

The future of cross-border payments 2021

Evolution or revolution?

Time for renewal in global cross-border payments





The future of payments 2021

Published by OMFIF Ltd.

Official Monetary and Financial Institutions Forum

6-9 Snow Hill, London, EC1A 2AY, United Kingdom

T: +44 (0)20 3008 5262

omfif.org [@omfif](#)

About OMFIF

With a presence in London, Singapore, Washington and New York, OMFIF is an independent forum for central banking, economic policy and public investment – a neutral platform for best practice in worldwide public-private sector exchanges.

For more information visit [omfif.org](#) or email enquiries@omfif.org

Acknowledgments

OMFIF thanks officials from the co-operating countries and cities for this publication, which will be joining us in launch partnerships around the world. We are grateful to many other associates and colleagues for their assistance and guidance.

Authors

Lewis McLellan

Editor, Digital Monetary Institute

Rebecca Brace

Simon Brady

Kanika Saigal

Editorial and Production

Clive Horwood

Managing Editor and Deputy CEO

Simon Hadley

Director, Production

William Coningsby-Brown

Production Manager

Fergus McKeown

Subeditor

Sarah Moloney

Subeditor

Marketing

James Fitzgerald

Marketing Manager

DMI team

John Orchard

Chief Executive Officer, OMFIF

Philip Middleton

Chairman, Digital Monetary Institute

Katie-Ann Wilson

Head of Policy Analysis, Digital Monetary Institute

Folusho Olotusin

Commercial Director, Digital Monetary Institute

Sinan Yilmaz

Programmes and Account Executive, Digital Monetary Institute

Report sponsors

Lead report sponsor



Lead chapter sponsors



Co-sponsors



© OMFIF Ltd 2021. The entire contents of this publication are protected by copyright. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior permission of the publisher. The views and opinions expressed by the authors and contributors to this publication are provided in the writers' personal and professional capacities and represent their responsibility. The publication does not imply that their contributions represent the views or opinions of OMFIF and must neither be regarded as constituting advice on any matter, nor be interpreted as such. The reproduction of advertisements in this publication does not in any way imply endorsement by OMFIF of products or services referred to therein.

While every care is taken to provide accurate information, the publisher cannot accept liability for any errors or omissions. No responsibility will be accepted for any loss occurred by any individual due to acting or not acting as a result of any content in this publication. On any specific matter reference should be made to an appropriate adviser.

Company Number: 7032533. ISSN: 2398-4236

Foreword

The high-stakes future of money

As technology increasingly renders cash obsolete and innovators disrupt payment processes with new forms of money, banks and traditional payment platforms are racing to meet the challenges of the future. By John Orchard, CEO, OMFIF.

Twenty-five years ago, the internet boom was in its infancy and mobile phones an expensive luxury. Friends Reunited, a clunky forerunner of Facebook, was still three years in the future, as was the binding together of internet access with mobile telephony through painfully slow 3G technology. RTGS-style systems, which allow banks to transfer funds by adjusting their central bank balances, had already been around for 25 years, as had SWIFT, the system for moving money between banks worldwide. These three technological arenas are now trying to meld to accommodate money – and securities – in new formats.

Why? How? And When? What does this mean for consumers, financial intermediaries, payment platforms, technology companies, regulators, central banks and the economy at large? Our guide to the future of payments, which convenes public and private players, incumbents and innovators, will take you on the tour.

'Why' is straightforward. Technology is rendering physical cash obsolete at speed, in both developed and developing economies. Disrupters with new tools, whether networks, settlement technologies or new forms of money combining both, are itching to replace the ageing and expensive payment processes that have evolved over the last 50 years. The incumbent banks, payment and settlement platforms are now responding to the challenge.

Central banks watch with a mixture of excitement, interest and worry. Not to be left out, they are introducing – or carefully thinking about introducing –

both wholesale and retail central bank digital currencies. There are multiple reasons for this: defending their production, control and supervision of money; enhancing the efficiency of money systems, treasury services, securities and markets; or improving access to money for the unbanked. They are being squeezed by new forms

'Disrupters with new tools, whether networks, settlement technologies or new forms of money combining both, are itching to replace the ageing and expensive payment processes that have evolved over the last 50 years.'

of private money such as stablecoins on the one hand, and contactless payments typically using commercial bank-created money on the other, while the mind-blowing potential of distributed ledger technology, which could upend, decentralise and privatise money entirely, emerges – largely working – from the sandboxes.

'How' is bafflingly hard. CBDC working groups quickly bring forth 'wicked problems'. How can oversight and privacy be reconciled? Our surveys show that key populations don't believe they will. How can they be convinced of the use cases? Should the public

sector set out to thwart a private system they already underpin and which already moves money without wicked problems?

The role that existing payment platforms and commercial banks play in the system is poorly understood by the most radical disrupters. Not only do they facilitate transaction services, they provide an infrastructure for regulating and supervising the movement of money. Others could, too, but the spirit of decentralised finance cuts the other way.

Innovators are working on this gap. Banks also create credit. A digital public money system might shrink them, and therefore constrain their bandwidth to support the economy, unless central banks sought to become direct lenders to the public, which most certainly are not. How would international interoperability work in any new architecture? Who would ultimately govern cross-border wholesale CBDC settlements? And what technology is robust enough to see off ingenious and malign cyberwarriors?

Technologists move fast to come up with answers. DLT and the wholesale financial system inch together. In any event, wholesale and retail consumers are very likely to benefit from faster and cheaper payments, and treasurers from better cash management, assuming new monopolists don't sneak through the revolution.

When? Somewhere between 'already' in some cases, and maybe never in others – which may accelerate important geopolitical shifts. Welcome to the high-stakes future of payments.

Contents

Foreword	5
Introduction	6
Key findings	7



CHAPTER 1: 8

Revolution: the potential role of digital currencies in cross-border payments

If digital currencies are to transform the payments landscape, it will be crucial for both central banks and payment service providers to co-exist in CBDC systems with roles defined for both.

CHAPTER 2: 18

Evolution: upgrading payment infrastructure for the digital age

Technology can drive existing payment rails to create a system fit for future purpose. To what extent depends on several factors.

CHAPTER 3: 28

Wholesale payments: curing the pain points

Corporates are crying out for quicker, cheaper cross-border payments. Banks and fintechs have to work together to make them happen.

CHAPTER 4: 36

Taking tokens into account

In the private sector, tokenised cash solutions for payments networks are already gaining substantial traction and user-bases. Could public sector tokens have a similar or even greater impact?

CHAPTER 5: 48

The road to better remittances

Remittances are a lifeline for the families of millions of migrant workers. Going digital will remove limits on how cheap, fast and convenient they can be.

CHAPTER 6: 62

Cybersecurity: regulation vs innovation

A new emphasis on resilience rather than cybersecurity is a first step but regulators want to go further. Should nascent resilience regulations be strengthened?



Enabling an instant, frictionless future for cross-border payments

Interoperability across technologies, currencies and geographies is key to enabling more inclusive global economies, writes David Watson, chief strategy officer, SWIFT.

THE WORLD IS BECOMING ever more interconnected, intensifying focus on cross-border flows. Add to that the accelerating speed of digitalisation, which is rapidly raising expectations of end customers and even challenging traditional notions of value altogether. From the development of central bank digital currencies and stablecoins, to the need for interaction across payments systems and solutions, the pace and scale of transformation required to meet the demands for the future is vast.

This report touches on the diverse opportunities – and challenges – that are ripe for co-operation and collaboration in the years ahead. It provides rich assessments of new initiatives in payments and, importantly, how the public and private sectors can come together effectively to support and drive innovation. Further, it covers the latest on risks and how they are evolving as new entrants and new ways of transacting reshape the payments ecosystem.

For SWIFT and our global community of over 11,000 banking and securities organisations, market infrastructures and corporate customers in over 200 countries, interoperability is key to the future. Bridging different jurisdictions, currencies, channels, standards and protocols is crucial to empowering the efficient flow of value and creating more inclusive economies. And, to that end, we are delighted to partner



with organisations across the financial industry and beyond, and, through the stewardship of OMFIF, contribute to thought-leadership in support of sustainable, meaningful advancements for the payments system.

We are committed to being a catalyst for fast, frictionless and secure cross-border payments from account to account, anywhere in the world. Working together, the SWIFT community already has significantly accelerated the flow of funds across borders, with most now reaching end beneficiaries in a matter of minutes. And we have a comprehensive strategy to go further, collaborating with central

banks, commercial banks, fintechs and more to tackle remaining frictions. This includes innovating in areas such as ISO 20022 adoption, CBDCs and artificial intelligence to meet the industry's needs for speed, predictability and transparency while maintaining strong guard rails on operational excellence.

Achieving cross-border payments that combine speed and efficiency with security and resiliency requires collaboration and partnership, with consideration for all types of end users at the centre of our coordinated efforts. We look forward to continue partnering with and supporting the community on this journey.

Introduction

Evolution or revolution?

The future of cross-border payments

A new era in cross-border payments is coming and it is coming fast. By Clive Horwood, managing editor, OMFIF.

A senior technology banker working in the transaction services division of a leading global bank describes the journey needed to upgrade the global payments system as similar to the move from Blockbuster to Netflix. Today, it feels like the move from renting videos to streaming movies happened almost overnight, but it took a long time for the transition to happen – even if the final stage of the switch was rapid.

The path of progress in upgrading the costly, slow and cumbersome infrastructure on which much of the global economy depends is at last under way. And not before time.

In particular, cross-border payments – which can involve multiple time zones, regulations and jurisdictions – have long been associated with greater challenges than their domestic equivalents. The G20 has made enhancing cross-border payments a priority, emphasising the role such progress could

‘The path of progress in upgrading the costly, slow and cumbersome infrastructure on which much of the global economy depends is at last under way.’

make in achieving faster, cheaper, more transparent and more inclusive services that would have widespread benefits for citizens and economies worldwide.

Payments sent over the correspondent banking network pass between multiple banks, which can result in delays, high costs and a lack of transparency over the status of individual payments. Inefficiencies can also arise as activities relating to financial crime compliance are often repeated in the payments chain. Data can be truncated as a result of discrepancies between standards and formats. These obstacles can frustrate the customer, with delays over the timings of payments and a lack of clarity over fees.

Some of these challenges were illustrated by a report published by Oliver Wyman and JP Morgan in 2021. It found that in 2020, global corporates spent \$120bn on transaction charges to facilitate cross-border payments, equating to an average fee of \$27 per transaction, excluding foreign exchange costs. The report also found that the average settlement time for cross-border transactions was two to three days.

This is an industry ready for renewal. The roadmap towards a better global system for cross-border payments was laid out in an interim report from the Financial Stability Board, published

in October 2021 after consultation with industry participants. It highlights five key areas: committing to a joint public and private sector vision to enhance cross-border payments; coordinating on regulatory and oversight frameworks; improving existing payments infrastructures and arrangements; increasing data quality and processing by enhancing data and market practices; and exploring the potential role of new payment infrastructures and arrangements, including digital currencies, tokenisation and related technologies.

This will not be easy. Global efforts to establish common frameworks in fragmented markets rarely achieve their goals. You only need to look at the near miss of the Basel protocols for the banking industry, or the still-nascent attempts to bring global standards to the collection and use of data, to see this.

This report examines the best way to bring about a global cross-border payments system fit for the digital age. There appear to be two routes towards it: evolution, through the transformative upgrading of existing infrastructure; or revolution, a great leap forward through the adoption of digital currencies, tokenisation and related technologies.

The likelihood is that these two paths will run together. Industry players have worked hard to transform payments infrastructure, including industry bodies such as SWIFT, payments providers like Visa and banks such as JPMorgan. Progress is being made at a pace which suggests a brighter future for payments even if more revolutionary technologies fail to live up to expectations. As the payments technology banker points out, while we now are moving out of the Blockbuster phase, only a few years ago the industry was more akin to analogue television with only a handful of channels available.

However, those same firms are also working closely with central banks and a newer breed of technology companies to explore the potential of central bank digital currencies and stablecoins. Initiatives such as the Partior project, promoted by DBS, JPMorgan and Temasek, and the m-CDBC Bridge created by the BIS Innovation Hub alongside the Hong Kong Monetary Authority and Bank of Thailand (and discussed in more detail in chapter 2 of this report) show how quickly blockchain-related initiatives are coming on stream. Advances in tokenisation should speed up these developments further.

There are major opportunities arising from the re-engineering of global payments infrastructures with the aid of new technologies, but only if public and private sectors work closely together to ensure system interoperability and cross-border regulatory alignment.

Key findings



CBDCs and stablecoins

Central banks have an opportunity to seize the initiative, but a duty to ensure that whatever payment solution becomes dominant, they are still able to fulfil their mandates and preserve stability.



Tokenisation

With the right governance architecture, tokenisation could help combat money-laundering, fraud and terrorist financing, but it may require a trade-off between privacy and oversight.



Infrastructure

Widespread technological innovation in transaction banking has reconfigured front- and back-end parts of the payments system as well as the very rails on which payments move.



Remittances

Global cross-border peer-to-peer standardisation would allow greater competition, cut the cost of remittances and allow policy-makers to share best practice. But this is difficult to achieve given the differing levels of digital and financial development between countries.



Wholesale payments

High-value payments systems are in the process of migrating to ISO 20022 standards, paving the way for richer structured data, more interoperability and better straight-through processing.



Cybersecurity

The infrastructure of the global payments system is 20 years old or more, and comprises legacy components designed long before cybersecurity was a threat. Instead of trying to shore up these systems, policy-makers should consider accepting that it is the underlying infrastructure, rather than the regulations, that should change.

Chapter 1

Revolution: the potential role of digital currencies in cross-border payments

If digital currencies are to transform the payments landscape, it will be crucial for both central banks and payment service providers to co-exist in CBDC systems with roles defined for both. By Rebecca Brace.

DIGITAL CURRENCIES WILL radically shake up the world of payments. The private sector has led the charge thus far, with cryptocurrencies and stablecoins promising instantaneous value transfers across borders and jurisdictions, disintermediating banks and disenfranchising regulators.

No one denies that problems exist in the present cross-border payments network, but the emergence of unregulated private sector digital currency solutions poses serious risks to financial stability.

Policy-makers face a new challenge. If they cannot modernise the cross-border payments network, they risk losing control of the system, outcompeted by solutions designed with no regard for financial stability mandates.

Then there are the benefits. A JPMorgan and Oliver Wyman report published in 2021 said that corporates spent \$120bn on transaction fees in 2020. Reducing these costs opens new avenues for profitable investment and economic growth.

Central banks have an opportunity to seize the initiative, but they have a duty to ensure that whatever payment solution becomes dominant, they are still able to fulfil their mandates and preserve stability.

Central bankers clearly take the issue extremely seriously and are energetically pursuing solutions. Claudine Hurman, director of infrastructures, innovation and

payments at the Banque de France, said at an OMFIF panel that central bank digital currencies are crucial in preserving the anchoring role of central bank money, adding that a 'digital wholesale CBDC could greatly enhance cross-border payments.'

'There are many, many intermediaries in cross-border payments,' continued Hurman. 'It's a really important process for populations, particularly remittances. The time to process the transaction can be drastically reduced if we implement new technologies like CBDCs.'

The financial industry has set out to tackle these challenges in different ways. For one, SWIFT global payments innovation has enabled banks to access real-time tracking, faster payments and more transparency over bank fees.

While these initiatives will no doubt incrementally improve the quality of cross-border settlements, there are certain frictions that are caused by things outside SWIFT's control. Changing the operating hours of bank settlement systems, for example, will likely require the intervention of the public sector.

Dirk Schrade, the Bundesbank's deputy head of payments and settlement systems, said on an OMFIF panel: 'There's a clear need to improve cross-border payments. The other systems are good, and improvements are still occurring, but it will take new technologies to achieve the most ambitious outcomes.'

The Financial Services Board subsequently developed a roadmap for enhancing cross-border payments, focusing on five areas – the fifth of which is to explore the potential of new payment infrastructures and arrangements, such as multilateral platforms, stablecoins and CBDCs.

The rise of CBDCs and stablecoins

CBDCs and stablecoins are both forms of digital currency. A stablecoin is a type of cryptocurrency that is intended to have a stable price by pegging its value to other assets, such as currencies and commodities. As such, they are not subject to the same volatility as other cryptocurrencies such as bitcoin.

Around 200 stablecoins are already either in use or in development, including Tether, True USD, Gemini Dollar and Diem – the latter being a digital coin under development by Meta (formerly Facebook) which was originally announced as Libra in 2019. At this stage, notes Olivier Truquet, blockchain lead, Asia Pacific, at GFT Group, 'The main use case for different currencies such as stablecoins is offshore cryptocurrency investments.'

In October 2021, the FSB published a progress report on the implementation of its high-level recommendations for regulation, supervision and oversight of global stablecoin arrangements. Discussing developments since the publication of the FSB's high-level recommendations in October 2020, the report says that fostering the



soundness of global stablecoins 'is an integral part of the roadmap for enhancing cross-border payments endorsed by the G20 in October 2020.'

Latest CBDC developments

The development of stablecoins is one of the factors that has been credited with prompting central banks to accelerate their work on CBDCs. The term 'CBDC' is understood to mean the virtual form of a country's fiat currency and is sometimes described as a 'virtual banknote' – but there are different types of CBDC, and definitions can vary. A report by Deloitte, 'Are central bank digital currencies the money of tomorrow?', explains that a CBDC is 'envisioned by most to be a new form of digital money with a central bank liability, denominated in an existing unit of account, which serves both as a medium of exchange and a store of value.'

As Sirish Kumar, former chief financial officer for India and Asean at PayPal, observes, 'CBDC systems are at a proof of concept stage. There has been good progress on the convergence of terms and definitions. I also see that groups working on CBDC systems have got an understanding of the existing technologies available.'

CBDCs come in two main categories: retail CBDCs (used by the public for low-value, high-volume payments) and wholesale CBDCs (used by financial intermediaries). While some central banks, such as the People's Bank of China, are focusing on the use of

'Central banks have an opportunity to seize the initiative, but a duty to ensure that whatever payment solution becomes dominant, they are still able to fulfil their mandates and preserve stability.'

CBDCs for retail payments, others, such as Banque de France, are looking at wholesale applications.

As of January 2021, 86% of the world's central banks were engaging in some form of work on CBDCs, according to the Bank for International Settlements. 'The last two years have seen significant process in the design, development and adoption of CBDCs,' says Madhav Soundalgekar, principal solutions consultant at Finastra, noting that over 80 projects around the world are currently in various stages of development. While the Bank of England has not yet decided whether to introduce a CBDC in the UK, a statement published in November noted that it will hold a formal consultation in 2022 on whether to proceed. If so, 'the earliest date for launch of a UK CBDC would be in the second half of the decade.'

China, meanwhile, is the clear leader

in the CBDC space. Progress on the digital yuan, or e-CNY, continues apace, with numerous pilots underway in different cities. While the digital yuan has not yet been officially launched, adoption is progressing rapidly. As of October, 140m people had opened wallets and the digital currency had already been used for transactions worth over \$9.5bn.

So, for many people CBDC is already a fact of life. 'When you go into a regular supermarket, if you have some e-CNY in your e-wallet, you can use it to make your everyday purchases,' says Truquet. 'You just go to the counter and show your quick response code, which is embedded into your e-CNY wallet. And then you can leave with your goods, just like you would if you were using an Alipay or WeChat Pay wallet.'

CBDC, stablecoins and cross-border payments

So how could digital currencies address the current pain points in cross-border payments? There is an argument that by reducing the number of parties needed to settle payments, a stablecoin or CBDC-based system could potentially reduce the costs, time and complexity involved in the process.

Aniko Szombati, chief digital officer at Magyar Nemzeti Bank, the Hungarian central bank, says they are aggressively pursuing this: 'We're exploring all opportunities to participate in international projects. We want to be at the forefront of research on CBDC.'

There's a lot of room for improvement in cross-border payments, helping banks to transact more quickly, cheaply and transparently.'

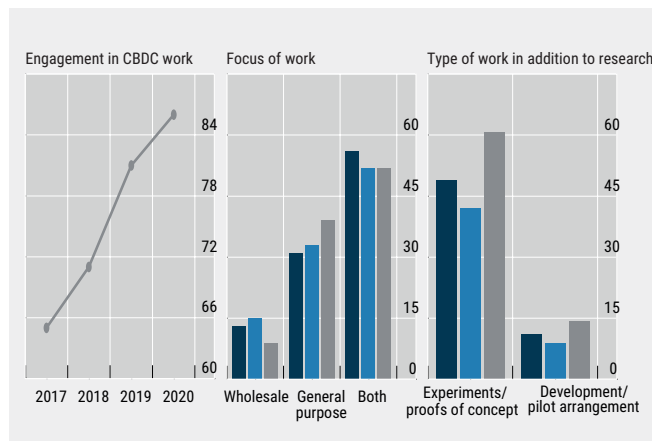
One benefit is that payments are instant, says Sky Guo, CEO and founder of blockchain company Cypherium, which supports interoperability between CBDCs and stablecoins. 'Right now, if a merchant receives a credit card payment, it can take several days to actually receive that,' he says. 'But with digital currency, that process can be made instant.'

Other benefits include a reduction in the risk of counterfeit payments associated with cash, eliminating the need to carry physical cash and the ability to make contactless payments – a feature which Guo says is particularly attractive against the backdrop of the global pandemic.

Tony McLaughlin, managing director, transaction banking at Citi, explains that one issue with settling cross-border payments is that the relevant systems are not open around the clock. 'In other words, if we're making a payment to another country and the real-time gross settlement system isn't on, we can't make that final settlement,' he says. 'To the extent that CBDCs deliver 24/7 central bank money, that will become useful for the participants in cross-border payments, because it will make that central bank asset available around the clock.'

However, McLaughlin warns that CBDCs are not a silver bullet solution where cross-border payments are concerned. 'There are multiple parties in a payment chain, so the central bank being available is just one part of the puzzle,' he says. 'The bank where the beneficiary is also has to be on. If the central bank is on, but the end beneficiary bank isn't, that doesn't solve the issue.'

So, while digital currencies may have the potential to improve cross-border payments, they may not be able to solve all the current challenges. There are also some further obstacles that may need to be overcome along the way. 'At some point, the majority of cross-border payments will be completed in digital currencies,' predicts David Creer, global distributed ledger technology and crypto lead at GFT. 'But I think there's a



1.1. Central banks exploring CBDC projects continues to grow

Share of respondents conducting work on CBDC

Source: International Monetary Fund, Oxford Economics, OMFIF analysis

140m

People who have opened wallets using China's digital yuan

\$9.5bn

Total value of transactions so far that have used the digital yuan

gap at this point in time in terms of knowledge, platforms and skills, and in terms of how to convert and swap digital currencies when you are creating cross-border payments.'

Creer points out that legal and regulatory considerations can present a challenge. 'I think stablecoins will get to the point at which they can be used globally for cross-border payments, to reduce remittance challenges and make cross-border payments faster and more fluid – but they're not quite there yet,' he adds.

Role of stablecoins

Truquet says a key difference between stablecoins and CBDCs is that stablecoins 'will make value available to anybody, regardless of your jurisdiction – and I think that's quite unique.' He comments that if stablecoins are backed by fiat reserves, that will come with regulations. 'But I think it's also interesting to see other kinds of stablecoins, not necessarily backed by fiat currencies, but collateralised or algorithmic stablecoins. Those are really free from any kind of government influence.'

Another consideration around stablecoins, says Creer, is the potential for large tech providers to get involved. 'This kind of stablecoin technology is going to make the act of sending money abroad much more integrated into your social media and your technology accounts – it's going to be a lot easier to set up wallets, compared to what you need today to link an account to PayPal.' In the future, he says, it is likely that big tech companies will have links to stablecoins that will enable them to

access the private tokenisation of cash.

However, McLaughlin notes that stablecoins do not currently fall within the regulatory perimeter: 'They are not currently officially sanctioned legal instruments – and that's going to make them very difficult for banks and other regulatory players to interact with.'

He adds that while the ability to send peer-to-peer payments using a stablecoin might solve the issues associated with cross-border payments, 'it is also very troublesome from a financial crime perspective, and might be used to avoid sanctions, capital controls and foreign exchange controls.' While anti-money laundering monitoring and sanctions checking might be perceived as friction, McLaughlin continues, 'That's not friction – that's making sure that criminals are not using the payment system for money laundering, terrorist financing, ransomware and other forms of financial crime.'

Need for interoperability

Improving cross-border payments is unlikely to be the main driver for embarking on a CBDC project, which tend to be motivated by domestic applications first and foremost. Nevertheless, considerable focus has been placed on the role that CBDCs could play in cross-border payments once they are established.

The need for interoperability is an important consideration. A report by Visa, 'Cross-border payments for Central Bank Digital Currencies via



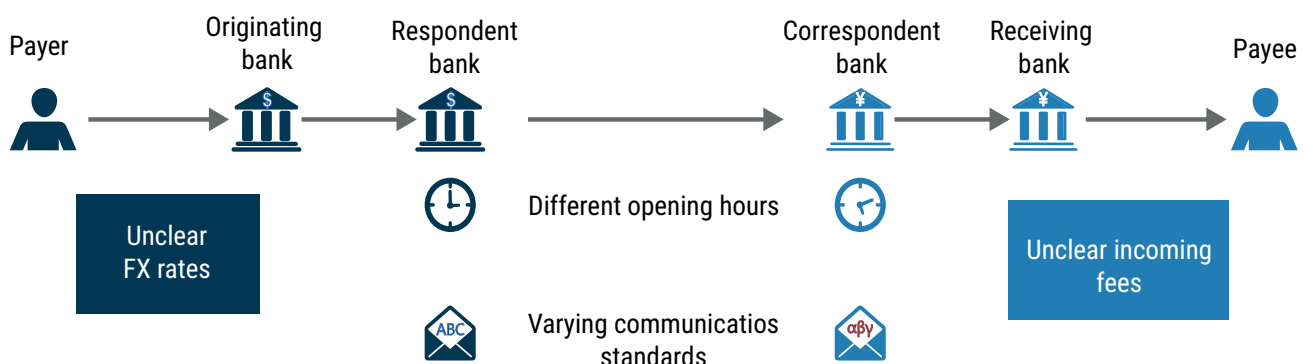
'While digital currencies may have the potential to improve cross-border payments, they may not be able to solve all the current challenges.'

Universal Payment Channels', notes that 'Existing CBDC initiatives involve different motivations, strategies, legislation, regulations, guidelines, and standards.' As such, 'These unique, but ultimately fragmented, CBDC initiatives could significantly impact their interoperability with other CBDC networks.'

Kumar says that while export-orientated economies will be keen to focus on building CBDC systems to cater to the large, untapped market of cross-border payments, 'This will need development of more real-time clearing and settlement systems, and a reduction in the number of parties

1.2. Current correspondent banking methods creates barriers for users

Source: International Monetary Fund, Oxford Economics, OMFIF analysis



involved in settlement processes today.' For two domestic CBDC systems to be interoperable, he says, 'it is important to focus on aligning on regulatory framework – the technical design and standards between two domestic CBDC systems can be addressed as the next priority.'

While interoperability represents a challenge, the potential benefits of a multi-CBDC network could be considerable. Oliver Wyman and JPMorgan's paper, 'Unlocking \$120 Billion Value in Cross-Border Payments', argues that 'A full-scale mCBDC network which facilitates 24/7 real-time, cross-border payments and foreign exchange PvP settlements could save global corporates nearly \$100 billion annually.'

Interoperability could come in different forms, as a paper published by BIS in 2021, 'Multi-CBDC arrangements and the future of cross-border payments', explains. Potential models could include compatible or interlinked CBDC systems, or a single system for mCBDC. The paper notes that each model comes with its own complexities – enhancing compatibility, for example, could lead to choice and competition, but might also result in some of the same challenges associated with traditional cross-border payments. The single system approach, meanwhile, could allow for more operational functionality and efficiency, but also increase governance and control hurdles.

A number of projects and initiatives are currently focusing on CBDC interoperability, including:

- The Multiple CBDC Bridge: A project being developed by BIS Innovation Hub, the Hong Kong Monetary Authority, the Bank of Thailand, the PBoC and the Central Bank of the United Arab Emirates. The project builds on Project Inthanon–LionRock, an initiative to build a common platform for multiple CBDC settlements. According to a report by BIS, the resulting prototype demonstrated 'a substantial improvement in cross-border transfer speed from multiple days to seconds, as well as the potential to reduce several of the core cost components of correspondent banking.'
- Project Dunbar: An initiative



'Improving cross-border payments is unlikely to be the main driver for embarking on a CBDC project, which tend to be motivated by domestic applications first and foremost.'

involving BIS Innovation Hub, the Reserve Bank of Australia, Bank Negara Malaysia, Monetary Authority of Singapore and South African Reserve Bank. The focus of the project is on testing the use of CBDCs for international settlement. As the BIS website explains, 'A multi-currency common settlement platform would enable transacting parties to pay each other in different currencies directly, without the need for intermediaries such as correspondent banks.'

While full interoperability between CBDCs may take time to achieve, other types of initiatives could also gain ground in the meantime. GFT, for example, worked on the Blockbuster IV project run by Deutsche Börse, Deutsche Bundesbank and Germany's finance agency, focusing on securities settlement using distributed ledger technology. 'What was interesting was that they were linking into traditional payment systems,' says Creer. 'So they were using a central bank trigger chain – but that central bank tokenised trigger chain was actually linking into the TARGET2 payment system.'

He adds, 'My hypothesis is that in the interim between wholesale and retail CBDCs taking place, especially

in Europe and America, I think we're going to see more work like this, where traditional payment systems are being used alongside cash on-chain solutions to provide some kind of interim payment services. It's going to be more effective and faster than traditional payment systems – but isn't going to be the full on CBDC centrally issued digital money.'

Other notable developments include Partior, a digital multi-currency payments network being developed by DBS, JPMorgan and Temasek which aims to speed up and reduce the costs of cross-border payments. It follows the results of Project Ubin, which explored the use of blockchain and DLT for the clearing and settlement of payments and securities.

The Oliver Wyman/JPMorgan paper notes that administrative, coordination and policy difficulties could prove to be a hindrance for initiating mCBDC networks at scale. The paper suggests that commercial bank networks such as Partior, and/or hybrid networks with both central bank and commercial bank liquidity, 'could provide more immediate and complementary pathways in a public-private partnership mode to help bootstrap these networks and prove benefits before large-scale adoption by the central banking community.'

Citi, meanwhile, has proposed the concept of a regulated liability network to tokenise regulated liabilities such as central bank money, commercial bank money and electronic money, with partitions for different participants. In this model, CBDCs can be held directly by end users, as well as being used by other RLN participants to settle obligations between each other.

Barriers and concerns

More broadly, a number of concerns and obstacles remain around the role of CBDCs and stablecoins moving forward. 'For stablecoins, I think the biggest hindrance is the regulatory side,' says Guo. 'In the US, for example, the Securities and Exchange Commission thinks stablecoins are still securities – but there's no legal framework.' As such, he says the US is still exploring the correct way to regulate stablecoins, because they carry a credit risk but are not insured by the Federal Deposit

'Other notable developments include Partior, a digital multi-currency payments network being developed by DBS, JP Morgan and Temasek which aims to speed up and reduce the costs of cross-border payments.'

Insurance Corporation. For CBDCs, meanwhile, privacy remains a significant concern – as Guo says, 'people don't want the government to monitor all of their transactions.'

Payments industry expert Ruth Wandhöfer, whose roles include chair of the Payment Systems Regulator Panel, partner at Gauss Ventures and member of the board of advisors at RTGS Global, likewise cites the implications of CBDCs on privacy and anonymity for low-value transactions. Under an account-based CBDC model, she explains, all users hold an account with the central bank. As a consequence, the central bank can see all data relating to CBDC transactions. 'This centralised data source for all flows has to be managed by the central bank, including from a security perspective and from a processing perspective. For me, that's a centralisation risk – if you centralise all the data within a central bank, the latter then becomes a very attractive honeypot in terms of data hacks,' she says.

Being the centralised issuer and processor of CBDC transactions also means that central banks need to weed through data and carry out AML/know-your-customer checks, something normally performed by banks. 'Furthermore, we have to question whether having all data with the central bank is acceptable from a data privacy perspective. If something goes wrong or wrong decisions are taken, you're fully exposed to a centralised digital infrastructure, with no way out.'

A further obstacle where digital currencies are concerned is the lack of clarity over the definition of settlement finality. As such, a consultative report on stablecoin arrangements published by the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions noted that a systemically important stablecoin arrangement should 'clearly define the point at which a transfer on the ledger becomes irrevocable and technical settlement happens and make it transparent whether and to what extent there could be a misalignment between technical settlement and legal finality.'

Finastra's Soundalgekar says other challenges 'will emerge from the

What policy-makers are saying

Regulators speak about digital currencies at OMFIF roundtables

‘Central bank digital currencies are perhaps the most promising area for development in cross-border payments, if only because of the sheer number of projects underway around the world.’

**Denis Beau, Deputy Governor,
Banque de France**



‘CBDC’s beauty is one significant shift: one process for moving money and another for moving assets... merging these two processes is the ultimate beauty of wholesale currency, to do this you need the private sector.’



**Sopnendu Mohanty,
Chief Fintech Officer,
Monetary Authority
of Singapore**

‘Although blockchain has demonstrated efficiency, further work has to be done to stress scalability and security.’

**Claudine Hurman, Director
of Infrastructures,
Innovation and Payments,
Banque de France**



‘While wholesale CBDC is extremely exciting, it has been around for a long time... much of the debate is around an innovation in technology rather than money.’

Tom Mutton, Director of Fintech, Bank of England



monetary value aspect of CBDCs, where CBDCs can be programmed to change value based on market circumstances to control inflation/hyperinflation situations.’ In addition, he points out that in the absence of standards or a global regulatory agreement on the technology supporting CBDCs and stablecoins, ‘consensus and standardisation would be needed to ensure consumers, corporates and central banks have faith in the system.’

Impact on banks and payment providers

Another consideration is the possible impact of CBDCs and stablecoins on banks and traditional payment providers in the future. One risk is that the use of digital currencies could lead to a reduction in transaction volumes and revenues. As Wandhöfer explains, if central banks can directly serve consumers and merchants with CBDCs, ‘you risk suddenly disrupting a whole ecosystem of payment processors and third-party providers that the European Union and our regulators have invited to compete in the market with banks.’

The nature of the challenges may depend to some extent on how traditional payment providers decide to integrate with CBDCs and stablecoins. ‘I think stablecoins can put a lot of pressure on traditional payment providers – and I don’t think many payment providers will be trying to integrate a lot of stablecoins into their systems,’ says Creer. ‘On the other hand, I think that CBDCs are quite interesting for traditional payment providers – and I think those providers are potentially going to be providing rails for payments via CBDCs in the future.’

Consequently, Creer does not believe that current payment systems such as SWIFT, PayPal and Visa and Mastercard will become redundant as a result of CBDCs and tokenisation. ‘I think they will embrace them and integrate them into their systems, and we will see a lot more offerings from them that will integrate with these services,’ he comments.

Catherine Gu, global CBDC lead at Visa, points out that CBDCs present ‘opportunity as well as risk’ to traditional payment providers. ‘From a central bank’s perspective, the first thing they

‘Being the centralised issuer and processor of CBDC transactions also means that central banks need to weed through data and carry out AML/know-your-customer checks, something normally performed by banks.’

need to think about is whether people will switch over to a new form factor of money, which is CBDC, and how easy is it for them to adopt,’ she comments. ‘From this angle, payment providers can provide valuable insights from a user-centric perspective around mass adoption, consumer experience and merchant acceptance, because we’ve been doing this for decades – we have a valuable network and can provide the seamless integration experience for consumers, merchants and governments themselves.’

Erin English, technology policy fellow at the Visa Economic Empowerment Institute, adds that many central banks have contacted Visa as part of their exploration of this topic, both when seeking information for discussion papers and for bilateral conversations about specific areas. ‘Central banks are serious about learning more about CBDC and are very open to outside expertise and insights,’ he observes.

Kumar notes that over the last 10 years, payments service providers

have built strong ecosystems and technologies for identity verification, real-time processing and micro payment capabilities. ‘Central banks will need to leverage and build on those technologies, and partner with private payment providers,’ he says. ‘It is crucial for both central banks and payment service providers to co-exist in CBDC systems with roles defined for both of them.’

Implications for banks

Last but not least, how could the rise of digital currencies impact banks? As author and commentator Chris Skinner points out: ‘If banks no longer manage money – if it’s democratised and decentralised, but issued by central governments directly to citizens and corporates – then what is the role of the bank? Maybe it’s to store the money; maybe it’s to manage digital assets.’

One risk is that if people withdraw some of their bank deposits in order to invest in CBDCs, banks will see a reduction in their deposit funding – and this could, in turn, reduce the credit that banks are able to supply to the real economy. A discussion paper published by the Bank of England in June 2021, ‘New forms of digital money’, cites an illustrative scenario in which, ‘as deposits migrate to new forms of digital money, banks are assumed to restore their liquidity positions, and hence their ability to continue lending, by issuing long-term wholesale debt. Since this is more costly than deposit funding, overall funding costs are assumed to rise.’ Nevertheless, the report notes there is ‘significant uncertainty’ around this illustrative scenario.

But while the rise of digital currencies could have significant implications for financial institutions, the role banks fulfil as regulated entities is not to be underestimated. ‘The question is whether or not money and payments are going to be in the hands of governments and regulated entities in the future,’ says McLaughlin. ‘We firmly believe that money and payments belong in the regulated sector. At the end of the day, money is the prerogative of the nation state and its authorised agents and I don’t see the regulated sector being disintermediated from money and payments.’ ●



Central bank digital currencies could revolutionise cross-border payments

Digital money can reduce risks and deliver benefits for cross-currency transactions, as a joint MAS and Banque de France project found, writes Naveen Mallela, global head of coin systems, Onyx by JP Morgan.

Global corporations move about \$23.5tn across borders every year. Despite this huge volume, the existing wholesale cross-border payments system continues to be challenged on efficiency, costs and transparency. Due to a lack of interoperability between infrastructure in different countries, organisations have to rely on long chains of correspondent banks to execute transactions, resulting in processing delays and accumulated fees. Research by JP Morgan and Oliver Wyman estimated the average cost per transaction at \$27, while settlement times of up to three days are not

'These breakthroughs could solve many of the challenges in the current payments system and make 24/7, real time, cross-border, cross-currency transactions a reality.'

uncommon. In total, approximately \$120bn is spent each year on processing fees. Additional costs also must be factored in, coming from foreign exchange conversions, trapped liquidity and delayed settlements.

Blockchain moves cross-border payments forward

Over the past ten years, there have been huge advances in central bank digital currencies and blockchain technology. These breakthroughs could solve many of the challenges in the current payments system and make 24/7, real time, cross-

border, cross-currency transactions a reality.

In support of this, the Monetary Authority of Singapore and Banque de France worked with JP Morgan's Onyx Coin Systems to create a simulation using a multi-currency central bank digital currency network. This approach could cut out intermediaries and make the system far more efficient and transparent.

The potential benefits of an mCBDC network include:

- **Simultaneous settlement:** With simultaneous settlement, challenges around trapped liquidity, transparency, Herstatt (or cross-currency settlement) risk, settlement risk and settlement delays will be mitigated.
- **'Always on' infrastructure:** Transactions can be executed on a 24/7 basis without cut-off times, helping to support regional and global currency flows.
- **Short transaction chains:** By reducing the number of intermediaries, transactions can be completed much more quickly, while transaction fees and liquidity requirements are reduced.
- **Prevalidation:** Transactions can be screened and checked before they are sent, reducing errors and improving regulatory oversight.

The BdF/MAS simulation was executed on Consensus Quorum, a permissioned fork of the Ethereum blockchain. Consensus Quorum supports smart contracts, which means that payment and settlement functions can be codified into a programme that executes them

automatically once certain conditions are met.

The simulation focused on cross-border and cross-currency transactions for the Singapore dollar CBDC and euro CBDC and resulted in a number of interesting findings.

- Efficiency: The simulation demonstrated that the

‘One drawback of an mCBDC network is that CBDCs may not be available for all countries or currencies.’

number of correspondent banking parties involved in a cross-border payment chain could be reduced, which may help reduce costs associated with increased intermediaries.

- Foreign exchange: The use of automated market-makers and liquidity pools could be a viable alternative to traditional order book infrastructure for foreign exchange.
- Visibility: The mCBDC network provided MAS and BdF with full visibility over cross-border payments using their CBDCs while retaining control over issuance and distribution.
- Interoperability: The simulation demonstrated interoperability across different types of public and private cloud infrastructures in both Singapore and France.

Moving beyond CBDCs

One drawback of an mCBDC network is that CBDCs may not be available for all countries or currencies. In this scenario another option would be

a multi-currency digital corridor network based on commercial bank money, rather than central bank money. The set up would be similar to an mCBDC with the main exception being that a commercial bank, rather than the central bank, assumes the role of settlement institution.

One such example of an mDCN is Partior – a joint venture between JP Morgan, DBS and Temasek that focuses on US and Singapore dollar transactions. Under this arrangement, the US dollar settlement services are completed by JP Morgan, while DBS undertakes the Singapore dollar component.

In addition, it is possible to build a hybrid model where liquidity in one currency is provided by a central bank, while liquidity in another is provided

‘Due to the administrative and procedural difficulties of on-boarding multiple central banks, networks like Partior or hybrid mCBDC/mDCN models may prove easier to set up and scale in the short term.’

by a commercial bank. Due to the administrative and procedural difficulties of on-boarding multiple central banks, networks like Partior or hybrid mCBDC/mDCN models may prove easier to set up and scale in the short term.

Whatever model wins out, CBDCs offer the potential to provide the type of fast, seamless and scalable cross-border payments that organisations are searching for.

Chapter 2

Evolution: upgrading payment infrastructure for the digital age

Technology can drive existing payment rails to create a system fit for future purpose. Large parts of the infrastructure have already been reconfigured. By Kanika Saigal.

CASH IS LOSING its touch. Slowly, we are ditching coins and paper money in favour of digital and electronic alternatives that allow us to make payments at the touch of a screen. Proponents of cashlessness argue that these new types of transactions are cheaper and more transparent, given the digital trail these types of transactions leave behind.

And while cashless transactions are convenient, there are also several potential social and economic benefits associated with them. According to the Financial Stability Board, cashless transactions spur economic growth, support international trade, drive global development and boost financial inclusion.

'But for electronic payments to provide a genuine alternative to cash, the value of the funds needs to be available immediately,' says George Evers, senior vice president, solutions development, Mastercard. 'Arguably, instant payments have been the biggest driver for change in the payments landscape to date.'

In an age of instant gratification, consumers expect their payments and transactions to be made immediately. And while instant payments may be convenient for individual consumers and small firms, they can have much broader ramifications for business. Depending on the size and type of company in question, instant settlement of payments may mean the difference between a successful,

smooth-running business and going under.

Real-time gross settlements – a system that allows for the instant transfer of money and securities and is usually run by a country's central bank – improves cash flow, makes it easier for businesses to manage funds, reduces late payments and speeds up the payment of invoices. Initiating, clearing and settling transactions are carried out in seconds, in contrast to intermittent batch settlements.

The move towards instant payments in retail and wholesale banking is driven by need and convenience, but it is made possible by technology. Widespread technological innovation in transaction banking has reconfigured front- and back-end parts of the payment system as well as the very rails on which payments move. As a result, new payment gateways, systems and currencies have come to fruition and transformed how we transact.

Stability

But the stability and momentum of this transition relies on the ever-evolving network of payments itself. Given the number of stakeholders involved – from both the private and public sectors, sometimes working in silos, sometimes using different technology and often at different stages of technological development – the current payment landscape is complicated. Indeed, the lack of interoperability and integration means high fees and payment delays –

the fundamental problem that payment providers aim to solve.

Muddying the water further are the countless, sometimes contradictory rules and regulations that exist between jurisdictions. This has limited the growth and adoption of instant cross-border payments, especially when they require settlement in different currencies.

When putting together recommendations for the standardisation of cross-border payments, the FSB takes into account not just the underlying payments infrastructure but 'international standards and guidance, national and regional data frameworks, operating hours of and access to payment systems, common elements of service level agreements/schemes, the use of payment-versus-payment mechanisms, the interlinking of payment systems and central bank digital currency design to provide a strong basis and guide for the operational improvements to come.'

But should interoperability be the end goal? 'We typically talk about interoperability in terms of technical interoperability, network interoperability and regulatory interoperability,' says Chad Harper, global payments fellow at the Visa Economic Empowerment Institute.

'Because regulatory interoperability, done well, enables the other two types, it is perhaps the most important to make progress on. Discussions of interoperability can sometimes turn



into recommendations for uniformity and rigidity, and we believe this can stifle innovation. Every time our search for interoperability lands us in a place where we think one platform/one route is the answer, we should turn back because we could be damaging resilience by introducing possible single points of failure.'

As Mark McNulty, head of payments and receivables for Europe, the Middle East and Africa at Citi says: 'While payments can be involved and complex, these complexities shouldn't impact the user. We need to ensure that their overall experience is seamless.'

Faster payments

Launched in 2008, the UK's Faster Payments Service – which enables mobile, internet, telephone and standing order payments to move quickly and securely between UK bank accounts, 24 hours a day – has grown exponentially. Usually carried out within minutes, faster payments can take up to 24 hours to settle but are becoming increasingly instant as technology and regulation evolves.

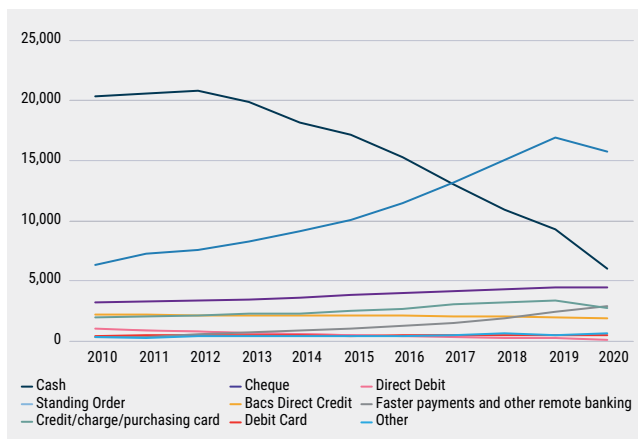
There are several other payment schemes available in the UK. There is the Clearing House Automated Payment System, which is used for retail and wholesale high value payments and are usually settled immediately, and the Banker's Automated Clearing Services. BACS is a much older system, dating back to the 1960s, and is used for bank transfers within the UK, including direct

'The move towards instant payments in retail and wholesale banking is driven by need and convenience, but it is made possible by technology.'

debits. Most people receive their salary via a BACS payment and it can take a couple of days for it to settle.

In retail banking, faster payment systems are gaining ground in several jurisdictions. In 2014, there were 14 faster payment schemes across the globe. Now, there are close to 50. The Unified Payment Interface, India's instant, real-time payment system developed by National Payments Corporation of India, launched in 2016. Demonetisation in India in the same year, where INR500 (\$6.71) and INR1,000 banknotes were withdrawn from circulation, drove up digital payment uptake in the country. In June 2021, UPI providers recorded a total of 2.8bn digital payment transactions, worth in total over INR5tn.

In 2012, Bankgirot, a Swedish clearing system, established BiR, a real-time settlement system for mobile



2.1 Debit cards overtake cash as most popular payment method

Number of payments using selected methods, m

Source: UK Finance



payments. Europe has TIPS, or TARGET Instant Payment Settlement, based on the single euro payments area, to facilitate real-time cross-border payments in euro. In Singapore, 15 banks and three non-bank financial institutions are signed up to PayNow, the city-state's version of real-time payments. PayNow's remit has extended to serve corporates as well as retail customers.

Australia's New Payment's Platform began operations in February 2018. In Brazil, the central bank launched PIX in December 2020 to allow for round the clock settlements. In Canada, the Real-time Payments Rail is due to launch in 2022. Peru, Indonesia, New Zealand and Colombia are also poised to launch instant payment systems in the next few years.

Instant payment systems across the globe work alongside some of the more traditional and slower systems that already exist. But 'we increasingly expect all payments to be instant and frictionless,' says Harry Newman, head of banking strategy, EMEA, at SWIFT, the global messaging system used by banks and financial institutions to send

and receive information, such as money transfer instructions, across borders securely.

'Domestically, this is much easier to achieve. Internationally, the payments industry is continuously evolving and adapting so that it can offer the same instant, seamless service,' he says.

As well as the domestic-international divide, the wholesale settlement system has lagged behind retail. 'The retail space has changed dramatically in the last few years and instant domestic payments are the norm. But the wholesale club hasn't evolved in step, and this is having a detrimental impact on cross-border payments,' says Dave Sissens, chief executive officer of RTGS.global, a cross-border liquidity network for banks that locks in and transfers liquidity ownership in real-time.

There are a number of reasons for this. An industry that has already seen profitability in decline may not have the breathing space to invest in change, existing fees on cross-border transactions may remain attractive to some players in payments or, lumbered with legacy infrastructure, banks may

not be able to adapt to more efficient cross-border payment methods.

But the roll out of open banking in the UK and similar initiatives around the world has led to the emergence of new players jostling for a piece of the growing payments sector. With rising competition, banks are having to adapt.

Open banking

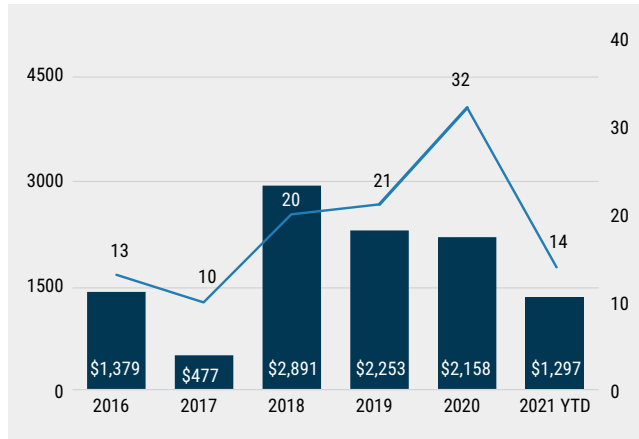
Open banking is a way to offer regulated companies secure and limited access to an individual’s financial data so that they can offer services that may be beneficial to the end user. It also means that, with permission, companies can take payments and access data directly from a customer’s bank account. Open banking is usually served by application programme interfaces, a software intermediary which allows two separate applications to share information easily and securely without having to leverage each other’s infrastructure or software.

Similar to open banking in the UK, the EU launched its second payment services directive in 2016, the HKMA issued an open API framework in 2018 and, in Australia, the consumer data right – a data policy initiative as opposed to a financial services one – will allow consumers to share their data with whichever authorised third party they choose. Other initiatives, such as those in India, Japan, Singapore and South Korea, are being driven by the market, as opposed to being implemented by regulators.

Open banking and its international iterations have thrown open the payments landscape as banks, fintechs and API developers leverage the latest technology to win over business. Competition has driven costs down for retail customers. Wholesale customers are increasingly looking at how they can replicate retail banking services for corporate clients.

As competition in payments heats up, there have been a number of key mergers and acquisitions in the sector involving new banks, fintechs, API developers and established banks looking to access technology that enhances payment gateways, point of sales, e-wallets and buy now, pay later schemes – all of which benefit the user.

In June 2019, PayPal bought point of



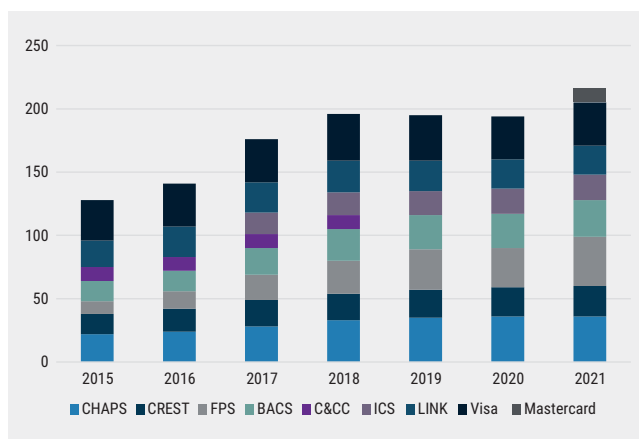
2.3 Big tech pushes into fintech

Total disclosed fintech funding involving participation from big tech venture funds, \$m (LHS), deal count (RHS)
Source: CB Insights

‘An industry that has already seen profitability in decline may not have the breathing space to invest in change.’

sale company iZettle for \$2.2bn. In July of the same year, tech company FIS acquired payment processing company WorldPay – one of the UK’s leading payment providers for small- and medium-sized enterprises – for \$43bn. In 2020, European payments solution company Worldline merged with Ingenico Group. The deal will combine Worldline’s coverage of the payment value chain and expertise in cross-border payments with Ingenico’s global exposure to online commerce.

In May 2021, payment processing company Stripe bought fraud prevention company Bouncer and, in June, Italian payment rivals Nets and Nexi merged to create one of the largest payments companies in Europe. In the same month, Deutsche Bank announced a joint venture with payments platform Fiserv and in September the bank acquired Berlin-based online payment processing company Better Payment. Also in September, digital payments company Square acquired Australian buy now,



2.4 Participation grows across a diverse set of payments systems

Settlement participants per payments system
Source: Bank of England



\$197

Canada boasts the highest contactless payment limit in the world

From cash to cashless

Ten years ago, cash was the most used method for transacting in the UK. For large transactions, cheques were a widely accepted and viable alternative. Businesses relied on slow and expensive interbank systems, such as CHAPS and BACS, for payments to settle.

Meanwhile, the strategy for the payments industry in the UK was being set by the Payments Council, the industry's self-regulating organisation, in a way that the Treasury believed 'did not give sufficient regard to consumer and business outcomes'.

Now, cheques are almost obsolete, cards are the most used payment method and contactless card and mobile payments are on the rise. As the Covid-19 pandemic took hold, stay at home and social distancing orders accelerated the adoption of digital payment methods.

In April 2020, the industry increased the spending limit on an individual contactless card payments from £30 to £45. Meanwhile, the UK's Faster Payments System – a nascent concept in 2010 – processed nearly 3bn payments throughout the year.

Between 2019 and 2020, the number of contactless payments made in the UK rose by 12% and accounted for 9.6bn transactions, or 27% of the total. This was up from 7% in 2016. The share of cash payments in the UK fell to just 14.6% in 2019 from 32.7% in 2010 and 50.5% in 2000. Today, paying for something in cash in one of the UK's high street shops is rare.

Facilitated by electronic payments, e-commerce sales have exploded. In 2019, 13.6% of total global retail sales were made online. By the end of 2021, that number is expected to reach 19.5% – a 45.8% increase in market share in just two years. By 2024, online retail sales are expected to reach \$6.39tn, accounting for around 21.8% of total retail sales globally.

The move away from cash towards electronic payments is not just a trend found in the UK. In Hong Kong, four out of five people above the age of 15 have a debit card. Canada has the highest contactless payment limits in the world at CAD\$250 (\$197). In Sweden, there are less than 32 ATMs for every 100,000 people in the country.

pay later company Afterpay.

As companies scramble to close deals that complement their existing offerings and networks, others – especially the larger banks and technology companies – are investing in innovation hubs and incubators. Level39 is one of Europe's largest technology accelerators, specialising in finance, retail and cyber-security. It was the starting point for Revolut, the UK's most valuable tech start-up. Fintech Innovation Lab offers a 12-week programme in London, Dublin, Hong Kong and New York run by Accenture to help start-ups refine and test their value proposition. Barclays, Citi, ING and a number of other financial institutions have also set up their own programmes with innovation sitting at the top of the transaction banking agenda.

But while all these payment companies have developed their own niche, most have one thing in common: they understand that most of these services need to be instant.

Language

Providing cross-border, multi-currency payments is complex. These types of payments must consider cross-border governance, different laws, diverging anti-money laundering regulations, foreign exchange conversion and liquidity management in foreign currencies, among other things. It is one of the reasons why, until recently, unassuming holiday goers would find that their credit cards had been cancelled or would receive a call from their bank referencing suspicious payment activity while abroad.

'If the end goal is standardisation and interoperability between payment systems, one way to do this is for payments to speak the same language,' says Newman from SWIFT.

SWIFT is innovating to make cross-border transactions much more efficient. SWIFT gpi, launched in 2017, provides complete end-to-end transparency around cross-border payments for corporates. The majority of payments on SWIFT, for example, move across SWIFT gpi. 100% of gpi payments are completed within 24 hours and 40% of payments are credited to the end beneficiary within five minutes. SWIFT's latest

development, SWIFT Go, is a product like gpi but in the person-to-person space, which provides consumers and SMEs with a frictionless and inexpensive service for small cross-border payments.

As is the case with other ISO standards, ISO 20022 creates a common payment processing language, which enables cheaper, faster and more secure payment processing. Launched in 2004, ISO 20022 has now become the data standard for financial messaging and has been accepted by major central banks and payment providers around the world.

Almost 200 market infrastructure-driven initiatives are either using ISO 20022 – including SWIFT – or are considering adopting the standard. The UK and US are predicted to adopt the standard in 2022 and 2023 respectively. Once globally adopted, ISO 20022 should lead to standardisation in cross-border payments and support interoperability between payment platforms globally.

‘En masse migration to ISO 20022 is huge,’ says McNulty. ‘It is spurring a great amount of change in payments, as new and enhanced messaging standards inevitably create a superior client experience. The migration of both domestic and cross-border infrastructures to ISO 20022 will bring the customer a much more standardised experience – regardless of the nature of their payment – and will enhance the overall resilience of the ecosystem as it facilitates much greater interoperability.’

But there may be some teething problems. ‘While ISO 20022 is considered the global standard in payments messaging, I have already heard how some institutions and financial services companies are adopting the standard in different ways – in complete contradiction to why it was introduced,’ says Sissens.

‘Ensuring a consistent adoption of the new standards is critical to the interoperability of systems in the future,’ he says.

RTGS

SWIFT and ISO focus more on the language used to facilitate cross-border payments as opposed to the



‘Once globally adopted, ISO 20022 should lead to standardisation in cross-border payments and support interoperability between payment platforms globally.’

payments themselves. This is because settling payments cross-border and in different currencies is a much more complicated business, where protectionist policies and foreign exchange conversion can become difficult to navigate.

Multi-currency RTGS systems do exist but are rare. In April 2020, the European Central Bank and Sweden’s central bank, Sveriges Riksbank, agreed to allow the settlement of electronic payments in Swedish krona on TIPS. The Directo a México, set up in 2005, came about to facilitate remittances from the US to Mexico and links the Federal Reserve’s automated clearing house (FedACH) with the Mexican RTGS system to allow dollar-peso payments.

Through its regional payments system, AFAQ, the Gulf Co-operation Council’s RTGS system will offer a regional payment system connecting the domestic RTGS payment systems of the six GCC countries, facilitating the efficient delivery of intra-GCC payments.

Launched by the Arab Monetary Fund in February 2020, Buna is a multicurrency payments system that improves the speed, cost and transparency of cross-border payment



\$2.2bn

Big tech invested large amounts in fintechs in 2020

flows in regional and key international currencies. In the Nordic region, P27 is a joint initiative by Danske Bank, Handelsbanken, Nordea, OP Financial Group, SEB and Swedbank, which is looking into how to establish a regional payments infrastructure for domestic and cross-border payments in Nordic currencies and euro.

Indeed, certain jurisdictions may have substantial volumes of payments between domestic financial institutions in one or more foreign currencies. As such, it might make sense to onshore these payments by building an offshore system so it can process payments denominated in a different currency to that of the jurisdiction. This is the case in Hong Kong. The Clearing House Automated Transfer System in Hong Kong is a group of RTGS systems, each of which settles in Hong Kong dollars, dollars, euro and renminbi. It is operated by Hong Kong Interbank Clearing, which is a private entity jointly owned by the HKMA and the Hong Kong Association of Banks.

In the P2P space, the BIS is working on a blueprint for instant cross-border payments by linking domestic instant and/or faster payment systems

internationally through one single platform – Nexus. According to the BIS, Nexus will provide a more scalable way to grow instant cross-border payment networks. In an experimental proof of concept, the BIS Innovation Hub is working with the MAS, Banca d'Italia, Bank Negara Malaysia, BCS in Singapore and PayNet in Malaysia to connect the payment systems of Singapore, Malaysia and the euro area.

'If the rules of the road around cross-border access to domestic instant payments can be harmonised, then they can be scaled up, and will enhance the cross-border payment experience,' says McNulty at Citi.

'At the moment, though, there is not a level playing field which means that while some countries open up their borders to cross-border payments, others don't for various reasons. Enhancing the level of cross-border access to domestic instant payment schemes globally and thus levelling this playing field is key,' he adds.

Perhaps delving deeper into the mechanics of the system should be a first step towards interoperability. 'At the moment, peer-to-peer payments are made possible by liquidity provided

by wholesale banking,' explains Sissens. 'This means that currently, international and domestic instant payments are supported by pre-funded wholesale banking systems that move liquidity in large volumes and value throughout the day. So, while they might look instant to the user, they are in fact supported by large liquidity pools which were moved well in advance.'

He continues: 'Liquidity management becomes even harder given that within one institution, wholesale markets and foreign exchange markets – which are in a continuous buy and sell loop of currency – often work in opposition to one another, so pools of liquidity may not be readily available to settle payments. If we did have more visibility throughout the system, we should be able to create further efficiencies.'

This is what RTGS.global hopes to provide. Using cloud-based technology – specifically through Microsoft's Azure platform – RTGS.global allows wholesale banking partners to lock both sides of the transaction's liquidity and settle payments in a variety of currencies instantly. 'Remittance companies often appear to settle cross-border transactions instantly but in fact there's an awful lot going on behind the scenes,' says Sissens.

And how relevant will RTGS.global's offering be if regional RTGS systems, such as that in the GCC, takes off? 'Right now, we believe it to be more of the same, we will enable the commercial banks, which underpin such services, to more efficiently and more instantly manage their liquidity. We intend to speak with many of these consortiums in due course,' says Sissens.

The push for payments

Big tech firms – with their existing global networks – are emerging as key players in the domestic and cross-border payments landscape. Currently, big tech works within frictionless, closed systems, which makes moving money and information within their networks relatively easy. Moreover, they sit on massive amounts of consumer data that provides them with the tools to tailor financial and payment products to customers, locking them into their burgeoning ecosystems.

Companies, including Facebook, Apple and Tencent, have all been investing in payments and fintech. They are harnessing their customer data to gain ground in financial services. In 2020, investment in fintech companies by big tech hit \$2.2bn. While this marked a 4% drop from the previous year, the number of deals made increased 52% year-on-year, with 32 agreements in total.

Facebook – or Meta as it has rebranded itself – has made a strong push for payments in particular. In August 2020, Facebook announced the creation of Facebook Financial to build a cohesive payments strategy across Facebook, Instagram, WhatsApp and Portal. In May 2021, WhatsApp relaunched its P2P money transfer services in Brazil (after it was blocked by the central bank nearly a year ago). And while Meta's first digital currency idea, Libra, fell by the wayside, the tech giant is taking another stab at it by being involved with a slightly watered-down version, Diem. Novi, Facebook's digital wallet project, will underpin the payment system.

In August 2019, Apple partnered with Goldman Sachs and Mastercard to launch Apple Card and in July 2020, Apple acquired Canadian company Mobeewave, which uses technology to allow merchants to use smartphones as payment terminals. By incorporating Mobeewave's features into Apple Pay, Apple can offer quick payments and transfers using an iPhone. In China, Alipay and WeChat Pay, owned by e-commerce giant Ant Group and tech conglomerate Tencent, respectively, have created a new paradigm with 'super apps' as payments platforms.

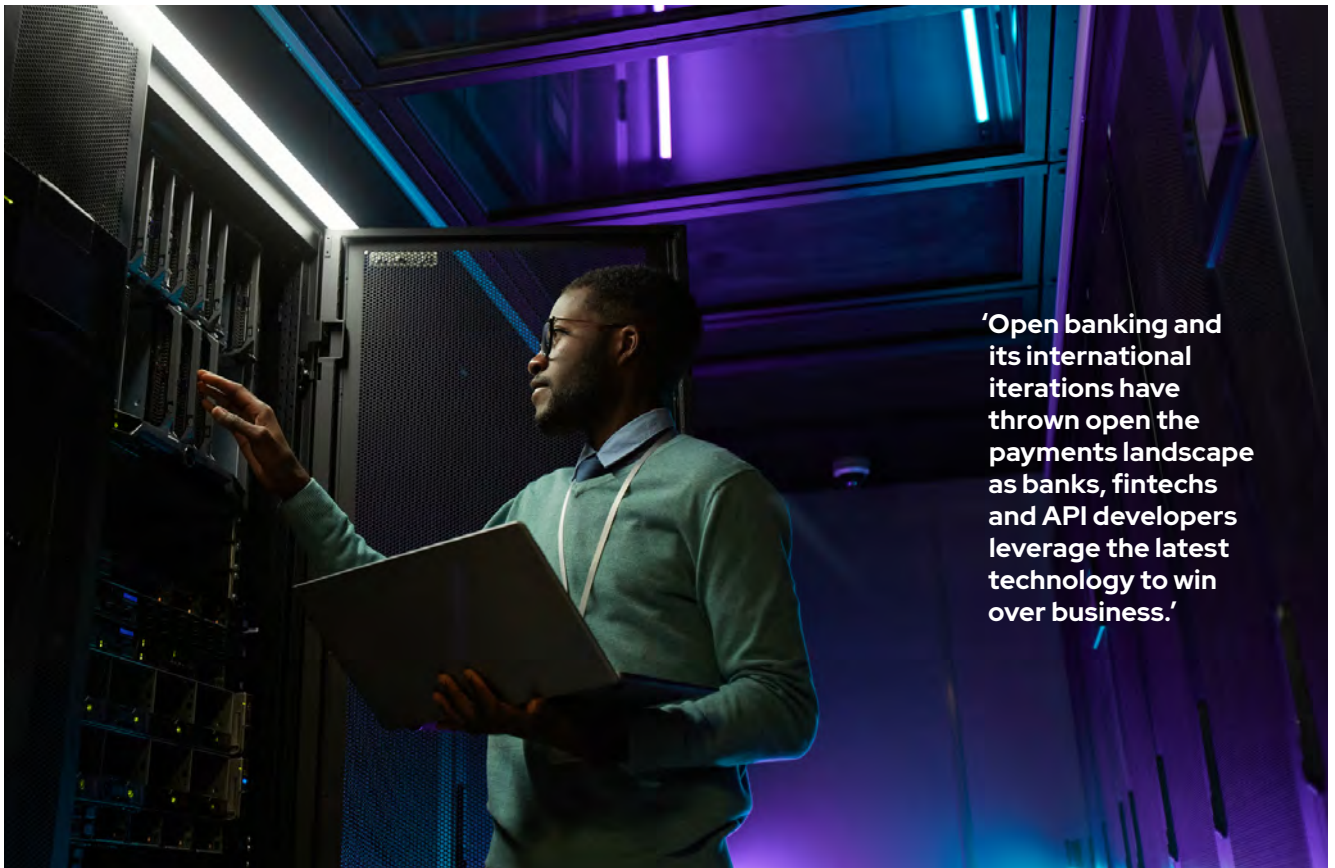
But there has already been some push back against big tech's foray into payments. In September, as China continued to double down on national tech giants in its anti-monopoly drive, Beijing ordered Ant Group to create a separate app for its microloans business. Then in October, an open letter to Facebook's CEO Mark Zuckerberg from Democrat senators in the US stated: 'Facebook cannot be trusted to manage a payment system or digital currency when its existing ability to manage risks and

keep consumers safe has proven wholly insufficient' and 'we urge you to immediately discontinue your Novi pilot and to commit that you will not bring Diem to market.'

As the payment landscape evolves at lightning speed, regulators and policy-makers will need to act fast to ensure the system remains stable, channels are transparent and that frictionless payments benefit the end user.

Indeed, well-established payment providers may have something to learn from big tech as they work towards these goals. As Sissens says: 'In the future, with finance and technology becoming increasingly intertwined, big tech companies have an obvious role to play in the global financial services sector. Without a shadow of a doubt, the public and private sectors must work hand-in-hand to make this future possible.'

'The public sector has an essential role in terms of regulation, compliance, stability and enabling competition. In turn, the private sector will drive innovation. Both sides are just as important.' ●



'Open banking and its international iterations have thrown open the payments landscape as banks, fintechs and API developers leverage the latest technology to win over business.'



Instant and frictionless cross-border payments: interoperability is king

SWIFT's head of banking strategy, Harry Newman, stresses the importance of interoperability in addressing the challenges facing cross-border payments, stating there are no silver bullets.

WHILE PROGRESS has been made in recent years, there are still many challenges facing cross-border payments. The Bank for International Settlements' committee for payments and market infrastructure highlights several key areas to address relating to international transactions. These tend to be expensive, can be slow and suffer from problems of limited access and transparency. The key lies in addressing the underlying issues in a structured way.

'Technology is tremendously important in improving some of these issues,' says Newman, 'but it's not a magic wand. Given the number of countries, each with their own approach, the key is interoperability. The adoption of a common standard, ISO 20022, will be critical and financial institutions need to act collaboratively and innovatively to build solutions that are mutually beneficial to all.'

Compliance, regulatory and data standards

Cross-border payments are inherently more challenging than domestic ones because they move between different jurisdictions with different currencies and varying regulatory and data requirements. They are often faster than many realise – the majority of payments on SWIFT, for example, move across SWIFT gpi which means most are credited to the beneficiary within an hour and very few take longer than one day.

Perhaps paradoxically, cross-border payments spend, on average, 80% of their transit time in the receiving country. Cross-border payments also use domestic systems to reach their end point much of the time; that's how the industry achieves global reach. Therefore, how the international space

integrates with the domestic is critical.

The issues within that integration are varied – perhaps the biggest reason is the differing controls that many countries exercise, for entirely valid economic reasons. 'This can mean payments end up queued at the border, just like lorries at customs control do,' says Newman. Other issues include differences in operating hours, legacy infrastructure, data inconsistencies and tighter financial crime controls around international payments.

Some of these issues can be resolved with new technology, others less obviously so. The key is to integrate the international and domestic space in a standardised and efficient way.

Many domestic payments systems were developed without much attention to international needs. 'It's only natural that they were built for local needs,' says Newman. 'But the result is that different jurisdictions have different data requirements.

Crossing multiple jurisdictions for cross-border payments can raise major compliance issues because

some domestic solutions aren't equipped to provide the same data as receiving systems expect.'

The fundamental problem is one of interoperability. 'Whatever solution we pursue for cross-border payments,' says Newman, 'it is vitally important that they interoperate to create a global solution rather than be a series of closed loops and digital islands.' Once data consistency between different international systems is achieved, new possibilities emerge, such as cross-border interlinking of the new breed of domestic instant payment schemes, which have aligned on the ISO 20022 standard. SWIFT is involved in several such initiatives,

'The adoption of a common standard, ISO 20022, will be critical and financial institutions need to act collaboratively and innovatively to build solutions that are mutually beneficial to all.'

leveraging its deep understanding of international payments, technology and data standards.

SWIFT is launching a new, more integrated approach to managing cross-border transactions. 'Our new model harnesses a transaction management platform to put the business transaction at the centre,' says Newman. 'This ensures complete, up to date data is available to all transaction participants and unlocks the potential for value-added services to be harnessed by all participants in the transaction.'

CBDCs: exciting, but interoperability is still key

A great many central banks around the world are working to create their own digital currencies – digital versions of central bank cash. CBDCs will require new technology and while they could result in improvements to domestic payment networks, they will not offer any benefits to cross-border payments systems unless they are developed with an eye for international standards.

Newman argues that pursuing interoperability as a foundation will be more successful than attempting to adapt a system later. 'We need everyone to start with that in mind,' he says. 'It needs to be developed as an open solution; retrofitting the international dimension will be very expensive.'

For CBDCs to be useful for international payments, the essential step is again interoperability and adopting an interoperable data standard that has already been defined. 'The versions of ISO 20022 that allow for rich data internationally have been worked out by the industry, so if new systems are designed with this in mind, there should be fewer problems of incompatible data formats,' argues Newman.

CBDC-based payments systems are likely to

be based on different technologies in different jurisdictions. Various distributed ledger technologies are being trialled and some systems will use other technologies. 'This is normal,' said Newman. 'These are choices driven by the goals of each system and no one technology is likely to serve all local needs. DLT, for example, may have advantages in some cases but also has its challenges in terms of scalability and ease of adoption.'

Whether or not CBDCs operate on distributed ledger architecture, fully digital, easily tradable versions of central bank currency under the control of the central bank could produce valuable savings, but only, says Newman, if they are designed to be interoperable from the start.

'CBDCs are a new form of money,' continues Newman. 'It's an important development. To get the most value from them they need to be designed to integrate with other forms of money domestically and be interoperable with other solutions of different design and technology on an international level.'

One of the key experiments

SWIFT's innovation team has run this year is to orchestrate payments across two CBDC solutions (on different DLT technologies) via the new platform and bridge those with an RTGS system. These have been very successful. It is therefore possible, as long as the systems have the necessary rich data and are designed to be open.

Cross-border payments have improved significantly over the past five years, and SWIFT and the financial community continue to evolve and improve the international payments experience. Interoperability is achievable, and frictionless payments from account-to-account, anytime, anywhere in the world, will soon be a reality.

'Our new model harnesses a transaction management platform to put the business transaction at the centre.'

Chapter 3

Wholesale payments: curing the pain points

Corporates are crying out for quicker, cheaper cross-border payments. Banks and fintechs have to work together to make them happen. By Rebecca Brace.

CORPORATE TREASURERS are on a constant mission to look for solutions to long-standing pain points in wholesale payments. These range from a lack of transparency over the status of payments to the need for efficiency and automation. 'What's the one thing I would like to see available today? I want payments to be seamless, to be automated, to be secure, to be transparent,' says Royston Da Costa, assistant group treasurer at plumbing and heating products distributor Ferguson. 'And it's frustrating that we're still talking about this.'

Cross-border payments tend to be particularly problematic. 'The biggest pain point we face is the paperwork involved when making commercial payments across borders to and from "restricted countries", i.e. those where there are currency controls,' explains Mumtaz Dole, director, cash and liquidity management and treasury business partner, Asia-Pacific at sustainable energy solutions company Vestas.

Vestas is present in more than 80 countries, but as it enters more challenging markets, payment processes are becoming more complex. 'Almost all of these complex markets have currency controls that require central bank reporting and/or submission of physical documentation to make payments,' says Dole.

In order to ensure the company can safely pay and receive funds, she adds, 'we have had to undertake a

massive exercise to map out all the individual requirements per restricted country' and introduce extra processes to ensure those requirements are met when payments are made. 'Unfortunately for us this means that we have had to introduce variances to our payment process, some of which are manual,' she continues.

Corporate clients are looking for faster and more transparent payments. The pandemic has led to some significant shifts in companies' payment needs. As Tom Halpin, global head of payments products management at HSBC, observes: 'Whereas treasurers previously sought certainty, transparency and efficiency, now it's all this and more. There is demand for speedy, friction-free payments to meet evolving business needs. Payments are becoming a by-product of business operations rather than an operation in themselves.'

Blurred boundaries

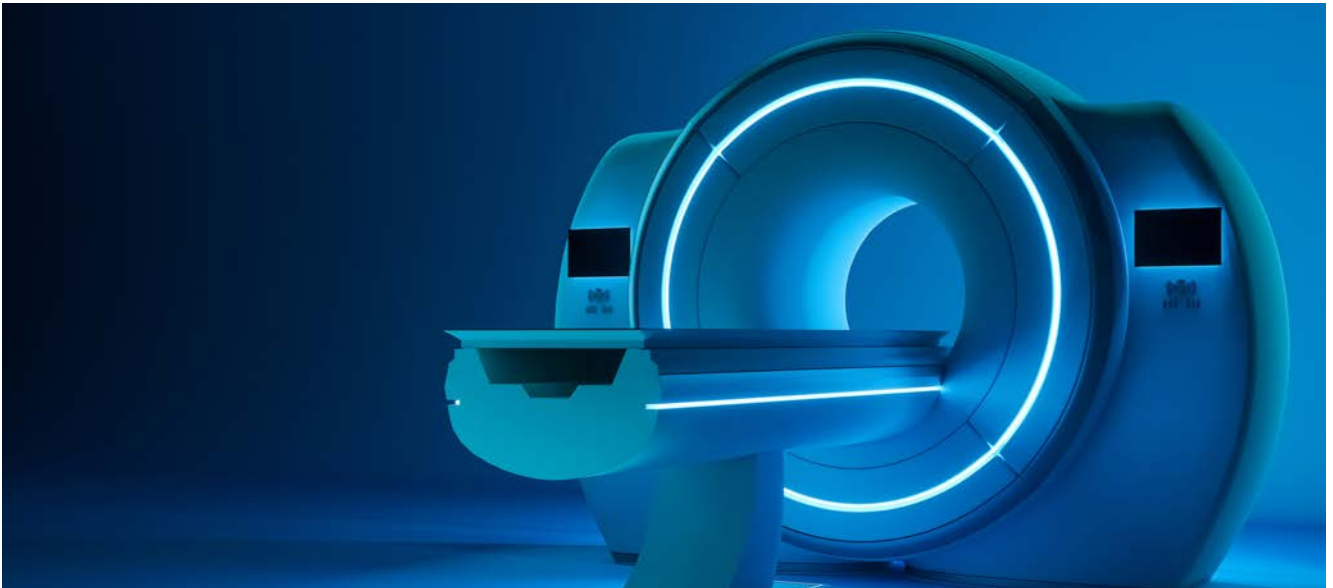
At the same time, companies are facing new challenges. The payments landscape has evolved considerably in recent years. Wholesale payments are no exception.

A 2018 report by Oliver Wyman, 'Wholesale Payments: Disrupt from Within', noted that wholesale payments and cash management generated \$250bn of revenue in 2017. As well as being 'an important source of stable funding for banks' – and an anchor relationship product that provides

opportunities to cross-sell other products – the report also warned that new competitors and technologies have the potential 'to profoundly reshape the industry'.

Since then, the world of wholesale payments has continued to evolve. Developments, including the rise of instant payments, the industry-wide move to the ISO 20022 standard and the impact of open banking, are all playing a part in reshaping this landscape, as is the Covid-19 crisis. A report published in October 2020 by Boston Consulting Group, 'Global Payments 2020: Fast Forward into the Future', noted that most wholesale payment providers would face revenue challenges in 2020 and 2021 'as a result of pandemic-related reductions in trade volumes, business spending and interest income.'

The concept of wholesale payments is itself something of a moving target. 'In my mind, "wholesale payments" is a tricky term,' says Mark McNulty, head of payables and receivables, Europe, the Middle East and Africa, at Citi. He notes that only a small portion of the payments that might fall under this heading fit into the narrowest definition of wholesale payments as business-to-business payments made between financial institutions and 'that definition could become more problematic as we move to the future'. For Citi, he says, 'when we look at what would be traditionally called our wholesale payments business,



we are seeing significant growth and opportunity in business-to-consumer flows and consumer-to-business flows, in addition to the traditional business-to-business flows.’ As a result, he says, the consumer intersection point ‘has become, and will continue to be, a very important lens to apply.’

There are a number of reasons for this increasingly blurred definition. One notable development is the extent to which the pandemic has prompted companies to initiate or speed up a transition to new direct-to-consumer business models. Lockdown conditions, with the closure of bricks-and-mortar stores and the arrival of social distancing, have played a part in prompting companies to embrace e-commerce models and this, in turn, has necessitated the adoption of new payment methods.

Adapting to these new models and methods may require something of a shift in mindset. ‘There are huge changes in the customer payment landscape, particularly for B2C companies,’ comments David Stebbings, director, head of treasury advisory at PricewaterhouseCoopers. ‘For treasurers, it’s important to understand these changes – but treasurers may not be the people who have been traditionally responsible for this area.’

As well as needing to understand the payment methods available, the shift to e-commerce may also mean that companies need to improve

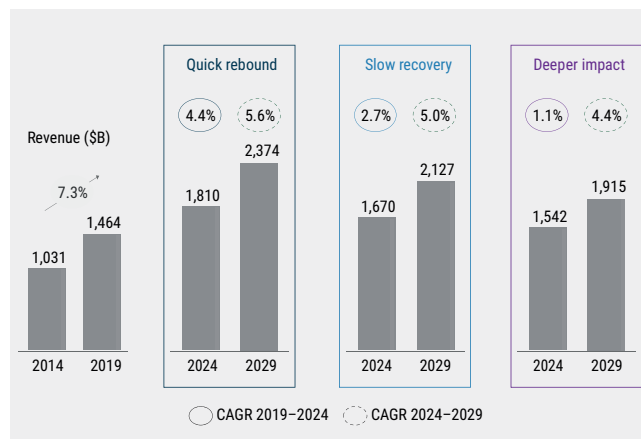
‘The payments landscape has evolved considerably in recent years. Wholesale payments are no exception.’

their order-to-cash processes, so that they can quickly identify when a payment has been made and ship the relevant product. In Europe, this is being facilitated by the single euro payments area direct debit or request-to-pay schemes, explains Bruno Mellado, global head of payments and receivables at BNP Paribas.

‘But internationally, this still needs to evolve – if a French company sells products in Chile, for example, you don’t know when your international payment will hit your account. So it’s important to speed up information about the date that a payment is made, so that you can ship the product.’ He adds that this type of cross-border use case is ‘the major challenge in payments today’.

Visibility and transparency

On one level, treasurers’ requirements



3.1 Wholesale payments set to grow even under pessimistic model

Wholesale payments revenue, %bn

Source: Global Payments Model 2020

are the same as they have always been: the more visibility treasurers have over the status of payments, the better placed they will be to manage cash effectively and make well-informed decisions about funding and investments. But in today's environment, these requirements are increasingly accompanied by an appetite for rapid, frictionless payments, and for more visibility over both the status of payments and the associated fees.

The last few years have brought some progress in this area. One notable development is SWIFT global payments innovation, which was launched in 2017. Among other benefits, the service enables banks to track payments as they progress through the correspondent banking network. Banks can also use it to let clients to track payments.

Mellado describes SWIFT gpi as a 'major evolution in payments', adding that the reason it has made a difference is the number of banks that participate in it: 'It's not the same if you have a super service that is only good for a few banks.' According to SWIFT's website, more than 4,000 financial institutions have signed up to gpi, with more than \$3tn sent over it every day.

However, different banks offer different levels of access to the payment tracking capabilities enabled by gpi, notes Da Costa. 'It's a bit hit and miss,' he says. 'There are some banks that are very much ahead of the game, but not everyone's providing that functionality and that visibility.'

Globalisation and standardisation

Other drivers affecting companies' payment needs include globalisation and the accompanying need for standardisation. 'We're more connected globally, which means that cross-border payments are more commonplace – and there's an expectation that those payments flow across borders as seamlessly as they do domestically,' explains Jacqui Kirk, co-head of product for global transaction services, EMEA, at Bank of America. 'People want to be able to move payments around the world on

3.2 Payments remains most popular bank product area for review

Responses to 'What bank product areas are you reviewing?', %

Source: CGI Banking Transaction Survey 2021

	2020	2021
Payments	72.9%	59.2%
Cash management services	67.7%	56.3%
Foreign exchange (including hedging)	45.1%	39.4%
Liquidity solutions (including pooling/netting)	42.9%	39.4%
Reporting	39.8%	35.2%
Credit/lending	38.3%	31.0%
Payables	34.6%	23.9%
Receivables	33.1%	25.4%
Trade finance (letters of credit, collections)	30.1%	39.4%
Depository services	24.8%	28.2%
Investment banking/capital markets	24.8%	19.7%
Forecasting	24.8%	25.4%
Open account (supply chain financing)	20.3%	21.1%
Other (please specify)	20.3%	2.8%
None of the above	6.8%	9.9%

'One notable development is the extent to which the pandemic has prompted companies to initiate or speed up a transition to new direct-to-consumer business models.'

the same basis, using the same type of payment messaging standards and means of initiation.'

The need for efficiency is another important consideration for companies handling large payment volumes. In practice, companies don't only need to make payments in a timely fashion – they also need to ensure that payments are accompanied by the right kind of data in a structured way, so that payments can be automatically reconciled and applied.

'The devil is in the detail as you look to execute across this new scale of payments – hyper-efficiency is a must for both the client and the provider,' McNulty notes. 'From the foundational things, like rejects and returns rates to the reconciliation of incoming payments, those all have to be super-efficient – or else clients are going to seek alternatives.'

SWIFT and high-value payment clearing systems are in the process of migrating to the ISO 20022 standard, paving the way for richer structured data, more interoperability and more

straight-through processing. This, in turn, will enable banks to operate more efficiently, as well as allowing them to help clients benefit from more efficient compliance and reconciliation processes.

Vestas' Dole sees extensible markup language-based payment solutions as a particularly interesting development. 'At Vestas, we use SAP in-house cash and payment factory to automatically transmit mass payment files using XML directly from our enterprise resource planning to our banks. Subsequently we introduced a robot who runs this process for us daily,' she explains.

Dole adds that this fully automated payment process has brought significant time and resource savings as well as efficiency gains. 'We don't need an army of people keying in payments into online banking portals and more people having to approve these payments and worry about the four-eye principle. We must, however, have a very strict process when it comes to master data maintenance in order to avoid payment fraud.'

Speed and security

Alongside the need for security, another notable driver is the rise of real-time and instant payments. 'If you look at the major platform companies around the world, it's increasingly core to their proposition to be distributing and collecting payments in a very instant way, and as 24/7 as possible,' says McNulty. 'More and more, we are seeing a demand to make those payments to the "platform supplier" on a transaction-by-transaction basis, as opposed to on some sort of daily or weekly schedule. This very real trend to "micro payments" will only continue and be a significant driver of volume growth in the years to come.'

But while there is growing demand for instant payments, there is still more work to do to ensure global consistency – not least because different schemes vary considerably in terms of rules and the payment experience they provide. What's more, not all instant payment systems can be accessed on a cross-border basis.

McNulty comments that the most significant use cases are currently still in the digital native space, 'where

3.3 Cross-border transaction volume, cost and time

Source: WTO, World Trade Statistical Review 2021, UNCTAD, World Investment Report 2021, JP Morgan, Oliver Wyman

20.5tn

Transaction volume

Flows in cross border transactions in 2020

120bn

Transaction cost

(excluding FX costs) spent to facilitate cross-border transactions in 2020 which equates to 1/3 of Singapore's GDP

2-3 days

Settlement time

to clear a cross border transaction on average

you have companies that integrate that instant payment experience very clearly into their overall business model. But we're also seeing more and more interest and a growing set of use cases from traditional corporate customers.' He adds that use cases include activities such as dividend distribution, with companies seeking to distribute dividends through a relevant instant payment scheme.

An important challenge is the need not only to initiate a real-time payment, but also to receive confirmation in real-time that the payment has been completed. If a payment arrives instantly, but the company is not aware of this until six hours later, it will not be able to benefit from the speed of the payment.

Meanwhile, the need for robust security remains a priority. As BoA's Kirk explains, 'As the payments infrastructure becomes more complex and sophisticated, so too does the threat from financial criminals. So, there's a lot of work needed to make sure the whole payments ecosystem remains secure from

fraud, cyberattacks and money laundering.’ Associated with this is the rise of more stringent requirements as regulators work to tackle financial crime and increase transparency over transactions.

Need for integration

For companies looking to take advantage of a wider range of payment methods, consideration needs to be given to how these can be incorporated into existing systems and processes.

‘Offering and accepting more payment methods gives a competitive advantage to a company,’ comments François Masquelier, chair of the Luxembourg Association of Corporate Treasurers. ‘The difficulty lies in the treasurer’s ability to integrate them into existing systems such as treasury management systems and payment factories.’ He adds that new players in the payment market are forcing fragmentation and are multiplying the payment methods available – a development which will complicate treasurers’ lives and ‘force them to automate everything’.

For treasurers, says Masquelier, the challenges presented by the changing payments landscape include difficulties navigating the array of solutions and payment methods available, as well as the lack of standards. He also notes that modern treasury systems need to adapt to accommodate the different payment methods that are emerging – and that emerging solutions will force traditional solutions to adapt.

What treasurers expect, he continues, is a standardisation of methods to avoid a level of complexity that would make their lives impossible. ‘They want secure and fast payment methods – time has become a vital differentiating factor in optimising the financial supply chain. They also want competition between players to put pressure on prices and costs. Finally, they expect TMSs and other IT tools to adapt to the new e-payments, to be able to manage them all through a single platform. Unfortunately, we are still far from these expectations.’

Challenges for banks

So, where do these developments leave banks? As BoA’s Kirk comments, ‘There’s



‘In practice, companies don’t only need to make payments in a timely fashion – they also need to ensure that payments are accompanied by the right kind of data in a structured way.’

just so much to do’. From evolving and innovating to partnering with new players – all while dealing with legacy infrastructure that has been built over a long period of time – banks are tackling multiple challenges as they work to modernise wholesale payments.

Also significant is the potential for new providers to make inroads in this market in the wake of the EU’s revised payment services directive, which has opened up competition to non-bank payment providers. ‘The competitive landscape in payments is intensifying and customer expectations are higher than ever,’ says Halpin. ‘Organisations that are just entering the market are leveraging new and existing payment rails for simple value propositions and, as a result, there is an unprecedented level of choice for consumers as to how to move money.’

Finastra’s Soundalgekar notes

that new providers like Wise, Revolut, Tide and Ripple are creating pressure on banks' fee income, as traditional players previously had a monopoly over corporate balances. He adds that open banking and APIs are enabling new players to provide a seamless customer experience when making or receiving payments. In particular, he says, the use of QR codes and real-time payments is making it simpler for customers to raise invoices and receive payments instantly using the RTP framework.

From competition to collaboration

The role of fintechs in this market continues to be hotly debated. While fintechs have a clear advantage when it comes to harnessing new technology in a more agile way, they lack the scale and extensive relationships that banks bring to the table. As such, treasurers are often cautious about working with fintechs that lack scale and a proven track record. At the same time, payments tend to form part of broader relationships. 'Most of our relationships with financial institutions are underpinned by their balance sheet being open to us for facilities,' explains Da Costa. 'So, we would probably only consider fintech-based payment solutions if those were offered through banks.'

Consequently, the conversation is increasingly about how banks and fintechs can work together. Mellado says that BNP Paribas is collaborating closely with new entrants, which means looking closely at what added value services fintechs can offer and how best to work together. The nature of these collaborations can also vary considerably.

'Sometimes these fintechs end up being our clients in a specific country – they may also become our partner for a specific use case,' he explains. 'Sometimes we are suppliers to them for payments. They are interested in our robust payment infrastructure and security and know-how, which enables them to focus on the front end and the digital journey.'

That said, not all fintech partnerships under consideration can ultimately come to fruition. Last year, BNP Paribas looked at over 80 fintechs and entered into deeper discussions

'For companies looking to take advantage of a wider range of payment methods, consideration needs to be given to how these can be incorporated into existing systems and processes.'

with 35 of them. 'And we ended up working with fewer than 10,' Mellado says. 'We invest in some of them as a minority stakeholder, especially the ones with which we combine our offers, so we can show commitment and take part in their strategic decisions.'

Beyond co-operation between banks and fintechs, other types of collaboration are also important. 'It's only through collaboration that some points of friction can be removed,' says Halpin. 'While banks are competitors with each other, it's vital that they work together to drive common standards which will take cost out of the system and drive a more interoperable system that can be consumed more effectively.' He adds that this is all the more important as more infrastructure and rails come to the fore, such as CBDCs.

The potential benefits of CBDCs were outlined in a recent report by Oliver Wyman and JPMorgan, 'Unlocking \$120 billion in Cross-Border Payments', which found that global corporates spend \$120bn in transaction charges annually due to the cost of wholesale cross-border payments processes. The report argued that a multi-currency CBDC network could 'provide an effective blueprint' to tackle many of the pain points associated with cross-border payments.

Speaking the right language

Banks also need to stay up to date with companies' evolving payment needs and priorities.

Enrico Camerinelli, a strategic adviser at Aite-Novarica Group, says that corporate users are increasingly looking for the ability to run all their operations directly from their ERP or treasury management systems, without having to move from one bank portal to another. 'The first reaction to this is to provide as many APIs as possible, so that users can consume products and services in a more seamless way,' he says. 'But that then requires banks to attract and work more closely with fintechs.'

In this environment, Camerinelli says that banks increasingly need to 'speak the corporate user language' and understand the dynamics of how



'Also significant is the potential for new providers to make inroads in this market in the wake of the European Union's revised payment services directive, which has opened up competition to non-bank payment providers.'

different departments within the organisation interact. 'Treasurers are trying to have a more strategic role within their companies, which means negotiating and talking to other departments – mainly procurement and IT. And so, banks also have to talk to these individuals that have never been the typical counterparts of bank relationship managers.'

What are banks doing?

How are banks adapting their services to evolving payment needs? From optimising customer experience to supporting companies' adoption of e-commerce models, these are some of the key areas of focus.

• Payments as a journey

Ad van der Poel, co-head of product for GTS EMEA at Bank of America, says BoA is designing a payments service that is more tailored towards different types of client to maximise the customer experience. 'We are also looking at payments as a journey,' he says. 'As the payment flows, what are the adjacent services we can offer the client as well as part of the payment? It's a lot more now about data – and even operational data, such as knowing that your payment has been processed and knowing that immediately. Because often that triggers another action or process on the client side.'

Van der Poel also cites the bank's 'open approach' to partnering with different players in the market, as well as the importance of finding a balance between the level of security and the usability of a solution. Kirk adds that BoA engages with industry bodies to talk about how the market is evolving. 'We're active in that dialogue, to help ensure we and the regulators work towards keeping the whole ecosystem safe, as things are evolving so quickly.'

• Collaboration and co-creation

Mellado emphasises the importance of working closely with corporate clients, citing BNP Paribas' treasury board event, which focuses on identifying opportunities for co-creation. He notes that the bank's strengths include the ability to address treasurers' key pain points by following up on feedback and through close relationships with

corporate clients.

‘As a global payments leader, and a cash management leader in Europe, we need to have a strong influence on the agenda in terms of co-operation for better services for business-to-business payments with technology/messaging operators like SWIFT, as well as clearing houses and central banks,’ Mellado adds. ‘That enables us to address the pain points that treasurers are bringing to us through different forms.’

• **Digital transformation**

Halpin says that HSBC is taking a customer-first approach, which means ‘making significant investments in infrastructure, client outreach, digital transformation, upskilling our staff and continuing to hone a culture of innovation to help our clients. Our large footprint means we’re able to share best practices across the globe, as well as harness datasets to provide better insights and services to our clients.’

At the same time, he says, the bank has accelerated its own digital transformation. ‘Our UK digital business banking proposition, HSBC kinetic, has onboarded over 14,000 customers in 2021, while HSBC global wallet, our multi-currency digital wallet which enables customers to pay and receive cash “like a local”, has boosted transaction volumes almost five-fold since it launched in the second quarter.’ The bank has also deployed API capabilities across 31 markets, enabling clients to initiate real-time payments and receive instant payment confirmations.

‘Finally,’ says Halpin, ‘we’ve announced a banking-as-a-service proposition to enable us to distribute products via APIs into third-party platforms, beginning with Oracle NetSuite, the cloud ERP software.’

• **Enabling e-commerce.**

For Citi, meanwhile, key initiatives include the recent launch of spring by Citi, a full stack payment processing solution that allows institutional clients to collect from consumers using a wide range of payment options. ‘In essence, it allows us to be that e-commerce payment collection provider for our clients as they make that shift to

‘While fintechs have a clear advantage when it comes to harnessing new technology in a more agile way, they lack the scale and extensive relationships that banks bring to the table.’

online selling,’ says McNulty. ‘We are building that out in partnership with other major players such as Mastercard from a payment gateway perspective, PPRO for a connection to alternative payment mechanisms and global payments for the cards processing.’

Other areas of focus include continuing to expand the bank’s connections to instant payment schemes, as well as ensuring the continual evolution of system architecture to handle increased volumes in the future. The cross-border space is also a major focus. ‘Historically, our ability to leverage our network across 96 countries to transact cross-border payments is a huge differentiator,’ McNulty says. ‘That continues to be a major focus and differentiator for us. We continue to leverage everything we’re doing in those 96 markets, including access to new instant payment schemes and wallet ecosystems, and wherever possible we’re making sure our cross-border proposition connects into these ecosystems.’

To compete effectively in this market, says Soundalgekar, banks ‘need to focus on digitalising and automating the complete value chain of payments, from order management to settlement and reconciliation, using the ISO 20022 framework.’ This, he says, will enable banks to ‘reduce the cost of processing, monitoring and reporting payments internally and to the regulators.’

He adds that the resulting savings need to be invested in innovations around customer journeys, seamless integration and embedded finance – both to retain customers and, potentially, to offer the new infrastructure to other, smaller banks through the agency framework.

It’s clear that banks are working to harness innovation, partner effectively with fintechs, adapt to real-time payments and meet the needs of companies moving into e-commerce. But while the payments landscape is increasingly complex, treasurers’ priorities remain largely the same as they have always been. As Da Costa comments: ‘It’s not rocket science – payments just need to be fast, accurate, efficient and secure.’ ●

Chapter 4

Taking tokens into account

In the private sector, tokenised cash solutions for payments networks are already gaining substantial traction and user-bases. Could public sector tokens have a similar or even greater impact? By Lewis McLellan.

MANY RETAIL CONSUMERS already experience the reality of digital cash when they buy coffee with a card, phone or watch. Generally, the system is sophisticated enough to prevent you from buying the coffee if you don't have enough money to do so.

Although the plumbing required to facilitate this process is not ideal, the user experience is certainly much better than it is for cross-border payments, where consumers can find themselves waiting two days for funds to arrive and absorbing the high costs required to keep the process afloat.

Should these problems be addressed by facilitating peer-to-peer value transfers, disintermediating a costly and inefficient correspondent banking network? Will banks effectively preserve their status as the dominant providers of international payment networks? Will central banks step in and create their own technological solution?

All three options will almost certainly make use of tokenisation and distributed ledger technology.

The term 'token' has held a variety of meanings over the past few years, depending on the background and ideology of the speaker. That has led to some vagueness about a token's qualities. Is a token programmable? Must a token operate on distributed ledger technology?

In payments, but outside of the cryptocurrency world, tokenisation typically refers to a process of substitution of sensitive data like

credit card information for a pseudo-randomly produced token, which can be shared without compromising the original.

For the purposes of this report, we will be leaving the conventional payment world's definition of tokenisation aside.

Tokenisation, for our purposes, is a form of dematerialisation, creating a digitally tradeable representation of an object. Often, this creates a version of the object where ownership can be transferred and tracked on a distributed ledger.

Within the crypto space, 'token' is something of a catch-all term, including cryptocurrencies like bitcoin and ethereum, as well as tokenised representations of assets – stocks, bonds, digital images, ownership certificates and so on.

The 2021 surge of non-fungible tokens, reflecting ownership of digital art, may be an early indication of what could form the backbone of the economy in Facebook's metaverse. Facebook, now rebranded Meta, Chief Executive Officer Mark Zuckerberg is investing heavily in a plan that seems to involve a marketplace for cosmetic digital assets within the metaverse.

Leaving to one side this burgeoning field of asset tokenisation, the tokenisation of cash – either by central banks or by private sector payment providers – has the goal of improving the efficiency of cross-border payments.

The problems of cross-border payments

The problems of the present cross-border settlement infrastructure are laid out in detail elsewhere in this report. The BIS committee on payments and market infrastructures highlighted four challenges: high cost, low speed, limited access and limited transparency.

Correspondent banking networks do not always share standards of transparency and data formatting. This can lead to manual reconciliation processes, which increase processing time and costs.

Regulators also impose complex compliance requirements, which may differ across jurisdictions.

Many bank settlement systems do not run 24/7. Differences in time zones might mean limited or no overlap in operating hours between correspondent banks, which can result in delays to settlement. Delays don't just slow down transactions. They increase settlement risk, which adds cost in terms of posted collateral.

Banks may also be relying on old systems that can slow down transactions.

These problems are compounded by the fact that direct connections between banks are costly, with some payments requiring multiple intermediaries.

The problems are particularly acute for more exotic currencies, which are rarely served by efficient payments



networks. Delays and volatile exchange rates can drive up transaction fees because of settlement risk.

Tokens versus accounts for compliance

Transparency into the current payments process and oversight to ensure regulatory compliance are both lacking. With the right governance architecture, tokenisation provides an avenue to combat money laundering, fraud and terrorist financing.

Accounts are the dominant representation system underpinning payments networks. They are, as Tony McLaughlin, managing director, transaction banking at Citi puts it, 'an artefact of double-entry bookkeeping'. As a means of keeping track of liabilities, it is an appropriate system. Transactions consist of a message from one bank to another to make a payment, followed by a separate settlement process.

Many digital currencies, bitcoin for example, are token based. This means that the transaction verification process relies on checking the validity of the payment token. With tokens, the transaction process is simpler. 'The functions of messaging and settlement are collapsed into one,' says McLaughlin.

The ability for tokens to carry additional information represents both an opportunity and a danger. Digital currency could potentially offer regulatory authorities greater scrutiny

'In payments, but outside of the cryptocurrency world, tokenisation typically refers to a process of substitution of sensitive data like credit card information for a pseudo-randomly produced token.'

over payments. The degree to which this scrutiny is allowed is an important issue for policy-makers.

The debate is sometimes characterised as 'token versus account'. The centralised payments networks in use today rely on systems of bank accounts, which are only granted when various identity verifications have been conducted.

Despite the relative simplicity of the transaction process, tokens are fundamentally bearer instruments – a structure that has historically carried risk of abuse.

'Often in the literature a distinction is made between account-based systems, requiring the verification of the identity of the payer, and token-based systems, requiring the verification of the validity of the payment instrument. We believe tokens can co-exist with accounts,' said Pietro Grassano, business solutions director at Algorand. 'The vast majority of digital currencies are pseudonymous rather than anonymous. The combination of public key and private key is a way to verify the identity. From the institutions' perspective, I think it's a question of how much [know-your-customer] information we want to require of people to set up a digital currency wallet.'

Even the purest token architecture also involves the verification of identity through public and private keys. This makes bitcoin pseudonymous, rather than anonymous.

And, of course, the purity of bitcoin's architecture is not, in fact, especially popular. Generally, people prefer not to hold their own bitcoin, favouring custody services that can provide convenient platforms for trading and spending, and reduce the risk of losing access to their bitcoin permanently by losing their private key.

Such custody services will, particularly if they are to form the basis of a regulated payments network with mass adoption, almost certainly require users to complete some level of KYC and identity verification, blurring the lines between token-based and account-based payments networks.

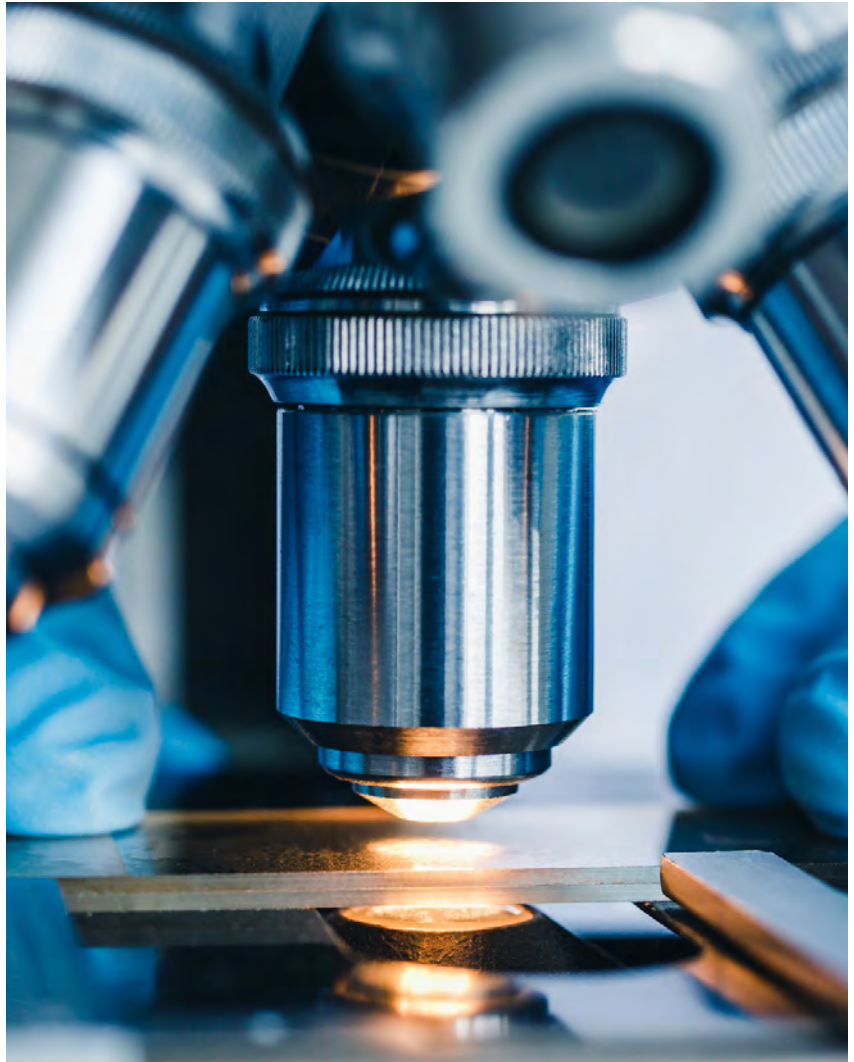
This could result in a hybrid payments network. Consumers would have digital accounts requiring identity verification, but each unit of digital currency would be a token, and therefore capable of carrying its own metadata, affording a greater degree of scrutiny for regulators.

This could give enforcement agencies the opportunity to prevent crime – fraud, money laundering, terrorist financing among others – but it implies a trade-off between privacy and oversight.

'There is a political choice to be made here, not a technical one,' says Grassano. 'How much traceability do we want to build into a decentralised payments network? That might depend on the type of transaction. Regulators might decide they don't need much oversight over small domestic payments. Large, cross-border transactions might merit more scrutiny.'

It is possible to imagine a system where cross-border payments via tokens are subjected to a greater degree of oversight than domestic payments.

Daniel Hardman, principal ecosystem engineer at SICPA, has highlighted that there may not in fact be any need to compromise privacy and regulator oversight. His process, which he calls reciprocal negotiated accountability, gives regulators access to encrypted transaction data, but holds the key to the encryption in escrow. The key is only released under predetermined circumstances – perhaps based on the results of zero-knowledge proof interrogations of the



'Digital currency could potentially offer regulatory authorities greater scrutiny over payments. The degree to which this scrutiny is allowed is an important issue for policy-makers.'

data, which might flag up suspicious transactions.

He believes the range of conditions is versatile enough to be suitable for cross-border payments, when multiple jurisdictional standards might apply.

Solutions for the problems of cross-border payments

There are several possible avenues to alleviate the problems in cross-border payments. The first solution, and intuitively the simplest, would be to attempt to improve the present architecture. Many countries have real-time gross settlement systems that provide high-efficiency domestic inter-bank settlement. Making these systems effectively interoperable could reduce the reliance on the correspondent banking network and lower costs and settlement times.

Second, the private sector could provide a payments network either

based on blockchain or on some other centralised architecture.

Third, central banks could issue digital currencies and co-operate on the establishment of a cross-border settlement network, whether on blockchain or otherwise.

Improving present systems

The committee on payments and market infrastructures drew up a 19-point roadmap for improving cross-border payments in July 2020. Blocks 9-13 outlined ways in which the existing payments infrastructures and arrangements could be improved to support the requirements of the cross-border payments market.

Though improving existing infrastructure might seem easier than developing a new system with new standards from scratch, in fact, many of the same challenges of finding mutually agreeable standards still apply and retrofitting is often more difficult and less effective than starting over.

The ISO 20022 standard is an attempt to develop a single, standardised approach to harmonise the data formats used internationally to reduce problems of incompatibility.

But some argue that even modern RTGS systems are not as reliable as they should be. 'Centralised systems, by definition, have a single point of failure,' says Grassano. 'Decentralised systems are the only way to avoid that issue.'

Target2, the European Central Bank's RTGS system, failed completely for almost eight hours in October 2020. The ECB blamed the outage on a third-party service provider, but Grassano believes that the only way to completely avoid such vulnerabilities is to use a decentralised architecture because the failure of any single point will not bring down the system.

It is worth noting, though, that should the node representing, for example, the UK go down, although the rest of the network might continue to function, that would not be any help to transactions involving the UK.

Private sector tokenisation of cash

Across the world, tokenised cash solutions for payments networks are already gaining substantial traction

'It is possible to imagine a system where cross-border payments via tokens are subjected to a greater degree of oversight than domestic payments.'

and userbases. Some, like China's WeChat and AliPay duopoly, are digital payments networks without distributed ledger technology. Others, like JPMorgan's JPCoin, operate on a blockchain (a private fork of the ethereum blockchain).

Some are payment solutions driven by finance incumbents, including JPMorgan. Others, by new players in technology, particularly in the cryptocurrency space.

Within the latter category sit stablecoins – cryptocurrencies pegged to sovereign fiat currencies. A global stablecoin, of the sort pursued by Meta in its Diem (formerly Libra) project, might ease many of the frictions of cross-border payments and would certainly disintermediate the incumbents, cutting not just correspondent banking networks but banks themselves out of the transaction chain.

However, there are two separate but related problems with this approach. First, a global stablecoin poses risks to financial stability. A globally accessible payments network based on a stablecoin might prove dangerous for small economies, which could see demand for their domestic currencies collapse. The FSB recommends 10 points of regulatory architecture that must be globally agreed to address the potential risks posed by a global stablecoin.

Second, a global stablecoin, by definition, operates beyond the reach of any single jurisdiction. Domestically, a stablecoin could operate as a payments solution under the scrutiny of its national regulator, but without a global body to provide oversight and enforcement, it would be difficult to effectively regulate a private sector global payments network.

Can a global payments network of systemic importance be left to the private sector? Private sector actors exist within jurisdictions under the oversight of national regulators.

These objections formed the basis of some of the objections raised during the House Financial Services Committee hearing on Libra (now Diem).

That does not mean there is no place for private sector involvement. Partior,

CBDC as part of the token economy

Tokenisation has the potential to transform payment methods, minimise the risk of fraud and improve customer trust. It's a topic that everyone's talking about and has implications for the future of payments, writes Raoul Herborg, business lead digital currencies at G+D.

TOKENISATION refers to the process of assigning digital identities to physical (or other) assets. A token is a piece of data that can be used to prove or transfer ownership, and as such it is an electronic bearer instrument. Digitalising an existing asset class through tokens enables the seamless trading of that asset, including exchanging one class of asset for another (such as currency for securities). The use of tokens has the potential to reduce friction in trade and – if available universally – can enable new business models, reducing the reliance on intermediaries.

In combination with central bank digital currencies, tokenisation could revolutionise the future of payments. Central banks have considered a great many critical design features of CBDCs, with resilience and universal access frequently topping the list. In terms of resilience, the design architecture is key.

Moreover, as a digital form of cash, CBDCs ought to be more a means of payment than a means of storage and governments are keen to impose thresholds on how much can be stored, in order to combat money laundering. In terms of universality, a token-based CBDC approach has the potential to help ensure it's a payment method available to all.

Understanding token-based CBDC solutions

It is important to distinguish between the two types of CBDC models. Account-based CBDC models require identity-based accounts for transactions to take place, while a token-based CBDC approach is based on cryptographic key pairs – ensuring high levels of privacy for the user, similar to cash. While account-based technologies can use technical solutions to protect user privacy, fully anonymous transactions are not possible.

Token-based CBDCs would be available to all, accessible to consumers and businesses alike. Offering high levels of privacy, the possibility for seamless offline payments and universal availability, token-based CBDCs can be seen as cash's counterpart in the digital economy. Payments are not redeemed – instead, CBDC tokens are spendable,

just as cash is. Same-currency payments are one transfer of data from sender to recipient, and by their very nature, offer borderless payment solutions.

With G+D Fila[®], G+D has developed a token-based CBDC solution that ensures the highest levels of security, maximum resilience with no single point of failure and the right balance of respecting user privacy and ensuring transparency, through the separation of information, access and systems. It also supports consecutive offline payments, again fostering inclusion.

Tokenisation in cross-border payments

At present, cross-border payments are plagued with challenges. Fragmented data formats, high costs, legacy platforms, compliance difficulties, lack of transparency and lack of inclusion are just some of the issues that have long caused headaches for users looking to make international transactions. A lack of standardisation leads to a lack of interoperability, meaning transaction time is long, costs are high and frustration is amplified. A common standard would help address the issue of interoperability, but how can tokenisation help overcome other challenges?

In terms of cross-border payments, trials have demonstrated that CBDCs could be implemented to help overcome the hurdles of high costs, long transfer times and complex transfer processes. The global use of token-based CBDCs would significantly reduce technical hurdles for a decentralised currency exchange.

Today, currency conversions are a particular hassle. The main challenge is that interbank settlement requires central bank money, and many different parties are involved in the transaction process. As a result, the applicable fees are opaque and the process is inefficient. Currently, fintechs avoid traditional currency conversions in payments by using multiple omnibus accounts in various denominations. CBDCs can solve this challenge too, in another way. By providing one universal payment instrument, a CBDC-based infrastructure would eliminate problems of multiple involved parties. Clearance is immediate, meaning transactions

cannot be reversed, thus ensuring mutual trust and lowering risk, and regardless of transaction volume, the fees and transaction duration would be the same.

In terms of bonds, several banks have successfully tested tokenised securities transactions in delivery versus payment transactions. Atomic swaps allow for quick exchange and can be used to make trades more efficient, reducing the counterparty risk for intermediaries like order matching engines. G+D Filia® has the potential to provide an additional business model for commercial banks, and can support non-currency tokens with wider functionalities.

Underlining new possibilities through legislation

For all of the innovative possibility that tokenisation brings, there is still much to bear in mind. For central banks, the question of design must be considered: should securities and currencies be based on the same token infrastructure? And in terms of securities and CBDCs, legislation remains a challenge.

In January 2020, Liechtenstein's token and trusted technology service provider act was introduced. In summer 2021, the eWpG, the German electronic securities act, went into effect. These are just two initial legislative examples within Europe that enable the trading of tokenised assets, including securities.

Regulatory frameworks for asset tokenisation are materialising and legislation will help to pave the way for a decentralised, token-based economy. The classification of digital assets is one measure necessary for regulation purposes. Not all digital assets are the same and different legislation is necessary for different assets.

The technology's potential is promising, yet acceptance remains one major challenge. If token-based CBDCs are to be widely accepted, they must balance anonymity with transparency. Legislation will help to pave the way to help the widespread adoption of token-based CBDCs. Regulators must remain on

the ball when it comes to evolving technology – with legislation comes stability, integrity, and protection.

Hurdles still to overcome

Besides the need to manage legislation in a timely manner, other challenges remain when it comes to the digitalisation of existing processes. Distributed ledger technology is an innovative infrastructure for recording and transferring tokens, but its performance is not yet sufficient to base an entire country's financial system upon. The infrastructure for asset tokenisation needs further development and DLT is not a strict requirement for this.

Some design questions are still open. How does interoperability work exactly? How can legislation support the introduction of CBDCs and cross-border payments? Central banks will have to find common ground to coordinate efforts and thus ensure compatibility and interoperability.

The other question is how intermediaries would evolve with the introduction of tokenised CBDCs. In our ever digital, ever developing world, adaptation is key to survival. That's why a CBDC infrastructure should open up opportunities for innovation. G+D Filia® focuses on an approach that will ensure CBDC is benefiting consumers, central banks and commercial stakeholders.

In general, the question of acceptance will determine the success of CBDCs and this is where tokenisation offers clear advantages. As a public payment method, CBDCs must be secure and interoperable, offer high levels of privacy and be resilient, thus preserving financial stability. If these design criteria are met, we can look forward to the introduction of tokenised CBDCs as a game changer in the payment world, fostering payment efficiency and representing a viable alternative payment method with many benefits. Cross-border CBDC payments will help promote economic development, making international trade faster, more efficient and less cost-intensive.

Regulatory frameworks for asset tokenisation are materialising and legislation will help to pave the way for a decentralised, token-based economy.

a public-private partnership between JPMorgan, DBS and Temasek with the collaboration of MAS, is an example of a project where the public and private sectors have been able to collaborate.

Public sector tokenisation of cash

CBDCs are perhaps the most promising area for development in cross-border payments, if only because of the sheer number of projects underway around the world.

But individual central banks producing individual tokenised versions of their own currencies will not get us closer to a cross-border payments solution. Interoperability between systems is its own challenge and a great deal of work will be required to ensure that individual CBDCs share enough technical and regulatory ground to ensure that they can operate on a common network for payments.

The Banque de France and MAS, working with JPMorgan's Onyx platform, have successfully demonstrated the technical feasibility of a multi-currency CBDC bridge.

The experiment simulated a number of transactions between fictitious banks in France and Singapore, modelling cross-border and cross-currency transactions.

In one instance, a bank sent euros to another bank, which received an equivalent amount of Singapore dollars provided via a liquidity pool. In another instance, the banks completed a PVP transaction, exchanging euros for an equivalent amount of Singapore dollars directly.

This system is, as yet, only bilateral, but Onyx's report claims that it is structured in such a way that it can be easily scaled to incorporate other central banks and their currencies. Rather than maintaining a network where every participant connects to every other participant, each simply connects to a common platform.

It is worth highlighting that, although central banks are eager to improve cross-border payments and to keep the transaction network in the regulated space, they are not necessarily keen to own the process themselves.

The Bundesbank's Schrade points out that a central bank monopoly over international payments might not be

'Across the world, tokenised cash solutions for payments networks are already gaining substantial traction and userbases.'

'the first, best outcome'. 'There's a clear need to improve cross-border payments, and this will need public intervention. The other systems are good and still developing, but it will be difficult to achieve the most ambitious outcomes like that. Wholesale CBDC might be one way of achieving real-time settlement of transactions across currencies, but I don't think it's the only way.'

Blockchain or centralisation

The excitement around DLT can sometimes blind people to the fact that many of the qualities of an ideal cross-border payments network – one that is cheap, provides instant settlement, is widely accessible and has an appropriate level of privacy and regulatory oversight – can be achieved without the means of a distributed ledger, or might require infrastructure changes beyond the introduction of a distributed ledger.

It is certainly possible to create a blockchain-based solution for many of the problems of speed and cost affecting cross-border payments. However, it is important to identify if a benefit is a consequence of blockchain architecture or whether it could be achieved with modern centralised data architecture.

For example, blockchain settlement systems are sufficiently automated to operate 24 hours a day. Because shared data standards are built into the architecture of blockchains, payments can be processed automatically without the need for manual oversight.

However, this is not something that can only be achieved with blockchain. Any system where all participants are sharing the same data standards and infrastructure could be automated to this degree. Around the clock operation is not a consequence of distributed architecture.

In any case, while such a settlement system would go some way to alleviating these delays, the form of its implementation is important. If the around-the-clock cross-border settlement layer occurs between central banks, then the settlement may still be delayed by commercial bank operating hours.

It's also important to note that some



of the delays in cross-border payments stem not from technical inadequacies, but from political and economic institutions like currency controls. There is no guarantee that DLT would obviate these delays.

Scott Hendry, senior special director of fintech at Bank of Canada, sums it up, saying: 'The fact is that the true advantage of blockchain is not decentralisation; it's centralisation. The big benefits come from getting everyone on a single system. If everyone could agree to use a single payments network provided, for example, by someone like JPMorgan, then that would work just as well.'

Hendry believes that, if the whole world were to access the same platform, we could achieve instantly settled, frictionless transfer of value within a centralised architecture. Even programmability and smart contracts, often touted as benefits only achievable via blockchain architecture, can technically be produced within a centralised context.

'CBDCs are perhaps the most promising area for development in cross-border payments, if only because of the sheer number of projects underway around the world.'

Algorand's Grassano would argue that such a system would be more vulnerable than a decentralised system because of the presence of a single point of failure.

Of course, such a system, while technically possible, would be extremely hard to implement because it would almost certainly require countries to devolve some of their ability to oversee and control their currency to an offshore party.

Hendry, who is otherwise sceptical of the value proposition of digitalised cash on a blockchain, does concede that the decentralised structure might make it easier to get countries to agree to shared standards.

'An mCBDC bridge, if it allows each country to control their currency while being part of a monolithic system, could be easier for central banks to agree on,' he says. 'Decentralisation might be a means of ensuring that each participating central bank feels it has sufficient control and ownership of its country's money to participate.' ●



Five things we learned building a blockchain-based CBDC

CBDCs can create as much value as the internet, if they are designed correctly, writes Co-Pierre Georg, member of the Algorand Foundation's economic advisory committee and associate professor at the University of Cape Town

OVER 80 CENTRAL BANKS, representing more than 90% of global gross domestic product, are currently in various stages of evaluating whether or not they should introduce a central bank digital currency. Among the most exciting projects are those that study whether central banks can open their balance sheets to the broader public. This could be done either with the help of intermediaries or in a hybrid system where balances are held directly at the central bank, but access is facilitated by payment service providers. These retail CBDCs have the potential to completely reshape our existing financial infrastructure. Through our engagement with various central banks, we have identified five common questions and trade-offs.

First, it is paramount that the public trusts the payment instrument unreservedly to ensure it maintains its value as highly as cash. The length to which central banks go to ensure that cash is a universally trusted payment instrument is one of the main reasons why the cost of cash is so high, totalling about 2% of GDP in the euro area, for example. Luckily, counterfeiting a CBDC is not possible on a decentralised blockchain, although additional cybersecurity risks naturally arise for any new digital means of payment. This implies, however, that central banks designing retail CBDCs need to ensure that the nodes validating transactions are properly decentralised. It also implies that centralised digital solutions will always struggle to generate the same level of trust that a highly

It is no coincidence that the majority of respondents in the European Central Bank's digital euro survey named privacy as their number one required feature.

decentralised payment instrument like cash does.

Second, a seamless user experience is key to adoption. It is tempting to think that a retail CBDC can be turned into legal tender by decree. The limits of this approach can be seen in countries like Zimbabwe, where a shadow monetary base withstood all attempts by the government to enforce the legal status of their own notes. Instead, central banks need to ensure that a CBDC is usable by customers and merchants alike. This means near-instant settlement and

interoperability between devices and payment methods. For a medium-sized country with about 50m people who transact on average twice per day this means the blockchain needs to facilitate at least 1,100 transactions per second. During busy shopping days before Christmas, for example, this number easily increases by a factor of five. What seemed like an impossibly tall order only a few years ago is well within reach of modern blockchains, even in a highly decentralised and

resilient setup.

Third, we need to strike a balance between privacy and auditability. It is no coincidence that the majority of respondents in the European Central Bank's digital euro survey named privacy as their number one required feature. Privacy is a non-negotiable feature of any CBDC system if it hopes to gain mainstream adoption. Even if the system does not provide the same level of privacy as cash which, after all, is also not fully and truly anonymous because bank notes can be traced, there are some principles central banks should heed. Chief among these is that a separation of

concerns is a powerful last line of defence.

It is tempting to create a central repository of users' personal information, which has to be collected for know-your-customer compliance, and their wallet addresses on the blockchain. But this would give the central bank the ability to monitor the economic activity of each individual in the country. A better way of organising the system is to ask individual payment service providers to hold the personal data of only a fraction of the total population. This would also ensure that law enforcement agencies can approach individual PSPs and request that the wallet ID of a suspicious owner is revealed or, vice versa, that the owner of a wallet engaged in suspicious activity is revealed.

Fourth, for a payment instrument to be universally accepted and trusted, it needs to be available to everyone in a country. This is a significant challenge for central banks because smartphone penetration is far from universal, even in the US where it stands at about 80%. This is even more the case in emerging markets like India where smartphone penetration sits at around 37%. Consequently, any retail CBDC design must make provisions for users without smartphones. Similarly, CBDCs need to make provisions for users who have intermittent connectivity. During our CBDC journey, Algorand has come up with several ideas for how to facilitate blockchain transactions for users without smartphones and for users faced with

intermittent connectivity.

Fifth, it is paramount to ensure interoperability and facilitate competition. The hardest part of designing new financial infrastructure is developing the protocols and processes in a robust and resilient way that is compatible not just with legacy systems but also with future requirements.

The choice that policy-makers and industry practitioners today face is between an open system like the internet or a walled garden like Facebook. If central banks want to design an

open system, they should spend less time picking commercial solution providers and more time supporting academics and engineers actively involved in designing CBDC protocols. While there are many laudable efforts underway to create protocols and ensure interoperability, we should not forget that it took 25 years to develop the internet to where it was ready for commercial use. Driven

While there are many laudable efforts underway to create protocols and ensure interoperability, we should not forget that it took 25 years to develop the internet to where it was ready for commercial use.

by concerns about competition from private stablecoins, central banks are now trying to achieve a similar task in just a fraction of the time. The design choices policy-makers make today will have far reaching consequences, not only for the future of finance, but for society at large.

If we can resist the temptation to take shortcuts that lead to closed-loop systems, and if we can find the right balance between privacy and auditability, CBDCs have the potential to become the same massive value creation machines as the internet.



Identity-based token blockchain eliminates many of the technology's drawbacks

MetaMUI shows how blockchain's limited volume of transactions per second, as well as other issues, can be overcome, writes Phantom Seokgu Yun, CEO, MetaMUI.

Anonymity is the fundamental characteristic of blockchain. In the anonymous token-based blockchain, every transaction is written based on an anonymous address, derived from the public and private keys of the user. The problem with this approach is that the ownership of an asset is bound to the private key. Proof of ownership can only be provided with the private key.

This means that if a user ever lost their private key, proof of ownership is also lost. If central bank digital currency is implemented this way, users could lose their entire balance.

MetaMUI is the first identity-based token blockchain. While most token technologies follow the design of cryptocurrencies, such as bitcoin, MetaMUI redesigns the blockchain structure based on the concept of identity. The main reason for this is to satisfy the regulatory framework of current financial systems, such as the Financial Action Task Force's travel rule.

If a user's private key is hacked, then there's a problem of ownership. The hacker and the original owner both have the same private key and both can control the account. Users can lose all their assets. There's no way for banks to transfer back stolen assets.

These kinds of problems can be solved with an identity-based token blockchain. MetaMUI's blockchain ledger records transactions using each user's identifier, instead of an address derived from the public key.

The identifier format follows Web3's decentralised identifier (DID) standard. A DID is a simple text string consisting of three parts: the DID uniform resource identifier, the identifier for the DID method and the DID method-specific identifier.

Therefore, it is a globally compatible account address that allows users to send and receive tokens over the internet. Since it is a random identifier and doesn't contain any kind of private information, the level of privacy protection is equal to that of an anonymous token blockchain.

MetaMUI has an identity blockchain that contains a decentralised public key infrastructure. The identity blockchain registers a user's identifier and public

key pair. Since these records are stored in the public permissioned blockchain, all public keys are known to all other users. In MetaMUI, the user still has to sign the transaction to authorise transfers with a private key. The user's authorisation signature can be verified by checking the corresponding public key in the identity blockchain.

If a user lost their private key, they can simply verify their identity and reset the private key in the identity blockchain by re-registering the identifier and public key pair. In this way, the user can relieve the burden of keeping the private key safe and secure. In addition, if hackers steal the private key and illegally transfer funds, it is possible to suspend the account by invalidating the public key of the hacker's account. Also, transferring the stolen asset back is possible by resetting the public key with a bank node-generated public key and initiating the transfer. With an identity-based token blockchain, current banking practice can be emulated in the digital world.

An identity-based token blockchain also solves the CBDC design trilemma, where identity, privacy and programmability cannot be achieved at the same time. Identity-based token blockchain can be used to implement privacy-preserving digital currency. Since MetaMUI uses the identifier of the user to record transactions, the user's private information is never stored on the blockchain. Similarly, privacy-preserving programmable money can be implemented with an identity-based token blockchain. This requires another blockchain technology, allowing smart contracts to run on the edge of the node.

MetaMUI has the meta-blockchain capability to achieve this. Once the decentralised operation of smart contract code is achieved, decentralised machine learning technologies, such as federated learning, can be applied. Private information is processed on the user's device and only the processed metadata can leave the device. User's personal information will never have to go outside of their device. This way, personalised service is achieved without violating privacy.

One of the major problems hindering the use of blockchain technology for CBDCs is how slowly it processes transactions. The fastest anonymous token blockchain, such as Solana, can achieve up to 50,000 transactions per second. Most enterprise token blockchains, however, can only reach 5,000 transactions per second. This would be inadequate for even lightly populated countries. For large nations, such as the US, these numbers are prohibitively small.

This slow performance is due to two major design problems in the protocol and structure of blockchain. Blockchain is structurally decentralised, but from the operational point of view, it is a heavily centralised and serialised system. All the nodes of the blockchain form a single virtual computer that can process the transactions one by one. It cannot process the transactions in parallel, limiting the total number it can handle.

Another problem is the lack of peer-to-peer money transfers. Bitcoin requires the consensus of all participating mining nodes to process transactions. This means there are many decentralised mediators. It is not a true peer-to-peer payment system where the sender and receiver can process and finalise the transaction directly, without intermediation.

With parallel and independent processing of transactions, a true peer-to-peer payment protocol, millions of transactions can be processed per second. MetaMUI is the first blockchain technology that has implemented this true peer-to-peer payment protocol. In MetaMUI, the receiver can verify the sender's signature using the identity blockchain and accept the payment without a mediator. By adding more nodes to process payments in parallel, it is a scalable solution.

Identity-based token blockchain can be used to implement asset tokenisation services. It can solve the oracle problem, where isolated chains cannot read or write information from other networks.

There is a race to find the solution to prove the legal

status of a generated token, information that might sit outside the blockchain. To properly solve this problem, the real-world asset must be connected to the digital token. It could be possible for the token generator to prove the existence of real-world assets with the help of trusted parties such as government organisations.

MetaMUI makes it possible to create a digital ID on the blockchain and issue certificates, called verifiable credentials, that are signed by the issuing entity. The issuer can not only create the token but also issue the certificate to prove the existence of the corresponding real-world asset. Issuers can also get certificates from third-parties with a public identity on the blockchain.

Transfers of tokens also takes place between the sender's identity, the seller, and that of the receiver, the buyer. This identity-based change of possession transfers ownership. With a proper regulatory framework, the need for registering the transfer is gone.

Identity-based token blockchain could transform the non-fungible token market. NFTs represent the ownership of unique irreplaceable assets, such as digital art, in-game items or clips from basketball games. But they cannot be recovered if a user forgets their private

key. Implementing NFTs on an identity-based token blockchain overcomes these difficulties.

As blockchains become more important in the financial system, inheritance becomes a problem. The ownership records of NFTs could disappear forever if a person dies suddenly, without ensuring an executor has access to their private key. If NFTs are implemented on an identity-based token blockchain, however, after appropriate identity verification, bequeathed NFTs can be transferred to their intended new owner.

MetaMUI's identity-based token blockchain innovates major blockchain applications, including CBDCs, NFTs and asset tokenisation. MetaMUI proves that combining decentralised identity with a decentralised token is a powerful concept and could improve banking, the digital asset market and more.

'If the user's private key is hacked, then there's a problem of ownership. The hacker and the original owner both have the same private key and both can control the account.'

Chapter 5

The road to better remittances

Remittances are a lifeline for the families of millions of migrant workers. Going digital will remove limits on how cheap, fast and convenient they can be. By Kanika Saigal.

IN ETHIOPIA, the war in Tigray has displaced 2m people while 400,000 people in the region face famine. The conflict has rippled through the country, spilling into nearby regions in Oromia and Amhara.

Unfortunately, national relief efforts have fallen short. Ethiopia's blanket supplementary feeding programme – the distribution of food to prevent widespread malnutrition – only reaches 40% of the population. Domestically, financial support is limited as the government grapples with the fallout of the Covid-19 pandemic.

Cash transfers have helped plug the financial support gap. Often arranged through non-governmental organisations and supported by international banks, cash transfers are payments made directly to affected populations during humanitarian crises that individuals receive as cash, credited into a mobile wallet or pre-paid debit card.

Remittances – the non-commercial transfer of money from migrant workers to friends and family back home – are another source of financial support.

Around 200m migrant workers across 40 countries transfer money to 800m people in 125 countries. In these countries, cash received via remittances represents, on average, 60% of household income and is spent on essential items such as food, medicines, education and housing expenses. Half of the total value of remittances is received in rural areas, where much

of the population is poor and often unbanked.

Remittances are an important source of income, not just for individuals receiving the funds, but for emerging market countries as a whole. Remittances to low- and middle-income countries in 2020, worth \$540bn, surpassed the equivalent value of foreign direct investment (\$259bn) and overseas development assistance (\$179bn) combined.

Ethiopia receives around \$5bn-\$6bn in remittances each year, largely from the diaspora in the US, Europe and the Middle East. Private, individual transfers, including remittances, are the single most important source of foreign currency for Ethiopia, covering 35% of imports. In 2019, remittance flows to sub-Saharan Africa reached \$48bn, with Nigeria accounting for half the total. Within the same period, Asia received \$315bn in remittances with India accepting the lion's share of about \$80bn. Neither figure considers informal flows of cash, however, which is likely to make the true value of remittances to emerging markets much higher.

Even as the Covid-19 pandemic unfolded, remittances remained resilient. While World Bank estimates suggested that the level of remittances would fall globally by 20% in 2020, instead, remittances declined by just 1.6% to \$540bn. This was largely down to better than expected fiscal stimuli of developed economies, the shift from

physical cash to digital wallets and the move away from informal channels of money transfer to formal ones.

Although remittances support economic development and widen financial inclusion, they face greater challenges than any other type of payment in the peer to peer retail space. All cross-border payments must adhere to regulation set by multiple authorities and apply for relevant licences. Remittances, however, are typically received by people in emerging markets. As a result, they are disproportionately affected by volatile foreign exchange rates, legacy technology and de-risking much more than remittances and cross-border payments sent to developed markets.

Navigating the licencing and regulatory landscape can also be tricky. In some jurisdictions, money transfer operators are required to obtain a licence – for example, a specific money remitter licence or a licence as a bank or payment institution – while in others they are required to enter into an agreement with banks. At the same time, payment infrastructure operators – systems used to settle financial transactions – may not be subject to any licensing requirements, supervision or even oversight, especially if they operate retail payment systems that are not considered to be of systemic importance within a particular jurisdiction.

As such, remittances are usually much more expensive, take longer and



can be much less convenient when compared to other cross-border P2P payments. ‘Remittances provide a lifeline to families struggling to make ends meet,’ says the Visa Economic Empowerment Institute’s Harper.

‘These global money flows are hugely important for hundreds of millions of individuals and for many countries. We all should be innovating to make them more efficient,’ he says.

Smart remittances

Just a decade ago, limited cross-border transfer options forced migrant workers to travel in person to banks or MTOs to send cash back home. After cash was deposited at an MTO, it made its way through correspondent banking channels before beneficiaries could pick up from their nearest agent.

The combination of bank fees, compliance checks and managing foreign exchange risk kept remittance costs high. The manual nature of the process meant that cross-border payments took a long time to carry out. MTOs such as MoneyGram, which was established in 1940, and Western Union, founded in 1851, dominated the market. In 2014, these two companies represented 37% of the market.

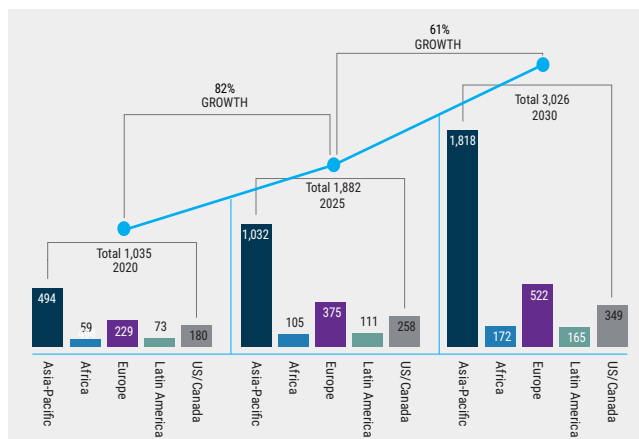
But widespread access to mobile phones from the mid-2000s onwards brought change. At the time, access to basic cellular services such as short message services (or texting) meant that users were able to initiate, send and receive payments at the touch of a

‘The combination of bank fees, compliance checks and managing foreign exchange risk kept remittance costs high.’

button. Removing physical agents and transferring and storing cash via mobile networks reduced costs, supported financial inclusion and overcame national geographical limits. Mobile money took off.

Fast forward 10 years and the landscape is unrecognisable. The introduction of mobile money paved the way for mobile wallets – which store card information and can be used in person to make transactions without a physical debit or credit card – and digital wallets, which are mainly used to carry out online transactions.

Digital remittances grew alongside mobile money. As opposed to having to travel to MTOs to send and receive in cash, fintech companies emerged that allowed the transfer of remittances from mobile phones, mobile wallets and digital wallets to another across borders. Technology accelerated the



5.1 Cashless transaction volume will more than double by 2030

Number of cashless transactions, bn
Source: PwC

change. Fintechs leverage biometric technology to verify identities and automate know your customer checks. These checks can be carried out by assessing available and submitted credit information to verify identity in person or online. They can also take place before a transaction is accepted and processed, limiting money laundering risk.

There are now more than 1bn mobile money wallets around the world and remittance providers continuously integrate with mobile money providers to build scale and reach. The abundance of mobile money transfer services and MTOs has driven down costs and increased efficiency. Those receiving remittances have multiple ways in which to use money deposited in their accounts, making such services much more convenient.

'Fintechs haven't necessarily created new technology or formed new payment rails, but they have used what was already out there to create frictionless cross-border payment experiences,' says Derrick Walton, head of emerging payments, global transaction services at Bank of America.

As such, the key to building market share in a crowded market is finding a niche – a jurisdiction or sector that you understand better and can serve better than another fintech out there.

Finding a niche

Migrant workers send between \$200 and \$300 home every one or two months. Finding a niche is important in an industry that profits on volume. Companies such as World Remit, Remitly, Wise (previously TransferWise) and Stellar have all emerged as prominent players in remittances. But each provides a slightly different product to appeal to a certain customer. In some instances, an MTO may focus on specific cross-border corridors, where it understands the market better than any other service provider. Others may target a specific type of migrant worker. Another may highlight its unique use of technology as a way to differentiate itself from others.

Remitly believes that its major unique selling point is safety – it is registered as a money services business with the US Treasury, licensed in Canada and

'While there is growing competition in the remittances space, banks and incumbent MTOs, such as Western Union and MoneyGram, benefit from experience, geographical reach and a deep understanding of the market and existing corridors.'

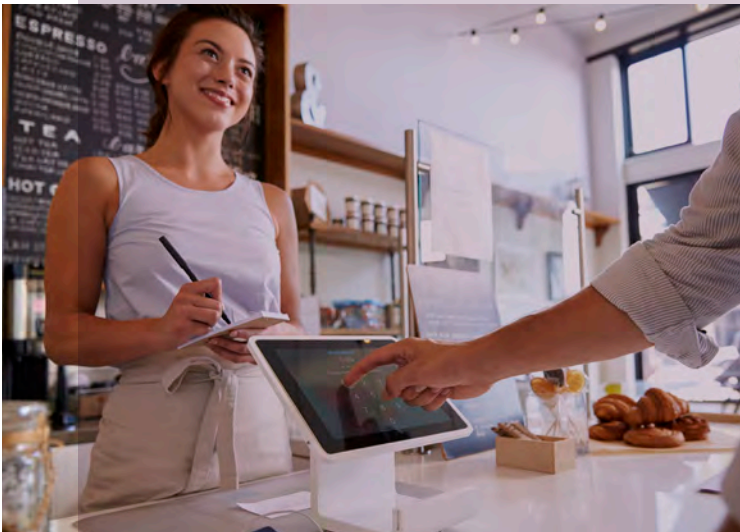
regulated by the Financial Conduct Authority in the UK. WorldRemit, for example, allows beneficiaries to accept a bank transfer, cash or even hold money in a mobile wallet. Wise allows users to send money cross-border but also allows customers to hold a variety of currencies in one account. And Stellar – an open-source network for currencies and payments – allows for cross-border money flows in fiat and cryptocurrency and has a built-in decentralised exchange for cryptocurrencies, foreign exchange and securities.

While there is growing competition in the remittances space, banks and incumbent MTOs, such as Western Union and MoneyGram, benefit from experience, geographical reach and a deep understanding of the market and existing corridors. Western Union and MoneyGram, for instance, still lead in terms of cash-in, cash-out remittances. Moreover, incumbents have deep pockets. This means that they can invest in technology, acquire or partner with fintechs and ensure that they are up to date in terms of licensing and regulation.

'It is a trend we have seen for some time,' says Genie Gloria, senior vice president, head of remittances, transaction banking group at BDO Unibank. 'But what is new is how some of these MTOs are starting to rebrand themselves as fintechs while some fintechs appear to be able to offer everything a bank can – and more.'

'In fact, remittance companies benefit from working with banks, who have good relationships with remitters, have bricks and mortar branches in places where recipients may need to cash out and have the capital to ensure regulations are met, licences are paid and they have the necessary liquidity to mitigate against foreign exchange risk,' she says.

As such, cross-border partnerships in payments and remittances abound. In October 2021, MoneyGram joined forces with the Stellar Development Foundation to integrate with the Stellar blockchain and allow cash funding and pay out in multiple currencies, including USD coin, a stablecoin governed by Coinbase and Circle. In May 2021, Google Pay launched international money transfers with Wise and Western Union, which will allow US users of the



'Mobile money providers have evolved and new players have emerged to offer credit, insurance and other financial products to small businesses notoriously underserved by the financial sector.'

Remittance lessons for MSMEs

APPROXIMATELY THREE-QUARTERS of remittances are used to cover essential items such as food, medical expenses, school fees or housing. But they can also be used for commercial endeavours. In emerging markets, where interest rates can be extremely high, micro-, small- and medium-sized enterprises sometimes support themselves with remittances.

The strength of remittances combined, with a lack of traditional financial support for MSMEs in emerging markets, has opened another niche in the payments industry. Mobile money providers have evolved and new players have emerged to offer credit, insurance and other financial products to small businesses notoriously underserved by the traditional financial sector. And it's quick. The plethora of data available creates a reliable profile of users, which means that credit can be offered within minutes.

In east Africa, Safaricom now offers products such as health insurance, credit and savings options. Established in 2019, Nigerian company Lidya provides working capital to small businesses via an app in seconds. In the Philippines, Mynt provides money transfer, savings, credit and investment products via an app. In November 2021, the company became the first Filipino fintech unicorn.

'Remittances are an important use of funds for businesses, but they shouldn't be the only source,' explains Dimieari Von Kemedi, chief executive officer of Angala Fintech. Remittances, by their nature, serve specific cross-border corridors, usually one way.

'If we want trading blocs such as the African Continental Free Trade Area to succeed, businesses in countries outside of important remittance corridors will need access to capital and to move money

between countries freely,' says Von Kemedi.

But there are obstacles to the free flow of cash. Non-convertible currencies, protectionist financial policy and limited access to foreign exchange can hinder cross-border trade and business development. Reliable access to liquidity is essential to support businesses focused on cross-border trade. As such, some fintechs follow a model used by the remittance sector.

Wise has access to local pools of liquidity to settle cross-border transactions domestically. AZA Finance leverages a similar model in the business-to-business space in emerging markets and the company has white labelled its API technology to allow money transfer companies to access liquidity through its own network. In fact, because of their reach across Africa, the Middle East and Europe, MTOs can integrate their API to facilitate and distribute remittances.

'This hub and aggregator model is growing rapidly because it reduces the cost and the risk for companies that do not have the same physical reach as we do,' says Charlene Chen, board member at AZA Finance.

Global blue-chip companies do not have the same concerns, however, and have made successful forays into MSME lending, leveraging existing customer networks and digital reach. Amazon has started to attack financial services from all directions. Amazon Lending extends working capital to affiliated business and, in June 2020, Amazon and Goldman Sachs' Marcus unit announced a partnership to provide lines of credit of up to \$1m to merchants selling on the e-commerce platform. Globally, regulators are keeping a watchful eye as big tech marches into payments and beyond.

payment app to send money to 80 countries served by the MTOs.

In June 2020, WorldRemit announced its partnership with Alipay. Through the partnership, consumers will be able to use the WorldRemit app or website for cross-border remittances. In 2019, Western Union developed a white label digital partner solution, which allows financial institutions to use their own branded interface to provide international money transfer services to their customers via Western Union's infrastructure. Transfers can be made to bank accounts, digital wallets, cards or in cash depending on Western Union's network.

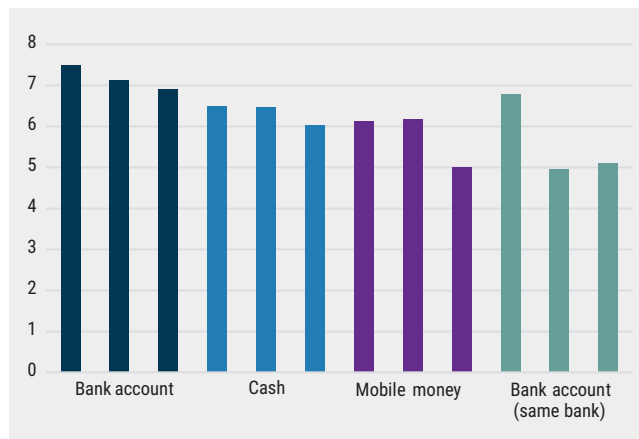
Wise allows banks to integrate with its 'Wise for banks' product, to offer their customers cheaper cross-border payment solutions. In April of this year, JPMorgan, DBS Bank and Temasek joined forces to launch distributed ledger technology payments platform Partior, for clearing and settlement of payments and securities.

This is all part of the evolution of payments. Newer remittance companies make a name for themselves by finding a niche. They build scale by partnering with larger, well known MTOs and banks. Incumbents pay to leverage technology developed by new entrants without having to upgrade legacy infrastructure all at once, while they ensure licences are up to date and regulatory requirements are met. At the same time, banks, fintechs and MTOs are adopting mobile wallet technology to provide customers with more options when it comes to remittances.

'All of this brings down cost and increases efficiency and creativity,' says Walton. 'The interconnectedness of the payments landscape is mutually beneficial and we are likely to see much, much more of this in the future.'

Unbundling payments

The vigour of banks to partner with companies in the payments and remittances sector comes in stark contrast to the derisking drive that has characterised the cross-border payments landscape over the last decade or so. Since the 2008 financial crisis, banks have pared back correspondent banking functions due to tighter regulation and a lower risk



5.2 How fast transaction costs are falling varies depending on method used

Cost of sending \$200, % of total transaction

Source: World Bank

'The combination of bank fees, compliance checks and managing foreign exchange risk kept remittance costs high.'

appetite. Those that fail to meet high global standards when it comes to cross-border payments risk hefty fines.

Around the same time, banks began to consider payments as a secondary business to other, more lucrative investment products, selling off payments assets as a result. In 2012, Deutsche Bank sold Deutsche Card Services to EVO International, a US company. In 2015, digital debit and credit card company InterCard was sold to Verifone. In 2017, digital payments company Concardis, of which Deutsche Bank, Commerzbank and UniCredit were shareholders, was sold to Advent and Bain. Between 2011-19, the number of active correspondent banking channels worldwide fell by 22%.

Meanwhile, the value of cross-border payments is increasing. According to the Bank of England, the value of cross-border payments is expected to increase from \$150tn in 2017 to over \$250tn by 2027. Moreover, with global growth expected to rebound in 2021 and 2022 as the world recovers from the pandemic, remittance flows to low- and middle-income countries are expected to increase by 2.6% to \$553bn in 2021 and by 2.2% to \$565bn in 2022. The decline of correspondent banking combined with the rise of cross-border payments has made way for payments – and remittances – to flourish outside of traditional banking networks.

'But we mustn't forget that fintechs will most likely need correspondent banking channels to support cross-border payments,' says Walton at Bank of America.

Banks will carry out due diligence in line with international regulations

and provide the required liquidity to access remittances at the last mile. As such, derisking and the decline in correspondent banking has created significant problems for the remittance industry as a whole. Through derisking, banks terminate or restrict business relationships with a whole category of businesses, including MTOs, without considering the individual circumstances of the operator in question. Without correspondent banking channels, some MTOs may struggle to survive.

Derisking can also have a negative effect on financial inclusion, as it limits access to important channels for humanitarian aid agencies and can push the cost of remittances up – despite all the ground gained in making them much more affordable. Derisking may also encourage the use of informal channels to move money across borders. These channels can destabilise the entire system as they bypass essential KYC and anti-money laundering checks in the process. There have been accounts of banks and aid organisations forced to move large amounts of cash by car, van and helicopter to those in need when formal money transfer channels have been too difficult to navigate or closed all together.

1bn

There are now more than 1bn mobile money wallets around the world and remittance providers continuously integrate with mobile money providers to build scale and reach.

But some of this may be unwarranted. As banks blame a lack of transparency of the underlying transaction as one reason to derisk, the reality is that MTOs and fintechs gather a lot of data about transactions. 'If the risk is passed on to MTOs to carry out their own AML and KYC checks, perhaps the decline in correspondent banking channels will abate,' says Gloria.

The Philippines is the fourth largest beneficiary of remittances in world, with \$35bn sent to the country in 2020. Despite the pandemic, remittances to the Philippines fell just 0.7% that year. Indeed, the cost of sending remittances to the Philippines is relatively cheap, at an average of 4.6% of the total transaction.

Part of the reason is down to recent changes in how non-banks in the country operate. Recent regulation changes in the Philippines streamlined the registration process for non-banks and authorities allow remittance providers to carry out their own due diligence of cross-border payment partners at the other end of the corridor.

As a report by the World Bank highlights, MTOs usually send remittances to and from a multitude of country pairs and some global MTOs cover a multitude of countries in the sending and receiving market. And because money is fungible, remittances can always be netted if the MTO has enough liquidity in the system.

Wise, for instance, has local pools of capital to settle cross-border transactions domestically. When local funds are unavailable, Wise leans on intermediaries and partners with liquidity in specific jurisdictions to settle payments. AZA Finance does something similar in the business-to-business space in emerging markets and the company has white labelled its application programming interface technology to allow third-party companies to access liquidity through its own network.

Driving down costs

Despite some of the issues in the remittance landscape, the plethora of options has driven up competition and pushed down costs. According to the latest figures compiled by The World Bank's remittance prices worldwide, the proportion of corridors with average costs of less than 5% has increased from 17% in the first quarter of 2009 to 38% in the



first quarter of 2021.

But there is still some way to go. The average cost of sending \$200 to low- and middle-income countries in 2020 was 6.58% of the total, more than double the sustainable development goal target of 3%. Currently, sub-Saharan Africa remains the most expensive region to send money to, costing on average 8.02%.

Banks remain the most expensive type of service provider, with average transaction fees of 10.66%. Mobile money remains the cheapest instrument to disburse remittances while debit/credit card overtook mobile money as the cheapest way to fund remittances in the first instance.

Foreign exchange risk in emerging markets is one of the biggest obstacles to overcome when it comes to remittances and will keep prices high, says Charlene Chen, board member and former COO of AZA Finance, an international payments, foreign exchange and treasury fintech company with a focus on emerging

markets. 'While the cost of remittances to Africa has come down over the past decade in some cases, intra-African remittances can still cost 20% or even 25% in transaction fees depending on the corridor,' explains Chen.

'A remitter may be able to access better exchange rates if they remit using a G10 currency, but this depends on whether the remitter has access to these currencies in the first instance,' she says. In Ethiopia, which suffers from a large trade deficit, access to foreign exchange is limited to several companies that import essential items into the country. In Nigeria, it is notoriously difficult to access foreign exchange when the oil price is down.

Where foreign exchange is hard to come by, parallel markets thrive. In Ethiopia, while the official rates can get you 47 Ethiopian birr for every dollar, on the black market you can expect it to cost nearly double. In Nigeria, the official exchange rate is around 411 naira to the dollar versus a black market rate of around 570. According to the World

Bank, the average cost of remittances to Ethiopia is approximately 6.9%. In Nigeria, the average cost is 7.1%. 'A lot of the time, foreign exchange allocation is prioritised for large companies and multinationals over individuals,' says Chen.

It is important to understand, however, that the landscape is nuanced. In February 2021, a Visa Economic Empowerment Institute study examined the costs associated with sending \$200 and \$500 of digital remittances via debit or credit in 28 key corridors. These corridors represented a mix of G20 sending countries, large remittance receiving countries and receiving countries that are dependent on remittances. 'We found that the average cost of sending remittances within these corridors was around 4% of the total for a \$200 transaction and a consumer that was able to shop around would be able to find a price of under 3% in 21 of these corridors,' says Harper.

'I've been asked before why it's free to send a high-resolution photo to someone in another country in seconds, but payments aren't as easy, cheap or quick,' says Walton of Bank of America. 'The reason lies in the vast variation of financial regulations across borders, which can be expensive to navigate.'

Mastercard's Evers agrees: 'Remittance companies grapple with regulation and compliance, foreign currency risk, capital controls and clearing and settling issues – and a growing expectation that senders and recipients expect payments and transfers to be instant.'

All of this still comes at a cost. In any case, when savings are made, it isn't guaranteed that they are always passed on to the customer.

Global cross-border peer-to-peer standardisation would allow greater competition, cut costs of remittances and allow policy-makers to share best practice. But this is difficult to achieve given the different stages of digital and financial development between countries. The Financial Stability Board cross-border payment roadmap aims to coordinate regulatory, supervisory and oversight frameworks, improve existing payment infrastructure and explore new roles of payments

'Since the global financial crisis, banks have pared back correspondent banking functions due to tighter regulation and a lower risk appetite.'





'Global cross-border peer-to-peer standardisation would allow greater competition, cut costs of remittances and allow policy-makers to share best practice.'

infrastructure and arrangements. Until then, remittances will remain a complex business to be in.

The role of cash

Some overseas Filipino workers who did lose their jobs in the service and hospitality industry, still sent money home – albeit in smaller, more frequent amounts. 'This is because they are duty bound to their family back home,' says Gloria at BDO Unibank.

As a result of the pandemic, digital remittances to the Philippines increased. According to data from the Philippines central bank, the volume of P2P monthly digital payments hit 42m, an 18.1% increase, in 2020 and the change was completely driven by remittances, says the central bank. Out of the 157m transactions made by individuals each month in 2020, valued at \$9.2bn, 27% were digital.

'Overseas Filipino workers adapted,' says Gloria. 'They downloaded money transfer apps to send money back home as stay at home orders prevented them from travelling to MTOs to send money physically.'

Perhaps the rise of digital remittances might not be as strong as remittance companies and fintechs will have you believe. 'For one, there is a trust issue. For Filipinos, there is something comforting about dropping off cash physically – checking that it is in the right hands – especially for larger transaction amounts,' says Gloria.

It is also much more than that, she says. 'Talking to friends, sharing stories, travelling to cities and towns where authentic Filipino food is available is a social event for many Filipino workers who miss their family and friends back home. It is much more of a ceremony than a chore,' she says.

The Philippines remains a cash-based economy. As such, cash will continue to play an important role in sending and collecting remittances. The fact remains that most emerging markets rely on cash despite the drive towards financial inclusion through the adoption of digital cash.

'Until digital infrastructure and financial education is widespread, the bulk of remittances will continue to end up in cash,' says Chen at AZA Finance.

This doesn't just mean having a mobile phone and being able to receive money directly into a mobile wallet but being able to spend money digitally as well.

'It's all well and good to send money from a more developed economy with the tap of a button, but if the recipient is not near a shop that accepts digital payments, they will still need to travel to a remittances agent and cash out,' says Chen. 'Only when these smaller, rural vendors are able to process digital payments will digital remittances take off.'

China might be the closest to achieving this, with plans for a digital currency that could rival cash given the prevalence of digital wallets and mobile money beyond large cities. But until then, cash users will not be able to fully participate in the evolution of payments that leads to lower costs and faster transactions when it comes to remittances.

'Picking up remittances in cash is inefficient and adds costs to the overall process,' Chen says. 'Without a truly digital end-to-end experience, there will be limits to how inexpensive they can be.' ●

Roundtable

REMITTANCES: CONTINUING THE JOURNEY BEYOND CASH

An OMFIF roundtable discusses how an accessible, easy to use and low-cost global remittance market is within reach if private sector providers can work with regulators to build, monitor and support it.



Moderator,
Philip Middleton,
chairman, OMFIF's
Digital Monetary
Institutee



Dong He
Deputy Director of the
Monetary and Capital Markets
Department, International
Monetary Fund



Alex Holmes
Chief Executive
Officer, MoneyGram
International



Matthew Saal
Digital Finance Specialist,
Financial Institutions
Group, International
Finance Corporation



**Ruben Salazar
Genovez**
Global Head, Visa
Direct

Philip Middleton: The volume of global remittances is increasing year on year. There are a number of countries that depend on remittances to support economic growth. Families across the globe, that may be excluded from conventional banking systems, may rely on remittances for their day-to-day lives. But remittances, as they stand, are expensive and can be difficult to send.

Dong He, what is the international community doing to try and bring down the cost of remittances and make them easier to send and receive?

Dong He: There are 190 countries that are part of the International Monetary Fund. Many of them are small, low- to middle-income countries for which the value of remittances is often larger than foreign direct investment and official assistance flows combined. According to the World Bank, remittance flows to low- and middle-income countries reached \$540bn in 2020.

Given the value of remittances, we can see that this is a very important topic. Yet the cost of sending a \$200

remittance is about 6.3%. It is coming down, but it is still much higher than the United Nations sustainable development goal for the cost to be 3%, on average, by 2030. Banks are the most expensive way to send remittances, charging more than 10% for a \$200 remittance.

Under the coordination of the of the Financial Stability Board, the International Policy Committee is exploring how we can enhance cross-border payments. This is more than just remittances, but remittances are an important part of this effort. To a certain extent, the FSB's reaction was due to the launch, or planned launch, of global stablecoins such as Libra – now Diem – back in 2019.

Nevertheless, one way to enhance cross-border payments is to reform the existing infrastructure to make it more efficient. Enhanced competition from alternative instruments has also energised efforts to reduce costs and increase access to and speed of remittances. Digital service providers, for example, have much lower charges.

The FSB report from October this year outlines an ambitious target around cross-border payments. For example, it outlines that 75% of all

the remittances should be available within one hour of initiation from sender to the receiver. Ideally, within one business day, everybody should have their funds available. Another goal is that no corridor should have an average cost of higher than 5%. Meeting the goals set out by the FSB and the SDG will be a huge undertaking but also a massive achievement.

PM: Alex, how easy is it to cut costs of remittances and the time it takes for remittances to reach the recipient?

Alex Holmes: It is not free to move money cross-border, largely due to the fact that most countries are structured as sovereign nations. International banking isn't really designed to facilitate the free flow of funds over borders because of compliance and other risks. That being said, I think there is a lot that can be done. For instance, cash handling is increasingly expensive and complicated. This means that smaller denominations tend to be more expensive to send and I think you see that in most pricing. Indeed, as you scale up in value, the prices

tend to come down.

Unlike the World Bank, we look at the cost of sending \$400 at MoneyGram. Currently the cost is below 3%. But, to Dong's point, we understand that this is not consistent across corridors. In certain markets, exotic currencies are much more expensive to source and there are central bank restrictions on the types of currencies allowed in and out of some countries. There are several other factors that affect the cost and speed of remittances.

At MoneyGram, we operate our system by prepositioning funds around the world and having pre-funded bank accounts to settle flows in real time. Broadly speaking, however, simplification through technology, enhanced connections on the banking side and initiatives and partnerships – for example, our partnership with Visa Direct – will enhance the free flow of currencies.

But there are risks associated with this. The highest fraud rates in the world today are all associated with online and digital payments, and this is one of the reasons we haven't seen the complete fall off in cost. Nevertheless, I do think the combination of what we're doing today is going to continue to facilitate improvements for the free flow of funds across the globe.

Matthew Saal: We are headed in the right direction in terms of lower costs but there are a couple of things to consider.

From our perspective, we're very much interested in competition and new entrants – not necessarily using ground-breaking new technology, but sometimes using better applications of existing technology. This aspect of competition is important. But we also must recognise that the prepositioning of liquidity that Alex describes is a real cost, particularly for newcomers. One approach that will reduce costs is the digitalisation of the end-to-end remittance process and this may be a reality for the next generation.

Another point to note is that research on remittances shows how important they are for the

'One way to enhance cross-border payments is to reform the existing infrastructure to make it more efficient.'

resilience of households, poverty alleviation and financial literacy. We cannot lose sight of these ancillary features because they really make a difference in people's lives.

PM: Visa have been doing a lot of work around the wider digital financial economy. So, Ruben, what do you think the key issues are with this and where should we be going?

Ruben Salazar Genovez: To continue our journey of digitising money flows, our network needs to expand beyond the traditional payment-purchase transactions. What we are doing with Visa Direct, for example, is to empower consumers, not only to pay, but also to get paid via our network so we can connect a consumer using a Visa card in the US with a consumer using their Visa card in Egypt, India or anywhere else their Visa credentials are stored. This eliminates a lot of friction in the transaction because user one can use their Visa credentials to 'upload' funds, while user two can use their Visa credentials to 'download' funds. This doesn't need any other physical or digital interaction.

Our role is to create an open network so MoneyGram and our other money movement partners

can provide differentiated solutions to their customers. The best user experience should win and our role is to empower our partners to leverage this connectivity.

PM: Essentially, what you're saying is that you are building a highway that will reach into all parts of the world, regardless of whether people have bank accounts, and that that highway will be available to all drivers.

RG: That's correct. Today we are connected to around 65 automated clearing houses, seven different real-time payment networks and, I believe, five or six different payment gateways. This means that a transaction may end up in a bank account in Bangladesh instead of in a Visa card. Whoever wants to use the network can and this will improve the user experience.

PM: What is Visa doing to educate people who may be reluctant to use digital payments?

RG: We work with our partners to show how digital payments benefit consumers and the community. For instance, some studies show that managing cash can cost [an economy] anything between 2% and 3% of gross domestic product, so there are significant benefits for markets to move to a cashless society.

We have talked a lot about financial inclusion and we have made significant improvements around this, but what is happening is that while a consumer may have a bank account or prepaid card, they may still be alienated from participating in digital commerce. This is where our effort should also be – pursuing financial inclusion and digital inclusion as well.

PM: What, then, should the public sector be doing to support this transition, Matthew?

MS: We need to facilitate innovation and upgrade infrastructure, to allow for things to move much more easily behind the scenes.

It's important to recognise that



'One approach that will reduce costs is the digitalisation of the end-to-end remittance process and this may be a reality for the next generation.'

the balance has shifted between public and private infrastructure. When it comes to domestic payments and settlements, public sector infrastructure plays an important role. In the international sphere, it has been the private sector – traditionally correspondent banks – that has bridged across separate national jurisdictions.

It is important to find links between the public and private sector, and enable public sector infrastructure and the regulatory environment to facilitate private sector innovation. For example, the current functions served by interlinked ledgers might be more efficiently executed with a distributed ledger system. While we understand that distributed ledger technology is extraordinarily inefficient in terms of processing power and electricity, it may be more efficient in transferring funds than the system we have now.

We also need to look at how we can adjust both the public and the emerging private infrastructure – whether it's payment service provider networks, telecom based mobile money, or something else – so that all of these different pieces of local and international infrastructure can link up efficiently, in a way that maintains integrity and financial stability.

We need to upgrade the infrastructure not only around the funds transfer, not only around settlement but also around digital

identity to enable instantaneous validation for more people – not just those with the right type of identification or history in the system.

PM: What is it, then, that regulators can do to facilitate this? Do they simply stand back and allow decentralised finance to take over, do they lighten know your customer and anti-money laundering regulations or is it something else?

MS: I don't think there needs to be a trade-off. In fact, you can improve KYC and AML checks by putting in place digital identity systems and create recognition of this across different jurisdictions. It may mean a move towards a 24/7 operation of some of the real-time payment systems, and while this may be expensive, you can explore options and create an optimal mix to speed up and improve the efficiency of the existing system without sweeping it all away.

That said, there's a lot to be explored in terms of new infrastructure. Certainly, DLT could solve some of these key challenges and should be looked at. Then regulators can explore the appropriate regulation to ensure integrity and compliance within those structures, whether it's a more distributed or decentralised approach. I think those things have yet to be fully resolved.

Either way, you do not need to sweep away the existing infrastructure in order to get closer towards real-time, efficient payments. For example, Singapore and Thailand have connected local retail faster payments infrastructure, PayNow and PromptPay, allowing users to make transfers between accounts in both countries.

DH: Traditionally correspondent banking relationships are multilayered and complicated. Alex described how many accounts he must maintain across the world and how this kind of split liquidity is expensive, and part of the reason why we have a high cost.

I think a number of panellists brought up the question of compliance checks as an important factor around cost. Here, again, technology can help to standardise compliance procedures, for example, the use of digital identities. Of course, it's not only a technology issue, it's regulatory consistency. But all of this would likely make it much easier to automate, not only compliance checks, but a lot of the middle office and back office operations

In 5-10 years' time, the picture is going to look very different. The cross-border payments landscape will be flatter, around the clock and regulatory compliance will be simpler, standardised and automated. All this will contribute to a reduction of cost.

We want to encourage

competition and we want to make regulatory frameworks conducive to efficient improvement. Official means of payment will also have to catch up or move with the times.

PM: I suspect that access to central bank digital currencies may be able to deliver some of the identity and conflict resolution approaches that you were outlining. Alex, where do you see things going?

AH: I think that competition and increased push for innovation is crucial, but it goes both ways. There is a lot of activity in the private sector, but I do think we need upgrades – through blockchain or other technology – to current systems, such as real-time payments.

At the end of the day, there will always be conflict because of the cross-border point. There will always be conflict around sovereign nations and there will not always be interoperability between foreign currencies. But this shouldn't mean that we stop looking at improvements to the freer flow of funds.

We talked about prepositioning cash. One of the most illiquid times we have is across weekends and holidays. This should not be the case, but it is. Banks aren't open for settlement over the weekend, so we end up sitting on piles of cash, long on various currencies. I do think we have a long way to go but I believe it is moving in the right direction. And I do certainly think that technological improvements are helpful.

One of the most interesting things that I've seen in our businesses is the propensity for me-to-me transactions. This means that people are sending money back from whatever country they are working or living into their bank account in their home country. This, I think, is illustrative of people who have left their home country and rather than just supporting their family, they are saving for themselves. This means that when they return, they have funds at home. This is an interesting pattern and is something we should continue to promote – particularly given the increased

'International banking isn't really designed to facilitate the free flow of funds over borders because of compliance and other risks.'

digitalisation on the receive side.

Blockchain, cryptocurrency and stablecoins could also greatly improve things. There's equal amount of competition there and where there is so much competition, there's always going to be disparate systems, which disaggregate the ability for continuity. But I think it's on all of us to continue to push for efficiency and lower prices, and to facilitate the flow of funds, because it's in everybody's interest to do so. And I think we've taken that initiative, responded to it well and we are trying to use technology to improve that to the greatest extent possible.

PM: Is cryptocurrency, such as bitcoin, part of the problem or is it a red herring? Does the solution need to come through fiat currency?

AH: I don't think that it's a mutually exclusive exercise. And that is something that I'm a bit frustrated by in terms of the way that some of the new crypto and blockchain companies position themselves – as if it's something exclusive. The global financial system needs a lot of improvement, but it's by no means broken. I mean, it clearly functions. Could it be better? Absolutely. But this doesn't mean it has to be completely replaced.

We have partnered with Ripple. We're now partnering with Stellar. Are there tremendous efficiencies to be made through these partnerships? Yes, absolutely. Are there an equal number of challenges and obstacles to overcome? Yes, 100%.

For example, it costs today on average about 1.5% to buy bitcoin and it costs you about the same amount to cash it out. Moreover, it's going to take several days to move it back and forth. If crypto is not taken at the point of sale, it's not a utility and ubiquitously used and you're going to have to exchange it. Whether it is crypto to fiat, or fiat to fiat, you are going to have to go through an exchange process, which is still slow and clunky. As such, it's not just about utility, but about interoperability. I think we are seeing some huge improvements to this, but it will take time and a conscious effort on everybody's part to participate actively and to drive forward improvements.

PM: Ruben, where do you think we're heading? And what is it the public and the private sectors are going to do together to get rid of the blockages?

RG: I agree with Alex in that the system is not broken and will continue to make significant progress towards both digital and financial inclusion to benefit the user.

We must remember, however, that there is probably no larger contributor to poverty alleviation than remittances around the world and yet there is very little focus in some markets to promote competition and eliminate barriers to entry.

There is a legitimate concern around terrorist financing and anti-money laundering in global money movement, but the costs for money transmitters to comply with these requirements is increasing. The widely-held aspiration to reduce the cost of remittances to 3% or under will require that policy-makers make some progress in the regulatory focus area of the cross-border roadmap, which looks to achieve more consistency.



Digital remittances bolster economic empowerment

Digital remittances are improving lives, but more can be done to improve their reach and effectiveness, writes Chad Harper, senior fellow, Visa Economic Empowerment Institute.

TRANSFERS OF MONEY by migrant workers to their home nations provide a lifeline for millions of families, as well as a boost to the gross domestic product of many countries around the world. According to the World Bank, as many as 28 countries receive up to 10% of their GDP via remittance flows. Historically, the cost of sending and receiving money across borders has created barriers, but many money transfer organisations are now offering solutions.

Key among the innovations are digital remittances, which bring with them the advantages of ecommerce. These digitally-initiated remittances have proven indispensable during the pandemic, as physically visiting an office and using cash became difficult. Digital remittances frequently take advantage of some newer money-movement networks and capabilities, and, in addition to being faster and more transparent than traditional remittances, digital remittances are more affordable and secure.

World Bank data show some interesting trends in the average cost of sending a \$200 remittance using different payment methods. As of the first quarter of 2021, only card-initiated remittances offer an average cost below 5% and have costs that have declined for the last five first quarters. It is the only method currently on a path to meet the UN's 3% cost target in the near future.

Digital remittances are also important for the economic empowerment of women. Currently, the term 'digital remittance' describes how a remittance is initiated – through a digital payment method. However, the vast majority of digital remittances are still picked up from a physical location in cash. While the sender of a digital remittance is moving money across borders from a smart phone or computer, the recipient, often a woman, is frequently picking the cash up in person.

This is a problem. The act of receiving these funds may involve traveling from remote locations, going to

an automated telling machine or agent and walking around with a significant amount of money. There is some sense of physical security in having funds directly deposited into a debit card or e-wallet, which allows greater access to other digital functions such as ecommerce and peer-to-peer transfers.

There is a savings dimension too. Enabling women to receive remittances digitally, in addition to providing more physical security and convenience, helps them keep more of their own money and manage it. For example, research from Women's World Banking has shown that women save on average 10%-15% of their earnings despite low and often unpredictable incomes. However, low-income women often face barriers to accessing a safe place to save – due

to mobility and time constraints, as well as lower levels of financial literacy. The research suggested that women can be forced to save in less reliable ways – at home in a drawer or under a mattress, by buying excess stock for their businesses or through a neighborhood savings club. Remittances received digitally can help them store the money they receive.

This added safety and convenience should not be accompanied by digital insecurity, so digital remittances and methods for receiving them must provide safety, resilience and reliability.

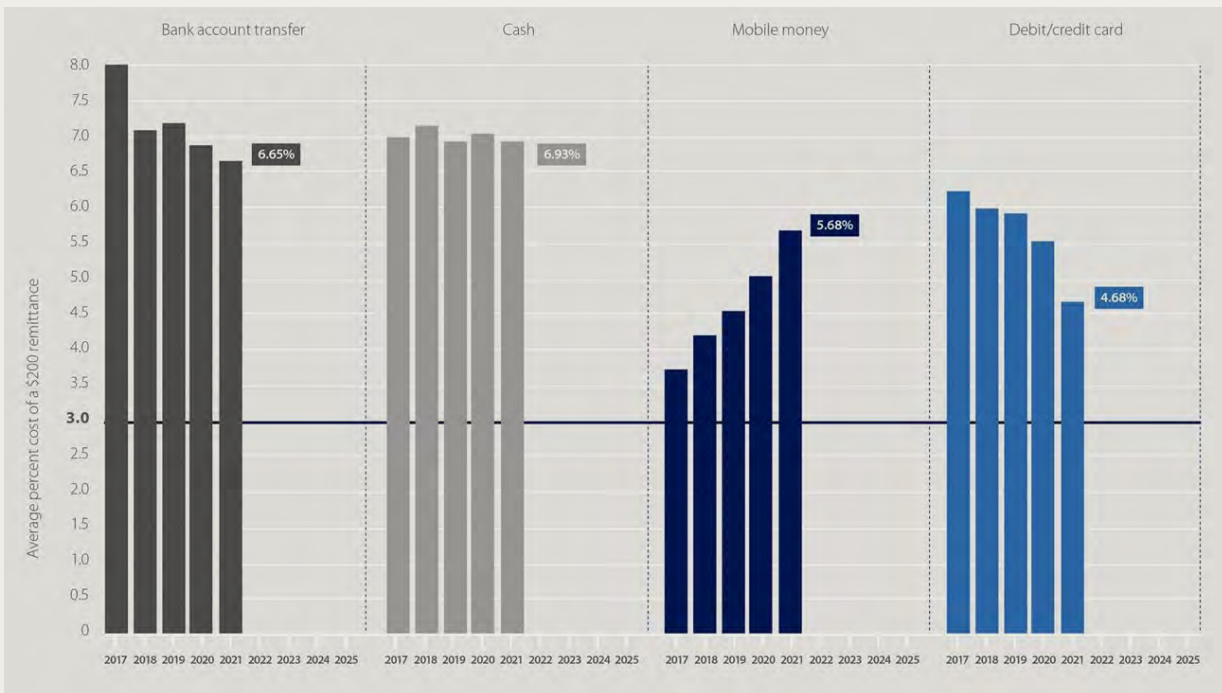
So, what do we need to do to bring the benefits of digital remittances to more people? We need to enable more migrant workers to move money digitally, of course. Money transmitters and fintechs are making great progress here. Other important steps include leveraging networks in innovative ways to reach more people and digitally enabling the people and communities who receive remittances.

Networks of networks are key to global reach

Next generation money movement capabilities are playing a starring role in the rise of digital remittances. Visa direct is one of these capabilities. It is a fast

'While the sender of a digital remittance is moving money across borders from a smart phone or computer, the recipient, often a woman, is frequently picking the cash up in person.'

'In 2021, Visa direct facilitated over 5bn transfers and leveraged a variety of card, automated clearing house and real time payment networks to move money.'



Remittance cost trends by funding method; Q1 (2017-21)

Source: World Bank Remittance worldwide quarterly

Bank account transfer
 Cash
 Mobile money
 Debit/credit card

and secure push payments platform that enables financial institutions to offer person-to-person, business-to-small-business, business-to-consumer and government-to-consumer payments. There are dozens of use cases, but the global reach of Visa direct is important to remittances. Visa direct can reach more than 5bn accounts and cards in more than 170 countries, greatly expanding payout and money transfer opportunities beyond what we typically think of as the card network. In 2021, Visa direct facilitated over 5bn transfers and leveraged a variety of card, automated clearing house and real time payment networks to move money. In the future, we hope to deliver money to digital wallets to reach even more people who do not have access to traditional banking.

Increasing access to digital services

At a basic level, digital enablement would mean that a person has an account, card or wallet which would allow them to receive and hold funds sent digitally. But this alone is not true digital enablement. Digital enablement means that there is an ecosystem available for the recipient to spend their money

digitally, otherwise we will just continue to see the remittance process end with a cash withdrawal, which has societal costs. For a person to be able to spend digitally, there has to be broad digital acceptance among businesses in that person’s community, which is no small feat in many countries.

This means that policy-makers must think about many things, some of which are quite fundamental. Beyond electricity and broadband availability, things like digital identity can also be thought of as helpful infrastructure. And then there is digital payments acceptance by sellers. Policy-makers must think of consumers and merchants together. Promoting access to digital infrastructure is just as important as encouraging digital payments. Countries that have driven digital most successfully over the last decade have worked to drive adoption on both sides, through a variety of tools and incentives.

In the end, true digital remittances will be achieved when families can receive money digitally then use it nearly ubiquitously in their everyday lives. This is where we want to be. Getting there will require the public and private sectors to work together.

Chapter 6

Balancing regulation with innovation

A new emphasis on resilience rather than cybersecurity is a first step but regulators want to go further. Should nascent resilience regulations be strengthened? By Simon Brady.

CYBERATTACKS ARE NOW the foremost risk to the global financial system. In the words of Fed Chairman Jerome Powell, 'I would say that the risk that we keep our eyes on the most now is cyber risk... That's really where the risk I would say is now, rather than something that looked like the global financial crisis.'

Powell is hardly alone. The Bank of England's systemic risk survey has consistently cited cyber risk as one of the top threats to the financial system. Elisabeth Steeman, an external member of the Bank of England's financial policy committee and its financial market infrastructure board, has emphasised the significance of cyber risk to the 'financial plumbing' that underpins the global financial system and highlights that 'the FPC has identified two priority areas to promote systemic operational resilience: cyber[risk] and payments.'

And Pablo Hernández de Cos, chair of the Basel Committee on Banking Supervision and governor of the Bank of Spain, referencing two recent BIS papers on operational resilience and operational risk, emphasises, 'The risks from cyber threats and incidents to the global banking system have been increasing over the past years. Covid-19 has further heightened these risks. In light of the evolving nature and scope of cyber risk, banks must continue to improve their resilience to cybersecurity threats and incidents.'

These fears are justified. Cybercrime

continues to grow in scale and sophistication at an alarming rate. In terms of overall losses, Cybersecurity Ventures expects global cybercrime costs to grow by 15% per year over the next five years, reaching \$10.5tn annually by 2025 from \$3tn in 2015. As it points out: 'This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined.'

This acceleration in attacks and losses is inevitable for a number of reasons.

Most obviously, extremely rapid digitalisation across both public and private sectors is expanding the so-called 'attack surface' available to malicious actors. The attack surface is every piece of information technology, every element of digital connectivity, that is susceptible to hacking. As businesses move their customer or supplier interfaces to mobile or the web, as they move storage, applications and processing to the cloud and as they and their counterparties rely ever more heavily on digital tools to move money and information, they multiply the points of access that an unauthorised person could use to enter their systems.

This digital evolution works both ways: just as businesses have embraced

technological innovation, so too have criminals. Hackers are now using the same behavioural analytics and artificial intelligence and machine learning tools as cybersecurity firms. It is not fanciful to foresee a looming battle between machines in cyberspace.

Hyperconnectivity dangers

The increasing interconnection of businesses and their financial counterparties means that third-party suppliers can be the trigger for domino-effect breaches in which a hacker gains access to one organisation and jumps from there to other client and supplier systems. BlueVoyant Research in 2021 showed that 82% of UK organisations who had experienced a cybersecurity breach stated that the breach originated from vulnerabilities in their vendor ecosystem.

These trends have been turbocharged by the Covid-19 pandemic. This has accelerated the shift towards remote working and created a host of new cyber threats. The increased attack surface, employee mistakes and weak authentication practices are all factors that cybercriminals have been able to exploit when looking to breach a company.

Criminal nations

Another development makes sophisticated attacks on financial infrastructure more likely. Over the past five years, the lines between



nation state-sponsored and organised crime gang hacking activities has become increasingly blurred. Traditionally, attacks which appeared to be financially motivated would be ascribed to criminals and those aimed at disrupting critical infrastructure, testing defences or disrupting political processes would be defined as nation state espionage or cyberwarfare.

These distinctions have broken down as governments conduct cyberattacks for financial gain, as they use or even nurture criminal gangs for political operations or as sophisticated 'exploits' (pieces of code that exploit a particular vulnerability in a piece of software) developed by governments fall into the hands of criminals.

This blurring suits both sides. Nation states shield themselves from attribution and culpability, while criminals find someone willing to pay them for their services and stolen data.

Brad Crompton, cyberthreat intelligence analyst, Intel 471, believes that this trend is here to stay. 'The trend of cross-over between nation states and the criminal underground is likely to continue for the foreseeable future, especially with this symbiotic relationship being a win-win for both parties. Cybercriminals can monetise accesses and glean data of interest while nation state actors can gather confidential information or intellectual property.'

The increase in attacks or threat sophistication would not matter if

'Cybercrime continues to grow in scale and sophistication at an alarming rate.'

organisations' defences against cyberattacks were solid. But they are not. There is a significant problem around disclosure of successful attacks, but the statistics that are available suggest that hackers are getting better at getting inside. For example, the CyberEdge Group's 2021 'Cyberthreat Defense Report' found that 86.2% of surveyed organisations revealed that they were affected by a successful cyberattack, up from 61.9% in 2014.

The cyberthreat to the payments system

The global payments system sits at the intersection of all these trends. This is perhaps why Powell, in defining cyberrisk as the greatest risk to the financial system overall, singled out as particularly worrying a hack that might shut down a major payment processor, causing a domino effect that could disrupt broad swaths of the financial system.

In his words: 'There are scenarios in which a large payment utility, for example, breaks down and the payment system can't work. Payments can't

be completed. There are scenarios in which a large financial institution would lose the ability to track the payments that it's making and things like that, where you would have a part of the financial system come to a halt, or perhaps even a broad part.'

One reason for this concern is that much of the underlying infrastructure of the global payments system is more than 20 years old. It comprises a set of legacy components designed long before today's cyberthreats emerged. This infrastructure includes that of central banks, commercial banks and their correspondents, the global automated clearing house network and local clearing houses, other regulated financial market utilities, core payments backbones such as SWIFT and major card processors like Mastercard and Visa.

Many of these systems have had cybersecurity bolted on as an afterthought at a time when they are under extreme stress from rising volumes. For example, the total volume of payments processed by the Fed's fedwire funds service is 50% higher than a decade ago. And payments via ACH payment networks – the type that are used to process payroll direct deposits, utility direct debit payments and other common transactions – have nearly doubled.

The problem is not just the total volume of payments. It is also the timing and importance of transactions. As business moves to a 24/7 operating

model, and real-time payments are becoming the norm, payments infrastructure must accommodate more payments, increasingly after hours and on the weekend, and the need to transfer funds from sender to receiver quickly. This creates both resiliency and security issues. Stressed systems are often vulnerable systems.

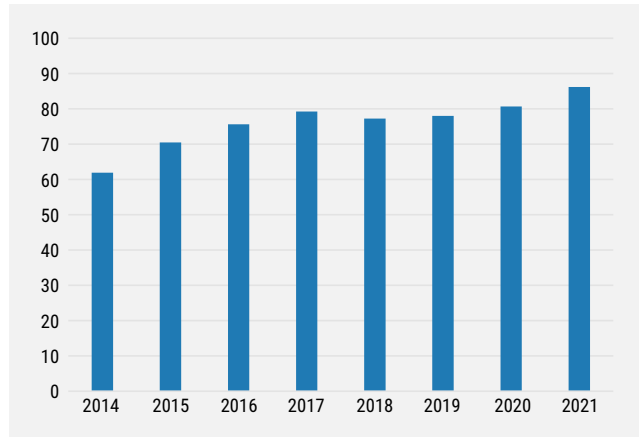
Whatever the cause, hacks associated with these legacy components are becoming more brazen and more successful. The Bangladesh Bank heist of 2015 showed how a combination of a nation state attack, compromised SWIFT credentials, malware and clever timing could net criminals \$81m stolen from a central bank even with the Fed watching.

Central banks also continue to be targets. In 2018, De Nederlandsche Bank President Klaas Knot reported that their own website was being attacked 'thousands of times per day'. In August 2019, the ECB reported that one of its websites had been hacked. In January 2021, the Reserve Bank of New Zealand said that one of its data systems had been breached by an unidentified hacker who potentially accessed commercially and personally sensitive information.

FMUs are also potentially the triggers for very significant feedback and amplification of cyberattacks both against the utilities themselves and any large bank in the system.

In 'Cyber Risk and the US Financial System: A Pre-Mortem Analysis', Fed staffers Thomas M Eisenbach, Anna Kovner and Michael Junho Lee model how a cyberattack may be amplified through the US financial system, focusing on the wholesale payments network. They find that 'a successful cyberattack on a large US institution would also have a significant impact on the liquidity of systemically important FMUs. Vice versa is also true – breakdown in normal functioning of FMUs that provide liquidity-savings, such as the Clearing House Interbank Clearing System or Continuous Linked Settlement, can dramatically affect liquidity if banks replace those intermediaries with payments through Fedwire.

'An FMU impairment would require a



6.1 Cybersecurity attacks are becoming more successful

Survey respondents saying their organisation had been compromised by at least one successful cyberattack, %
Source: 2021 Cyberthreat Defense Report

'The resilience of core payments infrastructure is inextricably bound up with the resilience of the large commercial banks that make it work and who are all dependent on each other.'

massive increase in payments value, requiring banks to process additional payments equal to about three times their daily reserves on average... We estimate that the impairment of any of the five most active US banks will result in significant spillovers to other banks, with 38% of the network affected on average.

'The impact varies and can be larger on particular days and geographies. When banks respond to uncertainty by liquidity hoarding, the potential impact in forgone payment activity is dramatic, reaching more than 2.5 times daily GDP. In a reverse stress test, interruptions originating from banks with less than \$10bn in assets are sufficient to impair a significant amount of the system. Additional risk emerges from third-party providers, which connect otherwise unrelated banks, and from financial market utilities.'

Systemic third-party risks

Mentioned almost as an afterthought, third-party providers are one of the most significant emerging risks to the system. Having been reluctant to move to the cloud for a number of reasons, large global and regional banks are now concluding that they have no choice. This creates significant new third-party dependencies with important ramifications for payment system security and regulation.

Among many examples, at the end of 2020 Deutsche Bank and Google Cloud signed a 'cloud and innovation partnership' to create the next generation of cloud-based financial services.

Around the same time, as part of a

multi-year transformation to operate entirely out of the public cloud with Amazon Web Services, Capital One exited all of its remaining data centres, moving all applications and systems to AWS. The bank’s senior vice-president of technology, Chris Nims, explains, ‘We sought to completely redefine who we are as a company, to build a technology company that does banking, instead of a bank that just uses technology. We needed to become great at building software. And we needed the top engineering talents to do it.’

And in September 2021, JPMorgan announced that it was moving its US retail bank onto an AWS-based cloud using software developed by UK fintech Thought Machine.

Given the concentrated nature of the market for cloud service providers, any large-scale move to the cloud by systemically important banks will create a critical dependency on an opaque and unregulated group of technology providers, themselves already open to cyberattacks, and becoming more attractive to both criminal and nation state actors as they become conduits for the world’s financial transactions.

The new ecosystem

Other connected third parties are multiplying fast as digitalisation and deregulation accelerate. As a result, the payments system has come to include a host of new and not-so-new platforms, from veterans like PayPal to newer global payment service providers of various kinds, such as Stripe, Square, Adyen and Wise. Digital wallets and mobile payments services, from Apple, Google or Amazon Pay, to those created by large retailers, such as Walmart, and phone providers, like Samsung, are proliferating.

And there are dozens of other payment gateways and merchant services providers overlaid onto the core payments infrastructure, including the burgeoning peer-to-peer app market, names like CashApp (owned by Square), Venmo (owned by PayPal) and Zelle (owned by Bank of America, Capital One, Truist Financial Corporation, JPMorgan, PNC Bank, US Bank and Wells Fargo.)

In particular, open banking initiatives around the globe are creating hundreds

\$10.5tn

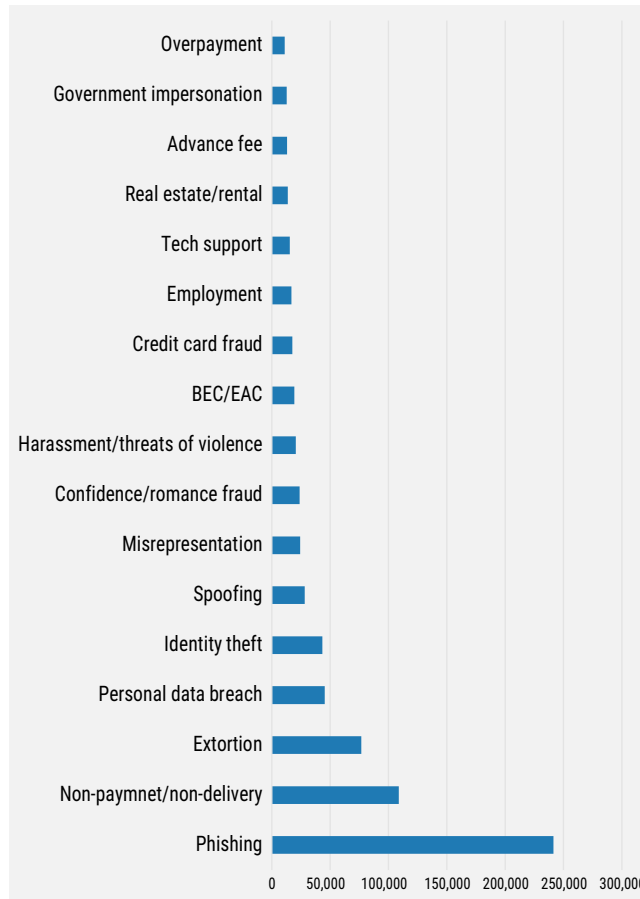
Expected cost of cybercrime by 2025

of new non-bank payment firms, many of whom are payment initiation service providers authorised to initiate transfers directly to or from bank accounts using the bank’s own tools. In Europe, for example, according to Mastercard, by the middle of 2021, 497 third-party providers were registered to provide open banking services in Europe – in addition to regulated banks.

In the US, the financial data exchange – a group of banks, fintechs and financial services groups – has aligned around a single data sharing standard and is supporting the adoption of open banking frameworks across the country.

In Europe, open banking legislation came into effect in September 2019 and the UK mandated data sharing among its biggest banks the year before.

In Asia Pacific, the first phase of Australia’s consumer data right, which facilitates open banking, went live in July 2020. In South Korea, the new MyData initiative builds on the existing



6.2 Phishing attacks are the most widely reported cyberattack

Types of cybercrime most frequently reported to the Internet Crime Complain Center

Source: Federal Bureau of Investigation

2019 open banking regulation. In India, the Unified Payments Interface is essentially an open banking platform. And there are initiatives from Nigeria, Brazil, the Middle East and Caribbean.

All of these platforms and players are vulnerable to cyberattack and, because in most cases they are linked via APIs to banking and card networks, they vastly increase the potential attack surface into those core elements of the payments system. The fact that most of them are also mobile applications as well as web-based creates additional cybersecurity risks that must be managed.

Digital payment services created by central banks have already been successfully hacked (see case study on Pixstealer) and the level of attacks on the big private sector platforms is astonishing. Alibaba Group thwarts 300m hack attempts per day, according to founder Jack Ma, and it intercepted 2.2bn cyberattacks on a single day – 11 November 2019, also known as Singles Day, China's version of black Friday or cyber Monday in the US – according to Jessie Zheng, chief risk officer at Alibaba.

Smaller platforms are targets too and the pandemic has caused a rise in downloads of payment apps and fraud attempts via those apps. One example is CashApp. According to the US Consumer Financial Protection Bureau, the agency has 'received 1,559 complaints concerning Square, under which any Cash App complaints are filed. The majority of which involved money transfer, virtual currency or money services issues.'

And in a notorious example, BuzzFeed News found US President Joe Biden's Venmo account after less than 10 minutes of searching for it, revealing a network of his private social connections, 'a national security issue for the United States and a major privacy concern for everyone who uses the popular peer-to-peer payments app.'

This threat landscape is being further expanded by the desire of banks to work with fintechs, as Deutsche Bank's chief technology, data and innovation officer, Bernd Leukert, makes clear: 'I want to reiterate that we want to onboard fintechs – we want to

'To reduce cyberrisk to the payments system, first that risk needs to be defined. This means moving away from talking about threats and cybersecurity – the technical means with which we attempt to stop threats – and towards a strategy for mitigating the impacts that those threats may create.'

partner. That is new for Deutsche Bank – this was a closed shop. And now we want to integrate them into our offering. We have a tremendous opportunity on giving them access to our huge customer base, and while on the other side, enabling them to consume our services, because when we moved to the cloud, it was quite cumbersome for them to be complementary in the past. And why not team up and offer the services which we offer to the customers as well to them?'

The complexity of this whole system, the rapidity of its evolution and the fact that it is 'where the money is' makes it an ever more attractive target for criminals looking for a financially rewarding target. For them, the faster and more efficient payments become, the faster and more efficient payment fraud becomes.

The system is also vulnerable to politically motivated attacks. Disrupting banking, commerce and the flow of money through an economy is an effective tool of cyberwarfare and attackers can cause havoc either by targeting key payments providers or by targeting individual banks.

Reducing cyberrisk: a policy roadmap

Tackling cyberrisks in this tangled payments infrastructure ultimately means ensuring that systemically important banks, central clearing and settlement mechanisms, core payment gateways and platforms, and other providers of technology upon which all these service providers depend, can maintain critical operations even when cyberattacks succeed.

This will require a complicated mix of private sector technology, updated regulation and legislation, better collaboration between the financial services industry and law enforcement, a better understanding of the key dependencies within the system and a re-evaluation of the role of the large payment platforms and the big cloud providers.

In this process, policy-makers must distinguish between the overlay systems that provide front-end services by using existing infrastructure to process and settle payments, such as ApplePay, Google Pay or PayPal, and the core infrastructure upon which they rely (the commercial and central banking systems and related clearing and settlement processes). Understanding and managing the interplay between these newer fintechs and the core payments system is critical.

Closed-loop systems which provide front-end to back-end services proprietary to their respective firms, and do not interact with or depend much on the existing payment infrastructure, such as Alipay, M-Pesa and WeChat Pay, should be considered separately.

More controversially, systemically critical payment functionalities now depend (indirectly for now at least) on commercial banks themselves increasingly reliant on largely unregulated third-party providers of public cloud services and other fintechs. If large cloud providers end up as the de facto platforms upon which the global financial system ultimately relies, then do they need to be regulated as critical national infrastructure just as key banks are today?

So what can be done to reduce

the risk that a cyberattack will cause material damage to a payment system or, via a payment system, the wider financial ecosystem?

Strengthen policy framework around resilience in regulated firms

To reduce cyberrisk to the payments system, first that risk needs to be defined. This means moving away from talking about threats and cybersecurity – the technical means with which we attempt to stop threats – and towards a strategy for mitigating the impacts that those threats may create.

The core risks to the payment system include:

- A reduction in the ability of payment, settlement and clearing providers to complete transactions in general
- Damage to a systemically important bank or FMU and the associated feedback loops
- Disruption to payment gateways reducing the ability of the public to be able to pay for goods and services
- The escalation of a single incident into a broader shock to confidence in the financial system.

All of these could be triggered by a cyberattack against a significant bank or platform. Even in the recent past, it would have been left to the cybersecurity functions of each of the threatened organisations to put technology solutions in place to create an impenetrable perimeter around the critical functions and data of the organisations.

That traditional view of cybersecurity has largely yielded to the realisation that digitally connected entities do not have a securable perimeter, that determined attackers will be able to breach any security technology and that therefore organisations and regulators must strengthen the policy framework around operational and cyber resilience, and around collaboration between regulated firms.

Unlike approaches that focus on repelling cyberattacks, resilience assumes process and service failure or degradation. It takes the traditional concept of operational risk and business continuity planning and

'Pix has already reached 40m transactions a day, moving a total of \$4.7bn a week.'



Pixstealer: hacking Brazil's instant payment ecosystem

To cope with demand and improve access to and awareness of financial services, banks and governments are developing new infrastructure, protocols and tools. One of the most successful examples of such initiatives launched during the pandemic is Pix, the instant payments solution created by the central bank of Brazil. Pix is a state-owned payments platform that enables consumers and companies to make money transfers from their bank accounts without requiring debit or credit cards. Released in November 2020, Pix has already reached 40m transactions a day and moving \$4.7bn a week.

That large number of transactions attracts hackers. In April 2021, security researchers noticed that two newly discovered malicious Android applications on the Google Play store specifically targeted Pix users and tried to lure them into transferring their account balances to criminals' accounts.

'The attackers distributed two different variants of banking malware, named PixStealer and MalRhino, through two separate malicious applications... to carry out their attacks,' according to Check Point Research. 'Both malicious applications were designed to steal money through user interaction and the original Pix application.'

PixStealer, which was found distributed on Google Play as a fake PagBank cashback service app, is designed to empty a victim's funds to an actor-controlled account, while MalRhino – masquerading as a mobile token app for Brazil's Interbank – comes with advanced features necessary to collect the list of installed apps and retrieve personal identification numbers for specific banks.

'When a user opens their Pix bank application, Pixstealer shows the victim an overlay window, where the user can't see the attacker's moves,' researchers said. 'Behind the overlay window, the attacker retrieves the available amount of money and transfers the money, often the entire account balance, to another account.'

These malware do not by themselves represent a threat to Brazil's core payments infrastructure. However, they do underscore the broader threat to stability. The more the public moves to these types of platform, the more disruption threatens to undermine confidence in the broader banking system and economy. This worries central banks and shows how even unregulated payment providers, if they carry enough payment traffic, become part of the broader financial core national infrastructure of a country. Is it time to regulate them as such?

extends those ideas to critical business processes. A bank or other financial services provider is 'operationally resilient' if, in the event of any operational disruption (no matter how big or small), it is able to continue to provide critical services.

Significantly, this concept of resilience is not related to levels of harm to the affected organisation nor to financial losses incurred by it. Institutions that have traditionally measured operational risk and identified critical operations in terms of their own financial loss now need to think about external harm to customers and financial stability as a whole.

The Bank of England, Prudential Regulation Authority and Financial Conduct Authority have taken the global lead in promoting the operational resilience of firms and financial market infrastructures firms. And, as the FPC's Steeman highlights, 'The FPC has identified two priority areas to promote systemic operational resilience: cyber and payments.'

These priorities are reflected in policy statements dating back to 2018 when the UK authorities published a joint discussion paper on operational resilience. This was followed, in December 2019, by a suite of papers to consult on the policy approach. Payment system resilience is at their heart.

The Bank of England's March 2021 supervisory statement, 'Operational Resilience: Recognised Payment System Operators and Specified Service Providers, March 2021', states: 'The Bank considers operational resilience of payment systems to be a key part of the task of protecting and enhancing financial stability. Payment systems should be both efficient and operationally risk-robust in order to play the critical role required of them within the UK economy. This is to ensure that they are both not a cause of financial instability and do not transmit and exacerbate financial instability that originates elsewhere.'

Elsewhere the Bank describes payments resilience as a primary objective of its entire resilience effort: 'To keep retail and wholesale markets open and functioning... Specifically, we aim to keep payment and settlement

2.2bn

Cyberattacks intercepted by Alibaba on a single day

\$81m

Amount stolen from Bangladesh Bank in a 2015 cyber heist

systems open to complete the day's business.'

To achieve this objective, the Bank has set out policies on the operational resilience of FMIs, payment system operators, central counterparties and central securities depositories. The FPC looks at the resilience of the system as a whole and sets out its priorities twice a year in its financial stability report. The prudential regulation committee and financial market infrastructure board focus on the operational resilience of regulated firms and FMIs. New rules will start to apply from 31 March 2022.

The Bank's basic approach to resilience and cyberrisk management is the same across all of the payments infrastructure it identifies: core firms and financial market infrastructures must establish a penetration-testing programme as the heart of their 'prevention' mechanism. More importantly, they must satisfy the authorities' baseline expectations for resilience, tailored to reflect the importance of firms and the services they provide for the financial system. Both the cyber and more generalised resilience capabilities must be regularly tested and firms should have clear and robust arrangements to respond to cyber incidents when they occur. Regular cyber stress testing will be used by the authorities to test firms' ability to meet operational resilience targets.

Theory versus practice

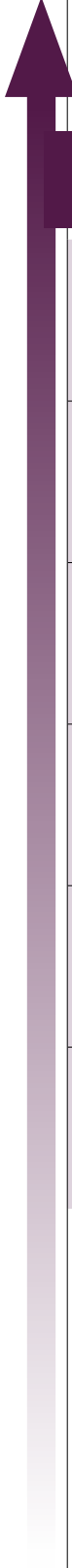
That is the theory. Difficulties begin when regulators try to operationalise these ideas. Assessing and quantifying cyber and operational risk is difficult, as is measuring and testing resilience. The FPC approach is to set 'impact tolerances' for how effectively critical financial companies should be able to restore vital financial services following a severe but plausible cyber incident. Consistent with the FPC's remit, these will be calibrated to ensure financial stability and avoid material economic harm. As such, these tolerances will not imply zero disruption.

However, at the moment, it has been left to banks and other FMIs to identify their own important business services (those that are systemically important).

6.3 Many different types of attacks can cripple ability to settle transactions

Cyberattack types and impacts

Source: Depository Trust & Clearing Corporation, Oliver Wyman

 <p>Increasing systemic consequences</p>	<p>Example</p> <p>Ransomware attack involving deletion of data at a custodian bank or a large central security depository, disrupting the purchase and sale of securities</p>	<p>Malware attack on stock exchange data centres to manipulate stock prices, with the goal of financial gain and disruption of market integrity</p>	<p>Disruption of a major wholesale payments system over a 24-hour period, causing inability to settle transactions, potential failures of banks and CCPs, lack of confidence, and a direct impact on stock markets</p>	<p>Initiation of multiple coordinated fraudulent transactions leveraging a major payments system, causing financial loss and lack of confidence in the integrity of the payments system</p>	<p>Initiation of fraudulent trades by insiders, using stolen non-public press release information provided by hackers</p>	
	<p>Credit and liquidity crisis</p>	●	●	●		
	<p>Widespread loss of trust</p>	●	●	●		
	<p>Eroded integrity and efficiency</p>	●	●	●	●	●
	<p>Inability to settle transactions</p>	●	●	●	●	●
	<p>Outage of a critical player</p>	●	●	●		
	<p>Significant financial loss</p>				●	●
<p>Cyberattack categories</p>	<p>Deletion of critical data Compromise of the availability of data critical for the accurate and effective functioning of payments, clearing, settlement processes through data deletion</p>	<p>Manipulation of critical data Compromise of integrity of data critical for the accurate and effective functioning of payments, clearing, settlement processes through data manipulation</p>	<p>Disruption of critical industry-wide services Disrupted availability of critical payments, clearing, and settlement services of multiple institutions for an extended period of time</p>	<p>Fraudulent transactions Initiation of fraudulent transactions leveraging critical payments infrastructure</p>	<p>Theft of critical non-public information Compromised confidentiality of industry-critical non-public information for use in insider trading, market manipulating action or intelligence gathering</p>	

It has been left to them to identify the processes required to deliver those services and to decide on the maximum tolerable disruption to each of those services.

Importantly, even the way that organisations test their resilience is left to them. For example, resilience testing is based on defining 'extreme but plausible scenarios' and then modelling the impact of these on the identified important businesses services and the knock-on effects on clients and financial stability.

This leaves the regulators in the odd position of not having defined the thing they want to promote (resilience and impact tolerance), the specific types of systemic harm they wish to avoid, the underlying systems and processes they would like prioritised or any kind of quantification of any part of the process.

Predictably, institutions have questioned this approach, arguing that to achieve any kind of standardisation, the authorities need to provide more clarity on these key issues. Off the record they describe the approach as little more than a 'fishing expedition' in which the regulators, unable to define any of these elements themselves, are waiting for the banks and other FMI to do it for them.

Worse, the lack of guidance has meant that most organisations have taken a narrow business continuity-based approach to the notion of impact tolerances. That is, they have defined an impact as a disruption to a key technology process and the tolerance as a single time-based metric for returning that process to the desired operational state. This is not a true resilience approach and differs little from previous operational risk management or disaster recovery processes.

An indication of the Bank of England's response to this type of criticism is this pushback in one consultation paper: 'The Bank expects central counterparties (CCPs) to undertake an assessment of the operational risks that are relevant to their important business services and incorporate those risks in the design of disruption scenarios for the purpose of testing. The nature and

'Last year, the Bank of England opened bidding for a cloud partner, with the goal of creating a fit-for-purpose cloud environment that could better support operations in a digital-first environment.'



severity of scenarios for CCPs to use may vary according to the risks and vulnerabilities identified. As such, the Bank does not consider that it would be helpful to provide a set of defined scenarios.'

It is also easy to question the authorities' resilience timeline. In a world of extremely rapid change, from political to technological, 'The Bank considers that the proposed timeframe of 12 months from the publication of the final policy is appropriate. This will provide enough time for CCPs to be able to identify important business services, set appropriate impact tolerances and regularly test their ability to meet tolerances with due regard to the mapping of dependencies. CCPs will have up to three years from 31 March 2022 when the policy takes effect to take all reasonable action to ensure they remain within impact tolerance for each important business service in the event of an extreme but plausible disruption. We believe this gives CCPs the necessary flexibility to take action to enhance their resilience.'

Global convergence

Other regulators have followed. In late 2020, the board of governors of the Federal Reserve System, the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation issued an interagency paper on sound practices to strengthen operational resilience. In March 2021, a few days after the UK's regulators finalised their supervisory approach to operational resilience, the Basel Committee on Banking Supervision published its finalised principles for operational resilience for banks. In the EU, political negotiations on the digital operational resilience act continue to proceed in both the European Parliament and European Council, and several EU financial supervisors have clarified their plans and expectations of firms.

There are differences in approach. The US paper is simply an aggregation of existing regulations around operational risk and supervision rather than policy-making. The BCBS restricts itself to banks. DORA is more specifically tied to technology.

And, outside the UK, the emphasis is still mostly on the ability of firms to withstand loss, rather than to maintain operations whose loss would threaten the stability of the national or global financial system. The definitions of core business services, impact tolerances and other key terms also diverge.

However, the key jurisdictions generally converge on the idea that operational resilience is the key to ensuring the stability of the financial system. They also share a belief that cyberrisk is a critical threat and the payments system is the most significant vector through which a systemic risk could spread. These papers represent a consistent global push to make resilience a core aspect of how banks think about operational risk, and how they construct and evolve their operating models.

Regulate cloud service providers as critical national infrastructure

The current resilience frameworks provide some confidence that regulators and the regulated can build systemic durability in the face of the cyberrisks they can imagine today. But they leave out the most significant vectors over which tomorrow's cyberrisks will be transmitted. If maintaining and regulating the current payments infrastructure is the right model, then the regulators will need to extend their reach to the digital dependencies already emerging and those that will come after.

The resilience of core payments infrastructure is inextricably bound up with the resilience of the large commercial banks that make it work and who are all dependent on each other. These, in turn, are becoming increasingly dependent on a range of unregulated third-party suppliers. Most visibly, they are moving rapidly onto public clouds.

The level of adoption has risen rapidly in the last 18 months and regulators have noticed. As Sam Woods, chief executive officer of the PRA, says, 'Our position [on whether or not to regulate] has moved on a bit. The reason for that is a very simple one. We've crossed a further threshold in terms of what sort of systems and what volumes of systems and data are

'The resilience of core payments infrastructure is inextricably bound up with the resilience of the large commercial banks that make it work and who are all dependent on each other.'

being outsourced to the cloud. As you'd expect, we track that quite closely.'

The accelerating level of reliance on the cloud, and the fact that cloud outsourcing has moved from peripheral banking systems to core systems, worries regulators for a number of reasons. Cloud giants are themselves at risk of attack, putting their customers at risk. In addition, they are notoriously unwilling to provide information on their own resilience, to such an extent that this opacity has been cited by respondents to Bank of England consultancy papers as a stumbling block in their efforts to meet their own obligations under the new resilience regulations.

As Bank of England Governor Andrew Bailey points out, 'Cloud service providers are an increasingly integral part of the infrastructure of the financial system... but as they become more integral, obviously systemic risks increase and it becomes much more of a matter of focus... [and] the model has been developed in quite an opaque and closed fashion. Now I understand part of the reason for that [is] we don't want people publishing how this thing works in great detail so that attackers get 'the guidebook' as it were... but as regulators concerned with financial stability, as they become more integral to the system, we have to get more assurance that they are meeting the levels of resilience that we need.'

In the UK, regulators have come to the conclusion that additional policy measures are needed to mitigate financial stability risks in this area. In the July financial stability report, the Bank of England wrote of cloud service providers, 'The FPC is of the view that additional policy measures to mitigate financial stability risks in this area are needed and welcomes the engagement between the Bank, FCA and HM Treasury on how to tackle these risks. The FPC recognises that, absent a cross-sectoral regulatory framework and cross-border co-operation where appropriate, there are limits to the extent to which financial regulators alone can mitigate these risks effectively.'

It's not just the commercial banks. Last year, the Bank of England opened bidding for a cloud partner, with the

goal of creating a fit-for-purpose cloud environment that could better support operations in a digital-first environment. At the time, the institution said that it had already been in talks with Microsoft's Azure, Google Cloud and AWS, and that it would likely be targeting Azure. The possibility of adopting a multi-cloud strategy was also raised.

Extend the regulatory framework to the broader payments ecosystem

If the principle is established that critical third-party dependencies must be regulated to preserve the resilience of core financial services entities, notably those that underpin the payments system, then it is difficult to stop at the major cloud providers. The payments system, and the institutions that provide its core, depend increasingly on (or can be attacked through) a broad ecosystem of unregulated payment gateways, internet providers, big tech payment services and even interdependent groups of smaller vendors.

Global regulators have noticed the implications. In the UK, the FPC's Stheeman says, 'In the past the payments value chain – from payment initiation, through processing, authorisation and clearing – was largely concentrated in a few entities. Payments used to be the preserve of commercial banks and core payment systems, with ultimate settlement taking place on the central bank ledger.'

'Now new entrants have emerged that could alter the established value chain. These range from small businesses and fintech start-ups (some rapidly achieving high market valuations) to big technology companies offering payment services in addition to their core business model, such as Apple. The FPC has identified two risks in particular from these developments. First, these structural changes could lead to systemically important activities increasingly being conducted by non-banks. Second, the changes also mean that the complexity of the payments chain is increasing. Therefore, it is becoming increasingly difficult for any single regulator to assess risks across the payments ecosystem.



'This desire to widen the regulatory net is logical, but is it workable? Should fintechs that provide services to regulated firms but which currently lie outside the scope of the rules be brought inside?'

'As a result, the FPC announced last year that the current regulatory framework will need adjustment in order to accommodate innovation in payments. The FPC has therefore developed the following three principles for payments regulation and supervision, which it has set out publicly and communicated to HM Treasury to be incorporated in the payments landscape review.

'First, regulation should reflect the financial stability risk, rather than the legal form, of payments activities – or said another way, the same level of risk should attract the same level of regulation. Given the increasingly diverse nature of companies becoming involved in payments, it is important to focus on the functions they undertake, and the risks these functions pose, rather than the nature of the company itself.

'Second, payments regulation should ensure end-to-end operational and financial resilience across payment chains that are critical for the smooth functioning of the economy. This

principle simply says that if a firm is a critical link in a payment chain, and that payment chain provides vital services to the real economy, then that firm should be regulated with a financial stability objective, as with the systemic payments systems the Bank currently regulates.

'The third principle ensures that sufficient information is available to monitor payments activities so that emerging risks to financial stability can be identified and addressed appropriately.'

In the same speech she makes it clear that 'regulators should identify firms that are not yet subject to relevant regulation, but which might be important for financial stability'.

Some regulators in the US have come to the same conclusion. In October 2021 the Consumer Financial Protection Bureau issued a series of orders to collect information on the business practices of large technology companies operating payments systems in the US.

The initial orders were sent to

Amazon, Apple, Facebook, Google, PayPal and Square. The Bureau will also be studying the payment system practices of Chinese tech giants, including Alipay and WeChat Pay.

These orders are motivated by consumer protection, not resilience, but they show that regulators across the spectrum understand that payment innovation creates new risks that need regulatory attention.

Commercial banks too want more regulation of non-financial players, and not just to be able to comply with new resilience regulations. They want a level playing field. In its response to the UK Treasury's payments landscape review's call for evidence, Barclays' published response agrees that 'policy-makers should look to regulate according to the principle of "same activity, same risks, same regulation". Given the rapid changes taking place within payments networks, we urge the government to consider how such an approach could be rapidly developed and deployed.'

Furthermore, Barclays notes that 'as payments chains become increasingly fragmented (and in places opaque), there is a danger that smaller or hidden players, currently outside of the regulatory perimeter, become key and necessary linkages. Should these linkages fail, there is potential for significant disruption. It is therefore vital the regulatory perimeter provides regulators with appropriate oversight across all of the payment ecosystem. (including an understanding of where such dependencies exist) and includes protections and provisions to avoid any vulnerabilities. Building on the previous paragraph's recommendation, we therefore believe that policy-makers should consider how the current regulatory perimeter could be updated to reflect changes in the payment landscape and bring into scope any parties currently outside the perimeter.'

Where to stop?

This desire to widen the regulatory net is logical, but is it workable? Should fintechs that provide services to regulated firms but which currently lie outside the scope of the rules be brought inside? Or should regulators rely on indirect mechanisms – for

'The problem with the current approaches, including DORA, is that they are whack-a-mole solutions to problems that will multiply and accelerate as innovation in payments and finance continues. Regulators are always playing catch up. Nowhere are they less qualified to do that than in technology.'

example will the required resilience mapping exercises force institutions to re-evaluate the resilience of third party providers?

And what about less visible dependencies? The solar winds/sunburst ransomware attack targeted software developed by US software company Kaseya and used to manage networks, systems and information technology infrastructure. The Kaseya ransomware attack occurred on 2 July 2021, when their servers were infected by ransomware which spread from several managed service providers to their clients, infecting about 1,500 companies worldwide. One high-profile victim was the Swedish Co-op, who had to close 800 stores for a week as the ransomware encrypted their point of sale software. The attack didn't affect the Co-op's IT infrastructure but targeted their supplier, Visma EssCom, which uses Kaseya technology and manages the servers used for Co-op tills.

This so-called software supply chain hack illustrates the difficulty with the 'regulate all critical dependencies' approach. Which company in this chain should be regulated – Kaseya, Visma EssCom or Co-op? Who is responsible for uncovering this dependency? And

what about every other operational dependency on pieces of low-level software?

As the FSB notes, 'This complexity even suggests the existence of interdependencies among third-party suppliers ("fourth parties"). FIs may thus be reliant on an aggregation or network of very disparate services.'

DORA – the way forward or a dead end?

One regulator seems to have understood the issues better than the rest. The European Commission's draft digital operational resilience act is unique in introducing specific requirements for information and communication technology providers. Primarily aimed at financial entities, including credit institutions, electronic money institutions, investment firms, insurance and re-insurance companies, it also covers critical ICT providers. It would mean that cloud service providers would formally come within the scope of European supervisory authorities for the first time. Significant penalties can also be imposed on the ICT service provider for non-compliance. A periodic penalty payment of 1% of the average daily worldwide turnover of the ICT service provider in the preceding business year can be applied daily until compliance is achieved.

This approach goes far beyond other regulators' resilience prescriptions and puts into draft rules the desires of the FPC and others to regulate according to risk and activity rather than by type of entity. It also reflects the views of bodies like the FSB which has accepted that dependence on tech firms 'could lead authorities to consider new approaches to micro and macroprudential supervision of firms, infrastructures and activities. In some jurisdictions, they may also raise questions for FSB members around their approaches to third-party risk and give rise to the potential for greater co-operation between financial authorities and non-traditional partners such as those responsible for IT and security.'

It also goes some way to addressing that last issue: if financial regulators do not regulate the technology providers as though they are financial firms,

then who should regulate them? As the FPC has said, '[We] recognise that, absent a cross-sectoral regulatory framework, and cross-border co-operation where appropriate, there are limits to the extent to which financial regulators alone can mitigate these risks effectively.'

So, should everyone adopt a DORA-like framework? Is this the solution both to reducing cyber and other systemic risks in the payment and financial systems? Does it remove the problem of having to get both financial and non-financial regulators?

Embrace the payment revolution? De-regulate not regulate?

The problem with the current approaches, including DORA, is that they are whack-a-mole solutions to problems that will multiply and accelerate as innovation in payments and finance continues. Regulators are always playing catch up. Nowhere are they less qualified to do that than in technology.

Moreover, key regulators acknowledge the benefits of cloud and other tech. The FSB's recent report, 'BigTech in finance: Market developments and potential financial stability implications', agrees that the entry of big tech firms into finance has numerous benefits, such as the potential for greater innovation diversification and efficiency in the provision of financial services, as well as helping with financial inclusion and SMEs.

A related report, 'Third-party dependencies in cloud services: Considerations on financial stability implications', also says that cloud service providers can offer benefits over previous technology, including by creating geographically dispersed infrastructures and investing in security. Cloud providers may offer significant improvements in resilience for FIs, as well as enabling them to scale more quickly, deliver improved automation and operate more flexibly. Economies of scale could also result in lower costs to clients.

And the PRA's Woods stressed at a July press conference that, 'I think it's important [to say that] we don't

want to give the message here that we think the cloud is somehow sort of structurally unsound: it isn't... it is a robust infrastructure... being managed to high standards of resilience.'

This suggests an entirely different path if regulators are willing to take it. Instead of trying to shore up an infrastructure that was never designed to be resilient through ever more burdensome regulation that is doomed to fail, why not accept that the underlying infrastructure, not the regulations, is what must change?

In February 2021, there was a more than three-hour disruption to over a dozen critical central bank payment services forming the backbone of the US banking system, including the Fed's fedwire funds, fedcash, national settlement service, fedwire securities service and some cheque clearing services. The episode followed two significant disruptions to the Fed's payment services that occurred in 2019.

That disruption, which turned out to be nothing more sinister than a 'glitch', emphasised the limits of regulation and made modernisation seem the more logical approach.

A vision of the future

- Accelerate the modernisation of every part of the payments lifecycle, from the devices that initiate payments to those that process payments such as banks, the Fed and other central clearing house providers.
- Instead of penalising cloud usage, prioritise it and 'as-a-service' models of payments processing (and other banking services). The benefits, as outlined by the FSB and PRA, outweigh negatives.
- Instead of stifling innovation by casting the regulatory net ever wider, regulators and central banks should work with fintechs and big tech to create the next stage in the evolution of the payments industry, with the encouragement of regulators.
- Make better use of existing standards: for example, any ecosystem participant providing payment processing and clearing and settlement services should ensure their services meet availability and compliance standards such as SOC1, SOC2 and ISO 27001:2013.

'Authorities should promote decentralised and distributed models rather than traditional centralised models. The former, like the internet and digital currencies, are more resilient than the latter.'

- Most controversially, authorities should promote decentralised and distributed models rather than traditional centralised models. The former, like the internet and digital currencies, are more resilient than the latter.

In this version of the future, cyberrisk reduction and resilience in the payment system do not rely on regulations which by definition cannot stay ahead of the problems. Instead, the technologies currently deemed a threat are recognised for what they really are: the solution to problems that are caused mostly by the current infrastructure's increasing inability to cope with modern requirements.

This leaves regulators and policy-makers in a difficult position. In the transition to the new digital world, they must balance the needs for stability with those for the freedom to innovate. Today, they, through the banks, may ultimately be responsible for ensuring the security of the payment system. Tomorrow, as the FPC's Stheeman anticipates, the responsibility for ensuring the security of digital payments may lie with technology companies themselves. ●

Subscribe to OMFIF

Stay up to date with the latest financial and monetary policy news and commentary from OMFIF's in-house analysts and global network of specialists. Receive the Digital Monetary Institute updates in your inbox, including information on upcoming meetings



'Extremely
valuable
research and
analysis'

Jean-Claude
Trichet, President
of the European
Central Bank
(2003-2011)



'OMFIF provides a valuable
platform for the exchange
of ideas among a wide set of
public and private sectors'

Eddie Yue, Chief Executive, Hong
Kong Monetary Authority

'OMFIF has become an
important forum where
market participants and
authorities from different
jurisdictions could come
together to discuss crucial
matters impacting the
financial systems'

Roberto de Oliveira Campos
Neto, Governor, Banco Central
do Brasil

DMI OMFIF®
Digital
Monetary
Institute

omfif.org/subscribe



**Official Monetary and
Financial Institutions Forum**

6-9 Snow Hill, London EC1A 2AY

T: +44 (0)20 700 27898

enquiries@omfif.org

omfif.org