

Central bank digital currencies

A collaboration between OMFIF
and IBM Blockchain World Wire



About IBM Blockchain

IBM Blockchain is recognised as the leading enterprise blockchain provider; working with hundreds of clients across financial services, supply chain, government, retail, media and healthcare to implement blockchain applications, and operate a number of networks running live and in production. The company's research, technical and business experts have broken barriers in transaction processing speeds, developed the most advanced cryptography to secure transactions, and are contributing millions of lines of open source code to advance blockchain for businesses.

Visit www.ibm.com/blockchain/industries/financial-services to learn more about our capabilities in the Financial Services industry.

About OMFIF

The Official Monetary and Financial Institutions Forum is an independent think tank for central banking, economic policy and public investment – a non-lobbying network for best practice in worldwide public-private sector exchanges. At its heart are Global Public Investors – central banks, sovereign funds and public pension funds – with investable assets of \$36tn, equivalent to 45% of world GDP.

With offices in both London and Singapore, OMFIF focuses on global policy and investment themes – particularly in asset management, capital markets and financial supervision/regulation – relating to central banks, sovereign funds, pension funds, regulators and treasuries. OMFIF promotes higher standards, performance-enhancing exchanges between public and private sectors and a better understanding of the world economy, in an atmosphere of mutual trust.

Additional information is available on www.omfif.org, or follow us on Twitter [@OMFIF](https://twitter.com/OMFIF)

This report, finalised on 21 September 2018, is intended not solely for specialists in digital currencies and payment systems, but for a more general readership interested in financial and regulatory development. See p.37 for note on frequently used acronyms.

04

Forewords

Jesse Lund (IBM) and Philip Middleton (OMFIF)

05

Introduction

06

Executive summary

08

Section 1

Defining wholesale CBDCs



14

Section 2

Technology considerations

20

Section 3

Practicalities

22

Section 4

Policy implications

24

Section 5

Case studies

36

Conclusion

39

Acknowledgments



Building on the bitcoin foundation

'The social movement behind bitcoin has perpetuated a mistaken idea that banks are no longer necessary actors for secure global money transfer.'



Jesse Lund
Vice-President of IBM Blockchain

BITCOIN introduced blockchain and distributed ledger technology to financial services, and in the process did a wonderful and terrible thing. On the one hand, it demonstrated that information technology and social readiness for autonomous payment systems have matured to a tipping point. On the other, the social movement behind bitcoin has perpetuated a mistaken idea that banks are no longer necessary actors for secure global money transfer. Similarly, central banks play an essential role in managing monetary policy, which should not be displaced by distributed autonomous organisations.

Building on the foundation laid by bitcoin, IBM believes central bank digital currencies will offer new efficiencies and inspiration for future payment innovations. Beginning with wholesale CBDCs that optimise interbank settlement, as well as settlement between central banks, IBM has already deployed pilot networks with marked success.

The observed benefits are compelling: improved trust between counterparties, increased regulatory transparency, tax collection benefits, reduced fees and financial statement risk. There are still many details to sort out, but cryptocurrencies are here to stay, and so we endeavour to apply the same benefits to fiat currency issuance without sacrificing traditional monetary policy, enhanced due diligence, and other compliance controls. ■

Central banks move to the fore

'Many central banks have devoted considerable effort to examining the viability of introducing digital fiat currency as a complement to physical cash.'



Philip Middleton
Deputy Chairman of OMFIF

THE HIGH TIDE of speculative mania surrounding blockchain-based cryptocurrencies may now have receded somewhat, although new units seem to be issued daily, with so-called 'stable coins' being the latest addition. Some may have enduring value as investment assets, although guessing which these will be is tricky. Similarly, initial coin offerings continue to proliferate despite indications that few will ever profit from them. It appears, for now, highly improbable that any privately-created electronic currency will displace fiat money as a widespread means of payment and exchange.

Despite – or perhaps because of – dispelling this threat to their authority, many of the world's leading central banks have devoted considerable effort to examining the viability of introducing digital fiat currency as a complement or indeed a replacement for physical cash. Most have concluded that, although such an introduction could deliver benefits in both payments system efficiency and the exercise of monetary policy, now is not the time, for a variety of practical and policy reasons, to proceed with a retail central bank digital currency.

However, in the wholesale domain, the prospects for digital payment or electronic token exchange appear capable of delivering significant benefits while avoiding most of the difficulties inherent in retail CBDCs. OMFIF is delighted to work with IBM in examining the challenges, opportunities and possible routes forward. ■

The promise and peril of digital currencies

THE issue of central bank digital currencies has come to the fore over the last two years. Although a relatively new popular phenomenon, digital currencies have existed for decades. Virtual in-game currencies are commonplace, as are the use of fiat currencies to purchase them and secondary markets where people trade in-game items for fiat currencies.

Businesses and merchants began to offer redeemable virtual currencies in the 1980s. Customers used these for purchases and transfers to other consumers, or stored them as credits. In 1989, David Chaum created DigiCash – the world’s first digital currency that was anonymous and could prevent double spending. In 1994, the company put forward the first electronic cash transaction over the internet. Although DigiCash went bust, numerous digital cash and web-based money companies have arisen since then.

This sets a precedent for the growth of cryptocurrencies. Most digital currency companies failed because they relied on a centralised third party to handle transactions. In 2008, Satoshi Nakamoto’s white paper first presented the concept of Bitcoin, private cryptocurrencies and the underlying distributed ledger technology. Bitcoin was intended to facilitate the instant and anonymous transfer of wealth, through a decentralised means, operating peer-to-peer. But the currency suffered from significant price volatility as it garnered popularity.

Bitcoin is not a universally accepted means of payment, and so remains unqualified as a medium of exchange. The usability of a cryptocurrency diminishes as it becomes a speculative vehicle with volatile purchasing power. CBDCs denominated in an established currency could resolve this problem.

Discussions on CBDCs give central banks the opportunity

to examine the potential design of their future infrastructure. It is not necessary for central banks to rush to issue digital currencies to compete with cryptocurrencies. Rather, central banks, responsible for maintaining the stability of payments and settlements, must understand the possible impact of these technologies on their overall operations.

The marginal cost for central banks to issue such liabilities is low, since they can use the market’s underlying trust in them. And it may not be necessary to apply blockchain to these currencies, since central banks – as ledger keepers – are considered sufficiently trustworthy already.

Central banks initially questioned the motivation behind and possibility of issuing CBDCs, and there was little distinction between retail and wholesale variants. A retail CBDC would provide all individuals with access to a digital version of central bank fiat money, while wholesale CBDCs are limited to financial institutions for interbank settlements.

There are several policy concerns, mainly with regard to financial stability and the implications of widening access to central bank accounts. No major central bank intends to implement a retail CBDC in the near term. However, the debate about wholesale CBDCs has moved on from questions of feasibility to practical considerations. This report focuses on the aspects considered during the development of wholesale CBDCs, which are certain to be implemented in the future. The report therefore concentrates on the development of wholesale CBDCs – the specific variant of digital currencies that will be of most relevance for the central banking and regulatory community and all those who follow and do business with central banks worldwide. ■

THIS REPORT explains the purpose of wholesale central bank digital currencies, as well as the motivations and business case for central banks to adopt wholesale CBDCs. It also outlines key characteristics of such a system, including: who the developer and issuer should be; the technology options and requirements for a successful payments system; the practicality and regulatory challenges; and the possible risks and policy implications.

The report findings were informed by 21 central banks, which participated in OMFIF's survey between July-September 2018. Respondents came from institutions that are researching and trialling wholesale CBDCs (38%) as well as those that are not currently active in this field (62%). The report provides a holistic view of approaches to setting up a wholesale CBDC and offers guidance for institutions on how to tackle the many challenges in store.

Section 1

Defining CBDCs

A WHOLESALE central bank digital currency may lead to significant improvements in efficiency, speed and resilience, as well as lower the cost and complexity associated with existing payments systems.

The current system is susceptible to technical faults and errors. The layering of different technologies on top of the real-time gross settlement system adds to this complexity. A system based on distributed ledger technology can reduce the number of steps in the process.

Most survey respondents believe a wholesale CBDC should be issued by the central bank. This removes credit risk and ensures stability of the token's value. Liquidity risk is removed as the central bank can issue more tokens.

Of respondents, 50% believe a wholesale CBDC should be designed in partnership with the private sector. They argue it is necessary to engage stakeholders from the start, rather than impose new technology on participants.

A wholesale CBDC token can be part of an atomic transaction, which involves multiple simultaneous changes to the ledger across multiple assets. This enables the full and final settlement of money coupled with the movement of, or change to, the asset. This increases the utility of the payments system.

Central banks will increasingly prioritise system resilience, say 69% of respondents. Independently validating multiple-node consensus mechanisms, which are a feature of decentralised interbank payment systems, will prevent contagion spreading from a hack of a single central point. If a single node in a wholesale CBDC system is brought offline, the system can continue to function.

A decentralised system does not need the central operator to be online. If the participants are online, they can continue to send tokens peer-to-peer and settle central bank money in real time.

Central banks concluded that blockchain systems must improve before they can overcome issues of scalability and speed.

Section 2

Technology considerations

A WHOLESALE CBDC would have to preserve the existing capabilities of RTGS systems without significant degradation. The system must also preserve confidentiality of payment transactions, the ability to pay interest, monitor compliance against regulatory reserve requirements, change the composition of participants and run liquidity savings mechanisms.

Improving access to central bank settlement ledgers will involve multiple policy changes, including extension of operating hours, opening membership to new member types, better compliance standards for system interfaces, supporting multicurrency and non-cash asset settlement through external system links.

The traditional design of payment message flows, which requires the central bank's authorisation or 'signature', can be incorporated into DLT platforms such as Hyperledger Foundation's Fabric or Corda. Such message designs endorse 'correctness' of transactions. An alternative design can remove the central bank as the authoriser, but still allows it to receive transaction information for real-time audit purposes.

Transaction privacy can be achieved through a multiple channel approach and the use of private data collection systems.

Liquidity saving can be achieved through use of smart contracts and netting algorithms.

Central banks' experiments with wholesale CBDC DLT systems have produced mixed results, due to differing objectives and the tendency of researchers to focus on novel avenues instead of building fully-realised RTGS replacement systems.

The challenge that remains for the main vendors of wholesale CBDC systems is to construct a convincing RTGS replacement that can be properly benchmarked against existing systems and meet the high standards for security, robustness, efficiency and speed.

Section 3

Practicalities

CENTRAL BANKS addressed critical design and technological questions, including who will have management responsibility, what a possible design of a wholesale CBDC would look like, and how new systems will interoperate with legacy ones.

Survey respondents agreed that central banks should oversee the implementation of CBDCs, but were divided on the issue of storage. Almost half of respondents claimed servers should be stored with individual participants, while the remainder insisted they should be stored with central banks.

Central banks surveyed almost unanimously stated that any wholesale CBDC should be backed by digitised fiat currency trading at par. Respondents agreed that regulators would have to be granted a 'see all' node on the decentralised system.

Piecemeal adoption would be the preferable and most feasible option, according to respondents. However, this may raise concerns about interoperability between various systems, and prevent central banks from reaping the full network benefits of DLT-based systems.

Differences in consensus mechanisms may hamper the smooth functioning of DLT systems. Central banks must address this issue in future planning and research phases.

Respondents expressed concerns over cybersecurity, the nature of regulation in a DLT system and the difficulties facing international regulatory co-operation on this issue. Respondents highlighted the importance of rapid, thorough regulatory harmonisation.

Overall, respondents underscored that wholesale CBDC research and trials are still in their infancy, and that doubts remain over DLT's ability to deliver on its promise.

Section 4

Policy implications

THE BROAD regulatory and policy implications of a potential wholesale CBDC depend on design and management choices, such as whether it would be backed by a single sovereign currency or a basket of assets.

Based on survey responses, the likeliest outcome is a central bank-issued, fiat currency-backed digital token. This would have no significant monetary policy implications.

Financial stability concerns depend on the scale of the wholesale CBDC. According to central bank respondents, a wholesale CBDC would be designed simply as a digital reserve. This model would have limited repercussions on policy-making.

A wholesale CBDC could be expanded to serve as a digital global reserve asset along the lines of the International Monetary Fund's special drawing right. This would have profound geopolitical and regulatory implications.

Clearing houses and existing payments systems would have to either adapt to new, more efficient systems or find themselves disintermediated from payment and settlement processes in the long term.

The dissemination of disparate payment systems may have financial stability, geopolitical and welfare consequences. Researching and safeguarding against potential shocks in global payments systems should be a central bank priority.

Cybersecurity concerns dominated the survey responses. Central banks were concerned about compliance with existing system-wide resilience standards. Tests and proofs of concept run by central banks typically tested safety requirements and node failure scenarios, mostly with positive results.

Section 5

Case studies

OMFIF'S CASE studies span a range of projects. They include exploratory endeavours, such as the European Central Bank and Bank of Japan's Project Stella, as well as more developed undertakings, such as the Bank of Canada's Project Jasper.

The case studies span a range of objectives, including delivery v. payments trials and longer-term aims, such as the Monetary Authority of Singapore's goal of leveraging DLT to strengthen the country's position as a global financial centre.

The studies cover a range of technological choices, from platforms built on Linux's Hyperledger Fabric to Ethereum. Various capabilities such as smart contracts and liquidity saving mechanisms were examined.

Cases presented also discuss the next steps to be taken in developing DLT-based payment and settlement systems. One area of focus was overcoming the high costs and complexity associated with cross-border payments.

None of the central bank case studies examined included the possibility of radically overhauling their payments systems in the near future. Most are satisfied with existing RTGS platforms. ■

Transforming central bank payment systems

This section looks at the current payments landscape and the definition of central bank digital currencies, as well as central banks' motivations to develop a wholesale CBDC and where the potential benefits may lie.

Central banks play a crucial role in providing the trust that supports most forms of money in the economy. The different types of money in the system vary according to their purpose (settling interbank transactions v. purchasing goods and services), who has access (commercial banks or consumers), who the issuer is (central banks or commercial banks) and the technology that underpins their functionality.

Commercial bank deposits comprise the largest form of money by value in the economy. Consumers hold these balances as a means of settlement between each other, underpinned by confidence in money as a store of value and medium of exchange. Normally, balances held at commercial banks can be exchanged on demand for banknotes. This guarantees direct convertibility into a central bank liability, which builds more trust in the value of this money (bank deposits) – an important feature for a widely accepted medium of exchange.

Commercial banks would need to settle transactions between economic agents (individuals and businesses) by transferring balances between different accounts and between other banks. This creates a role for the central bank. Transactions between accounts that are not in the same commercial bank will need to be conducted through a third party, where the banks or their delegates have funds on the same ledger. Such a system could be operated by another commercial bank or a central bank, or indeed a non-bank. The frequency of settlement and the delay between the initiation of the settlement and the final step where the transfer is irrevocable is the difference between a real-time and a deferred system. Commercial bank reserves are the ultimate medium for settling payments between banks.

Commercial banks hold reserves at the central bank at levels specified by liquidity

coverage ratio regulations (the ratio of cash and high-quality liquid assets to deposits). These reserves are the common currency that is required to transfer balances between commercial banks. When money needs to be moved between two commercial banks, reserves move across the central bank balance sheet as one bank is credited while the other is debited.

Correspondent banking networks

Cross-border transactions add additional complexity. This reflects the requirements of correspondent banking networks, in which foreign banks must have an account with a bank in the country in which they are active. This requires institutions to reach consensus in routing payments, performing currency conversions, and deploying and managing liquidity in different jurisdictions, while operating under different regulatory constraints.

Payment networks are highly complex owing to the fragmentation of the financial industry. This makes it difficult for individual financial institutions to deal directly with all other banks globally.

When a bank receives a payment request from a client, it must find a corresponding bank that is willing to take the client's funds and terminate the payment locally at the receiving bank.

This requires the correspondent bank to have a nostro or vostro account with the receiving bank or another correspondent bank that has access to the receiving bank, all while having enough prefunded liquidity to complete the payment on the client's behalf.

The vostro account is held in the currency of the country where money is on deposit. A nostro account is the record of the bank whose money is at another bank. The latter are often used to simplify trade and foreign exchange transactions.

Cross-border messaging systems

These cross-border transactions require a sophisticated messaging service. The network provided by the Society for Worldwide Interbank Financial Telecommunication allows banks to send electronic messages securely between themselves. This enables one bank to instruct another bank to credit the account of one of its customers, debiting the account held by the sender institution with the credited bank. Swift offers only the instructions, but the movement of value still requires debiting and crediting several accounts of each institution while relying on banks maintaining accounts with each other, either directly or through intermediaries. This makes the service complex, exposed to various financial risks and relatively costly.

Liquidity can become tied up in correspondent banks as they need to hold significant balances with each other for this payment method to function. There is therefore a large opportunity cost, as this is money that could have been lent or invested.

Deferred net settlement

The use of deferred net settlement systems, such as Bacs in the UK, can help lower the liquidity required through netting and setting. While this lowers liquidity constraints, it adds an additional central clearing party to the system that collects payment messages and calculates the net amount that needs to be transferred. This adds complexity and can protract settlement times.

All parties involved have different ledgers, and the coordination between these parties is slow and prone to error, often relying on manual interventions from back-office teams. Additionally, someone needs to perform a currency conversion at either end, and different parties need to manage liquidity levels in nostro/vostro accounts.

It is not always clear under the deferred net

settlement system when settlement finality has taken place. There is a delay between the time a payment instruction is issued and when the receiving bank obtains the net settlement value. The receiving bank must wait until it has received the netted settlement amount before it can credit the funds to its customer, as there is the risk of the paying bank failing in the interim (Herstatt risk).

Real-time gross settlement

The real-time gross settlement system removes the counterparty risk and the finality issue in domestic payments. The system works with the central bank to facilitate the real-time movement of funds between accounts held by commercial banks at the central bank. The UK’s system is Chaps, the US uses Fedwire and the euro area has Target-2. Under these systems, money moves almost instantly to credit and debit banks’ central bank accounts, with multilateral netting and with finality. Additional liquidity savings mechanisms are included, which prevents issues such as payment gridlock.

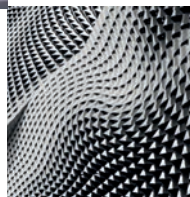
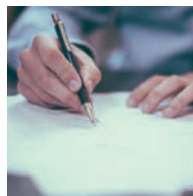
Continuous linked settlement system

Continuous linked settlement, a cross-border payment v. payment system that operates for the settlement of foreign exchange transactions, can reduce the credit risk associated with correspondent banking. CLS links together the settlement of all currency pairs by batch-processing these transactions within a set time period. To settle trades, each account is debited and credited on the book of the CLS with the use of Swift messaging.

Additionally, the operational time of CLS is limited to the time during which all involved RTGS systems are open, meaning that time zones and geography affect the speed of settlement. The longer a foreign exchange transaction takes (typically there is a two-day >>

‘One of the reasons for the interest in DLT is that many central bank-operated wholesale payment systems are at the end of their technological life cycles. The systems are programmed in obsolete languages or use database designs that are no longer fit for purpose and are costly to maintain.’

Bank for International Settlements



The number of days a foreign exchange transaction typically takes to be settled

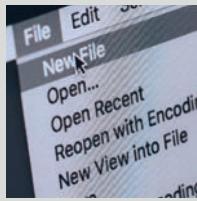


Percentage of survey respondents who believe that central banks should design a wholesale CBDC in partnership with the private sector



1

A hack at Bangladesh Bank in February 2016 through fraudulent Swift messages removed almost \$1bn in central bank money



‘It is important for the central bank to drive efforts where one of its key roles, such as being the operator of large-value payment systems, may be affected. Payment systems are networked ecosystems, and collaboration with industry will help ensure learning, understanding, buy-in across the board and potential unintended consequences are reviewed.’

South African Reserve Bank

settlement period), the greater the Herstatt risk. CLS is also permission-based, with restrictions on which members can join and which currencies can be settled.

Aspects of CBDCs

Central bank digital currencies can be divided into two forms based on who has access to them. A retail CBDC is a digital version of central bank fiat currency that is universally available, which entails public access to central bank liabilities, as it partially replaces banknotes. In the case of a wholesale CBDC, the accessibility to this form of money is limited to commercial banks and clearing houses that make up the interbank market. Wholesale CBDCs would replace reserves held at the central bank, and in other cases liabilities of private entities if the issuer is not a central bank.

The Bank for International Settlements taxonomised the forms of money available through its money flower diagram. It is categorised by who the issuer is (central bank liabilities or others' liability), what form it takes (digital or physical), how accessible it is (widely or restricted) and which technology it is based upon (token- or account-based).

Traditionally, the forms of money issued by central banks, commercial banks and private issuers have been account-based, meaning that balances are recorded on a ledger. Under this system, debiting and crediting of accounts occurs without transferring actual values.

A wholesale CBDC replaces the money currently used to settle interbank transactions (reserves held by banks at the central bank) with a digital token. Such a token would be a bearer asset, meaning transactions between accounts would transfer value from the sender to the receiver. The asset can be recorded on a distributed ledger. This requires consensus on changes in asset ownership by nodes (or participants), creating a decentralised system.

Currently, central bank reserves can be accessed only during the central bank's operating hours. A wholesale CBDC is more flexible and can operate at all times or within specified hours. It may also be possible to set up secondary markets for token-based interbank currencies that can operate outside central bank hours. This could enable the loaning/transfer of liquidity between bank and

non-bank institutions to alleviate liquidity pressures built up in the system as well as reduce counterparty risk associated with long settlement times.

A tokenised solution can create a degree of anonymity for the user institution. This depends on the transfer mechanism and whether it is centralised or decentralised. A centralised system will require an intermediary, such as the central bank. A decentralised solution facilitates peer-to-peer transfers, creating an option for total anonymity between institutions.

A wholesale CBDC can be interest-bearing, in the same way that central banks can use deposit and base rates to affect interbank activities. Additionally, smart contracts – self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code that exist across a distributed, decentralised blockchain network – can increase the functionality and simplicity of processes, given that mutual agreements and the code for execution of multiple tasks are self-contained in the blockchain. This increases the utility of this form of money.

Who the issuer should be

Most participants in the OMFIF survey believe that a wholesale CBDC should be issued by the central bank and denominated in the domestic sovereign currency, with which it holds a 1:1 parity in value. It must also be fully backed by the central bank's reserves.

Market risk can be significant for a tokenised asset owing to its vulnerability to steep fluctuations in value. This has been a problem for Bitcoin, and could present similar difficulties for tokens issued and backed by a commercial bank. If holders and users of the token do not trust or believe in the commercial bank's ability to hold the token's value, then parity will break down, exposing the token to high credit risk.

Despite the possibility of some central banks defaulting on their obligations – such as in the euro area, where national central banks could technically default on their Target-2 balances – a central bank is considered to be the most creditworthy institution in a country's financial system.

A central bank-issued wholesale CBDC

'Cross-border payments are widely regarded as an area in which significant efficiency gains exist. Current processes are slow and costly, involving significant compliance burden and a number of different financial institutions in different jurisdictions. New technologies and new business models could be used to address some of these frictions.'

Michelle Bullock, Reserve Bank of Australia

would remove the credit risk and provide stability in the token's value. This is crucial for a wholesale CBDC to act as a medium of exchange and store of value. Liquidity risk is removed, as the central bank can issue new tokens through traditional means of purchasing securities to increase the money supply. In some countries, such as the US, the central bank has no need to default if it is willing to print more money.

However, the private sector should still play an important role in the development of a wholesale CBDC. Almost 50% of respondents to OMFIF's survey believe that central banks should design a wholesale CBDC in partnership with the private sector with a technology provider, or with a consortium of commercial banks and a technology provider.

Developing a new payments system in co-operation with private sector users will ensure that it meets user needs. It will be necessary to engage stakeholders from the start, instead of imposing new technology on participants that may not take account of their needs.

There must be a clear distinction between a wholesale CBDC and a private digital asset used for interbank transactions. According to the BIS and its Committee on Payments and Market Infrastructures, only digital money issued by a central bank – with or without the support of a technology provider – can be called a 'central bank digital currency'.

All other variants by this definition are not a CBDC, despite their overlapping role in payments and settlements between banks. These assets may be private digital money, tokens or settlement assets. If they do not

have an identifiable and legitimate issuer and are not denominated in a sovereign currency, they should be classified as crypto-assets.

Motivations for wholesale CBDCs

The main motivations for pursuing a wholesale CBDC, according to survey respondents, lie in the potential to improve speed and cost efficiency. It may also help to overcome the limitations of existing systems, especially in system security and resilience.

Over the years, inefficiencies in the RTGS system have improved, as highlighted by survey respondents. However, it remains susceptible to technical faults, and there are complications in how certain trades are verified and settled.

One respondent explained the system remains prone to errors. Back-room manual interventions are frequently needed to correct these. In addition, the layering of different technologies on top of the RTGS, intended to make it more resilient, adds to the system's complexity. This is where a wholesale CBDC could fit in. A system based on distributed ledger technology, enabled with smart contracts trading a tokenised bearer asset, can reduce the number of steps in the overall process.

A wholesale CBDC can reduce operational risks and running costs due to productivity gains as more financial assets become tokenised and recorded on distributed ledgers. The movement of financial assets typically occurs in exchange for money, where the movement of the asset and the movement of money need to be reconciled by both >>

parties on two different ledgers (the asset ledger and the money ledger). This introduces reconciliation and operational risk. A wholesale CBDC denominated in fiat currency, issued by the least risky entity and recorded as a token on a blockchain, can reduce these risks.

One limitation with today's RTGS systems is that they only record cash, but most business transactions involve the movement of both cash and assets. DLT platforms permit the recording of transactions of any asset – money, equities, bonds, over-the-counter derivatives – as well as cash, allowing multiple, simultaneous changes to the ledger.

The freeing of central bank-backed liabilities from the RTGS would provide a token that may have more utility than the same liability trapped within the RTGS. The token can be part of an atomic transaction – which involves multiple simultaneous changes to the ledger across multiple assets. This would enable the full and final settlement of money coupled with the movement of, or change to, the asset.

This would mean that the concept of delivery v. payment – where one asset changes hands only if the other asset changes hands – can be achieved simultaneously, with no ambiguity as to which leg occurred first. This extends to invoices and payments. Two parties can know the status of an invoice at any time, and the payment can settle at the exact moment the invoice is marked as paid, with both parties noting this change of status. This could mean that transactions recorded on DLT could be cheaper in aggregate than transactions recorded across multiple siloed accounts.

Making systems more resilient has also motivated central banks' wholesale CBDC investigations. Outages of the RTGS system do occur, with many incidents left unreported. The Bank of England suffered a major outage in October 2014, while a hack at Bangladesh Bank in February 2016 through fraudulent Swift messages removed almost \$1bn in central bank money. System resiliency has become an increasing priority for central banks, as noted by 69% of respondents.

RTGS remains vulnerable to single points of failure given its centralised nature. A cyber attack or system failure would mean that participants are unable to transact central bank money. Independently validating multiple-node consensus mechanisms, which are part of a decentralised interbank payment system, will prevent disaster spreading from a hack on a single central point. If a single node is brought offline, the system can continue to function.

Complementing RTGS with a decentralised interbank payment system based on blockchain would not involve directly replacing the system. Instead, both can be run in parallel over the medium term, with the possibility of a permanent switch in the long term. Coexistence of the systems would also allow for disaster recovery if one goes offline.

Respondents highlighted the system's ability to operate during out-of-office hours as a key benefit. A decentralised system does not need the central operator to be online; if the participants are online, they can continue to send tokens peer-to-peer and settle central bank money in real time. In the current process, parties use a collateralised deferred net

settlement system while the primary system is closed, then make the final net settlements when the RTGS reopens.

Respondents emphasised high costs, inefficiencies, long settlement times and poor availability of information as significant drawbacks to the current cross-border processes. One central bank respondent said the adoption of a common messaging format will enable central bank systems to be better interlinked, which may mitigate some of the issues. Other central bank respondents see potential for a global settlement system that would enhance the efficiency of cross-border payments, but state that a wholesale CBDC may not be the preferred solution.

So far, central bank trials of wholesale CBDCs have focused on domestic interbank payments. However, central banks such as the Monetary Authority of Singapore and the Bank of Canada are considering cross-border payments in the next phases of their wholesale CBDC projects.

Business case for wholesale CBDCs

Central bank respondents said a sound business case is necessary for the implementation of a wholesale CBDC. This means the benefits of employing a wholesale CBDC must exceed its cost in the long run, and must be significantly better than current systems. Of institutions surveyed, 38% are researching or trialling a wholesale CBDC to inform the next upgrades to their RTGS system.

For smaller central banks, the cost of exploring a wholesale CBDC may be too high. Many are adopting a wait-and-see strategy, which leaves larger central banks to take the lead on experiments. The results of such trials will be of use to all central banks.

Of respondents not considering a wholesale CBDC, the majority state the current technology may not be mature enough to serve as core infrastructure. Early trials by some central banks do not suggest that a settlement solution based on a digital currency would be clearly superior to current systems.

61% of central banks said a blockchain may not be necessary as they have observed

'It is about resource allocation. For a smaller central bank, it is sometimes better to follow up the developments and react in due time. Today, it is still somewhat unclear which problems wholesale CBDCs could solve.'

Bank of Finland

few efficiency gains during trials, given that the technology is still in early stages of development. Central banks such as the Bank of England believe DLT holds promise, but at this stage the Bank concludes that the technology is not sufficiently mature to be the core of next-generation RTGS systems.

In other cases, such as Phase II of the MAS's Project Ubin and the South African Reserve Bank's Project Kokha, variations of DLT overcame initial challenges. The MAS found that the key functions of an RTGS system, such as fund transfer, queueing mechanisms and gridlock resolution, could be achieved through different techniques and designs.

Sarb found that the typical daily volume of the South African payments system could be processed in less than two hours with full confidentiality of transactions and settlement finality. Additionally, it was able to view the details of all the transactions, greatly improving regulatory oversight. Nonetheless, Sarb concluded that the main lesson at this stage is that the comparative safety and efficiency benefit of DLT remains unresolved.

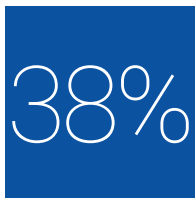
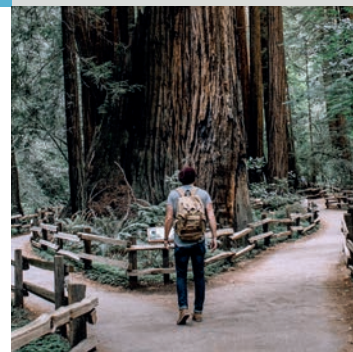
Central banks concluded that blockchain systems must improve before they can overcome issues of scalability and speed. There is a trade-off – a decentralised system can slow down transaction speeds as it must remain in consensus with other systems. □

'The high cost of the inherent consensus-building mechanism can make DLT uncompetitive for wholesale payments.'

Deutsche Bundesbank



Percentage of survey respondents who find significant issues with the current cross-border processes



Percentage of institutions surveyed that are researching or trialling a wholesale CBDC to best inform the next upgrade to their RTGS system



DLT reconfigures wholesale payments

This section focuses on the technical aspects of building a central bank digital currency system for wholesale transactions. It references the capabilities of existing wholesale payments systems and the probable capabilities desired for the next generation of systems that will use CBDCs.

Many central banks operate real-time gross settlement systems that provide users with a means to transact with each other using movements of funds across central bank reserve accounts.

The role of central banks would change if procedural logic associated with a shared ledger could be trusted to enforce logical consistency in transactions. This could be implemented through smart contracts or other means employing distributed ledger technology. This procedural logic would automatically and transparently prevent the sorts of collusion that would cause damaging side effects, such as increases in the money supply. Instead of operating the system directly and endorsing each transaction, central banks would simply be responsible for codifying the basic tenets of the wholesale payments service as smart contracts that would be run in a deterministic fashion by all parties. Such behaviour means the outcome of running the contract can be completely predicted before running the programmes.

The challenge of this model is that the central bank and all participants must be convinced the technology that runs this system is inviolable and absolutely correct under all circumstances. This would mean there is no opportunity for any form of

malicious behaviour to upset the logic of the system once set in place. This requires trust in the hardware, network, DLT and application layers.

This section focuses on the technical aspects of building a central bank digital currency system for wholesale transactions. It references the capabilities of existing wholesale payments systems and the probable capabilities desired for the next generation of systems that will use CBDCs.

Scope and goals

First, the scope of what a 'wholesale' system must be considered, a definition that would be guided in turn by decisions about the set of stakeholders. For instance, much attention from central banks around wholesale CBDCs has focused on RTGS systems where the central bank is a direct participant. However, these need not be the only type of wholesale CBDC systems. UBS's Utility Settlement Coin, which involves digital cash instruments backed by funds held off the balance sheets of the commercial banks, requires only the indirect participation of the central bank as the ultimate custodian of the funds.

Second, we should consider the goals of the new system's design. These goals may be derived from regulations, central banks' stated

policy intent, and the commercial or business requirements of the system's users.

The first goal for such wholesale CBDC systems would be to preserve the existing capabilities of RTGS systems without significant degradation. Users of the system must have absolute confidence that its results are final once confirmation is sent. The system must ensure the confidentiality of payment transactions is preserved, as well as the ability to pay interest, monitor compliance against regulatory reserve requirements, change the composition of participants (for example to exclude certain parties or add new ones), and run liquidity saving mechanisms.

The second goal would be to introduce 'next generation' capabilities to RTGS systems, as has been investigated by the Bank of England, European Central Bank and other monetary authorities. These capabilities include improved resilience, availability, scalability, accessibility and efficiency.

Minimising incidents of disruption (what some have called 'zero incident' operation) is an important feature given that the RTGS systems are critical to central banks' mandate of maintaining monetary and financial stability. Reducing incidents requires resilient design and would improve the availability metrics.

Improving access to central bank settlement ledgers will involve multiple policy changes, including extending office hours, opening membership to new member types, better standards compliance for system interfaces, multicurrency and support for non-cash asset settlement through external system links. The impact of these policy changes must be seen in totality. For example, extending system hours will potentially double settlement capacity, as office hours cover less than 12 hours per day. This additional capacity would allow the wholesale CBDC system to support non-traditional participants without expanding the processing capacity of the system by

'Ensuring confidentiality in a DLT implementation is still a challenge and constitutes an important research question. Moreover, financial markets are subject to regulatory oversight and so permission-less structures could pose a challenge, given their potential opacity.'

Bank of England

spreading the transaction load over time.

Scope of central bank involvement

In traditional, centralised RTGS systems, the central bank participates directly in every message flow, sitting in the middle of each transaction. In many jurisdictions, the irrevocable status of a transaction settled on an RTGS is protected by statute. There is therefore an expectation that the system helps to enforce the correctness of transactions. Figure 1 illustrates the most common models used to enforce correctness – the V-shaped and Y-shaped architectures.

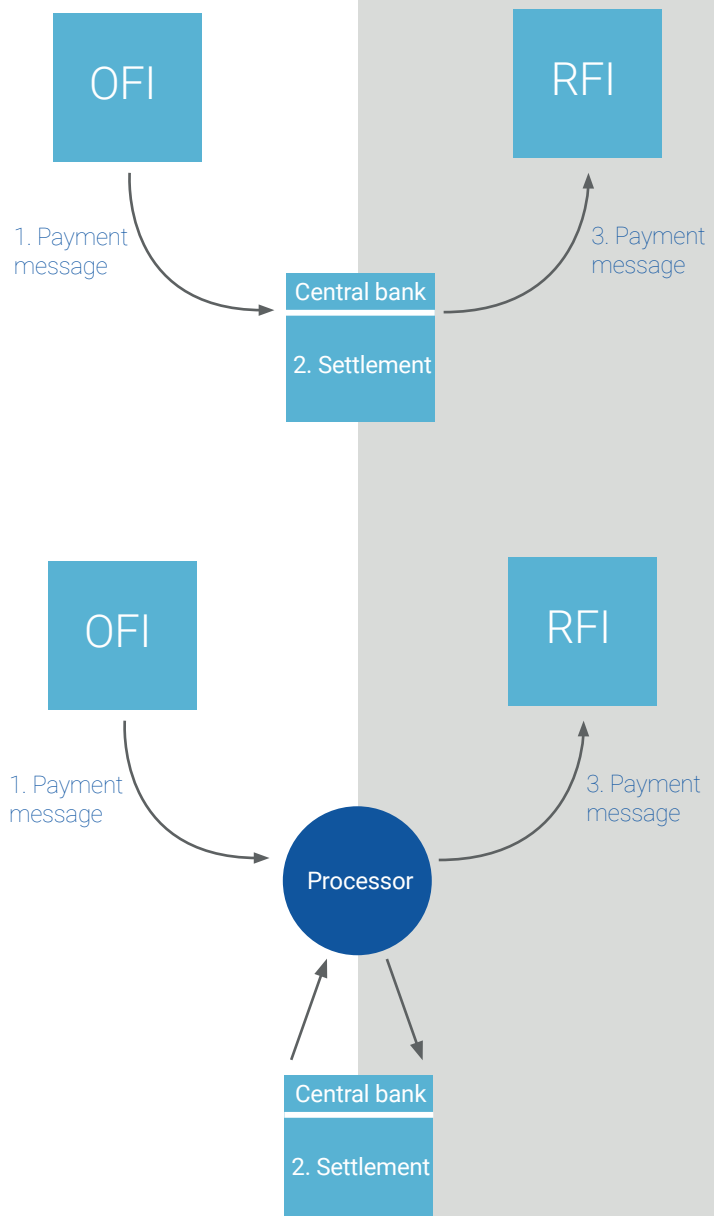
In the V-shaped message flow, the originating financial institution sends payment instructions to the central bank, which clears and settles it before sending it to the receiving financial institution. In the second, Y-shaped message flow, there is another utility that sits between the central bank and the financial institutions. The utility would copy certain important fields or the entire message, and send it to the central bank, which has the right to authorise the final delivery of the message to the receiving institution or to block it.

Mapping the Y- or V-shaped models

In both the Y- and V-shaped models, central bank validation (in the form of a signature) is required before transactions can be settled. This fits into DLTs such as the Hyperledger Foundation's Fabric or Corda's model, where one can define the endorsement policy or Corda contract to require the central bank's signature, as well as the signatures of the originating and receiving financial institutions to attest to this transaction's validity.

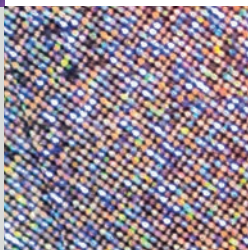
Alternatively, an entirely different paradigm may be developed – where the central bank merely receives a copy of the transaction information, and there is no authorisation step. This mechanism, also known as the T-shaped message flow, allows for the central bank still to audit the correctness of transactions and reduces

Figure 1: 'V-shaped' v. 'Y-shaped' the shape of message flows



System resiliency has become an increasing priority for central banks, as noted by 69% of respondents.

69%



the settlement time required. If the central bank detects an invalid or undesirable transaction, it would be able to step in and invalidate the transaction by notifying the originating and receiving institutions.

Examples of invalid transactions might be where the originating and receiving institutions collude to allow for the sending of more money than is held in the former's balance. This would effectively increase the potential money supply through the implicit creation of new central bank money and violates the principle of gross settlement. Even if the central bank were to detect and invalidate the transaction, the underlying economic transfer of goods and services that are being paid for by the monetary transfer would also have to be reversed. Therefore, this structure is seen as being incompatible with the basis of an RTGS system, where the users require certainty that the transaction is settled irrevocably on central bank money.

Mapping the T-shaped model

In the same way as supporting the V- or Y-shaped models, the channel and private data collection features can also be leveraged to support the T-shaped model in a DLT. The only differentiation comes from choices about whether the central bank's attestation of validity in the form of a signature is needed for final settlement.

As illustrated in Figure 2, the central bank plays the role of auditor in a T-shaped model rather than endorser as in the V- or Y-shaped models. Therefore, the central bank's signature is not needed to validate a payment between originating and receiving institutions. In this case, both the payment instruction and settlement transaction will be performed in a distributed manner and the transaction validation will be done only based on the self-endorsement of the transaction initiator – which provides scant comfort to the central bank.

The disadvantage of this model is that correctness cannot be guaranteed in real time, since the central bank does not endorse or validate the payment process. However, all transaction histories, including sensitive data (payment volume, account balance) and their cryptographic stamps, will be recorded in the private data collection and public

ledger, respectively. Therefore, any invalid or undesirable operation by commercial banks (intentional or not) will leave evidence in the ledger so long as the transaction is committed. This allows the central bank to monitor and audit transactions in real time, and step in immediately when exceptions are detected. The auditing and reaction can be completely automated, with the reaction being customised to exceptions of varying degrees of severity. Moreover, online data analytics and proactive strategies can be applied to further reduce risk in the payments system.

Transaction privacy in wholesale CBDCs

Transaction privacy is not a prerequisite for a successful payments system, given the wide adoption of Venmo, a US mobile payments service which also publishes users' transactions to the public. However, large wholesale payments would probably need a higher level of data protection than typically smaller retail payments. Financial institutions that make use of RTGS systems may not

wish to reveal a weak liquidity position to competitors, as this may raise their cost of funds. Likewise, trading institutions may not wish for competitors to monitor their payments patterns. This could reveal information about their securities purchases and, in turn, allow competitors to exploit one another's portfolio positions.

To meet the privacy requirements, one could separate each pair of transacting parties and the central bank into an isolated subnetwork, called 'channels'. These can share the same transaction logic linked to channel-specific validation policies. Instead of duplicating the logic, new channels would be created as new participants are added. This means the transaction logic can be upgraded or modified all at once across every channel using that code.

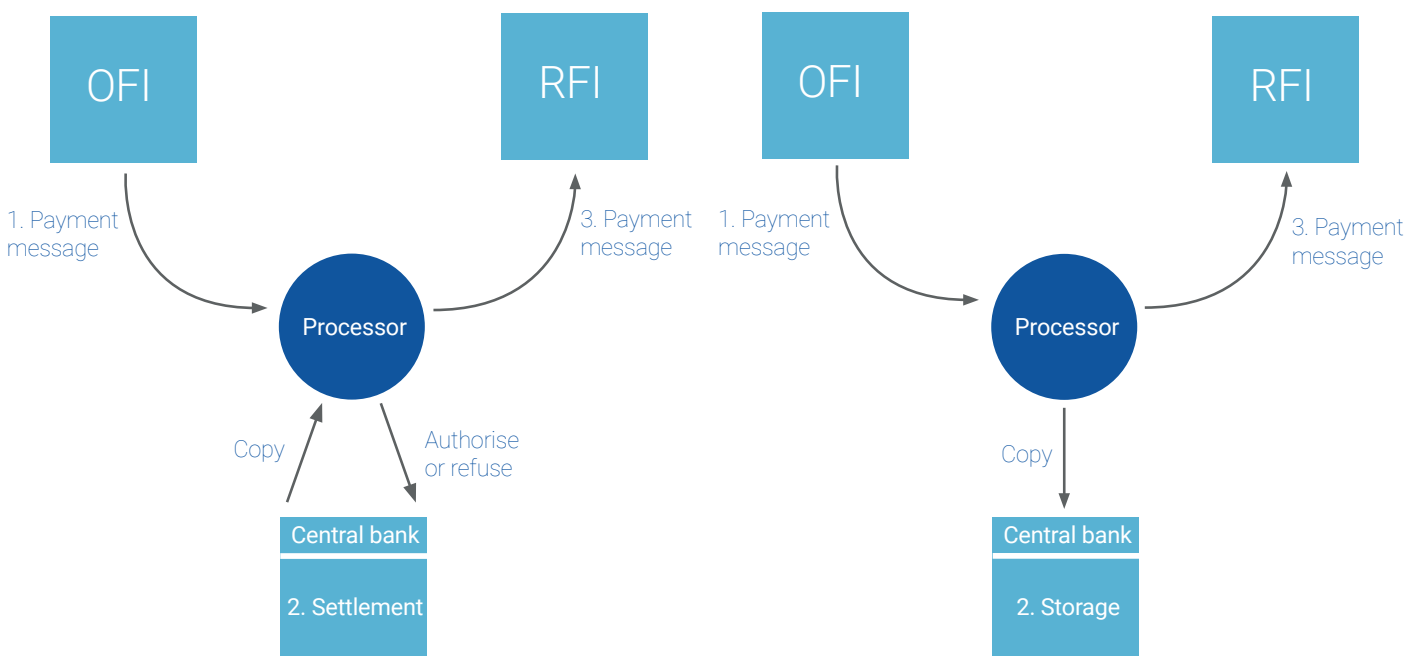
However, the number of channels still grows at a non-constant rate, which makes the system's scalability dependent on the overhead required for maintaining each channel. This design paradigm (while allowing for good privacy guarantees) when taken to the extreme

is similar to point-to-point propagation of data. This puts the onus of providing system redundancy and resilience on each individual party, which raises questions about the value of DLT.

Another design would use private data collections to maintain the bilateral payment relationship between each pair of originating and receiving institutions, as well as the bilateral account relationship between each commercial bank and the central bank. Such data collections provide detailed control of private data propagation in a need-to-know manner.

All data in each specific collection will be treated as sensitive information and will be broadcast and committed only to a dedicated local ledger of stakeholders. For example, the volume of payments will be recorded only in the local ledger of the originating and receiving institutions instead of the public blockchain, and thus will be available solely for the originating and receiving institutions to read and write. Constellations in platforms such as Quorum, Side-DB in Hyperledger Fabric and

Figure 2: Y-shaped v. T-shaped message flows



Corda all support this paradigm.

The use of private data collections provides lightweight data propagation control with more flexibility than in the case of systems that rely on multiple channels. The overhead to maintain a collection is much lower than that for maintaining a channel, which requires dedicated infrastructure. Private data collections offer better system scalability than multiple channel designs, although the volume of collections still grows quadratically as the network scales.

Liquidity saving mechanisms

Most DLT systems treat the distributed ledger as a log of settlement messages. However, it is also possible to allow transacting parties to send payment messages to one another through the DLT. Using both payment and settlement messages opens opportunities to introduce liquidity saving mechanisms.

Smart contracts will process correctly-formed settlement messages as long as there is sufficient liquidity and will also queue payment messages. Transacting parties can attach priority labels such as 'urgent', 'high' or 'normal' to these payment messages, and amend these labels for submitted messages where necessary. It is also possible for a transacting party to cancel a payment message to stop it from being settled.

Privacy-preserving netting

Popular netting algorithms preserve fairness among transacting parties while arriving at a nettable set of payments that can be settled while respecting priority. It is possible to decentralise these netting algorithms in the context of a DLT, so that the transacting nodes

communicate with each other to arrive at a nettable set of payments so that the liquidity constraints are not violated.

Cryptographic techniques may be used to encode payment messages so that payment amounts are not publicly known. However, a validator node may still parse a list of payment messages and arrive at the subset of nettable messages without violating liquidity constraints. These techniques have been termed 'zero-knowledge netting', and their performance has improved to a point where widespread use in RTGS systems is practical.

The practical application of privacy-preserving netting is a critical milestone for DLTs as they become competitive with traditional centralised RTGS systems, while still benefiting from heightened resilience and availability.

Experimental results

Most of the wholesale CBDC DLT experiments conducted by central banks have produced mixed results in meeting the above goals. This is partly because of the differing objectives of each experiment, and the tendency for researchers to focus narrowly on novel avenues of research instead of building fully-realised RTGS replacement systems – therefore not allowing for comprehensive comparisons to be made.

Most of the systems tested do not support the payment of interest on balances. This is not the result of a technical limitation, but rather reflects the complexity of identifying the appropriate policy rule for deciding on the balance for which interest should be computed. Moreover, the experimental systems have not been fully tested for security vulnerabilities.

In many of the investigations before 2017, data and transaction privacy were not a consideration. This is because there were fewer technologies available to support a privacy overlay on the distributed ledger, and because the major benchmarks were based on Bitcoin or Ethereum, which at the time did not support private transactions.

There is equivocal evidence on the issue of resilience. Decentralised arrangements for the validation and processing of transactions using DLTs reduce the impact of the failure of any single party in the network of parties that process each transaction. However, the architecture of DLT-based RTGS systems may still present single points of failure. For example, both phases of the Bank of Canada's Project Jasper included centralised components such as the private key, identity and system access management systems. Later, the project included the presence of notary and supervisory nodes that required high availability redundancy to ensure business continuity.

Similarly, the results of Project Khokha by the South African Reserve Bank point to the need for 'coordinated end-to-end procedures' and 'sufficient disaster recovery procedure facilities' to run any RTGS system, DLT-based or not.

Enthusiasm for smart contracts

A wholesale CBDC has the potential to bring significant improvements in efficiency, speed and resilience of payments, as well as make the current interbank payments system less complex and costly. By removing the simple messaging methods that are core to legacy systems, distributed ledger technology and smart contracts can bring new features that current systems do not possess or which require multiple steps to achieve.

Central banks surveyed by OMFIF expressed a wide range of demands from a potential wholesale CBDC or DLT-backed payments system. Most importantly, on the technology side, most said there are no immediate advantages to adopting blockchain-based systems over existing platforms.

Yet, when it comes to broader DLT-based systems, central banks have a variety of needs. All respondents show enthusiasm for smart contracts. These would grant central banks flexibility in determining variables in

'Global payments would benefit from development, however... we should concentrate on solving problems, not finding opportunities to implement a technology.'

Bank of Finland

their payment and settlement, including what form the token would take and what it would be backed by. The logic, characteristics and behaviour of the smart contract would remain mutable.

Respondents also voice a desire to develop DLT-based liquidity management facilities, which would enable bilateral transaction netting. This would potentially facilitate greater transactional flow volumes and reduce the need for prefunded buffer accounts, as was explored in the Bank of Canada's Project Jasper. These two related features were the only ones widely tested. Among major central banks examined in our survey, only the European Central Bank and Bank of Japan's Project Stella worked with hash- and time-lock capabilities, which would allow atomic swaps of value to take place across business networks.

Similarly, there was little analysis of different consensus mechanisms, as just one major central bank confirmed it had been working only with restricted and centralised consensus among the host of options. Enabling support for different consensus mechanisms would alleviate interoperability concerns and increase the robustness of any DLT system.

This is crucial for central banks, given their mandate to preserve financial stability. Only one major central bank claimed it had examined the possibility of offline transactions. Finally, central banks stated they had worked with a broad range of technology providers, including Hyperledger and Corda, indicating no clear preference for any particular option.

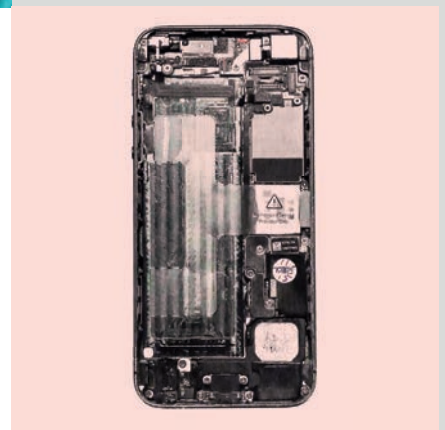
Optimistic outlook

Despite the rapid progress being made to bring wholesale CBDC systems in line with central banks' requirements for their next-generation RTGS systems, the former still fall short of expectations.

However, each iteration of these experiments continues to elaborate successfully on previous work, with most central banks maintaining an optimistic outlook that a workable DLT-based substitute for real-time wholesale payments will arise. Arguably, the challenge that remains for the main vendors of wholesale CBDC systems is to construct a convincing RTGS replacement that can be properly benchmarked against existing systems and meets high standards for security, robustness, efficiency and speed. □

61%

61% of central banks said a blockchain may not be necessary as they have observed few efficiency gains during trials, given that the technology is still in early stages of development.



Making CBDC technology work

This section examines the practicalities that central banks must consider in setting up a wholesale central bank digital currency, focusing on four primary themes: responsibility for management; design; legal and regulatory issues; and system interoperability.

Potential issuers of wholesale central bank digital currencies must consider who will oversee implementation, including costs and stakeholder management. Control may be left with the central bank or disseminated among network participants. Due to the nature of the service – an upgrade to real-time gross settlement – leaving management decisions to the central bank is preferable. For the central bank, this would entail running the infrastructure and bearing the cost of any distributed ledger technology.

All of our respondents stated that the central bank should own, manage and operate any wholesale CBDC system, as well as play the role of settlement agent. However, individual nodes on the network could be managed by participants. On the question of where host servers should be stored, almost half of respondents note that infrastructure is distributed and therefore should be hosted by individual participants, while the remainder of respondents suggest the central bank should host the servers.

Debates over access to the wholesale CBDC typically conclude that the central bank should determine the list of eligible participants. It would also be possible to vary the group of eligible participants over the lifetime of the system. Some platforms, such as Corda, permit this. It is assumed that existing members of the RTGS system will have access to the new payments system. Of those polled, 53% said the central bank would be ‘in the driver’s seat’ on determining access, while the remaining 47% believe the question cannot yet be answered owing to a lack of information and research. One of these latter respondents suggested these questions could only be resolved later ‘at the implementation phase’.

There is a debate over what the reference asset or backing for a digital currency should be, and what the relationship between this asset and the wholesale CBDC would look like.

The wholesale CBDC could be central bank-issued and serve as base money, as a digital depository receipt for reserves, or it could be issued entirely by a private sector entity. Each option has different implications for monetary policy and risk. For instance, if wholesale CBDCs are reserve-backed, then there is no potential for arbitrage in their value compared with the fiat currencies against which they are backed. All except one central bank noted that sovereign currency, in digitised form and trading at par, should back the wholesale CBDC. As one respondent said, any CBDC ‘would be exactly the same sovereign currency distributed on a different medium’.

The outlier respondent suggests the reference asset should be a basket of assets, which would better mitigate risk than a single asset by preventing excessive speculation. Establishing clarity on whether the wholesale CBDC is backed by the fiat currency, a basket of assets or another system will depend on central bank and financial stability needs.

Exploring regulatory concerns

Regulatory and legal questions have cast a long shadow over CBDCs. As the US Commodity Futures Trading Commission suggested in a white paper on distributed ledgers, DLT in trading and payments may allow financial institutions to ‘transcend the fragmented regulatory structure’. Our respondents disagreed, arguing the current system is easier to oversee and manage. Almost 76% of respondents explicitly state that it is uncertain whether DLT will be able to deliver on its promise, especially in areas such as regulation. Furthermore, regarding the question of ‘who has access to information’ on a permission-based ledger, all respondents suggested that strict privacy regulations should be in place, and that participants such as commercial banks should only be able to view their own details and transactions.

Similarly, all participants say that regulators and overseers should have a node on the system that allows them to ‘see everything’ deemed necessary by domestic legislation.

Despite this, there appears to be a lack of research by central banks on how regulation of DLT payments might work. The only legal framework mentioned explicitly was the Principles for Financial Market Infrastructures, to which some respondents say any wholesale CBDC would have to adhere. The Bank for International Settlements has identified potential risks stemming from the adoption of digital currencies that conflict with the PFMI.

Stipulations in the PFMI insist, for example, that ‘an FMI should provide clear and certain final settlement’ (principle eight on settlement risk) and that all financial market participants must be subjected to regular and rigorous stress testing (principle three on risk management).

Wholesale CBDCs will have to abide by the internationally agreed PFMI. Beyond discussion of the Principles, however, few respondents commented on regulatory interaction with wholesale CBDCs. Central banks should be aware of the legal implications of digital currencies, and should make regulatory co-operation crucial to their work.

Interoperability is crucial

Central banks must address questions of interoperability that arise from CBDCs, on both the regulatory and the technological level. Regulation across borders is not standardised, raising the possibility of arbitrage if some jurisdictions are more technology- or DLT-friendly than others. Furthermore, if central bank design relaxes permissions such that participants outside a country’s or network’s jurisdiction can participate in a DLT platform, this raises the more pressing concern that DLT networks could be used to circumvent capital controls. Nodes outside a network’s jurisdiction

would leave the possibility of arbitrage based on a country's exchange restrictions, such as those still in place in Indonesia. These arbitrage, interoperability and harmonisation issues should urgently be addressed by central banks.

One respondent said that a 'full set of new initiatives' on standardisation and harmonisation is a necessary precondition for their central bank conducting further research. Central banks' next steps must include examining how different DLT frameworks will interact – both with legacy systems and with one another. This involves several questions.

First, interoperability depends on the underlying technology. Respondents indicated that research has not yet progressed sufficiently to allow such nuances to be considered.

Furthermore, several respondents suggested that a gradual adoption process is most probable for any DLT or digital currency system. One respondent underscored the urgency of this issue, noting that 'the next phase of our DLT experimentation is to look at interoperability of ledgers in a cross-border payment context'. Central banks must work out how to minimise the potential risks of this gradual approach. This means working with providers and partners to configure support for different types of consensus mechanisms, whether through a notary service, with both parties in an agreement digitally signing off on a transaction, or otherwise.

This means they will have to consider the interoperability between new and old systems; yet, at the same time, DLTs rely on 'network effects' resulting from widespread adoption to yield their full benefits. Some have suggested that this 'domestic-first' piecemeal approach is the fastest and easiest way to adopt wholesale CBDCs. Starting with smaller steps minimises complexity and smoothes out interactions between differing wholesale CBDC projects and legal systems, making changes more palatable to legislators. □

'Digital tokens for wholesale payments and some aspects of distributed ledger technology – the key technologies underlying cryptocurrencies – may hold promise for strengthening traditional financial instruments and markets.'

Lael Brainard, Federal Reserve Board of Governors

53%

53% of those polled suggest that the central bank would be 'in the driver's seat' on determining access to a wholesale CBDC



76%

Of respondents, 76% state that it is uncertain whether DLT will be able to deliver on its promise, especially in areas such as regulation



Ensuring financial stability and security

This section examines the key policy questions and implications of issuing a wholesale central bank digital currency, building on the previous section on practicality, and delving deeper into the legal and regulatory issues, as well as the economic and security effects and considerations.

Central bankers, as well as academics and private sector financial institutions, have analysed extensively the policy implications of a retail central bank digital currency. These include the changing role of the central bank or the implications on the monetary policy transmission mechanism. However, the implications of a wholesale CBDC are less well understood.

From a legal and regulatory perspective, these largely depend on the type and design of the wholesale CBDC, as well as on the circumstances of each jurisdiction in which it is issued. They relate to differences in, for example, insolvency laws and recovery and resolution issues. These are particularly pertinent in the application of a wholesale CBDC to cross-border payments and settlements, where the relationship between rules governing different jurisdictions would need to be established.

Implications would also depend on the design and format of the wholesale CBDC. A crucial variable is which entities are allowed to participate in the platform. If they are limited to regulated entities (existing participants in the relevant real-time gross settlement systems), then there should be no major differences with the current system, which provides no interoperability between RTGS systems for different currencies. Instead, the existing system includes entities that may transact on multiple RTGS systems, either directly (the continuous linked settlement) or through other entities in their corporate group, with each conforming to local jurisdictional issues. Such an arrangement could be replicated under a DLT-based platform.

Monetary policy and financial stability

Respondents to the OMFIF survey generally agreed that wholesale CBDCs should be

issued only by central banks, and that they should not be made available to non-banks. In that respect, wholesale CBDCs would be no more than a representation of current central bank money for central bank account holders, with no policy implications.

In the case of wholesale CBDCs, projects and proof of concept exercises undertaken by central banks have so far been limited to trials and designed in such a way that precludes any financial stability implications. Ultimately, risks to financial stability would depend on scale: respondents noted that, as long as the wholesale CBDC replaces only a part of central bank reserves, any serious impact on financial stability can be avoided. However, risks may arise if a wholesale CBDC entirely replaces central bank reserves.

Central banks' projects surveyed in this report for applying distributed ledger technology to wholesale payments systems have all been exploratory. Legal, regulatory and policy issues were not addressed. Discussion of policy implications highlight that implementing the platforms tested is not expected to have an impact on the monetary policy transmission mechanism.

Digital tokens as reserves

The impact on monetary policy would further depend on whether the digital tokens in question have the status of reserves. As one respondent put it, 'If these tokens are considered as reserves, and the blockchain system is a new medium for recording transactions, then there should be no impact on monetary policy, and the existing tools may continue to be used.' Around 80% of survey respondents shared this opinion.

In today's system, the International Monetary Fund's aspiration for its special drawing right to become a global reserve currency has been held back by conflicting geopolitical interests and priorities of the

reserve-issuing central banks of the US, euro area, China, Japan and UK. CBDCs can circumvent such hurdles by enabling the private sector to work directly with the central banks to create a digital SDR to use as a unit of account and store of value.

Such an eSDR would be the quintessential reserve asset, because it would be fully backed by the reserve currencies in the IMF-determined ratio. The supply of eSDRs would in turn be dependent on market demand. This would require the creation of a sufficiently large eSDR-denominated money market.

Clearing houses and intermediaries

A DLT arrangement is likely to have a pronounced impact on the overall financial market architecture. In some cases, it can be seen as more of an incremental upgrade of current arrangements, and one that does not significantly alter existing business practices. In others, such as an unrestricted arrangement, DLT may lead to disintermediation of certain functions or entities. Such a change may affect the competitive balance in financial markets and introduce new, non-bank players that are not considered by existing regulatory regimes.

Beyond the immediate horizon, many industry participants see significant potential for DLT to increase efficiency and reduce reconciliation costs in securities clearing and settlement. A recent joint venture between the Deutsche Bundesbank and Deutsche Börse, which developed a functional prototype of a DLT-based securities settlement platform that achieves delivery v. payment settlement of digital coins and securities, represents progress in this area.

Implications for Swift

The application of DLT to wholesale interbank payments would provide an alternative to the

traditional correspondent banking method on which the Society for Worldwide Interbank Financial Telecommunication bases its messaging system. The DLT-based platform could be quicker, cheaper and more secure in sending money between currencies.

Swift has responded to the DLT threat by improving the efficiency of its messaging system and carrying out tests on the potential of blockchain technology. Specifically, Swift has launched an upgraded service, called Global Payments Innovation, which is being used by 165 banks. In some payments corridors, such as US-China, Global Payments Innovation accounts for four in every 10 transactions. However, to avoid confidential information being seen by rival banks, Swift has said it would need to build more than 100,000 subledgers to accommodate all of its 11,000 member banks.

International payment messaging systems are vulnerable to being replaced by alternatives that bring benefits of security and verifiability, but at a lower cost. Swift has the initial advantage of a standardised communication protocol, but this advantage by itself will probably be insufficient to sustain its business model. Indeed, many countries – such as China and Russia – are setting up their own payments systems to reduce their reliance on foreign payments systems and also as a gateway to the international payments system. Germany has recently called for a European system independent of the US. In other words, such countries could link their systems, routing bilateral international transactions through their own networks rather than relying on Swift.

The proliferation of payments systems could increase financial stability by creating multiple levels of redundancies, so that the failure of one payments system would not be harmful to the system as a whole. However, there are important considerations that could worsen instability.

Electronic systems have considerable technological vulnerabilities. These weaknesses, in addition to the lack of official backing, could expose these systems to crises of confidence. If this happens at a time when official payments systems have been sidelined as a result of competitive forces, there

could be dire financial and macroeconomic consequences.

Fragmentation and lack of oversight of payments systems could lead to pooling of counterparty risk in the payment hubs. This would make them more fragile at times of financial stress.

Cybersecurity

Wholesale CBDCs will need to ensure that central banks' systems are resilient and can cope with cyber attacks. This would require a wholesale CBDC to comply with already existing standards on system-wide resilience and cybersecurity, such as the European Central Bank's cyber resilience oversight expectations.

In addition to cybersecurity, a wholesale CBDC would need to fulfil requirements from an oversight and operational perspective (such as RTGS service-level agreements). Some central banks, such as the South African Reserve Bank, have used the Principles for Financial Market Infrastructures as a guide to testing prototypes for such requirements.

One of the key tests performed as part of the central bank proofs of concept was related to safety. Several central banks tested the scenario of node failures. Findings generally showed that, even if a specific node fails, the rest of the network can continue to operate.

A wholesale CBDC would need to fulfil these cybersecurity and operational functionality requirements irrespective of the specific technology adopted. Central bank experiments highlighted the differences between various platforms. Generally, blockchain-based networks rely heavily on cryptography, which in turn relies on the security and handling of private keys. Should private keys be lost or copied, funds can be locked or potentially stolen.

In a permissioned network, workarounds can be employed, especially when there is an issuer involved. This highlights the potential advantage of a private blockchain network with just one issuer. In those circumstances, a lost or invalid key would not be as problematic, as the central bank could issue new tokens and invalidate the old ones. □

'It is indispensable that we strengthen European autonomy by creating payment channels that are independent of the United States.'

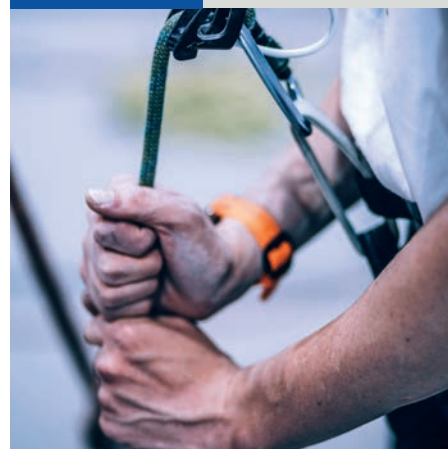
Heiko Maas, Federal Minister for Foreign Affairs, German Government

8%

Around 8% of survey respondents explicitly stressed that a wholesale CBDC would have an impact on monetary policy

165

Swift has launched an upgraded service, called Global Payments Innovation, used by 165 banks



Case studies for the next generation

This section describes current initiatives developing the next generation of interbank payment and settlement systems. Central banks have taken the lead on research and trials, using a variety of methods and technology platforms.

These initiatives often involve a variety of stakeholders and incorporate relevant industry participation. The decentralised nature of these projects emphasises the need for collaboration in establishing a system that meets user needs. The final case study in this section addresses LedgerConnect, a marketplace developed by IBM and CLS for blockchain-

based applications. The platform is designed to permit institutions to pick from a range of vendors and service providers, enabling them to deploy services on a shared distributed ledger. This allows banks to explore various options concerning the architecture of other distributed ledger networks they may construct.

01 South African Reserve Bank: Project Khokha

Objective: Simulate a 'real-world' trial of a distributed ledger technology-based interbank payments system modelled on South Africa's real-time gross settlement framework.

Results: The technology platform delivers the required performance, in some cases exceeding the current performance criteria. However, risks related to the integrity, security and availability of the network, as well as legal and regulatory factors, must be further evaluated before such a system can be implemented.

05 Bank of Canada: Project Jasper

Objective: Initial phases sought to explore how distributed ledger technology could improve payments systems in Canada and around the world.

Results: Phase 1 successfully delivered intended functionality, but concerns were raised around the consensus mechanism. The subsequent phase worked as intended, processing a high volume of transactions within an acceptable window.

02 Bank of Japan-ECB: Project Stella

Objective: Phase 1 investigated whether innovations in distributed ledger technology could ensure faster and cheaper payment processing and settlement. Phase 2 examined whether and how DLT can deliver securities against cash.

Results: In Phase 1, the technology's maturity was unsuitable for larger-scale systems. Phase 2 had success in exchanging securities against cash, but there must be more exploration of legal and security aspects before further use of DLT can be implemented.

06 Monetary Authority of Singapore: Project Ubin

Objective: Strengthen Singapore's position as a global financial centre through DLT use in interbank payments.

Results: Tests for scalability, performance and resilience were successful, as were safeguards preventing single points of failure. Phase 2 demonstrated that a real-time gross settlement system could be built and operated on cloud. Tests for scalability, performance and resilience were successful, as were safeguards intended to prevent single points of failure.

03 Bank of Thailand: Project Inthanon

Objective: Develop a wholesale central bank digital currency to enable faster and cheaper settlements between domestic banks.

Results: Proofs of concept with Thai domestic banks, which successfully tested key payments capabilities.

07 IBM: Blockchain World Wire

Objective: Overcome the complexities and inefficiencies associated with the traditional methods of cross-border payments and settlements.

Results: Allows two financial institutions to deal and send funds between their accounts directly, without multiple intermediaries.

04 Saudi Arabian Monetary Authority

Objective: Achieve greater transparency in domestic payments and facilitate the growth of a 'cashless society'.

Results: Recent deal to pilot digital payments system to modernise payments system and link its domestic network to global financial institutions; experiments with liquidity management facilities, offline transacting and other technology.

08 IBM and CLS: LedgerConnect

Objective: Establish a marketplace for blockchain-based applications for financial market participants.

Results: Successful proofs of concept and strong interest from financial institutions.

1

PROJECT KHOKHA

South African Reserve Bank: Project Khokha

In January 2018, the South African Reserve Bank launched Project Khokha (Zulu for 'pay'), a trial of the possible use of distributed ledger technology for interbank wholesale settlement. There has so far been one phase to the project, completed in April 2018. The results were successful and published in June 2018.

THE South African Reserve Bank's Project Khokha is a relative newcomer to the suite of central bank initiatives assessing the use of distributed ledger technology. The project is a proof of concept designed to simulate a 'real-world' trial of a DLT-based interbank wholesale payment system modelled on the South African Multiple Option Settlement system, the country's real-time gross settlement framework. The Sarb piloted the project in collaboration with seven banks, a technical service provider and a consulting practice. The project was built on DLT platform Quorum, using the Istanbul Byzantine fault tolerance consensus mechanism, Pedersen cryptography commitments, Whisper private messaging, and range proofs.

The project followed a staggered approach of banks establishing their own nodes on the network. This was followed by the development of the RTGS DLT platform's contracts and solution over four iterations, which gradually extended the functionality of the system. Performance tests were finally conducted for iterations three and four to determine the throughput the system could achieve and whether it could withstand the stress-test scenarios and other hypotheses investigated in the project.

Results

The results indicated that the Quorum platform can deliver the required performance, in some

cases exceeding the current performance criteria. The following hypotheses were proven:

1. RTGS transactions can be executed using standard payment message formats. The proof of concept was designed in compliance with ISO 20022, a standard payments message format.
2. Messages can be processed at sufficient scale in line with current system processing times. The typical daily volume of the South African payments system, and even double the current system's performance for transactions, could be processed in less than two hours, with full confidentiality and settlement finality. The third test-run for iteration three resulted in 90,000 transactions being processed in one hour and 16 minutes. Iteration four processed 70,000 transactions in just over one and a half hours, beating the target of 70,000 transactions in two hours.
3. Blocks should be propagated within one second to a 95% confidence level and within two seconds to a 99% confidence level. System latency was within the targeted times for the writing blocks, with 99% of blocks propagated through the network in one second and 100% in 1.25 seconds.
4. The confidentiality and privacy of transactions between commercial banks are maintained. The use of Whisper for private messaging, Pedersen commitments and range proofs ensured that the Quorum solution provided robust confidentiality while enabling

the required transaction throughput.

The visibility of the system is sufficient for oversight and operational management. The Sarb had no operational involvement in approving the transactions, although it was able to view the detail of all the transactions to enable regulatory oversight.

Next steps for Project Khokha

While Project Khokha was a successful proof of concept for a DLT-based wholesale settlement system in South Africa, the report concluded that the Sarb does not intend to replace the country's existing RTGS system with DLT at this juncture.

Complexities and risks related to the integrity, security and availability of the network, as well as legal and regulatory factors, demand closer examination before a DLT system could be implemented. This would need to include elements such as liquidity management and credit extension to provide full functionality.

The Sarb identified future avenues for this system to be developed, such as the settlement of bonds or securities, trade finance applications, cross-border payments and even the facilitation of monetary policy and other fiscal coordination across borders. The central bank also suggested it could oversee a cross-border experiment with the Southern African Development Community as one of the next steps. □

AUGUST 2017:

A fintech unit is formally established within the Sarb, with the intention of exploring the implications of fintech innovation for the central bank and financial services in South Africa



JANUARY 2018:

The Sarb's fintech unit initiates Project Khokha to explore the use of distributed ledger technology for interbank payments settlement in South Africa

JANUARY 2018:

Project Khokha runs for 14 weeks



MAY 2018:

The Sarb releases the Project Khokha report, outlining results

2



Bank of Japan and the European Central Bank: Project Stella

In December 2016, the Bank of Japan and European Central Bank launched a joint research project, Project Stella, which studies the possible use of distributed ledger technology for financial market infrastructures. There have so far been two phases to the project, completed in September 2017 and March 2018.

Phase 1

DURING the first phase of Project Stella, the Bank of Japan and European Central Bank conducted in-depth experiments to investigate whether the liquidity-saving mechanisms of their real-time gross settlement systems (BoJ-Net and Target-2) could be run in a DLT environment in an efficient and safe manner. These experiments were conducted by replicating the systems on Hyperledger Fabric Version 0.6.1.

Project Stella was run using two types of smart contract: one that processes payments without offering any queuing and offsetting, and another that includes liquidity-saving mechanisms based on the queuing and offsetting mechanisms of the banks' existing RTGS systems. The tests were conducted using simulated data, run through the DLT both at a constant rate and at a rate replicating the pattern of transaction traffic throughout the day. The code was first run

outside a DLT set-up, and then through two DLT set-ups to allow for comparison and to set a benchmark for efficiency: (i) a single node without a consensus mechanism, and (ii) a distributed environment with a consensus mechanism. The ECB conducted its experiment in a virtualised and restricted in-house test environment, while the BoJ used cloud computing services.

Efficiency

Performance was measured based on the latency of the system, estimated as the time taken between a transaction request being sent and the transaction being executed and written to a block, calculated across all nodes.

The project's findings suggest that DLT-based solutions could meet the current performance needs and process volumes of payment requests in the euro area and Japan.

Transactions modelled on the average traffic of the two centralised payments

systems (around 10-70 requests per second) were processed in less than one second on average. Peak payment traffic consistent with that of existing services was also processed without difficulty. However, performance suffered when the project teams raised traffic to 250 requests per second.

The study also confirmed the expected pattern of a DLT environment and the relevance of network configuration: the bigger the network, the longer it takes for a payment request to be executed and recorded in a block, and the more probable it is for messages to be ignored in the transaction processing. This result applied to both the simple payment transfers set-up and the liquidity-saving mechanism smart contract, suggesting that the mechanism's execution is not a major factor contributing to latency. A similar trade-off was observed in terms of the distance between the nodes and latency.

Safety

Stella focused on the impact of three specific scenarios on the functioning of the system:

- The temporary failure of one or more validating nodes;
- The temporary failure of a special node used in Fabric to certify participants and transaction requests;
- Percentages of transactions sent to the system with an incorrect data format.

The tests found the DLT solutions to be



Haruhiko Kuroda
Governor of the BoJ,
October 2017

'At this juncture, the Bank of Japan does not have any concrete plan to introduce a CBDC. Neither does it have an immediate plan to apply those technologies to its operating system.'

DECEMBER 2016:

The BoJ and ECB launch Project Stella, a joint research project to study the potential of DLT

JANUARY 2017:

Yves Mersch delivers a speech in Helsinki entitled 'Digital Base Money: An assessment from the ECB's perspective' – the first such speech by an ECB official



SEPTEMBER 2017:

Project Stella's first-phase findings are published, focusing on payments systems



OCTOBER 2017:

Haruhiko Kuroda delivers speech entitled 'Digital Innovations, Finance and Central Banking', discussing issues around CBDCs

resilient to the failure of individual network nodes. As long as the number of nodes required by the consensus algorithm was operational, system availability was not affected. Tests also confirmed that a validating node could recover irrespective of downtime.

The tested DLT solutions were able to withstand a high number of incorrectly formatted messages, with the system capable of detecting incorrect data formats without them affecting overall performance.

While the test series produced promising results, it was noted that no direct conclusions could be drawn from the test set-up with respect to the potential usage in production. It was instead concluded that, given the relative immaturity of the technology, DLT is not yet an appropriate solution for large-scale applications such as BoJ-Net and Target-2 at this stage of development. Questions around cost efficiency, market integration and oversight were left to be addressed in future studies.

Phase 2

In its second phase, Project Stella moved from payments to securities settlement, exploring how the delivery of securities against cash could be conceptually designed and operated in a DLT environment.

The project draws on existing delivery v. payment approaches, as well as innovative

solutions (functionalities such as 'cross-chain atomic swaps'). Prototypes were developed using basic and stylised scenarios of two counterparties, using three DLT platforms: Corda, Elements and Hyperledger Fabric.

The project found that DvP can run in a DLT environment with cash and securities either on the same ledger (single-ledger DvP, similar to the 'integrated model' in existing securities settlement mechanisms) or on separate ones (cross-ledger DvP with connection between ledgers, analogous to the 'interfaced model' in existing securities settlement mechanisms, or without connection between ledgers, which does not exist in the existing set-up).

It was also found that DLT offers a novel approach for achieving DvP between ledgers that does not require any connection between ledgers. Functionalities such as 'cross-chain atomic swaps' have the potential to help ensure interoperability between ledgers without necessarily requiring connections and institutional arrangements between them.

However, the project highlights that, depending on their specific design, cross-ledger DvP arrangements on DLT may entail a high degree of complexity and could give rise to additional challenges. For example, the conduct of DvP transactions between ledgers that have no connection requires several process steps and interactions between the seller and the buyer. Several risks could

'The Bank does not have a specific plan to issue digital currencies at this stage.'



Hiroshi Nakaso
Deputy Governor of the
BoJ, May 2016

materialise depending on the specific design, such as principal risk, replacement cost risk and liquidity risk.

Overall, while the exercises undertaken as part of this phase two showed that securities can technically be settled against cash in a DLT environment, the study highlighted that safety, efficiency and legal aspects would first need to be explored more thoroughly.

Next steps

Project Stella is an exploratory initiative, seeking to assess whether specific functions of existing systems can be safely and efficiently run in a DLT application. The BoJ and ECB do not currently have plans to consider a wholesale central bank digital currency. The focus of Project Stella is understanding the technological foundations and conducting experiments to understand better the potential applications and limitations of various DLT fabrics to support payments and settlement.

The ECB and BoJ continue to experiment with different software and set-ups. So far, the practical aspects – such as what the unit of account would be, whether the system would be in partnership with other central banks, and the monetary policy implications – have not been considered. □



Yves Mersch
Member of the Executive
Board of the ECB,
January 2017

'For the ECB, the discussion is mainly an analytical one. The ECB would in particular have to understand the impact – positive or negative – of digital base money on our primary objective of price stability before considering introducing it.'



FEBRUARY 2018:
Yves Mersch delivers speech for OMFIF in London, saying, 'There is currently no convincing motivation for the ECB to issue digital base money to the general public'

MARCH 2018:
Project Stella's second-phase findings are published, focusing on securities settlement systems



MARCH 2018:
ECB Executive Board Member Benoît Cœuré gives speech in Berlin concluding that, while 'the ECB is investigating the potential of DLT... we have come to the interim conclusion that the technology is not yet mature enough'

APRIL 2018:

BoJ Deputy Governor Masayoshi Amamiya delivers speech on 'Central Banking in the Digital Age', focusing on the impact of IT innovation on the currency and payment and settlement systems



3



Bank of Thailand: Project Inthanon

At a time of rapid change in financial technology in the country, the Bank of Thailand is developing and trialling a wholesale central bank digital currency to enable faster and cheaper settlements between domestic banks, with a launch expected later in 2018.

THE Bank of Thailand has announced it will research, develop and trial a wholesale central bank digital currency with the goal of enabling faster and cheaper settlements between domestic banks using a system of underlying tokens. Various Bank of Thailand figures, as well as papers published by the central bank, have emphasised that this system is not for immediate use. Nonetheless, Thai officials and financial institutions are optimistic that this project will enable long-term productivity gains and lower settlement costs, especially once disparate central banks are able to link their platforms together.

The project comes at a time of rapid

‘The Bank of Thailand and banks will co-develop a new way of conducting interbank settlement using wholesale central bank digital currency.’



Veerathai Santiprabhob
Bank of Thailand Governor

change in the country’s financial technology community. Major Thai institutions have been testing distributed ledger technology products; Kasikornbank, for example, collaborated with IBM in July 2017 to implement a Hyperledger-based system to issue letters of guarantee. All 14 major Thai commercial banks, as well as the central bank and other public institutions, announced in March 2018 that they would be collaborating to develop a shared, blockchain-based platform for trade financing through a working group dubbed the ‘Thailand Blockchain Community Initiative’.

The Thai finance minister announced that the domestic legislature was evaluating two crucial regulations on cryptocurrencies and coin offerings, suggesting that attitudes towards new technologies in the Southeast Asian state are warming.

Applications for the project

Project Inthanon builds on these efforts. Initially tested in the central bank’s sandbox, proofs of concept involving bonds issued over a blockchain followed. The Bank of Thailand foresees that the CBDC may make the allocation of savings bonds to investors more rapid, reducing waiting times to two days from 15 through scriptless issuance. Other long-term applications are being explored, including decentralised technologies that may be used for supply chain finance. Furthermore,

the central bank has announced that it has selected a handful of partners – including consultants Accenture, law firm Baker & McKenzie and the National Electronics and Computer Technology Centre – to resolve various technological and legal aspects.

On the other hand, the central bank has been adamant that it does not plan to use the underlying technology in any significant wholesale, or even retail, capacity in the near term. Rather, Governor Veerathai Santiprabhob suggested that ‘like other central banks, [the Bank of Thailand’s] goal is not to immediately bring CBDC into use’, but rather to explore and examine potentially interesting applications for ‘back-office operations’.

The central bank announced in August 2018 that it was in the early stages of a collaborative proof of concept for the issuance of a wholesale CBDC. It will work with eight Thai commercial banks to develop a prototype CBDC for domestic wholesale funds transfers, using R3’s Corda platform as a foundation. The central bank noted this would test key payment functionalities, including liquidity saving mechanisms and risk management. In the light of changes taking place in the Thai economy and legislature, as well as the central bank’s self-appointed role as a ‘catalyst for digital infrastructure development’, enthusiasm is warranted. □

JULY 2017:
Thai Kasikornbank collaborates with IBM to implement blockchain-based letter of guarantee issuance system



MARCH 2018:
Thailand Blockchain Community Initiative working group launched



MARCH 2018:
Bank of Thailand governor predicts that blockchain technology will improve productivity, lower costs and increase security at Bangkok Fintech Fair 2018

SEPTEMBER 2018
Bank of Thailand and eight local banks initiate Project Inthanon, an interbank payments project built on Corda

4



Saudi Arabian Monetary Authority: Partnerships

Hoping to modernise payments systems and link its domestic market to global financial institutions, the Saudi Arabian Monetary Authority has taken its first steps into the digital currency field in the form of a partnership with Ripple and a host of local banks.

MORE than a decade ago, the Saudi Arabian Monetary Authority began discussing with other regional states the viability of a single currency for the Gulf Co-operation Council. Although these talks faltered following the United Arab Emirates' exit from the project in 2009, Saudi Arabia and the UAE are now collaborating on the potential issue of a digital currency later this year.

This is only one of several avenues that Sama has pursued in its attempts to stake a claim in the digital currency space. Perhaps most importantly, Sama recently agreed to partner with Ripple to modernise its payments system and link its domestic network to global financial institutions. This is the first programme of its kind to be launched by a central bank.

Despite its ambition, however, the project is presently limited to smaller local banks and transfers between them. Sama has adopted Ripple's payment protocol without using the underlying currency, XRP, at the same time.

Instead, the Saudi central bank opted to use foreign remittance technology – a design choice that presumably makes the system more familiar but inhibits the transformative potential of Ripple's product. The kingdom will instead use xCurrent, another Ripple platform, to settle payments sent into and out of the country, enhancing transparency and reducing costs. Moody's has suggested that Sama can expect annual savings of up

to \$400bn by, among other things, halving the payment costs of remittance transfers.

The adoption of new payment systems has made financial services more accessible to small and medium-sized enterprises, which Sama plans to provide with thorough training on programme management. This will help boost non-cash transactions, a long-standing goal of the Saudi central bank. Adoption of these technologies has been accompanied by the development of a vibrant domestic market for fintech start-ups. Firms such as PayTabs have entered and established themselves with the broader aim of changing the payment processing industry.

In its exploration of wholesale CBDCs, Sama explained that it is focusing on integrating cross-border payments and using the most mature technologies available. With this in mind, the central bank has experimented with liquidity management facilities, offline transacting and other technological features, aiming to increase the speed, security and transparency of its payment system.

In its response to the OMFIF survey, Sama suggested that it is relatively far along in its research, and that several other projects are being conducted concurrently with the aim of improving proof of concept exercises and evaluating in greater detail the policy implications of a wholesale CBDC.

'By facilitating interactions between suppliers and buyers, our service will enable immense improvements in customer experience, financial management and collections, and bring about substantive benefits to the broader Saudi economy.'

Ziad Al Yousef
Managing Director of
Payment Systems,
Sama



In December 2017, following an open selection process, Sama and the Central Bank of the UAE chose IBM to collaborate on implementing their RTGS link and bridge currency experiment to enable easier cross-border transactions between Saudi Arabia and the Emirates. IBM's success in this open selection speaks volumes about its expertise in this field. □



DECEMBER 2017:

Saudi Arabia and the UAE work on the launch of a digital currency to be used for regional transactions



FEBRUARY 2018:

Sama signs a deal with Ripple to help Saudi Arabian banks settle payments

2030:

Year by which Saudi Arabia hopes to have achieved 'cashless society' status



5



Bank of Canada: Project Jasper

In March 2016, Payments Canada, the Bank of Canada, R3 and several Canadian financial institutions launched Project Jasper, an initiative intended to help understand how distributed ledger technology could transform the future of payments in Canada. There have so far been two phases to the project, completed in June 2016 and April 2017 respectively.

Phase 1

THE purpose of Project Jasper’s first phase was to investigate the use of central bank-issued digital receipts for deposited currency to support settlement on a distributed ledger technology platform. The Phase 1 platform, intended to host wholesale interbank settlement capability, was built on Ethereum, employing a proof of work consensus protocol. The settlement asset was a digital depository receipt reflecting a claim on Canadian-dollar deposits held in accounts at the Bank of Canada.

Phase 1 was successful in delivering the intended functionality in a non-production setting. However, the proof of work consensus mechanism raised concerns around operational efficiency, as it was demonstrated that this method could not provide the necessary throughput as volumes increased. This was because the proof of

work protocol required all R3 members to perform validation of a proposed exchange of digital depository receipts between two participants as a requirement for that exchange to be recorded on the database.

While this supported timely transaction processing, it was suggested that it could introduce constraints in future peak volumes.

Moreover, the platform did not support participant requirements for data privacy, as the Ethereum solution provided full visibility into the central ledger for all participants in the system. Finally, it was unclear when settlement finality was achieved in the proof of work solution.

Given the above, the analysis concluded that DLT platforms that employ a proof of work consensus protocol do not deliver the necessary settlement finality and low operational risk required of core settlement systems.

Phase 2

A major objective of Phase 2 was to evaluate the scalability and flexibility of DLT by moving to an alternative technology platform and continuing to build-in more of the functions present in the Large Value Transfer System, Canada’s interbank settlement system.

Specifically, the Jasper platform transitioned from Ethereum DLT to R3 Corda. The two settlement options supported by the platform are an ‘atomic’ option and a ‘liquidity-saving mechanism’ option. The latter takes the form of a central queue that draws on a payment-matching algorithm to routinely settle batches of queued payments on a net basis. This helps economise on liquidity and promote the smooth intraday flow of payment transactions.

Phase 2 also featured a distributed ledger system that employed an alternative consensus model on the basis of a ‘notary node’ that could deliver improvements with regard to settlement finality, scalability and privacy.

The notary node is one of three on the Jasper 2 platform, with the other two being a participant node and a supervisory node. The notary node plays a centralised role, managing a node that reflects all transactions on its ledger. Consensus on the Corda platform is achieved through two functions – a validation function and a uniqueness function. The first is performed by the



Carolyn Wilkins
Deputy Governor, Bank of Canada

‘There would be strong potential for more savings if other applications were built upon a core cash payment DLT system – for example, financial asset clearing and settlement, and trade finance.’

MARCH 2016:
Payments Canada, the Bank of Canada and R3, together with a number of Canadian financial institutions, launch Project Jasper, a proof of concept of a DLT-based wholesale payment system



JUNE 2016
Phase 1 of Project Jasper concludes, culminating with a demonstration of the platform at Payments Panorama



170

Total payments
in C\$bn that
LVTS clears daily

participants on the platform, and the second by a special trusted participant, the notary. The implication of the validation function is that participants in the system see information about more than their own transactions, but no more than is absolutely necessary to allow independent verification. This represents a significant advancement over Ethereum in terms of meeting the user requirements for privacy.

Increased volumes were not expected to be a concern for the Phase 2 platform, as it requires only the transacting parties, a supervisory node and the notary node to validate and record a transaction on the shared database. However, this comes at the expense of the operational resilience of the platform, as an outage of the notary node would stop the processing of all payments. This is because centralised activities can create a single point of failure.

A number of data-driven simulation exercises were completed as part of Phase 2 to evaluate the operation of the central queue

and payment-matching algorithm and the performance of the platform. This was done under a range of circumstances using real and artificial payments datasets for banks participating in the exercise. The team devised scenarios of low- and high-volume days to mirror the reality of the Canadian LVTS system and to test whether DLT could handle the volume of transaction activity observed in the incumbent systems.

LVTS clears a total payments value of more than C\$170bn daily. For the simulations, the hypothetical operating day was from 08:00-18:00. Total transactions for the low-volume day were around 26,000 with a value of C\$104.5bn, and for the high-volume day at 37,000 representing C\$227.9bn.

Testing in Jasper Phase 2 illustrated that current-day average volumes (50,000 payments per day, and at least 14 items per second) could be processed within an acceptable window. Further testing showed that the algorithm worked as intended in a range of scenarios, including one where the payments intended for atomic settlement cannot enter the queue under any circumstance.

Next steps

Project Jasper is an exploratory initiative and there are no immediate plans to include DLT as part of improvements for Canada's payments framework.

Evaluation against the LVTS was not included in the scope of Phases 1 and 2, and policy-makers concluded that it will be challenging for any DLT-based system to process payments more efficiently than the LVTS. This was, however, suggested as a possible long-term objective of Project Jasper.

One opportunity for further exploration is how to pledge general collateral instead of cash collateral at the Bank of Canada. A future phase of Project Jasper could look at the

'Bank staff are exploring the circumstances under which it might be appropriate for the central bank to issue its own digital currency for retail transactions. All central banks are researching this.'

Stephen Poloz
Governor, Bank
of Canada



advantages of a DLT solution based on central bank-issued digital cash equivalents provided for related processes, such as securities settlement. Another would be to explore the potential integration between Project Jasper and other types of DLTs, either domestically or internationally, and explore how a single-currency DLT zone could be connected with other currencies.

Phase 2 led to a system that could deliver settlement finality with improvements in scalability and privacy. However, operational reliability remains an issue.

This must be overcome for the core system to follow the Principles for Financial Market Infrastructure. While further analysis is required, the industry is improving DLT platforms' adherence to the PFMI, which must be met by any wholesale interbank payments system.

Policy considerations and the reform of legal constructs that will need to define the operational framework to support a DLT settlement solution were left for future study. □

MAY 2016:

Bank of Canada Deputy Governor Carolyn Wilkins delivers speech in Calgary entitled 'Fintech and the Financial Ecosystem: Evolution or Revolution?', suggesting that 'now is the time for financial institutions, new entrants and policy-makers to work together'

SEPTEMBER 2016:

Phase 2 of Project Jasper is launched, exploring the possibility of implementing a liquidity-saving mechanism on a DLT platform

APRIL 2017:

Phase 2 of Project Jasper ends



JUNE 2017:

'Project Jasper: Are distributed wholesale payment systems feasible yet?' is published in the Bank of Canada Financial System Review, summarising key aspects of Project Jasper

6



Monetary Authority of Singapore: Project Ubin

The Monetary Authority of Singapore's Project Ubin, which is looking into the prospect of central banks issuing their own digital currency, has built on the foundations laid by Canada's Project Jasper and seeks to improve the Southeast Asian country's position in global financial markets.

THE Monetary Authority of Singapore launched Project Ubin in November 2016 to see if it could use distributed ledger technology to enhance the country's competitive advantage as a global financial hub. The project put MAS at the forefront of central banks' exploration of issuing their own digital currency, enabling it to test how DLT can be used for more transparent, resilient and low-cost interbank transactions.

The collaborative approach taken by MAS underscored the importance of working with industry players and learning alongside them while testing the frontiers of new technology. Project Ubin benefited from the groundwork laid by Canada's Project Jasper, taking lessons from the latter's two concluded phases and applying them to Singapore's financial environment.

'The key breakthrough of blockchain technology is its ability to establish trust in a decentralised system.'



Ravi Menon
Managing Director,
Monetary Authority
of Singapore

Phase 1

The first phase of Project Ubin assessed the feasibility and practicality of conducting domestic interbank payments through DLT. A consortium of financial institutions and technology companies partnered with MAS to create SGD-on-ledger, a tokenised form of the Singaporean currency on DLT backed by an equivalent amount held by the central bank. R3, the blockchain firm that worked on Project Jasper, was an integral part of Project Ubin.

Phase 1 ran for six weeks and involved developing a prototype of a distributed ledger network that uses the digital SGD and can interface with the MAS Electronic Payment System (MEPS+), Singapore's real-time gross settlement system. Through MEPS+, MAS facilitates large-value SGD transfers between participating banks and settlement of Singapore government securities.

The prototype was built on a private Ethereum digital ledger and allowed participating banks to pledge cash into a custody account held by MAS, which then creates the equivalent in digital currency. Banks could then use the digital SGD to transfer funds to each other or to MAS.

Smart contracts were built into the prototype. These virtual agreements are encoded into the network to trigger a transaction when a predefined logical condition is met, such as when a stock price hits a certain level.

Transfers and payments on the distributed ledger can be made at any time, unconstrained by the operating hours of MEPS+. Potentially, a 24-hour system could remove the delays caused by payments made across time zones.

Phase 2

The next step for Project Ubin was to test DLT's suitability for specific RTGS functions. Phase 2 of the project focused on running liquidity-saving mechanisms in a decentralised system while ensuring the privacy of transactions.

RTGS typically relies on a centralised liquidity-saving mechanism to remove transaction gridlocks and maximise overall liquidity in a network. DLT removes the need for a central operator because the ledger is distributed among participating banks. The project sought to take advantage of this feature while developing additional protocols to protect transactional privacy.

Phase 2, run in partnership with the Association of Banks in Singapore, conducted trials on three different DLT platforms: Corda, Hyperledger Fabric and Quorum. As with the first phase, this was undertaken in collaboration with a number of banks and technology companies.

A key difference of the three Phase 2 prototypes from their Ethereum-based predecessor is that information can be strongly encrypted and made accessible

14 NOVEMBER –
23 DECEMBER 2016
Sought to evaluate possibility of
conducting domestic payments
through DLT through the creation
of a CBDC



JUNE –
SEPTEMBER 2017:
Applied DLT to RTGS payment systems to
determine whether essential features such
as privacy and regulation can coexist with
decentralisation

only to intended nodes. All three prototypes demonstrated that RTGS functions can be decentralised while preserving the privacy of transactions.

Aside from privacy, the three systems were tested for scalability, performance and resilience. Although tested on a small scale, each of the three prototypes can be expanded to handle much larger volumes of participants and transactions. They are also designed with safeguards to prevent single points of failure.

All three prototypes were hosted in cloud platform Microsoft Azure across 41 virtual machines. The success of Phase 2 demonstrated that an RTGS system using DLT can be successfully built and operated on cloud infrastructure.

Next steps

At the end of both phases, MAS published detailed reports explaining how the prototypes were developed, the conclusions drawn and how these findings can impact policy-making and regulation. MAS also released the source codes for Phase 2 to help other interested parties that plan to conduct trials – proof that Singapore is approaching the use of DLT as a continually evolving experiment.

Apart from developing the prototype’s technical aspects, Project Ubin has a research workstream that investigates its potential impact on policy and regulation. It looks at how the issuance of a central bank digital currency can affect monetary policy, as well as the role that a central bank or operator such as MAS should play in facilitating interbank payments on a decentralised distributed ledger network.

The Singapore Exchange, a participant in earlier phases of Project Ubin, is leading the next phase. This will apply DLT specifically to fixed-income securities trading and settlement. Together with MAS and private

sector technology partners, it will develop delivery v. payment systems using digital currency on different blockchain platforms. Using smart contracts, DvP settlement processes could be automated for a seamless flow of transactions, demonstrating a practical business application for DLT.

Succeeding phases of Project Ubin will test the use of DLT in cross-border payments, considered by MAS as the project’s ultimate goal and most valuable application. Fund transfers across jurisdictions involve costly

additional checks to prevent fraud, money laundering and other illicit activities. The process of verification typically takes several days, but this could potentially be done instantly with DLT.

MAS is partnering with the Bank of Canada and the Bank of England to explore DLT’s cross-border and cross-currency potential. It is also working with the Hong Kong Monetary Authority to use DLT in trade finance between Hong Kong and Singapore, with the eventual goal of expanding the network globally. □

	Corda	Hyperledger Fabric	Quorum
Privacy	Distributes ledger on a need-to-know basis rather than using a global broadcast method. Only parties involved have visibility of transaction details.	Sets up private channels between participants where each channel maintains an independent ledger. Channels partition the data to limit transaction visibility only to concerned stakeholders.	Private transactions are sent directly to specified recipients while the rest of the network can only see a hash. Transactions can be verified by comparing hashes without revealing actual amounts.
Scalability and performance	Adding nodes only requires installation, with minimum change required to the existing network setup. Need-to-know operation removes burden of storing and updating the entire ledger on every peer.	Use of bilateral channels means that network complexity increases with every additional participant.	Can support dynamic addition of new nodes using a higher version of Quorum.
Resilience	Network can continue to operate even if one of the participating nodes is unreachable.	Higher resiliency can be achieved by setting up redundant nodes in the system.	Network functions even if a node is disconnected, and transaction history is automatically synced when the disconnected node comes back online.
Finality	Notary signature indicates transaction finality.	Each transaction needs to be endorsed by the set of peers defined in the endorsement policy.	Uses Raft consensus model with an elected leader that verifies transactions before committing a block to the chain.

NOVEMBER 2017:

MAS announces that it is collaborating with the Bank of Canada on cross-border payments using blockchain technology. Memorandum of understanding between MAS and HKMA to develop the Global Trade Connectivity Network



JUNE 2018:

The Bank of England announces it is working with MAS, the Bank of Canada and private sector firms to improve interbank cross-border payments, including initiatives based on distributed ledger technology

AUGUST 2018:

MAS and SGX announce that they are collaborating

7



IBM Blockchain World Wire

IBM Blockchain World Wire seeks to overcome the complexities and inefficiencies associated with the traditional methods of cross-border payments and settlements. World Wire uses a digital asset on distributed ledger to circumvent traditional banking intermediaries, reducing capital requirements, clearing costs and time needed to process transactions.

GENERAL acceptance of digital assets backed by fiat money held in custody will deliver near instantaneous settlement, reducing the need for reconciliation work. This will lessen the need to build large operations for payment processing and status management. The elimination of the prefunded accounts through various correspondent bank accounts is another substantial benefit, especially for small enterprises. The ability to free up capital and keep money working to fund business activity is invaluable.

IBM's World Wire is a payments platform that supports the use of digital assets whose value is pegged to underlying fiat currency to process and settle transactions simultaneously using a single ledger with technical finality. World Wire digital assets are always redeemable for their fiat currency equivalents at par value as issuers must hold equivalent collateral in cash within segregated accounts. In countries where deposit insurance is available, World Wire digital asset issuers are expected to structure their collateral accounts to maximise insurance coverage.

The use of digital assets on a common ledger allows two financial institutions to deal and send funds between their accounts directly, without going through multiple intermediaries. This reduces the amount of prefunding needed on a systemic basis, since financial institutions no longer have to place

funds at multiple correspondents to reach different parts of the payments network. The effects of using a common ledger are akin to those derived from virtual pooling of liquidity, as the role of the Treasury function is simplified. The results should be improved liquidity management and lower costs for cross-border payments.

World Wire also supports the use of digital obligations, which serve as an agreed-upon store of value between the two parties until payment obligations are fulfilled with finality.

The blockchain is used as an immutable record of settled transactions, and World Wire supports advanced dispute resolution mechanisms that rely on cryptographic signatures and commitments that are stored on the blockchain to audit the accuracy of financial claims. The underlying blockchain technology utilises the 'permissioned' and open-source Stellar consensus protocol.

This system reduces capital requirements, clearing costs and the time needed to process new transactions as well as to integrate new markets into capital flows.

IBM World Wire can use any fiat currency provided it is agreed by participants in the transaction. Another strength of the IBM system is its flexibility. The platform integrates seamlessly with existing payment systems, and even provides alternative settlement methods for participants not immediately comfortable with the use of cryptocurrencies.

'New types of fiat-backed instruments have the potential to improve international banking operations and payments, giving banks an easier way to integrate with public blockchain networks.'

Jesse Lund
Vice-President of IBM
Blockchain



Through these options, the IBM platform overcomes concerns about the volatility and reliability of underlying digital assets. As more and more companies explore the viability of accepting cryptocurrencies as an alternative to conventional corporate methods of payments, such as credit cards, and with the introduction of new digital assets similar to bitcoin, digital assets are likely to become more common in corporate payments and gradually overcome the unsubstantiated concerns that they are a riskier method of payment. The success of wholesale projects will be key for central bank digital currencies to be accepted at a retail level. □

JULY 2018:

Stronghold, a financial services firm, announces it has produced a dollar-pegged digital asset on the Stellar network; IBM to 'explore uses'



OCTOBER 2018:

IBM plans to unveil its platform at the Sibos conference in Sydney



8

LedgerConnect

LedgerConnect

Following their collaboration in creating CLSNet, a bilateral payment netting solution, IBM and CLS are now developing LedgerConnect, a marketplace for competing blockchain-based applications targeting financial institutions. The platform will allow institutions to deploy and share services on a shared distributed ledger technology network.

IBM and CLS, a systemically important financial market utility responsible for the settlement of more than 50% of global foreign exchange transactions, are collaborating on the construction of LedgerConnect, a marketplace for competing blockchain-based applications targeting financial institutions. Nine major financial firms are participating in a proof of concept exercise that will feature approved vendors such as Baton Systems, OpenRisk and Copp Clark.

The LedgerConnect platform is designed to permit institutions to pick from a range of service providers, allowing them to deploy and share services on a distributed ledger technology network. Sanctions screening, know-your-customer processes and collateral management are some of the services that will be provided through this financial services app market.

LedgerConnect relies on a permissioned blockchain based on IBM's blockchain platform, built on Linux's Hyperledger Fabric. The platform has, however, been designed to facilitate the integration of other blockchain technologies.

This enables the provision of various services and facilities through a single network. This means financial institutions can remain concentrated on their business objectives, rather than devoting energy to platform development and the production of

multiple versions of the same application, or the creation of unique interpretations in silos. LedgerConnect has the potential to reduce redundancy, spur innovation and produce significant efficiencies and cost savings. This also addresses the existing 'connectivity gap' between fintech start-ups and large banks, which causes the duplication of distributed networks throughout the competitive market.

LedgerConnect will allow banks to explore various options concerning the architecture of other, future distributed ledger networks that they may choose to construct. Banks participating in this endeavour will experience a combination of centralised, market infrastructure-hosted nodes and more decentralised, bank-hosted nodes. This pairing gives participating institutions a sense of familiarity when making design choices in future DLT ventures.

At the same time, regulations that apply to banks' traditional services are still being adapted to platforms such as LedgerConnect. This is a complex process, and participating institutions must wait patiently for it to be completed. Furthermore, the success of the project requires IBM and CLS to rely on goodwill from financial institutions – they must give up the chance of gaining a competitive edge for a collective 'greater good' in payment systems. Whether they are willing to do so remains to be seen.

CLSNet

Prior to LedgerConnect, IBM and CLS had previously partnered on a bilateral payment netting solution (CLSNet), also built on Linux's Hyperledger Fabric platform. This allows financial institutions to make operational processes more efficient. This includes optimising intraday liquidity, enabling real-time awareness of currency and counterparty exposures, and reducing risk.

CLSNet has provided an array of benefits for member institutions. First, its ability to assist in risk management enhances liquidity. Second, its ability to provide netting, as opposed to compressing, in foreign exchange trades is a boon to smaller, emerging market currencies, as these often lack the liquidity to be traded adequately.

The CLSNet project has contributed to many features in the development of Hyperledger Fabric. It has provided important input on, for example, what security features are needed to run a network within financial markets, as well as how financial institutions should be sharing data on a blockchain network.

The solution presently sits alongside CLSSettlement and covers trades that are currently not settling on this platform. The intent is that CLSNet's coverage will include all currencies associated with jurisdictions that are not on official sanctions list that would prevent CLS from conducting business with that jurisdiction. □

EARLY 2015:

CLS, a foreign exchange clearing house, begins testing blockchain technology



SEPTEMBER 2016:

IBM and CLS begin work on a new settlement service



AUTUMN 2016:

CLS consortium demonstrates its new blockchain platform at Sibos, Swift's annual conference

JULY 2018:

IBM announces partnership with CLS to develop LedgerConnect

Cross-border collaboration critical to the future of digital currencies

Achieving real-time gross settlement for domestic and cross-border payments has traditionally been fraught with complexities, high costs and lengthy settlement times, leading to several risks in settlement finality. Central banks agree that, despite significant improvements in existing structures, these issues continue to undermine payments systems. Maintaining overall system resilience is a priority for central banks, especially as the current system remains vulnerable to single points of failure. The main motivations expressed by central banks in pursuing a wholesale central bank digital currency include potential improvements in speed, efficiency and resilience, as well as boosting system utility as non-cash assets become tokenised. However, realising these benefits depends on the success of the underlying technology.

Trials of wholesale CBDC systems illustrate how variations of distributed ledger technologies have the capacity to meet and, in some cases, exceed the performance of existing interbank systems. However, there is still a long way to go before the technology is mature enough to meet central banks' expectations for the next-generation of real-time gross settlement systems.

The costs of exploration are high, and success is not guaranteed. For smaller central banks, adopting a wait-and-see approach has been beneficial, while larger central banks with more resources take the lead in experimentation. When there is a viable business case, the central bank may opt to work with a small group of local banks and a systems integrator and build a 'tokenised' CBDC on a suitable distributed ledger platform.

The next step would be to produce a pilot programme and move actual capital. A central bank could, in a controlled environment, issue a legal liability to a participant, have it transferred to another participant, then have it redeemed. DLT experimentation focusing on the interoperability of ledgers in cross-border payments should follow.

Collaboration between private sector participants and the central bank will determine whether these initiatives find success domestically. For cross-border success, this collaboration must expand to include various national central banks from around the world.

International regulatory co-operation is critical. The Principles for Financial Market Infrastructure, although they provide a solid foundation, are insufficient for the long term, as problems are likely to arise from potential regulatory arbitrage in different jurisdictions. The PFMI will need adjustment to accommodate different, decentralised models. The PFMI's governance and legal basis principles were written with a centralised model of operation in mind. Now may be the right time for central banks to review these principles to reflect increasing multipolarity in the world economy, where users of global payment systems have greater autonomy in creating independent payment channels.

Regulatory collaboration should not be limited to the payments system. It must expand to address cybersecurity concerns and currency hegemony through compatibility with capital controls, all of which are intertwined with the question of wholesale CBDCs. □

Frequently used acronyms

CBDC, central bank digital currency: a digital asset issued by the central bank for the purpose of payment and settlement, in either retail or wholesale transactions. A 'retail' CBDC would be used by all people and companies, whereas 'wholesale' CBDCs can be used only by permitted institutions as a settlement asset in the interbank market.

DLT, distributed ledger technology: a consensus of replicated, shared, and synchronised digital data geographically spread across multiple sites, countries, or institutions, without a central administrator or centralised data storage.

RTGS, real-time gross settlement: the funds transfer system in which central banks facilitate the real-time movement of funds between accounts held by financial institutions at the central bank.

DvP, delivery v. payment: the security settlement process where the delivery of and payment for an asset occurs simultaneously.

PFMI, Principles for Financial Market Infrastructures: the international standards for financial market infrastructures (payments systems, central securities depositories, securities settlement systems, central counterparties and trade repositories) published by the Bank for International Settlements.

SDR/eSDR, special drawing right and electronic special drawing right: the International Monetary Fund reserve asset made up of a basket of currencies, and its digital counterpart.



The team consulted more than 20 central banks in writing this report, whom we thank for their views and opinions. Although some requested anonymity, we thank the following for their views and opinions: Central Bank of Brazil, South African Reserve Bank, Norges Bank, Bundesbank, Bank of Finland and the European Central Bank.

IBM

Jesse Lund
Vice President,
Blockchain and Cryptocurrencies

Stanley Yong
Chief Technical Officer,
Blockchain for Financial Services

Mollie Martin
Global Marketing Lead,
Blockchain for Financial Services

OMFIF

Bhavin Patel
Lead Author, Economist

Philip Middleton
Deputy Chairman

Danae Kyriakopoulou
Chief Economist and Head of Research

Kat Usita
Economist

Pierre Ortlieb
Research Assistant

**William Coningsby-Brown
and Simon Hadley**
Design and Production

Julian Frazer
Senior Editor

Oliver Thew
Business Development



IBM Blockchain World Wire
600 Anton Blvd
Costa Mesa, CA 92626
www.ibm.com/blockchain/solutions/world-wire



Official Monetary and Financial Institutions Forum
30 Crown Place, London, EC2A 4EB United Kingdom
T: +44 (0)20 3008 5262
www.omfif.org @OMFIF