

## The future monetary system

Speech by Hyun Song Shin

Economic Adviser and Head of Research, Bank for International Settlements

on the occasion of the Bank's Annual General Meeting  
in Basel on 26 June 2022

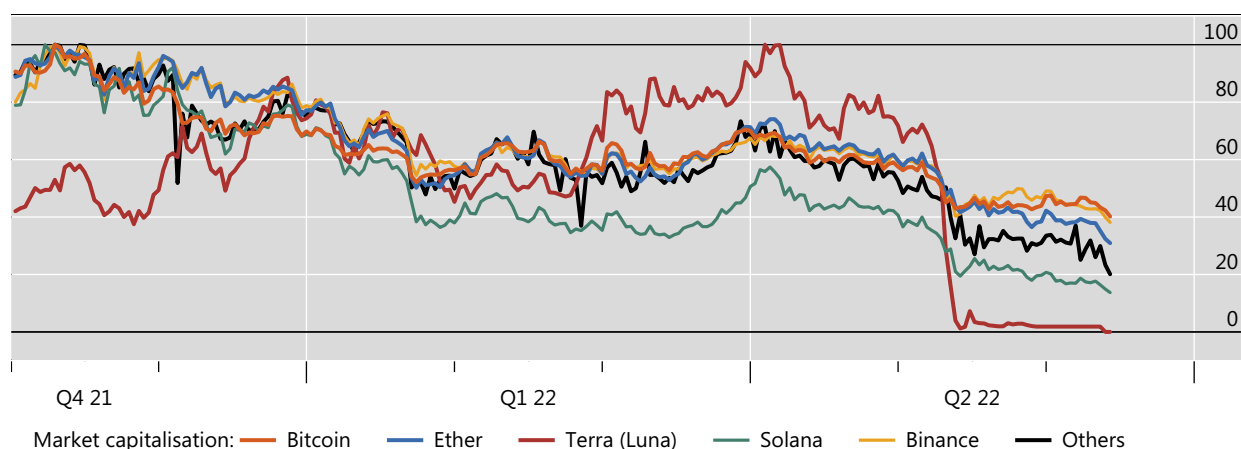
### Turmoil in crypto markets, and deeper structural flaws

We meet at a time of turmoil in the crypto universe. The collapse of the Terra stablecoin and of its twin coin Luna in May is only the most spectacular recent shock in the crypto sector. The ecosystem of crypto coins that add layers of leverage and illiquidity through the system is showing severe strain. The prices of Bitcoin and Ether have crashed, and many lesser-known coins have seen their prices drop by 90% or more relative to their peaks last year (Graph 1).

Crypto markets are in turmoil, with prices crashing and investors running to the exits

Peak = 100

Graph 1



The peak corresponds to the peak market capitalisation specific to each cryptocurrency over the period (Nov 2021–Jun 2022).

Sources: CoinGecko; BIS.

The sight of crashing prices and runs on illiquid crypto structures highlights the short-term risks to financial stability and consumer protection. Addressing these is indeed an urgent policy challenge. However, while we address these urgent challenges, we should not lose sight of the deeper structural flaws in crypto that make it unsuitable as the basis of a monetary system. We need to keep the longer-term structural issues on our dashboard as we think about the future monetary system. What are these deeper structural flaws of crypto as money?

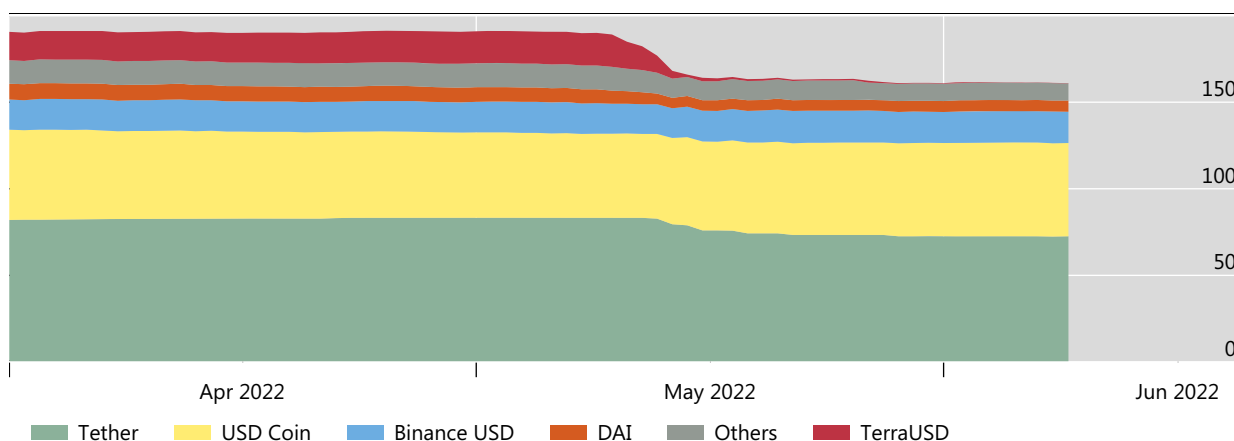
The first clue lies in the role played by stablecoins. The prevalence of stablecoins shows the pervasive need of crypto to piggyback on the credibility of the central bank. Stablecoins are cryptocurrencies that aim to maintain a stable value relative to traditional currencies, such as the

US dollar. Yet stablecoins are often far from stable. The market value of TerraUSD, which had been the third largest stablecoin, collapsed to nearly zero over a few days in May (Graph 2).

### The search for a nominal anchor: stablecoins promise stability, but the implosion of TerraUSD underscored inherent fragilities

In billions of US dollars

Graph 2



Sources: CoinGecko; BIS.

The fact that stablecoins play such a prominent role is a salient marker of crypto’s search for a nominal anchor. Crypto started by turning its back on central bank money, but it has quickly rediscovered the need for a stable unit of account – which is best provided by the stability of central bank money. The prevalence of stablecoins shows that if central bank money did not exist, it would need to be invented.

The same goes for money’s role as a medium of exchange. Money is a social convention; we accept money in transactions because we expect others to accept money in the future. Money is the perfect example of the benefits of network effects, which entail a virtuous circle of greater use and greater acceptance. This is why, typically, there is a “winner takes all” property of money. Central bank money emerges as the single money that wins general acceptance across an economy. Crypto does not work like that. Stablecoins are used as poker chips to facilitate transactions across more than 10,000 crypto coins, all competing for the attention of speculative buyers.

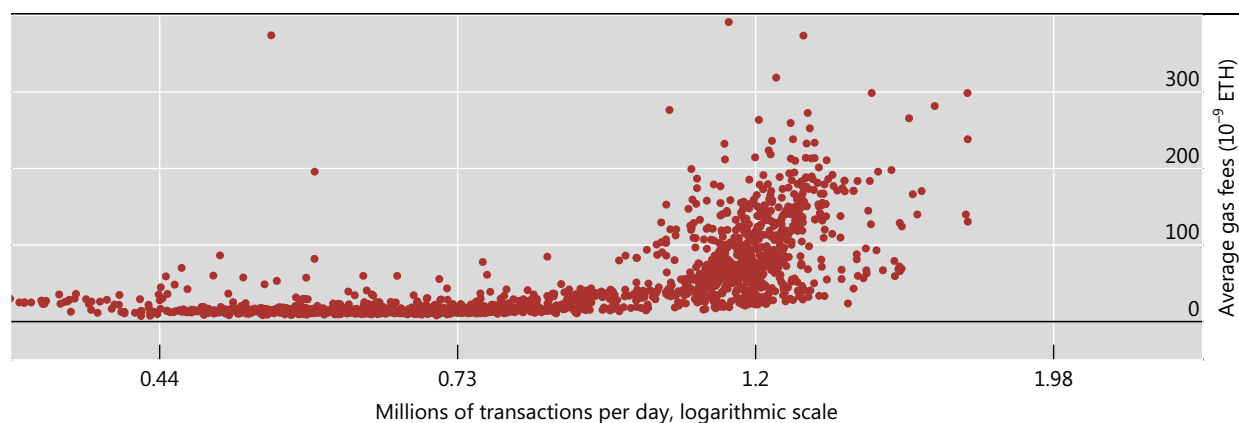
What is striking is this proliferation and the resulting fragmentation of the crypto universe. There is no “winner takes all” property that we would expect of something that serves as money. Instead, we have a severe form of fragmentation of the crypto universe, with many incompatible settlement layers jostling for a place in the limelight. Gone is any pretence that crypto money can serve a coordination role. Why is that?

The reason is that crypto runs under the banner of decentralisation, where settlement is done through consensus formed by validators. These validators can be miners as in Bitcoin, or large holders of coins – so-called whales – as in a proof of stake system. In the latter case, large coin holders make decisions like large shareholders in conventional firms. But whatever form these validators take, they are rewarded for their activities, and these rewards are key to giving them the

economic incentives to keep the system running properly. These rewards need to be large enough so that validators keep on validating. And one way that rewards are kept high is through congestion: when the crypto platform is used intensively by users, transaction costs (and hence rewards) skyrocket. This is seen for instance in the rising costs on Ethereum as transaction volumes increase (Graph 3). So, unlike money, which has the “winner takes all” property due to the virtuous circle of greater acceptance and greater use, crypto generates high costs, high rents to insiders and congestion. They open a gap for new entrants that boast higher capacity for transactions. Often this high capacity is achieved by cutting corners on security.

Network congestion leads to high gas fees on the Ethereum network

Graph 3



Sources: F Boissay, G Cornelli, S Doerr and J Frost, “Blockchain scalability and the fragmentation of crypto”, *BIS Bulletin*, no 56, June 2022; Etherscan; BIS.

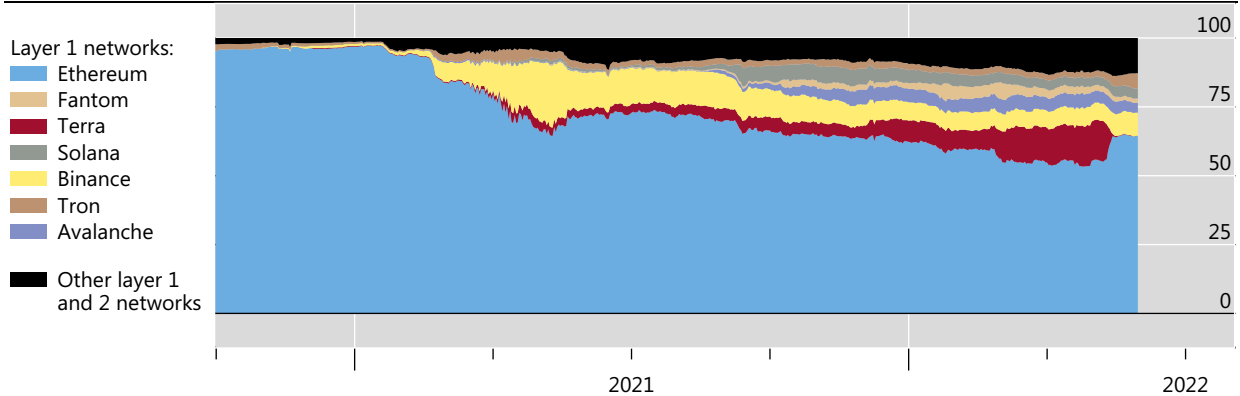
In fact, finding the right capacity at the outset is like balancing on a knife edge. Congestion is a feature, not a bug. It’s like a toll road collecting tolls from drivers. If capacity is too low and the tolls are too high, drivers move to other roads. But too much capacity means that no-one pays the tolls, which means that the system cannot be sustained.

To illustrate this point, look at the proliferation of different blockchains, or “layer 1” networks, in the decentralised finance (DeFi) sector. In late 2020, most DeFi applications ran on the Ethereum blockchain, where most collateral was posted. But over time, users moved increasingly to other blockchains, which exploited the gap created by congestion. By early May 2022, Ethereum made up only about half of the overall market. The Terra blockchain, shown in red here, was growing very rapidly and grabbing market share (Graph 4). However, all this came to an abrupt end when the Terra platform collapsed in May.

## Fragmentation of crypto: especially Terra was growing fast, up until its collapse<sup>1</sup>

As a percentage of total assets locked

Graph 4



<sup>1</sup> Based on total value locked, which corresponds to the aggregate of all the funds locked in a DeFi smart contract.

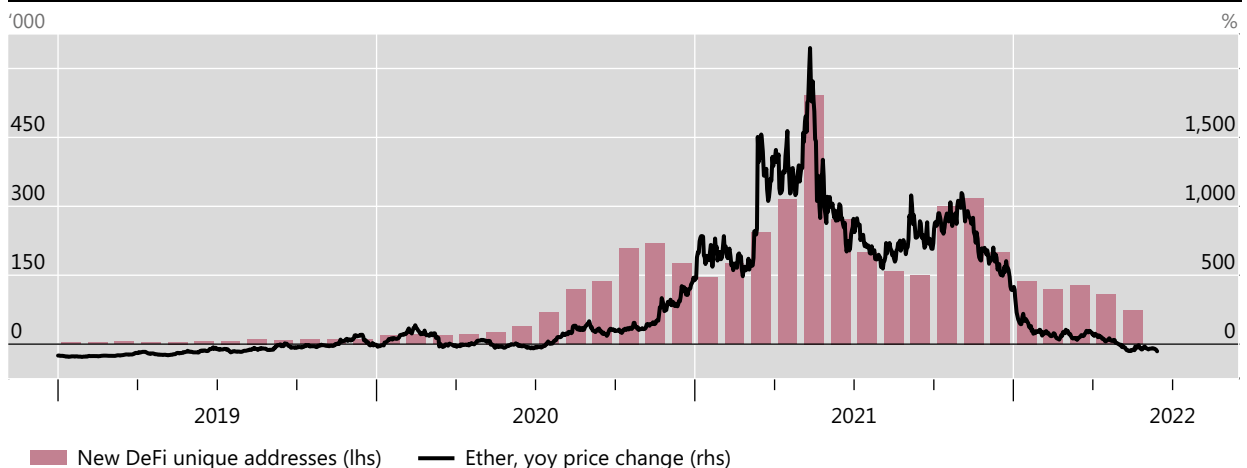
Sources: F Boissay, G Cornelli, S Doerr and J Frost, "Blockchain scalability and the fragmentation of crypto", *BIS Bulletin*, no 56, June 2022; DeFi Llama; BIS.

Money and its network effects should give rise to the property of "the more, the merrier": the more money meets general acceptance, the more it will be used. Instead, crypto illustrates of the opposite dictum; it's a case of "the more, the sorrier". The fact that crypto is so prone to fragmentation makes it unsuitable as the basis for the monetary system.

What is becoming clear in the turmoil in the crypto universe right now is that crypto only really works when coin prices are going up and there are inflows of new buyers of coins. Indeed, the number of new DeFi addresses follows the price action of the crypto coin itself (Graph 5). As we have seen over the last few weeks, when speculative inflows stop, the market can quickly unravel.

## The system is sustained by an influx of new users...

Graph 5



Sources: F Boissay, G Cornelli, S Doerr and J Frost, "Blockchain scalability and the fragmentation of crypto", *BIS Bulletin*, no 56, June 2022; @rchen8 via <https://dune.com/queries/2972/5739>; CryptoCompare.

When we look back, the rise of crypto over the last several years has been a remarkable spectacle. It highlights the place of technology in the popular imagination, and its galvanising role in debates on the shape of things to come. In this respect, crypto offers a tantalising glimpse of new arrangements and technical features. But as we argue in Chapter III of this year's Annual Economic Report, everything that can be done with crypto can be done better with central bank money – except, perhaps, for money laundering and ransomware attacks. And that is for good reason.

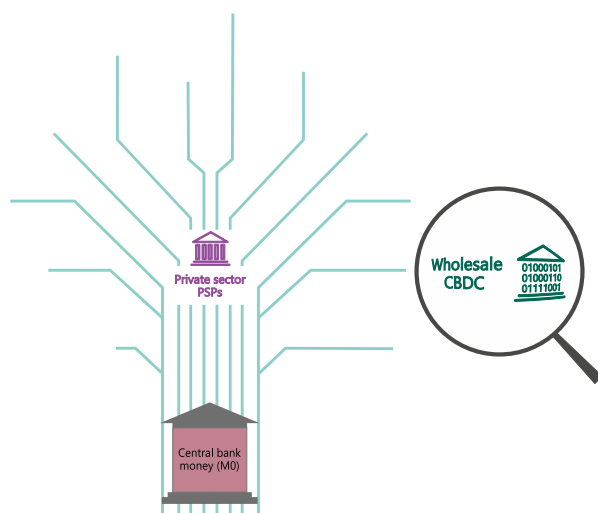
## A vision for the future monetary system

The vision for the future monetary system laid out in the chapter is the fusion of enhanced technical capabilities around the core of the trust provided by central bank money. Central banks are uniquely positioned to provide the core of the future monetary system. They issue central bank money, which serves as the unit of account in the economy. From the basic promise embodied in the unit of account, all other promises in the economy follow. The second fundamental role of the central bank, building on the first, is to provide the means for the finality of payments by using its balance sheet. The central bank is the trusted intermediary that debits the account of the ultimate payer and credits the account of the ultimate payee. Once the accounts are debited and credited in this way, the payment is final and irrevocable.

The metaphor that we use for the future monetary system is that of a tree. Its solid trunk is the central bank, and the tree supports a rich and vibrant ecosystem of services provided by private sector institutions and arrangements. The metaphor draws attention to the fact that the ecosystem is rooted in the settlement on the central bank's balance sheet.

What are the components of this monetary system?

As the foundation, we have central bank money, or M0, which supports the monetary system. Building on central bank money are the commercial banks and non-bank payment service providers (PSPs), who take on the customer-facing activities. Within this structure, we can envisage superior representation of central bank money available to banks and non-bank PSPs through wholesale CBDCs (Graph 6). If these wholesale CBDCs operate on distributed ledger technology (DLT), they could incorporate additional functionality such as atomic settlement and composability of transactions. These functionalities could be fully compatible with the requirement for using real names rather than hiding behind private keys (as in crypto).



Source: BIS.

How is finality achieved in permissioned DLT platforms? The mechanics can be explained through the simple analogy of a physical banknote. The recipient of a physical banknote wants to be assured that the note is genuine, not counterfeit. In a CBDC platform this can be done by proving the origin or “provenance” of the money. Crypto proves its provenance by publicly posting the full history of all transactions by everyone. When real names are used, such public posting would violate privacy and would be unsuitable as a payment system. No one needs to know where I buy my groceries. This is where cryptographic techniques such as zero-knowledge proofs (ZKPs) come in. Cryptographic techniques allow the payer to prove that the money was obtained from valid past transactions without having to post the full history of all transactions. Depending on the detailed implementation, a “notary” may also figure in the system to prevent the same digital token being spent twice; the central bank is a natural choice for this role.

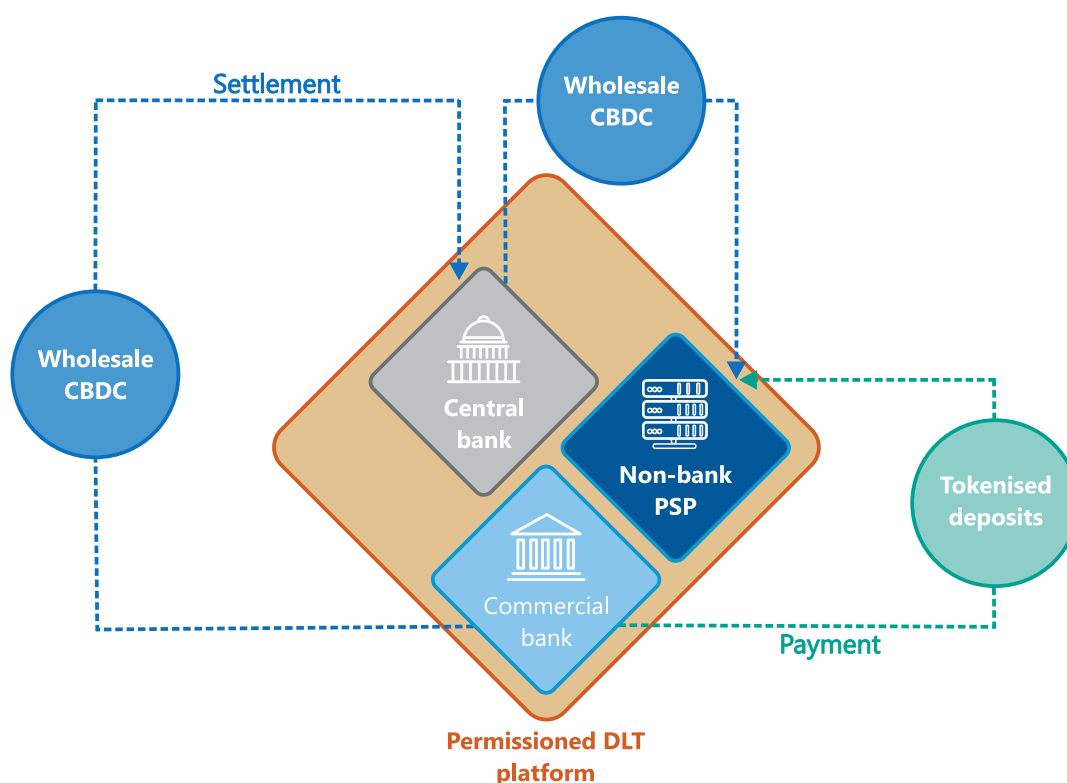
Whatever specific implementation is chosen, the point is that decentralisation and new capabilities can be achieved with all the benefits that come with central bank money. New capabilities may include programmability, or the ability to make payments conditional specific criteria being met. This can allow, for instance, for atomic settlement, whereby the two legs of a transaction are inseparable – either both sides go through, or none at all. Another capability is composability, or the capacity to combine together different functions (“money legos”). A third capability is tokenisation, or the creation of a digital representation of money or other assets. This could allow banks to offer tokenised deposits, which could be used for conditional payments. These transfers would be settled in central bank money.

How does this work? The classical notion of settlement by book entries of intermediaries can find new expression in DLT platforms where tokens are transferred in settlement, rather than through book entries. The economics remain the same, but the technological medium progresses. In this way, wholesale CBDCs could support the settlement of transfers of tokenised deposits.

For instance, the buyer of a house may wish to make a large, conditional payment to the seller of the house, but only when the title to the house is actually transferred. In turn, the seller wants to ensure that the title is transferred only when the money is received. They may do this with a tokenised deposit in a permissioned DLT system, together with a token that represents the house. In the background, the wholesale CBDC helps this transaction to settle, and these movements all occur in one bundle (Graph 7).

Payment with tokenised deposits settled with wholesale CBDC

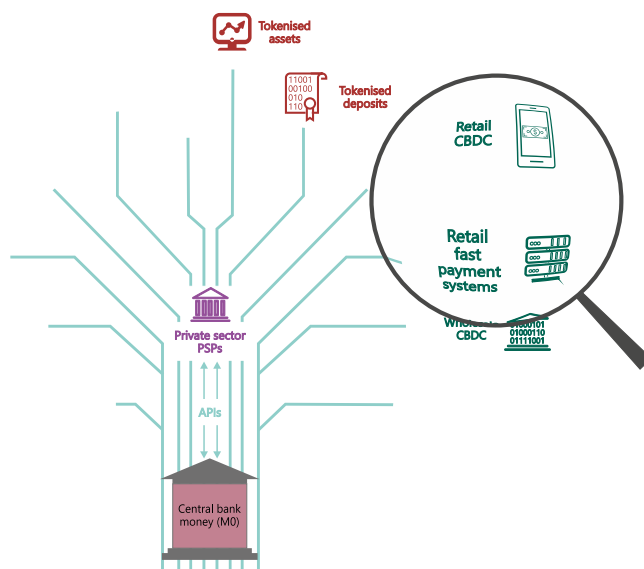
Graph 7



Source: BIS.

Or, to go even further, wholesale CBDCs could support the tokenisation of securities, such as stocks and bonds, or even real assets. This could enable fractional ownership of these assets and instant settlement, 24/7. By allowing private PSPs to offer these services in an open platform, central bank public goods could help to truly democratise finance.

So far, I have described wholesale applications. In parallel with wholesale solutions, financial inclusion can be enhanced in the retail domain through retail CBDCs and retail fast payment systems (FPS), both of which would allow for instant payments by households and businesses. As we discuss in the chapter, retail CBDCs and retail FPS bear a strong family resemblance. Both build on the interoperability enabled by application programming interfaces (APIs) that ensure interoperability of services provided by banks and non-bank PSPs. Interoperability ensures effective competition that lowers costs. The main difference between retail CBDCs and FPS is that CBDCs are a direct claim on the central bank, while an FPS only gives users access to the liabilities of banks and other PSPs.



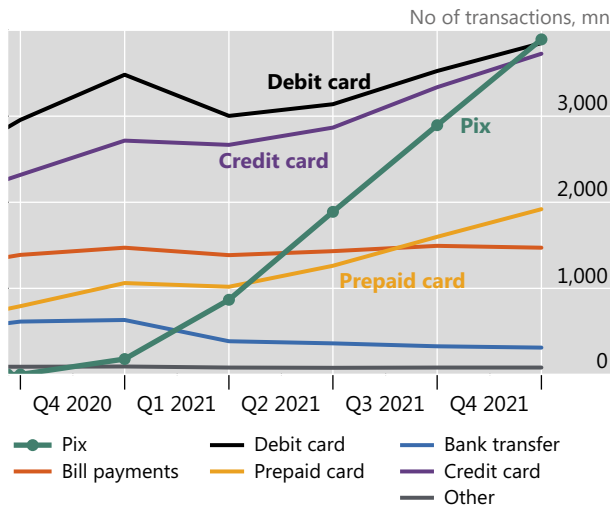
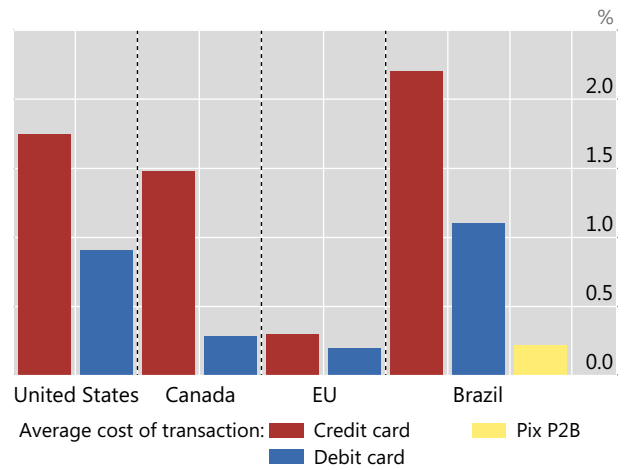
Source: BIS.

By creating an open, interoperable platform, retail CBDCs and FPS can allow for dramatic progress in lowering the cost of payments and in enhancing financial inclusion. For example, in Brazil, the Pix instant payment system was adopted by two thirds of the adult population in just over a year after its launch. In terms of use, it has now surpassed credit and debit cards by transaction volume (Graph 9.A). A full 50 million Brazilians have made a digital payment for the first time. For merchants, accepting Pix payments costs only 22bp. That is just one tenth the cost of accepting credit card payments (Graph 9.B). Work by various central banks shows that retail CBDCs hold similar promise, particularly if they are designed with interoperability and financial inclusion as key goals.



**Retail fast payment systems hold promise for rapid adoption and low costs**

Graph 9

**A. Pix is gaining market share rapidly in Brazil's growing digital payments market...<sup>1</sup>**

**B. ...and enables payment services at very low cost to users and merchants<sup>2</sup>**


P2B = peer-to-business

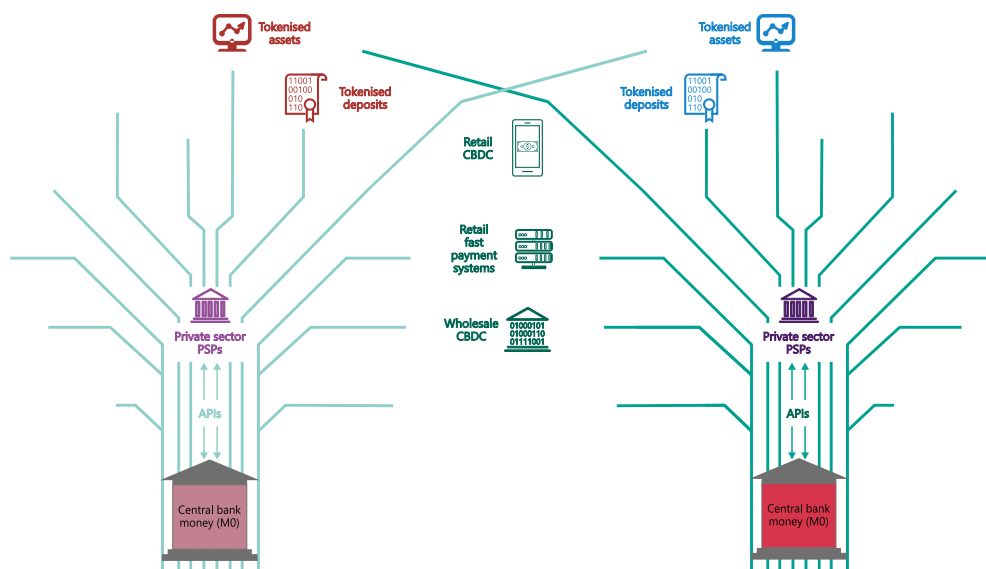
<sup>1</sup> Excluding recurrent utility payments. <sup>2</sup> For the United States, Canada and the EU, average of interchange fees on credit and debit cards. Total cost to merchants may be higher.

 Sources: A Duarte, J Frost, L Gambacorta, P Koo Wilkens and H S Shin (2022): "Central banks, the monetary system and public payment infrastructures: lessons from Brazil's Pix", *BIS Bulletin*, no 52, March; F Hayashi and V Nimmo (2021): "Credit and debit card interchange fees in various countries. August 2021 update", *Federal Reserve Bank of Kansas City, Payments System Research*; Central Bank of Brazil.

We started with a tree as the organising metaphor. When we zoom out, we get to the canopy of the forest where the tree branches meet. The canopy embodies an important additional component of the future monetary system in the form of multi-CBDC platforms (Graph 10). Such arrangements bring together CBDCs from several central banks all transacting on the same platform. These arrangements involve more than one central bank and hence more than one currency. This is why such arrangements are governed on DLT platforms.

CBDCs can also interlink across borders, supporting economic integration, like the canopy of a forest

Graph 10

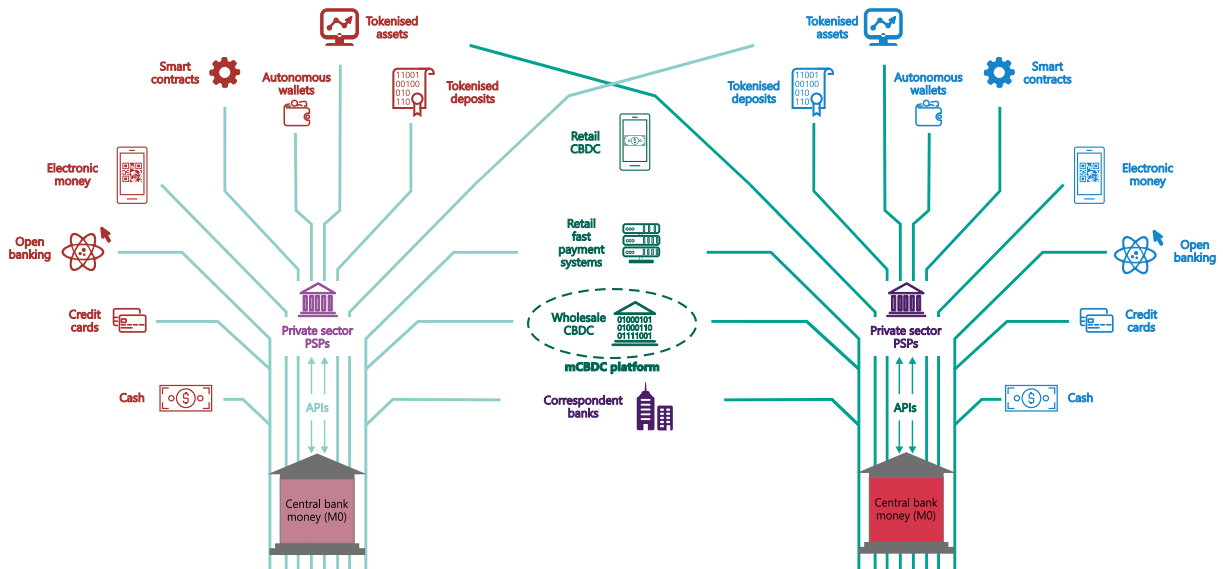


Source: BIS.

The BIS Innovation Hub has coordinated trials of several mCBDC platforms. In a new report, it has drawn initial lessons on their design and implementation. The early trials open the prospect of examining richer ecosystems with a diverse range of private sector service providers (Graph 11). The full extent of the possible innovations is impossible to foresee, but one thing is for sure. All of them will be supported by the tree; firmly rooted in the ultimate settlement on the central bank's balance sheet.

A strong canopy supports the global monetary (eco)system

Graph 11



Source: BIS.

## Conclusion

Let me conclude.

Central banks, as guardians of the monetary system, are embarked on a long journey in fulfilling the vision of the future monetary system. The objective is to put in place arrangements that anticipate future developments rather than merely to react to past developments. So, while the crypto universe is gripped in turmoil and attracting all the headlines, it is incumbent on us in the central bank community to look beyond the headlines to think about these longer-term goals.