

III. The future monetary system

Key takeaways

- A burst of creative innovation is under way in money and payments, opening up vistas of a future digital monetary system that adapts continuously to serve the public interest.
- Structural flaws make the crypto universe unsuitable as the basis for a monetary system: it lacks a stable nominal anchor, while limits to its scalability result in fragmentation. Contrary to the decentralisation narrative, crypto often relies on unregulated intermediaries that pose financial risks.
- A system grounded in central bank money offers a sounder basis for innovation, ensuring that services are stable and interoperable, domestically and across borders. Such a system can sustain a virtuous circle of trust and adaptability through network effects.
- New capabilities such as programmability, composability and tokenisation are not the preserve of crypto, but can instead be built on top of central bank digital currencies (CBDCs), fast payment systems and associated data architectures.

Introduction

Every day, people around the world make more than 2 billion digital payments.¹ They pay for goods and services, borrow and save and engage in a multitude of financial transactions. Every time they do so, they rely on the monetary system – the set of institutions and arrangements that surround and support monetary exchange.

At the heart of the monetary system stands the central bank. As the central bank issues money and maintains its core functions, trust in the monetary system is ultimately grounded in trust in the central bank. However, the central bank does not operate in isolation. Commercial banks and other private payment service providers (PSPs) execute the vast majority of payments and offer customer-facing services. This division of roles promotes competition and gives full play to the ingenuity and creativity of the private sector in serving customers. Indeed, private sector innovation benefits society precisely because it is built on the strong foundations of the central bank.

The monetary system with the central bank at its centre has served society well. Yet digital innovation is expanding the frontier of technological possibilities, placing new demands on the system.

Far-reaching innovations, such as those in the crypto universe, entail a radical departure. The crypto universe builds on the premise of decentralisation. Rather than relying on central bank money and trusted intermediaries, crypto envisages checks and balances provided by a multitude of anonymous validators so as to keep the system self-sustaining and free from the influence of powerful entities or groups. Decentralised finance, or “DeFi”, seeks to replicate conventional financial services within the crypto universe. These services are enabled by innovations such as programmability and composability (see glossary) on permissionless blockchains. Such systems are “always on”, allowing for global transactions 24/7, based on open-source code and knowing no borders.

However, recent events have revealed a vast gulf between the crypto vision and its reality. The implosion of the TerraUSD stablecoin and the collapse of its twin coin Luna have underscored the weakness of a system that is sustained by selling coins for speculation. In addition, it is now becoming clear that crypto and DeFi have deeper structural limitations that prevent them from achieving the levels of efficiency, stability or integrity required for an adequate monetary system. In particular, the crypto universe lacks a nominal anchor, which it tries to import, imperfectly, through stablecoins. It is also prone to fragmentation, and its applications cannot scale without compromising security, as shown by their congestion and exorbitant fees. Activity in this parallel system is, instead, sustained by the influx of speculative coin holders. Finally, there are serious concerns about the role of unregulated intermediaries in the system. As they are deep-seated, these structural shortcomings are unlikely to be amenable to technical fixes alone. This is because they reflect the inherent limitations of a decentralised system built on permissionless blockchains.

This chapter sets out an alternative vision for the future, one that builds on central bank public goods. This will ensure that innovative private sector services are securely rooted in the trust provided by central bank money.

Scaling on the back of network effects, central bank digital currencies (CBDCs) and retail fast payment systems (FPS) are well placed to serve the public interest through greater convenience and lower costs, while maintaining the system's integrity. Decentralisation and permissioned distributed ledger technology (DLT) can also play a constructive role, eg when central banks work together in multi-CBDC arrangements. These innovative payment rails are fully compatible with programmability, composability and tokenisation to support faster, safer and cheaper payments and settlement, both within and across borders. In this way, the future monetary system will be adaptable, allowing private sector innovation to flourish while avoiding the drawbacks of crypto. Such initiatives could open up a new chapter in the global monetary system.

This chapter is organised as follows. To set the stage, it first describes today's monetary system and the high-level objectives it needs to achieve, and to what extent changes in technology and the economic environment have opened up room for improvement. The next section discusses the promise and pitfalls of crypto and DeFi innovations. The chapter then discusses a vision for the future monetary system, built on central bank public goods. The final section concludes.

What do we want from a monetary system?

The monetary system is the set of institutions and arrangements that supports monetary exchange. It consists of money and payment systems.² What is required from such a system to serve society? While there is no canonical list of necessary features, a number of high-level goals stand out (Table 1, first column).

To ensure the **safety and stability** of the system, money needs to fulfil three functions: as a store of value, a unit of account and a medium of exchange. Where the monetary system relies on key nodes or entities (whether public or private), they need to be **accountable**, through specific mandates for public authorities and through proper regulation and supervision for private entities. The monetary system should be **efficient**, enabling reliable, fast payments to support economic transactions both at scale and also at low cost. Access to basic payments services at affordable prices, in particular transaction accounts, should be universal to spread the benefits of economic activity, promoting **financial inclusion**. Not least, the system must protect privacy as a fundamental right, and provide **user control** over

High-level goals of the monetary system

Table 1

High-level goals	Today's monetary system	Crypto universe (to date)	Future monetary system (vision)
1. Safety and stability – money needs to perform fundamental functions: as a store of value, unit of account and medium of exchange	Sovereign currencies can offer price stability, and public oversight has helped achieve safe and robust payment systems	Cryptocurrencies do not perform money's fundamental functions, and stablecoins need to import their credibility	Innovations grounded in trust in the central bank feature stable sovereign currencies and safe payment systems
2. Accountability – public mandates and regulation should ensure that key nodes in the system are accountable and transparent to users and society	Supervision, regulation and oversight tackle risks, promote competition and protect consumers, but public mandates may need to adapt to change	Crypto and DeFi create a parallel financial system to circumvent regulation, with no accountability to the general public	Clear mandates and regulation balance risks and benefits so as to harness innovation and stimulate efficiency
3. Efficiency – the system should provide low-cost, fast payments and throughput	Domestic payments are often expensive and financial institutions collect rents	High congestion and rents lead to costly transactions and new speculative incentives	New payment systems can significantly reduce payment costs and rents, supporting economic activity
4. Inclusion – the system should ensure universal access to basic services at affordable prices	Many people lack access to transaction accounts and digital payment instruments	Crypto and DeFi have not yet served to enhance financial inclusion	New service providers and interfaces can address barriers to inclusion and better serve the unbanked
5. User control over data – data governance arrangements should ensure users' privacy and control over data	Users trust intermediaries to keep data safe, but they do not have sufficient control over their data	Transactions are public on the blockchain – which will not work with "real names"	New data architectures can give users privacy and control over their data
6. Integrity – the system should avoid illicit activity such as money laundering, financing of terrorism and fraud	Payment systems are subject to extensive regulation, but illicit activity persists in cash and account fraud	Pseudo-anonymity is prone to abuse by illicit actors, and the DeFi sector is rife with fraud and theft; identification is needed	New technologies can help to better prevent illicit activity and improve on today's systems
7. Adaptability – the system should anticipate future developments and users' needs and foster competition and innovation	Payment systems are adapting to demands, but are not yet at the technological frontier	Programmability, composability and tokenisation give scope for new functions	Programmability, composability and tokenisation can be offered in a CBDC or through tokenised deposits
8. Openness – the system should allow for seamless cross-border use	Despite progress, cross-border payments are still slow, opaque and expensive	DeFi is by nature borderless and allows global transactions, but without adequate oversight	Multi-CBDC arrangements and other reforms mean cheaper, faster and safer cross-border transactions

Green denotes that a policy goal is broadly fulfilled, yellow that there is room for improvement and red that it is not generally fulfilled.

Source: BIS.

financial data. The **integrity** of the system must be protected, by guarding against illicit activity such as money laundering, financing of terrorism and fraud.

The monetary system is not just a snapshot of the economy as it exists today; it needs to evolve with structural changes in the economy and society. For this reason, the means of reaching the high-level goals set out in Table 1 should evolve with the monetary system itself and the technology underpinning it. In short, the monetary system must be **adaptable**: it should *anticipate* future developments and user needs. It must be attuned to technological developments and respond to the changing demands of households and businesses, and it must foster competition and innovation. To better serve an increasingly interconnected world, the monetary

system also needs to be **open**, interoperable and flexible, both domestically and across borders. Just as economic transactions transcend borders, the monetary system will need to serve a seamless web of interconnected entities, rather than sparsely connected islands of activity.

Today's monetary system has come some way towards these high-level goals, but there is still some way to go. Changes in users' needs and the concomitant shifts in technology have pointed to areas for improvement (Table 1, second column). Current payment services can sometimes be cumbersome and costly to use, in part reflecting a lack of competition. Cross-border payments are particularly expensive, opaque and slow: they usually involve one or more correspondent banks to settle a transaction, using ledgers built on different technologies.³ In addition, a large share of adults, especially in emerging market and developing economies, still have no access to digital payment options. But a globalised world that features an ever-growing digital economy requires a monetary system that allows everyone to make financial transactions domestically and globally in a safe, sound and efficient way. Catering to these changes in the demands that society places in the monetary system calls for advances in technology and institutional arrangements.

The promise and pitfalls of crypto

The crypto universe is in turmoil. The implosion of the TerraUSD stablecoin and its twin coin Luna is only the most spectacular failure in the sector, with many lesser-known coins having seen a collapse in price of more than 90% relative to their peak in 2021. Crypto commentators have begun to refer to recent events as the start of a "crypto winter".

As dramatic as these recent price collapses have been, focusing on the price action alone diverts attention away from the deeper structural flaws in crypto that render them unsuitable as the basis for a monetary system that serves society (Table 1, third column).

The prevalence of stablecoins, which attempt to peg their value to the US dollar or other conventional currencies, indicates the pervasive need in the crypto sector to piggyback on the credibility provided by the unit of account issued by the central bank. In this sense, stablecoins are the manifestation of crypto's search for a nominal anchor. Stablecoins resemble the way that a currency peg is a nominal anchor for the value of a national currency against that of an international currency – but without the institutional arrangements, instruments, commitments and credibility of the central bank operating the peg. Providing the unit of account for the economy is the primary role of the central bank. The fact that stablecoins must import the credibility of central bank money is highly revealing of crypto's structural shortcomings. That stablecoins are often less stable than their issuers claim shows that they are at best an imperfect substitute for sound sovereign currency.

Stablecoins also play a key role in facilitating transactions *across* the plethora of cryptocurrencies that have mushroomed in recent years. At the latest count there were over 10,000 coins on many different blockchains that competed for the attention of speculative buyers.

The proliferation of coins reveals another important structural flaw with crypto – namely the *fragmentation* of the crypto universe, with many incompatible settlement layers jostling for a place in the spotlight.

This fragmentation of the crypto universe raises serious questions as to the suitability of crypto as money. Money is a coordination device that serves society through its strong network effects. The more users flock to a particular form of money, the more users it attracts. For this reason, money has the "winner takes all"

property, in which network effects lead to the dominance of one version of money as the transactions medium that is generally accepted throughout the economy. The fragmentation of the crypto universe points in a very different direction: as explained below, the more users flock to one blockchain system, the worse is the congestion and the higher are the transaction fees, opening the door to the entry of newer rivals who may cut corners on security in favour of higher capacity. So, rather than the familiar monetary narrative of “the more the merrier”, crypto displays the property of “the more the sorrier”. It is this tendency toward fragmentation that is perhaps crypto’s greatest flaw as the basis for a monetary system.

Nevertheless, crypto offers a glimpse of potentially useful features that could enhance the capabilities of the current monetary system. These stem from the capacity to combine transactions and to execute the automatic settlement of bundled transactions in a conditional manner, enabling greater functionality and speed. Thus, one question to consider is how the useful functionalities of crypto can be incorporated in a future monetary system that builds on central bank money.

In order to develop the deeper insights on the flaws and possibilities of crypto, it is instructive first to explain some basic building blocks of the crypto world.

The building blocks of crypto

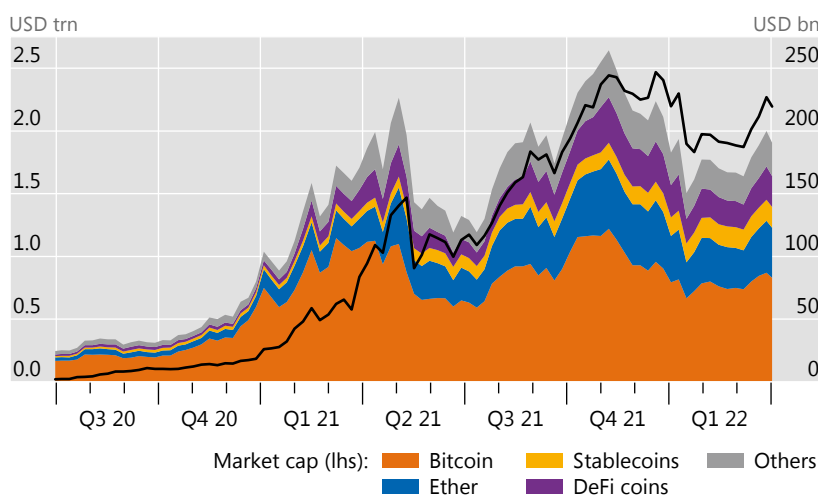
Crypto purports to reduce the heft of intermediaries and has been described as a broader movement toward decentralised finance and even a more decentralised internet (“Web 3.0” or “Web3”). The touted benefit is to democratise finance, granting users greater control over their data. Prior to the recent crash, the market size of cryptocurrencies and DeFi had expanded rapidly (Graph 1).

Crypto has its origin in Bitcoin, which introduced a radical idea: a decentralised means of transferring value on a permissionless blockchain. Any participant can act as a validating node (see glossary) and take part in the validation of transactions on a public ledger (ie the permissionless blockchain). Rather than relying on trusted

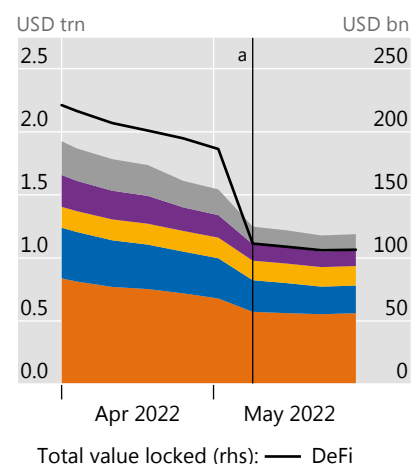
Market size of cryptocurrencies and DeFi¹

Graph 1

A. Rapid growth in crypto and DeFi...



B. ...followed by a collapse



^a TerraUSD and Luna collapse starting on 9 May 2022.

¹ See technical annex for details.

Sources: CoinGecko; Defi Llama; BIS.

intermediaries (such as banks), record-keeping on the blockchain is performed by a multitude of anonymous, self-interested validators.

Transactions with cryptocurrencies are verified by decentralised validators and recorded on the public ledger. If a seller wants to transfer cryptocurrencies to a buyer, the buyer (whose identity is hidden behind their cryptographic digital signature) broadcasts the transaction details, eg transacting parties, amount or fees. Validators (in some networks called “miners”) compete to verify the transaction, and whoever is selected to verify then appends the transaction to the blockchain. The updated blockchain is then shared among all miners and users. The history of all transactions is hence publicly observable and tied to specific wallets, while the true identities of the parties behind transactions (ie the owners of the wallets) remain undisclosed. By broadcasting all information publicly, the system verifies that the transaction is consistent with the history of transfers on the blockchain, ie that the cryptocurrency actually belongs to the seller and has not been double-spent.

However, for a decentralised governance system, economic incentives are key. The limits of the system are set by the laws of economics rather than the laws of physics. In other words, not only the technology but also the incentives need to work. Miners (or validators) are compensated with monetary rewards for performing their tasks according to the rules so that the system becomes self-sustaining. Rewards, paid in crypto, can come in the form of transaction fees but can also stem from rents that accrue to “staking” one’s coins in a proof-of-stake blockchain. The larger the stake, the more often a node will serve as validator, and the larger the rents.

Since the advent of Bitcoin in 2009, many other blockchains and associated crypto coins have entered the scene, most notably Ethereum, which provides for the use of “smart contracts” and “programmability” (see glossary). Smart contracts, or self-executing code that triggers an action if some pre-specified conditions are met, can automate market functions and obviate the intermediaries that were traditionally required to make decisions. As the underlying code is publicly available, it can be scrutinised, making smart contracts transparent and reducing the risk of manipulation. An important feature of smart contracts is their composability, or the capacity to combine different components in a system. Users can perform complex transactions on the same blockchain by combining multiple instructions within one single smart contract – “money legos”. They can create a digital representation of assets through “tokenisation” (see glossary). As smart contracts cannot directly access information that resides “off-chain”, ie outside the specific blockchain, they require mediators to provide such data (so-called oracles).⁴

Newer blockchains, with Terra (before its collapse) being a prominent example, have been touted as “Ethereum killers” in that they boast higher capacity and larger throughput (see glossary). However, these changes bring new problems. Capacity is often increased through greater centralisation in the validation mechanisms, weakening security and concentrating the benefits for insiders, as explained below.⁵

Stablecoins in search of a nominal anchor

A key development in the crypto universe is the rise of decentralised finance, or “DeFi”. DeFi offers financial service and products, but with the declared objective of refashioning the financial system by cutting out the middlemen and thereby lowering costs.⁶ To this end, DeFi applications publicly record pseudo-anonymous transactions in cryptocurrencies on permissionless blockchains. “Decentralised applications” (dApps) featuring smart contracts allow transactions to be automated. To reach consensus, validators are incentivised through rewards.

While the DeFi ecosystem is evolving rapidly, the main types of financial activity continue to be those already available in traditional finance, such as lending,

trading and insurance.⁷ Lending platforms let users lend out their stablecoins with interest to borrowers that post other cryptocurrencies as collateral. Decentralised exchanges (DEXs) represent marketplaces where transactions occur directly between cryptocurrency or stablecoin traders, with prices determined via algorithms. On DeFi insurance platforms, users can insure themselves against eg the mishandling of private keys, exchange hacks or smart contract failures. As activities almost exclusively involve exchanging one stablecoin or cryptocurrency for another, and do not finance productive investments in the real economy, the system is mostly self-referential.

Stablecoins play a key role in the DeFi ecosystem. These are so-called because they are usually pegged to a numeraire, such as the US dollar, but can also target the price of other currencies or assets (eg gold). In this sense, they often import the credibility provided by the unit of account issued by the central bank. Their main use case is to overcome the high price volatility and low liquidity of unbacked cryptocurrencies, like Bitcoin. Their use also avoids frequent conversion between cryptocurrencies and bank deposits in sovereign currency, which is usually associated with significant fees. Because stablecoins are used to support a wide range of DeFi activities, turnover in stablecoins generally dwarfs that of other cryptocurrencies.

The two main types of stablecoin are asset-backed and algorithmic. Asset-backed stablecoins, such as Tether, USD Coin and Binance USD, are typically managed by a centralised intermediary who invests the underlying collateral and coordinates the coins' redemption and creation. Assets can be held in government bonds, short-term corporate debt or bank deposits, or in other cryptocurrencies. In contrast, algorithmic stablecoins, such as TerraUSD before its implosion, rely on complex algorithms that automatically rebalance supply to maintain their value relative to the target currency or asset. To avoid reliance on fiat currency, they often do so by providing users with an arbitrage opportunity relative to another cryptocurrency.

Despite their name, stablecoins – in particular, algorithmic ones – are less stable than their issuers claim. In May 2022, TerraUSD entered a death spiral, as its value dropped from \$1 to just a few cents over the course of a few days (see Box A). In the aftermath, other algorithmic stablecoins came under pressure. But so did some asset-backed stablecoins, which have seen large-scale redemptions, temporarily losing their peg in the wake of the shock. Redemptions were more pronounced among stablecoins whose issuers did not disclose the composition of reserve assets in detail, presumably reflecting investors' worries that such issuers might not be able to guarantee conversion at par.

Indeed, commentators have warned for some time that there is an inherent conflict of interest in stablecoins, with an incentive for issuers to invest in riskier assets. Economic history is littered with attempts at private money that failed, leading to losses for investors and the real economy. The robustness of stablecoin stabilisation mechanisms depends crucially on the quality and transparency of their reserve assets, which are often woefully lacking.⁸

Yet even if stablecoins were to remain stable to some extent, they lack the qualities necessary to underpin the future monetary system. They must import their credibility from sovereign fiat currencies, but they benefit neither from the regulatory requirements and protections of bank deposits and e-money, nor from the central bank as a lender of last resort. In addition, they tie up liquidity and can fragment the monetary system, thus undermining the singleness of the currency.⁹ As stablecoins are barely used to pay for real-world goods and services, but underpin the largely self-referential DeFi ecosystem, some have questioned whether stablecoins should be banned.¹⁰ As will be discussed below, there is more promise in sounder representations of central bank money and liabilities of regulated issuers.

The collapse of the TerraUSD stablecoin

The implosion of TerraUSD (UST) highlights inherent fragilities in some versions of stablecoins. The use of UST grew rapidly over 2021–22 so that, prior to its collapse, it was the third largest stablecoin, with a peak market capitalisation of \$18.7 billion. An *algorithmic stablecoin*, it maintained value by adjusting supply in an automated arbitrage trading strategy with another cryptocurrency, Luna, on the Terra blockchain. UST aimed to keep a one-for-one peg to the US dollar by being convertible into one dollar's worth of Luna, and vice versa. For example, should Terra fall to 99 cents, a user could purchase UST on an exchange for 99 cents and then exchange their UST for \$1 worth of new units of Luna on the Terra platform. A crucial aspect of this arrangement was that users would only be willing to exchange UST into Luna if Luna's market capitalisation exceeded that of UST. As Luna had no intrinsic value, its valuation stemmed primarily from the influx of speculative users into the Terra ecosystem. To attract new users, the associated lending protocol Anchor offered a deposit rate of around 20% on UST. As long as users had confidence in the stable value of UST and sustained market capitalisation of Luna, the system could be sustained. The Terra/Luna pairing was regarded as being especially significant as it promised to offer a "self-levitating" version of money that did not piggyback on real-world collateral assets.

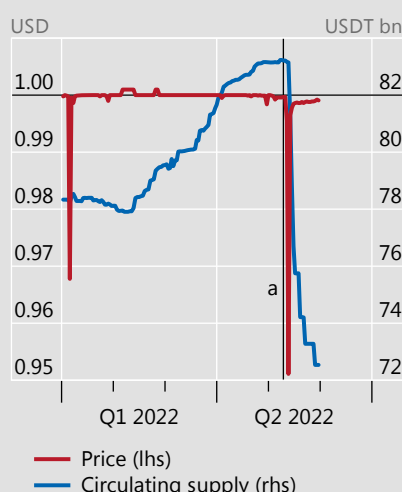
The TerraUSD implosion and fragilities in stablecoins

Graph A1

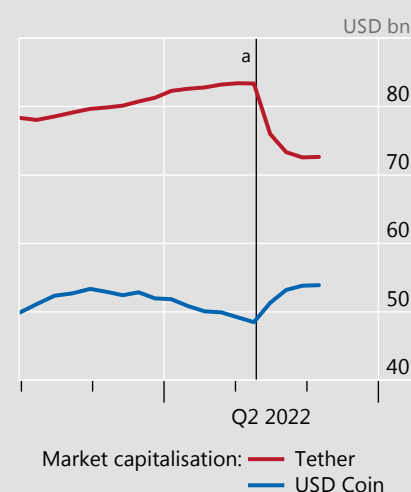
A. Terra and Luna coins dropped in value rapidly



B. Tether briefly lost its peg and suffered \$10bn in outflows¹



C. Investors moved to USD Coin and other asset-backed stablecoins



^a TerraUSD and Luna collapse starting on 9 May 2022.

¹ See technical annex for details.

Sources: CoinGecko; CryptoCompare; Messari; BIS.

However, this hope proved unfounded. Once investors lost confidence in the sustainability of the system, the arrangement unravelled. In May 2022, the value of UST plummeted to almost zero (Graph A1.A). As UST dropped below its peg, a classic run dynamic took hold as investors sought to redeem their funds. Users burned their UST on a large scale to mint \$1 worth of new Luna, in the hope of selling Luna as long as it still had some value. However, given the size and speed of the shock, confidence evaporated, meaning that there were not enough parties willing to buy all the newly minted Luna coins – and so the price of Luna collapsed.

The UST/Luna implosion spilled over to the largest stablecoin, Tether, which dropped to a value of \$0.95 before recovering. It saw outflows of over \$10 billion in the subsequent weeks (Graph A1.B). The de-pegging has been linked to Tether's unwillingness to provide details about its reserve portfolio: investors worried about whether Tether had enough high-quality assets that could be liquidated to support the peg. This argument is supported by the inflows experienced by the regulated stablecoin USDC (with better documented reserves), with funds probably coming from Tether (Graph A1.C).

Structural limitations of crypto

In addition to the immediate concerns around stability, crypto suffers from the inherent limitations of permissionless blockchains, which lead inevitably to the system's fragmentation, accompanied by congestion and high fees.¹¹ Tracing the reasons for fragmentation is revealing, as these highlight that the limitations are not technological but rather stem from the system's incentive structure.

Self-interested validators are responsible for recording transactions on the blockchain. However, in the pseudo-anonymous crypto system, they have no reputation at stake and cannot be held accountable under the law. Instead, they must be incentivised through monetary rewards that are high enough to sustain the system of decentralised consensus. Honest validation must yield higher returns than the potential gains from cheating. Should rewards fall too low, individual validators would have an incentive to cheat and steal funds. The consensus mechanism would fail, jeopardising overall security.

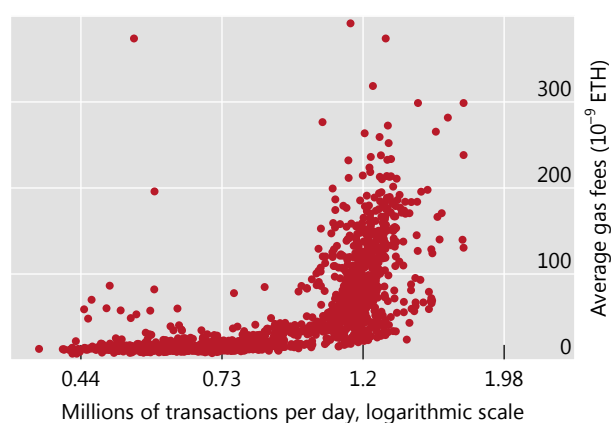
The only way to channel rewards to validators, thus maintaining incentives, is to limit the capacity of the blockchain, thus keeping fees high, sustained by congestion. As validators can choose which transactions are validated and processed, periods of congestion see users offering higher fees to have their transactions processed faster (Graph 2.A).¹²

The limited scale of blockchains is a manifestation of the so-called scalability trilemma. By their nature, permissionless blockchains can achieve only two of three properties, namely scalability, security or decentralisation (Graph 3). Security is enhanced through incentives and decentralisation, but sustaining incentives via fees entails congestion, which limits scalability. Thus, there is a mutual incompatibility between these three key attributes, preventing blockchains from adequately serving the public interest.

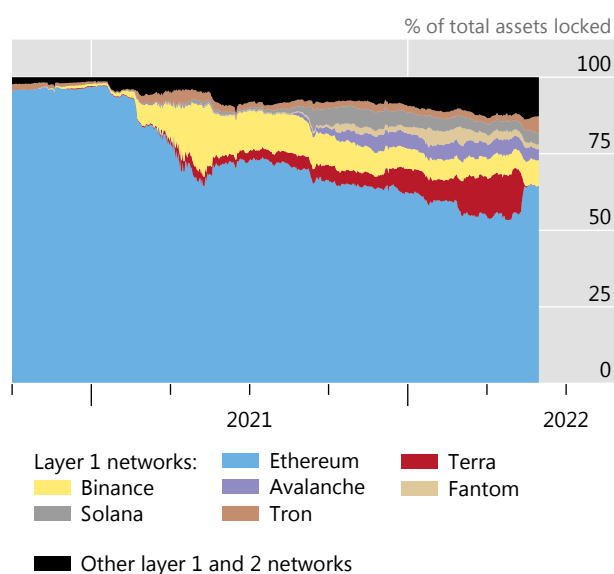
Blockchain congestion leads to fragmentation

Graph 2

A. Network congestion leads to high fees on the Ethereum network¹

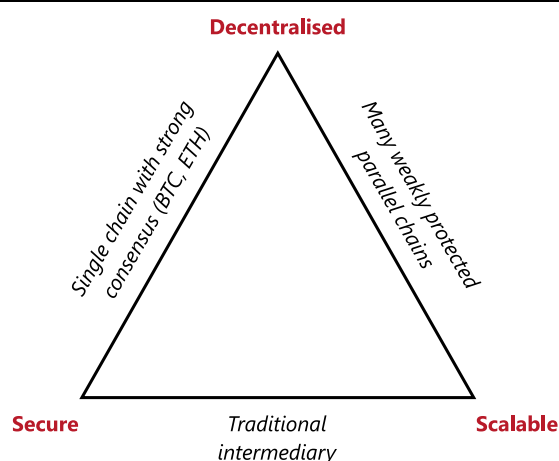


B. Fragmentation of layer 1 blockchains²



¹ See technical annex for details. ² Based on total value locked, which corresponds to the aggregate of all the funds locked in a DeFi smart contract.

Sources: Boissay et al (2022); DeFi Llama; Etherscan; BIS.



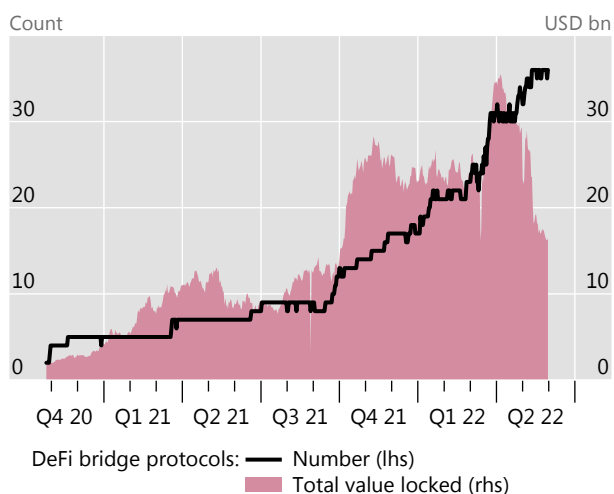
Sources: Auer et al (2021); Buterin (2021).

The limited scalability of blockchains has fragmented the crypto universe, as newer blockchains that cut corners on security have entered the fray. The Terra blockchain is just the most prominent of a horde of new entrants (Graph 2.B). Even as recently as the beginning of 2021, Ethereum accounted for almost all of the total assets locked. By early May 2022, this share had already dropped to 50%. The widening wedge (in red) accounted for by the failed Terra blockchain is particularly striking. Terra's collapse highlights the tendency of the crypto universe to fragment through its vulnerability to new entrants that prioritise market share and capacity at the expense of decentralisation and security.

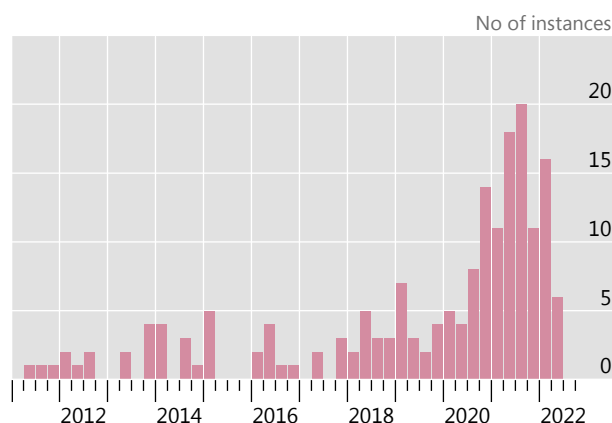
A system of competing blockchains that are not interoperable but sustained by speculation introduces new risks of hacking and theft. Interoperability refers here to the ability of protocols and validators to access and share information, as well as validate transactions, across different blockchains. Interoperability of the underlying settlement layers is not achievable in practice, as each blockchain is a separate record of settlements. Nevertheless, "cross-chain bridges" have emerged to permit users to transfer coins across blockchains.¹³ Yet most bridges rely on only a small number of validators, whom – in the absence of regulation and legal accountability – users need to trust to not engage in illicit behaviour. But, as the number of bridges has risen (Graph 4.A), bridges have featured prominently in several high-profile hacks (Graph 4.B). These attacks highlight the vulnerabilities to security breaches that stem from weakness in governance.

The striking fragmentation of the crypto universe stands in stark contrast to the network effects that take root in traditional payment networks. Traditional payment networks are characterised by a "winner takes all" property, whereby more users flocking to a particular platform beget even more users. Such network effects stand at the heart of the virtuous circle of lower costs and enhanced trust in traditional platforms. In contrast, crypto's tendency toward fragmentation and high fees is a fundamental structural flaw that disqualifies it as the foundation for the future monetary system.¹⁴

Despite fragmentation, speculation can induce high price correlations across different cryptocurrencies and blockchains. Attracted by high returns and the expectation of further price increases (Box B), the influx of new users can push up prices even more. As many cryptocurrencies share a similar user base and are tied to similar protocols, there is strong price co-movement. There are important

A. The number of bridges is increasing¹

B. Theft of cryptocurrencies over time

¹ See technical annex for details.

Sources: Boissay et al (2022); Comparitech; Defi Llama; BIS.

concerns about what happens to a system that relies on selling new coins when the new inflow of users suddenly slows.

The DeFi decentralisation illusion and the role of exchanges

Despite its name, the DeFi ecosystem shows a tendency towards centralisation. Many key decisions are taken by vote among the holders of “governance tokens”, which are often issued to developer teams and early investors and are thus heavily concentrated. Smart contracts tied to real-world events involve oracles that operate outside the blockchain. “Algorithm incompleteness”, ie the impossibility of writing contracts to spell out what actions to take in all contingencies, requires some central entities to resolve disputes. Moreover, newer blockchains usually aim for faster transactions and higher throughput by relying on concentrated validation mechanisms. For example, proof-of-stake mechanisms build on a limited number of validators who stake their coins.

Centralisation in DeFi is not without risks. Increasing centralisation of validators gives rise to incentive conflicts and the risk of hacks, also because these centralised nodes are often unregulated.¹⁵ Further, those in charge of an oracle can corrupt the system by misreporting data (the so-called oracle problem). Currently, there are no clear rules on how to vet or incentivise oracle providers.

Centralisation is also present in crypto trading activities, where investors rely mainly on centralised exchanges (CEXs) rather than decentralised ones (DEXs). While the latter work by matching the counterparties in a transaction through so-called automated market-maker protocols, CEXs maintain off-chain records of outstanding orders posted by traders – known as limit order books – which are familiar from traditional finance. CEXs attract more trading activity than DEXs, as they feature lower costs (Graph 5.A).¹⁶ In terms of business model and the way they operate, crypto CEXs are not fundamentally different from traditional exchanges, even though they are not subject to the same regulation and supervision.

CEXs have seen substantial growth since 2020 and have reached volumes that make them relevant from a financial stability viewpoint (Graph 5.B). Moreover,

Crypto trading and Bitcoin prices

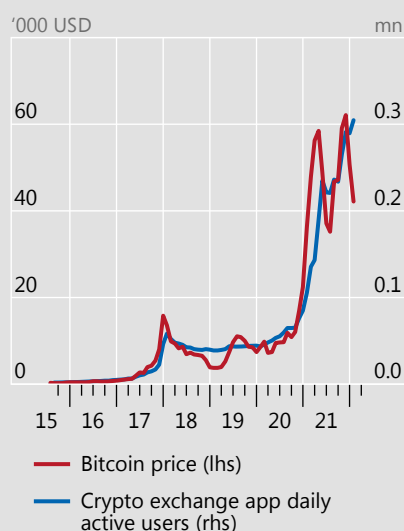
Speculation is a key driver of cryptocurrency holdings,¹ but retail investors may not be fully aware of the risks associated with investments in cryptocurrency. A recent BIS study assembles a novel cross-country database on retail use of crypto exchange apps at a daily frequency over 2015–22, focusing on the relationship between the use of crypto trading apps and Bitcoin prices.² The analysis shows that a rise in the price of Bitcoin is associated with a significant increase in new users, ie the entry of new investors, with a correlation coefficient of more than 0.9 (Graph B1.A). A one standard deviation increase in the daily Bitcoin price is associated with an increase of around 90,000 crypto exchange app users. Crypto app users are primarily younger users and men (Graph B1.B), commonly identified as the most “risk-seeking” segment of the population, and potentially motivated by a “fear of missing out”. These patterns are consistent with survey evidence on individuals’ risk tolerance: younger men are more willing than either women or older male respondents to take financial risks (Graph B1.C).

Quantifying the effect of Bitcoin prices on entry into crypto is difficult because of the possibility of reverse causality. Prices might also increase because of the entry of new crypto exchange app users. To address such concerns, it is possible to focus on specific exogenous shocks when Bitcoin price changes were due to specific factors, such as the crackdown of Chinese authorities on crypto mining activities and the social unrest in Kazakhstan. During each of these episodes, structural changes affected the global price of Bitcoin, independently of the entry of new users in crypto exchange apps. In these cases, the exogenous drop in the Bitcoin price was associated with an average reduction in the number of new app users of 5–10% in the two-weeks following the shocks. Results are further corroborated from a panel vector autoregression model, where a 10% increase in the Bitcoin price leads to a 3% increase in the number of app users.

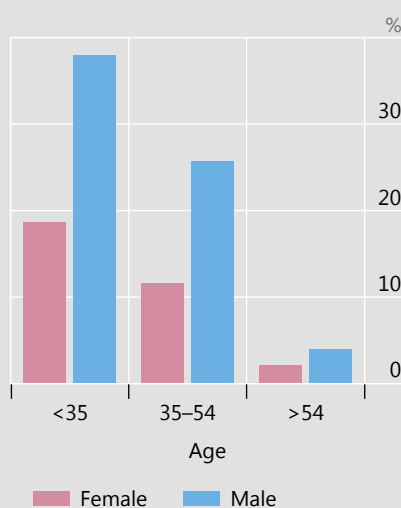
Retail investors are chasing past price increases in a risky strategy

Graph B1

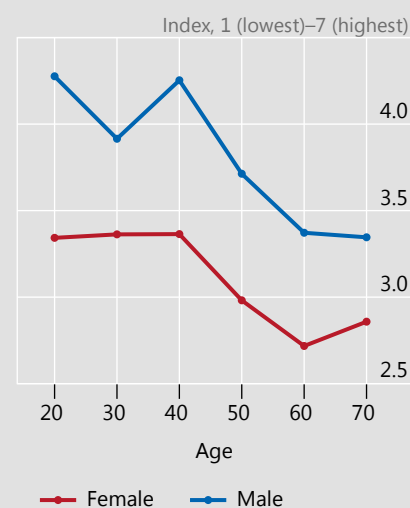
A. Retail cryptocurrency adoption closely follows Bitcoin prices¹



B. More than one third of crypto exchange app users are young men...



C. ...who are often willing to take financial risks¹

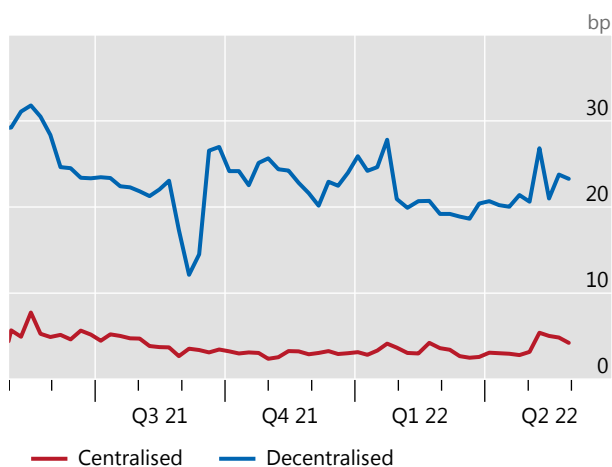


¹ See technical annex for details.

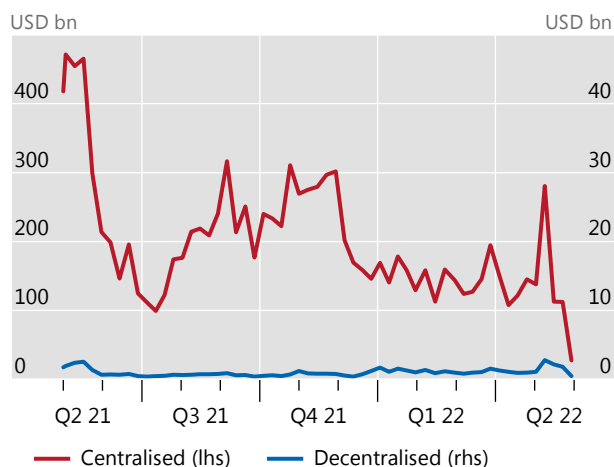
Sources: Auer et al (2022); Federal Reserve Bank of New York, *Survey of consumer expectations*; Sensor Tower.

¹ People invest in cryptocurrencies for different reasons, for example because they distrust domestic financial institutions, for cross-border money transfers or for the potential for pseudo-anonymity – for either legitimate or nefarious reasons. However, one of the main reasons is that cryptocurrencies are seen as investment assets. See Auer and Tercero-Lucas (2021), Foley et al (2019), Hileman (2015), Knittel et al (2019) and Swartz (2020). ² Auer, Cornelli, Doerr, Frost and Gambacorta (2022).

A. Transaction costs, Tether-ETH pair



B. Weekly trading volume



¹ See technical annex for details.

Sources: Aramonte et al (2021); Binance; Coinbase; CryptoCompare; Uniswap; BIS.

trading in CEXs shows a strong tendency towards market concentration: trading volumes in three large CEXs represented around half of the total in the first months of 2022. However, it is generally difficult to gauge the actual size of crypto exchanges, because CEXs hold a significant share of their custodial cryptocurrencies off-balance sheet. For example, the platform Coinbase reported publicly that it had \$256 billion of assets on platform (as of end-March 2022) but a balance sheet of only \$21 billion as of end-2021. Securities and Exchange Commission staff recently argued that the platform should report both liabilities (obligations to customers) and assets on its balance sheet.¹⁷ In addition, crypto service providers often perform a multitude of services, raising the question whether activities are appropriately ring-fenced and risks adequately managed. For example, together with third-party trading, they undertake proprietary trading, margin lending or token issuance, and supply custody services. Often, transactions involve interactions between on-chain smart contracts and off-chain centralised trading platforms, with the distributed nature of on-chain settlement giving rise to distinct risks as compared with those arising from traditional infrastructure operators.

A balanced assessment of the similarities and differences between the crypto market and traditional finance is a prerequisite for considering appropriate regulatory policies. Some activities of crypto service providers are common features in banks too, although their combination in one entity is not currently common in traditional finance. Moreover, differences in underlying technologies mean that risk features and drivers could differ between traditional finance and the crypto ecosystem.

Regulatory approaches to crypto risks

Regulatory action is needed to address the immediate risks in the crypto monetary system and to support public policy goals.

Above all, authorities need to rigorously tackle cases of regulatory arbitrage. Starting from the principle of “same activity, same risk, same rules”, they should ensure that crypto and DeFi activities comply with legal requirements for comparable traditional activities. Stablecoin issuers, for instance, resemble deposit-

takers or money market funds (MMFs). As such, legislation is needed to qualify these activities and ensure that they are subject to sound prudential regulation and disclosure. For systemically important stablecoins issuers, there must be robust oversight. Where stablecoins are issued by large entities with extensive networks and user data, entity-based requirements will be needed.¹⁸ The recent collapse of the Terra UST stablecoin has highlighted the urgency of the matter.

Second, policies are needed to support the safety and integrity of the monetary and financial systems. Cryptocurrency exchanges that hide the identity of transacting parties and fail to follow basic know-your-customer (KYC) and other Financial Action Task Force (FATF) requirements should be fined or shut down. Otherwise, they can be used to launder money, evade taxes or finance terrorism, and to circumvent economic sanctions. Similarly, banks, credit card companies and other financial institutions that provide entry and exit points between DeFi and the traditional system should require identification from users and perform KYC compliance.

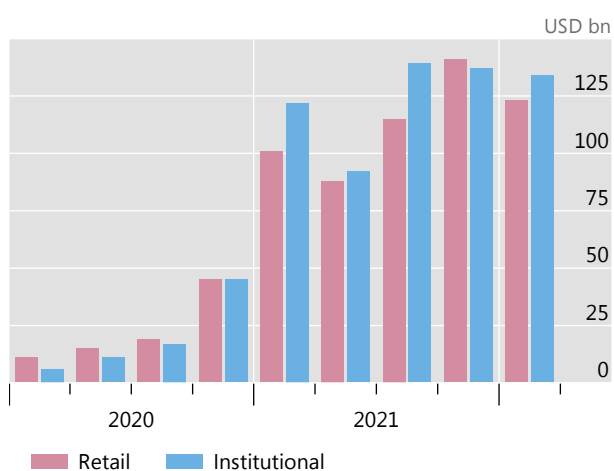
Third are policies to protect consumers. While investors should be allowed to invest in risky assets, including cryptocurrencies, there should be adequate disclosure. This implies sound regulation of digital asset advertising by crypto platforms, which can often be misleading and downplay risks. Practices akin to front-running may require the deployment of new legal approaches.¹⁹ In addition, decentralised platforms cannot, by design, take responsibility in case of fraud or theft connected to the platform, eg as a result of hacks. This stands in the way of providing incentives for the basic disclosure of risks and, as such, new approaches may be needed.²⁰ This logic also extends to the oracle problem. Sound regulatory rules need to ensure that outside information is not manipulated.

Finally, central banks and regulators need to mitigate risks to financial stability that arise from the exposure of banks and non-bank financial intermediaries to the crypto space. Fast-growing investments in cryptocurrencies by traditional financial institutions mean that shocks to the crypto system could have spillovers. Non-bank investors, family offices and hedge funds have reportedly been the most active institutional investors in cryptocurrencies (Graph 6.A). So far, the exposures of large traditional banks have been limited and direct investments in firms active in crypto markets are still small relative to bank capital (Graph 6.B).²¹ That said, bank funding from stablecoin issuers has increased, as bank liabilities such as certificates of deposit form a key part of stablecoins' asset backing.²² Addressing these risks implies a sound implementation of standards for bank exposures to cryptocurrencies, which should seek to ensure adequate resilience to large and sudden changes in prices or large losses through direct and indirect channels.²³ This may also require prudential regulation of crypto exchanges, stablecoin issuers and other key entities in the crypto system. This does not preclude an innovative approach; for example, supervision could be embedded in these markets, so that it is conducted "on-chain".

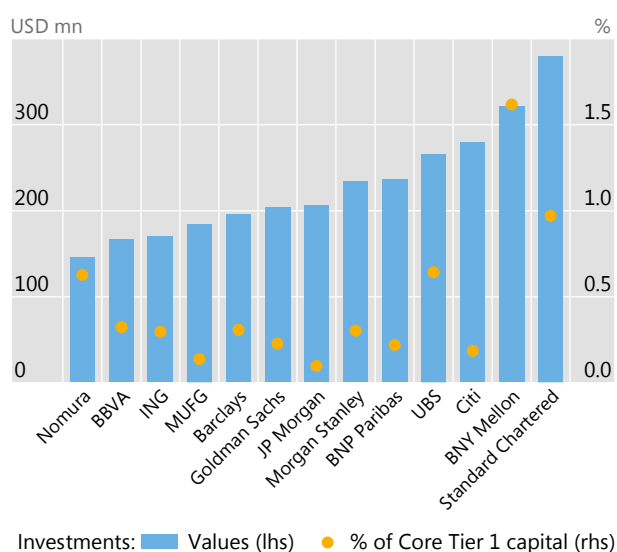
It is essential to fill data gaps and identify entry points for regulation. The growth of the crypto market has led to the proliferation of new centralised intermediaries. Additional entities, such as reserve managers and network administrators, have developed directly as a response to the growth of stablecoins. These centralised entities and traditional financial institutions provide a natural gateway for regulatory responses. These entities could also support the collection of better and more detailed data on DeFi activities, as well as the investor base.

Across all areas of regulation, the global nature of crypto and DeFi will require international cooperation. Authorities may need to actively exchange information and take joint enforcement actions against non-compliant actors and platforms. In some cases, new bodies such as colleges of supervisors may be necessary to coordinate policy toward the same regulated entities operating in different jurisdictions.

A. Assets on Coinbase are largely institutional, and off-balance sheet



B. Investments of large banks in crypto-active firms are still limited¹



¹ See technical annex for details.

Sources: Aramonte et al (2021); Auer et al (2022b); Bloomberg; Coinbase.

The BIS is contributing to this international cooperation through discussions in BIS committees such as the BIS Committee on Payments and Market Infrastructures (BIS CPMI) and the Basel Committee on Banking Supervision (BCBS). The BIS is actively engaged in the G20 discussion on the regulation of cryptocurrencies, as coordinated by the Financial Stability Board (FSB). The BIS is also developing applied technological capabilities in this area to inform the international policy dialogue. The Eurosystem Centre of the BIS Innovation Hub is developing a cryptocurrency and DeFi analysis platform that combines on-chain and off-chain data to produce vetted information on market capitalisations, economic activity and international flows.

Crypto's lessons for the monetary system

Overall, the crypto sector provides a glimpse of promising technological possibilities, but it cannot fulfil all the high-level goals of a digital monetary system. It suffers from inherent shortcomings in stability, efficiency, accountability and integrity that can only be partially addressed by regulation. Fundamentally, crypto and stablecoins lead to a fragmented and fragile monetary system. Importantly, these flaws derive from the underlying economics of incentives, not from technological constraints. And, no less significantly, these flaws would persist even if regulation and oversight were to address the financial instability problems and risk of loss implicit in crypto.

The task is not only to enable useful functions such as programmability, composability and tokenisation, but to ground them on more secure foundations so as to harness the virtuous circle of network effects. Central banks can provide such foundations, and they are working actively to shape the future of the monetary system. To serve the public interest, central banks are drawing on the best elements of new technology, together with their efforts to regulate the crypto universe and address its most immediate drawbacks.

Vision for the future monetary system

The future monetary system should meld new technological capabilities with a superior representation of central bank money at its core. Rooted in trust in the currency, the advantages of new digital technologies can thus be reaped through interoperability and network effects. This allows new payment systems to scale and serve the real economy. The system can thus adapt to new demands as they arise – while ensuring the singleness of money across new and innovative activities.

Central banks are uniquely positioned to provide the core of the future monetary system, as one of their fundamental roles is to issue central bank money (M0), 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 ultimate 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 third role of the central bank is to support the smooth functioning of the payment system by providing sufficient liquidity for settlement. Such liquidity provision ensures that no logjams will impede the workings of the payment system when a payment is delayed because the sender is waiting for incoming funds.

The fourth role of the central bank is to safeguard the integrity of the payment system through regulation, supervision and oversight. Many central banks also have a role in supervising and regulating commercial banks and other core participants of the payment system. These intertwined functions of the central bank leave it well placed to provide the foundation for innovative private sector services.²⁴

The future monetary system builds on these roles of the central bank to give full scope for new capabilities of central bank money and innovative services built on top of them. New private applications will be able to run not on stablecoins, but on superior technological representations of M0 – such as wholesale and retail CBDCs, and through retail FPS that settle on the central bank balance sheet. Central bank innovations can thereby support a wide range of new activities. Because central banks are mandated to serve the public interest, they can design public infrastructures to support the monetary system's high-level policy goals (Table 1, final column) from the ground up.

This vision entails a number of components that require both formal definitions and examples. The section first introduces and explains these components. It next gives a metaphor for what the future system will look like, both domestically and across borders. Finally, it dives into the specifics of reforms to central bank money at the wholesale, retail and cross-border level, before reviewing where central banks stand in achieving this vision.

Components of the future monetary system

The future monetary system builds on the tried and trusted division of roles between the central bank – which provides the foundations of the system – and private sector entities that conduct the customer-facing activities. On top of this traditional division of labour come new standards such as application programming interfaces (APIs, see glossary) that greatly enhance the interoperability of services and associated network effects. Not least are new technical capabilities encompassing programmability, composability and tokenisation, which have so far been associated with the crypto universe.

This vision contains components at both the wholesale and retail level, which enable a number of new features (in bold).

At the wholesale level, central bank digital currencies (CBDCs) can offer new capabilities and enable transactions between financial intermediaries that go beyond the traditional medium of central bank reserves. Wholesale CBDCs that are transacted using permissioned distributed ledger technology (DLT) offer **programmability** and atomic settlement, so that transactions are executed automatically when set conditions are met. They allow a number of different functions to be combined and executed together, thus facilitating the **composability** of transactions. These new capabilities not only permit the expansion of the types of transactions, but also enable transactions between a **much wider range of financial intermediaries** – not just commercial banks. Wholesale CBDCs also work together across borders, through **multi-CBDC arrangements** involving multiple central banks and currencies.

Within the new functions unlocked by wholesale CBDCs, one set of applications deserves special mention – namely, those stemming from the **tokenisation** of deposits (M1), and other forms of money that are represented on permissioned DLT networks.²⁵ The role of intermediaries in settling transactions was one of the major advances in the history of money, tracing back to the role of public deposit banks in Europe in the early history of central banking.²⁶ Bank deposits serve as the payment medium, as the intermediary debits the account of the payer and credits the account of the receiver. The tokenisation of deposits takes this principle and translates the operation to DLT by creating a digital representation of deposits on the DLT platform, and settling them in a decentralised manner. This could facilitate new forms of exchange, including fractional ownership of securities and real assets, allowing for innovative financial services that extend well beyond payments.

At the customer-facing, or “retail” level, the enhanced capabilities of the financial intermediaries benefit users in the form of improved **interoperability** between customer-facing platforms provided by intermediaries. Core to this interoperability are APIs, through which users of one platform can easily communicate and send instructions to other, interlinked platforms. This way, innovations at the retail level promote greater competition, lower costs and expanded financial inclusion.

Concretely, FPS and retail CBDCs constitute another core feature of the future monetary system. Retail FPS are systems in which the transmission of a payment message and the availability of final funds to the payee occur in (near) real time, on or as near to 24/7 as possible. Many are operated by the central bank. Retail CBDCs are a type of CBDC that is directly accessible by households and businesses. Both retail CBDCs and FPS allow for **instant payments** between end users, through a range of interfaces and competing private PSPs. They hence build on the two-tiered system of the central bank and private PSPs. Retail CBDCs and FPS share a number of further key features and can thus be seen as lying on a continuum. Both are supported by a **data architecture** with digital identification and APIs that enable secure data exchange, thus supporting greater user control over financial data. By providing an **open platform**, they promote efficiency and greater competition between private sector PSPs, thus facilitating lower costs in payment services. Through **inclusive design** features, both can support financial inclusion for users that currently do not have access to digital payments.

Details of the wholesale and retail components are expanded upon below. For each of these, an advanced representation of central bank money supports private sector services that serve the real economy. The central bank supports the singleness of the currency, and interoperability – the ability of participants to transact in different systems without having to participate in each.²⁷ This allows

network effects to take hold, whereby the use of a service by one party makes it more attractive for others.

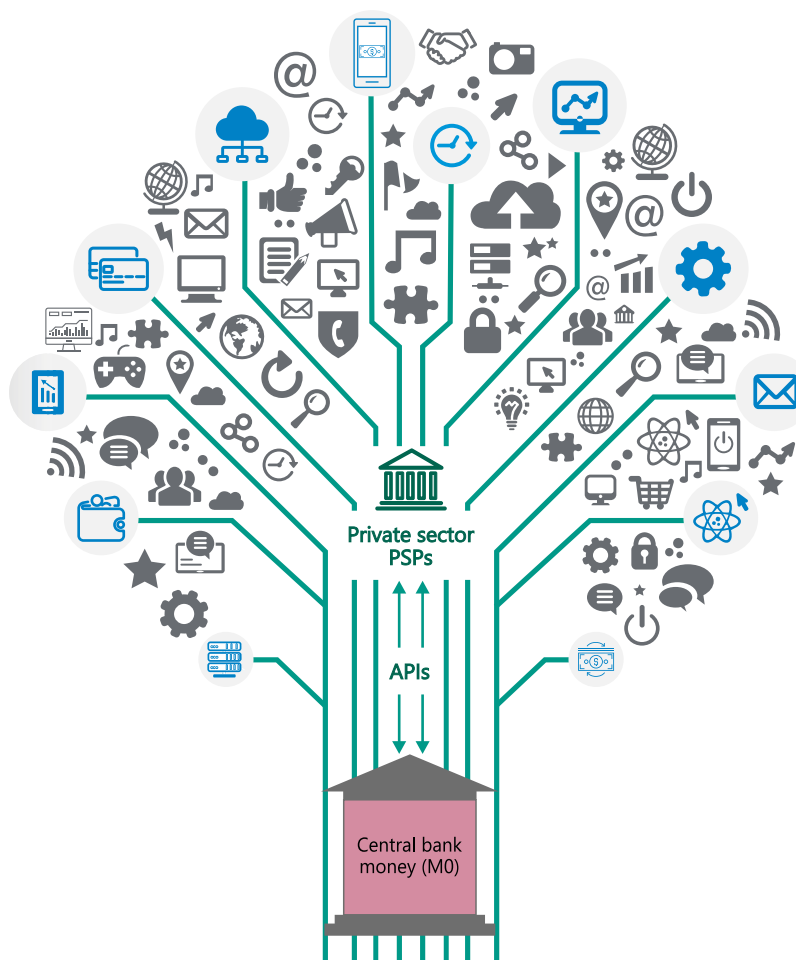
A metaphor for the future monetary system

The metaphor for the future monetary system is a tree whose solid trunk is the central bank (Graph 7). As well as exemplifying the solid support provided by central bank money, the tree metaphor expresses the principle of the monetary system being rooted (figuratively speaking) in payment finality through ultimate settlement on the central bank's balance sheet.

The monetary system based on central bank money supports a diverse and multi-layered vibrant ecosystem of participants and functions in which competing private sector PSPs can give full play to their creativity and ingenuity to serve users better. Underlying these benefits is the virtuous circle set off by network effects arising from the data architecture, consisting of digital identity and APIs, that enables interoperability both domestically and across borders.

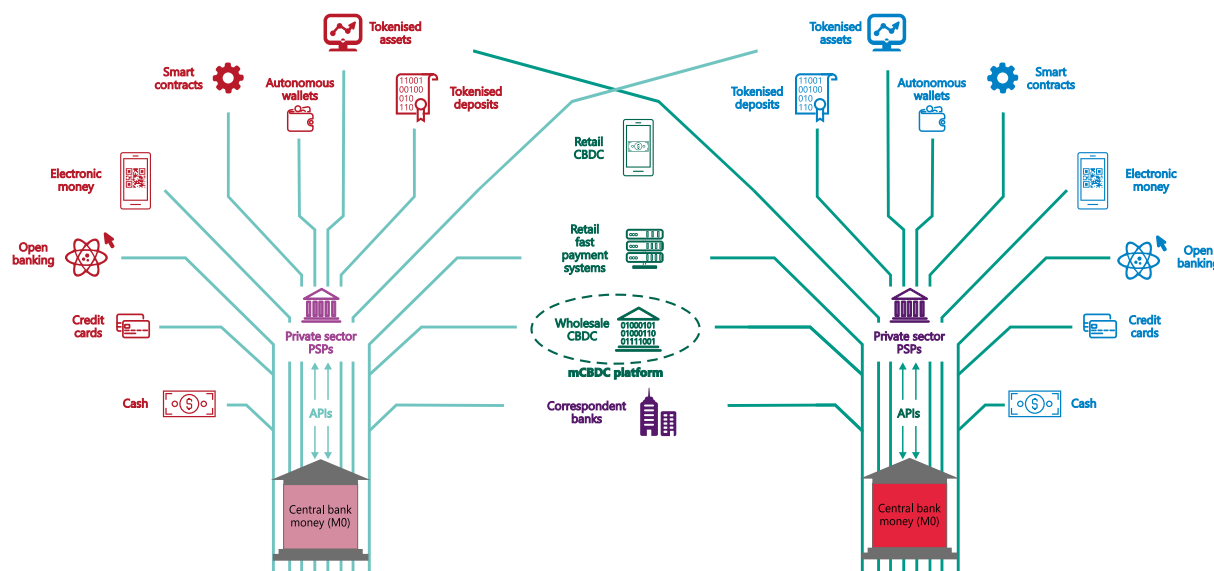
A metaphor: central bank as tree trunk supporting a diverse ecosystem

Graph 7



API = application programming interface; PSP = payment service provider.

Source: BIS.



API = application programming interface; CBDC = central bank digital currency; PSP = payment service provider.

Source: BIS.

Zooming out, the global monetary system can then be compared with a forest, whose canopy facilitates cross-border and cross-currency activity (Graph 8). In the canopy, infrastructures such as multi-CBDC platforms serve as important new elements of the system, as discussed in detail below. The functionality of new platforms in the canopy is ultimately rooted in the domestic settlement layers underneath.

Innovation is not only about the latest fashion or buzzword. Just as a tree cannot sustain a vibrant ecosystem without a solid trunk, getting the basics right is a prerequisite for private innovation that serves the public interest. Ongoing work at central banks is showcasing how public infrastructures can improve the payment system, taking advantage of many of the supposed benefits of crypto without the drawbacks. Wholesale and retail CBDCs, FPS and further reforms in open banking show how central banks can support interoperability and data governance. In fulfilling their public interest mandates, central banks are not working alone but collaborating closely with other public authorities and innovators in the private sector. The following subsections fill in the details of how the system functions, together with concrete examples of the functionalities.

Wholesale CBDCs and tokenised money

A CBDC is a digital payment instrument, denominated in the national unit of account, which is a direct liability of the central bank.²⁸ Much attention has recently focused on retail CBDCs that are accessible by households and businesses (discussed below). Yet wholesale CBDCs also offer new functions for payment and settlement, and to a much wider range of intermediaries than domestic commercial banks. They could unlock significant private sector innovation across a range of financial services.

Wholesale CBDCs can allow intermediaries to access new capabilities that are not provided by the reserves held by commercial banks with the central bank. These are particularly relevant in permissioned DLT networks, where a decentralised

network of trusted participants accesses a shared ledger. As discussed below, decentralised governance is a useful feature of multi-CBDC systems involving multiple central banks and currencies. Yet the functions could in principle be offered in more centralised payment systems. Key are self-executing smart contracts that let participants make their transactions programmable. Transactions thus settle only when certain pre-specified conditions are met. In security trading, such automation can allow payment vs payment (PvP) and delivery vs payment (DvP) mechanisms, meaning that payments and delivery of a security are made only all together or not at all. Such atomic settlement can significantly speed up settlement and mitigate counterparty risk.²⁹

One benefit of wholesale CBDCs is that they could be available to a much wider range of intermediaries than just domestic commercial banks. Allowing non-bank PSPs to transact in CBDC could make for much greater competition and vibrancy. New protocols built on wholesale CBDCs could be open source, making the source code freely available for a community of developers to develop and scrutinise. This feature would allow for libraries of protocols that can be used to combine functions, thus facilitating the composability of different functions and enabling new services to be built on top of the programmability function of CBDCs.

By construction, wholesale CBDCs would allow for finality in payments. The mechanics of how finality is attained in permissioned DLT platforms are described in more detail in Box C, but their essence can be explained through the simple analogy with a physical banknote. The recipient of a physical banknote wants to be assured that the note is genuine, not counterfeit. Ensuring that payment is in genuine money in a digital system is accomplished by proving the origin or “provenance” of the money transferred. 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. This is where cryptographic techniques such as zero-knowledge proofs (ZKPs) provide a solution. As the name signifies, “proof” denotes that a statement is true, and “zero-knowledge” means that no additional information is exposed beyond the validity of the assertion. 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 be needed to prevent the same digital token being spent twice; in many cases, the central bank can play this role. The common theme is that decentralisation can be achieved without the structural flaws of crypto.

As issuers of the settlement currency, central banks can support the tokenisation of regulated financial instruments such as retail deposits.³⁰ Tokenised deposits are a digital representation of commercial bank deposits on a DLT platform. They would represent a claim on the depositor’s commercial bank, just as a regular deposit does, and be convertible into central bank money (either cash or retail CBDC) at par value. Depositors would be able to convert their deposits into and out of tokens, and to exchange them for goods, services or other assets. Tokenised deposits would also be protected by deposit insurance but, unlike traditional deposits, they would also be programmable and “always on” (24/7), thus lending themselves to broader uses in retail payments – eg in autonomous ecosystems. This way, they could facilitate tokenisation of other financial assets, such as stocks or bonds. This functionality could allow for fractional ownership of assets and for the ability to exchange these on a 24/7 basis. Crucially, this could be done in a regulated system, with settlements in wholesale CBDC.

One possible system with tokenised deposits could feature a permissioned DLT platform. This platform records all transactions in tokens issued by the participating institutions, eg commercial banks (representing deposits), non-bank PSPs

Making use of DLT with central bank money

In a permissionless blockchain used for crypto applications, all transactions are public. Privacy is maintained by hiding the user's real identity behind a private key. In this sense, there is *pseudo-anonymity*.¹ By contrast, a monetary system based on users' real names raises the question of how to safeguard their privacy. Privacy has the attributes of a fundamental human right. Nobody else needs to know from which supermarket an individual buys their groceries. Therefore, a basic task of a decentralised monetary system based on real names is to find a way to ensure both that the ledger is secure without the need for a central authority, while at the same time preserving the privacy of the individual transactions.

One possible route is through permissioned DLT systems. In these systems, only select users that meet eligibility requirements can obtain access. Interactions between system participants are thus invisible to people outside the system. One example is the permissioned DLT system Corda, which is used by private financial institutions (eg for trade finance platforms) and in a number of central bank wholesale CBDC projects, including Projects Helvetia, Jura and Dunbar at the BIS Innovation Hub.

In Corda, updates to the ledger are performed through a validation function and a uniqueness function. Validation, which involves checking that the details of the transaction are correct and that the sender has the available funds, is done by the system participants. In fact, only the participants that are involved in a transaction are responsible for validating it. Checking that the sender has a valid claim to funds does not, however, ensure that they will not attempt to spend those same funds twice. Transaction uniqueness (ie the prevention of double-spending) is ensured by a centralised authority called a "notary". Notaries have access to the entire ledger and hence can ensure that funds being used in a particular transaction are not being used elsewhere. In the case of wholesale CBDCs, a natural candidate for the notary is the central bank, as this institution already plays a similar role in maintaining the integrity of the overall transaction record in centralised systems.

In such permissioned systems, a tension can arise between payment integrity and transactional privacy. Transactional privacy in a peer-to-peer exchange means that only the two participants involved in a transaction can see that it occurs – very much like when one person hands over a one-dollar bill to a friend. In the case of a digital banknote, the validation process performed by the participants requires that the recipient can trace the banknote back to its origin, which in turn entails seeing every one of the banknote's previous holders. In the context of Corda, this is called the "backchain problem". While the system does not allow everyone to see everything, it does allow participants to have a view beyond their own transactions. Solving the backchain problem is an important design problem in central bank CBDC projects. The challenge is to arrange matters so that they can truly emulate paper banknotes and preserve people's transactional privacy.

Recently, system architects have been exploring the use of zero-knowledge proofs (ZKPs) to generate a cryptographic record that a transaction has occurred, without revealing either the identity of a participant or the content of the transaction. ZKPs let one party prove to another that a statement is true without revealing any information beyond that fact. In a payment system, the goal is to prove that the sender of funds obtained those funds through a legitimate chain of transactions, going all the way back to and including the origination of the funds, without sharing any details of these transactions. The goal is achieved by replacing each individual transaction with a ZKP and transferring these proofs, in place of the individual transaction details, during each successive transaction. This technique allows recipients of a digital banknote to know that it can be traced back to its origin, without knowing the details of this banknote's history. Instead of seeing the history of all previous transactions, the verifier, and, if desired, the notary, can observe only a series of ZKPs (see Graph C1).

The ZKP technique is generally understood to be an effective means of generating transactional privacy, but using cryptographic proofs erodes system performance by reducing its speed. Currently, the most popular ZKP systems are the so-called succinct non-interactive arguments of knowledge (SNARKs), succinct transparent arguments of knowledge (STARKs) and Bulletproofs. Each solution has different costs in terms of verification and overall proof time and overall proof size; these are shown in Table C1. Long verification and proof times may reduce transaction throughput to levels that are insufficient to settle typical payment system volumes without adding an unacceptable amount of delay. Researchers are looking for ways to reduce these times.

Zero knowledge proof (ZKP) computation times and sizes

Table C1

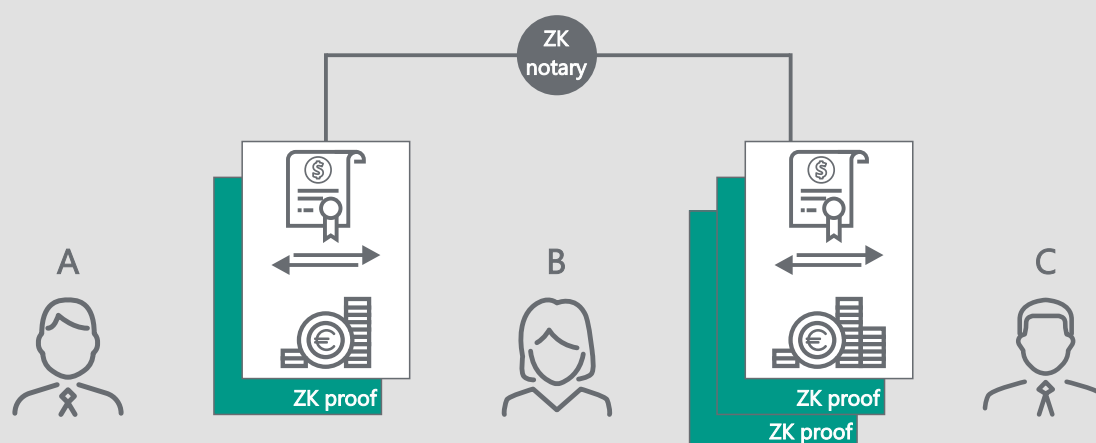
	SNARKs	STARKs	Bulletproofs
Proof time	~2.3 seconds	~1.6 seconds	~30 seconds
Verification time	~10 milliseconds	~16 milliseconds	~1.1 seconds
Size for one transaction	Tx: 200 bytes; Key: 50 MB	45 KB	1.5 KB
Size for 10,000 transactions	Tx: 200 bytes; Key: 500 MB	135 KB	2.5 KB

Sources: Various public research from Zooko Wilcox, Elena Nadilinki and Matter Labs.

Beyond ZKP, transactional privacy can be achieved through other means, such as homomorphic encryption, secure multi-party computation, differential privacy, blind signatures, ring signatures, Pedersen commitments, account abstraction and stealth addresses. Each of these methodologies employs different combinations of trusted setup and/or additional computational overhead. Currently the BIS Innovation Hub is experimenting with stealth addresses, which are one-time use addresses generated by a protocol, with the aim of obscuring the identities of the participants in a transaction.

Backchain solution

Graph C1

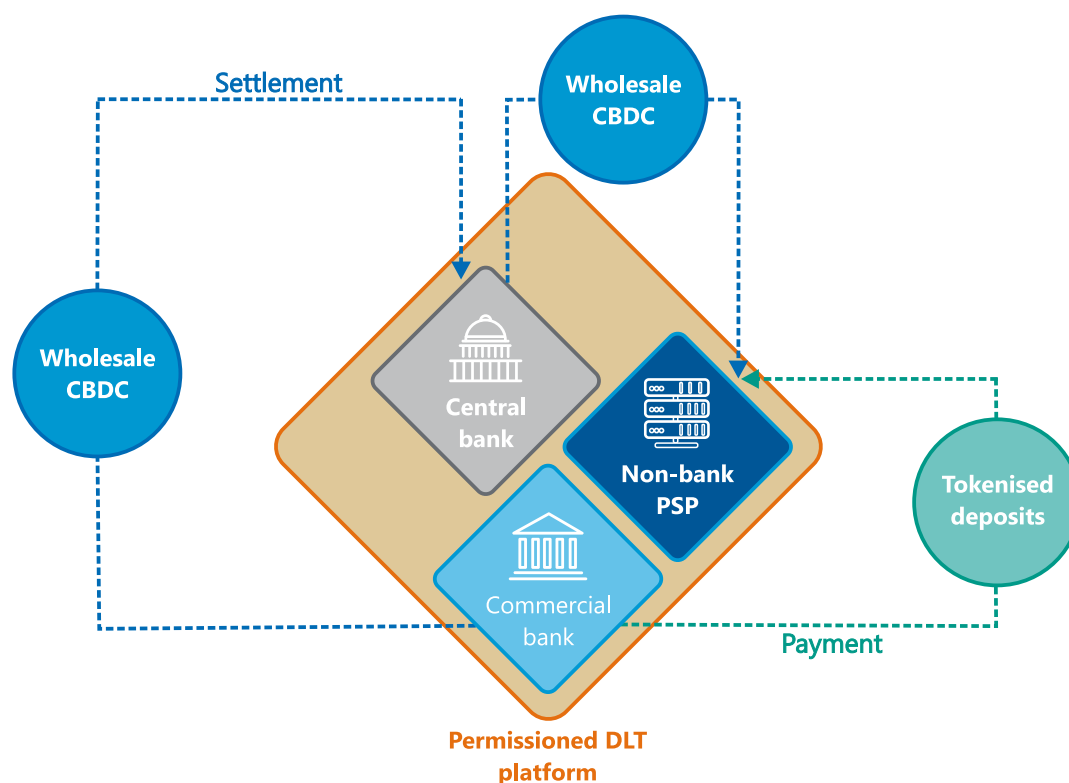


ZK = zero-knowledge.

Sources: Adapted from Annerie Vreugdenhil, ING Bank, CordaCon 2021.

¹ Transactions are not fully anonymous to the extent that, once personal information is linked to a wallet address, all transactions using that address can be traced on the blockchain.

(representing e-money) and the central bank (representing central bank money). Retail investors (depositors) would hold tokens in digital wallets and make payments by transferring tokens across wallets. The settlement of transactions between financial institutions on the DLT platform would rely on the use of wholesale CBDCs as settlement currency. To get a sense of how this would work, consider a depositor who holds a bank's tokens and wishes to make a payment to the holder of non-bank PSP tokens, representing e-money, for instance to pay for a house (Graph 9). Both parties may agree that the payment (green arrow) should occur at the same time the deed to the house is transferred. In the background, to settle the transaction, the bank would transfer wholesale CBDC on the DLT platform to the non-bank PSP (blue arrows). The non-bank PSP would transfer a corresponding amount of new tokens to its customer's wallet. All of these steps could occur simultaneously, as part of a single atomic transaction, executed through smart contracts. In this system,



DLT = distributed ledger technology; PSP = payment service provider.

The green arrows indicate the movement of liabilities and the blue arrows indicate the movement of assets.

Source: BIS, adapted from McLaughlin (2021).

wholesale CBDCs help to settle transactions and to guarantee the convertibility and uniformity of the various representations of money. The same system could also allow for digital representations of stocks and bonds. This would enable end users to easily access (fractions of) these assets in small denominations, 24/7, from regulated providers – and to settle the transactions instantaneously.

Programmable CBDCs could also support machine-to-machine payments in autonomous ecosystems.³¹ Autonomous machines and devices increasingly communicate and execute processes without human intervention through the Internet of Things, a network of connected devices. Looking ahead, machines may directly purchase goods and services from each other, and manage their own budget. Their interconnection will increase the need for smart contracts and programmable money. For example, they may be equipped with wallets, charged with a certain budget of digital money. Smart contracts may automatically trigger payments as soon as certain conditions are met, eg the arrival of the goods. This could lead to significant efficiency gains, for example in the goods logistics sector, where transactions often take several days and are still predominantly paper-based. The full potential of these technological developments can be realised only if machine-to-machine transactions are settled instantly, so that any settlement risk is removed. Existing private sector cryptocurrency projects for the Internet of Things are still exploratory and suffer from limits to scalability.³² They also raise concerns about the stability and convertibility of cryptocurrencies used for payments and would require on- and off-ramp bridges to connect with traditional payment rails. In this respect,

the industry could benefit from CBDCs, which could underpin a decentralised system, eg by enabling regulated financial institutions to issue programmable money.³³

In short, programmability, composability and tokenisation are not the preserve of crypto. The benefits of atomic settlement and open-source protocols are fully compatible with central banks being at the core of the validation process. Yet by relying on central bank money, wholesale CBDCs would benefit from the stability and singleness of the currency that central banks provide. They would also draw on the accountability of the central bank and of regulated intermediaries to society. By supporting innovative private sector services, they would facilitate adaptability so that the system can meet new needs as they arise.

Retail CBDCs and fast payment systems

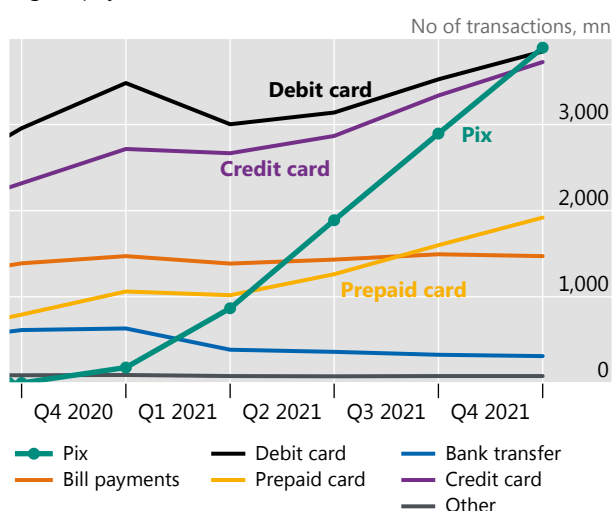
Retail CBDCs and retail FPS share many similarities. Retail CBDCs make central bank money available in digital form to households and businesses. Bank and non-bank PSPs provide retail-facing payment services. The key difference from retail FPS is that, for CBDCs, the instrument is a legal claim on the central bank. Retail CBDCs are thus sometimes seen as “digital cash” – another form of central bank money available to the public.³⁴ In retail FPS, many of which are operated by the central bank, the instrument being exchanged is a claim on private intermediaries (eg bank deposits or e-money). Nonetheless, both retail CBDCs and retail FPS build on public data architecture with APIs that ensure secure data exchange and interoperability between different bank and non-bank PSPs. Both feature high speeds and availability, as transfers occur in real time or near real time on a (near) 24/7 basis.

These retail payment infrastructures have already shown their mettle in enhancing efficiency and inclusion in the monetary system. Unlike crypto, which requires high rents and suffers from congestion and limited scalability, CBDCs and retail FPS allow for network effects to lead to a virtuous circle of greater use, lower costs and better services. Because of their explicit mandates, central banks can design systems to meet these goals from the ground up. An open payment system resting on the interoperability of services offered by competing private PSPs can challenge rents in concentrated banking sectors and reduce the payments costs for end users.

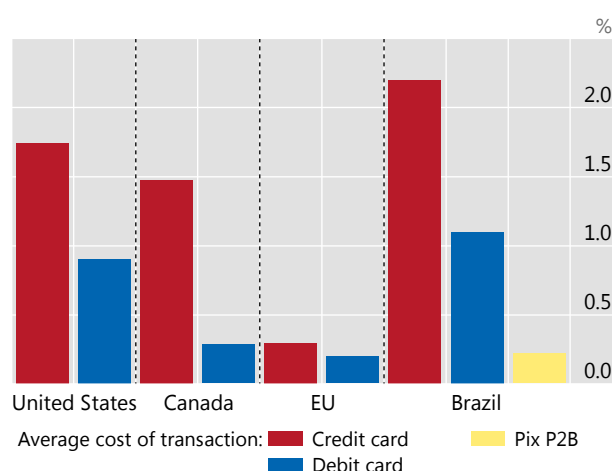
Retail FPS have already made impressive progress in lowering costs and supporting financial inclusion for the unbanked. For example, in just over a year after its launch, the Brazilian retail FPS Pix is used by two thirds of the adult population – with 50 million users making a digital payment for the first time. Powered by innovative products and services offered by over 770 private PSPs, Pix payments have now surpassed credit and debit card transactions (Graph 10.A). The costs to merchants of accepting person-to-business (P2B) payments average one tenth of the cost of credit card payments (Graph 10.B). Equally impressive progress in inclusive, low-cost payments has been made in other economies.³⁵

Retail CBDCs could play a similarly beneficial role as retail FPS, while offering additional technological capabilities. For example, Project Hamilton – a joint project by the Federal Reserve Bank of Boston and the Massachusetts Institute of Technology Digital Currency Initiative – has shown the technical feasibility of a CBDC architecture that can process 1.7 million transactions per second – far more than major card networks or blockchains.³⁶ The project uses functions inspired by cryptocurrencies, but it does not use DLT. In its next stage, Project Hamilton aims to create a foundation for more complex functionalities, such as cryptographic designs for privacy and auditability, programmability and self-custody. The code for the project is open-source and can be scrutinised by any developer, to maximise knowledge-sharing and expand the pool of experts contributing to the code base, including central banks, academia and the private sector.

A. Pix is gaining market share rapidly in Brazil's growing digital payments market...¹



B. ...and enables payment services at very low cost to users and merchants²



P2B = peer-to-business

¹ Excluding recurrent utility payments. ² See technical annex for details.

Sources: Duarte et al (2022); Hayashi and Nimmo (2021); Central Bank of Brazil.

Like retail FPS, retail CBDCs can be designed to support financial inclusion.³⁷ Many central banks are exploring retail CBDC design features that tackle specific barriers to financial inclusion, for instance through novel interfaces and offline payments (see Box D). For instance, Bank of Canada staff have researched the potential for dedicated universal access devices that individuals could use to securely store and transfer a CBDC. The Bank of Ghana has explored the use of existing mobile money agent networks and wearable devices.³⁸ Through tiered CBDC wallets with simplified due diligence for users transacting in smaller values, central banks can reduce the cost of payment services to the unbanked, thus fostering greater access to digital payments and financial services. By allowing new (non-bank) entities to offer CBDC wallets, they can also overcome the lack of trust in financial institutions that holds back many individuals in today's system.³⁹

Both retail CBDCs and FPS can be designed to protect privacy and grant greater user control over data. In the digital economy, every transaction leaves a trace, raising concerns about privacy, data abuse and personal safety. In addition, the resulting data are of immense economic value – which currently accrues mostly to financial institutions and big techs that collect, store and monetise users' personal data.

The power over data of individual PSPs stems from the fact that, in conventional payment systems, there is no single, complete record of all transactions. Instead, every PSP keeps a record of its own transactions only. While payments across PSPs are made through a centralised system and require instructions to be sent to a central operator, these instructions may involve batched payments or incomplete information about the purpose of the payment. Hence, even the central operator has no complete picture of all payments. Privacy in payments is thus maintained through a fragile combination of isolated record-keeping and the promise of confidentiality by the central operator – but it is not guaranteed. In some cases, data privacy laws give consumers the opportunity to grant or deny third parties consent to use their data. But this option is often difficult to exercise effectively.

Designing retail CBDCs to support financial inclusion

Many central banks around the world see financial inclusion as a key motivation for their work on retail CBDCs. This is particularly true in emerging market and developing economies (EMDEs), where access to digital payment and other financial services is constrained by several key barriers. These include (i) geographic factors, eg vast territories or islands; (ii) institutional and regulatory factors, such as a lack of identity credentials and informality; (iii) economic and market structure issues, including limited competition and high costs in the financial sector; (iv) characteristics of vulnerability, eg barriers by age, gender, income or disability status; (v) a lack of educational opportunities and financial literacy; and (vi) distrust of existing financial institutions. In many EMDEs, a majority of adults lack access to digital payment options.

A new study draws on the experience of nine central banks around the world in tackling financial inclusion challenges.¹ It finds that some central banks consider CBDCs as key to their mandate as a catalyst for innovation and economic development. Others see CBDCs as a potential complement to existing policies to support financial inclusion. The study argues that, if CBDCs are to be issued, they could be designed with several key design features that directly address barriers to financial inclusion. For instance, they might facilitate low-cost customer enrolment processes, for instance with simplified due diligence, electronic KYC arrangements and tiered wallets, as demonstrated in several live retail CBDC systems (Graph D1.A). Features such as the use of third-party agents help to reach isolated communities and to work around a lack of trust in financial institutions. Central banks can offer a robust, low-cost public infrastructure with a multitude of user interfaces (Graph D1.B). This includes offline functionality, and interfaces that specifically tailor to underserved users. And finally, CBDCs foster interoperability both domestically and across borders, thus contributing to greater competition and lower costs for end users (Graph D1.C).

Inclusive CBDC design features to tackle barriers to financial inclusion

Graph D1

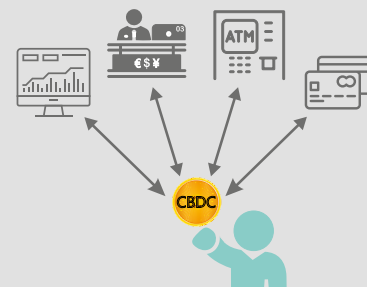
A. Simplified due diligence and tiered know-your-customer (KYC)



B. Multitude of private and public sector user interfaces



C. Interoperability with other means of payment



Source: Boakye-Adjei et al (2022).

¹ Boakye-Adjei et al (2022).

Such a setup implies that consumers may not always know whether their data are being collected and for what purpose.

Proponents of crypto argue that permissionless blockchains return the control over personal data to users, but a system based on pseudo-anonymity and a public ledger introduces severe risks to privacy and integrity. It is also incompatible with a system based on real names, which is required to ensure integrity and accountability.

The data architecture underlying both retail FPSs and CBDCs can give much greater user control over personal data, while preserving privacy and consumer welfare. Indeed, central banks have no commercial interest in personal data, and can thus credibly design systems in the public interest. Data governance systems can ensure user consent, use limitation and retention restrictions.⁴⁰ Similar to open banking, these data architectures can also allow users to port data in ways that

bring economic benefits to users, for instance when they apply for a loan, want to use financial planning services or in a range of other contexts. Importantly, such a system is based on identification – and this identity information may often be held only by the PSP and not by the central bank. The use of identification also allows financial intermediaries to screen borrowers to assess their creditworthiness, thereby ensuring that scarce capital is allocated to its best use.

In the process, central banks can make use of modern cryptography, which offers solutions to preserve the privacy of users and ensure the security of transactions. This can be achieved for instance through ZKPs, which verify the authenticity of the transaction without revealing its content (Box C). Nonetheless, the system would be based on users' true, verified identities, ie they would transact under their real names. Several central banks also see "electronic cash" in the form of retail CBDC as one potential solution for preserving people's transactional privacy.⁴¹

Identity-based designs are compatible with integrity in the financial system. With clear mandates and public accountability, systems can be designed to grant law enforcement authorities access to information with the requisite legal safeguards. These approaches are already commonplace in the form of bank secrecy laws and are being considered for retail CBDCs.⁴² Importantly, transactions would not be recorded on a public blockchain visible to all. In the corporate space, new corporate digital identity solutions could improve oversight of beneficial ownership, thus reducing fraud, tax avoidance and sanctions evasion.⁴³ Together with new regtech tools and capabilities inspired by blockchain analytics, there is potential for better tracking illicit activity while making compliance with regulatory frameworks less resource-intensive.

Finally, retail CBDCs and FPS offer opportunities to improve on accountability relative to today's system, and certainly relative to the crypto universe. Indeed, the design of new public infrastructures is not a task for the central bank alone. New systems require public dialogue on the role of the central bank in retail payments. Their operation will require legal mandates to be updated, as well as proper checks and balances and appropriate forms of central bank accountability to society. It is for this reason that many central banks have issued consultations on these initiatives and are promoting dialogue on legal tender and central bank laws.⁴⁴ A system built on public infrastructure would also ensure that private service providers are embedded in a sound regulatory and supervisory framework. Unlike in a parallel crypto financial system, parties can be held to account for their actions. In this new ecosystem, there will likely be new private sector business models that do not yet fit with current regulatory frameworks, but experience to date suggests that frameworks can adapt to allow for new types of innovative activity.⁴⁵

Achieving cross-border integration

Integrated global value chains mean that the world is no longer a collection of "island economies", but rather a dense network of interconnections that requires a flexible matrix of money, payments and broader financial services.⁴⁶ Wholesale and retail CBDCs as well as retail FPS, can support cross-border integration. The future monetary system will thus be commensurate with the task of providing robust payment and settlement rails that can support economic integration and public interest objectives.

The principles behind the construction of multi-CBDC platforms illustrate the potential for decentralisation to be applied constructively.⁴⁷ First, when there is more than one currency involved, more than one central bank needs to take part in the governance of the payment platform. One way to address the governance problem among multiple parties is to adopt decentralisation through a DLT platform. Trusted notaries can manage the shared ledger, and central banks are the

natural candidates to take on this task domestically, with shared infrastructure at the global level. Second, since the decentralisation has to be accomplished using real names, rather than using private keys as in cryptocurrencies, safeguarding privacy is an essential design element. Achieving both goals – of respecting privacy while using real names – can be accomplished by using public key cryptography.

There are different models for multi-CBDC platforms, ranging from simply coordinating on standards, through interlinking systems, to a fully shared, common mCBDC platform. On a common mCBDC platform, transfers are recorded on a single ledger in one step, and participants have full real-time visibility of their balances. The settlement process is thus simplified, obviating the need for reconciliation of balances across accounts as in conventional correspondent banking transactions.

A common mCBDC platform creates the opportunity to simplify processes. For example, business rules or conditions can be automated using the smart contract features on a DLT platform. Such process automation reaps efficiency gains both in costs and in transaction time. As mCBDC arrangements involve multiple central banks, each with their own currency, decentralisation can be a constructive feature, and permissioned DLT can play an important role. In addition to the currencies of each central bank in the platform, it could include tokens for other currencies, including international currencies. These platforms have some family resemblance with those used in crypto and DeFi, such as smart contracts and programmability that enable PvP or, in the context of security settlements, DvP across borders.

Linking of public infrastructures across borders is also possible for retail FPS. A recent project at the BIS Innovation Hub showed the potential for linking FPS in different jurisdictions so that payments take seconds rather than days, cutting costs and making fees and exchange rates transparent to senders before they commit to a payment. Achieving these benefits requires coordination in messaging formats and in several key policy areas, but it is technically feasible.⁴⁸

Taking stock of progress toward the vision

Where do central banks stand in achieving this vision of the future monetary system? Substantial efforts are under way, and central banks are working together with one another, with other public authorities and with the private sector to expand the frontier of capabilities in the monetary system.

Globally, a full 90% of central banks recently surveyed are doing some form of work on wholesale or retail CBDCs.⁴⁹ A number of wholesale CBDC pilots are under way, often involving several central banks in different jurisdictions. There are three live retail CBDCs and a full 28 pilots. This includes the large-scale pilot by the People's Bank of China, which now counts 261 million users.⁵⁰ Meanwhile, over 60 jurisdictions now have retail fast payment systems, with several more planned in the coming years – such as FedNow in 2023.⁵¹ The BIS Innovation Hub is developing mCBDC platforms in partnerships with member central banks. These are Project Jura (with the central banks of Switzerland and France), Project Dunbar (with Singapore, Malaysia, Australia and South Africa), and mBridge (with Hong Kong SAR, Thailand, China and the United Arab Emirates).

A recent stocktake by the Innovation Hub draws lessons from mCBDC experiments to date.⁵² These have demonstrated their feasibility from a technical perspective using different experimental designs. They have also shown the potential for much faster, lower-cost and more efficient international settlement, without the need for intermediaries such as correspondent banks. On the retail side, the Innovation Hub, through its Hong Kong, London and Nordic centres is advancing work on cyber-secure architectures, building an open API ecosystem for retail CBDCs, and exploring resilient and offline CBDC systems.

Achieving frictionless payments in the global monetary system requires strong cooperation between central banks, combined with innovation in the private sector. Supporting these efforts is a comparative advantage of the BIS that arises from its mandate for international settlements. Indeed, the BIS has already developed proofs-of-concept and prototypes in near real-world settings. These can help to draw policymakers' attention to the actual issues they are likely to encounter. They also show that cooperation is possible even when central banks take different approaches to some key policy issues.

In sum, central banks are working together to advance domestic policy goals and to support a seamlessly integrated global monetary system with concrete benefits for their economies and end users. The solutions they use will draw on a range of new technologies, some inspired by the crypto monetary system, but grounded in the solid institutional frameworks that exist today. By adapting the system now, central banks will help to make money and payments fit for the decades to come.

Conclusion

The monetary system is a crucial foundation for the economy. Every time households and businesses make payments across the range of financial transactions, they place their trust in the safety of money and payment systems as a public good. Retaining this trust is at the core of central bank mandates.

Rooted in this trust, the monetary system must meet a number of high-level goals to serve society. It must be safe and stable, and key entities must be held accountable for their actions. This way, the integrity of the system is ensured. Fast, reliable and cheap transactions should promote efficiency and financial inclusion, while users' rights to privacy and control over data must be upheld. Finally, in an ever-changing and globally connected world, the system must be adaptable and open.

Recent events have shown how structural flaws prevent crypto from achieving the levels of stability, efficiency or integrity required for a monetary system. Instead of serving society, crypto and DeFi are plagued by congestion, fragmentation and high rents, in addition to the immediate concerns about the risks of losses and financial instability.

This chapter has laid out a brighter vision of the future monetary system. Around the core of the trust provided by central bank money, the private sector can adopt the best that new technologies have to offer, including programmability, composability and tokenisation, to foster a vibrant monetary ecosystem. This will be achieved via advanced payment rails such as CBDCs and retail FPS.

A public-private partnership on these lines could make the monetary system more adaptable and open across borders. A decade hence, users may take real-time, low-cost payments for granted, and payments across borders may be as seamless as the cross-border exchange they support. Consumer choice in financial services should be increased, and innovation will continue to push the frontiers of what is possible.

In all of this, innovation must start from an understanding of the concrete needs of households and businesses in the real economy – and of the policy demands they put on a monetary system. While decentralised technologies such as DLT offer many possibilities, users' needs should stay at the forefront of private innovation, just as the public interest remains the lodestar for central banks.

In both the design of new infrastructures and in regulation, there is an ongoing need for global cooperation between central banks, and indeed a wide range of new stakeholders. Supporting this cooperation will remain a key goal of the BIS.

Endnotes

- ¹ See the BIS Red Book Statistics, which collect data for retail cashless payments in 27 countries, <https://stats.bis.org/statx/toc/CPMI.html>.
- ² See Giannini (2011); Borio (2018)); Carstens (2019).
- ³ See BIS CPMI (2016); BIS (2021).
- ⁴ At present, there are no clear and harmonised guidelines as to who can serve as an oracle, or who is held accountable if a smart contract acts upon incorrect off-chain information. As it is impossible to write ex ante a smart contract that covers every possible contingency, some degree of centralisation is needed to resolve disputes.
- ⁵ Security in DLT refers to the robustness of consensus, ie confidence that the shared ledger is accurate. Security can be threatened by malicious actors who compromise the ledger to execute fraudulent transactions, as in a 51% attack (see glossary).
- ⁶ See glossary for a definition, Schär (2021) for an in-depth description, and Aramonte et al (2021) and Carter and Jeng (2021) for an assessment of risks and decentralisation. It is noteworthy that, even if DeFi often relies on anonymous and permissionless DLT to achieve decentralisation, permissioned DLT also allows for the use of smart contracts and associated composability (Auer (2022)). In this case, a set of centralised validators are in charge of validating transactions.
- ⁷ See Aramonte et al (2021).
- ⁸ See Arner et al (2019); Catalini and de Gortari (2021); Frost et al (2021); Gorton and Zhang (2021).
- ⁹ See Brainard (2021); Garratt et al (2022).
- ¹⁰ See Allen (2022).
- ¹¹ See BIS (2018), Auer (2019); Auer et al (2021).
- ¹² The limit is around four transactions per second for Bitcoin and 30 for Ethereum. Possible solutions to the problem of high rents stemming from congestion scalability (eg via “sharding”) usually introduce further technological complexity and require a higher degree of centralisation in the governance structure. Further, the sustainability of the incentive structure is not yet fully understood.
- ¹³ Bridges can be divided into two main types: “centralised” and “trustless”. The differences lie in how bridge transactions are confirmed and how the escrowed assets are stored. In a centralised system, a network of pre-selected validators track token deposits on the source chain, lock them up and mint tokens on the target chain. In a trustless system, anyone can become a validator. For every bridging transaction, validators are selected randomly from a pool to minimise the risks of manipulation. In both cases, the consensus and custodial activities are performed by a limited number of validators.

- ¹⁴ The need for collateral in many transactions is also detrimental to achieving an inclusive system. Requiring collateral means that it takes money to borrow money. For example, unless users already have sufficient funds in the form of cryptocurrency to post as collateral, they cannot borrow another cryptocurrency on lending platforms. See Aramonte et al (2022).
- ¹⁵ See IOSCO (2022).
- ¹⁶ As discussed above, these “gas fees” are designed to compensate validators. Although transaction costs are higher in DEXs, some traders prefer these platforms, in part due to their greater anonymity and interoperability with other DeFi applications.
- ¹⁷ See SEC (2022).
- ¹⁸ See CPMI-IOSCO (2021); Carstens et al (2021).
- ¹⁹ See Auer, Frost and Vidal Pastor (2022).
- ²⁰ See Brummer (2022).
- ²¹ See BCBS (2021); Auer et al (2022).
- ²² Tether, the largest stablecoin by market capitalisation, reportedly holds half of its reserves in certificates of deposit and commercial paper (currently around USD 25 billion in total), making it a significant investor in this market.
- ²³ BCBS (2021).
- ²⁴ See Carstens (2022); BIS (2021); BIS (2020); CPSS (2003).
- ²⁵ See Garratt et al (2022); McLaughlin (2021) argues more broadly for a network of “tokenised regulated liabilities” and of assets.
- ²⁶ See Schnabel and Shin (2004, 2018).
- ²⁷ See Boar et al (2021).
- ²⁸ See BIS (2021).
- ²⁹ See Bech et al (2020).
- ³⁰ See Garratt et al (2022); McLaughlin (2021).
- ³¹ See Deutsche Bundesbank (2020); Forster et al (2020); Pocher and Zichichi (2022).
- ³² See Mercan et al (2021).
- ³³ See Forster et al (2020) and Bechtel et al (2022) for a discussion of these features.

- ³⁴ In a CBDC, a payment only involves transferring a direct claim on the central bank from one end user to another. Funds do not pass over the balance sheet of an intermediary, and transactions are settled directly in central bank money, on the central bank's balance sheet and in real time. By contrast, in an FPS the retail payee receives final funds immediately, but the underlying wholesale settlement between PSPs may be deferred (see Carstens (2021)).
- ³⁵ See BIS CPMI (2021). The Unified Payment Interface in India and Bakong in Cambodia have seen particularly rapid adoption and promotion of financial inclusion goals.
- ³⁶ See Lovejoy et al (2022). By comparison, major card networks can process several thousand transactions per second, and Ethereum processes 30 per second.
- ³⁷ See Carstens and Her Majesty Queen Máxima (2022).
- ³⁸ See Miedema et al (2020); Bank of Ghana (2022).
- ³⁹ See Gjefle et al (2021). In the United States, distrust of banks and uncertainty around transactions are persistent challenges for unbanked individuals.
- ⁴⁰ See Tiwari et al (2022).
- ⁴¹ See CGIDE (2020); ECB (2020).
- ⁴² For example, in the Bahamas, the central bank does not have access to the individual identity information of CBDC users and will only share transaction information with law enforcement if a court order is made. See Boakye-Adjei et al (2022).
- ⁴³ See Leung et al (2022).
- ⁴⁴ See eg Board of Governors of the Federal Reserve System (2022); ECB (2020); Bank of England (2022); Bank of Japan (2020); Sveriges Riksbank (2021).
- ⁴⁵ For instance, some jurisdictions have defined new roles for private intermediaries in the monetary system, such as payment initiation service providers (EU), third-party app providers (India) or virtual banks (China, Hong Kong SAR, Korea). These often result in new regulatory requirements tailored to newly defined activities.
- ⁴⁶ For instance, production of intermediate goods in multiple economies requires an increasing volume of credit. See BIS (2017); Shin (2017).
- ⁴⁷ See Auer et al (2021) and glossary.
- ⁴⁸ See BIS Innovation Hub (2021).
- ⁴⁹ See Kosse and Mattei (2022).
- ⁵⁰ See Auer et al (2020), as updated through January 2022.
- ⁵¹ See BIS CPMI (2021).
- ⁵² See BIS Innovation Hub (2022); BISIH et al (2021, 2022).

Technical annex

Graph 1: End of week values. Categories comprise the largest nine stablecoins, 59 DeFi coins and 56 other cryptocurrencies. DeFi coins correspond to cryptocurrencies issued by DeFi platforms and with a market capitalisation to total value locked ratio smaller than 50, as reported by DeFi Llama. Total value locked refers to the size of capital pools underpinning DeFi protocols. For more details, see Table A2 from Auer (2022).

Graph 2.A: Outliers larger than 450 Gwei (10^{-9} ETH) are excluded from the graph.

Graph 4.A: Based on bridges and cross-chain protocols.

Graph 5.A: Transaction costs are measured as the relative bid-ask spread, defined as $2 \times (\text{ask price} - \text{bid price}) / (\text{ask price} + \text{bid price})$ for Tether-Ether. Centralised is a simple average of crypto exchanges Coinbase and Binance. Decentralised is based on Uniswap. Weekly averages of daily values.

Graph 5.B: Centralised = Binance, Coinbase and FTX; Decentralised = Curve.fi, PancakeSwap (v2) and Uniswap (V2).

Graph 6.B: Companies with a focus on cryptocurrencies technologies. The full list of the companies is available at www.blockdata.tech/blog/general/banks-investing-blockchain-companies.

Graph 10.B: For the United States, Canada and the EU, average of interchange fees on credit and debit cards. Total cost to merchants may be higher.

Graph A1.B: The price corresponds to the low price.

Graph B1.A: Cross-country monthly averages of daily active users.

Graph B1.C: Willingness to take financial risks for US consumers of age 20–79. Weighted average (by survey weights) across respondents. The sample covers the period January 2020–July 2021.

References

Allen, H (2022), "We're asking the wrong questions about stablecoins", *Financial Times*, 2 June.

Aramonte, S, W Huang and A Schrimpf (2021): "DeFi risks and the decentralisation illusion", *BIS Quarterly Review*, December.

Aramonte, S, S Doerr, W Huang and A Schrimpf (2022): "DeFi lending: intermediation without information?", *BIS Bulletin*, no 57, June.

Arner, D, R Auer and J Frost (2020): "Stablecoins: risks, potential and regulation", *Bank of Spain Financial Stability Review*, November.

Auer, R (2019): "Beyond the doomsday economics of "proof-of-work" in cryptocurrencies", *BIS Working Papers*, no 765, January.

——— (2022): "Embedded supervision: how to build regulation into decentralised finance", *Cryptoeconomic Systems*, forthcoming.

Auer, R, P Haene and H Holden (2021): "Multi-CBDC arrangements and the future of cross-border payments", *BIS Papers*, no 115, March.

Auer, R, G Cornelli and J Frost (2020): "Rise of the central bank digital currencies: drivers, approaches and technologies", *BIS Working Papers*, no 880, August.

Auer, R, G Cornelli, S Doerr, J Frost and L Gambacorta (2022): "Chained to speculation? Feedback trading in crypto markets", *BIS Working Papers*, forthcoming.

Auer, R, M Farag, U Lewrick, L Orazem and M Zoss (2022): "Banking in the shadow of Bitcoin? The institutional adoption of cryptocurrencies", *BIS Working Papers*, no 1013, May.

Auer, R, J Frost and J Vidal Pastor (2022): "Miners as intermediaries: extractable value and market manipulation in crypto and DeFi", *BIS Bulletin*, no 58, June.

Auer, R, C Monnet and H S Shin (2021): "Distributed ledgers and the governance of money", *BIS Working Papers*, no 924, January.

Auer, R and D Tercero-Lucas (2021): "Distrust or speculation? The socioeconomic drivers of U.S. cryptocurrency investments", *BIS Working Papers*, no 951, July.

Bank of England (2022): *Responses to the Bank of England's Discussion Paper on new forms of digital money*, March.

Bank of Ghana (2022): *Design paper of the digital Cedi (eCedi)*, March.

Bank of Japan (2020): *The Bank of Japan's approach to central bank digital currency*, October.

Basel Committee on Banking Supervision (BCBS) (2021): *Prudential treatment of cryptoassets exposures*, consultative document, June.

Bech, M, C Boar, D Eidan, P Haene, H Holden and W Toh (2022): “Using CBDCs across borders: lessons from practical experiments”, BIS Innovation Hub, June.

Bech, M, J Hancock, T Rice and A Wadsworth (2020): “On the future of securities settlement” *BIS Quarterly Review*, March.

Bechtel, A, A Ferreira, J Gross and P Sandner (2022): *The future of payments in a DLT-based European economy: a roadmap*, German Institute for Japanese Studies.

Bank for International Settlements (BIS) (2017): “Understanding globalisation”, *87th Annual Report*, June, Chapter IV,

——— (2018): “Cryptocurrencies: looking beyond the hype”, *Annual Economic Report 2018*, June, Chapter V.

——— (2020): “Central banks and payments in the digital era”, *Annual Economic Report 2020*, June, Chapter III.

——— (2021): “CBDCs: an opportunity for the monetary system”, *Annual Economic Report 2021*, June, Chapter III.

BIS Committee on Payments and Market Infrastructures (BIS CPMI) (2016): *Fast payments – enhancing the speed and availability of retail payments*, November.

——— (2021): *Developments in retail fast payments and implications for RTGS systems*, December.

BIS Innovation Hub (BISIH) (2021): “Nexus: a blueprint for instant cross-border payments”, July.

——— (2022): “Deep dive into the experience gained across the BIS Innovation Hub multi-CBDC projects”, mimeo.

BISIH, Reserve Bank of Australia (RBA), National Bank of Malaysia (NBM), Monetary Authority of Singapore (MAS), and South African Reserve Bank (SARB) (2022): “Project Dunbar – International settlements using multi-CBDCs”, March.

BISIH, Hong Kong Monetary Authority (HKMA), Bank of Thailand (BoT), Digital Currency Institute of the People’s Bank of China (PBC) and Central Bank of the United Arab Emirates (CBUAE) (2021): “Inthanon-LionRock to mBridge: Building a multi-CBDC platform for international payments”, April.

Boakye-Adjei, N, R Auer, J Frost, J Prenio, H Banka, A Faragallah and H Natarajan (2022): “Central bank digital currencies (CBDCs): a new tool in the financial inclusion toolkit?”, *FSI Insights*, April.

Boar, C, S Claessens, A Kosse, R Leckow and T Rice (2021): “Interoperability between payment systems across borders”, *BIS Bulletin*, no 49, December.

Board of Governors of the Federal Reserve System (2022): “Money and payments: The U.S. dollar in the age of digital transformation”, January.

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

Borio, C (2019): "On money, debt, trust and central banking", *BIS Working Papers*, no 763, January.

Brainard, L (2021): "Private money and central bank money as payments go digital: an update on CBDCs", speech at the Consensus by CoinDesk 2021 Conference, Washington DC, 24 May.

Brummer, C (2022): "Disclosure, Dapps and DeFi", *Stanford Journal of Blockchain Law and Policy*, forthcoming.

Buterin, V (2021): "Why sharding is great: demystifying the technical properties", vitalik.ca/general/2021/04/07/sharding.htm.

Carstens, A, S Claessens, F Restoy and H S Shin (2021): "Regulating big techs in finance", *BIS Bulletin*, no 45, August.

Carstens, A (2022): "Digital currencies and the soul of money", speech at the Goethe University, 18 January.

——— (2021): "Digital currencies and the future of the monetary system", remarks at the Hoover Institution policy seminar, 27 January.

——— (2019): "The future of money and the payment system: what role for central banks?", lecture at Princeton University, 5 December.

Carstens, A and Her Majesty Queen Máxima (2022): "CBDCs for the people", *Project Syndicate*, 18 April.

Carter, N and L Jeng (2021): "DeFi protocol risks: the paradox of DeFi", in B Coen and D Maurice (eds), *Regtech, supotech and beyond: innovation and technology in financial services*, RiskBooks.

Catalini, C and A de Gortari (2021): "On the economic design of stablecoins", mimeo.

Committee on Payments and Settlement Systems (2003): *The role of central bank money in payment systems*, 12 August.

CPMI and International Organization of Securities Commissions (IOSCO) (2021): *Application of the Principles for Financial Market Infrastructures to stablecoin arrangements*, October.

Comparitech (2022): [Worldwide cryptocurrency heists tracker](#), February.

Consultative Group for Innovation and the Digital Economy (CGIDE) (2020): *Enabling open finance through APIs*, December.

Deutsche Bundesbank (2020): *Money in programmable applications*, report of the Working Group on Programmable Money, December.

Duarte, A, 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.

European Central Bank (ECB) (2020): *Report on a digital euro*, October.

Foley, S, J Karlsen and T Putnins (2019): "Sex, drugs, and Bitcoin: how much illegal activity is financed through cryptocurrencies?", *Review of Financial Studies*, vol 32, no 5, pp 1798–853.

Forster, M, J Gross, A Kamping, S Katilmis, M Reichel, P Sandner and P Schröder (2020): "The future of payments: programmable payments in the IoT sector", mimeo.

Frost, J, P Wierds and H S Shin (2020): "An early stablecoin? The Bank of Amsterdam and the governance of money", *BIS Working Papers*, no 902, November.

Garratt, R, M Lee, A Martin and J Torregrossa (2022): "The future of payments is not stablecoins", *Liberty Street Economics*, 7 February.

Giannini, C (2011): *The age of central banks*, Edward Elgar.

Gjefle, E, Z Herring, C Kubli, B O'Rea and G Rakusen, G (2021): *Centering users in the design of digital currency*, MIT Digital Currency Institute and Maiden Labs.

Gorton, G and J Zhang (2022): "Taming wildcat stablecoins", *University of Chicago Law Review*, vol 90, forthcoming.

Hayashi, F 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.

Hileman, G (2015): "The Bitcoin market potential index", *Proceedings of the Second Workshop on Bitcoin Research in Association with Financial Cryptography and Data Security*, Springer.

International Organization of Securities Commissions (IOSCO) (2022): *IOSCO decentralised finance report*, March.

Kosse, A and I Mattei (2022): "Gaining momentum – Results of the 2021 BIS survey on central bank digital currencies", *BIS Papers*, no 125, May.

Knittel, M, S Pitts and R Wash (2019): "The most trustworthy coin: how ideological tensions drive trust in Bitcoin", *Proceedings of the ACM on Human-Computer Interaction*, vol 3, no 36, pp 1–23.

Leung, D, D Arner, J Frost and B Nolens (2022): "Corporate digital identity: no silver bullet, but a silver lining?", *BIS Papers*, forthcoming.

Lovejoy, J, C Fields, M Virza, T Frederick, D Urness, K Karwaski, A Brownworth and N Narula (2022): "A high performance payment processing system designed for central bank digital currencies", February.

McLaughlin, T (2021): “The regulated internet of value”, Citi Treasury and Trade Solutions.

Mercan, S, A Kurt, E Erdin and K Akkaya (2021): “Cryptocurrency solutions to enable micro-payments in consumer IoT”, Cornell University, February.

Miedema, J, C Minwalla, M Warren and D Shah (2020): “Designing a CBDC for universal access”, *Bank of Canada Staff Analytical Notes*, no 2020-10.

Pocher, N and M Zichichi (2022): “Toward CBDC-based machine-to-machine payments in consumer IoT”, 37th ACM/SIGAPP Symposium on Applied Computing, April.

Schär, F (2021): “Decentralized finance: on blockchain- and smart contract-based financial markets”, *Federal Reserve Bank of St. Louis Review*, vol 103, no 2, April.

Schnabel, I and H S Shin (2004): “Liquidity and contagion: the crisis of 1763”, *Journal of the European Economic Association*, vol 2, no 6, pp 929–68, December.

——— (2018): “Money and trust: lessons from the 1620s for money in the digital age”, *BIS Working Papers*, no 698, February.

Securities and Exchange Commission (SEC) (2022): *Staff Accounting Bulletin*, no 121, March.

Shin, H S (2017): “Globalisation: real and financial”, speech at the BIS Annual General Meeting, 25 June.

Sveriges Riksbank (2022): “E-krona pilot Phase 2”, April.

Swartz, L (2020): *New money: how payment became social media*, Yale University Press.

Tiwari, S, S Sharma, S Shetty and F Packer (2022): “The design of a data governance system”, *BIS Papers*, no 124, May.

Glossary

51% attack: When a malicious actor is able to compromise more than half of the validators on the network, the actor can execute fraudulent transactions.

Application programming interface (API): a set of rules and specifications followed by software programmes to communicate with each other, and an interface between different software programmes that facilitates their interaction.

Atomic settlement: instant exchange of two assets, such that the transfer of one occurs only upon transfer of the other one.

Blockchain: a form of permissionless distributed ledger in which details of transactions are held in the ledger in the form of blocks of information.

Central bank public goods: goods and services provided by the central bank that serve the public interest, including payment infrastructures and trust in the currency.

Composability: the capacity to combine different components in a system, such as DeFi protocols.

Consensus: in DLT applications, the process by which validators agree on the state of a distributed ledger.

Cryptocurrency (also cryptoasset or crypto): a type of private sector digital asset that depends primarily on cryptography and distributed ledger or similar technology.

Data architecture: as used here, the combination of identification and application programming interfaces that allows for the secure use of data.

Decentralised applications (dApps): DeFi applications offering services such as lending or trading, predominantly between cryptocurrencies and stablecoins.

Decentralised exchanges (DEXs): marketplaces where transactions occur directly between cryptocurrency or stablecoin traders.

Decentralised finance (DeFi): a set of activities across financial services built on permissionless DLT such as blockchains.

Digital wallet: an interface that allows users to make transfers or otherwise transact in digital money and assets.

Distributed ledger technology (DLT): a means of saving information through a distributed ledger, ie a repeated digital copy of data available at multiple locations.

Gas fees: unit that measures the amount of computational effort required to execute specific operations on the Ethereum network. Gas refers to the fee required to conduct a transaction on Ethereum successfully.

Internet of Things: software, sensors and network connectivity embedded in physical devices, buildings and other items that enable those objects to (i) collect and exchange data and (ii) send, receive and execute commands, including payments.

Level 1: competing blockchains are sometimes referred to as “level 1” networks, to distinguish them from separate off-chain (“level 2”) networks that record transactions outside the distributed ledger.

Market integrity: the prevention of illicit activities in the monetary system, such as money laundering and terrorism financing, as well as market manipulation.

Monetary system: the set of institutions and arrangements around monetary exchange. This consists of two components: money and payment systems.

Multi-CBDC arrangements: solutions to make CBDCs compatible, interlink CBDC systems or create a shared system for cross-border, cross-currency CBDC payments.

Non-fungible tokens (NFTs): unique cryptographic tokens that exist on a blockchain and cannot be replicated, used to represent ownership of eg artwork, real estate or other assets.

Open banking: the sharing and leveraging of customer-permissioned data by banks with third-party developers and firms to build applications and services.

Open source: a feature whereby the original source code is made publicly available.

Oracle: a service that provides outside (“off-chain”) information for use by smart contracts in a DLT system.

Permissioned DLT: a form of DLT whereby only a pre-defined group of trusted institutions can act as a validating node.

Permissionless DLT: a form of DLT where any participant can act as a validating node, for instance with (permissionless) blockchains.

Programmability: a feature of DLT and other technologies whereby actions can be programmed or automated.

Proof-of-stake: a method by which validators pledge or “stake” coins that are used as an incentive that transactions added to the distributed ledger are valid.

Proof-of-work: a method by which validators compete to perform mathematical computations to verify and add transactions to the distributed ledger.

Pseudo-anonymity: a practice by which users are identified by an address or pseudonym, for instance in a publicly viewable ledger.

Security: in DLT applications, security often refers to the robustness of consensus, ie confidence that the shared ledger is accurate.

Smart contract: self-executing applications that can trigger an action if some pre-specified conditions are met.

Stablecoin: a cryptocurrency that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets.

Token: a digital representation of value in a DLT system. Assets that are represented with a token can be said to be “tokenised”. (This is unrelated to the distinction between account-based vs token-based payment instruments.)

Tokenised deposit: a digital representation of a bank deposit in a DLT system. A tokenised deposit represents a claim on a commercial bank, just like a regular deposit.

Total value locked: total value of assets deposited in a DeFi protocol.

Throughput: a measure of the number of transactions that can be processed in a payment system in a given period of time, eg per second.

Validator or validating node: an entity that verifies transactions in a blockchain. In some networks, this role is played by “miners”.

Zero-knowledge proof: a cryptographic technique that allows one party to prove to another party that a statement is true without revealing information beyond that fact.