

FUTURE OF PAYMENTS 2022



TURNING THE CROSS-BORDER PAYMENTS ROADMAP INTO REALITY



VISA

 Payoneer

 aws

 RTGS.global

 bitt

 BINANCE

 flutterwave

FUTURE OF PAYMENTS 2022

DMI

Official Monetary and Financial Institutions Forum

181 Queen Victoria St, London EC4V 4EG, United Kingdom

T: +44 (0)20 700 27898

enquiries@omfif.org

omfif.org

ABOUT OMFIF

With a presence in London, 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.


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
- Taylor Pearce**
Economist
- Julian Jacobs**
Economist
- Simon Brady**
Economist
- Katerina Liu**
Research Assistant
- ADDITIONAL RESEARCH**
- Nikhil Sanghani**
Managing Director, Research
- EDITORIAL AND PRODUCTION**
- Simon Hadley**
Director, Production
- Fergus McKeown**
Subeditor
- William Coningsby-Brown**
Production Manager
- Sarah Moloney**
Subeditor
- MARKETING**
- James Fitzgerald**
Deputy Head of Events and Marketing
- Henna Rattu**
Marketing and Events Coordinator
- Maya Turnbull**
Events and Marketing Coordinator
- DMI TEAM**
- Philip Middleton**
Chairman, DMI
- Katie-Ann Wilson**
Managing Director, DMI
- Folusho Olutosin**
Commercial Director, DMI
- Sinan Yilmaz**
Account Manager, DMI
- Max Steadman**
Programmes Manager, DMI
- David Coleman**
Commercial Assistant, DMI

REPORT SPONSORS






Lead report sponsor



Lead chapter sponsors

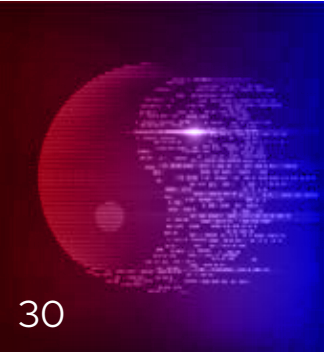


Co-sponsors



CONTENTS

- 4 **Foreword**
Dynamism in payments but cross-border developments lagging
- 5 **Foreword**
Enabling inclusive economies through the frictionless flow of value
- 6 **CBDC Survey 2022**
CBDCs sooner rather than later, say central banks
- 14 **Chapter 1**
Turning the cross-border payments roadmap into reality



- 22 **Chapter 2**
Crypto’s crucial appeal for emerging markets
- 30 **Chapter 3**
Promise and peril of central bank digital currencies
- 40 **Chapter 4**
Central banks must take the lead in payments cybersecurity
- 48 **Chapter 5**
The metaverse: a model for digital payments?

FOREWORD



DYNAMISM IN PAYMENTS BUT CROSS-BORDER DEVELOPMENTS LAGGING

New entrants and existing players are working hard to reimagine how payments work, writes Katie-Ann Wilson, managing director, Digital Monetary Institute.

There has rarely been such a dynamic and innovative time for the payments industry. The advent of novel technologies has galvanised efforts to improve the speed and security of payments, as well as to bring down costs and broaden access to financial services.

Progress in domestic payments has been rapid, with cheap and quick digital payments solutions already available, including in emerging markets where mobile payments have gained traction. Progress in cross-border payments has been less impressive, however, and problems weigh heavier in emerging markets, with higher costs disproportionately falling on those least able to bear them.

The problems of connecting different domestic payments environments, many of which have widely varying architecture, are incredibly complex and there are many solutions being explored. The Committee on Payments and Market Infrastructures has done an excellent job in defining the problems and laying out responses.

Traditional players are making important improvements to their services, improving speed and security with new frameworks, but there are still major obstacles that are yet to be surmounted including data localisation.

Outside of the traditional payments space, we examine the efforts of innovators to develop a new payments infrastructure that can sidestep some of the challenges facing the established industry. This is unlikely to be a 'winner-takes-all' kind of fight. The variety of payments systems will grow, creating competition and diversity in the marketplace.

As part of this work, we are delighted to

introduce our first survey on central bank attitudes and intentions regarding central bank digital currency. Our survey shows that improving cross-border payments is not the primary goal central banks are pursuing with their development of CBDCs. Nevertheless, many survey respondents said that they saw promise in the interlinking of domestic CBDCs as a means of improving cross-border payments.

We examine what promise CBDCs hold for emerging markets, where development is taking place most rapidly, as well as looking at the value cryptocurrencies and stablecoins offer to jurisdictions with unstable and unreliable currencies. While they offer valuable havens from inflation and, in some cases, cheap remittance channels, the absence of robust know-your-customer procedures and tools to prevent financial crime could limit their potential.

As these systems become more important, the technological expertise central banks require grows. Our survey shows that cybersecurity is the top concern for central banks examining digital currency. We explore the threats they face and the policies they can employ, particularly in emerging markets, to mitigate them.

Finally, we examine the development of the metaverse and discuss what payments solutions might be needed to serve the emerging use cases that a new digital environment will necessitate.

It is possible that by developing the infrastructure to support payments in globally accessible digital environments, we might end up with a solution that can help solve some of the problems in cross-border payments.

The payments industry is undergoing seismic changes. Both the established players and new entrants have work to do before they are able to address the challenges of cross-border payments, but the systems we use to send value to counterparties in other countries will change substantially over the next few years. •



THE PROBLEMS OF CONNECTING DIFFERENT DOMESTIC PAYMENTS ENVIRONMENTS, MANY OF WHICH HAVE WIDELY VARYING ARCHITECTURE, ARE INCREDIBLY COMPLEX AND THERE IS A VARIETY OF SOLUTIONS BEING EXPLORED.

FOREWORD



ENABLING INCLUSIVE ECONOMIES THROUGH THE FRICTIONLESS FLOW OF VALUE

New technologies risk fragmenting the payments landscape even more, but they also hold the promise of bringing it together, writes Thierry Chilos, chief strategy officer, Swift.

SINCE THE LAST edition of 'Future of payments', the world has continued to undergo significant change. Digitalisation has continued at pace as we emerge from the worst pandemic in 100 years, while geopolitical shifts, rising energy costs and inflation are all impacting people everywhere. At the same time, the financial ecosystem continues to evolve with new entrants, new technologies and innovative solutions, and customer expectations are higher than they've ever been.

These external factors are having a knock-on effect on the payments industry and contributing to increasing fragmentation. Enabling inclusive digital economies is therefore more important than ever. Without fast, frictionless flows of value, inequality will only increase.

But for money to flow smoothly and quickly across borders, interconnectivity is critical. Swift, and our community of more than 11,500 organisations in over 200 countries and territories, continues – as it always has – to be a symbol of global co-operation, finding opportunities to bring us all together.

Our strategy for achieving instant and frictionless cross-border payments is closely aligned to the priorities of the G20 for an enhanced cross-border payments experience. Improvements to speed, transparency, cost and access will be critical if we, as an industry, are to succeed in this mission.

While the last few years have seen excellent progress for wholesale cross-border payments,

the same focus also needs to be applied to the small business and consumer space, which is among the fastest growing segments in the cross-border payments industry. Individuals and small- and medium-sized enterprises that want to send money internationally face a time consuming, costly and uncertain process. If we don't fix that, we'll only be contributing to more fragmentation.

Access, as well, to the solutions that enable the rapid flow of value across borders must increase. Thankfully, while technology has played its part in fragmentation, it also brings us great opportunities. Cloud-based services and the rise of application programming interface technology mean that the financial industry can offer its services to more people and businesses in more places.

If we are to overcome fragmentation and achieve our collective goal, we must come together as a financial community and harness our collective strengths. Standardisation, led by the industry's adoption of ISO 20022, which begins next year, will be critical to achieving interoperability between systems and infrastructures.

Swift has championed responsible innovation for the future of payments, with experiments this year demonstrating that we can use the power of central bank digital currencies across borders, regardless of the underlying distributed ledger technology, and integrate them seamlessly with the ecosystems of today.

Collaboration and partnership will be essential in achieving frictionless cross-border payments. We are delighted to support OMFIF's 'Future of payments' report, which provides valuable thought-leadership in support of making the payments industry more efficient, accessible and inclusive. •



WHILE THE LAST FEW YEARS HAVE SEEN EXCELLENT PROGRESS FOR WHOLESALE CROSS-BORDER PAYMENTS, THE SAME FOCUS ALSO NEEDS TO BE APPLIED TO THE SMALL BUSINESS AND CONSUMER SPACE

CENTRAL BANK DIGITAL CURRENCIES SURVEY



KEY FINDINGS

- 1. Two-thirds of central banks surveyed expect to issue a CBDC within 10 years.
- 2. Central banks are pursuing CBDC for various reasons, but none cited improving cross-border payments as the main motivation.
- 3. Nevertheless, many thought that inter-linking CBDCs offers a promising avenue for improving cross-border payments.
- 4. Banks will not have the exclusive right to distribute CBDC. Instead, they will be joined by new, regulated players.
- 5. Avoiding low adoption of CBDCs is a primary concern for central banks, while bank disintermediation is a secondary concern.

IN this year’s ‘Future of payments’ report, we conducted a survey of central banks to uncover their aims and objectives for CBDCs, plans for implementation, availability of internal resources and views on technology to improve cross-border payments.

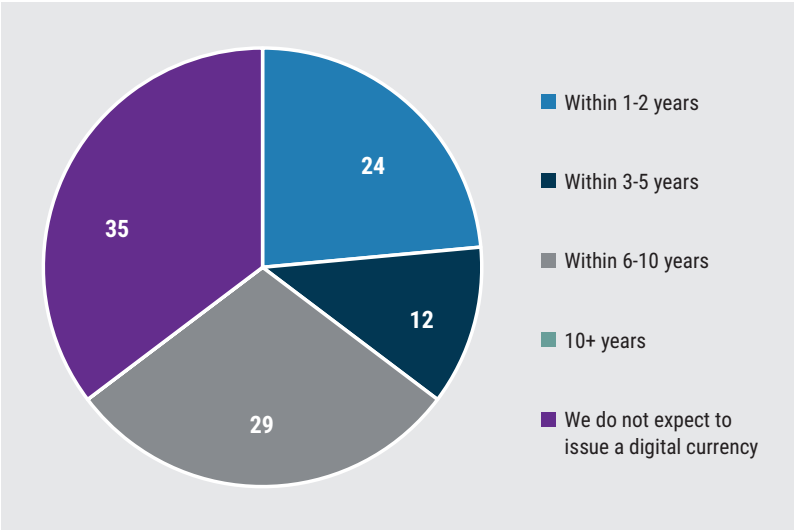
CENTRAL BANK DIGITAL CURRENCIES ARE GAINING MOMENTUM
Several central banks have launched CBDCs, either as pilots or as fully deployed systems. Many of their peers have been encouraged by the progress.
The Atlantic Council reported that 105 countries are now exploring a CBDC, up from only 35 countries in May 2020. Responses to our survey reflected that trend. Among survey participants, two-thirds reported that they expect to issue a CBDC within 10 years, while none expected to issue one in more than 10 years (Figure 1) Overall, if central banks decide to issue a CBDC, they expect deployment to come sooner rather than later.

Among the central banks that said they do not expect to issue a CBDC, many are actively researching the possibility of launching one. One central bank survey respondent commented that they ‘monitor the possible motivations and problems a CBDC can solve to see when will be convenient or necessary to prioritise efforts on this topic,’ while another stated that their ‘current stance on the issuance of a local CBDC may change should domestic or international factors justifying such a change emerge.’

Many central banks surveyed have been encouraged by their peers’ CBDC developments. Compared to a year ago, none of the survey participants are less inclined to issue a CBDC (Figure 2). Instead, their stances have either remained the same (62.5%) or they are now more inclined to issue a CBDC (37.5%). One survey participant more inclined to issue a CBDC explained that ‘central banks around the world have accelerated their CBDC research and experiments, with more and more practical examples of positive experiences.’

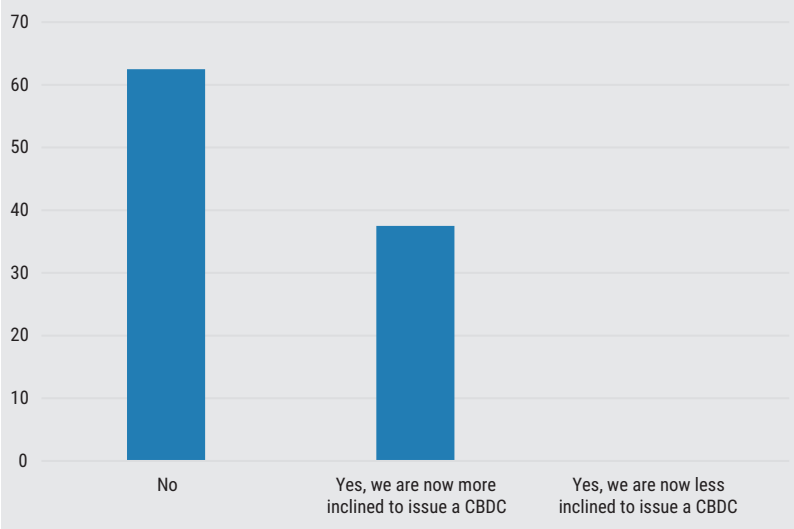
The presence of dedicated CBDC employees in central banks is indicative of their monitoring and research activities. The central banks surveyed – including those who state that they do not intend to issue a CBDC – have a median of five employees dedicated to researching or developing CBDCs in some capacity. Many also involve employees in CBDC projects on a part-time basis and include team members from various departments.

1: Two-thirds of central banks expect to issue a CBDC within 10 years
When do you expect to issue a Central Bank Digital Currency? Share of respondents, %



Source: OMFIF Future of payments survey 2022

2: Central banks are not discouraged by CBDC developments
Has your thinking on digital currencies changed in the past year? Share of respondents, %



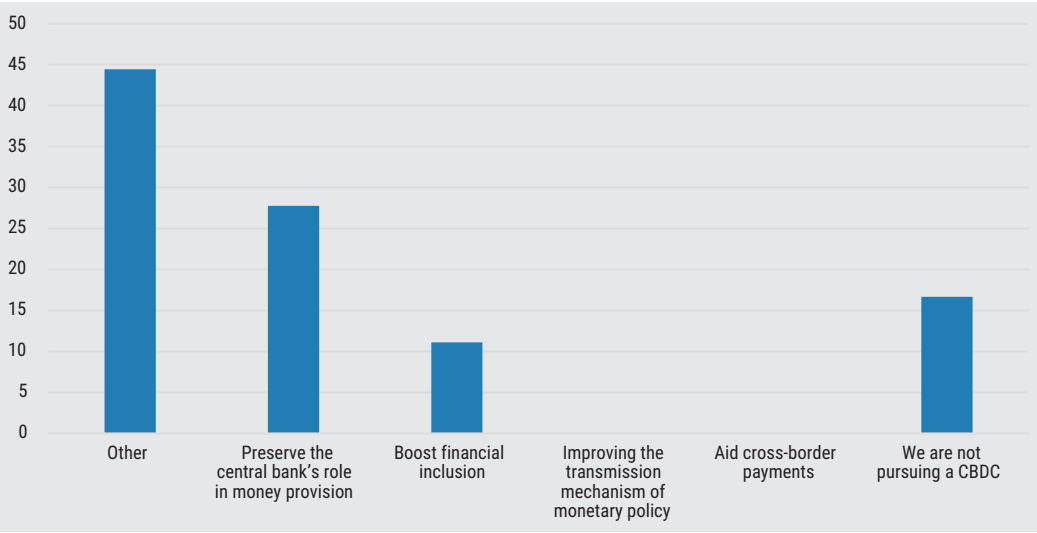
Source: OMFIF Future of payments survey 2022

CENTRAL BANKS AROUND THE WORLD HAVE ACCELERATED THEIR CBDC RESEARCH AND EXPERIMENTS, WITH MORE AND MORE PRACTICAL EXAMPLES OF POSITIVE EXPERIENCES

3: No strong consensus of central banks’ objectives for pursuing a CBDC

What is your main objective by pursuing a CBDC? Share of respondents, %

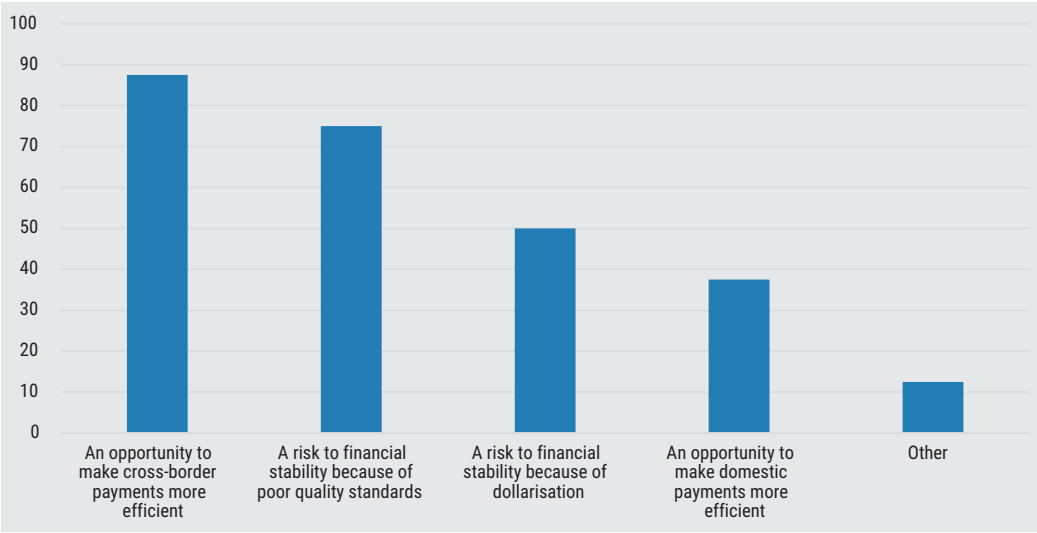
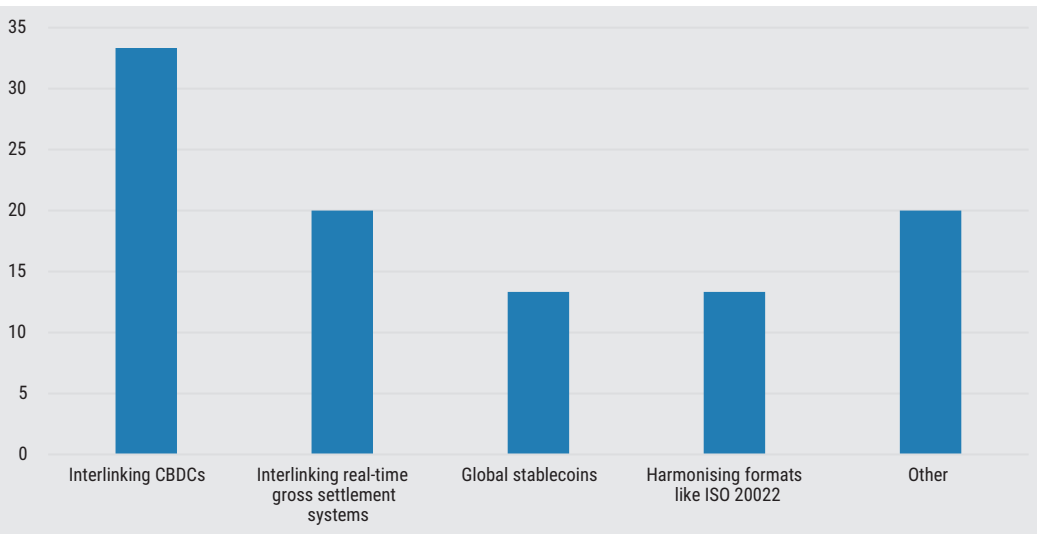
Source: OMFIF Future of payments survey 2022



4: Interlinking CBDCs shows most promise for cross-border payments

What do you think is the most promising avenue to improve cross-border payments? Share of respondents, %

Source: OMFIF Future of Payments survey 2022



5: Stablecoins also show some promise for cross-border payments, but remain a risk

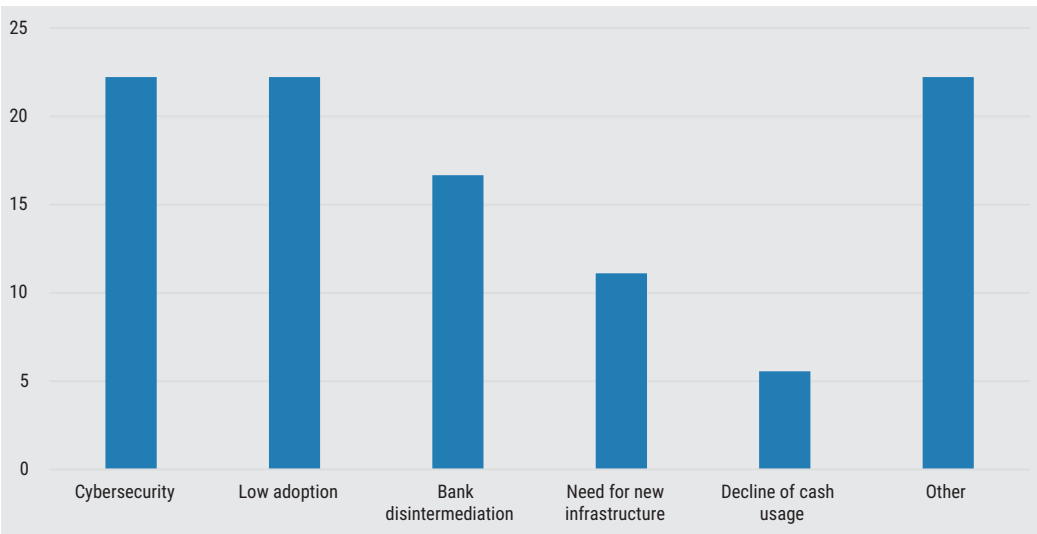
Respondents which view stablecoins as: Share of respondents, %

Source: OMFIF Future of payments survey 2022

6: Low adoption and cybersecurity tie as primary concerns over deploying a CBDC

What is your main concern over deploying a CBDC? Share of respondents, %

Source: OMFIF Future of payments survey 2022



NO CONSENSUS ON THE PURPOSE OF CBDC, BUT CROSS-BORDER PAYMENTS NOT A MAIN FACTOR

In this year’s survey, there is a wide spread of central banks’ objectives for pursuing a CBDC, though there is no strong trends towards any one objective (Figure 3).

Surprisingly, no central bank listed improving cross-border payments as their main objective for pursuing a CBDC. Instead, preserving the central bank’s role in money provision was the second most reported main objective.

‘Other’ encompassed a range of alternative objectives: digitalisation, improving the resiliency and efficiency of payments systems and interoperability. Some 75% of participants that responded with ‘other’ said they had multiple objectives, adding that they believe these flow into each other, with one survey participant explaining that they ‘do not necessarily see one compelling motivation, rather a number of them’.

INTERLINKING CBDCS A PROMISING AVENUE FOR CROSS-BORDER PAYMENTS

Although no central bank said it was their main motivation for pursuing a CBDC, many said that interlinking CBDC systems was the most promising option for improving cross-border payments.

Improving cross-border payments is a major priority for the Bank for International Settlements and the G20, underpinning the committee on payments and market infrastructures’ programme on enhancing cross-border payments.

A survey respondent commented that CBDCs may ‘provide a building block for better cross-border payments in the future,’ while another stated that the ‘possible issuance of a foreign CBDC that could be available on a cross-border basis’ would encourage their central bank to pursue a CBDC.

The debate around CBDCs and cross-border payments is still unsettled. A survey respondent pointed out that ‘there are a lot of factors involved in

cross-border payments. To improve these payments in terms of timing, speed, fees and compliance costs, there must be a comprehensive view and harmonised approach. These include aspects such as technical, operational, legal and possibly political.’ Simply launching a CBDC is unlikely to solve many of the challenges that cross-border payments face.

Stablecoins may be another solution for cross-border payments. Yet, only 13% of respondents indicated that stablecoins would be the best avenue to improve cross-border payments (Figure 4). Despite that, 88% of survey respondents viewed stablecoins as a possible opportunity for cross-border payments, but 75% also believed they pose a risk to financial stability because of poor standards (Figure 5). Stablecoins may become a viable option for cross-border payments if the regulatory environment is conducive, as explained by a participant who stated that global stablecoins will dramatically improve cross-border payments ‘assuming no adverse regulatory environment’.

LOW ADOPTION A PRIMARY CONCERN, BUT THE RIGHT TOOLS MIGHT OFFSET THAT

Central banks are particularly concerned about the risk of building a CBDC that ends up not being used. This is of particular concern for those central banks that see boosting financial inclusion as a key reason for launching CBDC. One survey participant stated that ‘low adoption would lead to significant reputational damage, but there are adequate tools to ensure its usage.’

Many survey respondents stated that their respective institutions had not yet made any official decisions to drive adoption but are developing strategies. Several participants suggested that offline functionality is crucial, ensuring that CBDC can operate in areas without widespread internet access.

Other suggested measures include mandatory distribution, interoperability, user-friendly wallets and direct incentives such as discounts for consumers.

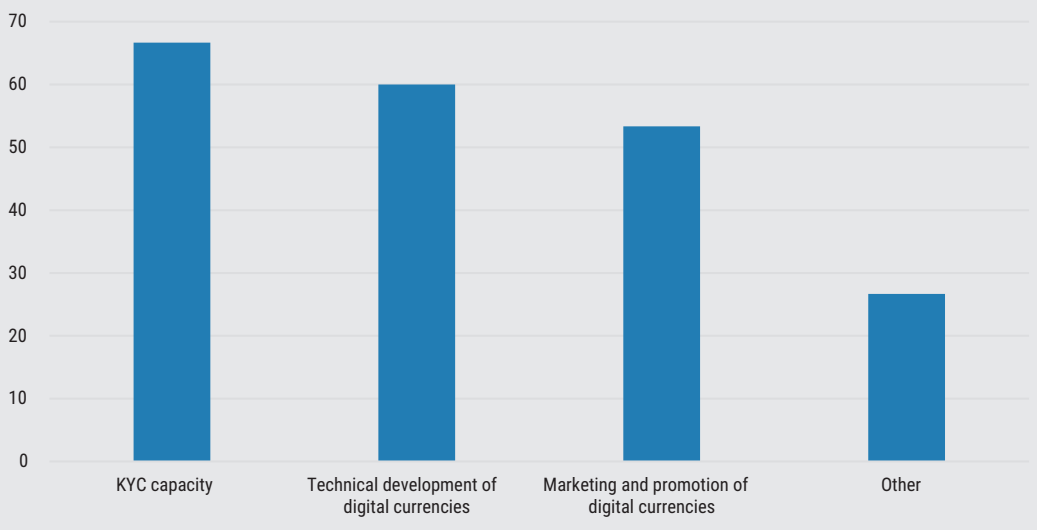
Some of these measures have been



7: There is almost an even spread showing central banks’ need for third-party services

What services do you need private sector third-parties for? Share of respondents, %

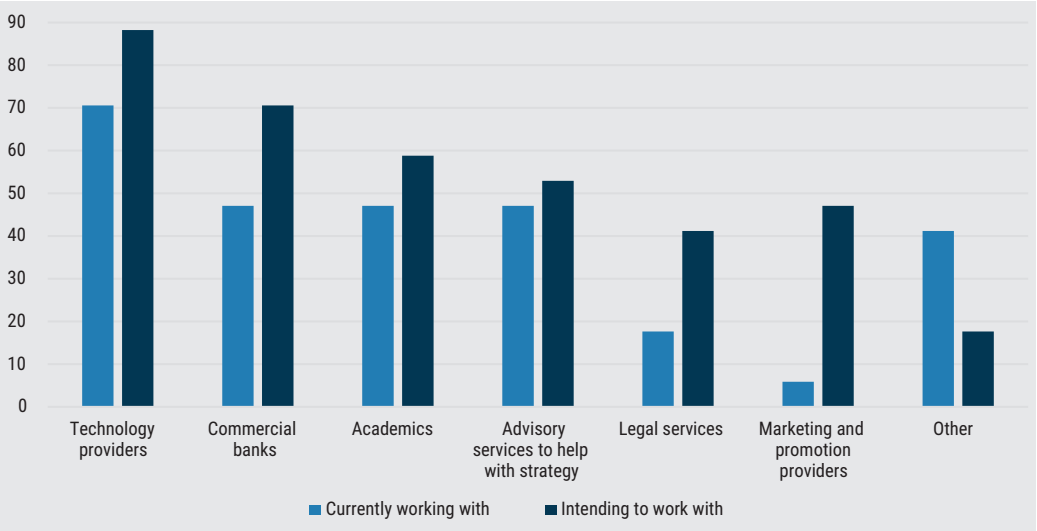
Source: OMFIF Future of Payments survey 2022



8: Central banks are working with the full range of third-party services

Which of the following third-parties are you currently working with/intend to work with on digital currencies? Share of respondents, %

Source: OMFIF Future of Payments survey 2022



employed by Nigeria (the Central Bank of Nigeria did not complete the survey) to boost usage of the eNaira, its CBDC. In August 2022, the CBN unveiled the use of unstructured supplementary service data short codes, which enable users without internet connection or bank accounts to set up an eNaira wallet using a non-smartphone. In October 2022, the CBN offered a 5% discount to drivers and passengers of motorised rickshaws who use the eNaira. While it is too soon to determine if these measures will improve adoption, it might take more time before the eNaira’s adoption rates increase, but the CBN is still optimistic – it is working with third-parties to innovate even more solutions.

One important method of driving adoption is to employ CBDC for government payments. Delivering pensions and benefits and taking taxes and other payments in CBDC is likely to ensure a high adoption rate.

Other central banks focused on cybersecurity as their main concern, which may indicate a need for third-party cyber-security consultation services. Bank disintermediation is a smaller concern.

Only 17% of survey respondents said they were worried that CBDC issuance would compromise banks’ business models or funding habits. In a separate survey on commercial banks’ thoughts on CBDCs, one respondent explained that they ‘do not believe it would be in the interest of central banks to disintermediate [commercial] banks.’ Rather, commercial banks expect to work alongside central banks for their CBDC projects – all respondents in the commercial bank survey indicated that they expect to be involved with central banks as a wallet provider, for credit creation and know-your-customer compliance.

BANKS WILL NOT HAVE EXCLUSIVE POWER TO DISTRIBUTE CBDC

While it is widely expected that central banks will work with commercial banks on CBDC, almost all surveyed central banks intend for their CBDC to be distributed by a range of new regulated private sector providers as well as banks.

Furthermore, survey participants reported the need for all private sector third-parties enquired about, including for the technical development of

digital currencies, marketing, promotion of digital currencies, and KYC capacity (Figure 7).

Central banks are clearly not working alone (Figure 8). Central banks, including 33% of the share of those who do not expect to issue a digital currency, are working with a range of third-party services. Central banks’ research and exploratory phases account for most of the involvement of these services.

Survey respondents are working with technology providers (71%), academics (47%) and strategy advisory services (47%) in this phase. The low concern with bank disintermediation is highlighted here too, with 47% of respondents working with commercial

banks and 71% intending to work with them in the future.

Looking to future involvement, 88% and 71% of respondents intend to work with technology providers and commercial banks respectively (Figure 8), reinforcing commercial banks’ beliefs that bank disintermediation will not be an issue. While few central banks are working with marketing and promotion providers right now (6%), many intend to work with them in the future (47%), indicating that respondents are taking steps to pre-empt low adoption as they move on to the pilot and launch phases of their CBDCs. •

THE FIRST CBDCs IN DEPLOYMENT

Developing economies, particularly those in the Caribbean, have been at the forefront of testing and launching central bank digital currencies.

BAHAMAS

March 2019: Selected NZIA as the preferred solutions provider and announced its pilot programme: Project Sand Dollar

May 2019: Signed partnership contract with NZIA.

November 2019: Special session of the National Payments Council was convened to confirm the approach to the central bank digital currency project.

Summer 2019: The central bank conducted a targeted baseline survey on financial inclusion and access for Exuma.

27 December 2019: Began Project Sand Dollar pilot in Exuma.

28 February 2020: Pilot expanded was to the Abaco islands.

October 2020: National rollout of Project Sand Dollar to the rest of the Bahamas.

July 2022: Value of Sand Dollars in circulation reached 300,000 Bahamian dollars, with 30,000 individuals who have mobile wallets and 845 merchants who accept it.



NIGERIA

July 2021: Design phase of CBDC project

30 August 2021: Announced a partnership with Bitt and issued preliminary guidelines for Project eNaira.

28 September 2021: The eNaira website goes live.

25 October 2021: eNaira launched.

December 2021: 600,000 eNaira wallets had been created and more than 35,000 transactions had taken place.

25 August 2022: The Central Bank of Nigeria releases the option to create an eNaira wallet with unstructured supplementary service data, where users dial a four-digit code on their mobile phones.



EASTERN CARIBBEAN CENTRAL BANK

(eastern Caribbean states)

2019: Began development of digital currency.

12 February 2021: First DCash transaction was successfully carried out.

31 March 2021: Launched DCash in Antigua and Barbuda, Grenada, Saint Kitts and Nevis, and Saint Lucia, becoming the first currency union central bank to issue digital cash.

30 July 2021: DCash was launched in Saint Vincent and the Grenadines.

7 December 2021: DCash went live in Dominica and Montserrat.

14 Jan 2022: DCash temporarily went offline due to a technical issue where customers could not transact using the wallet.

7 March 2022: DCash resumed service with an enhanced security design for the system.

29 June 2022: DCash was launched in Anguilla, its final member state



JAMAICA

17 July 2020: The Bank of Jamaica issued its formal invitation to CBDC providers to join its Fintech Regulatory Sandbo

May 2021: The BoJ started working with eCurrency Mint on regulatory sandbox project

9 August 2021: The BoJ minted 230m Jamaican dollars worth of digital currency.

December 2021: In partnership with the National Commercial Bank, the BoJ 57 customers were on boarded in the pilot.

31 December 2021: The BoJ announced the successful completion of the pilot.

February 2022: The BoJ announced name for CBDC, Jamaican Digital Exchange (JAM-DEX).

11 July 2022: JAM-DEX launched on the Lynk digital wallet.





DRIVING INTEROPERABILITY IN CROSS-BORDER PAYMENTS

New technology brings with it new challenges, such as integrating legacy systems with novel ones. Swift is making this possible though, writes Saskia Devolder, strategic programme director, cross-border payments, Swift

IN TODAY'S digital economy, transactions must be instant and frictionless – whenever and wherever they need to go.

That's no small feat when money starts moving across borders, especially when considering the myriad factors that must be taken into account, from navigating different time zones, processing approaches and domestic payments systems, to understanding compliance requirements in numerous jurisdictions. Increasingly, there's a need to consider possible new forms of value too – from central bank digital currencies to tokenised assets.

Swift sits at the heart of the cross-border payments ecosystem, ensuring payments reach their destinations quickly, securely and compliantly. Through our network of more than 11,500 institutions in over 200 countries and territories, money can be sent anywhere in the world – even to the most remote locations. And our commitment to responsible innovation means every day the experience gets faster and better while maintaining the highest levels of security, resiliency and reliability.

We've made strong progress over the past two years with a strategic focus on enabling instant and frictionless processing between 4bn accounts worldwide, aligned with the G20's objectives of improving speed, cost, transparency, choice and access in the cross-border payments experience. Swift's achievements include:

Speed: Most payments over Swift today use gpi and nearly half reach their end beneficiaries within five minutes and two-thirds arrive within one hour, well on the way to achieving the G20 goal of having 75% of international payments settling within 60 minutes by 2027. Correspondent banking has been delivering secure, compliant cross-border payments and banks use intermediaries to access the required currency within a specific jurisdiction. There has been a steady decline in the number of correspondent banks involved in a payment – today, 73.9% of all cross-border transactions involve just one or no intermediary.

Transparency: By embedding a unique tracking code in every transaction, Swift has enabled banks to have complete visibility on the status and costs of transactions with real-time tracking all along the process – just like tracking a parcel delivery. This has provided unprecedented insight into the frictions that slow down payments. We know from this data, for instance, that the biggest impact on speed comes from capital controls and domestic regulatory requirements. For banks in countries with capital controls, the time taken by the beneficiary side is nearly three times that for banks in countries without them. This issue has been recognised by the Committee on Payments and Market Infrastructures as part of its focus on an efficient legal, regulatory and supervisory environment for cross-border payments.

Costs: One of the other frictions is incorrect beneficiary information – such as typos and transposed account numbers – that breaks automated processing and requires manual intervention to resolve. Swift has introduced an application programming interface-based pre-validation service, which allows sending banks to verify beneficiary data upfront, before executing the transaction. For banks not ready for pre-validation, Swift provides a pre-check of the account details against pseudonymised and aggregated data from more than 4bn accounts to catch errors before a payment is sent. Its deployment, which could save the industry millions each year, currently covers 70% of beneficiary accounts in major markets.



FOR BANKS IN COUNTRIES WITH CAPITAL CONTROLS, THE TIME TAKEN BY THE BENEFICIARY SIDE IS NEARLY THREE TIMES THAT FOR BANKS IN COUNTRIES WITHOUT THEM

Choice: Swift has not only focused on bringing these benefits to high value wholesale payments, it's also improved the experience for small businesses and consumers who send low-value payments around the world. Through Swift Go, we have established a new standard for payments under \$10,000, bringing new levels of speed, transparency and certainty for account to account transfers. In 2022, signups for the service tripled to more than 500 banks across more than 120 countries.

The pandemic kick-started digitalisation. And with new technology and shifts in the geopolitical landscape emerging, market players continue to rush to develop new solutions to enhance cross-border payments, with a focus on front-end solutions. Central banks, too, are exploring digital currencies to pursue the G20's goals – but are largely focusing on domestic use. Taken together, these factors are increasing fragmentation. Without a focus on back-office evolution, we risk the emergence of digital islands: solutions that operate in silos and which are not compliant or interoperable with each other.

With digital currencies, stablecoins and other digital assets set to enter the market at scale, we need to guarantee interoperability with existing systems that consumers and businesses rely on and that have proven their value to the economic system.

Swift has always focused on interoperability. It is central to instant and frictionless payments. The importance of standardisation, too, has recently been recognised by the G20 in its reprioritised programme for cross-border payments enhancements, particularly the importance of ISO 20022. This new international standard can carry much more information than older solutions, but that data is also more structured, ensuring the efficient execution of compliance requirements for cross-border payments.

Swift's new transaction management platform, set to roll-out in 2023, enables interoperability

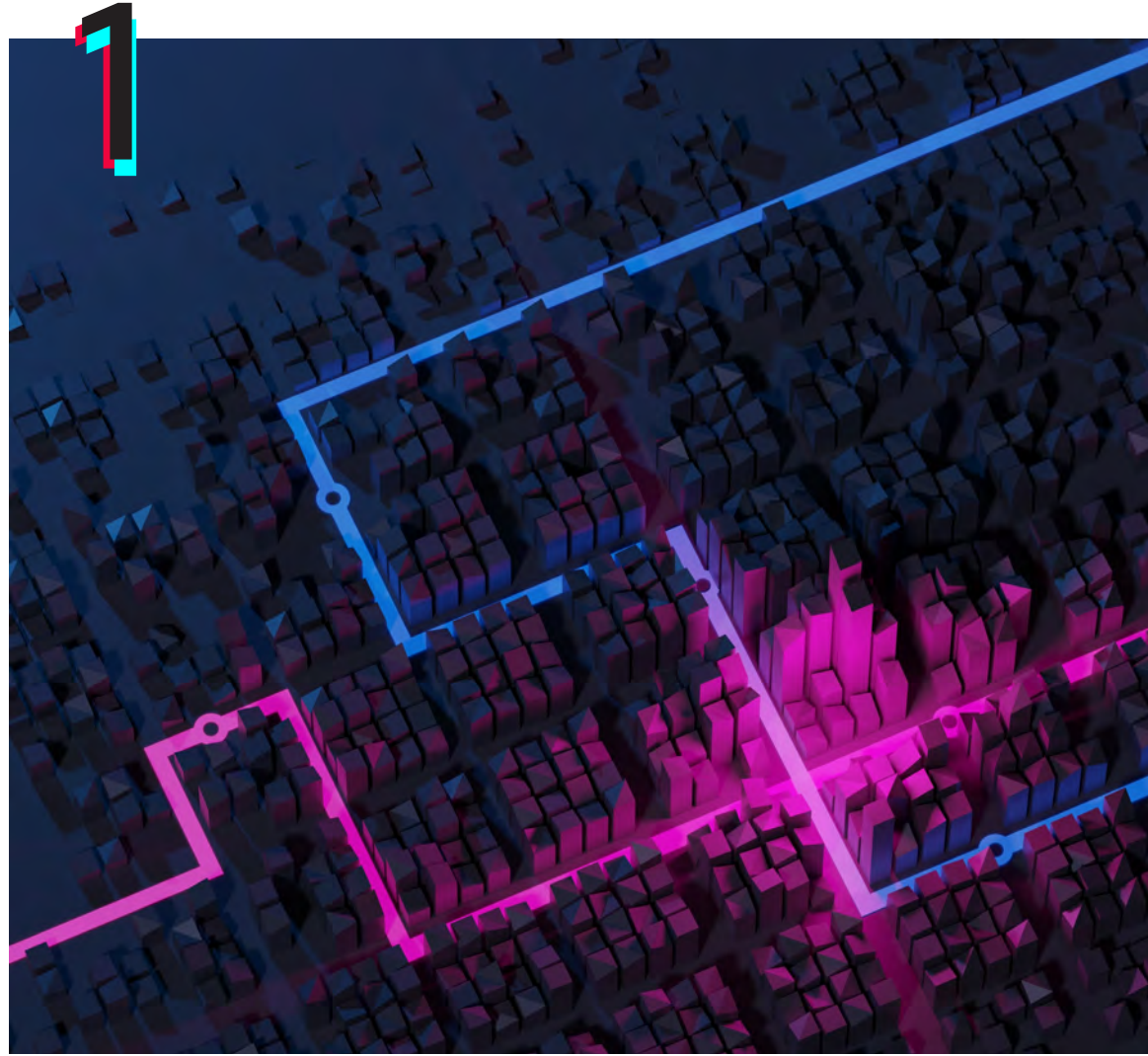


THE IMPORTANCE OF STANDARDISATION, TOO, HAS RECENTLY BEEN RECOGNISED BY THE G20 IN ITS REPRIORITISED PROGRAMME FOR CROSS-BORDER PAYMENTS ENHANCEMENTS, PARTICULARLY THE IMPORTANCE OF ISO 20022

between ISO 20022 messaging and legacy messaging, thanks to an integral in-flow translation service. The platform provides new orchestration capabilities, providing banks with richer, better structured data to make use of new API-based technology for an enhanced payment execution experience. Every bank in the chain will have access to all required data for compliance requirements. Other API-based tools, such as pre-validation, help remove friction while gpi instant allows an anchor bank to provide access to the domestic instant payments system in the destination market – giving fast settlement and the immediate posting of the funds to the beneficiary account.

Swift continues to closely monitor new payments methods, settlement mechanisms and currency types, including CBDCs. Our collaborative experiments early this year successfully demonstrated interoperability between CBDCs built on different distributed ledger technologies, and between these and fiat currency. This solution is now being tested further with 18 central and commercial banks. This experiment forms part of our robust innovation agenda in support of our strategic goals.

It is through experiments such as these that we will achieve interoperability in cross-border payments and enable customers of all types to make instant and frictionless transactions at any time, anywhere and for any purpose. •



TURNING THE CROSS-BORDER PAYMENTS ROADMAP INTO REALITY

Progress has been made on interoperability and regulatory frameworks, but bottlenecks remain on data localisation. By Taylor Pearce

CROSS-BORDER payments are the ‘forgotten corner of the world’s financial plumbing’. This bleak characterisation came in a 2020 stocktaking exercise conducted by the Bank for International Settlements Innovation Hub, International Monetary Fund and World Bank. While significant progress has been made within domestic markets – within which payments have become markedly faster, cheaper and more intuitive – sending payments abroad has developed much more slowly. Despite the manifold benefits of improving multilateral platforms, cross-border payments remain comparatively slow, costly and less transparent.

BENEFITS OF ENHANCED CROSS-BORDER PAYMENTS

For both correspondent institutions and end users, there are myriad potential benefits of enhancing cross-border payments. The turnaround on cross-border payments conducted through traditional bank transfers can take up to five days, compared to the nearly instant service offered domestically. Bank account balances can only be updated during the hours when the underlying settlement systems are open. In most jurisdictions, these systems are aligned to normal business hours, which can cause delays in clearance and settlement. As

KEY FINDINGS

1. The reception of the G20 Roadmap for Enhancing Cross Border Payments has been positive. Regulators and private sector stakeholders are largely aligned.

2. Both technological and regulatory progress is being made to enhance fiat-based cross-border payments in areas such as interoperability and regulatory harmonisation.

3. The challenge of facilitating cross-border data exchange presents a significant hurdle, undermining the potential for a fully centralised cross-border payments system with a global reach.

4. Regionally integrated payment networks offer an exciting prospect.

noted by the Committee on Payments and Market Infrastructures’ roadmap, mismatched operating hours of payments infrastructures can lead to higher liquidity costs and settlement risk for banks and financial intermediaries and to delays for payment recipients.

Moreover, in legacy systems, banks initiating cross-border payments rely on accounts in other banks (known as correspondent banks) in other jurisdictions to move money across borders and make payments on their clients’ behalf. This is not only slow, but expensive – fees compound as multiple intermediaries in the payment chain charge a fee. This can drive up costs even without factoring in foreign exchange spreads, which can themselves vary widely based on the user’s access to the best liquidity providers.

The frictions in cross-border payments systems are especially costly for developing countries. World Bank and IMF data indicate that the value of personal remittances received reached \$661bn in 2019 and is still rising. A 2022 report on digital remittances published by the Visa Economic Empowerment Institute estimated that the average cost of remittances at approximately 6% of the total sent (in line with the World Bank’s estimate), with the average cost of cash-funded remittances averaging slightly higher at 6.5%. While the same report found that a higher share of remittances is digitally initiated than ever before, this number still only reflects about a third (34%) of remittance flows. Given that cash-initiated remittances remain the most expensive way for

migrant workers to send money to their home countries, it is imperative to improve and expand digital remittance services.

Hence, the data reveals that facilitating better cross-border payments will bring down the cost and processing time of international transactions. For developing countries which receive a substantial proportion of their gross domestic product via remittance flows, improving payments infrastructure is even more important.

PROPOSED SOLUTIONS: CPMI ROADMAP

To understand the difficulties of enhancing cross-border payments systems, it is important to note the difference between a domestic payment and cross-border payment. Saskia Devolder, strategic programme director, cross-border payments at Swift, noted a few key factors which differentiate cross-border payments from their domestic counterparts: the need for foreign exchange and the need for compliance requirements, including sanctions screening according to the regulation in the destination country. For Devolder, although technological innovations can offer some improvements related to the speed and complexity of both foreign exchange and compliance, there is no ‘magic bullet’ to solving these issues.

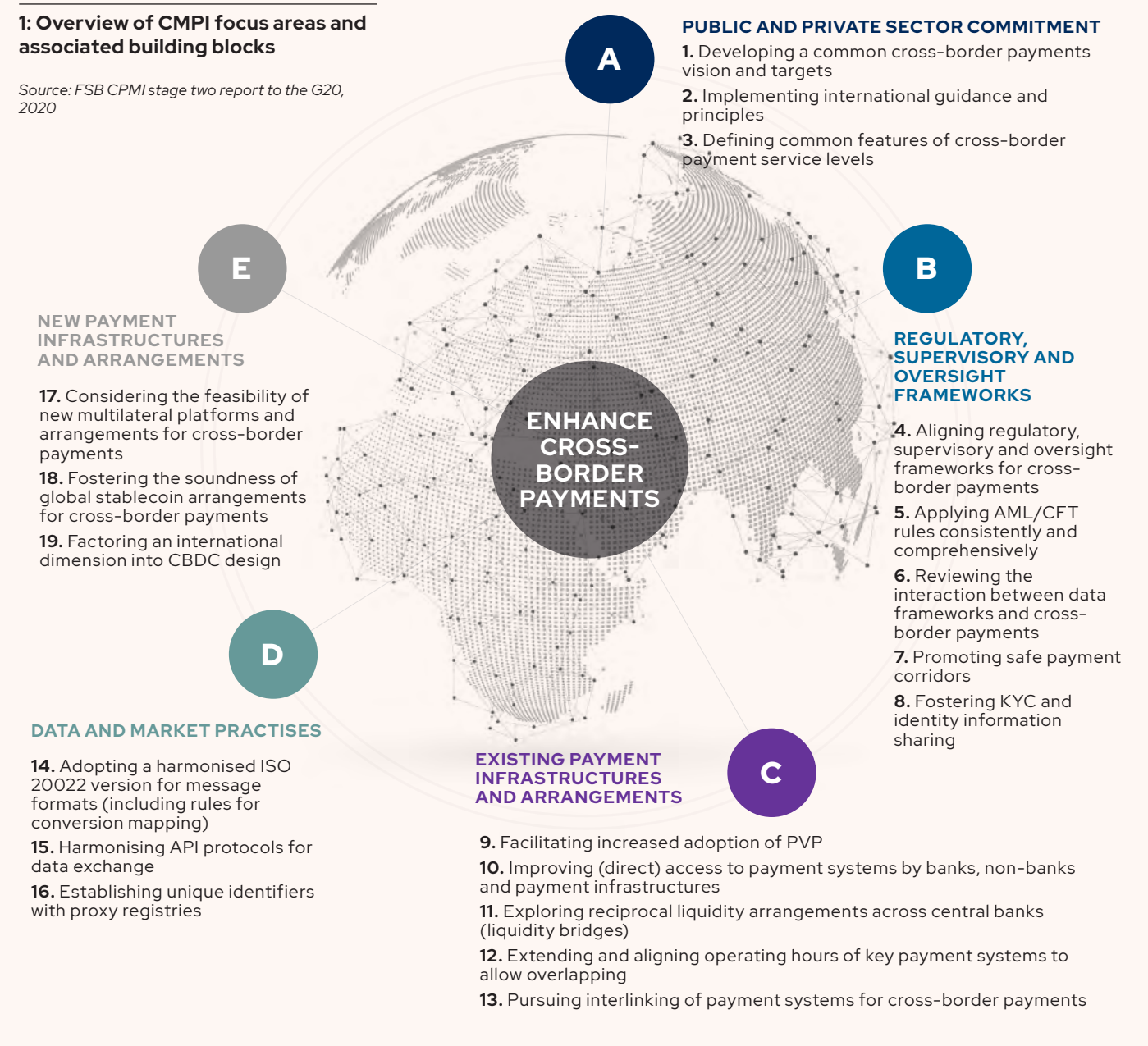
Correspondingly, while many players are trying to innovate their way around these challenges, ‘to think that this is about shaving off idiosyncratic differences between systems is wrong,’ noted one OMFIF interviewee from the payments industry. As those operating in the cross-border payments space are discovering, the differences between domestic payments infrastructures are nontrivial and the challenges facing legacy systems are not always able to be solved by technological innovation: ‘Different countries have developed payments systems in various social, political and historical contexts, and the inputs they require are genuinely different,’ as noted by the interviewee. Therefore, the first step to engaging with cross-border payments is recognising these challenges.

The most comprehensive effort to address the persistent difficulties involved in the deeper integration of cross-border payments systems is being spearheaded by the CPMI’s ‘Roadmap for Enhancing Cross Border Payments’ initiative, overseen by the Financial Stability Board. Its objectives consist of five focus areas (Figure 1) which, together with their respective building blocks, address three cornerstone issues persisting



THE CPMI ROADMAP INDICATES THE NEED FOR NBFIs TO BE SUBJECT TO REGULATIONS “PROPORTIONATE TO THE RISK THEY POSE.”





in present cross-border payments ecosystems: payments system interoperability and extension; legal, regulatory and supervisory frameworks; and cross-border data exchange.

PAYMENTS SYSTEM INTEROPERABILITY

On interoperability, several technological innovations are contributing to more efficient systems. One promising development is ISO 20022, a universal message standard for the financial industry introduced by the International Organization for Standardization and associated with building block 14 of the roadmap. By providing a metadata repository along with a maintenance process, ISO 20022 offers a common language for data exchange. In this way, the system provides a means for communication between financial

institutions and their payments ecosystems.

Over 70 countries have already migrated to ISO 20022, from South Africa and Japan to Switzerland. According to the ISO, convergence into one standard is the long-term objective. And it appears headed in that direction. From March 2023, Swift will also transition to ISO 20022 and a BIS publication from this year anticipated that most of the world’s payments systems will adopt the standard by 2025. The hope is that the standardisation brought about by ISO 20022 will alleviate some of the current bottlenecks in data processing across jurisdictions. Interviewees shared a positive outlook on the standard’s potential for easing interoperability.

Progress is also being made on building block 15, harmonising application programming interface protocols, software interfaces that

enable computers to communicate with one another, precluding the need for end user operation. Bringing APIs into alignment has the potential to help streamline payments operations though automation, significantly improving efficiency. Harmonising APIs can also facilitate payment orchestration. The latest iteration of the CPMI roadmap found that a growing number of payments systems are in the process of being interlinked by leveraging APIs, a trend that is anticipated to continue. In response, the CPMI intends to ‘play an active role in kick-starting’ the initiative for the harmonisation of APIs and is in the process of establishing a working group consisting of API developers and representatives from governance bodies to collaboration on harmonisation.

In addition, the increased adoption of payment-versus-payment mechanisms (building block 9) is helping streamline foreign exchange transactions across platforms. While PvP arrangements are available for the most-traded currency pairs, PvP adoption is needed in all jurisdictions to help remove frictions in correspondent banking. The CPMI is consulting with both domestic and international stakeholders until January 2023, the findings of which will be the basis of an implementation plan.

Discussions with practitioners in the cross-border payments space indicate that multilateral platforms are exploring the use of new tools and innovations, such as distributed ledger technologies, blockchain, cloud technology and artificial intelligence. Although they are still in the early stages of the development, these potentially more ‘disruptive’ technologies could also have significant potential to facilitate payments system interoperability within fiat-based systems.

REGULATORY AND SUPERVISORY FRAMEWORKS

Under building block four, the CMPI roadmap also highlights three areas where regulatory gaps exist and may need to be addressed by international standards. First, while robust regulation is in place for banks in respect of their cross-border payments activities, non-bank financial institutions are not yet subject to the same level of supervision. The CPMI roadmap indicates the need for NBFIs to be subject to regulations ‘proportionate to the risk they pose’, as inconsistent standards or implementation could lead to blind spots about potential risks or risk management gaps within the financial system. Devolder noted that creating a ‘level playing field’ among banks, NBFIs and fintechs is something the G20 is working towards. She emphasised that regulators in the fintech space need to strike the balance between fostering innovation and ensuring entities involved in payments are subject to the same regulations and operational requirements.



BUT THE CHALLENGE OF FACILITATING CROSS-BORDER DATA EXCHANGE PRESENTS A SIGNIFICANT HURDLE, UNDERMINING THE POTENTIAL FOR A FULLY CENTRALISED CROSS-BORDER PAYMENTS SYSTEM WITH A GLOBAL REACH

The second regulatory gap identified by the CPMI roadmap is the transparency of information provided to end users about transactions. According to a Swift white paper from January 2022, unique transaction identifiers could offer a solution. Industry-wide adoption of UTIs would help reduce risk and increase transparency across the transaction system, which could be brought to fruition with widespread migration to ISO 20022. Lastly, the roadmap highlights cyber/technology risk regulation as a potential regulatory gap, addressed by building block five by applying anti-money-laundering and countering terrorist financing rules consistently and comprehensively.

In response to the potential regulatory blind spot posed by a lack of comprehensive NBFi supervision, the FSB is establishing a working group to further explore and make recommendations related to the application of supervision to banks and non-banks concerning their cross-border payments activities. Meanwhile, regarding the transparency of information provided to end users about payment transactions and cyber risk regulation, the FSB is creating workstreams to evaluate both issues. Originally planned for March 2022–March 2023, but delayed by one year, the next step for facilitating regulatory harmonisation outlined by the CPMI roadmap is for the FSB to provide a report for public consultation on these three key areas. This stage should help address the gaps identified by the stock-taking exercise, which will then be followed by relevant national authorities to communicate their plans for alignment the following year.

CROSS-BORDER DATA EXCHANGE

Innovations like ISO 20022 are facilitating easier data exchange between financial institutions and payments services providers. But while demonstrable progress has been made on the technical interoperability of cross-border payments systems, as well as harmonising their regulatory and supervisory frameworks, an interviewee expressed concern that data localisation is ‘one area where things are moving aggressively and quickly in the wrong direction’. This, they explained, is in large part due to the proliferation of data localisation requirements, or laws requiring data to be collected, processed and/or stored within a given country before being able to be sent abroad.

According to data from the United Nations Conference on Trade and Development, over 70%



of countries have implemented some form of data localisation requirement. China, India and Russia have the highest number of localisation measures in place – three countries which have a low level of integration in cross-border payments system networks (though India began accepting cross-border payments this year following a law passed by the Reserve Bank of India in September 2022). The move towards mandated data residency has had tangibly negative impacts on the efficiency of cross border payments systems.

There are a variety of driving factors behind this trend. For one, there are genuine security concerns associated with storing data abroad. ‘Law enforcement wants to know that they can access relevant data in order to pursue cases to keep citizens safe,’ stated one interviewee. Therefore, ‘law enforcement sees keeping data on shore as one way to do this and avoid what could be a complicated process to subpoena someone if that data is stored abroad rather than if it is stored locally.’ The same case can be made for regulatory oversight, evidenced in the US Securities and Exchange Commission initially pursuing data localisation for financial oversight purposes before backtracking.

Another rationale for data localisation requirements is countries’ concern about the prospect of data being used by others and not by them for consumer protection considerations. Another expert in the digital payments industry noted that ‘cultural constructs and consumer preferences around privacy vary significantly from country to country,’ with the European Union being an outlier in prioritising consumer data protection through its comprehensive General Data Protection Regulation.

A less benign rationale in favour of data localisation is digital industrial policy, whereby policy-makers look to use data localisation requirements to favour local cloud service providers. This strategy, though it has gained support among United Nations Conference on Trade and Development and other heterodox economists, is essentially a form of trade protectionism. And while countries, especially emerging markets, may have legitimate developmental considerations which underly data localisation rules, the more barriers to cross-border data flows there are, the more difficult it will be to facilitate cross-border payments.

GLOBAL PROBLEM, REGIONAL SOLUTION?

In the absence of a globalised multilateral payment system, an interconnected regional system could be the way forward. In 2018, the Eurosystem launched its Trans-European Automated Real-time Gross settlement Express Transfer (TARGET) Instant Payment Settlement (TIPS) infrastructure service, enabling individuals and financial institutions to ‘transfer money between each other within seconds,



THE MOST COMPREHENSIVE EFFORT TO ADDRESS THE PERSISTENT DIFFICULTIES INVOLVED IN THE DEEPER INTEGRATION OF CROSS-BORDER PAYMENTS SYSTEMS IS BEING SPEARHEADED BY THE CPMI.

irrespective of the opening outs of their local bank.’ As a currency union, the euro area has the benefit of bypassing the foreign exchange challenges facing cross-border payments systems, making it easier to develop payments infrastructure among member countries. Since its inception, however, the central banks of Sweden, Denmark and Norway have also expressed interested in joining TIPS. The Eurosystem and Sveriges Riksbank are actively exploring a potential cross-currency settlement feature (including PvP) with TIPS, which would integrate transactions between the euro and krona.

Among developing countries, Association of Southeast Asian Nations member states are also working towards a regionally integrated payments network. In April 2021, the Monetary Authority of Singapore and the Bank of Thailand inaugurated a novel linkage of real-time payments systems, which resulted in markedly lower transaction costs and faster processing speeds for cross-border payments between the two countries. What originated as a bilateral system has since become a blueprint for establishing a region-wide payments ecosystem.

In November 2022, a memorandum of understanding on co-operation in regional payment connectivity was reached by several countries at the G20 Bali summit, expanding the system to include Bank Indonesia, Bank Negara Malaysia and Bangko Sentral ng Pilipinas. This collaboration is a part of Asean’s aspiration for a region-wide connected payments system by 2025. Speaking at the summit, Ravi Menon, managing director of MAS, confirmed that Asean’s effort in the cross-border payments space ‘is aligned with the G20’s goal of addressing existing frictions in global cross-border payments, creating new business opportunities and enabling inclusive growth’.

Another pioneering initiative in regional integration is the Pan-African Payment and Settlement System. PAPSS was developed in response to a fundamental problem facing the African continent: ‘Africa doesn’t trade with itself – it has the lowest trade among all continents, and trade is critical to economic prosperity,’ explained PAPSS Chief Executive Officer Mike Ogbalu. ‘Considering all the different things that affect trade, we came to the realisation that, unless we deal with the subject of payment, African trade will not take off, and that will have an effect on the prosperity of the continent.’ The idea of the African

Export-Import Bank, PAPSS is seeking to transform how payments are made across borders in Africa, facilitating the expansion and diversification of interregional and international trade on the continent.

At present, 80% of commercial cross-border transactions within Africa must travel halfway around the world to be processed, mostly through the US or UK, before returning to the continent. This results in higher costs and more delays in cross-border payments, which PAPSS is aiming to alleviate.

The PAPSS infrastructure supports multiple settlement currencies. Within the platform, each country can set their rates against any other currency. Each transaction then creates a settlement obligation, with only net positions moving between the different counties. Liquidity is provided by central banks, largely in line with the Principles for Financial Market Infrastructures’ settlement model, but the system supports multiple settlement models as well. ‘We recognise that there will be balance of trade issues and that flows may be skewed in favour of certain entities,’ stated Ogbalu. In response, a settlement guarantee fund of \$500m was developed for west Africa, with intentions to increase this to \$3bn as PAPPSS scales across the continent.

Currently, eight central banks, 50 commercial and seven switches (including both national and private sector ones) are connected to the PAPSS ecosystem. An additional five entities are in alliance with the network, including the settlement platform operated by the Arab region’s payment and clearinghouse system, Buna. And the PAPSS network is expanding fast: ‘We should be able to double the footprint we have today by the end of Q2 next year,’ stated Ogbalu. ‘We are hoping to cover 70%-80% of the continent in the next three years,’ with the end goal being complete regional integration in payments systems across Africa.

Ogbalu expressed optimism at the prospect of developing region payments systems and having another platform, such as Swift, facilitating transactions between regional systems, thereby offering a hub-and-spoke model of cross-border payments. Dave Sissens, chief executive officer of RTGS.global, a financial market infrastructure facilitating cross-border payments in the wholesale market, also expressed optimism about a regionalised approach. He noted that: ‘Given the existing trust between trading countries and counterparties, it makes perfect sense for regional solutions to thrive.’

With the launch of its pioneering project Nexus, a model for connecting national payment systems into a cross-border platform, a hub-and-spoke model is also being support by the BIS. Having entered the testing phase, the initiative is using simulated payments to test the interlinkage of the

80%

The majority of cross-border transactions in Africa have to travel outside of the continent to be processed

>70

More countries are migrating to the ISO20022, a universal message standard for the financial industry

\$661bn

Value of personal remittances in 2019

>70%

Data localisation rules have been put in place by most of the world’s countries

payments systems of Singapore, Malaysia and the euro area, with the hope of expanding to include more national payments systems.

THE WAY FORWARD

Conversations with experts in the cross-border payments systems space suggest that the CPMI roadmap has been positively received – there appears to be a general sense that regulators and private sector innovators are aligned in their desire to improve the cross-border payments landscape. Technological and regulatory progress is being made, with developments in both interoperability and regulatory harmonisation.

But the challenge of facilitating cross-border data exchange presents a significant hurdle, undermining the potential for a fully centralised cross-border payments system with a global reach. Cross-border data flows are a crucial element to the development of any efficient multilateral payments ecosystem, but the protectionist trend reflects a world which is becoming more fragmented, undermining the globalisation of payments systems.

Concluding the final action for building block 17, the CPMI will publish a report considering the feasibility of new multilateral platforms and arrangements for cross-border payments by the end of 2022. In the meantime, regionally integrated payments networks offer an exciting prospect. Where multilateral initiatives stall, stand-out cases like Asean’s RPC and PAPSS illustrate the promise of regional projects, which could be especially exciting for developing markets. As a completely globalised and centralised retail payments system seems increasingly unlikely, a hub-and-spoke model is certainly an alternative worth exploring for the future of fiat-based cross-border payments. •



WHY REMITTANCES MUST GO DIGITAL

Remittance inflows are critical—and they have been resilient in challenging times, by Chad Harper, senior fellow, Visa Economic Empowerment Institute

REMITTANCES proved surprisingly resilient during the pandemic and inflows for 2021 were very strong, reaching \$773bn globally and \$605bn for low- and middle-income countries. In addition to being a critical lifeline for families, remittances play an important role in the economies of many countries. In 2021, 30 countries received over 10% of their gross domestic product from remittances.

Border closures and business lockdowns in the early days of the Covid-19 helped digital money movement options flourish. These offer a variety of advantages for senders and receivers, including cost, security and speed. However, only a third of remittances are initiated digitally and only one-third of those are picked up digitally. Focus needs to be on how to enable more of these digital transfers (see Figure 1).

Costs are still high for the average remittance, but are much lower for digital remittances and in cases where people can compare multiple options.

As of the second quarter of 2022, World Bank remittance price data show that:

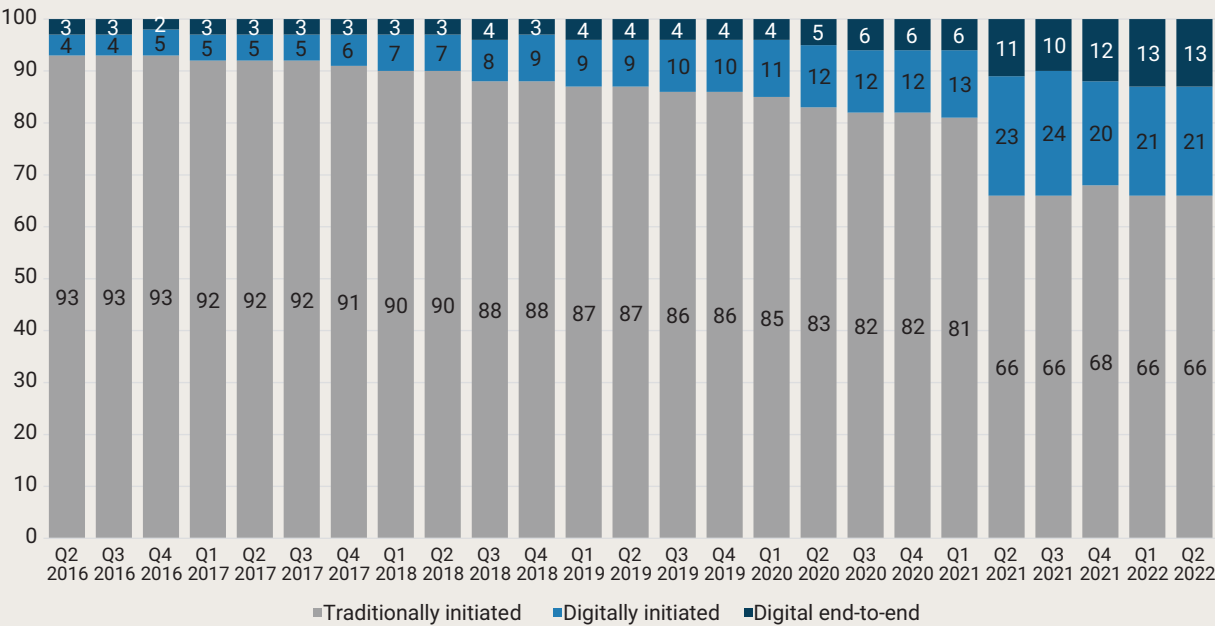
- The average \$200 remittance costs 6% – this is the headline number policy-makers most often mention.
- The digital remittances index (for remittances digitally initiated in an online or self-assisted way) is 4.8%.
- The Smart Remitter Target (SmaRT) index (a measure of what a savvy consumer with access to sufficiently complete information could pay) is 3.4% – almost at the 3% UN sustainable development goal target.

These observations are confirmed by Visa Economic Empowerment Institute modeling of card-initiated digital remittances over the last two years. In the modeling, VEEI determined costs across several money transfer operators for 25 key global corridors and compiled three measures: the average cost, lowest cost and highest cost.

- The average costs for a \$200 remittance across all

Figure 1: There has been a shift to digital remittances, but most are still traditional

Digital remittance trends over 24 quarters, 2016-2022



Source: VEEI/Devtech Systems analysis of WBG Remittance Prices Worldwide Quarterly data

MTOs and corridors declined to 3.9% from 4.2% in 2022, a drop of 10%.

- The average of the lowest costs declined to 2.1% in 2022 from 3%, a decline of almost 30% – this measure is roughly analogous to the World Bank’s SmaRT index.
- By contrast, the average of the highest costs went up to 7.1% from 6.2%, driven largely by two corridors, where MTOs were offered dramatically different pricing. Migrant workers without the ability to check multiple options could have paid exceptionally high prices (and some undoubtedly did) during this period.

Overall, while the average price of a remittance in the research was 3.9%, VEEI was able to find costs below 3% in 20 of the 25 corridors in 2022.

Clearly, the ability to send remittances digitally and to easily compare transfer options make a big difference to senders and their families. So, what needs to happen?

Traditional remittances must become digital. Cash-initiated remittances are the most expensive way to send a remittance and it is perhaps worse on the receiving end – many MTOs maintain vast cash out networks in receiving countries and this adds appreciable costs to remittances today.

Migrant workers must be able to compare options and send remittances digitally. Their families must be able to then spend the funds digitally at businesses in their communities. None of this can happen without basic digital infrastructure.

Innovation must be facilitated by more consistently applied compliance rules and consumer choice needs to be promoted by making it easier for remittance providers to bring new innovations to market.

UNLOCKING THE BENEFITS OF DIGITAL REMITTANCES

Five steps will help unlock the benefits of innovation and digitalisation for more people while also uplifting businesses and communities.

First, begin with digital enabling infrastructure if it does not already exist. The digital receipt and use of remittances will be a non-starter without basic enabling infrastructure. For millions of people, basic infrastructure like electricity will be a barrier to the digitalisation of remittances, payments and commerce. Beyond electricity, internet connectivity – and broadband connectivity – will be crucial.



MIGRANT WORKERS MUST BE ABLE TO COMPARE OPTIONS AND SEND REMITTANCES DIGITALLY. THEIR FAMILIES MUST BE ABLE TO THEN SPEND THE FUNDS DIGITALLY AT BUSINESSES IN THEIR COMMUNITIES

Second, focus on digital enablement broadly, keeping both consumers and businesses in mind. While the digital receipt of remittances is critical for further progress on efficiency, the larger goal is to digitally enable everyone, everywhere to fully participate in this new world. Individuals need to be able to receive remittance funds and use them digitally, with ubiquity. This requires digitally enabling businesses, especially small businesses, helping them to accept digital payments and to connect them to digital marketplaces. Therefore, consumers and businesses must both be part of the equation in achieving digital ubiquity. Countries that have driven digital ubiquity most successfully over the last decade have worked to drive adoption on both sides.

Third, aim for an open, interoperable digital ecosystem built on a foundation of resilience and security. Interoperability should be favored over uniformity – more paths are better than one. A truly interoperable service should be able to reach as many endpoints as possible: traditional bank accounts, prepaid accounts and digital wallets.

Fourth, streamline the compliance environment to reduce cross-border frictions. While the private sector is innovating, competing and improving speed and efficiency, policy-makers have a key role to play. Remittances go through a number of regulatory regimes that currently add frictions. But these can be reduced by streamlining and aligning compliance rules as much as possible.

Finally, simplify the licensing process to allow remittance innovation and competition to thrive. Policy-makers can also help the private sector introduce innovations more quickly and with less burden. Consistent licensing requirements would help remittance service providers enter and operate across multiple geographies with less friction. Streamlining licensing requirements and processes will help new market entrants bring the benefits of digital remittances to more corridors, and therefore to more people. •



CRYPTO'S CRUCIAL APPEAL FOR EMERGING MARKETS

The benefits of accessibility offer the best hope for digital currencies to have a profound impact on payments systems. By Lewis McLellan

IN developed markets, cryptocurrencies have had little hope of catching on as mainstream channels for payments. If one can rely on stable prices and trustworthy institutions, the volatility of cryptocurrencies makes them an unpopular choice as a means of exchange, though they are a popular speculative investment.

The currency in which most goods and services are paid for, and taxes and wages are paid in, is typically the currency in which most citizens will keep their assets. If the systems and institutions serving fiat currency function effectively, then the primary appeal of cryptocurrencies for most will be as a speculative asset.

However, when a domestic currency is dysfunctional, citizens are more eager to look for an alternative. Traditionally, this has been the dollar. The arrival of cryptocurrencies and their stablecoin

cousins has added new alternative systems for citizens and businesses.

A cryptocurrency is a token traded on a distributed ledger — a form of record-keeping that can provide security without the need for an intermediary. Stablecoins are cryptocurrencies that, rather than having a value determined by the marketplace, seek to maintain parity with another asset's value, typically the dollar or another fiat currency.

There are three basic advantages that cryptocurrencies offer in cross-border payments when compared to traditional methods. First, because cryptocurrencies can be traded in the absence of an intermediary, they do not rely on institutions' opening hours for operations. This simple distinction offers a major advantage in cross-border payments, where time zones mean that, for

KEY FINDINGS

1. For countries with high inflation and strict capital controls, cryptocurrency offers a popular, though risky, alternative to the traditional financial system.
2. Stablecoins offer many of the benefits of cryptocurrencies without the volatility, but not all are safe and robust solutions.
3. Vulnerable nations should invest in bringing down the cost of remittances and broadening access to financial services to reduce the exposure of vulnerable economic groups to volatile and unsafe cryptocurrency products.

some corridors, settlement can take over a day as transactions wait for correspondent banks to open to be settled.

Second, though cryptocurrency transactions are not free, many can offer savings versus some of the more expensive remittance corridors.

Crypto's final advantage is accessibility. This is particularly an issue in emerging markets. According to the World Bank, 1.4bn people around the world are unbanked. Whether the challenge is simply accessing physical infrastructure, overcoming high fees, a lack of trust in institutions or the absence of the requisite identity documents, cryptocurrency offers an opportunity for many of these people to have access to digital money, rather than relying on cash.

There are, of course, risks that come with embracing cryptocurrency as an option, discussed below. However, there are drivers behind demand for cryptocurrency in emerging markets distinct from the primarily speculative demand in high income countries.

POTENTIAL DOMESTIC CURRENCY PROBLEMS

Inflation

Many cryptocurrency fans claim that one of the chief advantages of bitcoin over fiat currencies is that it provides a hedge against inflation: the erosion of purchasing power by price increases. Unlike fiat currencies, bitcoin has a fixed supply. More bitcoins are being produced at a steady and declining rate. There are currently around 19m bitcoins in existence and there will never be more than 21m.

Bitcoin proponents believe that this fixed supply will protect bitcoin against inflation. While over its 12-year existence, bitcoin's value and purchasing power has grown on average, that does not mean

it will necessarily continue to do so or that it will remain stable. While money supply growth is a major contributor to inflation, there is little evidence to suggest that a fixed supply of bitcoins would have a constant stable purchasing power, particularly in a world where taxes and salaries continue to be denominated in fiat currency.

Gold is often regarded as a hedge against inflation. On a sufficiently long timeline, demand has kept its price ahead of inflation, meaning gold holdings have maintained their purchasing power. Bitcoin is often likened to a digital form of gold, with fans claiming that it provides a similar hedge against inflation but can be held and transacted digitally, without intermediaries.

Bitcoin, though it has proven relatively stable over the past few months, fell in value from around \$47,100 at the end of March 2022 to around \$17,300 in mid-November. This kind of precipitous decline undermines its value as an inflation hedge. It will be a long time before bitcoin has earned the same trust as an inflation hedge that gold has achieved.

However, some fiat currencies around the world have long track records of painful inflationary dynamics. According to an article in [EL Pais](#), Argentina's average annual inflation over the last 100 years has been 105%.

This kind of inflation is one of the principal reasons citizens lose faith in their domestic currencies. For citizens of countries with comparatively low and stable inflation, it can be difficult to imagine living in a situation where the purchasing power might be drastically lower just a month after a salary has been paid.

Citizens in such countries typically turn to the dollar, where the value of their savings is relatively stable, rather than being eroded by domestic inflation. Many merchants will accept payments in dollars for the same reason.

A similar dynamic has been at play in Turkey, where the latest annual inflation figure was 85.5%. In such conditions, the dollar becomes a more popular option and hugely in demand.

Bitcoin is, for many, even more easily accessible than the dollar since it does not require either a bank account or access to physical cash. Accordingly, adoption is high since it can provide a means for citizens to shelter their savings from inflation. Some will choose to exchange as much of their salary as possible for dollars or cryptocurrency, only buying enough of their local currency to cover expenses.

However, when collapses like this year's monumental decline do occur, many of the victims are likely to be in lower income economies in economically fragile situations.

Stablecoins are a possible alternative to the instability of bitcoin and other cryptocurrencies. The most common stablecoins have values pegged to the dollar. Users are still exposed to the foreign exchange risk of a decline in the value of the dollar,



but this is a far less troublesome risk than exposure to bitcoin’s performance.

However, stablecoins bring their own risks, discussed below.

Capital controls

Domestic inflation creates an incentive for citizens to buy foreign currency, particularly dollars. The frequent selling of domestic currency for foreign exerts a downward pressure on the value of the domestic currency, exacerbating inflation. To stem this, many governments choose to impose capital controls.

This can make purchasing goods and services abroad – holidays, foreign tuition or international e-commerce for example – challenging and expensive. There is therefore a demand for a means of moving money across borders outside of government scrutiny.

Some governments in this situation attempt to control the value of their currency with a peg: an official exchange rate. As of November 2022, the Central Bank of Argentina will purchase dollars for 157 pesos and sell them for 165. On the unofficial market, buying a dollar costs 285 pesos and they sell for 289.

Those holding dollars will therefore benefit hugely from using illegal exchange rate providers, rather than the official sector. These conditions are far more fertile ground for the adoption of cryptocurrencies than the conditions in much of the global north.

Traditionally, unofficial exchange rate providers rely on smuggling physical cash over borders but these methods are always vulnerable to loss through accident, robbery or seizure by law enforcement. With peer-to-peer digital transactions enabled by cryptocurrency, these risks can be mitigated.

While such techniques for circumventing capital controls are illegal and the resultant capital flight can prove damaging to vulnerable emerging market economies, it is undeniable that using cryptocurrency and stablecoin for this is part of the appeal they hold in these economies.

Access

Many emerging markets have large rural populations with limited access to banking services. For those in remote, rural areas, they may simply have to travel a long way to reach physical banking infrastructure, but even for those with access to remote banking services or local infrastructure, banking services can still be difficult to access.

Some accounts cost money to open or maintain, which many in emerging economies can ill afford. Even the cheapest accounts typically have overdraft fees. Simply avoiding banking services eliminates the risk of being hit with these fines. Particularly for those who have never used the banking system, these risks can seem uncertain and difficult to manage.

Even for those who might be willing and able to



STABLECOINS ARE CRYPTOCURRENCIES THAT, RATHER THAN HAVING A VALUE DETERMINED BY THE MARKETPLACE, SEEK TO MAINTAIN PARITY WITH ANOTHER ASSET’S VALUE, TYPICALLY THE DOLLAR OR ANOTHER FIAT CURRENCY

access banking services, a frequent limiting factor is that they are unable to produce the documentation necessary to verify their identity to the satisfaction of the banks.

One of the consequences of reliance on cash is that it is difficult or impossible to build up an economic history that might be used by lenders to assess their creditworthiness. Without access to capital, their economic opportunities are limited.

Access to the internet and, in particular, mobile phones has given many in emerging markets the opportunity to use banking services in ways they would not previously have been able to.

But these still mostly require some identity verification. Cryptocurrency offers many an opportunity to engage in investment, borrowing and international commerce with lower barriers to entry.

With internet access outpacing banking access, many turn to cryptocurrencies and stablecoins as a means of accessing digital payment systems and value storage, as well as credit via decentralised finance.

However, the lower standards of investor protections and the volatility that periodically grips the cryptocurrency market can result in severe financial losses in economically fragile communities.

Lack of trust in institutions

A factor that often accompanies high inflation and an unstable currency is low trust in financial or public sector institutions. Argentina provides a valuable case study. During the 2001 recession, many citizens and companies were exchanging pesos for dollars and withdrawing them from banks, typically with the intention of transferring them to offshore accounts.

To halt the flow of money out of the country, the government froze all bank accounts in early 2002, allowing only small weekly withdrawals from peso-denominated accounts. Eventually, dollar holdings were redenominated into pesos at a rate well below the market rate of the time, with many people losing 65% of the value of their dollar holdings.

With risks of events like this, it is no wonder that citizens of countries with unstable economies have concerns about leaving their assets in the control of financial institutions and the reach of governments that most in more stable economies do not share.

Cheapening remittances

For many economies in emerging markets, remittances form a substantial part of their gross

domestic product. Money transmitters often charge substantial fees for remittance corridors. The United Nations aims to bring the average cost of a remittance down from 6.4% to 3%, with no corridors charging more than 5%. This would result in savings of more than \$18bn – a substantial contribution to the GDP of remittance recipient countries.

Making remittances more efficient and reducing the share of value captured by money transmitters is a key policy aim for the Bank for International Settlements’ committee on payments market infrastructures.

Though there are a variety of possible schemes for the improvement of remittances, some are already turning to cryptocurrency. The peer-to-peer nature means there are fewer intermediaries and the process can be completed more efficiently.

Vietnamese remittances, around \$18bn in 2021 (just under 5% of GDP), cost an average of 7% in 2020, according to statistics from the World Bank.

Much of the population, particularly in rural areas, may struggle to access the services of conventional fiat money transmitters.

It is perhaps unsurprising therefore that cryptocurrency use in Vietnam is among the highest in the world, much of which is driven by remittance traffic. Second only to Nigeria, some 21% of Vietnamese respondents to a 2020 Statista survey

said that they used or owned cryptocurrency.

Peer-to-peer networks like bitcoin might cut out the middleman, but cryptocurrency transactions are not free. At present, bitcoin transaction fees are less than a dollar and are likely to provide savings compared with traditional remittance channels. However, these fees can fluctuate widely based on demand, peaking at over \$60 in April of 2021.

Nevertheless, despite the variability, these networks can, in theory, provide a valuable channel, particularly with the addition of other layers like the Lightning network (a layer 2 addition to the bitcoin blockchain that eases the load of transactions via netting).

However, not everyone is keen to adopt bitcoin for remittances. In September 2021, El Salvador’s president, Nayib Bukele, spearheaded a drive to make bitcoin legal tender in the country. One of Bukele’s stated aims was to make it easier for citizens to receive remittances from abroad.

The move was, however, widely protested by citizens and, according to a survey conducted by the Salvadoran chamber of commerce, only 14% of merchants in El Salvador had processed a bitcoin transaction as of March 2022.

Around 24% of El Salvador’s GDP came in the form of remittances in 2020. World Bank data suggest El Salvador already operates a fairly cheap



105% Argentina’s average annual inflation over the last 100 years’



remittance corridor, losing only 2.9% on average per transaction – below the UN’s target of 3%. Despite this, some corridors are markedly more expensive and many require senders and recipients to present and collect cash in person. Some 16% of remittance corridors take more than two days. And 24% make funds available the following day.

According to El Salvador’s central bank, a mere 1.7% of the remittances sent from the US to El Salvador in the first half of 2022 were denominated in cryptocurrency (almost all of it in bitcoin).

While it is possible that, over time, acceptance of bitcoin for remittances will grow in El Salvador, download figures for the state sponsored Chivo Wallet application have been low since the initial surge. Many users downloaded the app and used the \$30 worth of bitcoin they were given free by the government but have made little further use of it.

There is another issue with using cryptocurrency for remittances. Since few people are paid in bitcoin or, even in El Salvador, can use it for many of their day-to-day purchases, senders will have to buy it in their local currency, send it to the recipient, who will have to sell it for their local currency or, more likely, sell it for dollars and then buy their local currency with dollars.

This adds foreign exchange risk to the transaction that, particularly with bitcoin, can seriously impact the amount sent and received.

This risk might be mitigated in cases where the domestic currency is suffering from high inflation or an otherwise unstable value.

Using stablecoins might mitigate this risk, although there may be liquidity issues in exchanging the stablecoin for local fiat currency.

STABLECOINS

Many of the risks and frictions relating to the use of cryptocurrencies for payments in emerging markets stem from the fact that for most day-to-day users, spending them creates foreign exchange risk because, even where cryptocurrencies are accepted for payments, prices are almost always denominated in fiat currency.

Stablecoins obviate that risk since they are typically pegged to the dollar or another major fiat currency.

Stablecoins, though designed to have a fixed value relative to a given fiat currency or commodity, are nevertheless not risk free.

It is important for stablecoin users to understand that the risks they face when holding stablecoins are not equivalent to the risks posed by holding dollars, either in cash or in a bank account.

The risks of cash are simple and well-known. The purchasing power may fall thanks to inflation or moves in foreign exchange rates, and theft or damage are always risks. It is obviously limited in applicability since it can only be used in person.

Bank accounts prevent loss from theft and



1.4bn
Number of people who are unbanked,
according to the World Bank

damage. Interest offers some compensation to inflationary value erosion. Bank deposits, however, represent a claim on the bank’s credit and create risk. To some degree, this can be mitigated with state deposit protection schemes, but particularly in emerging markets, these are not infallible.

While bank accounts facilitate digital transactions, many citizens of emerging markets are unbanked and find it difficult to obtain traditional banking services, limiting their value.

Many countries in emerging markets have, to a greater or lesser extent, adopted the dollar as the currency for everyday use. Smaller currencies with thin foreign exchange liquidity struggle with acceptability offshore. This means there is a need for dollars to pay for imported goods and the dollar therefore underpins substantial amounts of economic activity in many emerging markets.

Dollar-denominated stablecoins offer a potentially valuable means for citizens of emerging

market countries to get access to digital dollars, which might otherwise prove challenging because they cannot access traditional banking services.

This can offer them a means of engaging in international e-commerce, buying and selling goods and services internationally. Freelancers around the world can compete for jobs in a global marketplace. The low transaction fees for on-chain transactions typically represent a saving versus most digital payments providers and, combined with relatively quick settlement times (usually minutes rather than hours or days) and smart contract automated payment-versus-payment foreign exchange conversions.

This also makes it a potentially valuable channel for the distribution of aid payments. For those without access to traditional banking services, but with internet access and smartphones, it offers a means of making aid payments in a more secure, traceable and useful manner than physical cash, which can be lost, damaged or stolen more easily than digital equivalents.

The US government has made use of stablecoins to send foreign aid to Venezuela. Since they are peer-to-peer, they offer a means of circumventing transaction systems and banks that might be under the control of a hostile or dangerous government.

Since stablecoins exist on blockchains, which can process transactions 24 hours a day, stablecoins can also facilitate foreign exchange transactions by enabling payment-versus-payment transactions. This eliminates settlement risk by ensuring that one currency is transferred only if the recipient currency is also sent. This reduction of risk means less capital is required and brings down the cost of currency exchange.

RISKS

The risk profile for stablecoins is different to that of cash or bank accounts. Indeed, it is difficult to generalise since the risk profile will be different for each protocol.

Much of the risk stems from the assets that collateralise stablecoins. In early 2022, the world was treated to an example of the damage a collapsing stablecoin can do. Terra was an algorithmic stablecoin that attempted to maintain parity with the dollar through a peg to Luna, a cryptocurrency promising yield based on staking (a form of high-yield lending operation in the cryptocurrency world).

When trust in Luna’s yield failed, a run on Terra began and the inability to meet investors’ demands to cash out shook confidence in the cryptocurrency ecosystem, triggering a broad devaluation, resulting in several high profile margin calls and insolvencies.

To be sufficiently reliable for widespread use for the purposes described above, stablecoins must be backed by cash and cash-like assets. There must be a sizable proportion held in cash such that they are able to meet large-scale redemptions immediately.

Some stablecoins have large, highly liquid, frequently audited reserves capable of meeting redemptions. Others have less high-quality collateralisation and lower standards of transparency. Either through limited choice or limited information, emerging market users may not always be able to rely on the provision of high quality stablecoins.

The risks grow as the size of the stablecoin grows since even highly liquid assets take time to sell in large volumes and can cause market movements. Holdings large enough to collateralise a widely-used, globally-available stablecoin will have a wider effect on the economy. A rapid sale of large amounts of assets – short-dated government securities for example – might drive down the price and force margin calls or otherwise disrupt funding operations.

As well as issues around collateralisation, there are potential operational risks. Stablecoins operate on blockchains. While the core of blockchain cryptography is typically robust, there are several different layers of services – such as custodians/ wallets, interoperability bridges, on/off-ramps and smart-contract payments –which bring their own vulnerabilities and have been exploited by hackers.

DOLLARISATION

The very ease of access and use that stablecoins provide creates further risks for emerging market countries. While the risk of citizens moving their savings into dollars has been present for far longer than stablecoins have been around, the availability of physical cash, risk of storage and accessibility of merchants prepared to accept dollars have all proven checks on the viability of stockpiling the currency.

However, with the advent of a digital, globally accessible dollar-like cash instrument, many of these difficulties disappear.

The International Monetary Fund warned in June this year that stablecoins could displace national currencies, particularly currencies seen as less convenient to use or volatile in value.

The publication suggests that even volatile cryptocurrencies like bitcoin might ‘in addition to enabling capital flight, be preferred to the local currency during economic turmoil’. However, it adds that the dollar is likely to be the preferred choice, particularly if an easily available digital version exists.

This substitution effect might exacerbate fragilities in emerging market banking systems as they lose deposits to stablecoins, particularly if these are remunerated.



THE INTERNATIONAL MONETARY FUND WARNED IN JUNE THIS YEAR THAT STABLECOINS COULD DISPLACE NATIONAL CURRENCIES, PARTICULARLY CURRENCIES SEEN AS LESS CONVENIENT TO USE OR VOLATILE IN VALUE



BASKET-BACKED STABLECOINS

Thus far, the discussion has focused on fiat-pegged stablecoins, since these are the most common. However, there are a variety of proposals for stablecoins backed by a basket of assets, with a value determined by those assets. Libra, a project of Meta, sought to establish a global stablecoin backed by a basket of currencies.

Such a project would have had an enormous impact on cross-border payments. There would have been a clear benefit for using it, since a sender could buy this basket-backed coin with their local currency and send it to a recipient in another country who could redeem it in their own currency.

However, the structure underpinning a basket-backed currency is complex. Either the value will fluctuate based on the changing value of the components, or the components must be adjusted dynamically.

If redemptions are unbalanced – if a great many of the stablecoin are redeemed in euros, but not in dollars – then there will have to be purchases of euro assets to keep the composition stable. This kind of system can have destabilising effects on the broader economy, particularly for smaller and less liquid markets.

The risk of currency substitution is clear. Libra’s main proposal for the avoidance of substitution was to assist in the development of local currency stablecoins for concerned central banks.

CONCLUSION

Many emerging market economies share certain features that make them particularly receptive to cryptocurrencies and stablecoins. Unstable currencies with high inflation encourage citizens to seek refuge in freely available digital alternatives like bitcoin. Strict capital controls encourage citizens to seek out less easily policed alternatives. Large unbanked populations, particularly those with cultural mistrust of financial or government institutions, are inclined to seek out alternative methods of payments outside of the traditional sector.

There are certainly benefits. Competition in the remittances space can only encourage better outcomes in terms of speed and cost for users and merchants. Reducing dependency on cash and promoting access to global markets can promote economic development.

Insofar as cryptocurrencies and stablecoins can provide cheap and efficient payments systems, as well as opportunities to shield assets from inflation, they offer more value for emerging markets than they do for developed markets.

However, many emerging markets users are in economically fragile situations and are not equipped to deal with the losses that the volatility of cryptocurrencies make likely. It is important for central banks, commercial banks and payments services providers to work together to ensure they can establish alternative systems that can offer the same benefits with fewer risks. •



BITCOIN IS, FOR MANY, EVEN MORE EASILY ACCESSIBLE THAN THE DOLLAR SINCE IT DOES NOT REQUIRE EITHER A BANK ACCOUNT OR ACCESS TO PHYSICAL CASH



CRYPTOCURRENCIES CAN IMPROVE SPEED, COST AND EASE OF ACCESS OF PAYMENTS

Proper regulatory guardrails are needed for people to enjoy the benefits of a payments revolution, writes Rana Kortam, director, global public policy at Binance.

ALTHOUGH CRYPTOCURRENCY is still in nascent stages, 91% of crypto holders believe it’ll become as common as card payments. Despite making major strides, existing electronic payment systems suffer in regards to cost, efficiency and access.

Legacy systems still fall short of providing access to financial services to 1.7bn adults or efficient cross-border retail payments. Blockchain technology brings the benefits of faster settlement, access to new customers and lower barriers to entry.

Blockchain networks handle international transactions in minutes as opposed to the traditional days or hours. They can settle transactions for under \$0.01, considerably cheaper than traditional payment card networks. The rise of stablecoins has highlighted shortcomings in traditional cross-border payments. Studies show that distributed ledger technology improves the efficiency of cross-border payments and blockchain technology could help banks save \$27bn by 2030 on international transactions.

Cross-border payments matter. They account for 15%-20% of ecommerce value. Small- and medium-sized enterprises, making up 90% of businesses and 50% of jobs globally, need easier access to international payments. Remittances are a \$589bn market and a major source of capital for developing countries. They are also a lifeline for 281m migrants. Cryptocurrency is making a dent in this market, dominated by international operators, with Africa seeing \$562m worth of cryptocurrency inflows. Although various forms of cryptocurrencies are used for payments, stablecoins and central bank digital currencies have won favour for their stability. Stablecoins are primarily used for trading, lending or borrowing digital assets, but could become used widely as a means of payment if well designed, interoperable and buttressed by regulatory guardrails.

Payments giants are taking notice: Visa’s network allows people to settle transactions in USD Coin, a dollar stablecoin, and Moneygram partnered with Stellar to offer stablecoin for fiat remittances in India. International remittances cost an average of 6.4% for \$200. A transaction could involve up to four intermediaries. Fluctuating exchange rates exacerbate inefficiencies. And the burden is disproportionately borne by

underprivileged segments, with fees for cross-border retail payments reaching 10%.

The Financial Stability Board wants to get remittance fees to the UN sustainable development goal of 3% and 1% for retail fees by 2027. International stablecoin transactions cost less than 0.1%. Sending crypto to another user on the Binance Smart Chain costs between \$0.01-\$0.10.

Cross-border retail payments can take days to clear due to the number of intermediaries. Crypto transactions clear within seconds; a great way to meet the FSB’s target of clearing 75% of transactions within one hour.

All financial institutions must have a cross-border payments option, for retail, wholesale and remittances. Cryptocurrencies can address access challenges such as multilateral settlement eligibility and the lack of correspondent bank relationships.

Users must be provided with information about how much a transaction will cost, how long it will take, its status as well as terms of service – all automatically visible in a blockchain’s public ledger.

These improvements are consistent with the G20 Roadmap for enhancing cross-border payments and its four challenges and targets, covering cost, speed, access and transparency, to be met by 2027.

CBDCs offer ‘the unique advantages of central bank money: settlement finality, liquidity and integrity,’ with emerging markets leading on adoption. Interoperable CBDCs are key for cross-border payments. Interlinking CBDC systems through a hub and spoke or single system might bring more improvement to the market than compatibility or single access points. International co-operation in early stages is necessary to address underserved cross-border corridors. Crypto for payments regulation should follow a risk-based approach specific to the tool’s structural features, usage and risks.

With risk management and regulatory guardrails, stablecoins and CBDCs could become the go-to payments solution for cutting edge technology, such as in the metaverse. Stablecoins have been critical to decentralised finance’s. The future of payments, backed by new digital currencies, is looking bright. •



PROMISE AND PERIL OF CENTRAL BANK DIGITAL CURRENCIES

Both developed and emerging markets are working toward implementation of CBDCs, but much of the action is concentrated in emerging markets, where the value propositions are clearer. By Julian Jacobs

CENTRAL bank digital currencies may overhaul how the global financial and monetary system works. By supplanting traditional fiat cash with a digital equivalent, CBDCs promise greater ease of use, access, convenience and oversight. These elements are, of course, beneficial for developed countries. Yet, it is in emerging markets that the benefits of CBDCs are clearest. As of 2022, 1.7bn people remain outside the traditional financial system, the vast majority of which are in emerging markets. The results are economic inefficiency and less impactful stimulus policy. And limited access to affordable financial products can also lead to debt traps and

cyclical poverty dynamics. These elements were exacerbated by the Covid-19 pandemic. A well-designed and implemented CBDC could improve access to the financial system, while also helping stamp out criminal activity and making cross-border payments more efficient. Yet along with the benefits of central bank digital currencies, there is also the potential for considerable risk, most notably in the form of financial instability, obstacles to CBDC adoption and trade-offs between security and freedom from governmental oversight. A CBDC, then, is likely to be immediately useful in developing countries

KEY FINDINGS

- 1. Central bank digital currencies hold the potential to significantly improve payments efficiency, particularly across borders, strengthen financial inclusion and ward against illicit economic activity
- 2. Despite these benefits, poorly constructed CBDCs threaten to erode trust in a country's currency and monetary systems, while also assisting excessive government oversight and the growth of financial fraud
- 3. Although developed countries continue to research and conduct small pilots of CBDCs, early evidence from deployment in several emerging markets is promising. Moreover, cross-currency CBDC exchanges, which are underdevelopment, may greatly improve foreign transaction efficiency.

with weaker existing financial infrastructure and a greater share of the economy outside of the banking system. The benefits of a CBDC for developed countries will require a different analysis of its relative risks and rewards.

CENTRAL BANK DIGITAL CURRENCIES MAY IMPROVE FINANCIAL INCLUSION, SECURITY AND EFFICIENCY

A general purpose CBDC would transform any economy. Instead of currency being largely deployed in physical cash and commercial bank liabilities, a government sponsored digital currency would assemble a digital ledger tracking and executing transactions between parties. Although some central banks are considering deploying a CBDC, not to replace cash but instead to complement it, the movement towards a wholly digital economic system would nonetheless be significant. The Bank for International Settlements predicted that 20% of the global population will use a CBDC over the next three years. According to the Atlantic Council's CBDC tracker, some 72 countries are exploring or developing CBDCs with a further 26 either launched or running pilots.

The potential benefits that emerge from this are distinctive. Estimates about illicit activity unsurprisingly range. About 2%-5% of global GDP (\$800bn-\$2tn) is hidden to avoid taxation. Meanwhile, about \$500bn is tied up in the illegal narcotics industry. A central bank digital currency would not eliminate these issues, but proponents

argue it could greatly reduce the presence of these elements in the economy for one reason: using a distributed ledger makes it easier to track, monitor and account for the movement of a digital currency. Illicit activity would be easier to spot and governments would have more transparent access to all market behaviour denominated in their currency.

These elements may be true for both developing and developed countries. However, they are particularly helpful in emerging markets, where there is often more limited infrastructure to track and ward against illicit finance. This is only true insofar as illicit activity is conducted in digital currency, since cash remains difficult to trace and monitor. Although cash is still an extremely important channel for illicit economic activity, the presence of a CBDC might reduce legitimate reliance on cash and improve enforcement agencies' ability to pursue criminal activity.

These mechanisms of oversight and access are also what can make a CBDC an excellent tool to help reduce barriers to financial inclusion. By bringing individuals who might otherwise not meet the baseline requirements of a traditional bank into the system, governments can use the technology to extend financial access to underserved groups. Such efforts would be helped by using e-wallets and more simplified digital banking tools, which can be used on any smartphone. Nigeria's e-naira, for example, provides financial access to individuals without identification or traditional addresses.

A promising sign for CBDCs is that digital technology and mobile phone use is outpacing the growth of transaction bank accounts. The implementation of a CBDC can exploit that divergence by helping phone-owning individuals access bank and transfer services without having to hold cash or visit a physical location. Access to mobile banking will, of course, need to improve. However, greater access to digital technology would make the impact of CBDCs on financial inclusion greater, given transaction account growth is lagging. It is also possible to offer simplified digital or mobile banking tools with limited ID verification requirements without launching a CBDC. Indeed, a CBDC may not be the simplest means of achieving this kind of financial inclusion.

“FOR A CBDC TO BOOST ECONOMIC INCLUSION, GOVERNMENTS MUST PUT DIGITAL WALLET AND BANKING TOOLS IN THE HANDS OF INDIVIDUALS WHO ARE OFTEN EXCLUDED FROM THE FINANCIAL SECTOR.”





20%
The Bank for International Settlements predicted that one-fifth of the global population will use a CBDC over the next three years.

Yet if a CBDC does succeed at opening banking to individuals traditionally outside of the financial system, the compounding effects of this could be considerable. Since individuals who do not engage in online banking may have little to no financial history, their access to credit, investments and finance is limited. The concentration of financial activity, access to credit and equity exposure have grown more pronounced both globally and within domestic markets. If a CBDC offers an opportunity for new demographics to develop a credit history and savings structure, global financial access inequity could be reduced.

Benefits also include speed and cost efficiency, both of which can support individuals typically kept outside the financial system. The cost to serve customers restricts access for some, so bringing this down can help with financial inclusion.

According to analysis by the Tony Blair Institute for Global Change, CBDCs could lower transaction costs by up to 50% while simultaneously improving the speed and directedness of financial flows. In OMFIF's survey of central banks, all respondents said a key benefit of a CBDC might well be its capacity to make cross-border payments more efficient. This has two positive implications. The first is that it might support direct transfers from governments or non-governmental organisations

to people in need of support. Almost 35% of adults in low-income countries opened their first financial account to receive government payments.

The second benefit is the increased ease of transfer for migrant remittance payments. Instead of incurring the often significant costs and barriers that can emerge through cross-border payments, migrants would be able to transfer cash with greater ease, speed and at lower costs. In 2019, migrants sent about \$554bn home and migrant workers send between \$200-\$300 home every one or two months. About 75% of these remittances are used to provide food and coverage for medical, education and housing expenses. Yet these payments remain expensive and are often logistically challenging. World Bank data indicates that the average cost of a remittance is over 6% of the money sent home, with some corridors much more expensive.

Given these benefits, CBDCs may be most productive and useful for those countries with more limited existing financial infrastructure and a greater share of individuals outside of the financial system. This is why CBDCs appear to, at least for now, make the most sense and provide the most benefits in developing countries. Developed countries, in contrast, might find it ultimately cheaper and more productive to extend the coverage of existing

financial infrastructure. In emerging markets with less robust financial infrastructure, a weaker capacity to enforce regulations and a reliance on cash, which aids both leakages and opportunities for crime, CBDCs hold great potential.

CBDCS MAY POSE RISKS TO STABILITY, ECONOMIC FREEDOM AND SECURITY

It is not inevitable that central bank digital currencies will spur greater economic inclusion and efficiency. Indeed, there are considerable challenges that complicate the overall picture. The key issues around CBDCs take on a few forms. First, to promote inclusion, governments may need to take significant actions to reduce barriers to entry, presenting new security challenges. Then there are legal, political and ethical challenges of greater oversight. Finally, there is a threat of more significant volatility due to the speed of transferring currencies and the possibility of currency exchange rushes.

For a CBDC to boost economic inclusion, governments must put digital wallets and banking tools in the hands of individuals who are often excluded from the financial sector. The challenges in doing this, particularly in emerging markets, is individuals that are most likely to be excluded from the financial sector also tend to have more limited exposure to digital technology, internet access and formal identification. As a consequence, the CBDC financial inclusion mission presents a conundrum: how can governments provide access to a central bank digital currency if the vehicle to do so relies on digital technology and requires some form of identity verification?

CBDC optimists have an answer. Through the existing mobile phone infrastructure – smart and otherwise – central banks can extend mobile banking access to individuals who have only the most basic access to digital technology. Offering reliable broadband and mobile data can be costly and physically challenging in remote places, but it is likely to be more cost-effective than establishing bank branches. So, while providing access to the connectivity necessary to process payments is both a logistical and financial challenge, it may be the least difficult option to encourage an economic system that is more powerful than a closed network of cash only transactions.

Beyond this, many individuals outside of the traditional financial system are missing identification documents necessary to fulfil basic know-your-customer requirements. This would make it difficult for CBDCs to promote universal inclusion without either a concerted effort to improve dedicated identification resources or a lowering of KYC standards. The former may be challenging for a myriad of social and practical reasons. And the latter comes with significant risks. Moreover, there may be cultural barriers. Regions



OVER THE COMING YEARS, NEW PILOTS IN THAILAND, MALAYSIA, GHANA, SINGAPORE AND KAZAKHSTAN MAY RESULT IN THE OFFICIAL LAUNCH OF NEW CBDCs

that have traditionally not engaged in mainstream banking often have lower levels of financial and digital literacy. This corresponds with a preference for cash as well as possible scepticism of financial institutions – many central banks cite such lack of trust as a blockage to financial inclusion.

Given these dynamics, a crucial question for central banks and governments is how to establish guidelines that will enable easy access to CBDCs while simultaneously ensuring its security. If a CBDC – or any currency – is particularly vulnerable to fraud, theft or illicit activity, businesses and consumers will avoid it in favour of other assets. This may reduce the utility of the CBDC, as individuals and businesses opt for safer forms of money.

Indeed, history is filled with examples of how the ease of counterfeiting a currency led to a cratering of its value (for example, the continental currency notes of 1775). The risk, then, is that disruptions and fraud erode trust in a CBDC, which in turn hinders central banks' ability to maintain monetary stability and macroeconomic health. Modern cash contains numerous tools to ward against counterfeiting – from holograms to watermarks. Central banks will face a corresponding challenge to ensure that their digital currencies cannot be counterfeited. They appear aware of these risks, however. In our survey, issues around CBDC security were the most widely cited challenge among respondents. Even though cryptocurrencies have a poor reputation for cybersecurity, these problems typically are not inherent to the underlying technology itself. Security issues tend to emerge from layers built on top of the base blockchain technology, such as smart contract operated payments and digital wallets.

Given the need to maintain security, governments might be compelled to adopt greater oversight over transactions. This brings with it economic freedom and government overreach concerns. Given the decentralised finance visions from which cryptocurrency emerged, it is ironic that CBDC diffusion could increase government oversight. With a CBDC, there is effectively no limit to how much control a government could exert, since it could completely see how money flows through the economy. For governments with poor human rights records, this might serve as an additional tool to stamp out dissent and



to limit financial resources for already harassed demographics and undesirable socio-political entities. For societies which value economic freedom and less oversight, CBDCs might be politically toxic.

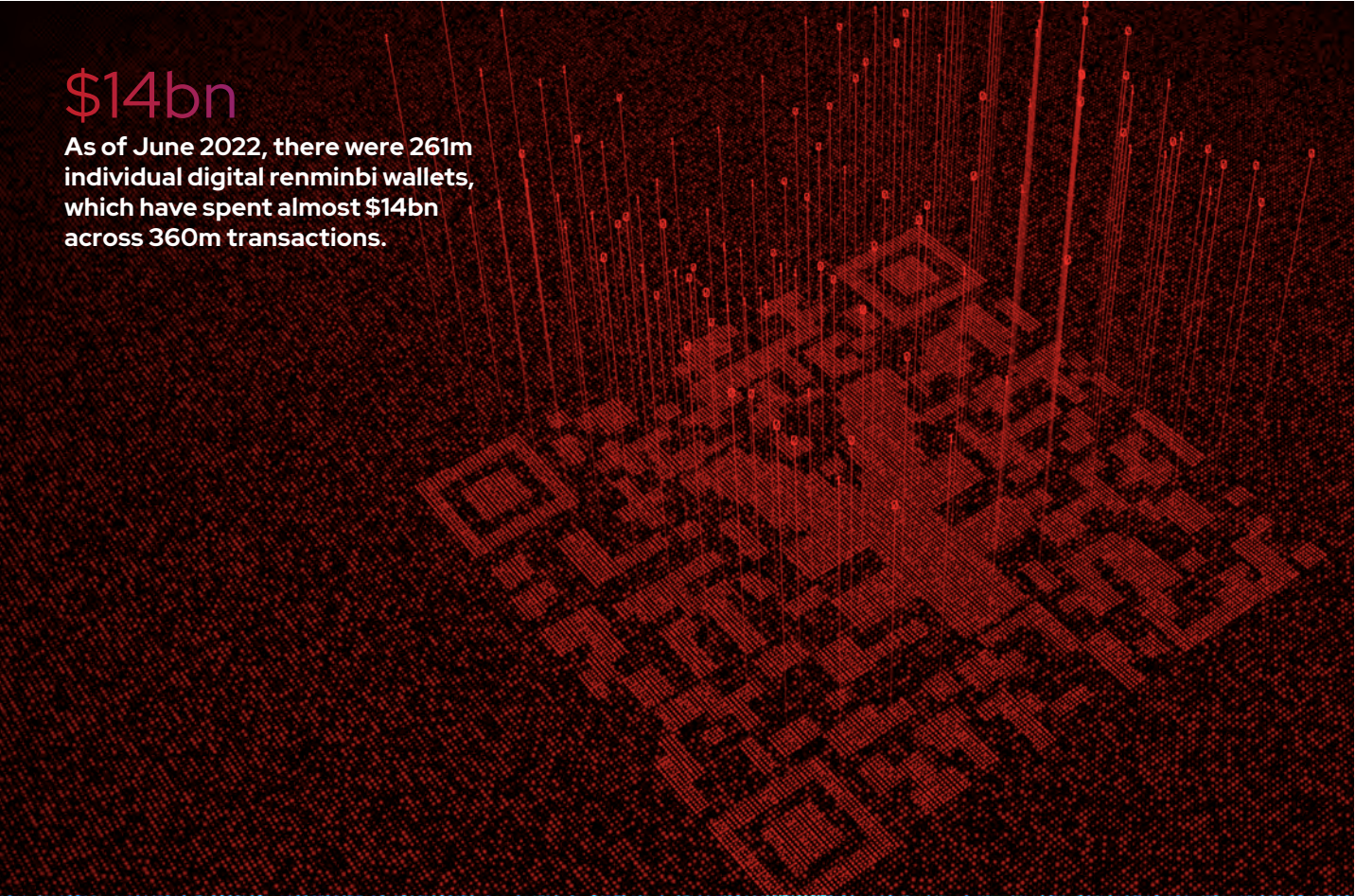
CBDC proponents might argue, however, that these issues of oversight would not necessarily be exclusive to a digital currency. Indeed, governments are already capable of exerting substantial control over traditional finance. They can still instruct banks and money service providers to restrict payments to accounts. Canada exercised this power when it used emergency government powers to freeze the accounts of truckers during the protests of early 2022 in Ottawa. The greater capacity for government to intrude on people’s finances might be a feature of an increasingly digital financial system, rather than a quality unique to CBDCs. And yet there is little question that CBDCs offer governments a greater ability to track the flow of money. They represent an increase of the overwatch capacity.

Perhaps the greatest challenge CBDCs pose is far more systemic and innate to the nature of a fully digital currency. In a best-case scenario, where CBDCs do proliferate and offer improved efficiencies and speed in transferring currencies, these improvements could also expose economies to greater systematic financial risk brought on by volatility and sudden foreign exchange fluctuations, particularly if the CBDC is available for offshore use. Just as the ease of investing in financial entities kindled the potential for violent and rapid crowd-driven instabilities – for instance, Game Stop equity price volatility – CBDCs risk causing extremely disruptive currency fluctuations, particularly for emerging markets where thinner liquidity makes prices more vulnerable to movements. Such swings could result in rapid fluctuations in debt burdens, net exports and GDP growth.

Central banks must manage these trade-offs between security and access. A CBDC that does not provide sufficient security would risk imploding a country’s economic and monetary system. A CBDC that offers no benefits to how easily money is transferred, however, would be an expensive project with limited benefits.

DEVELOPING COUNTRIES ARE RESEARCHING AND DEVELOPING DIGITAL CURRENCIES

Most CBDC pilots are taking place in emerging markets. By contrast, advanced economies are developing and, in some cases, still researching their own CBDC models. The US, for instance, issued executive orders looking into the topic and in September 2022 released seven reports that examined key issues around security, environmental damage, illicit activity and risks associated with CBDCs. Meanwhile, in the UK, the House of Lords



in early 2022 declared there would be little benefit from a CBDC for Britain. Despite this, the Bank of England is continuing to explore the topic through a collaboration with the Massachusetts Institute of Technology’s Digital Currency Initiative.

The Bank of Canada, meanwhile, is also partnering with MIT’s Digital Currency Initiative to help it assess the merits of testing and launching a CBDC. Canada’s Project Jasper is a CBDC initiative that includes testing cross-border payments with the UK and Singapore. The European Union is also developing a digital euro with the support of individual euro area countries. In May 2022, Christine Lagarde, president of the European Central Bank, gave her support to the digital euro and the EU announced partnerships with Amazon, the European Payment Initiative, Nexi, CaixaBank and Worldline to support its development. At the individual country level, France has been conducting successful tests of CBDCs, while Germany’s Bundesbank tested the blockchain-enabled use of distributed ledgers for digital securities in 2021, which could limit the need for CBDCs. In Spain, Iberpay in 2021 conducted experiments with 16 Spanish banks to test the possible functions of a digital euro. All this implies that, while CBDCs are generally not being deployed in pilots by developed

countries, their swift but cautious development indicates that some form of CBDC will emerge more widely in the coming years.

A major exception to the slow moving approaches of developed countries is Sweden, which has already started its CBDC pilot. In 2017, the Riksbank began studying the utility of a CBDC. And in 2020, it began work to build a Swedish CBDC with Accenture, culminating in the Riksbank’s development of the e-krona, which is currently being tested for both large commercial and small retail payments. The country’s ministry of finance is planning to use the results of this project to assess whether the e-krona should be launched, with a goal of moving away from the inefficiencies of cash and towards a more optimised system of digital transactions. In Eastern Europe, a similar pilot has emerged in Lithuania, through its development of LBCOIN.

China became the first major economy to pilot a CBDC when it launched the digital renminbi in 28 cities across 10 regions. As of June 2022, there were 261m individual wallets, which have spent almost \$14bn across 360m transactions. This included the People’s Bank of China’s pilot during the 2022 Winter Olympics in Beijing, during which 2m yuan was used daily, without foreigners having to create

a bank account. This is part of a broader effort to expand China’s efforts for improving cross-border transactions through its multiple central bank digital currency (m-CBDC) bridge.

EMERGING MARKETS CONTINUE TO PILOT AND IMPLEMENT THEIR OWN DIGITAL CURRENCIES

Despite growing interest in CBDCs among developed countries, the presence of more advanced digital currency projects is overwhelmingly concentrated in emerging markets. Indeed, all 11 CBDC projects that have been officially launched are in developing countries. This includes Jamaica, Nigeria, the Bahamas and several eastern Caribbean islands. The Bahamas’ sand dollar – launched in October 2020 – was the first, with the digital currency available now for all Bahamas citizens. Nigeria, meanwhile, launched the eNaira in 2021 as part of its phased integration into the economy. At the start of 2022, over 600,000 eNaira wallets had been created and 90% of transactions were between individuals and businesses. Finally, Jamaica’s work with the Ireland-based eCurrency Mint organisation supported the country’s efforts to launch the Jamaican digital exchange (JAM-DEX) in February 2022.

Each of these CBDC projects was created at least partly to support countries’ efforts to improve security and inclusion. The Bahamas’ swiftness in releasing the sand dollar came from an explicit goal of promoting financial inclusion while warding against enduring issues of illicit economic activity. The eNaira, meanwhile, is expected to help Nigeria reach its target of increasing financial inclusion by extending access to banking from 64% of the population to 95%. It is projected that a well-managed eNaira could add \$29bn to the country’s GDP over the next 10 years. JAM-DEX is projected to save Jamaica \$7m a year due to the waste and storage costs of relying on cash.

Over the coming years, new pilots in Thailand, Malaysia, Ghana, Singapore and Kazakhstan may result in the official launch of new CBDCs. Yet it is too early to say how successful current CBDC projects have been. This is partly because they are still incredibly young, but it is also in large part because they are subject to gradual roll outs. What is clear, however, is the confidence some central banks have in the notion that they might be able to use a CBDC to move forward the size, sophistication and inclusion of their financial systems.

COUNTRIES ARE WORKING TOGETHER TO CREATE MORE ROBUST CROSS-BORDER CBDC NETWORKS

A key promise of CBDCs involves making cross-border payments easier, encouraging greater global financial market cohesion and efficiency while simultaneously supporting the ease of migrant





ONE YEAR LATER: ENAIRA AS A FORCE FOR FINANCIAL INCLUSION AND DIGITAL PAYMENTS

Despite successes, some marginalised groups still face financial exclusion. The eNaira's continuing development is trying to solve that, writes Olugbenga Agboola, founder and chief executive officer of Flutterwave.

CENTRAL BANK DIGITAL CURRENCIES are one of the innovative ways central banks are diversifying. A key consideration for decision-makers is how such digital currencies could improve the efficiency of commerce and cross-border payments. CBDCs have launched already in 11 countries, while 15 more are testing and 26 are developing one. Nigeria is a leader here, with its already launched eNaira already impacting local and cross-border payments.

During the 2022 eNaira Hackathon, Central Bank of Nigeria Governor Godwin Emeiele pointed to the encouraging growth in eNaira adoption. Emefiele said, 'Since the launch of this great initiative, the eNaira has reached 840,000 downloads, with about 270,000 active wallets comprising over 252,000 consumer wallets and 17,000 merchant wallets. In addition, the volume and value of transactions on the platform have been remarkable, reaching above 200,000 and ₦4bn[\$9m], respectively.'

At the first anniversary of the eNaira's launch, Bitt, CBN's technology partner, talked about introducing unstructured supplementary service data, or quick codes, as a way to further develop the digital currency. This represents a massive opportunity to bridge the gap in national and sub-national financial inclusion levels.

By implementing quick codes, the eNaira could improve access to finance for individuals and businesses through digital channels, lower the cost of transactions and increase the flow of credit to consumers and businesses.

Financial inclusion is key for Nigeria's economic development strategy. Despite the obvious successes, women, youth, small- and medium-sized enterprises, and people living in rural areas are still disproportionately excluded from the financial system. The introduction of USSD shows that there is a roadmap towards deepening access for the unbanked.

Payments networks must be able to integrate the eNaira to fully onboard these new entrants into the national financial system. Then they can take part fully in ecommerce and other value-adding financial services without having a bank account. Beyond financial inclusion, the eNaira is also useful in

cross-border payments and transfers. Remittances represent one of the most compelling use cases for digital currencies. By eliminating intermediaries, the eNaira could be a reliable low-cost payments solution for consumers and businesses. The Bank for International Settlements outlined in a 2021 report the benefits of CBDCs in reducing costs and increasing the speed of remittances. It stated that CBDCs could reduce transaction times from 3-5 business days to seconds. It also reported a PricewaterhouseCoopers estimate showing a possible 50% reduction in the cost of cross-border payments.

Flutterwave has recently announced the integration of eNaira on Flutterwave for Business. Merchants and consumers can now transact using the safe and convenient eNaira on all Flutterwave channels.

One year on from its launch, the eNaira continues to grow. But there's still a long way to go, especially in local and cross-border payments.

Out of the 19 recommendations made in the 2021 BIS report, there are five that stand out as the most important. Institutions and firms must first develop a common cross-border payments vision and targets and then implement international guidance and principles. The community must also align regulatory, supervisory and oversight frameworks, as well as factoring in an international dimension into CBDC designs. Finally, it must pursue the interlinking of payments systems.

If the frameworks and building blocks are available, Africans will adopt CBDCs, just as they did smartphones. The continued adoption of the eNaira would provide more data for the design of better macroeconomic policies that will positively affect consumers and business owners.



BY IMPLEMENTING QUICK CODES, THE ENAIRA COULD IMPROVE ACCESS TO FINANCE FOR INDIVIDUALS AND BUSINESSES THROUGH DIGITAL CHANNELS.



\$29bn

How much a well-managed eNaira could add to Nigeria's GDP over the next 10 years.

remittances. Current cross-border payments in many corridors are very sluggish. While domestic payments offer an opportunity to transfer money directly between banks on a single platform, there is no such platform for settling international transactions. A multi-currency CBDC platform would enable more effective settlement without the need for intermediaries.

This is where multi-CBDC initiatives come in. Consider, for instance, Project Dunbar, which is a project led by the BIS Innovation Hub and includes the Reserve Bank of Australia, the Central Bank of Malaysia, the Monetary Authority of Singapore and the South African Reserve Bank. So far, the project has a developed platform that might support international settlements for digital currencies issued by different central banks and offers suggestions on how to expand such a model to G20 countries more broadly. Meanwhile, Project Jura — a collaboration between the French and Swiss central banks — is experimenting with the more specific case of direct transfers of euros and francs, using a single distributed ledger to use payment-versus-payment and delivery-versus-payment mechanisms to settle trades. Finally, there is LionRock: another multi-CBDC platform, which includes participation from the BIS Innovation Hub, Hong Kong Monetary Authority, Bank of Thailand, People's Bank of China and the Central Bank of the United Arab Emirates. The project began in the aftermath of Thailand's Project Inthanon in 2018, during which the country began testing a wholesale domestic CBDC.

Free flowing cross-border CBDC systems would help reduce the fragmentation of the global financial system. It would enable more efficient integration through, in the case of Project

Dunbar and in Project Aber, PvP foreign exchange settlements that reduce complexities and barriers to foreign money transfers. Cross-border CBDCs could therefore be an important piece of the future financial ecosystem that might make remittances cheaper and more accessible. They would create greater international financial cohesion and connection, which could bolster the free flow of capital and value, spurring economic growth and dynamism.

It is important to get a cross-border CBDC right, however. With greater ease of currency exchange and foreign movement of capital, there is the prospect for significant exchange rate volatility and herd-driven capital flight. Regulations are necessary to ensure stability in global exchange rates and capital movement. In the absence of such restrictions, a cross-border CBDC might serve to promote widespread currency substitution, exacerbating the reliance on desirable 'dominant' global currencies to the detriment of others. A consequent lack of confidence in a particular currency's value could then erode countries' monetary and economic systems while simultaneously spurring global instability.

Such disruption in the global financial and currency exchange system is not inevitable, however. Initiatives like Project Dunbar, Project Jura and LionRock represent major steps to better grasp the promises and risks of cross border CBDCs. With the right regulatory framework and exchange movement control, countries may be able to strike at an often-elusive balance: between the need for greater efficiency, ease of use and the free flow of capital on the one hand and the need for security and limits on violent, frenzied swings in value on the other. •



MONETARY AUTHORITIES MUST PUT INTEROPERABILITY AT THE CORE OF THEIR DIGITAL TRANSITION

Future of central bank digital currencies will involve multiple ‘layer 1’ transaction networks, writes Simon Chantry, Chief information officer at Bitt.

MANY MONETARY AUTHORITIES have been waiting for US authorities to reveal their central bank digital currency roadmap. While official publications from the US Department of Treasury and New York Federal Reserve do not commit the Fed to a digital dollar, they could signal the way ahead for the world’s pre-eminent reserve currency. With high expectations in the international financial community, CBDC functionality is coming under increased scrutiny, and for good reason.

One critical CBDC element is interoperability, with respect to cross-currency integration as well as integration with legacy financial networks. All signs point to a future where CBDCs are issued on multiple ‘layer 1’ transaction networks or protocols.

Many CBDC design choices are yet to be made. However, the US Treasury has identified eight key objectives that the digital dollar must meet:

- 1. Provide benefits and mitigate risks for consumers, investors and businesses.
- 2. Promote economic growth and financial stability, and mitigate systemic risk.
- 3. Improve payment systems.
- 4. Ensure the global financial system has transparency, connectivity, and platform and architecture interoperability or transferability, as appropriate.
- 5. Advance financial inclusion and equity.
- 6. Protect national security.
- 7. Provide the ability to exercise human rights.
- 8. Align with democratic and environmental values, including privacy protections.

While it’s straightforward to list policy objectives, it’s more complex to design a CBDC architecture that achieves them, not least because some of these objectives are, at times, operating at cross-purposes. Promoting growth, ensuring stability and mitigating risks require a focus on interoperability, allowing central banks to better adapt to the multi-network future and to integrate with a variety of tools. The future of payments and web3 depends on interoperability, as participants continue to build valuable use cases on different platforms.

Bitt’s CBDC platform enables smooth integration with multiple transaction networks, with proven network security and privacy protections. It has been engineered to provide financial intermediaries with a way to compete to drive down the cost of payments, integrate with new digital currency networks and provide technically provable security and privacy guarantees to users. These tools should be interoperable with the most advanced transaction networks, including private permissioned networks, such as Hyperledger and Corda, and MIT’s OpenCBDC-tx, as well as public networks, such as bitcoin. Ethereum, and Stellar. This is where Bitt’s efforts are focused – in providing next generation monetary platforms, tools and applications.

INTEROPERABILITY CREATES NETWORK EFFECTS

While the public may not recognise it, all credit card payments, Venmo transactions, ATM cash deposits or remittances leverage numerous integrated payment systems that work together to deliver money from sender to receiver. As we lay the rails for the financial system of the future, we can assess the strengths and weaknesses, pros and cons, and integrative capabilities of the existing financial system to inform how the shift towards internet-native payments networks will enable new services, bring about efficiencies, lower costs, and decrease fraud and abuse. CBDCs should be designed to make users’ lives easier, with the ability to work with new payments networks and methods at their core.

Interoperability enables network effects and provides users with options for participating in connected financial ecosystems. These options can be useful in times of distress, but also for expanding business activity and accessing more counterparties. Interoperability also creates a greater opportunity for central banks to facilitate innovation and competition, to promote inclusion and to provide opportunity for all economic stakeholders. However, it demands that monetary authorities have modern and comprehensive tools that can help them manage their national digital currency on at least one new

Figure 1: Central banks have been testing several transaction networks for use in a future CBDC rollout.

Ethereum	Hyperledger Fabric	Corda	Quorum
Reserve Bank of Australia	European Central Bank	Bank of Canada	Monetary Authority of Singapore
Bank of Canada	Bank of Japan	Monetary Authority of Singapore	South Africa Reserve Bank
Hong Kong Monetary Authority	Monetary Authority of Singapore	Bank of Thailand	Bank of Canada
Bank of Thailand	Banque of France	Banque of France	Banque of France
New York Federal Reserve	Saudi Arabian Monetary Authority	Hong Kong Monetary Authority	BIS Innovation Hub
Norges Bank	Central Bank of the United Arab Emirates	Bank of Thailand	Swiss National Bank
	Eastern Caribbean Central Bank	BIS Innovation Hub	Bank Negara Malaysia
		Swiss National Bank	South Africa Reserve Bank
Stellar	OpenCBDC	Bank Negara Malaysia	Hong Kong Monetary Authority
National Bank of Ukraine	Federal Reserve Bank of Boston	South Africa Reserve Bank	Bank of Thailand
	Bank of England	Peoples Bank of China	Peoples Bank of China
	Bank of Canada	Central Bank of the United Arab Emirates	Central Bank of the United Arab Emirates
Unknown		Swiss National Bank	Reserve Bank of Australia
Bank of Jamaica		Reserve Bank of Australia	
Peoples Bank of China		National Bank of Khazakistan	
Central Bank of the Bahamas		Riksbank	

Source: Bitt

network, if not multiple networks. This includes all elements of managing the digital currency lifecycle, the most crucial of which is the monetary authority’s ability to confirm that only authentically minted digital currency is circulating. Central banks also recognise the possibility to improve the precision through which they implement, monitor and adjust monetary policy in real-time. A robust CBDC platform should include such functionality, while preserving privacy and being flexible enough to adapt to future financial and monetary conditions.

This list illustrates the criteria central banks are using to evaluate networks. Each transaction network comes with its own unique structure and capabilities, including:

- Unspent transaction output or account-based structure
- Hosting structure
- Developer and community support
- Availability and depth of supporting documentation
- Compatible software languages and libraries
- Transaction throughput and scalability metrics
- Validation process and consensus mechanisms
- Governance structure
- Security considerations

Further practical considerations include the use of the network in other projects, which enables collaboration and shared operating experiences. Similarly, a given monetary authority may have previous bias, based on their exposure to a particular network, or the experience and inclinations of their IT department. Ultimately, central banks will decide on several networks with which to test and pilot their CBDC, but they must be ready to integrate with one another’s networks as cross-currency and multi-currency functionality is critical to the success of CBDCs.

EXPANDING MANDATES

Historically, a monetary authority’s mandate is to use monetary policy to optimise growth and ensure price stability. As central banks evolve to provide public financial infrastructure, they will be taking on new responsibilities, including CBDC platform security, availability and instant payments. Central banks must level up on the technology front as a result. This is happening in the form of public-private partnerships, increased IT hiring and international collaboration through bodies such as the Bank for International Settlements and World Bank, and the International Monetary Fund.

Given the competition, it is difficult for central banks to decide on a transaction network layer. The financial system of the future is likely to be a composite of multiple transaction networks, working with one another to process and settle transactions. Therefore, in order to achieve their traditional mandate, as well as new responsibilities in operating a CBDC network, monetary authorities require toolsets that are interoperable with multiple underlying transaction networks.

The Digital Currency Management System’s Numa architecture, created by Bitt, defines deployment parameters for any digital currency issued by the client monetary authority. Numa allows for many monetary policy actions, integration with any transaction network, role-based permission settings for all stakeholders and configurable wallet types and tiers, along with the capacity to develop and implement both internal and external application programming interfaces and software development kits for a wide array of use cases. Bitt is enabling monetary authorities to transition smoothly to web3 with a CBDC architecture and toolset and a resilient and secure platform that has been designed for the future of finance. •



CENTRAL BANKS MUST TAKE THE LEAD IN PAYMENTS CYBERSECURITY

Once new rules and regulations are in place, the finance sector must set the standard in defending this new component of critical national infrastructure. By Simon Brady

THE benefits of payments innovation are clear. Digitalisation of payments lowers transaction costs, increases transaction speed and reduces the complexity of making payments. It allows millions of the poor and the unbanked to use their mobile phones to access financial services that those in developed markets take for granted. The benefits of reduced fees to the billion migrants paying an average of between 6%–7% in fees on their remittances demonstrate the gains to be made from improving the efficiency of payments.

And users have not been slow to take advantage.

According to the International Monetary Fund, in India alone, digital payment volume 'has climbed at an average annual rate of about 50% over the past five years. That itself is one of the world's fastest growth rates, but its expansion has been even more rapid – about 160% annually – in India's unique, real-time, mobile-enabled system, the Unified Payments Interface where transactions more than doubled, to 5.9bn, in June 2022 from a year earlier as the number of participating banks jumped 44%, to 330.' Growth of this kind is occurring throughout emerging markets, from Brazil and Indonesia to

KEY FINDINGS

1. The rapid spread of digital payments has spurred the development of a complex and often unregulated ecosystem of new payments providers in emerging markets.
2. Emerging markets are particularly exposed to cyberattacks as they are more lightly regulated and businesses spend less on cybersecurity.
3. Central banks have not yet fully grasped the threat these new entrants pose to the financial system nor put in place sufficient cybersecurity-related regulation.
4. Central banks and the financial sector as whole must take the lead in lobbying for better legislation, driving cybersecurity best practice down into supply chains, raising consumer awareness and setting cybersecurity and resilience standards for payments systems as well as traditional banks.

Kenya and Kazakhstan.

Open banking initiatives, which are key drivers of payment system innovation, continue to be rolled out across developing markets. In November, the Saudi Central Bank announced a new open banking framework along with 'tracking the development of banks and fintechs to ensure their readiness to launch open banking services within the first quarter of next year'. Some fintechs have already been testing open banking services through the SCB's regulatory sandbox.

NEW PLAYERS, NEW RISKS

However, the extraordinary proliferation of alternative payments providers in emerging markets, combined with the many government-driven digital initiatives, including cross-border payments solutions and central bank digital currencies, create their own complexities and problems. Most significantly, the proliferation of payments platforms and ecosystems creates a hugely attractive new target for cybercriminals and digitally enabled fraudsters.

Many of these will aim to steal directly from the platforms, extract ransoms and steal user credentials to commit fraud. But they will also increasingly be joined by others. Payments systems, whether private or public, also become, by default, part of a country's critical national infrastructure. They are then a target for nation-state actors who

may penetrate or disable them as an act of cyber-warfare or espionage. In a society that has become dependent on digital payments, disruption can not only disable important financial functions, it can also quickly cause broader issues and even civil unrest. As emerging markets become more significant players on the world's stage, these nation-state attacks will only increase.

These issues are not confined to one country or region, but the characteristics of emerging markets favour cybercriminals and the potential for material damage is greater.

At an organisational level, there is already a security divide between financial services firms in the developed and developing worlds. As digital payment flows increase in the latter, malign actors will shift their attention from well-protected entities in developed markets to the comparatively less secure firms in emerging economies, many of which still have small to non-existent cybersecurity budgets.

At the level of the individual, the widespread and rapid adoption of new financial technologies by those previously unbanked creates an opportunity for sophisticated fraudsters and cybercriminals to take advantage of populations with little education or experience around cybersecurity. And many emerging markets also have large populations of low-income earners and those in precarious employment. They are frequently targeted by criminals who exploit financial distress to persuade employees to give them access to key network resources which they then use to launch ransomware and other attacks. The younger and more technically skilled may also turn to cybercrime as a lucrative source of income.

FINANCE MUST LEAD

Digital payments are here now and payments platforms, accessed via mobile apps, whether built by central banks or fintechs, are becoming the de facto money transmission infrastructure for emerging markets. This is an opportunity for the finance sector to extend good cybersecurity practices to customers and suppliers. If central banks and financial authorities put in place effective security and resilience regulations now, and banks and other financial services firms drive these standards down into their supply chains, customers and countries will be much better protected against the threats posed by cybercriminals.

The first step is for central banks to ensure that



THE PROLIFERATION OF PAYMENTS PLATFORMS AND ECOSYSTEMS CREATES A HUGELY ATTRACTIVE NEW TARGET FOR CYBERCRIMINALS AND DIGITALLY ENABLED FRAUDSTERS



they themselves are secure. Not only should they be setting the best possible examples of best practice for those they supervise, but they also need the highest standards of security to protect critical financial infrastructure.

This is not a given. In February 2022 security firm Kaspersky found evidence that hackers had stolen data that allowed them to gain access to the entire infrastructure of an unnamed central bank, including the systems for international money transfers. They were offering this data to others on the dark web, which is how Kaspersky found it. They contacted Interpol and in a joint investigation all vulnerabilities in the corporate networks of the bank were closed and any opportunities for additional attacks were blocked.

Stephen Kavanagh, executive director of Interpol Police Services, said: 'Over the past few years, we've seen many ransomware attacks carried out by these "hybrid" teams. Previously, however, their targets were mainly commercial companies. We are happy that together, with our partner Kaspersky, we were able to prevent an attack that could have affected the region's economy. It is only through effective co-operation on the international level and striving to be ahead of the curve that we will be able to effectively protect the global community.'

This is not an isolated example. In January 2022, Bank Indonesia confirmed a ransomware attack hit

its networks. During the attack, on a central bank office on the island of Sumatra, the perpetrators allegedly stole 'non-critical' employee data and deployed ransomware payloads on several devices on the network. The attack was said to be the work of the Conti ransomware group, hackers ultimately tied to Russian actors.

DEVELOP EFFECTIVE, SPECIFIC REGULATION AND SUPERVISION

Beyond their own security, central banks, as supervisors and overseers of banking and payments systems, are responsible for ensuring that appropriate regulations on operational and cyber risk are in place. In developed markets, for example, the Bank of England and the Federal Reserve have published detailed operational guidelines and cyber resilience expectations which are likely to develop into more prescriptive regulations on technology and security over time. Emerging market central banks must follow suit, in conjunction with other bodies responsible for the supervision and oversight of payments systems.

Emerging market central banks certainly understand the issues. In a September 2022 Bank for International Settlements working paper, 'Cyber risk in central banking', members of the Global Cyber Resilience Group, a group set up in 2020 as a forum for central bank chief information security

officers to discuss both tactical and strategic cyber resilience topics, were surveyed.

It revealed that emerging market central banks are ahead of their peers in the advanced economies. Asked if 'the relevant supervisory authority in your jurisdiction provides a risk management framework to financial firms on cyber security?', more than 80% of emerging market respondents replied in the affirmative, compared to just over 60% from advanced economies. The report also stated that 'while supervisory authorities in most emerging markets provide a framework for the collection of information on cyberattacks on financial institutions, less than half of those in advanced economies do. Similarly, while supervised firms are mandated to report losses related to cyberattacks to the central bank in almost all emerging markets, only two-thirds of advanced economy respondents report that such disclosure is required.' As yet, no jurisdiction requires firms to disclose such losses publicly.

Of direct relevance to payments innovation, respondents reported that they see fintechs to be more at risk from a cyberattack than big techs, even though most respondents agree that a successful attack on a big tech would lead to materially higher costs than an attack on a fintech.

'Relative to a financial institution, three-quarters of respondents from advanced economies and two-thirds of emerging market economy respondents think that fintechs are more at risk of becoming the target of a successful cyberattack. When it comes to aggregate losses in terms of gross domestic product, however, these patterns are strikingly different. Among emerging economy and advanced economy respondents, the majority thinks that a successful attack on a fintech will lead to a similar or lower loss in terms of GDP than a successful attack on a traditional financial institution. Among big techs, however, only one-quarter of AE respondents and no respondent from an EME assess the cost to be lower than that of an attack on a traditional financial institution.'

This points to other ways in which central banks can contribute to payments system integrity. They can establish sandboxes or other types of similar arrangements in which fintech firms and firms involved in cybersecurity can collaborate on projects and build in cybersecurity from the outset. Second, they can regulate and incentivise the fintech industry to further improve its cybersecurity capabilities.

Some central banks are doing a better job of this than others. For example, in late September 2022, in a speech on financial crime, Nor Shamsiah Mohd Yunus, governor of Bank Negara Malaysia, focused predominantly on the cyber threat to banking and payment systems, saying that 'BNM requires banks in Malaysia to adopt high standards of security, especially for internet and mobile banking



DIGITALISATION OF PAYMENTS LOWERS TRANSACTION COSTS, INCREASES TRANSACTION SPEED AND REDUCES THE COMPLEXITY OF MAKING PAYMENTS

services,' with the bank now specifically mandating 'a migration from SMS one time passwords to more secure forms of authentication for online activities or transactions relating to account opening, fund transfers and payments.'

This detailed guidance from a central bank is rare and to be welcomed. As Yunus pointed out, 'these controls may also inevitably lead to some friction or inconvenience in the online banking experience of customers... while these measures entail some inconvenience, they are important to protect the interests of customers.'

The governor of the Central Bank of Nigeria, Godwin Emefiele, has also issued a risk-based cybersecurity framework and guidelines for the financial sector which include specific minimum requirements. In addition, there are a series of fintech-based policies and guidelines which cover regulatory sandboxes, open banking and cybersecurity, among others. Revised versions of these guidelines must be adhered to by early 2023.

'The extent of technology risks and the level of sophistication of cyber-attacks are rapidly expanding. This development has demanded that financial institutions, including other financial intermediaries, strengthen their cyber resilience and take proactive steps to secure their critical information assets to ensure their safety and soundness,' Emefiele added in a recent speech.

In Brazil at the end of 2021, new rules came into effect that subject cloud service providers to greater scrutiny by the country's central bank but stop short of banning bank data from being sent abroad. The regulation was the first issued by Brazil's National Monetary Council (CMN) to deal with cybersecurity issues and is the first that forces organisations of any kind in Brazil to appoint data protection officers.

The CMN not only forces financial institutions to be fully compliant with its cybersecurity policies, but also gives the central bank unfettered access to data hosted by third parties anywhere, at any time. It also allows the central bank to block deals with third-party data handlers located abroad and urges financial institutions to only send information to countries that have information-sharing agreements with Brazil.

However, there is still too little explicit cybersecurity regulation and oversight from central banks and governments given the scale of the threat. And there is too little oversight of non-bank



THIS ECOSYSTEM IS RIPE FOR EXPLOITATION BY CYBERCRIMINALS AND WITHOUT A MUCH QUICKER RESPONSE FROM GOVERNMENTS AND REGULATORS, THERE WILL BE SYSTEMIC REPERCUSSIONS



payments providers.

As the threats to financial systems grow, it may also be necessary for regulators to go further than broad guidelines and to develop more detailed and prescriptive rules around specific technologies and operational details such as testing. Given the importance of threat-led penetration testing in assessing cybersecurity, it may be that central banks and related regulators should set up testing frameworks for entities they regard as systemically important. Few do.

STRENGTHEN THE SUPPLY CHAIN

A significant challenge for both regulators and the regulated in the financial sector is the reliance of participants on each other and on critical third-party service providers, such as cloud service operators, security vendors and hardware providers. Hackers often attack via these third parties because they are weaker links in the security chain.

As the World Bank recommended, ‘Financial authorities and central banks [should] conduct sector mapping to establish a clearer understanding of which third-party service providers are of systemic importance to their financial sector and ensure that the relevant providers also comply with the applicable cyber regulations, operational guidelines and cyber resilience expectations.’

Here there are templates available in developing markets, notably the European Union’s digital operational resilience act. The significance of DORA is two-fold. First, it does not cover only financial institutions and service providers, it also covers critical information and communications technology third party providers, including cloud service providers. It imposes significant penalties on ICT service providers for non-compliance. For example, a daily penalty payment of 1% of the average daily worldwide turnover of the ICT service provider in the preceding business year can be levied until compliance is achieved.

Second, it recognises the limitations of uncoordinated national initiatives in combatting a cross-border, global threat. Reliance upon country-by-country regulation results in overlaps, inconsistencies, duplicated requirements, as well as high administrative and compliance costs. In Europe, this can be addressed by the EU. Emerging markets must leverage existing regional forums to promulgate consistent regional regulation to avoid beggar-thy-neighbour approaches and to present a united front against borderless cybercrime. Again, there is clearly a role for central banks to play.

ENCOURAGING CROSS-BORDER COLLABORATION

Here there are encouraging signs. For example, in October 2022, the Gulf Cooperation Council’s ministerial committee for cybersecurity held its first meeting at the headquarters of the general

“
THESE ISSUES ARE NOT CONFINED TO ONE COUNTRY OR REGION, BUT THE CHARACTERISTICS OF EMERGING MARKETS FAVOUR CYBERCRIMINALS AND THE POTENTIAL FOR MATERIAL DAMAGE IS GREATER

secretariat in Riyadh, Saudi Arabia. The meeting focused on co-operation between the GCC states in the field of cybersecurity, including developing frameworks, policies and joint procedures to address cyber threats, and the exchange of knowledge, expertise, studies and experiences related to cybersecurity. It has the aim of creating a safe cyberspace to protect the GCC states from threats. Additionally, the first Gulf cybersecurity exercise was launched during the meeting.

In January 2022, the Association of Southeast Asian Nations digital ministers’ meeting announced the launch of the Asean cybersecurity co-operation strategy 2021-25. A key objective of this is to strengthen the collective efforts of member states, with a view to securing the region’s cyberspace and to promoting the digital economy. And there are longer-standing initiatives from the African Union and Organization of American States.

In July 2022, Bank Indonesia and the Reserve Bank of India signed a memorandum of understanding for closer co-operation in areas including fintech.

Signed on the sidelines of a G20 meeting in Bali, the central banks of two of the four biggest countries in the world by population have pledged to work more closely together in payments systems and digital financial innovation, including in the areas of cyber- and financial crime.

The MoU is the latest to be signed by BI with other central banks – it signed a similar arrangement with the Central Bank of the United Arab Emirates in November 2021 and with the Bank of Korea in February 2022.

More initiatives like this are needed. Central banks and financial authorities should reach out to their peers in their region to coordinate follow-up actions regarding recommendations and to co-operate in joint initiatives where appropriate. As the European Commission and the European Central Bank do at the level of the EU, the institutions of African co-operation and/or economic and monetary integration initiatives could play a facilitating role in this.

LOBBY FOR BETTER LAW

Ultimately, central banks can only do so much to improve the cybersecurity of payments systems by themselves. However, they can call upon governments to bring forward legislation and to

develop efficient and credible judicial and law enforcement systems around cybersecurity.

Currently, that legislative framework and the resourcing of law enforcement are insufficient. Cybercrime pays well because many countries do not have adequate security and privacy laws in place.

For example, Interpol’s latest Africa cyberthreat assessment report stated that ‘This [digital financial] transformation highlights the urgent need to ensure cybersecurity parameters and standards meet the demands and future needs of this community... However, the absence of these standards is pervasive in Africa. 90% of African businesses are operating without the necessary cybersecurity protocols in place. Without these protocols, threat actors are able to exploit increasing vulnerabilities as they continue to invent new cyberattack vectors.’

The report quoted Tarek Sharif, executive director of the African Union Mechanism for Police Cooperation: ‘On this young continent, every economic challenge generates an innovative solution that may sometimes, unfortunately, be at the limit of what the law allows. For example, the low rate of banking facilities for African populations has led to the creation of new financial services such as mobile banking, but also to the resurgence of new forms of scam linked to these new technologies.’

Governments have responded slowly to the

challenge. The African Union – as part of its agenda 2063 for transforming Africa – has identified cybersecurity as a key priority to ensure that emerging technologies benefit African people and companies. The initiative is guided by the African Union Convention on Cyber Security and Personal Data Protection (known as the Malabo Convention), which was drafted in 2011 but only adopted in June 2014. Its purpose is to establish ‘a credible framework for cybersecurity in Africa through organisation of electronic transactions, protection of personal data, promotion of cybersecurity, e-governance and combating cybercrime.’

However, by May 2022, the convention had only been ratified by 13 out of 55 AU member states. By the same month, only eight African countries had in place national cybersecurity strategies and only a handful of countries had laws in place to protect consumers and businesses. The International Telecommunication Union’s global cybersecurity index 2021 showed that of 54 African countries assessed, only 29 had introduced cybersecurity legislation.

Africa is not an exception. India is not party to any convention on the protection of personal data which is equivalent to the EU’s General Data Protection Regulation and it has not yet enacted specific legislation on data protection. Countries such as Vietnam and Indonesia have no consolidated data protection law, just scattered legislation covering



“
BEYOND THEIR OWN SECURITY, CENTRAL BANKS, AS SUPERVISORS AND OVERSEERS OF BANKING AND PAYMENTS SYSTEMS, ARE RESPONSIBLE FOR ENSURING THAT APPROPRIATE REGULATIONS ON OPERATIONAL AND CYBER RISK ARE IN PLACE





DIGITAL MONEY IN THE CLOUD: BUILDING THE FUTURE OF PAYMENTS ON AWS

Stakeholders need secure, resilient and scalable infrastructure to deploy CBDC and digital asset ecosystems, writes Xiaochen Zhang, global head, innovation and GTM, Amazon Web Services, and Hugo Dante, Market Insights & GTM Analyst AWS

IN A RAPIDLY CHANGING digital landscape, public finance institutions worldwide face an array of opportunities and risks. They must explore ways to update their national monetary systems and asset management approaches to meet the needs and demands of a new digital economy. As a result, according to Atlantic Council, at least 105 central banks, representing over 95% of global gross domestic product, are exploring central bank digital currencies. In addition, central banks and other public finance institutions are investigating new ways to create and manage digital assets to meet their policy objectives.

To build and deploy CBDC and digital asset systems, stakeholders require secure, resilient and scalable infrastructure. Amazon Web Services provides cloud services and tools that can be used to experiment, develop and launch secure, scalable, interoperable and resilient fit-for-purpose CBDCs and digital assets. Performance requirements for CBDCs and other types of digital assets are similar. Some of the benefits of CBDC development and deployment on AWS include:

Security: Security is the priority at AWS and is a critical design consideration for CBDC solutions. AWS offers a set of cloud security tools that can support central banks in safeguarding CBDC systems. These tools support user authentication, security from threats and error, incident response, cryptographic tools to secure messages and compliance. AWS's core infrastructure is built to satisfy the security requirements for the military, global banks and other high-sensitivity organisations. Security services like AWS Shield and AWS WAF protect against distributed denial of service attacks and structured query language injection attacks. AWS supports 90 security standards and compliance certifications, and all 117 AWS services that store customer data offer the ability to encrypt that data.

Resiliency and scalability: CBDC infrastructure requires high resiliency, with global connectivity and internet of things integration being critical considerations for CBDC development. AWS global infrastructure is designed for the scalability and resiliency required to support our global customers including CBDC systems. The AWS Cloud spans multiple availability zones within 30 geographic regions

around the world, which comprise of physically separated datacenters. It has data and network redundancy to ensure high availability, quick recovery and operational continuity with minimal intervention in case of disruption. Automated scaling of cloud resources, automated data backup and failover, and databases delivered on the AWS Cloud provide multi-region design disaster recovery and high availability benefits.

Data collection and analysis: As central banks explore and launch CBDCs, they must develop frameworks for supervision, data collection and risk mitigation. AWS offers a broad set of tools for public sector customers to automate secure data collection and analysis, monitor illicit activities and identify risks. AWS Artificial intelligence and machine learning services support anti-money laundering compliance, large scale data analysis and fraud detection. Additional advanced analytics products can be deployed to incorporate CBDC transaction data as an additional source for research-focused use cases.

Prototyping and design: Keeping up with rapid technological innovation requires infrastructure that is flexible and open to experimentation. AWS offers opportunities for customers to engage in low cost experimentation to support the rapid and secure deployment of new CBDC features. Central bank customers can leverage AWS services such as Amazon Managed Blockchain and specialised AWS partners to develop sandboxes, as well as to prototype and deploy CBDC solutions.

Sustainability: Sustainability is a hallmark of AWS. By building CBDCs on the cloud, central banks can make sure that the innovation of tomorrow does not come at the expense of the planet today. Amazon is on a path to power its operations with 100% renewable energy by 2025 – five years ahead of its original target of 2030. AWS provides customers with tools to help them meet their sustainability goals. The AWS customer carbon footprint tool calculates the carbon emissions generated from using AWS, enabling customers to incorporate this into their own sustainability reporting. AWS data exchange offers a wide variety of environmental, social and governance, and sustainability datasets that central bank officials can use as they design their CBDC. •

specific sectors. That is just data privacy, not cybersecurity. Many other emerging markets are in the same position. Across all these markets, cybercriminals threaten the availability of payments services, the integrity of payments infrastructure and the confidentiality of citizens' data.

All need programmes to raise cybersecurity awareness among their populations. They need additional policies and legislation to fight cybercriminals. And they need to put in place technologies on a national and international scale to reinforce cyber defence.

MORE RISKS COMING

As payments innovation accelerates, the cybersecurity risks inherent in the payments system will increase. Populations will become ever more reliant on a complex ecosystem of private sector platforms whose security posture will be hard to control. And central banks have one final role to play in that risk landscape.

The Atlantic Council's central bank digital currency tracker now shows that 105 countries and currency unions are currently exploring the possibility of launching a CBDC, either retail – issued to the general public – or wholesale, used primarily for interbank transactions. That's up from an estimated 35 as recently as 2020. But to what extent do CBDCs embed cybersecurity and privacy risks and what do central banks have to do to design safe CBDCs?

CBDCs generally involve the centralised collection of transaction data. This data not only

creates privacy issues (and could be used to monitor citizens' payment activity, movements and other sensitive personal information), it also creates a hugely attractive target for hackers, meaning it would require impenetrable security.

The underlying technology chosen also changes the security and privacy calculus of any given CBDC. Retail CBDCs, such as the eNaira launched in Nigeria in October 2021, that use blockchain technology require the involvement of third parties as validators of transactions. This introduces a new role for third parties in central bank money operations. Critically, the security guarantees of the ledger would depend on the integrity and availability of third-party validators, over which the central bank may not have direct control.

The BIS also found that central bank CISOs believe that the introduction of CBDCs will require an increase in cybersecurity budgets.

CENTRAL BANKS AT THE FOREFRONT

Emerging markets are likely to leapfrog many years of payments systems evolution, moving directly to a world in which consumers and businesses transact via dozens of different mobile and web-based applications, some of which will bypass the traditional banking system entirely. This ecosystem is ripe for exploitation by cybercriminals and without a much quicker response from governments and regulators, there will be systemic repercussions. Central banks must be at the forefront of efforts to secure both traditional banks and newer entrants into the payments space. •





THE METAVERSE: A MODEL FOR DIGITAL PAYMENTS?

The metaverse should prove a catalyst for development in the payments industry. By Lewis McLellan

AS a term, metaverse has leapt from the pages of Neal Stephenson’s 1992 novel Snow Crash and entered common parlance thanks, in no small part, to Facebook’s decision to rebrand itself as Meta, and the company’s colossal spend on infrastructure to develop the metaverse, which it calls the next evolution in social connection.

Huge promises of the economic activity the metaverse will enable are becoming commonplace. Citi estimated the total addressable market as between \$8tn and \$13tn. McKinsey, more conservatively, estimated that it could reach \$5tn by 2030, of which around \$2.6tn will be in e-commerce. Exactly what the payment rails enabling this kind of activity will look like remains an unsettled question.

The metaverse is often conflated with a shared

virtual reality space – perhaps because that is how it was used in the novel that coined the term – but the definition is broader. After all, VR – and more particularly, shared VR spaces – may grow in popularity as the technology improves and access grows but it is likely to struggle to achieve the same ubiquity as smartphones.

While virtual and augmented reality applications will form part of the metaverse offering, for many people, computers and phones will continue to be their main method for interacting with digital spaces.

That does not mean that nothing will change, however. Along with Web3, the metaverse is, first and foremost, a model for a digital economy. It will be the venue for the exchange of digital goods and services. For such a marketplace to take off, goods

KEY FINDINGS

- 1. Traditional payment rails may prove too slow and costly to enable the instant micropayments that are expected to be a major use case in the metaverse.
- 2. Cryptocurrencies are a natural fit for the metaverse, but have achieved little traction as a means of payment.
- 3. Stablecoins, with increasing government involvement and regulation, are likely to offer most people a more convenient and familiar means of payment in the metaverse.
- 4. Developing the infrastructure to make metaverse payments stable, secure, interoperable and free from financial crime will have a huge impact on the broader payments landscape.

must have value beyond that imparted by a single institution. Licensed digital cosmetic assets, for example, will be much more valuable if they can be used throughout a broader ecosystem than if they are only usable within one game or platform.

Tracking ownership of assets like this will, almost certainly, be a function of blockchains, which can register ownership in a decentralised fashion. This kind of capacity might lead to a reduction in unauthorised trading in digital assets and help to protect creators’ revenue.

This is likely to mean major changes to business models. In gaming – one of the few industries in which virtual asset ownership is already prevalent, generating some \$54bn of revenue in 2020 – developers’ revenue comes increasingly from sales of game cosmetics, rather than from game or platform sales. A metaverse that enables those assets to travel between game environments could bring major changes for these business models, since a user who purchases a skin, which changes the appearance of a character, in game A and wears it in game B is less likely to spend money on a similar cosmetic in game B.

The metaverse, then, will consist of a shared ecosystem of digital asset ownership running on a variety of interoperable blockchains. Some but not all these digital assets will be used in virtual and augmented reality.

The infrastructure regarding asset ownership is developing gradually, with interoperability a key area of focus. To some extent, several competing or complementary models for the metaverse

payments infrastructure already exist.

The first question to address is the degree to which traditional fiat digital payment systems are viable in the metaverse. They have already made themselves key to the functioning of e-commerce but there are some unique features in the metaverse that may make them less able to adapt to its requirements.

THE NEED FOR AN ON-CHAIN PAYMENTS SYSTEM

Digital payments made through conventional systems work reasonably well for e-commerce transactions, so it is not inevitable that new payment solutions are needed for the metaverse.

Mastercard, Visa and American Express are making moves to support the provision of payments in the metaverse, filing trademark applications to provide their suite of services in the new arena.

However, if many of the assets transacted in the metaverse will be either blockchain native or blockchain tokens representing ownership, then providing a means of payment on the blockchain brings a number of benefits.

First, cost. Although conventional digital payments are typically free for users, the fees levied on merchants by payments providers mean that only transactions above a certain threshold are economically viable.

This is one of the main reasons behind the dominance of the subscription model for digital content provision, rather than paying per use. Processing a payment for a month’s access to a service is economically viable where paying to read a single article may not be.

Instant micropayments, available 24/7, are likely to be the main mode of payment in the metaverse. Operations like paying small fees to unlock additional features or distributing royalties to creators are likely to require extremely small value payments at high volume. Delivering this with the present system is challenging and expensive.

There are speed and efficiency benefits that come with a new system. One of the benefits of exchanging assets in a blockchain environment is the opportunity for instantaneous, atomic settlement and the removal of counterparty risk.

Achieving this within the metaverse will not be simple. Exchanging delivery and payment on the same blockchain is a simple and efficient matter.

“ALTHOUGH CONVENTIONAL DIGITAL PAYMENTS ARE TYPICALLY FREE FOR USERS, THE FEES LEVIED ON MERCHANTS BY PAYMENTS PROVIDERS MEAN THAT ONLY TRANSACTIONS ABOVE A CERTAIN THRESHOLD ARE ECONOMICALLY VIABLE



Exchanging assets between blockchains requires interoperability bridges.

The metaverse will not consist of a single blockchain. Rather, it will consist of multiple, interconnected networks of blockchains. Developing this infrastructure is a significant challenge. Many efforts to create interoperability bridges between blockchains have been the subject of cyber-attacks and hacks, causing major losses.

The challenges such systems will face are similar to those faced when providing cross-border payments networks in fiat currency. While domestic payments may operate efficiently, sending payments between domestic networks can be challenging because they are differently configured. They might have different numbers and types of participants, different formats for data, and different levels of security and protection. Harmonising all of these disparate standards is an immense challenge in the fiat cross-border payments world and is likely to remain a challenge in the metaverse.

While such a metaverse system may well be developed, it will need to meet extremely high standards of resilience and security in order for it to underpin the payments network.

CRYPTOCURRENCIES

For many, payments in the metaverse means payments using cryptocurrency. In some sense, this makes sense. Cryptocurrencies were the first use case of blockchains and, given blockchain is likely to form a major part of the infrastructure for the metaverse, it is no surprise that they are an early contender to become a payments solution.

The infant stages of the metaverse have, in many cases, been constructed by and for cryptocurrency users. Decentraland, for example, is on the Ethereum blockchain. Users buy plots of virtual land (where ownership is represented by non-fungible tokens), using a Decentraland native cryptocurrency called MANA, which is typically purchased with ether, Ethereum’s cryptocurrency.

However, cryptocurrencies have, overall, failed to take off as a mainstream means of payment. Most people are reluctant to transact in units other than those in which their salary and taxes are denominated. The exchange risk this entails puts off most except those who wish to speculate.

At present, the lack of stability in the value of bitcoin and the rest of the cryptocurrency ecosystem renders it too volatile for use as a major channel for payments since costs and revenues would be too unpredictable.

Many metaverse infrastructure providers will launch their own cryptocurrencies, which are typically redeemable for services they provide. While they may only be redeemable for services in a specific environment, ideally they should be tradeable across the metaverse.



If there is sufficient, consistent demand for a service paid for in a cryptocurrency, this can give it a stable value across the metaverse and make it more suitable for use in payments. If the connective architecture provides a sufficiently seamless and risk-free experience, then the value of MANA and its ilk should not fall even when it is being traded in a different environment from the one where it can be redeemed.

One potential issue with this is that it can lead to a large range of cryptocurrencies that metaverse users might wish to pay with.

This can lead to a great deal of difficulty for merchants, who might struggle to manage the complexity of such a range of cryptocurrencies, where fungibility and interoperability are not necessarily simple.

If they have to pay suppliers with a particular currency but are typically paid in a range of others, they will have a complex liquidity management operation to conduct.

It may be possible for service providers to remove this complexity, managing an automated exchange system that allows users to pay in the method of their choosing and merchants to receive the cryptocurrency or other payment method of their choice.

In the future, if the metaverse becomes ubiquitous and highly liquid, some envisage a fully invested world where the distinction between a means of payment and an investable asset collapses. Digital tokens representing entitlement to future earnings or discounts on goods and services can all theoretically be used as a means of payment in a world where such assets are sufficiently liquid and can be efficiently and impartially valued and traded. Matthew Harris, a partner at Bain Capital Ventures, believes this is where the metaverse will take us.

This is a radical vision for what payments in the metaverse may eventually look like at some distant time, but it is worth considering that our conception of money is not necessarily fixed permanently and may evolve over time.

STABLECOINS

Stablecoins might offer a more promising means of providing an in-metaverse on-chain payments solution, particularly in the short term. Stablecoins are crypto-tokens pegged to the value of fiat currencies. They maintain this peg typically by holding reserves of the fiat currency, which users can withdraw at will, redeeming their stablecoins.

In essence, this replaces the counterparty or credit risk that depositors take on when they deposit fiat currency in a bank and replaces it with counterparty risk on the stablecoin issuer. While banks are typically stable and insured institutions, it is possible for a stablecoin with robust, transparently audited reserves to command a similar degree of confidence.

Not all stablecoins have this high quality of reserves to draw upon and some have failed catastrophically, resulting in huge losses for investors. The collapse of the algorithmic stablecoin Terra and its associated cryptocurrency Luna triggered a substantial fall in the value of the cryptocurrency market.

However, a secure and well-collateralised stablecoin would give people a means of transacting on-chain and in-metaverse.

This is a particularly attractive option because it should be invisible to the user. Individuals should be able to transact freely and instantly in stablecoins in the metaverse without considering that the money is any different from the digital commercial bank money they use to buy groceries with outside of the metaverse.

BANK SERVICES IN THE METAVERSE

As the metaverse becomes more mainstream, existing players in financial services are already seeking ways to offer their services to a new hub of economic activity.

Some have already planted a flag in the metaverse to ensure they are not left behind. JP Morgan opened a lounge in Decentraland, touting a market opportunity of \$1tn. HSBC and Standard Chartered also purchased land in the metaverse, choosing the Sandbox for their first digital space, as has Thailand’s Siam Commercial Bank.

Banks are anticipating a world of digital economic activity in which they can offer their traditional services in new ways, providing credit and transaction services to individuals and businesses in the metaverse.

There are also digital first challenger banks like Zelf and Sokin, which tailor their offerings to the needs of metaverse users, particularly in gaming.



IN THE FUTURE, IF THE METAVERSE BECOMES UBIQUITOUS AND HIGHLY LIQUID, SOME ENVISAGE A FULLY INVESTED WORLD WHERE THE DISTINCTION BETWEEN A MEANS OF PAYMENT AND AN INVESTABLE ASSET COLLAPSES

TOKENISED DEPOSITS

Banks hold a privileged position in finance because of the regulation they are required to comply with. These risk management principles should make deposits relatively safe and, in the event of the bank failing to meet its obligations, there is state-provided insurance that can reimburse depositors.

These protections are unique to banks. As discussed above, well-designed stablecoins can offer extremely high levels of security. However, some individuals may prefer to operate only within the sort of regulated banking framework with which they are familiar, and some businesses may operate under mandates that prevent them from taking on unfamiliar risks.

Accordingly, as the metaverse grows in scale and reach, there will be a demand for traditional bank-operated transaction services within it. Creating tokens tradeable within the blockchain that represent deposits will be the first stage.

Although these are conceptually similar to stablecoins, in that they are crypto-tokens designed to maintain the value of a fiat currency, they are different in that the security of stablecoins rests entirely on the quality of their collateralisation, while tokenising bank deposits allows users to trade in digital money that has the same risk profile they are used to.

LENDING

As these services develop, it will become possible for in-metaverse assets to be used to collateralise loans in traditional fiat currency, and vice versa.

Tokens that can be redeemed in the metaverse for goods and services, or assets that have demonstrated a consistent value in a digital marketplace – perhaps in-game cosmetics or non-fungible token equivalents of designer products – might form the security for loans made in fiat currency.

However, most lenders will likely demand extremely steep overcollateralisation at present since the performance of digital assets in 2022 has been so poor.

Liquidating digital asset-based collateral can be a difficult process since, in many markets, the liquidity is so thin that the value can crash rapidly if forced sellers begin offloading large volumes.



This has been demonstrated in the cryptocurrency market, where the collapse of the Terra/Luna ecosystem and the subsequent reduction in the value of bitcoin resulted in widespread margin calls and the bankruptcy of several firms.

Having a large, liquid market for these assets will be pivotal to the sustainability of their value. Ensuring that such a market exists requires that these assets be valuable to the broadest possible network, which requires interoperability between networks.

INTEROPERABILITY AND DIGITAL IDENTITY

Ensuring that assets and the means of payment are not bound to a single chain or institutional network but can be traded freely between users in different environments will be important to ensuring a stable, liquid marketplace.

Technically, this is complicated. Ensuring environments are compatible means solving some sophisticated engineering challenges.

One of the key components of the metaverse is likely to be a form of verifiable digital identity that is valid across multiple environments. Users must be able to verify that their counterparty is appropriate for the type of transaction they are undertaking. Age and location verification will be important, as will a successful know-your-customer check.

The ideal solution here is that digital identity can be verified to a counterparty’s satisfaction without exposing personal data.

For it to be valuable in the metaverse, this verification must be able to operate across a broad range of environments.

This kind of verification will be key for payments in the metaverse, ensuring that people can safely and securely exchange value.

Ideally, this identity should form the core of a wallet, which can be used to hold various digital assets and methods of payment, whether these are cryptocurrencies, stablecoins or something else.

This wallet should be able to ‘travel’ to different environments in the metaverse, enabling a variety of different interactions without losing the core identity.

CROSS-BORDER PAYMENTS

Although interoperability between different metaverse environments will be a challenge, one of the opportunities that the development of the metaverse presents is a means of simplifying the process of sending money across borders.

At present, the challenge of connecting the widely varying types of domestic payments networks is proving immensely difficult to address.

Stablecoins and cryptocurrencies present one possible means of circumventing some of the problems (although they bring their own issues).



Simply purchasing a cryptocurrency, sending it to a contact (who may be in another country) who then sells it for their local currency is a quick and simple means of sending value across borders. Right now, this kind of system is likely to have wider foreign exchange spreads and therefore higher costs, which might offset the transaction fee savings, but if sufficiently large liquidity providers join the space, then this gap could be minimised.

However, a system like this is partly cheaper and quicker because it does not adhere to the same standards of KYC, anti-money laundering, countering terrorist financing and other regulations that prevent financial crime. Without monitoring systems in place, cross-border stablecoin transmission could become a channel for criminal payments.

The metaverse, particularly with a robust system for digital identity verification, might provide an opportunity for this type of cross-border payments solution to function more effectively, giving the benefits of simple peer-to-peer transfer in an environment where identity is verified, so KYC and AML standards can be enforced.

ON-RAMPS AND OFF-RAMPS

A key component to all of this is the design of the on- and off- ramps that allow users to transfer value between the metaverse and their conventional fiat accounts.

In the future, it is possible that the payments systems used in the metaverse will become so commonplace that this on-ramp/off-ramp process will be theoretical only and that we will use the same tools to pay in real life as we use to pay for digital goods and services in the metaverse.

For the moment, however, users are likely to maintain a balance in stablecoins or cryptocurrencies for use in the metaverse, distinct from their main stores of value with which they pay for rent, taxes and groceries.

Accordingly, services must exist to allow them to on-board value from fiat to the metaverse environment and the reverse.

Many cryptocurrency exchanges already offer this service, allowing users to buy stablecoins and cryptocurrencies for fiat. Perhaps because of the newness of the industry, many exchanges offer wallets as part of their service, but there is no reason why this would necessarily be the case for payments in the metaverse.

Making this process both secure (adhering to local standards of KYC and other regulation) and efficient will be important to the success of the metaverse.

One way to achieve this is through integration with existing services. Banks, and other financial institutions and payment providers, are the most obvious choice. If they begin providing digital wallet architecture, one could seamlessly move money between a fiat and a digital account without additional layers of identity verification.

Other service providers are likely to attempt to compete with banks for this market. Since wallet provision does not need a full banking license, there will be opportunities for providers to generate value by integrating payments with their own services. Social media and messaging services could add a digital payments function to their service and offer convenient payments within an environment that people are already comfortable with.

Integrating purchase methods within apps, rather than having to set up verification through a separate provider as is typically the case, might improve conversion in online sales, lowering the barrier for purchases.

Another method which already exists is the crypto-debit card. Services allow you to pay in fiat currencies, directly realised from your cryptocurrency holdings. This allows cryptocurrency holders to pay from their holdings to merchants that do not accept cryptocurrency without having to maintain a fiat balance. The money they need is converted automatically from their cryptocurrency account on demand.

One can easily imagine this relationship working in both directions, where a debit card or other payment platform might automatically convert fiat holdings into a cryptocurrency or stablecoin at the point of sale to meet the method required by the merchant.

Convenient payments services are, of course, desirable, but it will be even more important that authorities are able to oversee and police payments.

With cryptocurrency’s pseudonymous nature, the primary means of combatting criminals who make use of it for payments is to police off-ramps, where criminals sell their cryptocurrency for fiat currency.

For this reason, the necessity to verify identity at the level of the service provider is key to the development of a safe and secure metaverse payments environment.

RENT-SEEKING IN THE METAVERSE

Virtual payments can, in theory, be substantially cheaper and more efficient (particularly for low-value payments) than traditional digital fiat payments. However, platform providers may constrain growth by levying transaction fees. These would be justified as a means of paying for the development and maintenance of the platform, rather than processing the payment securely, but would have a similar effect.

While payments providers in the real world typically charge a fee of up to a couple of percentage points of the transaction, major technology providers routinely charge much higher fees for transactions on their platforms. Apple’s approach to monetising its app store is the clearest example. Transactions in the app store or on services distributed by it are subject to a 30% fee.

Meta wishes to adopt a similar model, levying a 30% store fee, and variable platform fees on top, suggesting that creators will receive around half of the revenue from sales in Meta’s version of the metaverse.

Whether these fees are justified by the work the providers do to construct and maintain the platforms on which creators rely is a complicated and difficult question, but whatever the answer, this level of fee will restrict the type of development that is economically viable in the metaverse.

A CATALYST FOR DEVELOPMENT

Momentum around the development of the digital asset ecosystem has understandably stalled because of the destruction of so much value in the NFT and cryptocurrency marketplace over the past year. But the demand for digital assets to exist beyond the issuing institution will grow and the need for a payments industry designed to service those needs will expand too.

The trajectory is not yet certain – and interoperability remains a substantial technical hurdle. For the moment, cryptocurrencies dominate the metaverse and discussions around it, but they are unlikely to ever to achieve dominance as a means of payment. Stablecoins offer a more promising path and there will likely be growing involvement by the state and existing financial players in their provision.

Stablecoins offer a means of quickly sending money across borders. But doing so in the absence of a rigorous monitoring infrastructure opens too many opportunities for crime. The development of the metaverse, and the digital identity infrastructure required to serve it, might carry the institutional heft to offer a solution to this problem. •





PAYMENTS IN THE METAVERSE: INNOVATION FOR BOTH THE PHYSICAL AND DIGITAL WORLDS

Experimentation in the metaverse could spark innovation in physical world payments, writes Robert Clarkson, chief revenue officer of Payoneer.

When thinking about what payments in the metaverse will look like, it’s easy to get distracted by the idea that the metaverse represents a new world or dimension. It does, of course. It’s a fifth dimension, a virtual environment where commerce and creativity will take place in ways that might not even be possible to be imagined right now.

Value, however, will be moved into, out of and within the metaverse. And by disaggregating payments into discrete components, we can better understand where the current models and systems are well-prepared to serve a purely digital world – and where innovation is still needed.

First, it’s important to clarify what is meant by the ‘metaverse’. It won’t just be one single new system. There will be a collection of different metaverses that we can collectively call the metaverse.

THREE COMPONENTS TO THE METAVERSE FOR PAYMENTS

Breaking down the use cases for payments in the metaverse, there are three distinct components. The first refers to putting value into the metaverse from the physical world. The second covers transactions within and between metaverses. The third is about repatriating value from the metaverse into the physical world. Because the first and third components are simply different directions of the same payments flow, they can be addressed as a single aspect of payments pertaining to the metaverse.

This breakdown between putting value into and out of the metaverse as opposed to intra-metaverse payments provides a useful framework for identifying where innovation might be anticipated and required. It also supplies instances where existing models and infrastructure might already be suited for meeting the needs of the different actors expected to be active in this new virtual environment.

FROM PHYSICAL TO VIRTUAL VALUE

Flows into and out of the metaverse have strong parallels with existing flows in the real world, as it is fundamentally a question of transferring fiat currencies to digital currencies. This is already done with credit cards, digital wallets and new digital currencies like bitcoin and stablecoins.

Value will need to enter the metaverse in a way that is recognised as valid and having specific value. If a distinct metaverse has a coin or token that is used to purchase (virtual) goods or services within that environment, that token needs to be denominated in a way that allows us to value it in the physical world. This is neither difficult nor novel, as gamers around the world are already doing this. And it’s already happening in the metaverse: buyers purchase ‘real estate’ in The Sandbox using The Sandbox’s currency \$SAND. Those purchases originated from fiat, for example to fund a cryptowallet or by purchasing \$SAND with a credit or debit card.

A second factor is that the value derived from commerce in the metaverse will still need to be extracted to the physical world so that creators and businesses can benefit from their metaverse labour. Digital value already exists in our daily lives. One common example is when we use frequent flier miles, originally purchased with fiat, to buy luggage allowances or flights.

It is entirely possible that some value created in a metaverse in the form of digital currency will remain there and be reinvested. However, unless and until it is extracted into the physical world, the value of



THIS BREAKDOWN BETWEEN PUTTING VALUE INTO AND OUT OF THE METAVERSE PROVIDES A USEFUL FRAMEWORK FOR IDENTIFYING WHERE INNOVATION MIGHT BE ANTICIPATED.

these digital currencies will remain intangible and dependent upon the benefits that they provide within the metaverse itself.

Will the need for on and off-ramps for the metaverse drive new innovations in payments? Not necessarily, at least at first. Right now, existing rails and forms of money, including digital currency, provide a variety of options for accessing value in the metaverse. However, regulation around stablecoins and cryptocurrencies could impact their utility as a medium between fiat and metaverse currencies.

INTRA-METAVERSE PAYMENTS

What is fundamentally different in payments within the metaverse is the potential impact on the scale and speed demanded of payments. This is true for a single metaverse and is only amplified when it comes to payment flows between different metaverses.

Within a specific metaverse, the parameters of commerce could be upended. These virtual worlds offer literally infinite supply, with expectations of instant delivery that also create demand for truly instant payments to the supplier, beyond today’s expectations. If a metaverse customer purchases a designer shirt for their avatar using that metaverse’s digital currency, they will expect to see it on their avatar immediately. Currently, they can use credit cards to purchase Robux, the currency of Roblox. Once it is in their account, they can use it to instantly purchase that shirt. While the platform accepts the associated friction, will this work for the potentially billions of micropayments that could take place within any metaverse? And if the traditional payments methods are replaced by blockchain-based payments mechanisms, will that system be able to handle them?

Furthermore, the metaverse can be seen as transcending physical borders, but the truth is that there will be digital borders between different metaverses. When it comes to payments, these borders could have the same impact as borders between nations, adding considerable frictions to the transaction. How will one metaverse’s currency be used in another metaverse?

The current discussions around interlinking fiat payments systems might offer some hints on how cross-border payments in the metaverse could work. In its July 2022 report to the G20, the Bank for International Settlements outlined four stylised models for interlinking cross-border payments systems. Under the single access point model, a single gateway entity gives participants in one domestic payments system access to a foreign



EXPERIMENTATION IN THE METAVERSE IS GOING TO CONTINUE AND THE INNOVATION IN THIS VIRTUAL WORLD IS GOING TO SHAPE COMMERCE AND CREATIVITY AROUND THE GLOBE.

system. The bilateral link model connects two payments systems to each other so that participants can directly access all participants in the other system. The hub-and-spoke model links multiple systems through a common intermediary or hub that takes care of accounting and settlement. This model envisages a common payments system, running on an integrated technical platform, so that all the participants are operating within a single system.

Each of these models could translate into the metaverse, but each would face the same challenges and constraints they do in the physical world – challenges that are only magnified in the virtual, instant world. For example, one metaverse could agree protocols through a single gateway for transferring value with another or a hub could offer multiple metaverses the opportunity to interlink. Such approaches, however, would result in the same frictions that institutions like the BIS are trying to reduce in the physical world. While the common platform model might seem to be the ideal way to build a fully interoperable metaverse when it comes to payments, it is difficult to conceive of all the various metaverse stakeholders from the public and private sectors ceding such authority to a single entity.

PAYMENTS IN THE METAVERSE: NEXT STEPS

Experimentation in the metaverse is going to continue and the innovation in this virtual world is going to shape commerce and creativity around the globe, including in ways that cannot even be imagined today. It will drive important discussions about payments in the real world, most significantly around enhancing cross-border payments. Enabling interoperability and ensuring know-your-customer and anti-money laundering standards will be as challenging – and as necessary – in the metaverse as they are in the existing global financial system. Payoneer looks forward to working with the public and private sector stewards of this system to tackle the opportunities offered by the metaverse, not only to build a robust and reliable payments system in the fifth dimension, but also to improve cross-border payments in the service of global commerce in our physical world. •



FUTURE OF PAYMENTS 2022

OMFIF.ORG/DMI