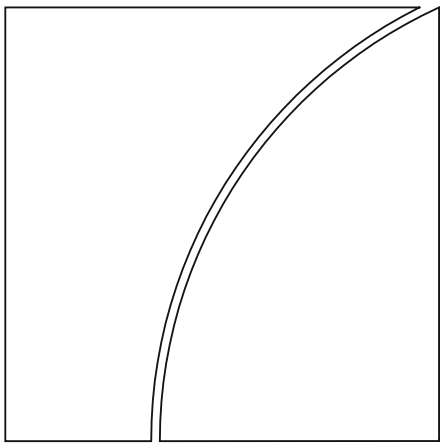
Financial Stability Institute

FSI Insights

on policy implementation

No 33



Fintech and payments: regulating digital payment services and e-money

By Johannes Ehrentraud, Jermy Prenio, Codruta Boar, Mathilde Janfils and Aidan Lawson

July 2021

JEL classification: E42, G18, G23, G28, O30, O38
Keywords: fintech, regulation, digital payment services, e-money, stablecoins

BANK FOR INTERNATIONAL SETTLEMENTS

FSI Insights are written by members of the Financial Stability Institute (FSI) of the Bank for International Settlements (BIS), often in collaboration with staff from supervisory agencies and central banks. The papers aim to contribute to international discussions on a range of contemporary regulatory and supervisory policy issues and implementation challenges faced by financial sector authorities. The views expressed in them are solely those of the authors and do not necessarily reflect those of the BIS or the Basel-based committees.

Authorised by the Chair of the FSI, Fernando Restoy.

This publication is available on the BIS website (www.bis.org). To contact the BIS Media and Public Relations team, please email press@bis.org. You can sign up for email alerts at www.bis.org/emailalerts.htm.

ISSN 2522-2481 (print)
ISBN 978-92-9259-477-0 (print)

ISSN 2522-249X (online)
ISBN 978-92-9259-478-7 (online)

Contents

Fintech and payments: regulating digital payment services and e-money[1]

Executive summary

This paper explores how non-bank payment service providers (NBPSPs) are regulated. Improvements in technology, coupled with growing demand for digital payment methods, are increasingly reshaping the way payments are made. Covid-19 too is changing how consumers and companies purchase goods and services and make payments. While the payments space continues to be dominated by banks in many countries, the role of NBPSPs operating a variety of business models is gaining prominence. This paper provides a cross-country overview of the regulatory requirements for digital payment and e-money services offered by NBPSPs. It benefited from responses to a CPMI survey of 75 jurisdictions conducted in early 2021 and was supplemented by a desktop review of public documents issued by selected authorities.

Payment systems involve a wide range of NBPSPs. On a broad level, one can distinguish between NBPSPs that offer consumer-facing or retail services at the "front end" and those that play roles in clearing, settlement and processing at the "back end". Some NBPSPs operate closed-loop systems which combine both front-end and back-end arrangements under one roof. Among them are large technology firms – big techs – that offer payment services as part of a much wider set of activities.

The proliferation of NBPSPs in retail payments in many jurisdictions has raised questions about their regulation. The growing importance of fintech-driven NBPSPs presents opportunities. Aside from promoting financial inclusion, they could also enhance competition and efficiency in payments markets. However, this comes with potential risks in terms of consumer protection, operational and cyber resilience, the protection of funds in transit or storage, data protection, digital exclusion and market concentration. Authorities are therefore assessing whether their existing regulatory frameworks are adequate.

Among the payment services that NBPSPs can offer, e-money issuance is currently the most intensively regulated, while the provision of virtual asset services is the least. On average, jurisdictions where non-banks can issue e-money impose nine types of requirement on this service. In the case of virtual asset services, only around four types of requirement are imposed on average. Anti-money laundering (AML) and countering financing of terrorism (CFT) requirements are most commonly imposed on payment services offered by NBPSPs. Other common requirements are those relating to risk management and data protection, while the least common are those relating to interoperability. In general, this underscores that "mature" payment services tend to have well defined and fairly established regulatory frameworks but those for newer services may still be evolving. Thus, there is scope for authorities to learn more about the regulatory approaches (including the rationale for these approaches) in other jurisdictions when it comes to new payment services. This ensures that all risks arising from these services are adequately addressed in regulations.

Application of some regulatory requirements for payment services varies widely. Requirements related to AML/CFT, risk management and cybersecurity, data protection and consumer protection are, in general, uniformly applied across payment services. However, this is not the case for

[1] Codruta Boar (codruta.boar@bis.org), Johannes Ehrentraud (johannes.ehrentraud@bis.org), Aidan Lawson (Aidan.lawson@bis.org) and Jermy Prenio (jermy.prenio@bis.org), Bank for International Settlements, and Mathilde Janfils (mathilde.janfils@outlook.com), former FSI Graduate. We are grateful to Tara Rice, Committee on Payments and Market Infrastructures, and Mariam Yeghiazaryan, Central Bank of Armenia, for their involvement in earlier stages of this paper, the authorities that participated in the survey and to Patrizia Baudino, Jon Isaksen, Tanai Khiaonarong, Thomas Lammer and Alexandre Stervinou for helpful comments. Esther Künzi provided valuable administrative support.

requirements related to authorisation, minimum capital, safeguarding of funds and interoperability. The objectives of these requirements may be the same, but how they are applied across payment services can be quite different. Moreover, the practices of implementing these requirements vary significantly across jurisdictions even with the same payment service.

Non-banks can offer more types of payment service and tend to be less intensively regulated in advanced economies (AEs) than in emerging market and developing economies (EMDEs). In some jurisdictions – mostly AEs – non-banks can offer all types of payment service included in the survey, while in some EMDEs non-banks are only able to offer few. Moreover, NBPSPs in EMDEs, particularly those acquiring payment transactions, providing e-wallet services and issuing e-money, face more regulations than those in AEs. Given the potential of NBPSPs to foster financial inclusion, authorities in EMDEs might already start considering strategies for expanding their payment services markets and reviewing the appropriateness of existing regulations for these players. In this way, they can promote innovation while ensuring the safety and integrity of their financial systems.

Novel technologies are creating the potential for new means of payments to emerge. While the market capitalisation of cryptoassets is growing, it is increasingly clear that their high price volatility makes them ill-suited as a means of payment. Stablecoins, a new type of cryptoasset that emerged in 2014, are designed to maintain a stable value relative to a specified asset, or a basket of assets. While the role of stablecoins as a new payment method could potentially increase over time, the jury is still out on whether one or more stablecoins will be widely adopted as a payment method.

Regulatory approaches for stablecoins are starting to evolve. Work is under way in some jurisdictions to adapt their regulatory framework for cryptoassets, and stablecoins in particular. Prominent examples are ongoing initiatives in the United Kingdom (consultation by HM Treasury) and the United States (statement by US President's Working Group on Financial Markets, STABLE Act proposal). At present, according to a 2020 FSB survey, most jurisdictions do not have regulations that are specific to stablecoins but see the need for adjustments to existing regulations. The EU's MICA Regulation proposal, on the other hand, proposes a bespoke regulatory regime for cryptoassets including stablecoins. Absent a dedicated regulatory framework, if a stablecoin resembles an already regulated product or service, authorities will likely treat the stablecoin as such under existing regimes, which apply in whole or part depending on the coin's characteristics.

The role of big techs in payments and their potential involvement in global stablecoin (GSC) arrangements will likely receive further attention. Big techs have already captured a sizeable market share in digital payments in some jurisdictions. But even where they have not, this could change quickly due to the unique features of their business models. At present, big techs are subject to the same requirements as those of other market participants when providing financial services (including payments); and there seems to be a case for relying more on entity-based rules for big techs in certain policy areas to address the risks stemming from the different activities they perform (Carstens (2021a) and Restoy (2021)). In future, some big techs may become involved in GSC arrangements. For policymakers, it will be important to appreciate the unique combination of a very specific type of entity (big techs) providing a very specific type of activity (provision of GSC), and to consider the potential implications of this interplay.

Section 1 – Introduction

1. **Improvements in technology, coupled with growing demand for digital payment methods, are increasingly reshaping the way payments are made.** Recent advances in technology have opened up new ways to pay, in line with consumers' demand for payment methods that are convenient, easy to use, frictionless, low-cost and contactless.[2] As a result, consumers have been shifting from cash to cashless payment instruments (CPMI (2020a)) in recent years. In 2012, the average number of digital payments in CPMI jurisdictions was 176 per inhabitant; in 2019, it was 303. A similar shift in service channels has occurred in advanced economies (AEs). While the number of bank branches and automated teller machines (ATMs) have declined, point-of-sale (POS) terminals and payment applications have become more widespread (CPMI (2020a)).

2. **The Covid-19 pandemic has further accelerated the trend towards more digital payments.** Covid-19 has changed the way consumers purchase goods and services. Fuelled by concerns that the coronavirus could be transmitted by cash, many consumers have displayed a certain degree of hesitancy in using cash since the pandemic hit (Auer et al (2020)). To avoid having physical contact with a surface or object that is potentially contaminated, many opted for contactless payment methods, which work by waving a card or a phone.[3] In addition, shelter-in-place requirements and other restrictions have induced many customers to shift from shopping in brick-and-mortar stores to online platforms, which have always been supported by digital payments. Overall, Covid-19 has accelerated the shift toward the increasing use of digital payments during the pandemic and potentially beyond.[4]

3. **Changes in consumer preferences and technological innovation have encouraged private sector competition and diversity in payments.** As such, the landscape now includes NBPSPs that offer their payment services by placing an overlay on existing payment infrastructures, while others use their own proprietary standalone systems. Large technology firms – big techs – also offer payment services as part of a much wider set of activities, using a business model that benefits from competitive advantages stemming from the so-called **d**ata analytics, **n**etwork externalities and interwoven **a**ctivities (DNA) loop.[5] Thanks to their DNA, big techs can leverage strong network effects, as well as their extensive customer networks and access to large troves of data.

4. **Digital payment services will be affected by ongoing work at the international level to address challenges in cross-border payments.** These challenges include high costs, low speed, limited access and insufficient transparency.[6] In response, the G20 made enhancing cross-border payments a priority during the 2020 Saudi Arabian Presidency. In July 2020, the CPMI responded by publishing a report that identifies a set of building blocks where further joint public and private sector work could enhance cross-border payments. The 19 building blocks are arranged into five focus areas, one of which is coordinating on regulatory, supervisory and oversight approaches.[7] The report notes that while much of

[2] For example, electronic (e)-wallets allow consumers to use their personal devices to make payments both online and at the point of sale. Examples include Apple Pay, Google Pay, Samsung Pay and PayPal.

[3] While transactions above certain thresholds require a signature or a PIN entry on a merchant-owned device, many countries have raised these limits to increase the scope for truly contactless payments.

[4] As one example, in Canada, a November 2020 survey found that two thirds of small businesses now accept payments online—and half of them started doing so only recently (Lane (2020)).

[5] See BIS (2019) and Crisanto et al (2021).

[6] See www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/cross-border-payments/.

[7] Building blocks under this focus area are (i) align regulatory, supervisory and oversight frameworks; (ii) apply AML/CFT consistently and comprehensively; (iii) review interaction between data frameworks and cross-border payments; (iv) promote safe payment corridors; and (v) foster KYC and identity information-sharing. See CPMI (2020b) and FSB (2020c).

the focus for removing frictions in cross-border payments has typically been on technology and operations, equal attention should be paid to divergent regulation, supervision and oversight frameworks across jurisdictions.

5. **Against this backdrop, questions are growing louder as to whether the regulatory framework for NBPSPs would benefit from adjustments.** The rise of non-banks in payments, challenges in cross-border payments and the collapse of Wirecard AG[8] in 2020 may have been the impetus in some jurisdictions to look into payments regulation and oversight. In September 2020, the Chair of the SSM's Supervisory Board noted that "the development of non-bank institutions providing payments and other bank-like services under a lighter regulatory regime might require some further reflections by legislators at the national and European level on the perimeter of regulation and supervision."[9] For authorities, when assessing the regulatory framework, the question is whether it is commensurate to the risks NBPSPs bring to the financial sector, or whether adjustments can foster financial stability and customer protection while not compromising other policy objectives such as promoting financial inclusion and innovation.

6. **This paper provides a cross-country overview of the regulatory requirements for digital payments and e-money services provided by NBPSPs.** Following the conceptual framework in Ehrentraud et al (2020) (Chart 1), we assess fintech activities that make use of technology to facilitate payment transactions (digital payments services and e-money). While these activities could be carried out by banks and non-banks alike, the focus of this paper is on payment service providers that are not classified and regulated as banks.[10] The analysis in this paper has benefited from responses to a CPMI survey of 75 jurisdictions in 2021 (Annex 1), as supplemented by a desktop review of published documents and our own analysis.

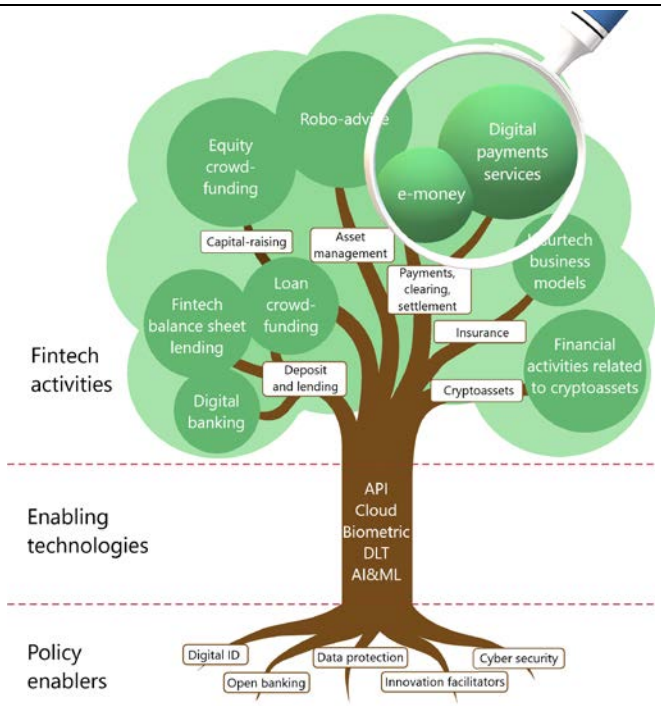
7. **The paper is structured as follows.** Section 2 gives an overview of the architecture of payments and describes the different types of NBPSP and the payment services they provide. Section 3 reviews the regulatory requirements for digital payments and e-money services. Section 4 outlines more recent innovations in payments in the form of stablecoins, and the emerging regulatory responses. Section 5 offers considerations for financial authorities and concludes.

[8] On 25 August 2020, the Local Court of Munich opened insolvency proceedings regarding the assets of Wirecard AG, a global company specialising in electronic payments systems and technology. See Enria (2020a) and www.wirecard.com/2020/08/25/opening-of-insolvency-proceedings-concerning-assets-of-wirecard-ag-dr-jur-michael-jaffe-appointed-as-insolvency-administrator/.

[9] See Enria (2020b).

[10] In particular, given our emphasis on activities that have seen significant changes due to innovation in recent years, we focus on NBPSPs that play roles in front-end arrangements, ie PSPs (including big techs) that offer their services directly to end users (payer and payee), and which may use overlay and/or standalone systems. See Section 2.

Fintech tree: a taxonomy of the fintech environment Chart 1



Source: Adapted from Ehrentraud et al (2020).

Section 2 – A taxonomy of the retail payments environment

Architecture of payments

8. **A payment system is a set of instruments, procedures and rules for the transfer of funds.**[11] Depending on the payment type, payment systems can be qualified as retail or wholesale. Retail payments are used between individuals and businesses while wholesale payments are between banks, financial market infrastructures and other financial institutions. At the same time, retail payment systems execute large volumes of relatively low-value transactions while wholesale payment systems generally handle large-value payments. When it comes to the operator of a payment systems, retail payment systems are usually run by public and private sector providers while wholesale payment systems are typically owned and operated by central banks.[12]

9. **A payment system's infrastructure involves front-end and back-end arrangements.** Front-end arrangements involve elements that initiate the payment, while back-end arrangements process, clear and settle payments (Chart 2). The focus of this paper is on front-end arrangements for retail payments, for which we distinguish three elements: the underlying transaction account, the payment instrument and the service channel/access point.

[11] See Committee on Payments and Market Infrastructures and International Organization of Securities Commissions (CPMI-IOSCO), *Principles for Financial Market Infrastructures*, April 2012, p 8.

[12] See BIS (2020a,b) for a detailed description of key facts in payment systems.

- ***The underlying transaction account*** **represents the source of the funds and generally encompasses bank accounts and e-money transaction accounts.** These accounts are similar in nature as they can be used to make and receive payments and to store value. However, some features vary such as the ability to incorporate a credit facility, and aspects related to regulatory classification,[13] coverage under deposit insurance schemes[14] and the redemption guarantee/safeguarding mechanism.[15] Alongside this broad classification of accounts, transaction accounts can differ in price and the services they offer.[16]

- ***Payment instruments*** **are used to initiate a transfer of value.** They can be further classified into cash (banknotes and coins) and cashless instruments (eg cheques, credit transfers, direct debits, card and e-money based instruments[17]). Since its introduction, e-money has assumed a prominent role among payment instruments. The various types of e-money-based instrument include online money when the payment instruction is initiated via the internet, mobile money[18] when initiated via mobile phones, and prepaid cards. (CPMI-WB, (2016)). For an instrument to be considered e-money, it typically needs to (i) serve as a multipurpose medium of exchange; (ii) be accepted as a means of payment by parties other than the issuer; and (iii) be issued only on receipt of funds (e-money is prepaid).[19] A more detailed description of e-money is provided in Box 1.

- ***The service channel/access point*** **connects the payer/payee and payment service provider (PSP).** They can be differentiated into in-person (eg bank branch, ATM, POS) and remote access points (eg payments initiated via internet, mobile applications). The shift to digital payment services is accelerating, with the network of traditional access points thinning out and fewer options for consumers to access cash (CPMI (2020a)). In the case of *digital payment services,* providers make use of technology to facilitate payment transactions by transferring money and clearing or settling balances digitally without the use of physical money. As such, they digitally channel funds from payers to payees, by either handling payers' money themselves or initiating payment orders on behalf of payers with respect to transaction accounts held at other financial institutions.[20]

[13] Bank deposits vs e-money.

[14] Covered for bank accounts and mostly not covered for e-money accounts.

[15] Such as prudential regulation/supervision, central bank liquidity facilities for bank account vs safeguarding measures as per national regulation for e-money accounts.

[16] For example, payment accounts operated by NBPSPs are intended for holding funds that are linked to future payment transactions, which is why they can be described as flow-through accounts. Furthermore, some accounts offer only a limited set of services at low or no fees while others offer the full set of services expected from fully fledged retail customer or corporate accounts (CPMI-WB (2016)).

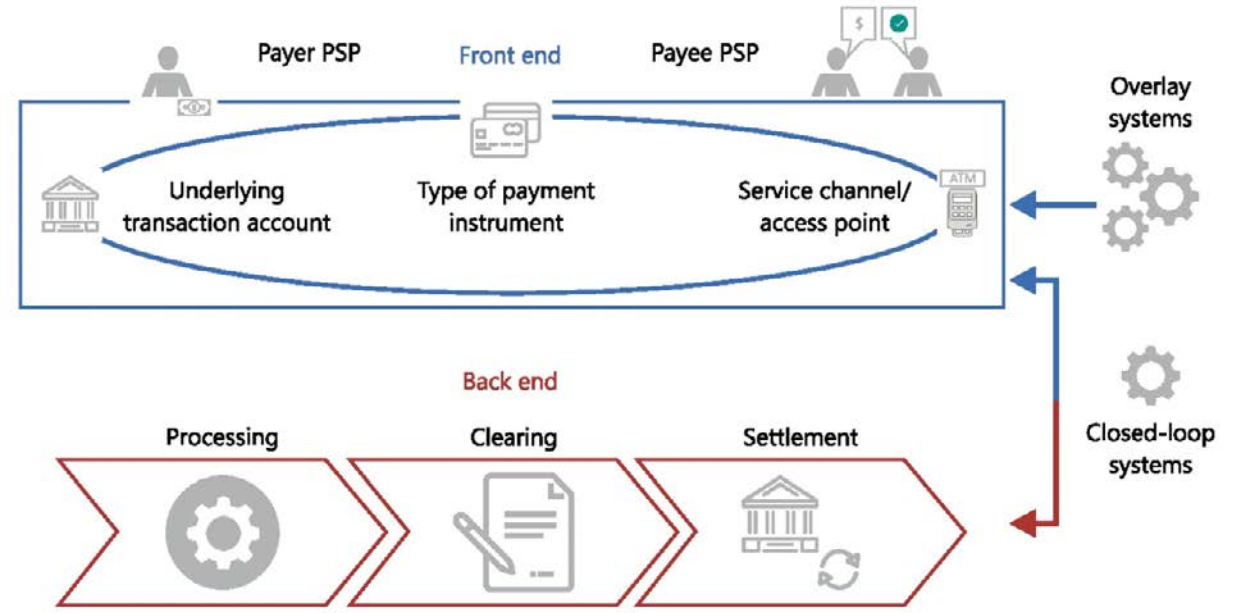
[17] This classification of payment instruments follows the methodology of the statistics on payments and financial market infrastructures in the CPMI countries (Red Book statistics). Other payment instruments may include country-specific payment instruments. This may also include payment instruments resulting from innovation (eg digital payment token transfers).

[18] Mobile money is a pay-as-you-go digital medium of exchange and store of value using mobile money accounts, facilitated by a network of mobile money agents. It is a financial service offered to its clients by a mobile network operator or another entity that partners with mobile network operators, independent of the traditional banking network. For more information, see the IMF's Financial Access Survey Guidelines and Manual (accessible at http://data.IMF.org/FAS).

[19] See Ehrentraud et al (2020).

[20] See Ehrentraud et al (2020).

Payments infrastructure elements and arrangements Chart 2



PSP = payment service provider (ie banks and non-banks).

Source: BIS, *Annual Economic Report*, Chapter 3, "Central banks and payments in the digital era", June 2020.

10. **There are two types of system, ie, overlay and standalone systems.** While overlay systems use existing payments instruments (eg traditional credit or debit cards stored in a digital wallet) and payment infrastructure to process, clear and settle payments, standalone systems are "closed-loop" payment systems that do not depend on existing payment infrastructure. Both types of system involve innovative customer interfaces at the front end.

Box 1

What is e-money?

E-money refers to debt-like instruments that an entity issues on receipt of funds for the purpose of facilitating payment transactions. More, specifically, from a:

- **balance sheet perspective, e-money is a fixed value claim on the balance sheet of the entity issuing it.** When a user exchanges fiat currency for e-money, she purchases a claim against an entity, which represents a liability on the issuing entity's balance sheet. That claim (ie the e-money the user receives) is (i) typically redeemable in fiat currency at a pre-established face value upon demand, which makes it similar to sight deposits held by banks; and (ii) denominated either in the same currency as the underlying balance sheet liability or in a fictitious unit of account that is tied to a sovereign currency.
- **risk perspective**, **e-money is a transaction device that offers stability of value through redemption guarantees provided by the issuer.** The guarantee of redeemability at face value is a promise by the e-money issuer to e-money holders. To avoid breaking this promise, an issuer needs to ensure that it holds enough assets that are sufficiently liquid to meet all redemption requests upon demand at all times.① Unless these assets are held as deposit at a central bank, which is possible or mandated only in few jurisdictions, they are subject to risks that could reduce their value.② By how much, though, depends on how e-money issuers choose or are required to invest or hold the assets that back up e-money claims.
- **user perspective, e-money is an attractive means of payment because of its convenience.** E-money is a digital alternative to cash that people like to use because it makes it easy to pay for goods or services or to transfer a payment to another user. As such, it can be seen as a form of purchasing power (monetary value) bought for future transactions. Before it can be used though, it needs to be purchased.③ Because users typically have the right to redeem their e-money at face value at all times, they may perceive e-money as functionally equivalent to fiat currency.
- **technical perspective, e-money is an electronic store of monetary value on a technical device.** There are two broad types.④ The first includes hardware-based products where the purchasing power resides in a personal physical device (eg chip card) and monetary values are typically transferred by means of device readers that do not need real-time network connectivity to a remote server; and software-based products where the purchasing power resides in a specialised software (eg e-wallets) and monetary values are transferred by using a personal device to connect to a remote server.④ The second are distributed ledger technology (DLT) applications that form the basis of digital representations of value that can be used as a means of payment.

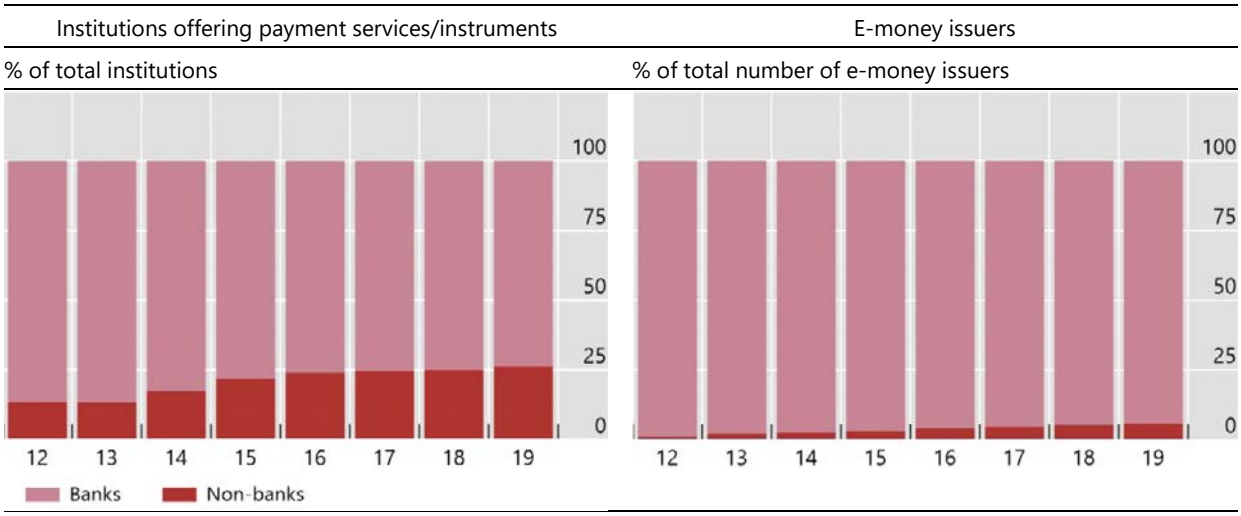
① Because customers expect at least to get their money back, e-money is subject to run risk similar to constant net asset value funds. The difference, however, is that an e-money issuer defaults if it is unable to redeem its outstanding e-money in full. In contrast, there is no similar obligation for money market funds. See Adrian and Mancini-Griffoli (2019a). ② The amount of assets available to satisfy e-money claims may fluctuate due to credit risk, liquidity risk and market risk. In addition, if the e-money issuer itself defaults, there is a risk that other creditors will attempt to seize all of an e-money issuer's assets, including those that back up e-money claims. ③ In this transaction, users relinquish ownership over one form of value (eg cash or deposits) in exchange for another form of value (ie e-money) (Bossone (2017)). ④ See www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html.

Broad categorisation of NBPSPs and the payment services they provide

11. **The payment system comprises a broad spectrum of PSPs.** Depending on the particular application, PSPs have different business models, operate at different stages of the payment chain and engage in various payment-related activities (CPMI (2014)). The main categories of institutions offering payment services/instruments are (1) central banks; (2) banks; and (3) non-banks.

12. **The NBPSP category comprises two overlapping subcategories.** They are (1) those offering storage of value in a payment account or on a device (for example non-bank (e-money) institutions and post office giro institutions) and (2) those not offering it themselves but relying on storage of value offered by others (eg merchant and ATM acquirers, payment initiation service providers[21] and account information service providers[22]) (CPMI (2017)). Across CPMI jurisdictions, non-banks represent more than a quarter of the institutions offering payment services or payment instruments (Chart 3, left-hand panel). At the same time, the share of non-bank e-money providers has increased by about 40% in the last three years. (Chart 3, right-hand panel).

Payment service providers — Chart 3



Source: CPMI Red Book.

13. **To explore the regulatory approaches for NBPSPs, this paper classifies them according to the front-end payment services they provide (see Table 1).** This builds on the categorisation in CPMI (2014), which classifies non-banks based on the stages of the payment chain in which they engage, the type of payment service provided and their relationship with banks. In particular, we focus on the front-end providers that provide services directly to end users such as consumers and businesses/corporates.[23]

[21] Payment initiation service providers are entities offering a service to initiate a payment at the request of the end user, accessing value stored on payment accounts held at another institution offering payment services.

[22] Account information service providers are entities offering a service to provide consolidated online information on one (or more) payment account(s) held by end users with one (or more) other entity or entities offering payment services.

[23] The other three categories are (i) back-end providers that typically provide services to banks; (ii) operators of retail payment infrastructures; and (iii) end-to-end providers that combine front-end services to end users with clearing and settlement services.

Classification of digital payment and e-money services Table 1

	Type	Definition	Selected examples
Accepting, managing or transferring value	Provision of transaction accounts	Transaction account held with NBPSPs that can be used for making and receiving payments.	Payment transaction accounts held with NBPSPs
	Provision of e-money transaction account	Account based on e-money that can be offered by banks and other authorised deposit-taking financial institutions, as well as by non-deposit-taking payment service providers such as e-money issuers. Such accounts include prepaid accounts.	Airwallex, Revolut, Wise
	Provision of electronic wallet services	Payment arrangements that enable end users to access, manage and use a variety of payment instruments issued by one or more PSPs via an application or a website.	Airwallex, PayPal, Wise
	Issuing of payment instruments	Means a payment service by a PSP contracting to provide a payer with a payment instrument to initiate and process the payer's payment transactions.	APS Payments
	Acquiring of payment transactions	Means a payment service provided by a PSP contracting with a payee to accept and process payment transactions, which results in a transfer of funds to the payee.	Stripe, WorldPay
	Money or value transfer services	Financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. No transaction account in the name of the payer or payee is opened for that purpose.	Western Union, Wise, WorldRemit
	Virtual asset services	Service to enable a digital representation of value to be digitally traded, or transferred for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies.	PayPal
	Processing of electronic funds/value transfer for third parties	Processing includes IT and network communication services, such as authentication and authorisation, which enable the payment service providers to conduct transfers of value. These can be direct debits, credit transfers, card payments and e-money transfers.	Ayden, Square, Stripe, Fiserv
Providing ancillary services	Payment initiation services	Service to initiate a payment order at the request of the payment service user with respect to a payment account held at another PSP.	Giropay, Sofort
	Account information services	Online service to provide consolidated information on one or more payment accounts held by the payment service user with either another PSP or with more than one PSP.	Intuit, Xero, Moneyhub

Source: CPMI publications and public sources.

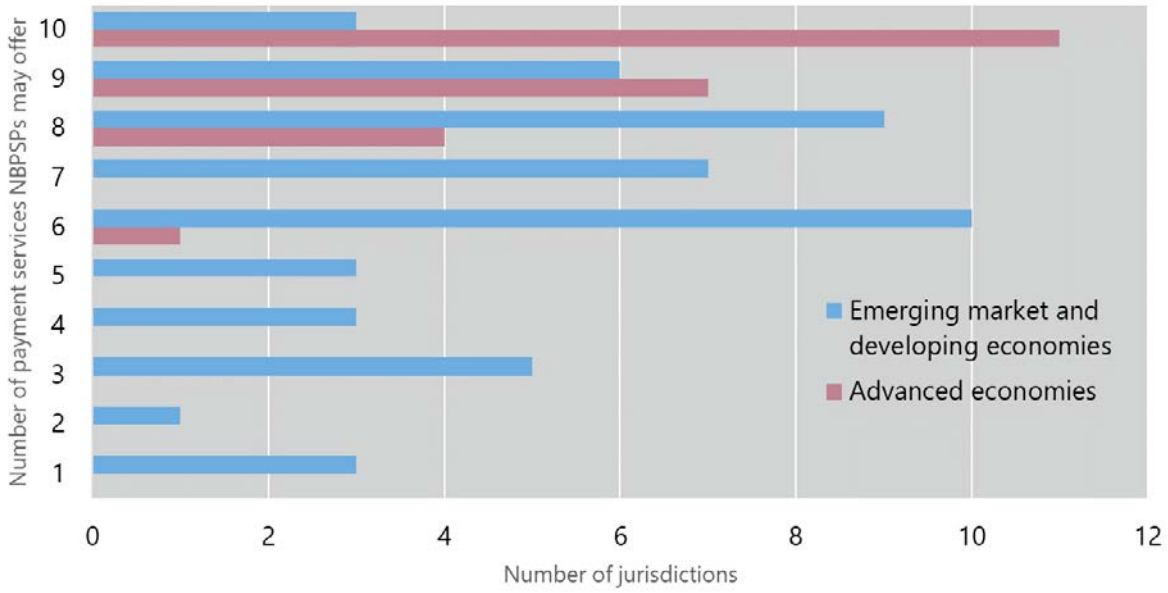
Section 3 – Regulation of digital payment and e-money services provided by non-banks

Overview of regulatory requirements

14. **This section provides an overview of regulatory requirements around the globe.** It is based on a CPMI survey conducted in early 2021. Of the 75 jurisdictions surveyed, 23 are AEs and 52 are EMDEs; and 27 are members of the CPMI.[24]

15. **Non-banks in most jurisdictions are able to offer at least some of the digital payment and e-money services defined in Section 2.** All 75 respondents except two indicated that non-banks are able to offer payment services in their jurisdictions. Respondents indicated a wide range in the number of payment services that non-banks can offer. In some jurisdictions – mostly AEs – non-banks can offer all types of service mentioned in Section 2, while in some EMDEs non-banks are only able to offer one type of service (in two cases, none). On average, non-banks in AEs are able to offer nine types of payment service while those in EMDEs can offer only six (Chart 4).

Number of services offered by type of jurisdiction — Chart 4



Source: Survey of central banks.

16. **Non-banks are able to offer "mature" or traditional payment services in most jurisdictions.** Provision of e-money accounts (ie e-money issuance) and processing of electronic funds for third parties are the most common payment services that non-banks are able to offer (Chart 5, left-hand panel). This is followed by the provision of e-wallet services, acquiring of payment transactions, and money transfer services. However, it is not as common for non-banks to be able to offer newer types of service. This is especially true for virtual asset services and, to a lesser extent, for payment initiation and account

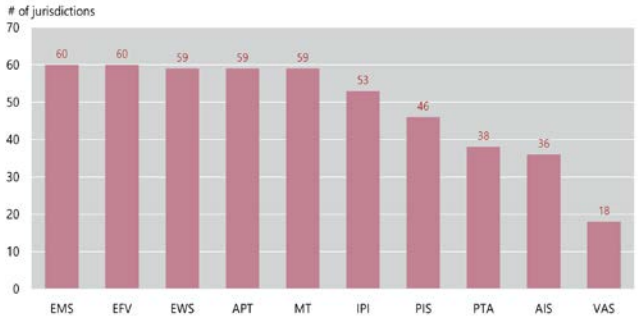
[24] The discussion in this section complements the World Bank Global Payments Systems Survey report published in 2020, which provides a comprehensive overview of regulation of payment systems globally.

information services. It is also not as common for non-banks to be able to provide transaction accounts (other than e-money) given that these accounts are generally considered to be deposit accounts and thus reserved as a banking service.

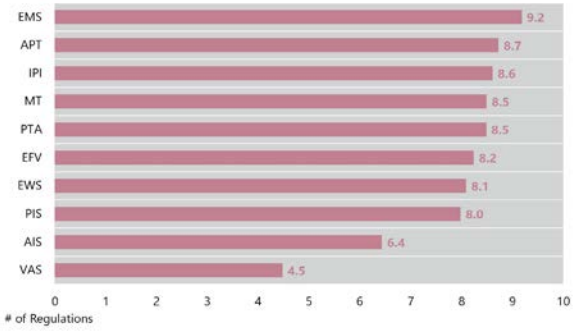
17. **E-money issuance is subject to the most intensive regulation, and the provision of virtual asset services to the least.** The survey asked whether payment services offered by non-banks are subject to regulatory and other oversight requirements. Thirteen types of requirement were included in the survey: licensing; registration; capital requirements; security deposits at central banks; ownership restrictions; mandatory partnerships with banks; safeguarding of customer funds; risk management; cyber security; anti-money laundering (AML); consumer protection; data protection; and interoperability. On average, jurisdictions where non-banks can offer e-money issuance impose nine types of requirement on this service. In the case of virtual asset services, jurisdictions where non-banks can offer such services impose only around four types of requirement on average (Chart 5, right-hand panel).

Payment services offered by NBPSPs — Chart 5

Payment services offered by NBPSPs across surveyed jurisdictions



Average number of regulations on payment services offered by NBPSPs



EFV: Processing of electronic funds/value transfer for third parties (eg direct debits, credit transfers, card payments and e-money transfers), EMS: Provision of e-money accounts and services, EWS: Provision of electronic wallet services, APT: Acquiring of payment transactions, MT: Money or value transfer services, IPI: Issuing of payment instruments, PIS: Payment initiation services, PTA: Provision of transaction accounts (other than e-money accounts), AIS: Account information services, VAS: Virtual asset services.

Source: Survey of central banks.

18. **On average, NBPSPs in EMDEs are more intensively regulated than those in AEs.** Across all payment services included in the survey, the difference in the average number of regulatory requirements imposed on NBPSPs in EMDEs and AEs is insignificant (8 vs 7.6). However, there is a particularly marked difference in the following payment services: (1) acquiring payment transactions (9.1 vs 8); (2) e-wallet services (8.5 vs 7.4); and (3) e-money issuance (9.5 vs 8.6). Only in virtual asset services and provision of transaction accounts do NBPSPs in AEs face more regulation than those in EMDEs (4.9 vs 3.9 and 8.6 vs 8, respectively). In general, mandatory partnerships with banks, minimum capital, security deposits at the central or a commercial bank, and interoperability are the regulatory requirements that NBPSPs are more commonly subject to in EMDEs than in AEs, while the reverse is true when it comes to consumer protection. This could be a reflection of the early stage of development of regulatory framework for NBPSPs in EMDEs, where there might be tendency to apply the regulations intended for banks.

19. **Among the different types of regulatory requirement included in the survey, AML/CFT requirements are the most common across payment services and jurisdictions,**[25] **while**

[25] This is consistent with the 2020 World Bank Global Payments Systems Survey report, which also covered NBPSPs, particularly supervised non-bank financial institutions, money transfer operators and non-bank e-money issuers.

interoperability is the least common (Table 2). On average, about 87% of jurisdictions impose AML/CFT requirements on non-banks providing payment services. In one jurisdiction, for example, non-banks are basically free to offer any payment service and must comply only with AML/CFT requirements. Even the provision of virtual asset services, which is typically subject to very few regulatory requirements, is subject to AML/CFT requirements in most of the jurisdictions where non-banks can offer such services.[26] Other common requirements are those relating to risk management and data protection. Authorisation requirements (ie licensing and/or registration) are also common but their application varies (see below). Meanwhile, only about a fifth of jurisdictions impose interoperability requirements on non-banks providing payment services.

20. **Regulatory requirements for payment services provided by non-banks may be applied in either a differentiated or a uniform manner.** Some requirements, while imposed across payment services, may be applied differently. This is the case for licensing/registration requirements; minimum capital; safeguarding funds and other security requirements; and interoperability. Other requirements are in general uniformly applied across payment services, such as those relating to AML/CFT; risk management and cyber security; data protection; and consumer protection. The discussions that follow, which are based on a desktop review of published documents, are organised along these two types of regulatory requirement.

Share of surveyed jurisdictions with regulations for non-bank payment services (%)*

Table 2

Regulation**	EFV	EMS	EWS	APT	MT	IPI	PIS	PTA	AIS	VAS	AVG
AML	88	97	88	92	93	91	85	92	64	78	**87**
CAP	79	92	76	83	85	85	81	87	28	30	**73**
CP	76	88	79	86	77	83	79	82	77	35	**76**
CYB	81	83	74	88	79	83	85	77	79	39	**77**
DP	81	85	76	90	82	83	85	79	79	48	**79**
INT	24	30	21	27	16	26	23	21	10	0	**20**
LIC	83	92	78	81	84	81	75	85	51	26	**74**
OWN	36	40	31	41	41	43	38	44	21	17	**35**
PAR	31	28	29	25	34	28	23	21	10	4	**23**
REG	45	53	52	51	51	43	46	44	67	57	**51**
RISK	83	87	78	88	87	85	83	85	77	39	**79**
SAFE	66	90	71	73	74	78	42	79	26	22	**62**
SEC	36	40	38	31	31	31	23	31	18	17	**30**

*EFV: Processing of electronic funds/value transfer for third parties (eg direct debits, credit transfers, card payments and e-money transfers), EMS: Provision of e-money accounts and services, EWS: Provision of electronic wallet services, APT: Acquiring of payment transactions, MT: Money or value transfer services, IPI: Issuing of payment instruments, PIS: Payment initiation services, PTA: Provision of transaction accounts (other than e-money accounts), AIS: Account information services, VAS: Virtual asset services.

**AML: Anti-money laundering rules, CAP: Minimum capital requirements, CP: Consumer protection, CYB: Information and cyber security, DP: Data protection, INT: Interoperability requirements, LIC: Licensing requirements, OWN: Ownership restrictions, PAR: Mandatory partnerships with banks, REG: Registration requirements, RISK: Risk management, SAFE: Safeguarding of funds, SEC: Security deposit with the central bank, government authority, or commercial bank.

[26] This could be attributed to the Financial Action Task Force (FATF) finalising changes to its Standards in June 2019. These clearly apply anti-money laundering and countering the financing of terrorism obligations to virtual assets (VAs) and virtual asset service providers (VASPs). In March 2021, the FATF issued a consultation updating its Guidance on the risk-based approach to VAs and VASPs.

Regulatory requirements with differentiated application

Authorisation – licensing/registration

21. **Some jurisdictions have general licensing frameworks for all, or at least multiple, payment services.** For example, Brazil has a general "Payment Institution'" licence.[27] The EU's Second Payment Services Directive (PSD2) also provides a general licence for the different types of payment service that are defined therein.[28] E-money issuance, however, is subject to different licensing requirements under the Electronic Money Directive 2. Turkey's licensing frameworks as well as those in the United Kingdom are similar to those of the EU. Indonesia issues one type of licence for "Payment System Service Providers", which encompasses a variety of payment system functions or services. However, non-banks that offer pre-paid payment instruments and e-money issuance require different licences.

22. **Jurisdictions may also have different licences depending on the size or type of service provided.** For example, Japan's regulatory framework categorises Funds Transfer Service Providers (FTSPs) into three segments, depending on the maximum transaction value they can execute. Authorisation is required for FTSPs that are not subject to any maximum transaction value limit, while registration is required for FTSPs subject to a limit of JPY 1 million (~$9,300) and JPY 50,000 (~$465) per transaction. Singapore, on the other hand, has three licences for non-bank payment service providers: Standard Payment Institutions (SPIs), Major Payment Institutions (MPIs), and money-changing. SPIs are subject to specific thresholds based on the number/type of services offered.[29] MPIs are not subject to any volume restrictions but are subject to more stringent regulation and supervision. Money-changing licencees, meanwhile, can provide only the service of buying and/or selling foreign currency in Singapore.

23. **Jurisdictions may also have different licensing requirements depending on the geographic areas covered by the service.** In China, licensing requirements vary slightly depending on the geographic coverage of the business (ie whether nationwide or limited to a single province). Geographic heterogeneity for licensing requirements is best illustrated in the United States, where all money transmitter licensing is done entirely at the state level.[30] While both the federal government and consortiums of state regulators have made efforts to harmonise money transmitter licensing requirements, there is no unifying framework as yet (Box 2).

24. **Almost all jurisdictions where non-banks may issue e-money require licensing and/or registration, and there are specific licensing models for this purpose.** In some jurisdictions, only banks are allowed to issue e-money (eg South Africa). This is because e-money issuance and the acceptance of cash in return may be legally interpreted as a deposit-taking activity in these jurisdictions. Two types of

[27] The licensing regime in Brazil is dual, ie it requires the authorisation of payment schemes' rulebooks (assessment of access criteria, risk management etc) and payment institutions (non-financial payments service providers). Payment scheme licensing is required for schemes with yearly volumes that exceeds BRL 20 billion or 100 million transactions. There are some exemptions: (1) schemes related to social benefits (eg meal vouchers); (2) schemes with a "limited scope" (eg restricted to buying digital contents – music, apps etc). Payment institutions must be authorised, except for acquirers and post-paid payment instrument issuers (eg credit card issuers) with yearly volumes not exceeding BRL 500 million. Furthermore, payment institutions that participate exclusively in exempted payment schemes are also exempted from licensing.

[28] PSD2 does not apply to payment instruments that are used in a limited capacity, such as those used (1) to acquire a very limited range of goods and services; (2) to acquire goods or services within a limited network of service providers; or (3) exclusively in one member state for specific social or tax purposes to acquire specific goods or services. Additionally, payment transactions conducted by providers of electronic communications networks that involve the purchase of digital content, voice-based services, tickets, as well as charitable donations are all excluded so long as the value of a single transaction does not exceed EUR 50 (~$61) and the monthly total for an individual subscriber does not exceed EUR 300 (~$366).

[29] S$3 million (~$2.27 million) in monthly transaction volume for any single payment service; S$6 million (~$4.54 million) in monthly transaction volume for two or more payment services; S$5 million (~$3.78 million) of daily outstanding e-money.

[30] Only one state – Montana – has no licensing requirement in place.

licensing model are used in jurisdictions that allow non-banks to issue e-money: the narrow bank model and the non-bank model.

Box 2

Money Transmitter Licensing in the United States

Providers of digital payment services in the United States usually hold licences as Money Transmitters (MTs), which are classified by the Financial Crimes Enforcement Network (FinCEN) as a specific type of money service business (MSB). Registration must take place with the designated agency in *each* state that the money transmitter is active in. Licensing occurs at the state level and allows providers to conduct a single type of business. Thus, a money transmitter that is active in 38 states would then need to register with 38 state-level authorities (the New York Department of Financial Services (NYDFS) also has a "Bitlicense" for out-of-state entities that engage in virtual currency business activity involving New York State or any person that resides, is located, has a place of business, or is conducting business in New York State; however, this does not replace any other licences required under New York law, eg money transmitter licence). As a type of MSB, money transmitters are required to register with FinCEN 180 days after being established, and these registrations must be renewed every two years. They must also comply with federal AML/CFT and consumer protection regulations issued by FinCEN and the Consumer Financial Protection Bureau (CFPB), respectively.

In an effort to harmonise licensing requirements, the Conference of State Bank Supervisors (CSBS), an association of state financial regulators and supervisors, developed the Nationwide Multistate Licensing System (NMLS) in 2008. This "one-stop shop" system allows MSBs with operations in different states to apply, amend, update or renew their licences for different states via a single set of uniform applications. Currently, 28 states are using the NMLS to offer multistate money transmitter licences via its Multistate MSB Licensing Agreement Program.

The Office of the Comptroller of the Currency (OCC) attempted in 2018 to reduce the barrier to entry by creating Special Purpose National Bank Charters for fintech firms, allowing them to circumvent the complex state-by-state licensing method. More technically, it would allow them to operate as "special purpose national banks (SPNBs)". Fintech firms that become SPNBs would still be subject to the same level of federal oversight that national banks are subject to, but would not be allowed to take deposits. They could, however, lend money and pay checks. Additionally, all companies seeking an SPNB charter would need to make a commitment to financial inclusion and present and adhere to a quasi-resolution plan that could require them to sell, wind-down, or merge with non-bank affiliates.

State banking regulators, such as the NYDFS, as well as the Conference of State Bank Supervisors (CSBS) challenged the legality of these new charters, stating that the federal government was illegally pre-empting state regulation. The CSBS lawsuit was eventually dismissed. However, the CSBS recently filed a second complaint about the application of Figure Technologies, Inc for an SPNB charter. Figure's main goal in applying was to reduce the complexity of its businesses, stemming from the over 200 licences the company would have in the absence of a single national charter. The NYDFS lawsuit, on the other hand, is still ongoing. While the future of the OCC's SPNB charter remains uncertain, the OCC granted a full service national bank charter to fintech startup Varo Money in July 2020. Meanwhile, recent OCC interpretive letters allowing national banks to provide cryptocurrency custody services (Interpretive Letter #1170, July 2020), hold deposits that serve as reserves for certain stablecoins (Interpretive Letter #1172, October 2020), and use independent node verification networks and stablecoins to engage in and facilitate payment activities (Interpretive Letter #1174, January 2021), have driven some non-banks to obtain a national bank/trust charter.

Fintechs have even explored the possibility of becoming Industrial Loan Companies (ILCs), as this would allow them to take deposits and obtain FDIC insurance. ILCs are required to hold significantly higher capital levels than banks, and their parent companies (which are non-banks) must be able to act as "sources of strength" for the depositories. However, until recently, the FDIC had not approved any ILC charters for years. From 2013 to 2019, there were no new ILC charters approved despite six large companies applying for them. The FDIC denied all of them. Three of these companies refiled, and two – Square and Nelnet – obtained approval in March 2020.

On the same day that Square and Nelnet received their approvals, the FDIC issued a proposed rule that would provide further regulation to the parent companies of ILCs, which was eventually finalised after comment in December 2020. Due to the unique risk profile of these new ILCs, the new rule requires parent companies of ILCs that are not supervised by the Federal Reserve to be subject to additional requirements, such as more restrictive corporate governance procedures; FDIC examination of the parent and all subsidiaries; filing of annual reports on the parent's

operational and financial risks and risk management techniques; annual audits of all ILC subsidiaries; maintaining capital and liquidity levels set by the FDIC; and recovery and wind-down plans for the ILC if needed.

25. **Under the narrow bank model, non-banks can apply for a limited banking licence (eg payment bank licence) that allows them to offer a limited set of banking services.** Payment bank licences are available under the Indian and Mexican legal frameworks, as well as in Switzerland in a slightly different format (fintech licence). Even though payment banks are not able to provide the full range of banking services (eg lending is prohibited), the fact that they are banks means that they are able to issue deposits covered by deposit insurance and offer interest-bearing products, something typically unavailable for their non-bank counterparts. Payment banks, however, are regulated under the banking law and therefore subject to stricter rules than traditional e-money issuers (EMIs) since they have to comply with most of the prudential requirements applicable to traditional banks (eg capital, liquidity and leverage ratio). In practice, payment bank licences remain underused in the countries where they are available, which may be related to the regulatory burden that comes with having a banking status.[31]

26. **The non-bank model allows specific types of non-bank institution to issue e-money (eg e-money institutions, prepaid instrument issuers or stored value issuers).** Jurisdictions whose framework allows such institutions include Brazil, China, the European Union, Russia, Singapore, the United Kingdom and the United States. This is also a common approach in jurisdictions that want to foster financial inclusion. According to the Bill and Melinda Gates Foundation (BMGF) 2019 Digital Financial Services Regulation and Supervision Reference Guide, this is the case in Colombia, Ghana, Kenya, Malaysia, Myanmar, Peru, Rwanda, Sri Lanka and Tanzania. In these jurisdictions, mobile network operators (MNOs) leverage their existing telecommunications channels, extensive customer bases and strength in marketing and branding digital products in venturing into e-money issuance. MNOs are typically required to establish a special purpose vehicle for providing this service.[32]

Minimum capital

27. **Most jurisdictions have initial and ongoing capital requirements for non-banks that provide payment services.** Initial capital requirements are typically flat but may vary depending on the payment volume allowed under the licence. This is the case for SPIs in Singapore, which have a capital requirement of only S$100,000 (~$75,700), as compared with the S$250,000 (~$189,250) required for MPIs. Some jurisdictions adjust the initial capital requirements based on changes in payment volume and the adjusted value constitutes the ongoing capital requirement. These adjustments are generally calculated by taking a percentage (around 1–2%) of payment volume over a specified horizon and adding it to the initial capital requirement. These percentages may be part of a sliding scale with different surcharges based on the marginal increase in payment volume – as is the case in the EU, Turkey, and the United Kingdom – or just a flat percentage of rolling transaction volume, such as in Brazil.

28. **Some jurisdictions have capital requirements that are contingent on the location of the NBPSP or the type of payment service provided.** For US money transmitters, initial and ongoing capital requirements vary heavily across states and must be complied with if a money transmitter wishes to add out-of-state locations. In China, capital requirements are significantly lower – RMB 30 million (~$4.7 million) versus 100 million (~$15.7 million) – if the payments provider operates exclusively within one province. The EU requires only EUR 20,000 (~$24,450) for remittance services and EUR 50,000 (~$61,120) for payment initiation services, compared with EUR 125,000 (~$152,820) for all other payment services (except account information services).[33]

31 Dias and Staschen (2019).

32 See BMGF (2019).

33 See Article 7 of PSD2.

29. **For non-banks that issue e-money, ongoing capital requirements are typically set as a percentage of the e-money float.** These are usually around 2–5% of the e-money float. Colombia, the EU, Peru, and Saudi Arabia all have requirements of 2%, whereas Australia's requirement is 5%. In the EU and the United Kingdom, capital requirements may increase if the e-money issuer provides other services, such as granting credit (see also Box 3 for a discussion of permissible activities by e-money issuers).

Box 3

Permissible activities for e-money issuers

E-money issuers are subject to specific requirements regulating the type of activities and services they are allowed, obligated or prohibited to conduct or provide.

Redeemability of e-money

In most countries, e-money issuers have an obligation to redeem the e-money received at par value. In a few jurisdictions, however, certain types of e-money issuer are not allowed to redeem e-money. For example, in Hong Kong SAR, India and Turkey, whether there is an obligation to redeem depends on the type of provider and/or product. In Singapore, e-money issuers are prohibited from withdrawing e-money in the form of physical Singapore currency (ie notes and coins) but they can allow users to redeem the e-money at par value by other means, eg by transferring the par value to the user's bank account. In Japan, issuers of prepaid payment instruments are prohibited from redeeming e-money whereas Funds Transfer Service Providers are not.

Payment of interest

The payment of interest on the float to e-money holders is prohibited in most countries. This prohibition aims at helping consumers distinguish between e-money and bank deposits, as only the latter are covered by deposit insurance in these countries. In India and Mexico, only payment banks are allowed to pay interest on e-money.

Provision of other payment services

The provision of other payment services is often included in the e-money licence. In some countries such as Singapore, the e-money issuer has to apply to include other applicable payment services in its payments licence to be entitled to provide those payment services in addition to issuing e-money.

Provision of loans

In some countries, e-money issuers are allowed to provide loans or grant credit, often under certain conditions. These loans often have to be connected to their e-money activities (eg overdraft facility in the context of an e-money transaction) and are subject to certain conditions in terms of amount, maturity etc. E-money issuers typically have to hold additional capital when providing these services.

Certain countries prohibit the provision of loans by e-money issuers and non-banks in general (Brazil, China, Russia, Saudi Arabia and Turkey). In India and the United States it depends on the type of issuer, its licence and the product in question.

Safeguarding of funds and other security requirements

30. **Safeguarding of funds is a very common requirement for non-banks offering payment services that involve handling such funds.** It is required in almost all jurisdictions where non-banks are able to issue e-money, and in the majority of jurisdictions where non-banks are able to provide transaction accounts. In both types of service, safeguarding requirements aim to ensure that e-money holders can redeem their e-money at face value if and when they need it. There are various methods for safeguarding funds observed in different jurisdictions. These include deposits in the form of cash or government securities at the central bank or commercial banks; a bank guarantee; setting aside unencumbered assets;

segregating and ring-fencing funds; and any other form that authorities may require. Given that this requirement is more prevalent for e-money issuance, the discussion that follows focuses on this service.

31. **Methods to safeguard assets that back e-money claims (reserve assets) are meant to protect customers from the risk that EMIs may not have sufficient funds to repay them or the risk of EMI insolvency.** Typically, reserve assets are segregated and ring-fenced from EMIs' own funds.[34] Reserve assets need to be deposited in a commercial bank or the central bank or invested in high-quality liquid assets. These deposits or investments may be in the form of a trust, fiduciary or escrow account with EMI customers as the beneficiaries. Thus the funds cannot be used to satisfy claims by EMI creditors (other than e-money holders) in the event of its insolvency. In other jurisdictions, segregation and ring-fencing are not mandated and instead EMIs are required to acquire protection in the form of insurance or a guarantee. Some jurisdictions combine or allow EMIs to choose any of the safeguarding methods (eg the EU), while others allow only one method.

32. **"Residual" risks may still arise even with the use of safeguarding methods, but these risks are mitigated by deposit insurance in some jurisdictions.** Safeguarding measures may be subject to legal challenges or there may be unanticipated operational issues that could impede access to or transfer of reserve assets in the event of insolvency of the EMI or the bank holding the funds. One way of mitigating such risks is to extend the scope of deposit insurance to cover e-money.[35] The effectiveness of such an approach would be dependent on the design of the deposit insurance framework of individual countries (ie sufficiency of funds, speed of payout etc). This could be done through either a direct or a pass-through approach.

- **Direct approach:** EMIs are members of the deposit insurance scheme and e-money they issued is included in the definition of "deposits". It is therefore covered by deposit insurance in the event of an EMI's insolvency. This is the case for e-money issued by payment banks in India and Mexico.
- **Pass-through approach:** E-money float accounts held in a bank are treated as deposit liabilities. Deposit insurance coverage is "passed through" to each individual e-money customer in the event of insolvency of a bank holding the float. This approach is applied in the United States for certain types of e-money account.[36] The European Commission has recently issued a consultation asking respondents whether a similar approach should be adopted in Europe.[37]

Interoperability

33. **Interoperability[38] is the least common regulatory requirement, but its application also varies across payment services.** For example, it is required in a noticeably smaller number of jurisdictions for account information services and money transfer services, and it is not required at all for virtual asset services. Brazil and Singapore are examples of jurisdictions that require interoperability or have the power to do so for at least some payment services. Brazil requires it for e-money issuance, acquiring of payment transactions and payment initiation services. In Singapore, the Payment Services Act reserves the right for the MAS to mandate that payment service providers (including e-money institutions) to adopt "any common standard" to ensure interoperability.

[34] Typically, safeguarding requirements apply to 100% of the float.

[35] See Izaguirre et al (2019).

[36] FDIC (2008).

[37] EC (2021).

[38] The CPMI defines interoperability as the technical or legal compatibility that enables a system or mechanism to be used in conjunction with other systems or mechanisms. This allows participants in different systems to conduct, clear and settle payments or financial transactions across systems without participating in multiple systems.

34. **However, there are soft requirements or ongoing plans to achieve interoperability in other jurisdictions.** Indonesia, where QR codes have been heavily adopted as a method of payment, has created national frameworks for QR code interoperability. Similarly, China is promoting the establishment of industry-level QR code payment interoperability. The EU recently adopted a new retail payments strategy, explicitly desiring that future retail payments systems will be "pan-European" and interoperable.[39] The United Kingdom published its New Payments Architecture (NPA) blueprint in 2017. One of the key design principles mentioned in the blueprint was "end-to-end" interoperability. In Japan, a consortium of private institutions led by the five major Japanese banks set up a commission to explore ways to make small-amount digital payments infrastructure more interoperable.[40] These initiatives are meant to increase efficiency and enhance competition in the payments markets. Other initiatives that aim to enhance competition involve granting NBPSPs access to the payment systems and accounts at central banks. Box 4 provides examples of these initiatives in a few jurisdictions.

Box 4

Non-bank payment service provider access to central bank systems

Most jurisdictions do not allow NBPSPs to access services provided by or accounts at their central banks. Access to these services is governed by a number of regulatory requirements (eg minimum capital and liquidity requirements) and involves compliance with technical standards, which are meant to ensure the safety and efficiency of the payment infrastructure and the markets it serves. Satisfying these requirements and standards can be challenging for NBPSPs, which may not have the same resources as banks. This forces these companies to either partner with banks to access these services or to forgo them entirely and use separate ones, potentially forcing non-banks to charge higher fees and be at a competitive disadvantage relative to banks for payments purposes.

The United Kingdom and Hong Kong SAR are examples of jurisdictions that have granted non-banks direct access to central bank payment systems. In the United Kingdom, the Bank of England, working with the Financial Conduct Authority, established a framework to allow NBPSPs to apply for and open a settlement account at the Bank, in order to directly access payment systems. Wise (formerly Transferwise) became the first NBPSP to gain direct access to the BoE's systems in April 2018. In Hong Kong SAR, Alipay and WeChat are two of the 11 NBPSPs that have also obtained access to the HKMA's Faster Payment System. Additionally, the Monetary Authority of Singapore also allowed non-bank access to the FAST and PayNow retail payments systems, which are owned and operated commercially, in November 2020. These jurisdictions all emphasised the importance of competition, innovation and generally levelling the playing field between incumbent providers and new ones. Of these three jurisdictions, only the United Kingdom explicitly prohibits non-banks from accessing intraday credit, as they do not perform maturity transformation activities.

This approach contrasts with Australia's decision to not allow direct access to its New Payments Platform, which launched in early 2018 – shortly after the United Kingdom's decision. Access to the NPP requires the approval of incumbent firms, all of which are banks, which prompted some concern by government competition authorities on the availability of the NPP for non-banks and "specialist" payment providers. NPP Australia, which runs the platform, responded by pointing out that indirect access (IE - through banks) still offers plenty of opportunity for non-banks, but requires "rigorous standards to safeguard the platform". As of October 2020, over 100 institutions have connected to the NPP, but only 11 are directly connected. However, non-banks can connect directly as senders of "non-value" messages, such as payment initiation messages or as an end users. Finally, NPP Australia pointed out that the United Kingdom's classification of NBPSPs differs from Australia's to the extent that those that are allowed to open central bank accounts "[do] not have a close equivalent in Australia". Different classification frameworks may make it difficult to compare NBPSPs' access to central bank systems or accounts across jurisdictions.

[39] See EC (2020a).

[40] See announcement by the Task Force for the Next-Generation Payment Systems: www.zengin-net.jp/en/announcement/pdf/announcement_20210330Report.pdf.

Regulatory requirements with uniform application

AML/CFT

35. **As noted above, AML/CFT requirements are the most common type of requirement across payment services and jurisdictions.** AML/CFT requirements are fairly standardised and are meant to mitigate specific money laundering (ML) and terrorist financing (TF) typologies found in payment services. These requirements include, among others, implementation of broad know-your-customer (KYC) and customer due diligence (CDD) standards, as well as documentation and reporting of suspicious transactions. Some jurisdictions such as India, the Philippines and Russia apply a "tiered" approach to KYC and CDD, in which low transaction or balance limits result in reduced KYC/CDD requirements.[41] In a few cases, jurisdictions may exempt from AML requirements payment services that are considered to have low ML/TF risk. For example, Singapore adopted a risk-based approach and exempted certain low ML/TF risk products from AML/CFT requirements, while applying more stringent AML/CFT requirements for higher-risk areas. Furthermore, jurisdictions have requirements in place that aim to increase transparency in money transfers. Following the FATF recommendation 16, countries require information on payers and payees of transactions for the purposes of preventing, detecting and investigating ML/TF incidents. The amount and type of information required depends on whether the transactions are national or international. In the EU, for example, this requirement is implemented in Regulation 2015/847.[42]

36. **Compliance with AML/CFT requirements is quite important for NBPSPs to avoid "de-risking".** NBPSPs are often seen as having higher ML/TF risks because they are not subject to the same level of supervision as banks. This could lead banks, which are needed by non-bank payment service providers to facilitate transactions, to refuse to partner with them. More recently the EBA issued a statement clarifying that compliance with AML/CFT requirements "does not require financial institutions to refuse or terminate, business relationships with entire categories of customers that they consider a higher ML/TF risk".[43]

Risk management and cyber security

37. **Risk management, including internal controls, requirements are largely uniform across payment services provided by non-banks.** These usually relate to ensuring operational resilience at the legal entity level (ie the entity providing the payment service) and regulatory compliance is often assessed during on-site inspections. This is also true for NBPSPs that are part of big tech groups, even if operational incidents that could arise from their non-financial services might generate systemic disruptions.[44] These requirements also cover outsourcing or third-party dependencies, which puts the ultimate responsibility of monitoring and assessing the risks of such third parties on NBPSPs. They have to ensure that the third parties they deal with have risk management policies, procedures and controls that are at least as stringent as those required for regulated firms. China, however, does not allow outsourcing or third-party partnerships, particularly for "core payment services".

38. **Information security and cyber security requirements for NBPSPs are quite common across jurisdictions.** NBPSPs are required to develop cyber security policies commensurate with their business characteristics, size, risk profile, nature of transactions, sensitivity of underlying data, and other factors. The criteria for such assessments may be included in broad operational resilience frameworks, such as in

41 BMGF (2019).

42 See https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0847&from=EN.

43 See www.eba.europa.eu/eba-takes-steps-address-%E2%80%98de-risking%E2%80%99-practices.

44 Restoy (2021).

Brazil, or through specific "cyber hygiene" requirements, such as in Singapore. Compliance with these requirements is assessed through a combination of regular reporting and on-site inspections. In addition to the aforementioned cyber hygiene requirements, Singapore requires a "penetration test" for any applicant intending to provide online payment services. In the United States, all money transmitters are subject to federal cyber resilience requirements, though individual states are allowed to implement more rigorous rules.[45]

Data protection

39. **Data protection laws usually cover a broad range of institutions, including NBPSPs.** These laws generally define "consent" standards to process data or transfer data, outline the rights of data subjects and explicitly define personal data (and in some cases "sensitive" data). The EU, for example, has the General Data Protection Regulation (GDPR), which broadly applies to all organisations that do business in the EU including those based in other countries. Turkey's Data Protection Law (DPL) mandates consent to process data, the right to delete all data and other consumer data privacy rights. The DPL also requires data controllers to register with the Personal Data Protection Board (DPB) and provide it with their data processing inventory, personal data retention policy, and personal data destruction policy. In February 2020, China updated its standards on the protection of personal financial information (PFI). The updated standards include a right to view and delete PFI and apply not just to licensed financial institutions, but to any institution processing PFI.

40. **Data protection laws may also cover cross-border transfers of data.** South Africa's Protection of Personal Information Act (POPIA), which was passed in 2013 but entered into force in July 2020, has extensive cross-border data transfer requirements.[46] Japan's Act on the Protection of Personal Information (APPI) was amended in June 2020 to enhance provision of information to individuals whose data are subject to cross-border transfers. Other jurisdictions may require approval for the cross-border transfer of very sensitive data (GDPR and Turkey). Moreover, both POPIA and APPI include reporting requirements for data breaches.

Consumer protection

41. **Some jurisdictions have dedicated consumer protection requirements for NBPSPs.** In addition to general consumer protection laws, those jurisdictions have consumer protection rules that are specific to the financial sector (eg South Africa) or specific even to payment services following an activity-based approach (eg China, the EU, Indonesia, Japan, Singapore and the United Kingdom). Consumer protection requirements in the payment space mainly focus on transparency and disclosure of certain information, such as fees, as well as handling of complaints and prevention of fraud.

42. **Disclosure of transaction fees is an important theme in consumer protection requirements for money transfers.** Jurisdictions generally require service providers to disclose in advance the total amount of fees charged for a transaction (general fee and exchange rate margin). The EU's Cross-Border Payments Regulation 2 (CBPR2), for example, sets rules on the cost of cross-border payments and on the transparency of currency conversion charges within the EU. It applies to national and cross-border payments that are denominated either in euros or in a national currency of a Member State other than the

[45] This has been done in seven US states, with more legislation pending. The most notable of these is the regulation passed in New York, which requires financial services institutions in the state to submit detailed cyber security plans, designate Chief Information Security Officers, and maintain rigorous reporting standards.

[46] This prompted some large companies, such as Amazon and Microsoft, to create local data centres to more easily deal with these requirements.

euro and that involve a currency conversion service.[47] The issue of transaction costs is especially important in the case of remittances, where fees can account for up to half of the amount sent by migrant workers to their country of origin.[48] The issue's importance is highlighted in the United Nations' 2030 Agenda for Sustainable Development, where reducing the transaction costs for migrant remittances to less than 3% and eliminating remittance corridors with costs higher than 5% are included as specific targets.[49]

Section 4 – Innovation and the emerging regulatory response

From cryptoassets to stablecoins

43. **Novel technologies are creating the potential for new means of payments to emerge.** The advent of distributed ledger technology (DLT) and blockchain paved the way for Bitcoin, which was the first cryptoasset introduced in 2009.[50] A wide range of others have followed since then. While there are currently about 4,200 privately issued cryptoassets available, Bitcoin continues to dominate the crypto market with roughly 60% in terms of market value (Citi GPS (2021)).

44. **Since its introduction, doubts have emerged over Bitcoin's suitability as a means of payment.** In his 2008 white paper, Satoshi Nakamoto envisaged Bitcoin as a "system for electronic transactions without relying on trust". He further described Bitcoin as a "purely peer-to-peer version of electronic cash [which] would allow online payments to be sent directly from one party to another without going through a financial institution".[51] Yet in practice, experience accumulated over the years suggests that Bitcoin is more of a speculative asset than a means of payment or even a store of value.[52]

45. **On a general level, cryptoassets suffer from several shortcomings that hamper their usage as an everyday means of payment.** While the market capitalisation of cryptoassets has kept growing over the years, it has become increasingly clear that their high price volatility, restricted scalability, limited throughput of transactions, and lack of payment finality make them ill-suited as an efficient payment means.[53] In addition, there is an ongoing debate around the significant carbon footprint of crypto-mining

47 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0518&from=EN.

48 One entry even records a total fee of 75% of the amount sent. Source: Remittance Prices Worldwide, World Bank. See https://remittanceprices.worldbank.org/en.

49 https://sdgs.un.org/2030agenda.

50 Cryptoassets refer to a type of private asset that depends primarily on cryptography and distributed ledger or similar technology as part of their perceived or inherent value (FSB (2019)).

51 See Nakamoto (2008).

52 See Carstens (2021b).

53 See BIS Annual Economic Report (2018).

activities;[54] and the significant criminal exploitation of cryptoassets.[55] Research suggests, for example, that almost half of all transactions in Bitcoin can be linked to illegal activity.[56]

46. **Meanwhile, stablecoins have emerged as a new variant of cryptoassets.** The first stablecoins (eg Tether, BitShares, NuBits) were introduced in 2014, designed to maintain a stable value relative to a specified asset, or a basket of assets.[57] There are two broad types. Asset-linked stablecoins are purportedly linked to fiat currencies, commodities, financial instruments or other cryptoassets. Algorithm-based stablecoins, in contrast, use algorithms in an attempt to stabilise their value by managing the supply of outstanding coins in response to changes in demand. Importantly, asset-based and algorithmic stablecoins differ not only in terms of their stabilisation mechanism but also in the attributes that define a means of payment. While asset-linked stablecoins are claim-based (ie payment involves the transfer of ownership of a claim on value existing elsewhere from one party to another), algorithm-based stablecoins are object-based (ie payment involves the hand-over of an object which triggers immediate settlement as long as the parties deem the object to be valid).[58]

47. **Stablecoins come in various forms.** They differ not only in the stabilisation mechanism but also in the overall setup for their redemption. For some stablecoins, holders have redemption rights against the issuer and/or a direct claim on the reserve assets while others do not. Certain stablecoins promise their holders redemption at a pre-established and fixed face value (similar to debt instruments); others do so at a variable value determined by the prevailing market prices of the assets that back the claim (similar to equity-like instruments). Finally, asset-backed stablecoins differ in terms of the amount of reserve assets available that could be used to satisfy redemption requests; and how the promise of a fixed value redemption is backstopped.

48. **While the jury is still out, the role of stablecoins as a new payment method could increase over time.** While stablecoins have several potential use cases, some – particularly those that achieve a value with very low or no price volatility – may evolve over the years to become a convenient means of payment for e-commerce (particularly when integrated into online platforms) and peer-to-peer and micro-payments, thereby challenging current means of payment such as credit cards, electronic wallets or traditional bank payments (Arner et al (2020)).[59] Widely adopted stablecoins, in particular those with a potentially global reach (so-called "global stablecoins" or GSCs), could become systemically important,

[54] Bitcoin's energy intensive proof-of-work (POW) consensus protocol consumes more electricity than Argentina or Norway. In this context, some argue that the environmental impact of cryptoassets could be reduced by using more renewable energy sources and migrating to a proof-of-stake protocol, which is less energy intensive than POW. See Citi GPS (2021).

[55] For example, Houben and Snyers (2020) report that most legal activity in cryptoassets takes place for speculative purposes whereas it appears that many who use cryptoassets to make payments do so primarily for illicit purposes, such as the buying and selling of illegal goods or services online in darknet marketplaces, money laundering, evasion of capital controls, payments in ransomware attacks and thefts.

[56] Foley et al (2019) estimate that Bitcoin involves USD 76 billion of illegal activity per year, which is close to the scale of markets for illegal drugs in Europe and the United States.

[57] See FSB (2020). Examples are Tether, USD Coin, Dai, Paxos and True USD. In terms of market capitalisation, Tether is by far the dominant player in the stablecoin space. See Graph 2 in Arner et al (2020).

[58] In addition, for claim-based means of payments, redemption of the claim can be either at fixed or variable value. The concept of redemption does not apply to object-based means of payment. See Adrian and Mancini-Griffoli (2019a).

[59] Stablecoins may also serve as a digital monetary instrument to embed in DLT applications, including for programmable money or smart contracts. For details see Arner et al (2020).

including as a means of payment (FSB (2020)).[60] The adoption of stablecoins could, however, be affected by the issuance of central bank digital currencies (CBDCs).[61]

Emerging regulatory approaches

49. **Regulatory responses to cryptoassets, including stablecoins, are in flux and vary widely.** In many cases, jurisdictions have issued warnings to investors and consumers, clarified the regulatory treatment of cryptoassets and related activities, and, in some cases, implemented crypto-specific licencing, authorisation and registration regimes.[62] Absent a dedicated crypto-specific licencing regime, cryptoasset service providers may nevertheless be required to hold other types of licence. In a large-scale global survey conducted in 2020, the Cambridge Centre for Alternative Finance (CCAF) found that (i) just over two out of five surveyed firms were licensed or in the process of obtaining a licence; (ii) licence holders primarily held a crypto-specific licence (42%), a payment or e-money licence (29%) or a money business licence (28%); and (iii) of the licensed and registered entities, licences and registration were issued primarily by the United Kingdom (23%) and United States (23%) regulatory authorities (CCAF (2020)).

50. **Most jurisdictions do not have regulations that are specific to stablecoins.** In 2020, the FSB conducted a survey on regulatory and supervisory approaches to stablecoins. It found that the majority of surveyed jurisdictions where stablecoins are available do not have regulatory or supervisory regimes that are specific to stablecoins; but that existing regimes apply in whole or in part to stablecoins. It also found that, while stablecoins could fall under multiple regulatory classifications,[63] they are most frequently classified as e-money.[64] In advanced economies, they are also often classified as collective investment schemes (CIS), securities other than CIS and deposits, and in emerging markets, as payment instruments.

51. **The regulatory treatment of a stablecoin depends on its features and how it is set up.** In the absence of a dedicated regulatory framework, if a stablecoin arrangement or parts thereof resemble an already regulated product or service, authorities will likely treat it as such. For this, however, they need to assess the applicability of existing regimes on a case-by-case basis. The questions they may ask in this assessment are about the intended function and purpose of a stablecoin, which may be used as a means of payment or exchange (payment token); as an investment instrument (security token); or as a means of granting its holders access to a digital platform or service (utility token). Other questions might be about the stabilisation mechanism (asset-linked or algorithmic) and expected reach and therefore systemic importance (global and other).[65] Answers to these questions will determine inter alia whether a stablecoin

[60] The ECB Crypto-Assets Task Force identifies three scenarios for the uptake of stablecoins. Stablecoins may (i) have a "crypto-asset accessory function" (ie serving as a less volatile class of cryptoassets within the crypto space), (ii) become a new payment method; or (iii) serve as an alternative store of value. Under the second scenario, the Task Force notes that stablecoins "could reach a scale such that financial stability risks can become material, and the safety and efficiency of the payment system may be affected". See ECB (2020).

[61] See Adrian and Mancini-Griffoli (2019b).

[62] See Ehrentraud et al (2020).

[63] In some jurisdictions, stablecoins are legally required to be classified under only one category (FSB (2020)).

[64] When considering how best to regulate stablecoins, policymakers may ask whether stablecoins should in principle be regulated like e-money. The key to answering this question is the fact that, while stablecoins share a number of characteristics, no two are alike. They come in different forms and have a wide diversity of structures and operating models, with different attributes such as (i) whether there is a claim involved and who the counterpart of that claim is; (ii) what the conditions for redeemability are; and (iii) what type of stabilisation mechanism and reserve assets are involved (see Annex 1 in FSB (2020). The combination of these attributes will determine whether a stablecoin shares more or less functional similarities with e-money, and can therefore be classified as e-money by regulators.

[65] For details see Table 1 in Coelho et al (2021).

falls under the purview of financial laws such as those for securities or payment services; and therefore what requirements apply.

52. **Among the regulatory requirements applicable to stablecoins, AML/CFT is the most common.** According to the FSB survey cited above, jurisdictions apply different requirements to different activities within a stablecoin ecosystem. While AML/CFT requirements apply to most activities in most countries, other requirements such as investor and consumer protection, cyber/technology risk, safety/soundness, and data privacy apply less often.[66]

53. **The majority of jurisdictions surveyed by the FSB see the need for adjustments to their existing framework for stablecoins.** This is because the risks identified may not be adequately addressed by applying existing frameworks. Potential gaps include (i) the potentially incomplete or non-existent implementation of the revised FATF standards; (ii) obstacles for supervision if the legal classification of a stablecoin falls outside an existing regulatory framework; (iii) incomplete regulatory coverage of stablecoin activities; (iv) insufficient risk mitigation tools; and (v) the lack of adequate competition policies. In response, some jurisdictions indicated their intention to take legislative action, either to address gaps in their regulatory regimes or to introduce a new regulatory framework (FSB (2020)).

54. **At the international level, global standard-setting bodies are acting on stablecoins.** In June 2019, the G20 mandated the FSB to examine regulatory issues raised by "global stablecoin" arrangements (GSCs) and to advice on multilateral responses. In response, the FSB carried out an analysis of financial stability risks raised by GSCs and developed a set of regulatory recommendations with respect to these arrangements (Box 5). In October 2019, the G20 mandated the FATF to consider AML/CFT issues relating to stablecoins. The resulting report, issued in July 2020, found that stablecoins display many potential ML/TF risks by virtue of their potential for anonymity, global reach and layering of illicit funds.[67] It also highlighted that revised FATF standards apply to stablecoins, which the standards treat as either virtual assets or traditional financial assets.[68] Meanwhile, in March 2020, IOSCO issued a report on the possible implications of global stablecoin initiatives for securities markets regulators. It found that GSCs could fall within securities market regulatory frameworks; and that the applicability of existing IOSCO principles and standards depends on a GSC's legal and regulatory characteristics and features.[69]

Against this background, work is under way in some jurisdictions to modify their regulatory framework for cryptoassets, including stablecoins. In some cases, regulatory initiatives cover all cryptoassets, with stablecoins as a specific category of cryptoassets (eg draft MICA Regulation in the EU); in others, they only target stablecoins (eg the STABLE Act proposal in the United States). Annex 2 provides an overview of emerging regulatory approaches in the EU, the United Kingdom and United States.

66 See Table 1 of Annex 3 in FSB (2020).

67 See FATF (2020a).

68 Under the revised FATF standards, entities involved in stablecoin arrangements – such as central developers, governance bodies, wallet providers, exchange and transfer service providers – generally have to observe AML/CFT obligations. The concrete obligations depend on what activity an entity undertakes and its specific role in the stablecoin arrangement. Nevertheless, in October 2020, only 25 of the FATF's 39 members have transposed the revised FATF Standards into their domestic frameworks (FATF (2020b)).

69 See IOSCO (2020).

Box 5

Regulation, supervision and oversight of "global stablecoin" arrangements

The FSB's high-level recommendations for addressing the regulatory, supervisory and oversight challenges raised by GSC arrangements

Following the G20's mandate to advise on multilateral responses to address the financial stability risks posed by GSC arrangements, the FSB developed a set of regulatory recommendations intended to promote coordinated and effective regulation, supervision and oversight of GSC arrangements, both at the domestic and international level. The recommendations call for regulation, supervision and oversight that is proportionate to the risks, and stress the value of flexible, efficient, inclusive and multi-sectoral cross-border cooperation, coordination and information-sharing arrangements among authorities that take into account the evolving nature of GSC arrangements and the risks they may pose over time.

The 10 recommendations are:

1. Authorities should have and utilise the necessary powers and tools, and adequate resources, to comprehensively regulate, supervise and oversee a GSC arrangement and its associated functions and activities, and enforce relevant laws and regulations effectively.

2. Authorities should apply comprehensive regulatory, supervisory and oversight requirements and relevant international standards to GSC arrangements on a functional basis and proportionately to their risks.

3. Authorities should cooperate and coordinate with each other, both domestically and internationally, to foster efficient and effective communication and consultation in order to support each other in fulfilling their respective mandates and to ensure comprehensive regulation, supervision, and oversight of a GSC arrangement across borders and sectors.

4. Authorities should ensure that GSC arrangements have in place a comprehensive governance framework with a clear allocation of accountability for the functions and activities within the GSC arrangement.

5. Authorities should ensure that GSC arrangements have effective risk management frameworks in place especially with regard to reserve management, operational resilience, cyber security safeguards and AML/CFT measures, as well as "fit and proper" requirements.

6. Authorities should ensure that GSC arrangements have in place robust systems for collecting, storing and safeguarding data.

7. Authorities should ensure that GSC arrangements have appropriate recovery and resolution plans.

8. Authorities should ensure that GSC arrangements provide users and relevant stakeholders with comprehensive and transparent information necessary to understand the functioning of the GSC arrangement, including with respect to its stabilisation mechanism.

9. Authorities should ensure that GSC arrangements provide legal clarity to users on the nature and enforceability of any redemption rights and the process for redemption, where applicable.

10. Authorities should ensure that GSC arrangements meet all applicable regulatory, supervisory and oversight requirements of a particular jurisdiction before commencing any operations in that jurisdiction, and adapt to new regulatory requirements as necessary.

The FSB noted that the establishment of effective regulatory, supervisory and oversight approaches for GSC arrangements supports the implementation of a key building block of ongoing work to enhance cross-border payments commissioned by the G20. To keep pace with the evolution of GSC arrangements and market developments, the FSB, in close cooperation with relevant standard-setting bodies, is planning to review the recommendations on a

regular basis; and to undertake a review of implementation, including how any gaps identified could be addressed by existing frameworks, by July 2023.

Source: FSB (2020b).

Section 5 – Concluding remarks

55. **Improvements in technology and a growing demand for digital payment methods are increasingly reshaping the way payments are made.** Recent advances in technology have opened up new ways to pay that respond to consumers' demand for payment methods that are convenient, easy to use, frictionless, low-cost and no-touch. The Covid-19 pandemic further increased demand for digital payment methods. While some of the changes in payment choices may be reversed as the pandemic recedes, others might be retained, with a lasting effect on how people and companies make payments.[70]

56. **The growing importance of NBPSPs in retail payments in many jurisdictions has raised questions about their regulation.** While the payment space continues to be dominated by banks in many countries, the role of fintech-driven NBPSPs operating a variety of business models continues to increase. This presents opportunities to foster financial inclusion, competition, and efficiency in payments markets. However, it also comes with potential risks in terms of consumer protection, operational and cyber resilience, the protection of funds in transit or storage, data protection and privacy, digital exclusion and market concentration.[71]

57. **Non-banks can offer a broader variety of payment services in AEs than in EMDEs and they are subject to more intensive regulation in the latter.** In advanced economies, non-banks can offer several types of payment service. However, non-banks in many EMDEs can offer only a few. Moreover, NBPSPs in EMDEs, particularly those acquiring payment transactions, providing e-wallet services and issuing e-money, face more intensive regulation than those in AEs. This could be due to a number of fundamental issues that authorities first need to address, such as the maturity of the financial system, the quality of IT and communications infrastructure and limited technical resources. At the same time, given the potential of non-bank players to foster financial inclusion, authorities in EMDEs may already start considering strategies for expanding the payment services market and reviewing the appropriateness of existing regulations for these players. In this way, they can promote innovation while ensuring the safety and integrity of the financial system.

58. **Application of some regulatory requirements for payment services varies widely.** This is especially true for requirements related to authorisation, minimum capital, safeguarding of funds and interoperability. The objectives of these requirements may be the same, but how they are applied across payment services can be quite different. Moreover, how these requirements are implemented varies significantly across jurisdictions, even for the same payment service. There may be scope for harmonising at least some of these requirements across payment services within and across jurisdictions for the same payment service. In determining the right regulatory approach, authorities need to ensure that the risk profile of each payment service is appropriately reflected in regulations.[72]

59. **The regulatory framework for newer payment services is less developed.** While jurisdictions tend to have well defined and fairly established regulatory frameworks for more "mature" payment services

[70] See Mester (2020).

[71] See CPMI and WBG (2020).

[72] See Khiaonarong and Goh (2020).

(eg e-money), the regulatory framework for newer services (eg virtual asset services) is still evolving. Aside from AML/CFT requirements, which are the most common requirements even for newer payment services, it seems that jurisdictions are still considering if and how other regulatory requirements should be applied to these services. For example, on average, jurisdictions impose only four types of requirement on virtual asset services. This is about half as many types of requirement as are imposed on other services. While legal and regulatory frameworks differ across jurisdictions, authorities may benefit from learning more about regulatory approaches (including the rationale for these approaches) in other jurisdictions when it comes to new payment services. This would ensure that all risks arising from these services are adequately addressed in regulations.

60. **Regulatory frameworks for digital payments and e-money are broadly similar but differences stand out.** Where there are differences in the frameworks for e-money and digital payments services, e-money institutions are almost always subject to more extensive requirements. This is because digital payments services generally refer to the digital facilitation and channelling of funds, while e-money services operate more as stored value facilities and thus can be seen as more "bank-like" activities.[73] Against this background, in case a jurisdiction intends to modify its regulatory framework, it may opt to assess the differences in regulation for digital payments and e-money services and compare them with requirements in other jurisdictions.

61. **Emerging technologies are creating the potential for new means of payments to develop.** While cryptoassets such as Bitcoin fail to qualify as a payment instrument due to their high volatility,[74] the role of stablecoins as a new payment method may potentially increase over time. The adoption of stablecoins, however, could be affected by the rollout of CBDCs, which might be perceived as attractive alternative. Because there is as yet no dedicated regulatory regime for stablecoins, the regulatory treatment of a stablecoin will depend on its specific features and setup.

62. **Regulatory approaches for stablecoins as one variant of cryptoassets are under consideration in a few jurisdictions but nothing has been finalised yet.** In the EU, the European Commission proposed the establishment of a European framework for markets in cryptoassets in September 2020, which would introduce a range of requirements (eg capital requirements, custody of assets, a mandatory complaint holder procedure available to investors, and rights of the investor against the issuer) for cryptoasset issuers and providers, with more stringent requirements applicable to issuers of GSCs.[75] In the United Kingdom, the Treasury published a consultation on its proposed approach to regulating cryptoassets and stablecoins in January 2021. It proposes to bring stablecoins that are used as means of payment into the regulatory perimeter. Finally, in the United States, a proposal to regulate stablecoins, known as the STABLE Act, was published in November 2020. It would inter alia require any stablecoin issuer to obtain a federal banking charter.

63. **The role of big techs in payments is likely to receive further attention.** Big techs have already captured a substantial market share in digital payments in some jurisdictions.[76] But even where they have not, this can change rapidly due to the unique features of their business models and they could quickly become systemically important – or "too big to fail". At present, big techs' financial operations (including

[73] Because e-money activities can be construed as banking activities, the regulatory burden may be much higher if the jurisdiction uses a "narrow-bank" framework. Even though e-money institutions may need to obtain banking licences under these systems, they are still not allowed to engage in certain banking activities, such as maturity transformation.

[74] See www.bloomberg.com/news/articles/2021-03-25/bis-s-coeure-says-bitcoin-has-failed-test-on-being-a-currency.

[75] See https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684.

[76] In China, for example, Alipay reportedly has a 54% share and Tenpay/WeChat Pay 39% of the mobile-payments market by value (Economist (2020)). Overall, big tech firms processed payments equivalent to 38% of GDP in 2018 (FSB (2020)).

payments) are subject to the same requirements as those of other market participants;[77] and there seems to be a case for developing rules that are more entity-based for big techs in areas such as competition and operational resilience, which would address the risks stemming from the different activities they perform (Carstens (2021a) and Restoy (2021)).

64. **Regulators will likely pay particular attention to big techs' potential involvement in global stablecoin (GSC) arrangements.** In October 2020, the FSB published high-level recommendations for the regulation, supervision and oversight of GSC arrangements. It noted that "a widely adopted stablecoin with a potential reach and use across multiple jurisdictions [...] could become systemically important in and across one or many jurisdictions, including as a means of making payments." Due to the higher risks GSCs pose to financial stability, monetary policy transmission and monetary sovereignty, as compared to more limited stablecoins, GSCs arguably require specific regulatory treatment.[78] From a regulatory perspective, it will be important to appreciate the unique combination of a very specific type of entity (big techs) providing a very specific type of activity (provision of GSC), and consider the potential implications of this interplay.

[77] Because big techs' financial operations (including payments) are subject to the same requirements as those of other market participants, they need to hold appropriate licences to perform regulated financial activities or provide their services in partnership with financial institutions that meet the regulatory requirements. See Crisanto et al (2021).

[78] A key challenge, however, is the identification of GSCs. See Arner et al (2020).

References

Adrian, T and T Mancini-Griffoli (2019a): "The rise of digital money", *Fintech notes*, July.

——— (2019b): "From stablecoins to central bank digital currencies", IMF Blog, 26 September.

Arner, D, R Auer and J Frost (2020): "Stablecoins: risks, potential and regulation", *BIS Working Papers*, no 905, November.

Auer, R, J Frost and G Cornelli (2020): "Covid-19, cash, and the future of payments", *BIS Bulletin*, no 3, April.

Bank for International Settlements (2018): "Cryptocurrencies: looking beyond the hype", *BIS Annual Economic Report*, June, pp 91–114.

——— (2019): "Big tech in finance: opportunities and risks", *BIS Annual Economic Report*, June, pp 55–79.

——— (2020a): "Innovations in payments", *BIS Quarterly Review*, March, pp 21–35.

——— (2020b): "Central banks and payments in the digital era", *BIS Annual Economic Report*, June, pp 67–95.

Bill and Melinda Gates Foundation (BMGF) (2019): "Inclusive digital financial services: a reference guide for regulators", July.

Bloomberg (2021): "BIS's Coeure Says Bitcoin failed test on being a currency", 25 March.

Bossone, B (2017): "Electronic money versus money: An assessment of regulation", *VoxEU*, 25 January.

Cambridge Centre for Alternative Finance (2020): *3rd global cryptoasset benchmarking study*, September.

Carstens, A (2021a): "Public policy for big techs in finance", introductory remarks at the Asia School of Business Conversations on Central Banking webinar, "Finance as information", Basel, 21 January.

——— (2021b): "Digital currencies and the future of the monetary system", remarks at the Hoover Institution policy seminar, 27 January.

Citi GPS (2021): "Future of money", *Citi GPS: Global Perspectives & Solutions*, April.

Coelho, R, J Fishman and D Garcia Ocampo (2021): "Supervising cryptoassets for anti-money laundering", *FSI Insights on policy implementation*, no 31, April.

Committee on Payments and Markets Infrastructures (2012): *Principles for financial market infrastructures*, April, p 8.

——— (2014): "Non-banks in retail payments", *CPMI Papers*, no 118, September.

——— (2017): "Methodology of the statistics on payments and financial market infrastructures in the CPMI Countries (Red Book statistics)", *CPMI Papers*, no 168, August.

——— (2020a): "Payments go (even more) digital".

——— (2020b): "Enhancing cross-border payments: building blocks of a global roadmap", July.

Committee on Payments and Markets Infrastructures and International Monetary Fund (2019): "Investigating the impact of global stablecoins", *G7 Working Group on Stablecoins,* October.

Committee on Payments and Markets Infrastructures and the World Bank Group (2015): "Payment aspects of financial inclusion – consultative report", *CPMI Papers*, no 133, September.

——— (2016): "Payment aspects of financial inclusion", *CPMI Papers*, no 144, April.

——— (2020): "Payment aspects of financial inclusion in the fintech era", *CPMI Papers*, no 191, April.

Crisanto, J C, J Ehrentraud and M Fabian (2021): "Big techs in finance: regulatory approaches and policy options", *FSI Briefs,* no 12, March.

Dias, D and S Staschen (2019): "Nonbank e-money issuers vs payments banks - how do they compare?", *CGAP Technical Note,* December.

The Economist (2020): "A dynamic duopoly: do Alipay and Tencent misuse their market power?", 8 August.

Ehrentraud, J, D Garcia Ocampo, L Garzoni and M Piccolo (2020): "Policy responses to fintech: a cross-country overview", *FSI Insights on policy implementation*, no 12, January.

Enria, A (2020a): "Letter from Andrea Enria, Chair of the Supervisory Board, to Mr Martin Schirdewan, Member of the European Parliament", August.

——— (2020b): "Letter from Andrea Enria, Chair of the Supervisory Board, to Mr Herbrand, Member of the German Bundestag, on banking supervision", September.

European Banking Authority (2021): "The EBA takes steps to address 'de-risking' practices", March.

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

European Commission (2020a): "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a retail payments strategy for the EU", September.

_____ (2020b): "Digital Finance Package", September.https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684

——— (2020c): "Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937", September.

——— (2021): "Targeted consultation on the review of the crisis management and deposit insurance framework", *EC Consultation Documents*, January.

European Union (2019): "Regulation (EU) 2019/518 of the European Parliament and of the Council of 19 March 2019 amending Regulation (EC) No 924 / 2009 as regards certain charges on cross-border payments in the Union and currency conversion charges", *Official Journal of the European Union*, March.

Federal Deposit Insurance Corporation (2008): "Insurability of Funds Underlying Stored Value Cards and Other Nontraditional Access Mechanisms", *Federal Register*, vol 73, no 220, November.

Financial Action Task Force (2020a): "FATF Report to G20 on So-called Stablecoins", July.

——— (2020b): "FATF President's remarks to G20 Finance Ministers and Central Bank Governors meeting", October.

Financial Stability Board (2019): "Crypto-assets: Work underway, regulatory approaches and potential gaps", *FSB Progress Reports*, May.

——— (2020a): "BigTech firms in finance in emerging market and developing economies: Market developments and potential financial stability implications", *FSB Reports to the G20*, October.

——— (2020b): "Regulation, supervision and oversight of "global stablecoin" arrangements: Final report and high-level recommendations", *FSB Reports to the G20*, October.

——— (2020c): "Enhancing cross-border payments: stage 3 roadmap", October.

Foley, S, J R Karlsen and T J Putniņš (2019): "Sex, drugs, and bitcoin: how much illegal activity is financed through cryptocurrencies?", *Review of Financial Studies*, vol 32, no 5, May.

García, J, S Lynch and R Tlaib (2020): "Stablecoin Tethering and Bank Licensing Enforcement (STABLE) Act", *United States House of Representatives*, 116th Congress, December.

HM Treasury (2021): "UK regulatory approach to cryptoassets and stablecoins: consultation and call for evidence", January.

Houben, R and A Snyers (2020): "Crypto-assets – Key developments, regulatory concerns and responses", study requested by the ECON committee, April.

International Organization of Securities Commissions (2020): "Global stablecoin initiatives", March.

Izaguirre, J C, D Dias and M Kerse (2019): "Deposit Insurance treatment of e-money: an analysis of policy choices", *CGAP Technical Note,* Consultative Group to Assist the Poor, Washington DC, October.

Izaguirre, J C, T Lyman, C McGuire and D Grace (2016): "Deposit insurance and digital financial inclusion", *CGAP Brief*, October.

Khiaonarong, T and T Goh (2020): "Fintech payments regulation: Analytical framework", *IMF Working Papers*, May.

Lane, T (2021): "Payments innovation beyond the pandemic", remarks at the Institute for Data Valorization, 10 February.

Mester, L (2020): "Payments and the pandemic", remarks at the keynote session, 20th Anniversary Chicago Payments Symposium – Federal Reserve Bank of Chicago, September.

Nakamoto, S (2008): "Bitcoin: A peer-to-peer electronic cash system".

Office of the Comptroller of the Currency (2020a): "Re: Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers", Interpretive Letter, no 1170, July.

——— (2020b): "OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association Authority to Hold Stablecoin Reserves", Interpretive Letter, no 1172 September.

——— (2021): "Federally Chartered Banks and Thrifts May Participate in Independent Node Verification Networks and Use Stablecoins for Payment Activities", Interpretive Letter, no 1174, January.

President's Working Group on Financial Markets (2020): "Statement on Key Regulatory and Supervisory Issues Relevant to Certain Stablecoins", December.

Restoy, F (2021): "Fintech regulation: how to achieve a level playing field", *FSI Occasional Papers*, no 17, February.

Shin, H S (2019): "Big tech in finance: opportunities and risks", speech on the occasion of the BIS Annual General Meeting, June.

United Nations (2015): "Transforming our world: the 2030 Agenda for Sustainable Development", *UN General Assembly*, October.

Annex 1 – Jurisdictions covered

Jurisdictions covered in the survey conducted by the CPMI in early 2021

	Classified as:		
	CPMI member	Advanced economy	Emerging market/ developing economy
Algeria			✓
Argentina	✓		✓
Armenia			✓
Australia	✓	✓	
Austria		✓	
Bahamas			✓
Bahrain			✓
Belgium	✓	✓	
Belize			✓
Bolivia			✓
Brazil	✓		✓
Canada	✓	✓	
Cayman Islands			✓
Chile			✓
China	✓		✓
Chinese Taipei		✓	
Colombia			✓
Croatia			✓
Curacao			✓
Czech Republic			✓
Dominican Republic			✓
Eastern Caribbean Currency Union			✓
Ecuador			✓
Egypt			✓
El Salvador			✓
Eswatini			✓
Ethiopia			✓
Euro area	✓	✓	
France	✓	✓	
Germany	✓	✓	
Ghana			✓
Guatemala			✓
Guyana			✓
Honduras			✓
Hong Kong SAR	✓	✓	

India	✓		✓
Indonesia	✓		✓
Italy	✓	✓	
Jamaica			✓
Japan	✓	✓	
Jordan			✓
Kuwait			✓
Latvia		✓	
Lesotho			✓
Madagascar			✓
Malaysia			✓
Malta		✓	
Mauritius			✓
Mexico	✓		✓
Mongolia			✓
Morocco			✓
Namibia			✓
Nepal			✓
Netherlands	✓	✓	
Pakistan			✓
Paraguay			✓
Poland			✓
Portugal		✓	
Romania			✓
Russia	✓		✓
Saudi Arabia	✓		✓
Singapore	✓	✓	
Slovenia		✓	
South Africa	✓		✓
South Korea	✓	✓	
Spain	✓	✓	
Sudan			✓
Sweden	✓	✓	
Switzerland	✓	✓	
Trinidad and Tobago			✓
Turkey			✓
United Arab Emirates			✓
United Kingdom	✓	✓	
United States	✓	✓	
Vietnam	✓		✓

Source: FSI.

Annex 2 – Regulatory approaches for cryptoassets and stablecoins

Regulatory approaches for cryptoassets and stablecoins are starting to evolve. Work is under way in some jurisdictions to modify their regulatory framework for stablecoins. Prominent examples are ongoing initiatives in the EU (MICAR proposal), the United Kingdom (HMT consultation) and the United States (STABLE Act proposal, WG report), as described below.

Regulatory developments in the EU

The Markets in Crypto-assets Regulation (MICAR)[79] is a regulatory proposal put forward by the European Commission in September 2020. It is part of the Digital Finance package, a package of measures aiming to enable and support the potential of digital finance in terms of innovation and competition – while mitigating the associated risks – in the EU. As noted by the European Commission, the current EU regulation for cryptoassets is fragmented and potentially fails to encompass some types of cryptoasset.[80] MICAR fills in those gaps as it covers cryptoassets falling outside existing EU financial services legislation.

MICAR classifies cryptoassets in the following subcategories.

- **General cryptoassets,** refer to cryptoassets that do not qualify as e-money tokens or asset-referenced tokens. Examples of these could be pure cryptocurrencies, but also utility tokens which are intended to provide digital access to a good or service, available on DLT, and only accepted by the issuer of that token. Utility tokens would be subject to very limited rules and are eligible for exemptions.
- **Asset-referenced tokens** refer to a type of cryptoasset that purports to maintain a stable value by referring to the value of several fiat currencies that are legal tender, one or several commodities or one or several cryptoassets, or a combination of such assets. Asset-referenced tokens are considered the most risky of the three subcategories and would be subject to extensive requirements.
- **Electronic money tokens or e-money tokens** refer to a type of cryptoasset that purports to maintain a stable value by referring to the value of a fiat currency that is legal tender. E-money tokens are deemed to be e-money and therefore subject to similar requirements as e-money generally, such as redemption at par and investment of funds received by the issuer in secure, low-risk assets. In addition to the e-money directive, MICAR adds specific rules for e-money tokens.
- **Significant tokens** refer to e-money and asset-referenced tokens that have a considerable scale and/or international reach. These tokens raise specific challenges in terms of financial stability, monetary policy transmission and monetary sovereignty, and would therefore be subject to more stringent requirements than other tokens. Additional requirements include, for example, higher capital requirements, interoperability requirements and the establishment of a liquidity management policy.

[79] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593.

[80] On a related note, the EC also noted that some EU provisions might inhibit the use of distributed ledger technology (DLT) in the Union. Work is currently ongoing to address this issue, which is part of the DLT pilot regime allowing for exemptions from specific provisions to test DLT solutions within financial market infrastructures. See https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0594&from=EN.

MICAR defines cryptoasset service providers as any person providing cryptoasset services on a professional basis. The provision of cryptoasset services includes, among others, the custody and administration of cryptoassets on behalf of third parties, the operation of a trading platform for cryptoassets and the provision of advice on cryptoassets. Proposed requirements on cryptoasset service providers include market abuse rules, organisational requirements and/or prudential requirements depending on the concrete types of service they provide.

The authorisation process for token issuers depends on the type of token to be issued.

- **Issuers of general cryptoassets** (including utility tokens) would not need specific authorisation but have to comply with consumer protection requirements, are required to draft a cryptoasset white paper and notify competent authorities as explained below. Some exemptions are possible if, for example, the tokens are offered for free, offered to a limited number of persons, or the total amount stays below a certain threshold.
- **Issuers of asset-referenced tokens** would need to be authorised as such and be incorporated in the form of a legal entity established in the Union. The authorisation for issuers of asset-referenced tokens would depend on the type of investors concerned. No authorisation is needed if the tokens are offered exclusively to qualified investors or, in some instances, when the offer to the public is below a certain threshold. Credit institutions would not need a separate authorisation to issue tokens to the public but would be required to provide a white paper and notify its competent authority, as explained below.
- **Issuers of e-money tokens** would have to be authorised either as credit institutions or as e-money institutions.

Besides provisions on authorisation, MICAR has requirements related to consumer protection, governance, capital, prudent management of the reserve assets (for asset-referenced and significant tokens) and supervision.

- **Provisions related to consumer protection** include the publication of a cryptoasset "white paper" and the obligation to notify the competent authority accordingly; the right of withdrawal for consumers during a limited period of time after they have acquired a token; the provision of clear, fair and not misleading information; the provision that issuers should always act honestly, fairly and professionally and in the best interest of the holders; the need to have clear procedures in place for handling complaints and conflicts of interest. For e-money tokens specifically, holders should always be provided with a claim on the issuer and a redemption right at par value with the fiat currency referenced at any moment.
- **Provisions related to governance** include fit and proper assessments of senior management, risk management and internal control mechanisms and requirements regarding outsourcing.
- **Capital requirements for asset-referenced tokens** are calculated as the greater of EUR 350,000 or 2% of the reserve assets backing the value of the tokens. This percentage is increased to 3% for significant asset-referenced tokens. Significant e-money tokens must also abide by this requirement.
- **Provisions related to the management of the reserve assets** require a one-to-one relationship between the reserve assets and the outstanding value of the tokens. Also, a concrete process must be in place to manage the reserve assets and link them to the value of the tokens to be described in detailed policies; a custody policy and the segregation of the reserve assets from the issuer's own assets. Reserve assets should (i) be kept at a credit institution or an authorised cryptoasset service provider; (ii) not be encumbered or pledged as collateral; and (iii) be invested

in high-quality liquid assets.[81] In addition, no interest should be paid to users and issuers should have an orderly wind-down plan in place.

The supervision of both e-money and asset-referenced tokens as well as cryptoasset service providers lies within the remit of the national authorities. The EBA will supervise significant asset-referenced tokens while for significant e-money tokens dual supervision by both competent authorities at the national level and the EBA will take place. The EBA will also establish colleges of supervisors for issuers of significant asset-referenced and e-money tokens.

Regulatory developments in the United Kingdom

The UK government (HM Treasury) published in January 2021 a consultation on the UK regulatory approach to cryptoassets and stablecoins.[82] As noted by HM Treasury, the UK government proposes to bring stablecoins that are used as means of payment into the regulatory perimeter, following the principle of "same risk, same regulatory outcome".

The consultation puts forward categories of tokens that are similar to those under MICAR. Tokens are classified under e-money tokens, security tokens and unregulated tokens (which include utility and exchange tokens). A new regulated category is also introduced: stable tokens.

- **E-money tokens** are defined, broadly speaking, as digital payment instruments that offer the holder a direct claim on the issuer and can store value and be redeemed at par value at any time.
- **Security tokens** have characteristics of shares or debt instruments. These are likely to be tokenised, digital versions of traditional securities.
- **Unregulated tokens** are neither e-money tokens nor security tokens and include utility tokens, ie tokens used to buy a service or access a DLT platform, and exchange tokens, ie tokens that are primarily used as a means of exchange.
- **Stable tokens** are tokens that have their value indexed to the performance of one or more assets, such as fiat currency or a commodity. These would also include other forms of tokenised payment and settlement assets, as well as tokenised forms of central bank money. According to the consultation paper, it is not clear if algorithmic stablecoins would fall under this category.

The regulation of stablecoins would be based as much as possible on existing payment and e-money regulations (PSR/EMRs). Tokens where users are provided with a claim on the issuer and where funds are redeemable at any time at par value already fall within the scope of the EMRs. Tokens that could reliably be used for retail or wholesale transactions are subject to minimum requirements and protections as part of the authorisation regime proposed in the document. Some exceptions are provided (eg for stable tokens within limited or closed loop networks). Market actors[83] such as stablecoin issuers, cryptoassets exchanges, and stablecoin wallets that are involved in or facilitate the use and issuance of stable tokens would also be subject to regulation. Stable token arrangements that play a similar function to existing payment systems might be subject to designation as such. This applies equally to stable token arrangements reaching a systemic scale and where existing systemic payments regulation could apply.

[81] For e-money tokens, reserve assets have to be in the same currency as the currency referenced by the tokens.

[82] www.gov.uk/government/consultations/uk-regulatory-approach-to-cryptoassets-and-stablecoins-consultation-and-call-for-evidence.

[83] "Key participants or entities are likely to include: (i) issuers or systems operators, responsible for managing the rulebook of a system, the infrastructure, burning and minting coins (among others); (ii) cryptoassets exchanges, enabling consumers to exchange tokens for fiat money or other tokens; (iii) wallets, which may provide custody of tokens and/or manage private keys. Along with exchanges, these are often the main consumer interface." (paragraph 3.23). Please see a list of activities/functions that would also be in the scope of the regulation (paragraph 3.21).

The consultation also provides a preliminary list of anticipated activities, entities and requirements, with financial crime requirements applying to all entities and activities.

The proposed UK framework differs from the EU's MICAR in its classification of stablecoins and tokens. The United Kingdom's approach relies as its starting point on the FCA Guidance on Cryptoassets (PS10/22), which identifies four categories of cryptoassets and provides guidance on whether they are likely to fall within the regulatory perimeter. Utility tokens are not regulated in the UK proposal, while they are in MICAR. HM Treasury is consulting on expanding the regulatory perimeter to regulate a subset of cryptoassets (described as stable tokens, ie those tokens that seek to stabilise their value by reference to an asset or currency) used as a means of payment. HM Treasury identifies two categories of stable token: (1) single-fiat tokens, where the value is linked to a single fiat currency; and (2) other asset-linked tokens, where value is linked to an asset other than a single fiat currency (eg gold or multi-currency). The consultation suggests that the former may be subject to the same requirements as are set out in the existing e-money regime but that a bespoke regime may be required for other types of stable token. HM Treasury has also called for input to support consideration of the case for bringing a broader set of cryptoasset market actors or tokens into an authorisation regime.

While the United Kingdom's proposed framework does suggest some additional requirements for "systemic" stablecoins, these are not as detailed as those found in MICAR. Broadly speaking, systemic stablecoins would be subject to Bank of England regulation and the additional requirements would be grounded in the CPMI's Principles for financial market infrastructures. UK regulators are also exploring the possibility, amongst other options, of requiring issuers of systemic stablecoins to hold their reserves in accounts at the Bank of England, while MICAR does not address this possibility.

Regulatory developments in the United States

In the United States, initiatives and preliminary documents on the regulation of stablecoins have also been issued. The US President's Working Group on Financial Markets released a statement on "key regulatory and supervisory issues relevant to certain stablecoins" in December 2020.[84] At the same time, a proposal to regulate stablecoins was published in November 2020, known as the US STABLE Act.[85]

The statement released by the US President's Working Group on Financial Markets sets out key regulatory and supervisory considerations for participants in significant US-based stablecoin arrangements that are intended primarily for use in retail payments. The Working Group did not propose a new, all-encompassing framework like MICAR. However, it emphasised the fact that responsible payment innovation is encouraged but that stablecoins must comply with applicable US legal, regulatory and oversight requirements. This includes:

- All applicable AML/CFT and sanctions obligations;
- US federal securities, commodity and/or derivatives laws depending on the design of the stablecoin and whether it constitutes a security, commodity or derivative subject to such laws;
- Additional provisions if the stablecoin is adopted on a significant scale in the United States, including provisions aimed at safeguarding financial stability, end user protection, market integrity, operational resilience, the smooth functioning of payments and trading markets, macroeconomic and international monetary stability and the facilitation of comprehensive cross-border supervision.

[84] https://home.treasury.gov/news/press-releases/sm1223.

[85] https://tlaib.house.gov/media/press-releases/tlaib-garcia-and-lynch-stableact.

Similarly, the proposed STABLE Act aims to regulate issuers of stablecoins by restricting who can issue them to federal banks and depository institution. Issuers will also be required to place their uninsured reserve funds with the Federal Reserve. The STABLE Act would require any company offering stablecoin services to follow relevant federal and state banking regulations. It would also mandate any company or bank issuing stablecoins to (i) notify and obtain approval from the Federal Reserve, the FDIC and the appropriate banking agency six months prior to their issuance; and (ii) maintain an ongoing analysis of potential systemic impacts and risks it is facing. The proposed bill exclusively focuses on stablecoins and not on other non-bank dollar liabilities. Any prospective issuer of a stablecoin would be required to obtain a banking charter, FDIC insurance, and maintain reserves for uninsured liabilities at the Federal Reserve to ensure that the stablecoin can be readily converted into dollars on demand. Currently the bill has been referred to committee and is being discussed.

In January 2021, the OCC issued an interpretive letter to clarify national banks' increasing use of "independent node verification networks" (INVNs) and stablecoins to perform services such as payment activities that require a banking licence. INVNs are often distributed ledgers used to record cryptocurrency transactions across all participants, who validate the transactions, store the data, and broadcast the data to other participants (OCC (2021)). The OCC's guidance, they state, falls well within regulatory and legal precedent, as it has repeatedly recognised the rights of banks to conduct permissible payment activities with new and evolving technologies. The regulator compared the increased usage of stablecoins with existing electronically stored value (ESV) systems that are currently being used to facilitate cash payments, and opined that stablecoins are just a "new means of performing that function." Any national bank that plans on using stablecoins and INVNs should understand and monitor the operational risks while ensuring compliance with existing federal regulation (eg Bank Secrecy Act).

In July and September 2020, the OCC provided guidance on cryptocurrency custodianship services and stablecoin reserves. The OCC clarified that regulated institutions are allowed to provide cryptocurrency custodianship services and hold stablecoin reserves on behalf of issuers (OCC (2020a,b)). In the case of custody, the OCC determined it fell well within the business of conventional banking, and has before allowed banks to operate as non-fiduciary custodians for a wide variety of assets, including those that are "unique and hard to value". For stablecoin reserves, the OCC specified that its guidance applied only to issuers of stablecoins backed by a single fiat currency and fully redeemable on a one-to-one basis. The OCC stated that cash reserves for these issuers are functionally equivalent to normal deposits, and reiterated that any national bank taking them should understand all the applicable laws and regulations, especially with respect to AML/CFT and the deposit insurance coverage of the reserves. Additionally, the OCC recommended that national banks should reach agreements with stablecoin issuers to regularly verify the number of outstanding coins to ensure reserves are sufficient to satisfy redemption requests.