, and regulatory reporting are also increasingly moving to the cloud, in part motivated by the success of fintech companies and open banking initiatives.

3.3.2. Risks and regulation

The use of cloud computing services in the financial sector comes with risks. The adoption of cloud computing services in the financial sector introduces a range of risks that, while not unique to the industry, require heightened attention due to the critical nature of financial services. Some of the most significant risks include:

[71] KPMG (2024).

- **Dependency on cloud service availability:** The provision of essential financial services increasingly relies on the uninterrupted availability of cloud services. Outages caused by technical failures, cyber-attacks, or actions by public authorities can create severe operational risks, potentially disrupting critical banking functions and undermining financial stability
- **Market concentration and vendor lock-in:** The cloud computing market is dominated by a small number of providers, creating risks of vendor lock-in if switching to alternative providers is prohibitively costly or technically challenging. Furthermore, the growing reliance on cloud providers for critical services may alter the traditional banking value chain, potentially reshaping long-term business models in the financial sector
- **Systemic risks from market concentration:** The high concentration of cloud service providers introduces systemic risks as the failure or disruption of a single dominant provider could have widespread financial stability consequences
- **Data security and privacy risks:** Storing sensitive data on cloud services exposes IDTIs to data security and privacy risks that could result in financial and reputational damage. However, while local storage on in-house infrastructure may seem like an alternative, it often carries similar risks. Given their scale and specialised expertise, cloud providers may, in many cases, be better equipped to implement robust cybersecurity measures and manage these risks more effectively.

Financial market standards and regulation aim at mitigating some of these risks. Global standards-setting bodies such as the FSB and BCBS emphasise the need for financial institutions to integrate cybersecurity into their operational resilience framework.[72] Standards focus on the adoption of robust governance, risk management, and incident reporting practices. The Digital Operational Resilience Act (DORA) in the EU, for instance, requires financial institutions to identify critical cloud service providers, implement risk management practices to ensure operational resilience, and to report significant ICT-related incidents. Similar notification requirements exist in other jurisdictions, such as the Computer-Security Incident Notification Rule in the US, which mandates IDTIs to notify regulators within 36 hours of a significant cybersecurity incident.

3.3.3. Relevance for deposit insurers

Cloud computing-related risks present a dual challenge for deposit insurers, as they can simultaneously threaten the viability of IDTIs and disrupt the insurers' ability to fulfil their critical functions during crises. The occurrence of operational, reputational, or financial stability risks associated with cloud computing could lead to the failure of an IDTI. In such cases, deposit insurers would need to intervene to protect depositors and uphold confidence in the financial system. However, the same disruptions to critical cloud services that cause these failures could also hinder deposit insurers' ability to access depositor records, process payouts, or coordinate resolution actions effectively. This dual vulnerability highlights the need for deposit insurers to incorporate cloud-related risks into their contingency planning and bolster

[72] See for example the BCBS Principles for Operational Resilience and the Revisions to the Principles for the Sound management of Operational Risk. The FSB's work on a Format for Incident Reporting Exchange (FIRE) aims at harmonising cyber incident reporting.

their operational resilience to ensure they can respond effectively and maintain stability during such scenarios.

3.3.4. Further questions

25. What cloud computing risks (if any) should deposit insurers incorporate into their strategic planning to ensure operational resilience and depositor protection?

This may involve identifying vulnerabilities associated with cloud service providers, such as service outages, data breaches, and vendor lock-in, which could impede access to depositor information and delay critical functions like reimbursements or resolution actions during crises.

26. What prerequisites must deposit insurers address to fully realise the benefits of adopting cloud computing while maintaining operational resilience and depositor protection?

Cloud computing offers numerous advantages for deposit insurers, including improved operational efficiency, scalability, and cost-effectiveness. However, to fully unlock these benefits, deposit insurers may need to ensure certain critical prerequisites. These include robust cybersecurity frameworks to protect sensitive data, ensuring strict compliance with regulatory requirements, and building resilience to potential service disruptions. Furthermore, deposit insurers may need to carefully evaluate the implications of storing sensitive depositor data on cloud infrastructure and address potential legal, regulatory, and data sovereignty issues.

3.4. Artificial Intelligence

AI refers to a broad field of computer science that enables machines to perform tasks typically requiring human intelligence, such as learning, reasoning, problem-solving, and decision-making. Key components of AI include machine learning neural networks, and algorithms designed for tasks such as prediction, classification, optimisation, and automation. In the financial sector, AI applications range from traditional machine learning models used for credit scoring, fraud detection, and risk assessment to more advanced generative AI systems. These systems can create content, analyse unstructured data (eg text, images, and audio), and power conversational interfaces like chatbots and virtual assistants. Modern AI systems, such as those powered by large language models, utilise billions of parameters trained on extensive datasets to perform sophisticated natural language processing, sentiment analysis, and complex decision-making tasks.

In the financial sector, AI is driving significant innovation by enhancing operational efficiency, enabling advanced data analytics, and improving regulatory compliance processes. It facilitates the development of personalised financial products and services tailored to individual customer needs and preferences. However, despite its growing adoption and potential, comprehensive data on the use and impact of AI in the financial sector remains limited, posing challenges for understanding its full implications and benefits.[73]

[73] FSB (2024c).

3.4.1. Risks and regulation

Recent reports have highlighted several vulnerabilities associated with the growing adoption of AI in the financial sector. These include risks stemming from third-party dependencies, particularly those tied to cloud infrastructure, as discussed in the previous chapter. Additional vulnerabilities include increased market correlations due to multiple institutions relying on similar AI models, heightened exposure to cyber risks through AI-enabled attacks, model risk arising from flawed or biased algorithms, and the potential for AI-driven financial fraud and the spread of disinformation. These risks underscore the need for robust safeguards to ensure the safe and responsible use of AI in finance. Recognising these challenges, the FSB has called on authorities to strengthen their oversight of AI in the financial sector. The FSB recommends enhancing regulatory and supervisory capabilities to address AI-related risks effectively. This includes adopting AI-powered tools for monitoring, which can help authorities detect and manage emerging risks, ensure compliance, and safeguard financial stability in the face of rapid technological advancements.[74]

3.4.2. Relevance for deposit insurers

AI has significant potential to enhance various deposit insurance processes. AI can play a critical role in risk assessment and early warning systems by analysing vast amounts of data to identify patterns and detect signs of financial distress in insured institutions. Additionally, AI can streamline the processing of reimbursement claims, automating tasks to ensure faster and more accurate payouts to depositors in the event of IDTI failures. Furthermore, AI can support resolution planning by providing data-driven insights and predictive analytics, enabling deposit insurers to develop and implement more effective and timely resolution strategies.

3.4.3. Further questions

27. What deposit insurer activities would benefit most from AI applications?

Deposit insurers could explore how AI can enhance critical processes such as risk assessment, early warning systems, reimbursement claim processing, and resolution planning. Specific applications could include fraud detection, depositor eligibility verification, and predictive modelling for identifying early signs of financial distress in insured institutions. The integration of AI could lead to faster identification of vulnerabilities, preventing bank runs and protecting depostiors by enabling proactive interventions.

28. How should AI be approached responsibly to mitigate associated risks?

To mitigate the risks associated with AI, such as model biases, data privacy issues, and cybersecurity vulnerabilities, deposit insurers may need to adopt safeguards to ensure transparency and explainability in AI systems to build trust and complying with relevant regulatory and ethical standards.

[74] FSB (2024c) and Bank of England (2025).

AI use by the Financial Services Compensation Scheme (FSCS) – UK

In the United Kingdom, FSCS is investing in AI technology to help deliver high-quality service and provide the best value to its levy-payers. The claims the organisation receives are becoming increasingly complex and require a greater volume of evidence and documentation from customers or third parties, which must be worked through before a decision can be made. Most claim processing time is spent gathering evidence from third parties to build a full picture of the customer situation at the point of failure.

To improve the efficiency of this process, new search functionality and AI are being utilised to help claim handlers. This approach is exemplified by the organisation's use of data lake and search tools. The data lake is a large pool of unstructured data, such as emails, policy documents and application forms, which a trained handler would normally need to look through. The tool uses machine learning to search and highlight those words that the claims handlers should search for, significantly reducing the time taken to locate key documents. It is also used to assist the claim handler in identifying the product a claim relates to and the activity of a failed firm.

The organisation is also exploring other practical uses for AI, including analysing information on forms, extracting text, tables and structures from documents (including being able to read handwriting), and even transcribing audio from phone calls. Experienced claim handlers will then review this output and produce assessments of the claims to ensure quality and consistency are maintained. All final decisions on a claim are made by the claim handler.

3.5. Quantum Computing

3.5.1. What is quantum computing?

Quantum computing presents both significant opportunities and substantial risks for the banking and financial sectors, including deposit insurance operations. On the one hand, quantum computers have the potential to revolutionise the industry by solving a subset of complex problems that are currently beyond the reach of classical computers. In banking and finance, quantum computing could enhance risk assessment, improve the accuracy of macroeconomic models, optimise portfolio management, and enable more robust stress testing by processing vast amounts of data and running simulations at unprecedented speeds. This may require recalibration of bank risk models or models used for pricing derivatives. The overall capabilities of quantum computing could provide deposit insurers with deeper insights into financial risks and improve the precision and timeliness of their decision-making. On the other hand, quantum computing poses a serious threat to the security of current encryption methods which are widely used to protect sensitive financial data. Quantum computers could potentially break these encryption techniques, rendering traditional cryptographic systems vulnerable. For deposit insurers whose operations depend on secure systems to protect highly sensitive data such as depositor identities, account balances, and payment instructions, this poses a critical risk. If encryption is compromised, it could lead to severe consequences,

including data breaches, fraud, privacy violations, manipulation of financial records, and a significant erosion of public trust in deposit insurance systems.

3.5.2. Risks and regulation

The primary threat posed by quantum computing is its potential to break widely used encryption standards. To address this emerging threat, the US Quantum Computing Cybersecurity Preparedness Act enacted in December 2022 requires federal agencies to prepare for the transition to quantum-resistant cryptography. The Act mandates federal entities to identify systems vulnerable to quantum threats, develop strategies to mitigate risks, and begin migrating to quantum-resistant cryptographic standards once they are established. These efforts aim to ensure the long-term protection of critical systems and sensitive data against potential quantum-enabled attacks. Similar initiatives are underway in other jurisdictions, including Australia, Canada, the EU, Japan, Singapore, and the United Kingdom, where governments and institutions are working to advance research and development in post-quantum cryptography.

3.5.3. Relevance for deposit insurers

Quantum threats pose risks to deposit insurance operations that rely on the secure processing of highly sensitive data. This data includes depositor identities, account balances, and payment instructions, all of which are protected by current encryption standards that could become vulnerable to quantum-enabled attacks. If these encryption methods are compromised, the consequences could be severe. Potential risks include fraud through unauthorised claims on deposit insurance funds, privacy breaches exposing sensitive depositor information, integrity failures that could allow the manipulation or falsification of payout records, and, ultimately, a loss of public confidence in the reliability and security of deposit insurance systems.

3.5.4. Further questions

29. How should deposit insurers anticipate quantum-related risks and opportunities?

To mitigate these risks, deposit insurers may need to assess their cryptographic vulnerabilities and prepare for the transition to quantum-resistant cryptographic standards. This may involve working closely with other financial safety-net participants, regulators, and cybersecurity experts to ensure that systems and processes are resilient against future quantum threats, thereby safeguarding depositor data and maintaining trust in the financial system.

References

Adrian, T, P Bains, M Bechara, E Cerutti, S Forte, F Grinberg, A Gullo, M Hengge, K Kao, T Mancini-Griffoli, S Martinez Peria, M Miccoli, M Reuter, N Sugimoto (2025): "Understanding Stablecoins", *IMF Departmental Paper,* no 2025/009, December.

Ahmed, R, I Aldasoro (2025): "Stablecoins and safe asset prices", *BIS Working Papers,* no 1270, May.

Aldasoro, I, M Aquilina, U Lewrick and S Hyuk (2025): "Stablecoin growth – policy challenges and approaches", *BIS Bulletin,* no 108, July.

Auer, R, U Lewrick and J Paulick (2025): "DeFiying gravity? An empirical analysis of cross-border Bitcoin, Ether and Stablecoin flows", *BIS Working Papers,* no 1265.

Bai, C, L William, M Luo and P Xie (2025): "Adoption of central bank digital currencies: Initial evidence from China", *Journal of Corporate Finance*, 91, April.

Bains, P, (2025): "Blockchain consensus mechanisms: A primer for supervisors", *IMF Working Paper,* no 2025/186, September.

Bank for International Settlements (BIS) (2020): "Central bank digital currencies: foundational principles and core features", *Joint Report by the Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors of the Federal Reserve and Bank for International Settlements*, October.

——— (2021a): "Application of the Principles for Financial Market Infrastructures to stablecoin arrangements", *Joint CPMI-IOSCO Report*, October.

——— (2021b): "Developments in retail fast payments and implications for RTGS systems", *CPMI Papers*, December.

——— (2024a): "Project Pyxtrial: monitoring the backing of stablecoins", *BIS Innovation Hub Report*.

——— (2024b): "Tokenisation in the context of money and other assets: concepts and implications for central banks", *Joint BIS-CPMI Report*, October.

——— (2025a): "International banking and financial market developments", *Quarterly Review*, March.

——— (2025b): "The next-generation monetary and financial system", *Annual Economic Report*, Chapter III, June.

Banco Central Do Brasil (2025): *PIX Statistics*. https://www.bcb.gov.br/estabilidadefinanceira/estatisticaspix. Accessed on 15 October 2025.

Bank of England (2025): *Financial stability in focus: artificial intelligence in the financial system*, April.

Basel Committee on Banking Supervision (BCBS) (2024): *Digitalisation of finance*, May.

Bindseil, U and R Senner (2024): "Destabilisation of bank deposits across destinations: assessment and policy implications", *ECB Working Paper Series,* no 2887.

Branch, S, Y Cooper, C Franco, J Frost, P Koo Wilkens, Y Lyu, J McIntosh, C Mu, T Phillip, E Salinas, L Ward, T Walker and A Wright, (2025): "Retail CBDCs in practice: the experience of the Sand Dollar, E-CNY and JAM-DEX", *SSRN Working Paper*, September.

Chainalysis (2025): *The 2025 Geography of Crypto Report*, October.

Coinmarketcap (2025). *Stablecoin dashboard*, https://coinmarketcap.com/view/stablecoin/. Accessed on 22 October 2025.

Crisanto, J C, J Ehrentraud and D Garcia Ocampo (2024). "Stablecoins: regulatory responses to their promise of stability", *FSI Insights,* no 57, April.

European Banking Authority (EBA) (2024): *Report on tokenised deposits*, EBA/REP/2024/24, December.

European Banking Authority (EBA) (2024a): Final Report, Draft Regulatory Technical Standards to further specify the liquidity requirements of the reserve of assets under Article 36(4) of Regulation (EU) 2023/1114, EBA/RTS/2024/10

European Central Bank (ECB) (2020): "Stablecoins: implication for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the Euro area", *Occasional Papers*, no 247.

——— (2025): *Technical data on the financial stability impact of the digital euro*, October.

European Systemic Risk Board (ESRB) (2025): "Crypto-assets and decentralised finance: Report on stablecoins, crypto-investment products and multi-function groups", *ESRB Crypto-asset Task Force Report*, October.

Fascione, L, J Jacoubian, B Scheubel, L Stracca, and N Wildmann (2025): "Mind the app: do European deposits react to digitalisation?", *ECB Working Paper Series,* no 3092.

Federal Reserve Financial Services (2025): "2024 Business Payments Study", *Insights Brief*, April.

Financial Action Task Force (FATF) (2020): *FATF Report to the G20*, June.

Financial Stability Board (FSB) (2023): *High-level recommendations for the regulation, supervision, and oversight of global stablecoin arrangements*, July.

——— (2024a): "Depositor behaviour and interest rate and liquidity risks in the financial system", *Report to the G20*, October.

——— (2024b): "G20 roadmap for enhancing cross-border payments", *Consolidated progress report,* October.

——— (2024c): "The financial stability implications of artificial intelligence", *Report to the G20,* November.

——— (2024d): *Global monitoring report on non-bank financial intermediation*, December.

——— (2024e): The Financial Stability Implications of Tokenisation, October.

——— (2025): "Thematic review on FSB global regulatory framework for crypto-asset activities", *Peer Review Report*, October.

G7 Finance Ministers and Central Bank Governors (2021): *Statement on central bank digital currencies (CBDCs) and digital payments*, October.

Garcia Ocampo, D (2025): "Stablecoin-related yields: some regulatory approaches", *FSI Briefs* 27, October.

Garratt, R, and H S Shin (2023): "Stablecoins versus tokenised deposits: implications for the singleness of money", *BIS Bulletin,* no 73, April.

Gross, M, M Miccoli, J Verrier, G Villegas-Bauer (2025): "Evaluating the Implications of CBDC for Financial Stability", *IMF Fintech Notes*, no 2025/008, November.

Ilves, A, A Kosse, and P Wierts (2025): "Advancing in tandem – results of the 2024 BIS survey on central bank digital currencies and crypto", *BIS Papers,* no 159, August.

IADI (2014): *Core principles for effective deposit insurance systems*, November.

——— (2021): "Central bank digital currencies – the motivation", *Fintech Brief,* no 5, November.

——— (2026): *E-money and deposit insurance: policy options (forthcoming)*.

International Organization of Securities Commissions (IOSCO) (2025): *Thematic review assessing the implementation of IOSCO recommendations for crypto and digital asset Markets*, October.

KPMG (2024): *Industry Cloud for Financial Services Sector*, February.

Maechler, A (2025): "How deposits can harness tokenisation", Remarks by the deputy general manager and acting head of BIS Innovation Hub, Bank for International Settlements (BIS), at the Singapore Fintech Festival, Singapore, 12 November 2025.

Panetta, F (2022): "Demystifying wholesale central bank digital currency", Speech at the Symposium on "Payments and securities settlement in Europe – today and tomorrow", September.

Petralia, K, T Philippon, T Rice and N Véron (2019): "Banking disrupted? Financial intermediation in an era of transformational technology", *Geneva Reports*, no 22, September.

Ree, J (2023): "Nigeria's eNaira, One Year After", *IMF Working Paper,* no 2023/104, May.

Reuter, M (2025): "Decrypting crypto: how to estimate international stablecoin flows", *IMF Working Paper*, no 141, July.

United States (US) Department of Treasury (2025): "Digital money", *Treasury Borrowing Advisory Committee Presentation*, April.

World Bank (2021): *Considerations and lessons for the development and implementation of fast payment systems*, September.