DMI
Digital Monetary Institute

CYPHERIUM

CENTRAL BANK DIGITAL CURRENCIES AND BLOCKCHAIN

Exploring new technology solutions

August 2020

Participants at roundtable, August 2020

Moderator,
Chris Ostrowski,
Commercial Director,
OMFIF

Cees van Wijk
IT Team Manager,
ING Nederland

Sky Guo
Chief Executive Officer, Cypherium

Simon Scorer
Senior Fintech Specialist, Bank of England

Aniko Szombati
Chief Digital Officer,
Magyar Nemzeti Bank

Thomas Moser
Alternate Member,
Governing Board
Swiss National Bank

CENTRAL BANK DIGITAL CURRENCIES AND BLOCKCHAIN

Exploring new technology solutions

WITHIN THE next two years, the first fully operational central bank digital currency will have been launched. This was the view of 51% of respondents to a poll held at OMFIF's recent panel discussion about the prospects for CBDC.

The question intentionally left some room for interpretation. While it excluded experiments of the kind that a number of central banks throughout the world have already undertaken, it did not specify whether it referred to wholesale or retail CBDC. Nor did ask attendees to express a view on whether the first operational CBDC will be issued in a developed country or an emerging economy, where the motivation for accelerating the introduction of CBDC may be very different.

In cashless Sweden, for example, concerns about the marginalisation of cash are the main driver for exploring the potential of an e-krona. In emerging countries with extensive unbanked populations, financial inclusion is regarded as the main benefit of introducing CBDC. More broadly, according to respondents to the OMFIF poll, it is the enhanced efficiencies to be extracted from CBDC that are most appealing to central banks.

Nor were attendees asked to forecast whether central banks will favour a public or private blockchain as the most efficient technology for supporting CBDC, which is a subject on which most remain open-minded. As the International Monetary Fund notes, 'some [central banks] are focusing on running on a centralised ledger, and some on a distributed ledger technology platform in which the ledger is replicated and shared across several trusted participants within a private permissioned network.'

Technological innovation, which is progressing at a breakneck speed, is already dispelling some of the traditional misgivings about the adoption of blockchain. Concerns about transaction speed have traditionally been at the forefront of these. But attendees echoed the strongly held view of a number of panellists who insisted that recent technological advancements have nullified worries about slow transaction speed. A strikingly low 13% of poll respondents regard this as a barrier to blockchain adoption.

This compares with almost three-quarters whose principal concern remains interoperability, liquidity and technology risk. Their reservations about interoperability are a reminder that the importance of cross-border payments is such that research into the potential of CBDC undertaken in isolation is of limited practical utility. As panellists emphasised, collaboration between central banks will be imperative if CBDC is to realise its potential. As Lael Brainard of the Federal Reserve cautioned in a recent speech, 'a poorly designed CBDC issued in one jurisdiction could create financial stability issues in another'.

While the speed and method of implementation of CBDC therefore remains open to question, the direction of travel is unmistakable, with only a handful of poll respondents forecasting that a fully operational CBDC is still more than five years away. ●

CHRIS OSTROWSKI, OMFIF: Although central banks vary dramatically in their expectations for digital currencies, they all agree that CBDC is much more than just another small technical change.
There is also a big divergence of central banks' views on the technology supporting CBDC. Some say there is no need for blockchain technology. Others believe there is no point in launching or issuing a CBDC without the advantages that blockchain can bring.
I'd like to begin this session by asking the central bank panellists what they have been doing with regard to CBDC, and what they see as the primary benefit they are seeking to achieve with the potential launch of a CBDC.
ANIKO SZOMBATI, MAGYAR NEMZETI BANK: MNB believes this is an area that needs to be implemented step by step, beginning with small pilot projects and learning from the process.

This September we are launching a students savings scheme, which is a very simple application for a limited number of schools in the first year. This allows students to participate in quizzes where the prizes are digital coins which can be exchanged, collected, and ultimately redeemed for prizes from the central bank foundation.

If this goes well, next year we'll expand the programme to include real life payment possibilities. This will be the point at which we consider putting the system on a centralised distributed ledger technology platform.

We launched a second project recently which will go live next year to coincide with the 75th anniversary of our national currency, the forint. This will allow precious coins to be registered on a blockchain system. We'll have a special programme related to the anniversary, in which the six letters spelling out 'forint' can be earned in a digital form by participants successfully completing quizzes on financial literacy. Participants collecting all six letters will earn physical coin sets that can be entered into the coin registry system and tracked via special identifier codes.

These projects may seem to be small-scale, but we believe they will play an essential role by supporting financial education and encouraging the adoption of electronic payments among young people. By adopting innovative technologies and identifying where the potential bottlenecks or legal problems may exist in projects of this scale, we are preparing for the smooth completion of large CBDC projects. By utilising blockchain technology, we also believe we are leading by example for the Hungarian public sector.
CO: Simon, the Bank of England has done a huge amount of research on this subject. What would the Bank like to see from the launch of a CBDC?
SIMON SCORER, BANK OF ENGLAND: It's important to emphasise that we haven't yet made a decision on whether to launch a CBDC. But we are seriously considering the implications of a retail CBDC, and we published a discussion paper earlier this year on the benefits, implications and practicalities of issuing one. We don't have all the answers yet; the paper was intended as a starting point for the discussion, inviting experts in a wide range of fields to comment on the issues raised.

As to why we're looking at it, we recognise that we are in the middle of a period of rapid change in money and payments. Technological advancements are creating new ways to save and to pay, and there are new forms of private money on the horizon. Some of these, like stablecoins, may become systemically important in time, but they may also pose risks to monetary and financial stability.

Currently, the Bank of England provides the safest and most trusted form of money – as banknotes and electronic reserves - but households and businesses can only access this in the form of banknotes. This raises the question of whether we should leverage advancements in technology to provide a new type of central bank-issued electronic money, in the form of a CBDC, which could be held by the public as a complement to cash.

'By utilising blockchain technology, we also believe we are leading by example for the Hungarian public sector.'

We don't see a decision on a CBDC as a direct substitute for other forms of central bank, or privately issued, money. A CBDC would sit alongside cash but it would also need to be positioned alongside private sector payment developments. Finding a space for a CBDC is one of the important challenges that we need to address.

Any CBDC would clearly be at the heart of everything we do. It presents a lot of opportunities for monetary and financial stability, as well as for payments.

Several of these opportunities were outlined in the paper we put out in March. These include supporting a more resilient payments landscape; avoiding some of the risks of private money creation; encouraging competition, efficiency and innovation in payments; and helping to meet future payment demands in a digital economy, for example through the use of smart contracts, or to enable micro payments.

It's also worth noting that the motivations for creating CBDC vary dramatically from country to country and jurisdiction to jurisdiction. For example, financial inclusion could be an important motivator in certain parts of the world, while the decline in the use of cash may be a key driver in others.
CO: The Swiss National Bank has also been a pioneer in this area. When can we expect to see a CBDC from Switzerland?
THOMAS MOSER, SWISS NATIONAL BANK: In the case of Switzerland, the CBDC initiative did not originally come from the central bank, but from the Swiss Stock Exchange, which plans to go live next

year with a DLT-based digital exchange. Named SDX, this will be a fully integrated, end-to-end digital asset trading, settlement and custody service.

For us, this raised the question of how participants on this DLT will pay, and what will be done with the cash lag. SDX is addressing this by creating a stablecoin backed by the Swiss franc. This led us to ask if it would make sense to have central bank money on the DLT. Particularly where systemically critical infrastructure is involved, as a central banker you would normally want to minimise risk by ensuring that payment is made with central bank money, because it is the only type of money without counterparty risk.

So we are working on two proofs of concept. The first involves the issuance of wholesale CBDC on the SDX DLT platform. The second is looking at whether we could hook up the DLT to our traditional real-time gross settlement system.

'I believe that both wholesale and retail CBDCs will be necessary. A central bank confining itself to using a wholesale CBDC will need to manage both digital currency and cash in its financial system, limiting the efficiency of the CBDC.'

We intend to issue our report on this together with the BIS Innovation Hub by the end of the year, but we don't yet know whether we'll go live with one of these solutions. Even if we don't, SDX will go live with its own stablecoin at the beginning of 2021.

So our motivation is a little bit different from other central banks in the sense that we're partnering not with an experiment but with a real live case.

CO: Where will accountability reside between the SDX and the SNB for Swiss franc-backed stablecoins?

TM: SDX intends to open a settlement account with the central bank, which will then be used as collateral for the stablecoin. Negative interest rates may make full collateralisation for stablecoins expensive. This is another reason why for SDX it would be more interesting to have real central bank money on the blockchain. For the banks it would also be appealing because it would reduce their capital exposure, and hence their regulatory costs.

CO: So does this herald the end of RTGS?

TM: I don't think so. The Bank of Canada, Monetary Authority of Singapore, Bank of England, European Central Bank and others have all done some wonderful research demonstrating that if you just want to do payment versus payment among banks, there aren't many additional benefits to be generated from having a blockchain. This suggests there is no need to replace a modern RTGS which is just as efficient.

CO: Sky, Cypherium has done a lot of interesting work on blockchain innovations that can support the development of CDBC. From your experience, who do you think the winners and losers will be from CBDC?

SKY GUO, CYPHERIUM: I believe that both wholesale and retail CBDC will be necessary. A central bank confining itself to using a wholesale CBDC will need to manage both digital currency and cash in its financial system, limiting the efficiency of the CBDC.

If I had to pick a winner, I'd go with retail CBDC. Retail CBDC is designed to replace cash, which has many disadvantages, such as physical insecurity, vulnerability to forgery, lack of hygiene and other practical inefficiencies. Retail CBDC addresses these drawbacks and can accelerate the propagation of monetary policy. For example, if a central bank wants to adopt negative interest rates, it could do so more easily with a retail CBDC than with cash.

CO: Cees, what plans does ING Bank have for ensuring it is a winner from the launch of CBDC? Can you tell us a bit about some of the technology work that ING has done?

CEES VAN WIJK, ING: In my role as IT manager of ING Bank's blockchain team, I believe that the winners will be those who have the most experience with this technology.

I see two possible scenarios for the impact of CBDC on banks. An unlikely scenario is one in which a retail CBDC is positioned as a savings product which is free of counterparty risk, and competes with private sector banks. This would erode customer deposits, impact the size of wholesale banks' balance sheets and reduce their lending capacity. This in turn would have negative consequences for the economy.

In a more likely scenario, retail CBDC will be positioned as an alternative to cash and will be used only to make payments. In this scenario, the losers will be the banks that are too conservative and unable to adapt their traditional business models.

Let's talk about the winners. They will be the banks that invest extensively in blockchain and DLT, understand the benefits of the technology and respond by developing a new business model. This may involve providing and running the necessary blockchain infrastructure or technical solutions, which are an advance on the centralised technology used in today's payments systems.

Many of these systems require improvements to their scalability, defined as the number of transactions per second they can process. Their privacy features also need to be upgraded, ensuring that sensitive data can be kept private, which is less evident in a decentralised system. Banks which master these challenges will be the winners in a post-CBDC scenario.

At ING, we want to be a tech company with a banking licence, which is why we have been contributing to the improvement of blockchain technology ever since its introduction. This is not to say our ambitions in technology are limited to the use of blockchain, because we're also actively involved in areas such as machine learning.

Specifically for CBDC, we have gained a lot of experience working with Finality and its Utility

Settlement Coin solution. Its platform could serve as the infrastructure underpinning CBDC.

When it comes to retail CBDC, somebody will need to manage the private keys that access these digital currencies. As we've seen with public cryptocurrencies, this can be messy because consumers can lose their private key, and therefore lose access to their assets. At ING we have decades of experience with private key infrastructure and managing those keys.

In managing digital assets on blockchain, we use military-grade hardware security modules to safeguard private keys. We also have a state-of-the-art, home-built multiparty computation threshold signature solution which protects customers against losing their keys, because only if the majority of their keys are lost do they lose their assets. In these areas we have already filed three patents to protect our IP.

We believe we can be a winner by generating fee income from the provision of our services, which is completely different from the traditional wholesale banking model.

CO: Sky, do you believe CBDCs are best served by a public or private blockchain?

SG: I believe that public and private blockchains can both be used for CBDC. Central banks are likely to use private blockchains because they need to protect the privacy of their financial systems and of their citizens using the CBDC. However, private blockchains create barriers of trust and interoperability, which could be resolved by the use of public blockchains.

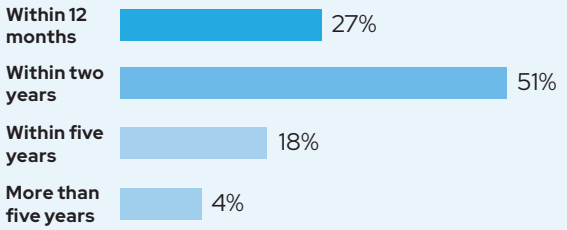
So far, most CBDC research has focused on private blockchains, but public blockchains have better availability and robustness. For example, the bitcoin network has been running on an uninterrupted basis for over a decade. Also, by allowing for an unobstructed flow of data and messages, public blockchains are protected against government interference. Because public blockchains usually have tens of thousands of peer-to-peer nodes, they are practically impossible to shut down.

Moreover, public blockchains are easy and inexpensive to operate, with no membership fees required to access them. Their transparency also means they can serve as a witness to private blockchain transactions, proving that payments have been made and safeguarding against double-sending money. It's impossible to violate a well-defined public blockchain programme.

Central bank control can also be achieved on a public blockchain with greater trust. Moreover, public blockchains may improve the internalisation of a currency. Stablecoins backed by fiat currencies have already been successfully implemented on public blockchains and used for cross-border transactions.

The high levels of transparency and trust in public blockchains are crucial to any international business. Take the use case of a simple letter of credit. Using a public blockchain, the importer can process the payment into a smart contract which will only release the payment to the exporter after receiving confirmation from the shipping company. Each party can see and verify the smart contract and trust the execution of the public blockchain.

1. When do you think a fully operational CBDC will be launched?



AS: Coming back to your question about public versus private blockchains, for our students savings programme, we plan to use a private blockchain, or DLT system. A major benefit of this is that offline transactions can be executed as well.

CO: What is the biggest barrier to blockchain adoption among central banks? What are the things that keep the governor of the Bank of England awake at night when you present him with proposals on introducing a CBDC?

SS: My view is that a blockchain isn't automatically necessary for a CBDC. In theory, you could set up a wholesale or retail CBDC using another form of technology. I think it's important to note the origins of blockchain in this context. The starting point for bitcoin was that it was designed as an alternative to a system that depends on trust in commercial banks as well as central banks. A CBDC is clearly a very different proposition. By definition, it's a central bank asset and therefore suggests a high level of trust in the central bank, which changes the dynamic significantly.

Having said that, clearly the world of blockchain and DLT provides a host of innovations that may be useful in creating a CBDC. It may not be a question of adopting all the features of blockchain but of picking and choosing different features. The way I look at it is not to say we will or will not take a blockchain approach, but aim to identify some of the innovations that are emerging, to see where they are useful and where they may be problematic in the thinking around a design for a CBDC.

Thinking about your question on the barriers to adopting blockchain, I don't think the biggest challenges relate to the technology in isolation but to the end-to-end proposition of any of these developments. I'm thinking here about what the wider implications are – the legal implications, the implications for the wider financial system, the implications for commercial bank deposits, the implications for how this would interface with existing payments infrastructure. There is a whole host of interconnected issues and assessing the holistic

proposition of any CBDC is the biggest challenge.

CO: Sky, what is it that makes blockchain so special? Why is it different from other technical innovations that could help improve the financial system?

SG: There are many elements that make blockchain uniquely useful and necessary, and which will underpin its continued growth.

'At ING, we want to be a tech company with a banking licence, which is why we have been contributing to the improvement of blockchain technology ever since its introduction.'

The first is that it does not rely on bank accounts. Simple encryption is all that is needed to boost financial inclusion in countries with large unbanked populations.

Blockchain can reduce the risk of a single point of failure, making CBDC systems resilient to crash, hacking, physical damage and natural disasters. It can also support decentralised digital management and prevent massive data breaches because the technology does not rely on any single centralised system to store personal sensitive data.

Also, blockchain establishes a distributed form of decision-making and consensus, enabling governance by multiple parties. This is because each consensus participant has equal voting power, and a quorum must be formed before decisions are made.

Additionally, smart contracts are easy to integrate with artificial intelligence, big data and other modern technologies, increasing productivity exponentially. They lay a rich foundation for future financial innovations which are not always achievable in our current framework.

Blockchain can help to combat financial crime, as all transaction records are on a distributed network, and so-called Wirecard fraud can be detected by the blockchain technology. It can also support offline payment giving digital currencies the same benefits as physical cash. A digital signature and fingerprint can ensure that offline transactions aren't fabricated.

Some believe the main roadblock to blockchain adoption for CBDC is the lack of transaction speed. This is no longer a barrier, given recent technological advancements. These can now settle thousands of transactions in a few minutes or even seconds, whereas traditional transactions usually take several days to complete.

CO: More specifically, what value does Cypherium add for central banks exploring the potential of CBDC?

SG: Cypherium is an enterprise-grade blockchain smart contract platform. By using a combination of the industry's most cutting-edge Byzantine fault tolerance consensus algorithm and Java Virtual Machine, Cypherium is able to process thousands of transactions per second with instant finality, reaching speeds beyond even those of Mastercard and Visa without sacrificing the principles and security of decentralisation.

As a smart contracting platform, the Cypherium Virtual Machine runs Java, the most used coding language in the world. This enables access to billions of legacy devices waiting to be enfranchised by the world of blockchains, providing seamless integration with mobile and financial applications. Cypherium's technology has been vetted through several partnerships with tech giants such as Amazon Web Services, IBM and Google Cloud Platform. The blockchain's efficacy has been proven through a to-scale use case with Randstad, one of the world's largest HR providers, for whom Cypherium provided an identity solution to protect the data privacy of millions. Recently, their technology has garnered interest for its uses relating to CBDC. Cypherium's Digital Currency Interoperability Framework, which allows CBDCs to interact and interoperate with one another as well as other digital currencies, has garnered interest from policy-makers, bankers and technologists.

CO: Pivoting back to what Simon said, if the starting point is that there is a trusted core ledger and source of issuance for currency, can central banks maintain sufficient trust and control on a fully decentralised blockchain?

SG: The CBDC is a technological representation of the government-issued fiat currency. In a private system, this is backed by the trust and credit of the central bank. However, a CBDC on a public blockchain would be governed by a smart contract code and a consensus algorithm.

CVW: In a centralised system, it's very easy for the party which controls the system to control who gets access to which data. But if it's a decentralised system, where multiple parties are involved in validating the ledger updates – which is the process we call a consensus – then how can you keep confidential information confidential, while allowing others to validate updates? You can't simply encrypt the data, because this would make it almost impossible to do any validation – which is why ING is working on zero-knowledge proofs.

In the past, we created libraries that integrated with Ethereum and Quorum. Today we're working on a zero-knowledge proof protocol that integrates with R3's DLT, Corda. This keeps all your information secret, but it also allows everyone else to verify the cryptographic proof that your ledger update is valid. In other words, it adheres to the rules of the protocol.

A simple example in a bitcoin payment would be that a payment can only be made by the owner of the bitcoin who knows the private key of the address to which the bitcoins belong.

Bitcoin is a good example to use because the validation rules are very simple and everyone can relate to them. For CBDC there will be similar rules but there will be more to them. In a decentralised ledger, multiple parties must validate the transactions, and only if the majority are honest can you be confident that a completely genuine transaction will be recorded.

CO: We often hear about filter theory, which is the idea that if you launch a wholesale CBDC it will eventually filter down to the individual. Would that be a realistic expectation if the SNB were to set up a CBDC?
TM: I don't think one naturally leads to the other. Today, central banks have digital money exclusively for the banks in the form of the wholesale system which is not open to retail customers. It's possible that a similar situation could be created with a wholesale CBDC being accessible to certain financial institutions but not to households at large.

Another interesting question might arise if you have a blockchain for a digital exchange and the rules on who can participate are determined by the exchange. In the future, will we see an exchange where trading is not restricted to financial institutions, in which households can also participate directly? If so, the question becomes more complicated: is it then a wholesale or a retail system?
CO: Aniko, when you look at the technology underpinning what the MNB is doing, do you expect a wholesale system to filter down to a retail system?
AS: I agree that the development of an end-to-end project is complex and expensive. So when you are doing your cost-benefit analysis, on the benefit side you must have a dedicated public policy goal identifying what you want to achieve. You also have to look at the alternatives. In our case, the major driving force has been the synergy between existing central banking goals and having the opportunity to experiment with new technologies.

But a complete, large-scale wholesale or retail CBDC has so many connection points, and even if you're providing the complete set of legal, operational and infrastructural elements that are required, after a while this has to apply on a cross-border basis as well. So I don't think the filter theory would apply in this case. A lot of work, a lot of collaboration and a lot of progress is needed globally if we are to reach a point where CBDC can flourish in all jurisdictions.
CO: How important has the question of interoperability been in the Bank of England's technology research?
SS: It is absolutely vital. We haven't yet reached the stage of designing a system, so we haven't made any concrete decisions on the technology. But it's clear that interoperability needs to be thought about from the beginning, and that central banks will need to collaborate in order to understand where there is common ground. If they are to be useful or cross-border use, it is important that as CBDCs emerge in different parts of the world they are not incompatible.

We will also need to think about what interoperability actually means. It is sometimes assumed it means that everybody needs to operate the same system on the same platform, which is not necessarily the case.
CO: Sky, what do you see as the best way of achieving a minimum common ground to ensure interoperability between different CBDCs?

SG: I believe a hybrid architecture is the best solution for enabling interoperability between CBDCs. Because CBDCs are closed and private systems, they can't interact with each other without an intermediary. This creates a barrier because central banks will never expose themselves to the risk of malicious sabotage or eavesdropping by giving other countries direct access their systems.

Libra intends to become a retail currency for billions of users. This goal is almost impossible to achieve in reality because no country will be willing to allow another party to have full access to its domestic financial transactions, compromising the independence of its monetary policy.

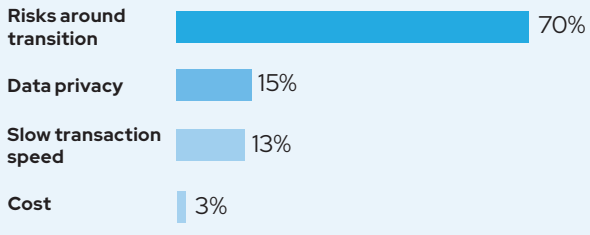
'Cypherium's Digital Currency Interoperability Framework has garnered interest from policy-makers, bankers and technologists.'

A likely scenario is therefore that central banks will issue their own CBDC on private ledgers and connect to other CBDCs via a public ledger.

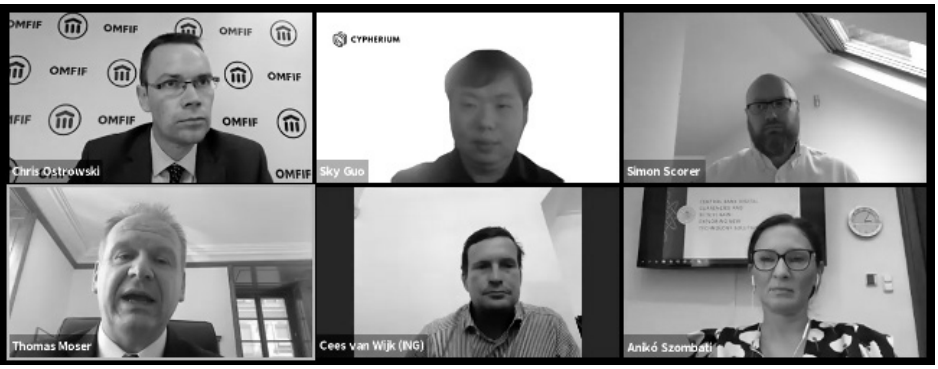
Smart contracts are another potential pillar of interoperability, which has already been done between currencies on public blockchains such as Ethereum's ERC20 standard.

Interoperability involves data exchange and message transmission. A common message format is required, such as the ISO20022 standard. This should be taken into consideration at the design stage of the CBDC. A blockchain-based interoperability framework for CBDC would require more sophisticated design and functionalities than Ethereum. The most common use case here is the exchange of two CBDCs. For example, imagine that Alice wants to exchange her digital euros for Bob's digital dollars. Both parties are concerned that the other won't fulfil their promise and steal their money. To prevent this, they can create a smart contract on a public blockchain, each lock up the money to be exchanged, and release the locks only after the transaction on both sides has been completed.
CO: What are the panel's views on how existing systems such as Swift will be affected by cross-border CBDC payments?

2. What is the biggest barrier to blockchain adoption in central banking?



'A DLT ecosystem will grow up around central banks, and that we will see different types of financial market infrastructure taking shape based on DLT'



CVW: I believe there will be a blockchain or DLT system for each currency zone. If you look at a concrete example of a popular technology like Corda developed by R3, which has been used in many central bank experiments, they provide out-of-the-box interoperability between different Corda distributed applications.

Most public blockchains have full replication, whereby all the nodes store all the transactions and the complete history of the blockchain. That is not required in Corda, where you only have those transactions that are relevant to you, and which only validate those transactions that you're involved in. One example of a clever way in which they distribute who gets to store which transactions is the possibility of using multiple notary services, which provide consensus on the uniqueness and timestamping of transactions. This means you could have separate euro area and sterling notary services, for example. Only when you have a foreign exchange payment from euros to sterling or vice versa would you have a cross-notary transaction.

CO: Simon, what's your view on the current systems and the role they'll play as these technologies evolve and cross-border CBDC payments become possible?

SS: I think it's still an open question. To some extent it hinges on the primary motivations and use cases that CBDCs are being designed for, and whether they're for domestic or cross-border use. Even if they're designed for domestic use they may facilitate a certain amount of cross-border use.

We're primarily thinking about this from a domestic point of view, but we are aware that one of the potential benefits is as a building block for better cross-border payments in future. At this stage many central banks are at the relatively early stage of thinking about these things and I don't know if we have fully worked out what those interactions will look like.

The way I see CBDCs is not as a replacement for everything. They will need to coexist with existing as well as potential emerging infrastructures.

CO: Sky, how do you think blockchain will be different from existing systems such as Swift?

SG: As a completely new technology, blockchain definitely requires a new system separate from the legacy systems for interoperability. Swift usually requires manual entry of the recipient's information and multiple intermediaries. It takes several days and costs hundreds of dollars to send a message. It also charges expensive membership and installation fees.

If a CBDC still uses Swift, its performance will be hostage to the limits of the legacy system, whereas adopting a new infrastructure can unlock all the benefits of CBDC because blockchain can match the speed of the CBDC and is much cheaper. A transaction can be executed simply by scanning a quick response code and can be settled in a few seconds.

CO: We often talk about scalability, by which I mean the number of transactions per second and the cost reductions that can be generated as volumes rise. Is there enough trust in blockchain as a technology to allow scalability to run its own course once the central bank has established the core ledger?

AS: This is a very valid question. When we were developing our pilot project I was aware of the pressure the central bank was under to develop a blockchain project with verifiable, trusted technology that could be applied elsewhere in the public sector. I was aware that it would be a huge breakthrough if the central bank could come up with a system using blockchain technology.

Learning as we go is the right method and if the central bank can come up with smaller scale projects, as time passes and the system proves to be trustful it can be scaled up in further use cases.

CO: Is there a tension between scalability and decentralisation? Is it the case that if you want more scalability you have to accept some loss of control?

SS: One of the most frequently discussed subjects within the blockchain world is the inverse relationship between decentralisation and resilience on the one hand and scalability on the other. There have been continuing advancements on that front so it may be becoming more possible to achieve scalability. But reading the roadmap of the different features you need, and understanding which technologies can deliver the best mix of those is the key question we're all grappling with.

The scalability challenge is probably the main one for any CBDC. It's hard to mimic some of this challenge in order to simulate how it would perform in a real world scenario, in which a CBDC is used across

the entire population of the country. Understanding the demands this would make of the technology is a significant challenge.

CO: Cees, as someone pioneering this technology in a private sector organisation, what solutions can you provide to meeting the scalability challenge while ensuring that the role of the central bank is respected and understood?

CVW: We are strongly in favour of a fully decentralised blockchain or DLT solution, because it is only if a DLT is deployed on a fully decentralised basis that you can trust that your view of your data is genuinely your copy of the ledger. This is important because it means you don't need to keep a shadow book that you have to keep comparing and aligning with the DLT, as you do with traditional central systems.

In practice, a blockchain solution sometimes starts with a very centralised set-up, where a fintech runs all the nodes and controls all the keys. But that doesn't make much sense. Instead, you need all the network participants to run their own nodes and control their private keys, with a decentralised consensus algorithm, which is what you have in the case of a wholesale CBDC. Only then can you extract the benefits of DLT. These mean that you have full trust that your shared data is correct and you no longer need to compare the books you have with the books of your counterparty. This is the process known as reconciliation, which is very inefficient.

CO: To wrap up, how do panellists think central banks will be using blockchain technology in five years' time?

CVW: I think their role will be confined to issuing and redeeming CBDCs and controlling their amount. The rest of the infrastructure will be decentralised, with banks running their own nodes, and with tasks like know-your-customer and anti-money laundering remaining the responsibility of the individual banks.

Coming back to the concerns participants expressed about scalability, I can only reiterate the point Sky made, which is that modern technology and consensus algorithms can easily process thousands of transactions per second.

SG: Because they are likely to issue CBDC using blockchain, it will be essential for central banks to keep up with the latest trends and innovations in technology, which are moving at unprecedented speed. An example is cross-border decentralised finance, known as defi, which is popular in the cryptocurrency world. It began with decentralised exchanges and automatic market makers, and is increasingly replacing human intervention with computer algorithms.

What's noteworthy about defi is that the pace of its evolution has far exceeded the reaction time of the authorities. A few days ago, one defi project received over $600m of cryptocurrency deposits in the space of a few hours. But one line of the code went wrong, allowing an infinite number of coins to be created and within a few hours the project had collapsed, losing 99% of its value. This example shows how irrational the defi market can be. Central banks must learn from incidents of this kind and maintain a close relationship with the private sector, and especially with fintech companies, to keep up with these radical changes.

TM: There's a high probability that a DLT ecosystem will grow up around central banks, and that we will see different types of financial market infrastructure taking shape based on DLT. The question for central banks will then be, how can they get central bank money on that DLT?

When it comes to a pure retail CBDC, I'm in the camp of those who believe you don't need a blockchain or a DLT and that it's more efficient to use different technology. I am working on a research project with David Chaum and Christian Grothoff from the University of Bern assessing the potential of issuing a retail CBDC, based on public key cryptography but not on blockchain technology.

SS: I agree that the key question is the ecosystem that grows up around this, and I believe we may come to see blockchain as the catalyst for innovation.

AS: I believe central banks will use blockchain technology in fields where they find it to be the most effective, but I don't see it having a special status. Instead, it will be one of a range of options open to central banks.

Coming back to what Cees said about ING's ambition of becoming a tech company with a banking licence, central banks' role will also have to change. They won't just be responsible for issuing prudential and consumer protection standards. Increasingly, they will also have to issue technical standards for the industry and for its partners and to determine minimum acceptable technological criteria as well. So it'll be a very exciting time ahead for all of us.

CO: Indeed. Many thanks to you all for your contributions. ●

3. What are the main motivations for issuing a CBDC?