III. Blueprint for the future monetary system: improving the old, enabling the new

Key takeaways

- Tokenisation of money and assets has great potential, but initiatives to date have taken place in silos without access to central bank money and the foundation of trust it provides.
- A new type of financial market infrastructure – a unified ledger – could capture the full benefits of tokenisation by combining central bank money, tokenised deposits and tokenised assets on a programmable platform.
- As well as improving existing processes through the seamless integration of transactions, a unified ledger could harness programmability to enable arrangements that are currently not practicable, thereby expanding the universe of possible economic outcomes.
- Multiple ledgers – each with a specific use case – might coexist, interlinked by application programming interfaces to ensure interoperability as well as promote financial inclusion and a level playing field.

Introduction

Throughout history, developments in the monetary system and society at large have been closely interwoven. This interplay has been a story of one side pulling the other, leading to dramatic leaps in economic activity over time. On the one hand, the evolving needs and demands of society have spurred the monetary system to adapt. On the other hand, key innovations in money and payments have unleashed latent demand for new types of economic activity that have led to dramatic spurts of economic growth and development.

The rapid expansion of trade and commerce over the past 500 years would be scarcely imaginable if buyers and sellers still had to cart around heavy chests full of metal coins to pay for goods and services. The advent of money in the form of book entries on ledgers overseen by trusted intermediaries opened the door to new financial instruments that bridged both geographical distance and the long lags between the delivery of goods and settlement of payments.[1] With the advent of the electronic age, paper ledgers became digital, adding impetus to the "dematerialisation" of money as well as claims on financial and real assets. Electronic bookkeeping accelerated paper-based processes, allowing accounts to be updated at the speed of light. Through dematerialisation and digitalisation, the interplay between money and the economy has wrought profound changes on society at large.

Today, the monetary system stands at the cusp of another major leap. Following dematerialisation and digitalisation, the key development is **tokenisation** – the process of representing claims digitally on a *programmable* platform. This can be seen as the next logical step in digital recordkeeping and asset transfer. Tokenisation could dramatically enhance the capabilities of the monetary and financial system by harnessing new ways for intermediaries to interact in serving end users, removing the traditional separation of messaging, reconciliation and settlement. Tokenisation could unlock new types of economic arrangement that the frictions inherent in the current monetary system have hitherto made impractical.

Crypto and decentralised finance (DeFi) have offered a glimpse of tokenisation's promise, but crypto is a flawed system that cannot take on the mantle of the future of money.[2] Not only is crypto self-referential, with little contact with the real world, it also lacks the anchor of the trust in money provided by the central bank. While stablecoins have mushroomed to fill this vacuum by mimicking central bank money, the implosion of the crypto universe in the past year shows that there is no substitute for the real thing. Away from crypto, efforts by commercial banks and other private sector groups have explored the capabilities of tokenisation for real-world use cases. But these efforts have been hampered by the silos erected by each project and the resulting disconnect from other parts of the financial system. These projects also lack integration with a tokenised version of the settlement asset in the form of a central bank digital currency (CBDC).

The collapse of crypto and the faltering progress of other tokenisation projects underline a key lesson. The success of tokenisation rests on the foundation of trust provided by central bank money and its capacity to knit together key elements of the financial system. This capacity derives from the central bank's role at the core of the monetary system. Among its many functions, the central bank issues the economy's unit of account and ensures the finality of payments through settlement on its balance sheet. Building on the trust in central bank money, the private sector uses its creativity and ingenuity to serve customers.[3] In particular, commercial banks issue deposits, the most common form of money held by the public. Supported by regulation and supervision, this two-tiered structure preserves the "singleness of money": the property that payments denominated in the sovereign unit of account will be settled at par, even if they use different forms of privately and publicly issued monies.

While the current monetary system has served society well, pinch points in the system that emerge from time to time highlight the frictions that users chafe against. These frictions result from the current design of the monetary system where digital money and other claims reside in siloed proprietary databases, located at the edges of communication networks. These databases must be connected through third-party messaging systems that send messages back and forth. As a result, transactions need to be reconciled separately before eventually being settled with finality. During this back-and-forth process, not only do participants have an incomplete view of actions and circumstances, but the uncertainties and misaligned incentives preclude some transactions that have clear economic rationale. While workarounds such as collateral or escrow can mitigate such frictions, these solutions have their limits and create their own inefficiencies. Tokenisation is a more fundamental route towards addressing the shortcomings of the current system.

New demands are also emerging from end users themselves as advances in digital services raise their expectations. Indeed, these emerging demands may be just the tip of the iceberg. As services delivered through smartphone apps make deep inroads into people's daily lives, users expect the same seamless operation of the monetary and financial system as the seamless interactions of apps on their smartphones. These demands are beginning to outgrow the siloed domains and their reliance on the to-and-fro processes at the edges of the network.

This chapter presents a blueprint for a future monetary system that harnesses the potential of tokenisation to improve the old and enable the new. The key elements of the blueprint are CBDCs, tokenised deposits and other tokenised claims on financial and real assets. The blueprint envisages these elements being brought together in a new type of financial market infrastructure (FMI) – a "**unified ledger**".[4] The full benefits of tokenisation could be harnessed in a unified ledger due to the settlement finality that comes from central bank money residing in the same venue as other claims. Leveraging trust in the central bank, a shared venue of this kind has great potential to enhance the monetary and financial system.

A unified ledger transforms the way that intermediaries interact to serve end users. Through programmability and the platform's ability to bundle transactions ("composability"), a unified ledger allows sequences of financial transactions to be automated and seamlessly integrated. This reduces the need for manual interventions and reconciliations that arise from the traditional separation of messaging, clearing and settlement, thereby eliminating delays and uncertainty. The ledger also supports simultaneous and instantaneous settlement, reducing settlement times and credit risks. Settlement in central bank money ensures the singleness of money and payment finality.

Moreover, by having "everything in one place", a unified ledger provides a setting in which a broader array of contingent actions can be automatically executed to overcome information and incentive problems. In this way, tokenisation could expand the universe of possible contracting outcomes. The unified ledger thus opens the way for entirely new types of economic arrangement that are impossible today due to incentive and informational frictions. The eventual transformation of the financial system will be limited only by the imagination and ingenuity of developers that build on the system, much as the ecosystem of smartphone apps has far exceeded the expectations of the platform builders themselves. Even in the near term, a unified ledger could unlock arrangements that have clear economic rationale. Possibilities include new types of deposit contract that bolster financial stability, improvements in supply chain finance and new ways to improve the financial system's resilience and integrity.

The unified ledger concept can be broad or narrow, with the first instances likely to be application-specific in scope. For example, one ledger could aim at improving securities settlement, while another could facilitate trade finance in supply chains. Tokenised forms of money would figure in each ledger to provide the transaction medium. Each unified ledger would bring together only the intermediaries and assets required for each application. The scope of a ledger will also determine the relevant players that must be involved in the governance arrangements. Separate ledgers could be connected through application programming interfaces (APIs), or, as their scope expands over time, they could incorporate additional assets and entities, or merge together.

Some of the benefits envisaged from the unified ledger could be reaped by interlinking existing systems through APIs into a "network of networks". While such a network of networks would still consist of separate systems and fall short of fully fledged programmability across systems, the worst drawbacks of siloed systems could be mitigated.

This next stage in the financial system's journey will be one that combines the best efforts of both the private and public sectors. Central banks could work with regulated private entities to develop technological solutions and standards to meet specific use cases. With their public interest mandate, central banks are best placed to establish a common venue for each use case by interlinking with the monetary system. Proper oversight and supervision will be a prerequisite for this endeavour.

In embracing evolution and change, central banks and the private sector should follow key guiding principles to ensure that the monetary system harnesses innovation for the public interest. First, the tried and tested division of roles between the public and private sector in the two-tiered system remains the cornerstone. The second principle is upholding a competitive level playing field that promotes innovation and financial inclusion. And third, the future monetary system needs to meet the highest standards of data security and privacy, while ensuring system integrity by guarding against illicit activity such as money laundering, financing of terrorism and fraud.

The rest of the chapter introduces the concept of tokenisation and how it could be mobilised in the design of key elements of the future monetary system: central

bank digital currencies, tokenised deposits and tokenised claims on financial and real assets. The chapter then proposes unified ledgers to integrate these components seamlessly. Concrete examples show how this kind of integration could improve the old and enable the new. The final section discusses high-level guiding principles on scope, governance, incentives for participation, operational resilience and privacy.

Tokenising money and assets

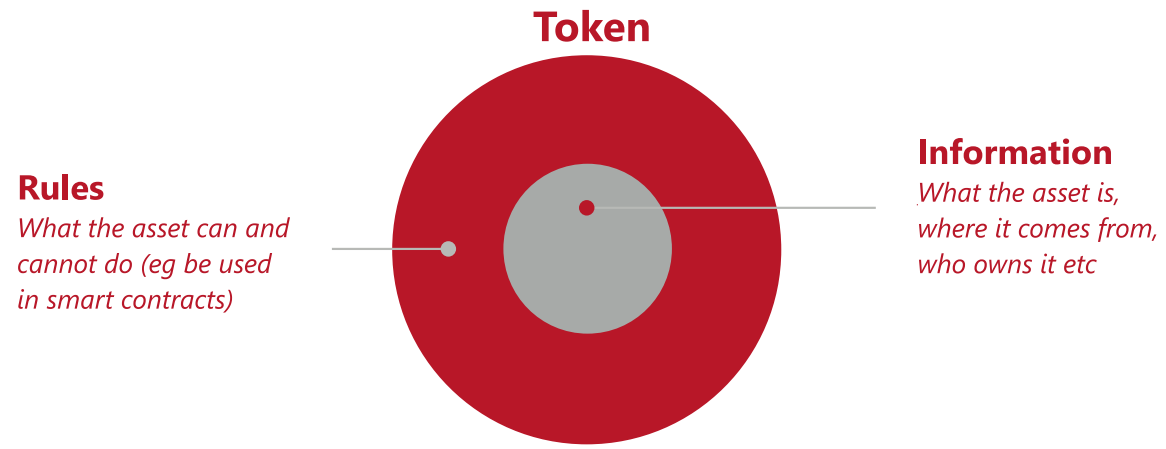
The blueprint for the future monetary system rests on several key concepts surrounding tokenisation.

Tokenisation basics

Traditional ledger systems and tokenised systems operate under fundamentally different rules. In traditional ledger systems, account managers are entrusted with maintaining and updating an accurate record of ownership. In contrast, in a tokenised setting, money or assets become "executable objects" that are maintained on **programmable platforms.** They could be transferred through the execution of programming instructions issued by system participants without the intervention of an account manager. While tokenisation does not eliminate the role of intermediaries, it changes the nature of that role. The role of the operator in a tokenised environment is as a trusted intermediary serving in a governance role as the rule book's curator, rather than as a bookkeeper who records individual transactions on behalf of account holders.

The claims traded on programmable platforms are called **tokens**. Tokens are not merely digital entries in a database. Rather, they integrate the records of the underlying asset normally found in a traditional database with the rules and logic governing the transfer process for that asset (Graph 1). Hence, whereas in traditional systems the rules that govern the updating of asset ownership are usually common to all assets, tokens can be customised to meet specific user or regulatory requirements that apply to individual assets. We discuss in a later section how this dual nature of tokens could be used to good effect in a supervisory and compliance setting by

Tokens both define assets and specify what can be done with them — Graph 1



Source: Aldasoro et al (2023).

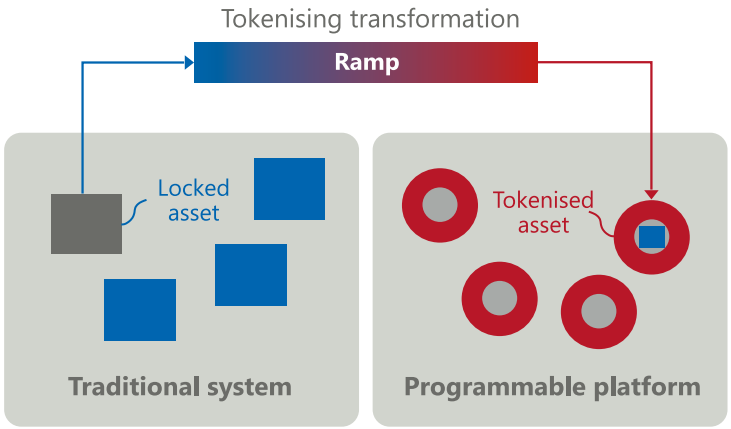
directly embedding supervisory features into the token itself, which can be tailored to specific rules.

Tokenisation – the process of recording claims on financial or real assets that exist on a traditional ledger on a programmable platform – introduces two important capabilities. First, by dispensing with messaging and the reliance on account managers to update records, it provides greater scope for **composability**, whereby several actions are bundled into one executable package. Second, it enables the **contingent performance of actions** through smart contracts, ie logical statements such as "if, then, or else". By combining composability and contingency, tokenisation makes the conditional performance of actions more readily attainable, even quite complex ones.[5]

This chapter examines several use cases of such contingent performance of actions. One is in the design of supply chains in which several participants interact under uncertainty and with incentives that may not be perfectly aligned. Another example is the design of banking deposit contracts where built-in contingencies that depend on the actions of *other* depositors alter the incentives of depositors to be a first mover in a bank run setting. Such contingent deposit contracts could nullify the so-called first-mover advantage.

Many interesting real-world applications require the tokenisation of assets that currently exist in traditional databases. These assets could range from financial securities whose ownership is recorded in securities depositories to real assets, such as commodities or real estate. The tokenisation process for such assets occurs through so-called ramps that define a mapping between assets in traditional databases and their counterparts in tokenised form (Graph 2). The assets in the traditional database are immobilised or "locked" to serve as collateral that backs the tokens issued on the programmable platform. The locking of assets ensures that the transfer of their tokenised counterparts guarantees the transfer of the underlying assets.

Ramps map assets to their tokenised counterparts on programmable platforms Graph 2



Source: Aldasoro et al (2023).

Central bank digital currency and private tokenised monies

The full potential of tokenisation needs a monetary unit of account that denominates transactions, as well as the accompanying means of payment. In crypto, stablecoins that reside on the same platform as other crypto assets perform the role of the means

of payment. However, for reasons highlighted already, central bank money and the settlement finality that it brings is a much firmer foundation for tokenisation.[6] The full potential of tokenisation is therefore best harnessed by having central bank money reside on the same venue as other tokenised claims. This is because programmable transactions could incorporate settlement using the economy's unit of account as an essential part of the tokenised arrangement.

For this reason, the development of a wholesale CBDC is core to the functioning of a tokenised environment. As a tokenised means of settlement, wholesale CBDCs would serve a similar role as reserves in the current system, but with the added functionalities enabled by tokenisation. Transactions in wholesale CBDC could incorporate all the features such as the composability and contingent performance of the actions mentioned above. The BIS Innovation Hub, in partnership with central banks around the world, stands at the forefront of experimentation with CBDCs and tokenisation (Box A).

Enhanced digital representations of central bank money could include a retail variant open to use by ordinary users. A retail CBDC is a digital version of physical cash that can be used by households and firms for everyday transactions. By providing the public with a ready way to convert alternative private digital monies into digital cash, ie a direct link to the sovereign unit of account in digital form, the central bank would further support singleness.[7]

While the role of CBDCs in a tokenised environment is clear, there is greater room for debate concerning the appropriate form of private tokenised money that complements CBDCs. There are currently two main candidates for private tokenised monies: tokenised deposits and asset-backed stablecoins.[8] Both represent liabilities of the issuer, who promises customers that they can redeem their claims at par value in the sovereign unit of account. However, tokenised deposits and asset-backed stablecoins differ in how they are transferred and in their role in the financial system. These differences have implications for their attributes as a tokenised form of money that complements CBDCs.

Tokenised deposits could be designed to resemble the workings of regular bank deposits in the current system; see McLaughlin (2021). They could be issued by commercial banks and represent a claim on the issuer. Like regular deposits, they would not be directly transferable. Central banks' liquidity provision for settlement would continue to ensure smooth functioning of payments.

To bring out the parallels between tokenised deposits and conventional deposits in the current system, consider how a payment is made currently, using deposit balances. When John makes a payment of GBP 100 to Paul, Paul does not receive a GBP 100 deposit at John's bank. Rather, John's account balance at his bank is reduced by GBP 100, while Paul's balance at his bank increases by the same amount. Meanwhile, the adjustments in the individual accounts at the two banks are matched by a transfer in central bank reserves between the two banks. The same payment outcome could be achieved in a tokenised world by reducing John's tokenised deposit holding at his bank and increasing Paul's tokenised deposit holding at his, while simultaneously settling the payment through a concurrent transfer of wholesale CBDC (Graph 3). Paul continues to have a claim only on his bank, where he is a verified customer, and has no claim on John's bank, nor on John.

Tokenised deposits would not only preserve but at times enhance some key advantages of the current two-tier monetary system.

First, tokenised deposits would help preserve the singleness of money. In the current system, singleness of money for payments involving commercial bank deposits is achieved because central banks operate settlement infrastructures that guarantee the ultimate transfer of payments at par value in terms of the sovereign unit of account. Tokenised deposits would preserve this arrangement. However, the fact that

Box A

Experiments with wholesale central bank digital currencies and tokenisation

The BIS Innovation Hub stands at the forefront of experimentation with central bank digital currencies (CBDCs) and tokenised assets (Table A1). The work includes projects within and across jurisdictions and in multiple currencies, often in partnership with the private sector.

Experiments with CBDCs[1] have shown that tokenisation can reduce the complexity of securities settlement by facilitating simpler and more direct holding systems, as shown in Project Helvetia. The findings from Helvetia also suggest that using wholesale CBDC, as opposed to linking real-time gross settlement systems to a financial infrastructure, could provide greater scope for future innovation and efficiency gains in the settlement process. In this context, tokenisation facilitates increased automation through the use of smart contracts. It can speed up settlement as tokenised assets typically settle automatically, ie both legs of a transaction settle simultaneously and instantly. Tokenisation also increases operational transparency, as shown in Projects Jura, Dunbar and mBridge. These three completed wholesale CBDC projects focus on use cases where CBDCs were transferred against either another CBDC (payment versus payment, PvP) or tokenised securities (delivery versus payment, DvP). While systems exist to cater to both cross-border PvP and DvP, coverage is not universal in terms of currencies and jurisdictions, and costs are often deemed too high for universal usage. These projects were able to offer new solutions to long-standing operational challenges and policy questions. For example, in Project Jura, subnetworks allow the platform to respect jurisdictional boundaries and data location requirements and notaries allow central banks to control and monitor transactions in their currencies both in terms of payments and PvP settlements. Moreover, programmability allows new types of contingent payment, while certain policy measures (eg capital controls) can be built in from the start.

Beyond CBDCs, other projects have explored the practical and technological complexities of tokenised assets in the context of green finance (Project Genesis) and trade finance (Project Dynamo).

A bird's eye view of BIS Innovation Hub projects on CBDC and tokenisation — Table A1

	Helvetia	Jura	Genesis	Dunbar	mBridge	Dynamo
Main use case	Tokenised assets settlement in wholesale CBDC	Cross-border settlement with wholesale CBDC	Tokenised green bonds + delivery of carbon credits	International settlements using multiple CBDCs	Multilateral payments using multiple CBDCs	Smart contract programmability in trade finance
BIS IH Centre	Switzerland	Switzerland	Hong Kong SAR	Singapore	Hong Kong SAR	Hong Kong SAR
Participants	SNB	BDF, SNB	HKMA	MAS, SARB, RBA, BNM	HKMA, BOT, PBC, CBUAE	HKMA
Relevant currencies	CHF	EUR, CHF	HKD	AUD, MYR, SGD, SAR	HKD, CNY, THB, AED	HKD
PvP	✗	✓	✗	✓	✓	✗
DvP	✓	✓	✓	✗	✗	✗

PvP = payment versus payment; DvP = delivery versus payment.

BDF = Bank of France; BNM = Central Bank of Malaysia; BOT = Bank of Thailand; CBUAE = Central Bank of the United Arab Emirates; HKMA = Hong Kong Monetary Authority; MAS = Monetary Authority of Singapore; RBA = Reserve Bank of Australia; SARB = South African Reserve Bank; SNB = Swiss National Bank.

Source: BIS.

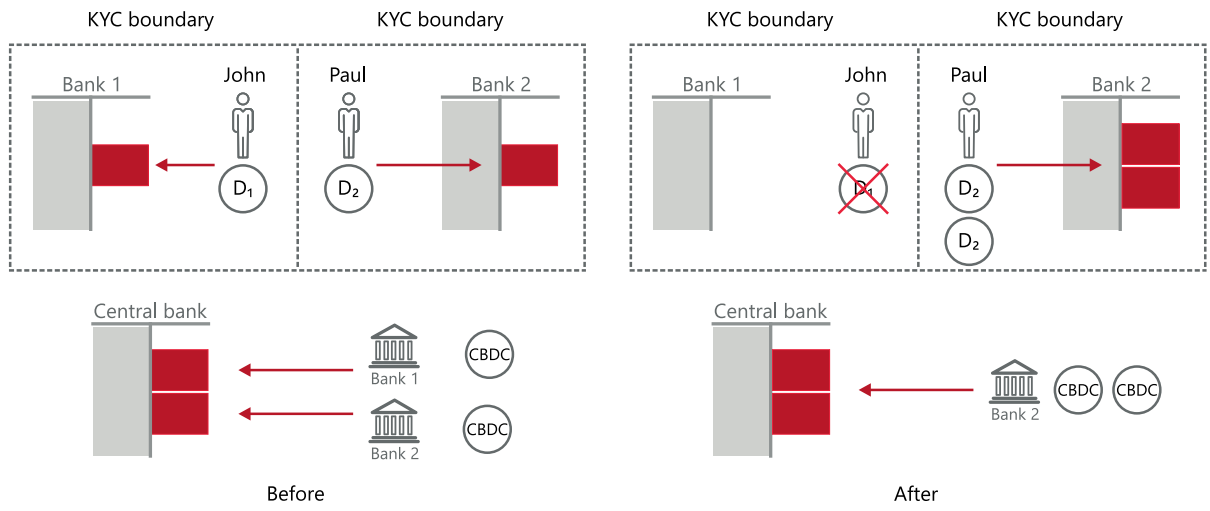
[1] See BIS Innovation Hub (2023).

settlement in wholesale CBDC is automatically triggered through smart contracts would improve the immediacy of the current process, further narrowing time gaps to reduce risks.

Second, payments in tokenised deposits settled in wholesale CBDC would ensure finality. By using its own balance sheet as the ultimate means of settlement, the central bank provides the means for ensuring the finality of wholesale payments. As the trusted intermediary, it is the central bank that debits the account of the payer

Non-bearer instrument model of tokenised deposits

Graph 3



Dotted lines denote know-your-customer (KYC) boundaries. The red rectangles indicate the liabilities of the respective issuers (Banks 1 and 2 and the central bank), with red arrows originating from the holder of those liabilities. D_1 and D_2 denote the tokens held by John and Paul, which are liabilities of their respective banks.

Source: Garratt and Shin (2023).

and credits the account of the payee, after which the payment is final and irrevocable. In the above example, finality ensures that Paul does not have a claim on John (or John's bank), but on his bank only.

Third, tokenised deposits would ensure that banks could continue to offer credit and liquidity in a flexible way. In the current two-tiered monetary system, banks provide individuals and firms with loans and on-demand access to liquidity through, for example, credit lines. Most of the money that circulates in the monetary system today is created in this way. This is in large part possible because the recipients of credit can simultaneously hold deposit accounts at banks, allowing banks to create deposits when making a loan.[9] Unlike narrow banking models, this flexibility allows banks to adjust to the needs of firms and households in the light of changing economic or financial conditions. Of course, adequate regulation and supervision are required to prevent excessive credit growth and risk-taking.

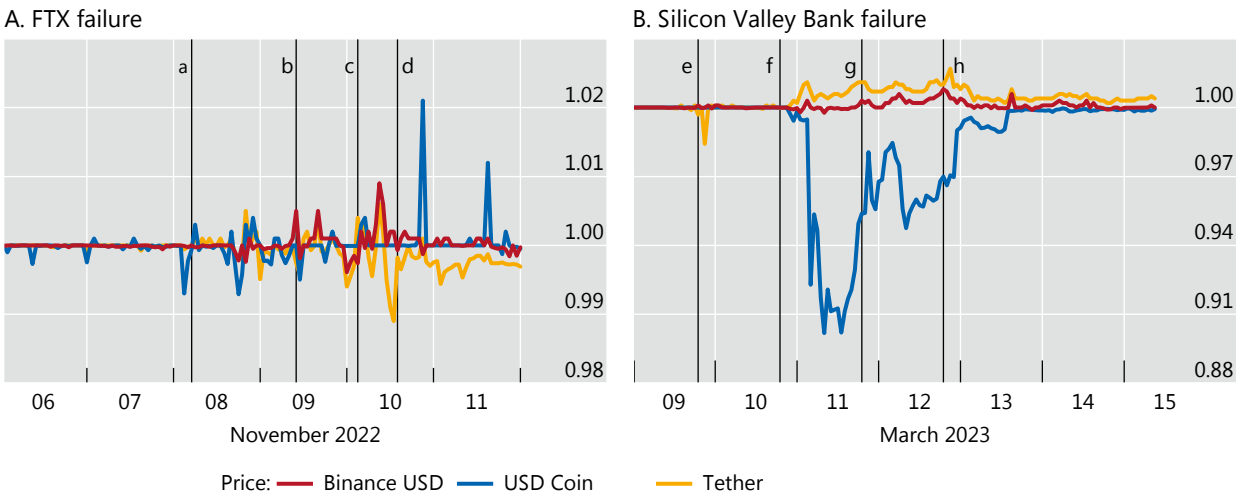
Stablecoins are an alternative form of private tokenised money, but they have important shortcomings.[10] In contrast to tokenised deposits, stablecoins represent a transferrable claim on the issuer, akin to a digital bearer instrument. A payment using stablecoins transfers the issuer's liability from one holder to another. Imagine that John holds 1 stablecoin unit (SCU) issued by a stablecoin issuer. When John pays Paul SCU 1, John's claim on the stablecoin issuer is transferred to Paul, who did not have a claim on that issuer before the transfer. There is no need to update the stablecoin issuer's balance sheet, and there is no settlement on the central bank's balance sheet. Whoever holds the instrument has a claim on the issuer and can transfer it without the need for consent or involvement of the issuer. In this case, Paul is left with a claim on an issuer he may not trust.

As stablecoins are tradable, their prices can deviate from par, thus undermining the singleness of money. Deviations from singleness can occur if there are differences in liquidity across stablecoins or if variations in the quality of the backing or characteristics of the issuer lead to differences in the perceived creditworthiness of different issuers. Even higher-order uncertainty can arise, such as that associated with

Failures of FTX and Silicon Valley Bank coincide with stablecoin price volatility

In US dollars

Graph 4



[a] FTX strikes an acquisition deal with Binance for its non-US business. [b] Binance backs out of the deal. [c] FTX CEO Sam Bankman-Fried apologises on Twitter. [d] Bahamas securities regulator freezes FTX assets. [e] Silicon Valley Bank announces that it will raise additional capital by selling stock. [f] SVB Financial seeks a buyer. A few hours later, a California regulator shuts Silicon Valley Bank and appoints the Federal Deposit Insurance Corporation (FDIC) as receiver to take control of its parent company. [g] Employees of Silicon Valley Bank offered 45 days of employment at 1.5 times their salary by the FDIC. [h] "Depositors will have access to all of their money starting Monday, March 13," say the US Treasury, Federal Reserve and FDIC in a statement, adding that no losses associated with the resolution of Silicon Valley Bank will be borne by the taxpayer.

Sources: CCData; Garratt and Shin (2023).

doubts about whether *others* harbour doubts about the value of a stablecoin, which can lead to discounting and hence undermine singleness.[11] For these reasons, as well as the absence of a clear regulatory and supervisory framework and the lack of a central bank as a lender of last resort, there have been multiple recent episodes where stablecoin prices have lost their pegs (Graph 4).

Asset-backed stablecoins also do not allow for the elastic provision of a general means of payment. Any dollar against which a stablecoin is issued should be, at least in principle, invested directly in safe and liquid assets. Stablecoins thus reduce the overall supply of liquid assets that are available for other purposes.[12] Even if well regulated and supervised, stablecoin issuers would operate like narrow banks.

Finally, tokenised deposits have advantages over stablecoins in terms of compliance with know-your-customer (KYC), anti-money laundering (AML) and combating the financing of terrorism (CFT) rules. Going back to the example above, Paul holds the liability of the stablecoin issuer after the transfer from John. But the issuer did not perform any identity verification or compliance check on Paul, which creates a risk of fraud. To ensure compliance with KYC, AML and CFT regulation for stablecoins, a significant regulatory overhaul would be necessary.[13] In contrast, tokenised deposits, by closely resembling the traditional deposit transfer process, could leverage the existing regulatory and supervisory frameworks for financial institutions.

Achieving seamless interoperability through unified ledgers

The potential of tokenisation lies in its ability to knit together transactions and operations that encompass money and a range of other assets that reside on the

programmable platform. Money in tokenised form provides the essential means of payment that mirror the underlying economic transactions. At the heart of the system lies central bank money in tokenised form that facilitates settlement finality.

This section outlines the concept of a unified ledger where central bank digital currencies, private tokenised monies and other tokenised assets coexist on the same programmable platform. In simple terms, a unified ledger could be considered a "common venue" where money and other tokenised objects come together to enable seamless integration of transactions and to open the door to entirely new types of economic arrangement.

The concept of a unified ledger does not mean "one ledger to rule them all" – a sole ledger that overshadows all other systems in the economy. Depending on the needs of each jurisdiction, multiple ledgers, each with a specific use case, could coexist. APIs could connect these ledgers to each other and existing systems (Box B). Over time, they could incorporate new functions or merge as overlaps in scope expand. The scope of a unified ledger would also determine the parties involved in each ledger's governance arrangements.

While the creation of a unified ledger would require the introduction of a new type of financial market infrastructure (FMI), some of the envisaged benefits could

Box B

Connecting ledgers through application programming interfaces

A unified ledger combines tokenised money and assets on a common platform. By doing so, it enables programmability, composability and multi-asset atomic settlement. On the road to a unified ledger, an intermediate solution would be to integrate legacy systems and existing infrastructures with new programmable platforms through application programming interfaces (APIs). APIs can interconnect systems and implement ramps that lock assets in traditional ledgers and unlock them in programmable platforms. If well designed, APIs may guarantee settlement finality as conventionally defined (CPSS-IOSCO (2012)). However, because APIs involve multiple systems with different operators and protocols, API implementations cannot achieve atomic settlement. Graph B1 shows three different models that range from the smallest incremental enhancement to a fully fledged unified ledger.

In the first model, an API connects the existing payment system to a programmable platform that contains only a limited number of asset classes (Graph B1.A). The programmable platform does not contain tokenised private monies or central bank digital currency (CBDC). Clearing and settlement of payments are achieved using traditional accounts at banks and via the conventional settlement system (eg a real-time gross settlement system). A set of APIs coordinate workflows by sending and receiving messages across systems. The operators from both systems establish the standards for APIs. Settlement finality is achieved in the usual way. However, in this model, atomic settlement involving transactions with private monies, central bank money and other assets would not be feasible.

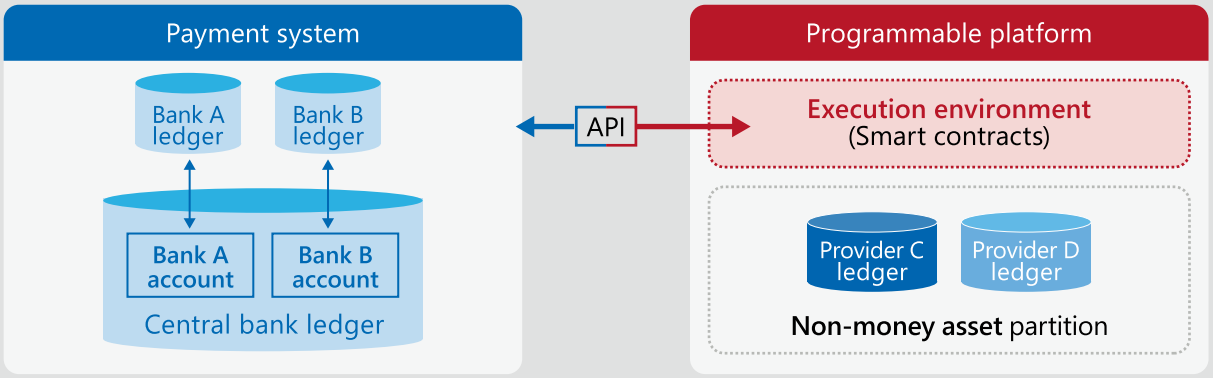
In the second model (Graph B1.B), the programmable platform contains tokenised private monies and tokenised assets, and APIs connect these to the central bank's settlement infrastructure.[1] The platform contains no partition for the central bank. Tokenised private money partitions are connected to traditional systems through APIs and smart contracts. These contracts contain rules that ensure that the updating of accounts across participants is accompanied by settlement in central bank money in the traditional settlement system, which is triggered through APIs. This model guarantees atomic settlement for private monies and other assets, but not for transactions that involve CBDC.

In the third model (Graph B1.C), wholesale CBDC, tokenised private monies and tokenised assets coexist on a fully fledged unified ledger. Wholesale CBDCs could be provided in two ways. In the first, CBDCs may take the form of a central bank liability that is issued directly on to the unified ledger. Alternatively, the central bank could tokenise existing reserves using an API that connects the unified ledger to the current reserve system. This system supports settlement finality and atomic settlement for transactions involving wholesale CBDC, private tokenised monies and tokenised assets.

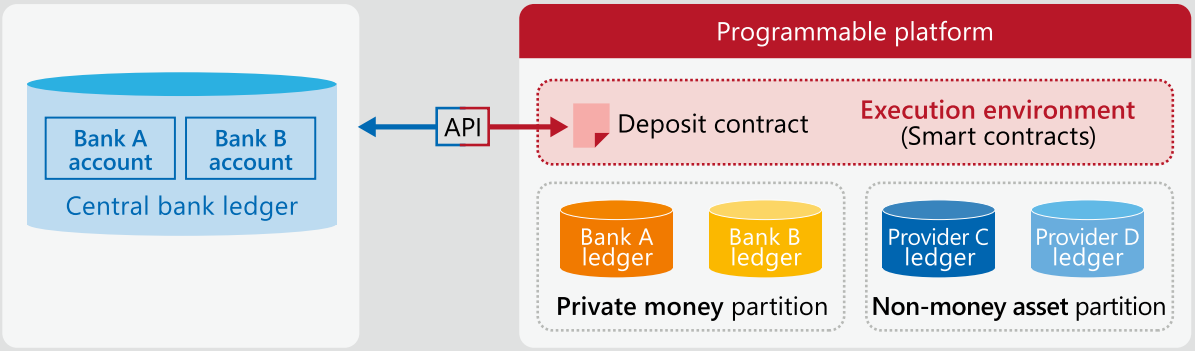
[1] The latter approach is being adopted in the Brazilian Digital Real pilot project (Central Bank of Brazil (2023)).

Standardised APIs enable interoperability between old and new systems Graph B1

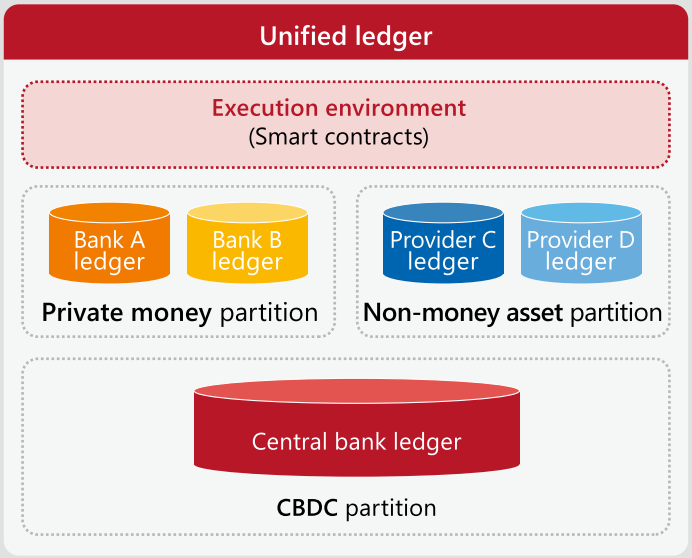
A. Payment messaging model



B. Private tokenised ledger model



C. Fully fledged unified ledger



Source: BIS.

also be reaped through more incremental changes to existing systems and interlinking them through APIs into a network of networks. Weighing the pros and cons of a big leap against those of a series of incremental changes is important when considering innovation of any kind but it is especially important for the large discrete changes entailed by new infrastructures such as a unified ledger. Some automated processes for exchanging data that resemble operations in tokenised environments could be achieved by connecting existing systems through APIs. In the short term, modifying existing systems would require lower upfront costs and less coordination among stakeholders than creating a unified ledger.

Yet history shows that incremental fixes have their limits, especially when they accumulate on top of legacy systems. Each new layer would need to look forwards while being constrained by having to look backwards to ensure compatibility with legacy systems. These constraints will become more binding as more layers are added on top, eventually holding back innovative developments. The history of computing and software is replete with such examples.[14]

For these reasons, it is often the case that harnessing the benefits of technological advances necessitates a fundamental rethink of the financial infrastructure that supports new types of operation. Tokenisation presents another such opportunity, where the introduction of programmable platforms could bring long-term benefits that far outweigh the short-term costs arising from investment as well as the costs and coordination efforts in shifting to new standards and procedures. Of course, the relative balance between the benefits of a unified ledger and those from interlinking existing systems through APIs will depend on the state of technology and the specific needs of each jurisdiction. There is no one size fits all.

The building blocks of a unified ledger

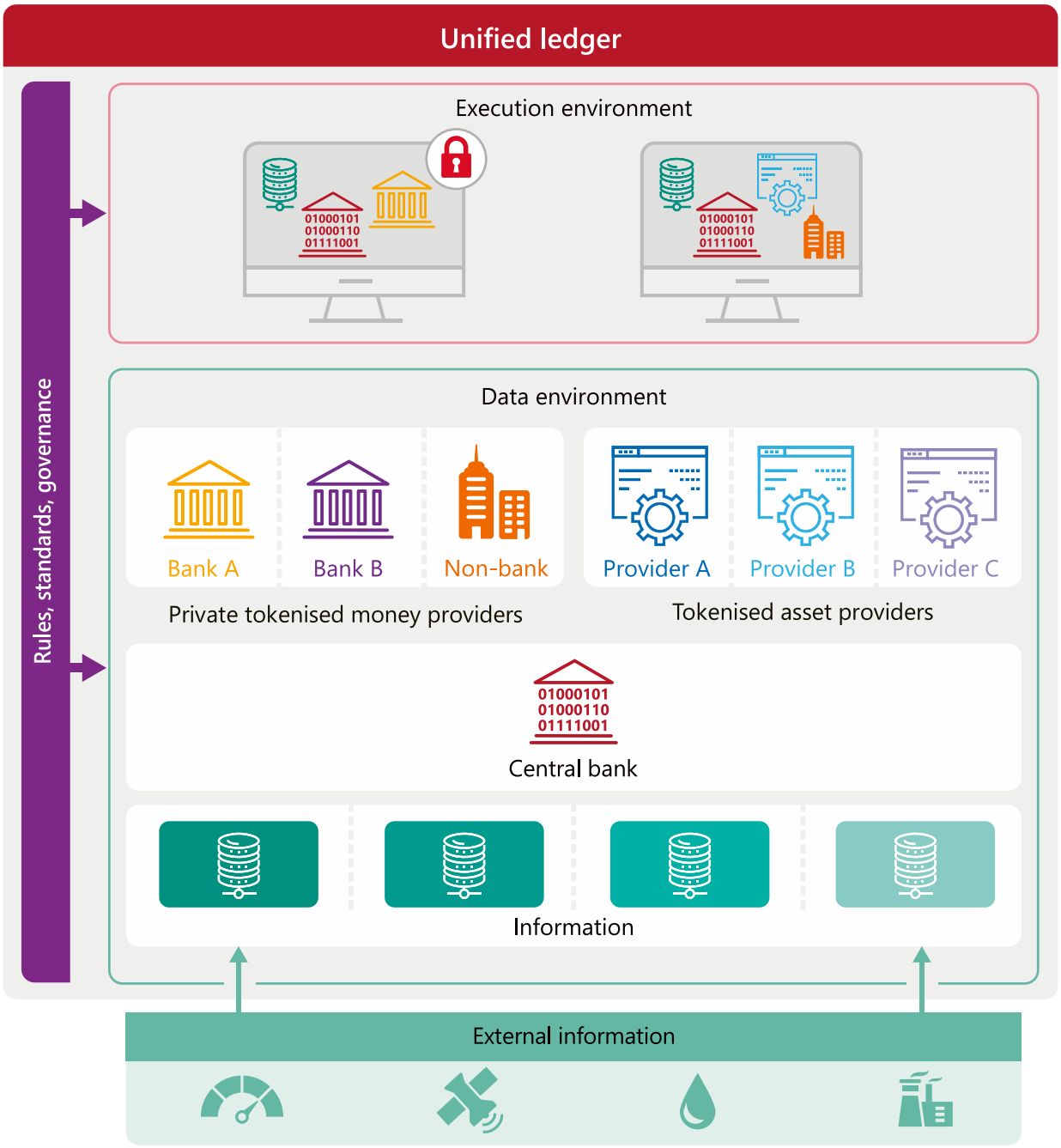
A unified ledger leverages the benefits of tokenisation on a common platform. Based on a secure environment for storing and sharing data through encryption, it could enable new forms of transaction, thus expanding the universe of contracting outcomes.

There are two key aspects to the design of a unified ledger. The first is that it combines all the components needed to complete a transaction on one platform, ie it has everything in one place. The second is that it features money and assets as executable objects, which means they could be transferred safely and securely without going through external authentication and verification processes and without relying on external messaging systems.

The structure of a unified ledger can be described in terms of the following building blocks (Graph 5). The ledger comprises a data environment and an execution environment, which are subject to a common governance framework. The data environment contains the digital representations of money and assets in separate partitions that are owned and operated by the respective competent operating entities (dashed lines). The data environment also includes information necessary for the operation of the ledger, such as the data required for the secure and legal transfer of money and assets. The data environment also encompasses all information necessary to incorporate real-world events into any contingent performance of actions. Information can be a direct result of transactions on the ledger or may be obtained from the outside environment.[15]

Any operation involving one or more of these elements is carried out in the execution environment, either directly by users or through smart contracts. For each specific application, operations in the execution environment combine only the intermediaries and assets required for each application. For example, a payment between two individuals, executed via a smart contract, would bring together the users' banks (as providers of tokenised deposits) and the central bank (as provider

Stylised representation of a unified ledger Graph 5



The unified ledger comprises its data and execution environments as well as the rules, standards and governance applying to those environments. The data environment contains money, assets and information (internal or external to the ledger). Each of these includes partitions (denoted by dashed lines) delineating ownership and/or access by the relevant entities. Operations involving one or more of these elements are carried out in the execution environment, either directly by users or through smart contracts. The lock indicates that some operations may be performed on confidential encrypted data.

Source: BIS.

of CBDC). Should the payment be conditional on some real-world contingency, that information would also be included.

The common governance framework specifies the rules and standards of how the different components interact in the execution environment, as well as which privacy rules apply. Preserving strict confidentiality is a prerequisite if a unified ledger

is to be a practical proposition. Confidentiality and data control are achieved in two mutually reinforcing ways: data partitions and data encryption (denoted with a lock in the execution environment). Partitions guarantee that data and information are visible and accessible to only the respective authorised parties for each partitioned domain, ensuring strict confidentiality. At the same time, cryptographic techniques could ensure that data can be shared confidentially as inputs in the execution environment. The details are discussed in the following sections.

Use cases: improving the old

While the monetary system has served society well, its current design could lead to the emergence of pinch points. Digital money currently sits at the edges of communication networks, where it resides in siloed proprietary databases operated by banks and non-banks. External messaging systems are required to link these databases. The separation of messaging, reconciliation and settlement can lead to delays and means that participants often have an incomplete view of completed actions. Consequently, errors may go undetected for longer, leading to higher error resolution costs and increased operational risk. For these reasons, payment processes can be costly, cumbersome, slow and opaque. And they can fall short of meeting users' changing demands.

The complexity and lack of transparency in existing payment systems is evident even in a simple payment involving customers of two different banks (Box C). A transfer of funds from payer to payee involves a large number of messages, internal checks and adjustments. Participants generally cannot track the progress of their payments in real time. In particular, the payee does not see when the process is initiated, and the payer does not know when it is completed.[16]

The payment process is even more complex in cross-border transactions, further amplifying frictions. For one, these require international messaging systems on top of domestic ones. Differences in operating hours and/or holidays as well as inconsistencies across operating systems, for example in the form of different messaging standards, can lead to further delays, increasing settlement risk. In addition, the involvement of more intermediaries (eg correspondent banks) increases operational risk. For cross-border payments involving different currencies, there is also foreign exchange (FX) settlement risk, namely the risk that one party to a currency trade fails to deliver the currency owed.[17]

A unified ledger could improve the way payments are executed. Having private tokenised monies and CBDC on the same platform eliminates the need for the sequential messages across siloed databases. This enables so-called atomic settlement, in which two assets are exchanged simultaneously, such that the transfer of one occurs only upon transfer of the other.[18] In the process, settlement, ie the wholesale leg of the payment from one intermediary to another, also occurs instantaneously in wholesale CBDC.[19] At the same time, the use of a partitioned data environment with appropriate access controls allows full transparency for the transacting parties, while keeping the transaction private from those who are not involved. Finally, by combining messaging and payment rails on the same platform, the ledger eliminates delays in the payment process, thereby mitigating settlement risk.

Securities settlement could benefit greatly from execution on a unified ledger. The current process for securities settlement involves multiple parties, such as brokers, custodians, central securities depositories, clearing houses and registrars. Accordingly, there is a need for various messaging instructions, money flows and reconciliation procedures, all of which lengthen the process, increase the costs and expose parties to additional risks. By bringing tokenised money and securities together on a programmable platform, some of these risks could be mitigated by

Box C

Messaging in a standard person-to-person wire transfer

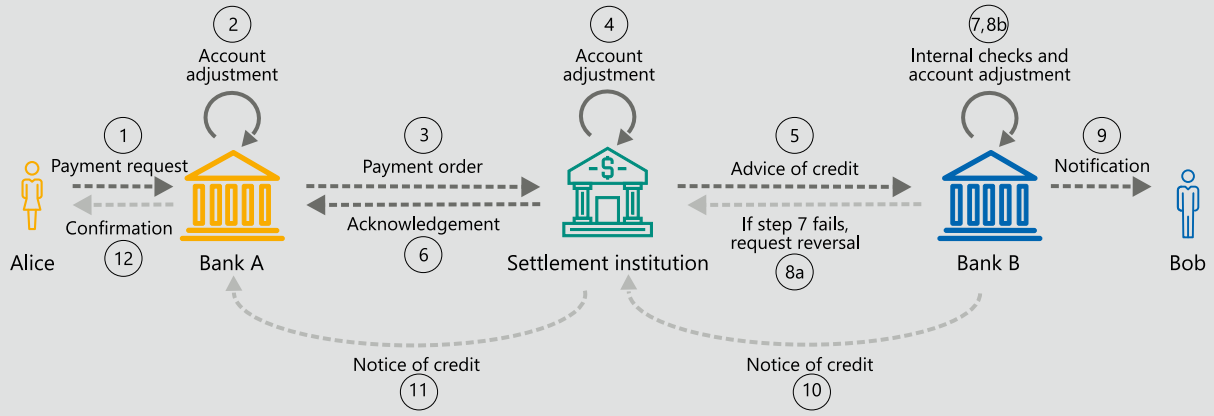
Messaging that governs digital money is currently located at the edges of communication networks and money transfers involve multiple messages through third-party messaging systems. At each step of the process, participants often have only a limited view of the completed actions.

The complexity and lack of transparency in existing payment systems can be illustrated with a simple example of a wire transfer from Alice to Bob (Graph C1). The process begins with Alice sending a payment request to her bank using the bank's mobile app (step 1). Bank A responds by debiting Alice's account by the transfer amount together with any fees (step 2) and sending a payment order to the settlement system (step 3). The settlement system debits Bank A's settlement account and credits Bank B's account (step 4) and sends an advice of credit with a reference number to Bank B (step 5). There follows an acknowledgement with a reference number to Bank A (step 6). Bank B must ensure Bob has an account and perform any know-your-customer or anti-money laundering checks (step 7). If any of these checks fail, then Bank B will need to send a reversal request to the settlement institution (potential step 8a shown in light grey). Otherwise, Bank B credits Bob's account (step 8b) and sends a message to Bob notifying him of the adjustment to his account (step 9).

In some payment systems Bank B must accept the transfer by Bank A before it takes place. In this case, steps 5 and 7 come before step 4. It is also worth emphasising that in the description provided in Graph C1, Alice is not notified that Bob has received the transfer. This can be achieved through additional messages from Bank B to the settlement system (step 10), from the settlement system to Bank A (step 11), and then with a final confirmation message from Bank A to Alice (step 12). These steps appear in light grey in Graph C1 to show that they are not common to all systems.

Messaging in a standard domestic wire transfer

Graph C1



Source: BIS.

shortening settlement lags and obviating the need for messaging and reconciliation. Moreover, the simultaneous execution of the delivery and payment legs could expand the scope of securities covered in delivery-versus-payment (DvP) arrangements, further contributing to risk mitigation. Box D discusses this possibility in more detail.

Another important use case is the mitigation of settlement risk in the multi-trillion dollar FX market. Existing netting and payment-versus-payment (PvP) mechanisms help to mitigate settlement risk, but do not fully eliminate it, not least as existing PvP arrangements are at times unavailable, unsuitable for some trades or deemed too costly by market participants.[20] Atomic settlement around the clock, instead, could eliminate settlement lags. Moreover, smart contracts that combine currencies with authorised FX providers could allow more currencies to be integrated on a common platform at a lower cost, expanding the scope of PvP arrangements.

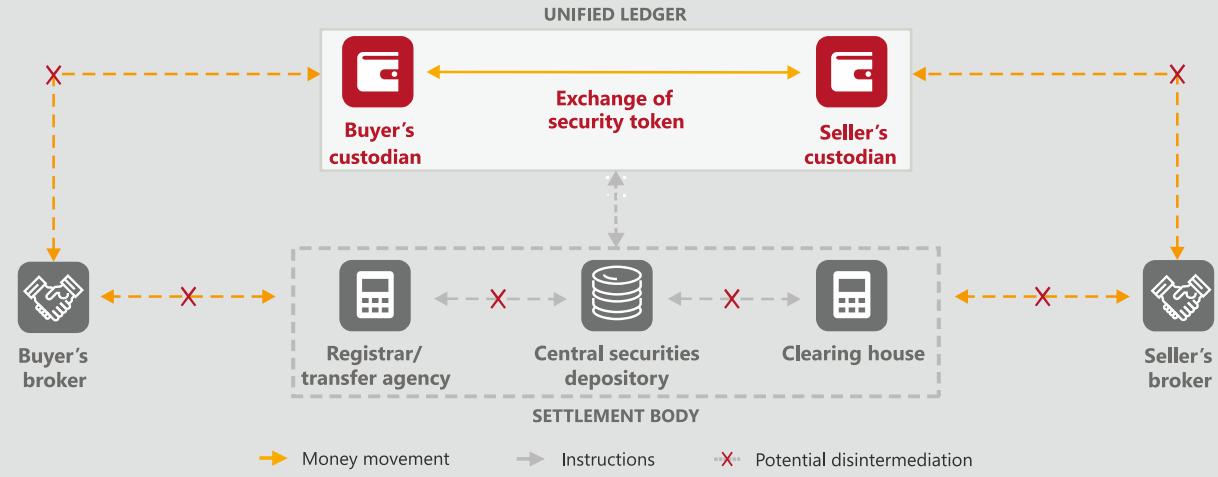
Box D

Streamlining securities settlement through a unified ledger

Today, the process of trading securities and settling securities transactions involves multiple parties, with a myriad of messaging instructions, reconciliation efforts and money flows involved (Graph D1). Central securities depositories (CSDs) electronically manage securities either directly or indirectly (eg through a custodian) for the security's beneficial owner. A securities buyer or seller initiates the process by instructing her broker or custodian to initiate the trade. During the time between trading and final settlement (the "settlement cycle", which can take up to two days), parties are exposed to replacement cost risk (ie the risk of a trade failing to settle and having to be replaced at an unfavourable price). In addition, during the settlement process itself, counterparties are exposed to principal risk (ie the risk that one counterparty does not fulfil the agreement – failing either to pay or to deliver the security). The CSD must verify the identity of account holders and ensures reconciliation and confirmation of what is being settled with the relevant third parties (eg clearing agents).

A unified ledger could reduce these risks by reducing the number of counterparties and shortening confirmation and reconciliation times. If both tokenised money and securities are hosted on a common platform, the risks and costs that arise from having them reside in separate ledgers can be reduced substantially. The simultaneous execution of the delivery and payment legs could also expand the scope of securities covered in delivery-versus-payment (DvP) arrangements, helping to mitigate principal risk between counterparties. Appropriate liquidity saving mechanisms would need to be instituted, as atomic settlement also puts higher liquidity demands on the system – much like the move from deferred net settlement to real-time gross settlement.

A stylised example of the securities settlement process and the unified ledger — Graph D1



Source: BIS.

Use cases: enabling the new

Beyond improving existing processes, a unified ledger could open the door to entirely new types of "arrangements and transactions" that expand the universe of possible contracting outcomes. This is made possible through the combination of smart contracts, a secure and confidential environment for storing and sharing information and the execution of transactions enabled by tokenisation.

Smart contracts increase the scope for successful coordination. In many instances, mutually beneficial outcomes cannot be achieved when participants need to undertake costly joint efforts. The reason is that individual participants may have

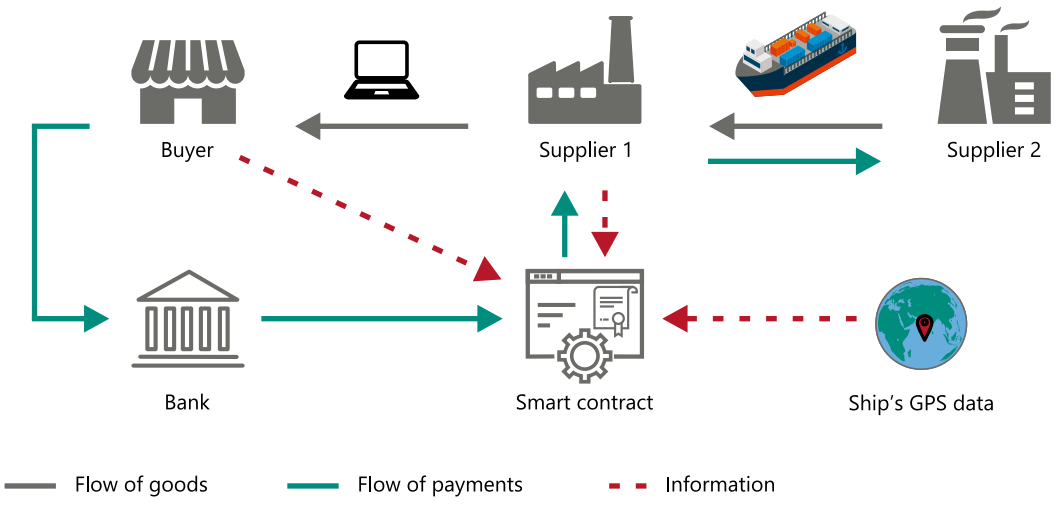
an incentive to free ride on the contribution of others. Contingent performance promises to overcome such coordination problems. For example, a smart contract could specify that each participant contributes only a certain amount to a joint venture if all other participants also contribute. This way, free-riding is eliminated.

Overcoming coordination problems may be particularly useful in the context of banking, where the use of contingency in term deposit contracts could contribute to the stability of bank funding and the banking sector more generally. Typically, term deposit contracts are bilateral arrangements between the bank and the depositor. Yet from time to time, the value of deposits can depend on the collective decisions of all depositors, especially during stress periods in the banking sector. In this context, strategic uncertainty arises as early withdrawals are met on a first-come, first-served basis, while the bank invests funds in illiquid assets. Depositors who withdraw first thus have an advantage and this can lead to bank runs. This problem could be mitigated by allowing explicit coordination through the design of new types of deposit contracts that impose contingent performance of actions on depositors. Such contracts could ensure that early withdrawers do no better than late withdrawers, thus eliminating the motivation to withdraw funds purely out of fear that others might do the same. This type of arrangement would not prevent all potential types of run from occurring, but it could mitigate the textbook case of first-mover advantage and coordination failures.

Supply chains are another possible use case that would make full use of a unified ledger's capabilities to incorporate real-time information into smart contracts. The problem of supply chain financing has been a notoriously difficult one to solve in real-world settings. Supply chain financing has attributes of a DvP problem as explained below, but one which also features uncertainty and information asymmetries about the underlying state of the world.

Graph 6 depicts a stylised supply chain. A buyer (usually a large firm) purchases goods from suppliers (often small and medium-sized enterprises, SMEs), which in turn require goods from other suppliers for production. A common problem is that the buyer would prefer to pay for the goods only once delivered. However, suppliers need to pay their workers and purchase materials to produce the goods beforehand. They thus require some form of financing until they receive payment from the buyer.

Trade finance on a programmable platform — Graph 6



Source: BIS.

For well known reasons, including the risk that the buyer will not pay upon delivery, obtaining trade credit usually requires firms to pledge collateral.[21] For example, an SME in Italy might expect delivery of intermediate goods via ship from its Indian supplier in one month's time. To set up production now, it can pledge these goods as collateral to obtain a loan from a bank or its suppliers. Should the company default, the creditor can reclaim the collateral. However, creditors might be reluctant to provide sufficient credit or charge a prohibitively high interest rate, as the collateral might lose value due to pirate attacks or storm damage to the ship. The firm might also engage in fraudulent behaviour and try to pledge the collateral to different parties simultaneously, which is common in trade finance.[22] These frictions to obtaining financing imply that suppliers often have to rely on their own funds to meet their working capital needs.

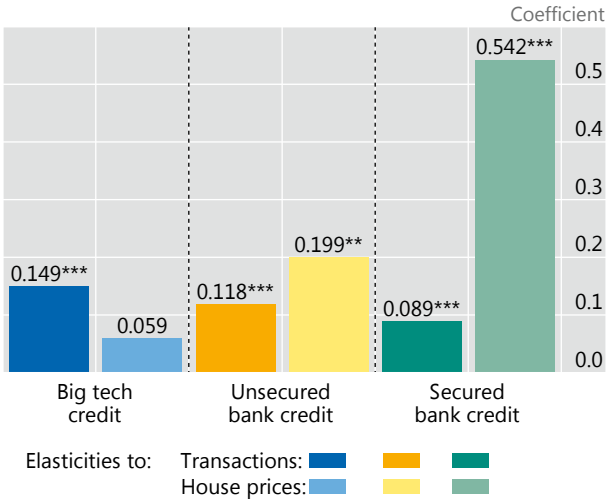
By combining the different components of the supply chain relationships and the steps of the financing process in one place, a unified ledger could mitigate the problems plaguing trade finance. Contracts that formalise the conditional performance of actions could eliminate incentive problems. Smart contracts could specify an automatic payment from the buyer to its suppliers upon delivery of goods, or partial early payment when intermediate steps are reached. This way, creditors would not need to worry about the risk that the buyer will not honour its obligations. Banks could extend loans featuring smart contracts that act upon real-time information on shipments provided by internet-of-things (IoT) devices, such as GPS data. In the above example, the interest rate could automatically fall, or additional credit be granted, once the ship passed the Horn of Africa, a notoriously high-risk area for piracy. This way, suppliers could finance part of their working capital needs as early as the production phase. Finally, because all trade finance contracts would be written on a shared ledger, it would be impossible to write duplicate loan contracts tied to the same collateral, which would further enhance lenders' willingness to extend credit to firms.

In addition, by providing a **secure and confidential environment for storing and sharing information**, the ledger could harness the benefits of data to lower the cost of and improve access to credit. The use of data can bring both benefits and costs. Data allow lenders to better assess the riskiness of borrowers, reducing both costs and the need for collateral. For example, lending by big techs, which use big data and machine learning to assess credit risk, is less sensitive to changes in real estate collateral values than bank credit (Graph 7.A).[23] But network effects can lead to market concentration and ultimately higher costs for households and firms: the analysis of large troves of data enhances existing services and attracts further users, which in turn create new data, leading to a data-network-activities or "DNA" loop.[24] Moreover, privacy concerns can make individuals reluctant to share their data. With data-sharing technologies (discussed below), mathematical computations can be performed directly on encrypted or anonymised data. Users hence retain control over their data when sharing them on the ledger. Through improved data-sharing arrangements, the unified ledger could enhance financial inclusion, in particular among disadvantaged segments of the population such as racial minorities and low-income households. These "thin credit file" applicants stand to benefit disproportionately from screening via non-traditional data: as banks' traditional credit scores are noisier indicators of their default risk than for other groups of the population, additional data yield a more precise signal of their credit quality (Graph 7.B).[25] In turn, lenders can offer loans at lower rates.

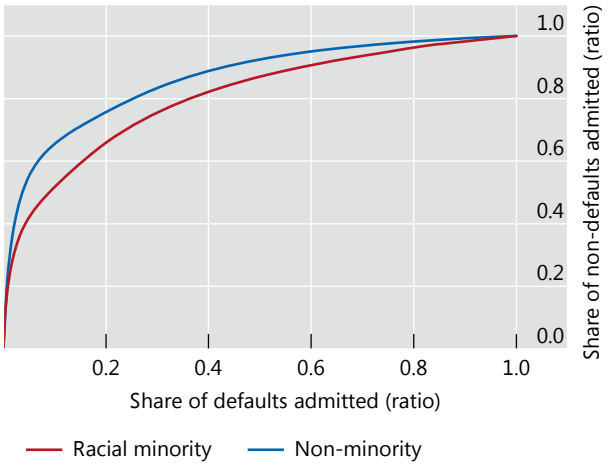
Through encryption technology, a unified ledger could also enable new ways to enforce AML and CFT requirements. Financial institutions safeguard highly sensitive and proprietary data that often need to be kept confidential by law. However, the inability to share such sensitive data without exposing confidential information can

Data can obviate the need for collateral and improve credit scoring models[1] Graph 7

A. Use of big data and machine learning reduces the importance of collateral in lending[2]



B. Traditional credit scores are worse at predicting default for disadvantaged segments of the population[3]



[1] See technical annex for details. [2] ***/** denotes statistical significance at the 1/5% level. [3] The red and blue lines show the receiver operating characteristic (ROC) curves for the VantageScore 3.0 credit score in a sample of mortgage applicants in the 2009–16 period for racial minorities and non-minorities, respectively.

Sources: Blattner and Nelson (2021); Gambacorta et al (2023).

hinder efforts to combat money laundering and other illicit activities. The use of a unified ledger could provide transparent and auditable records of transactions, transfers and ownership changes. Encryption methods allow financial institutions to share these data confidentially with each other and across borders to detect fraud and money laundering while remaining compliant with domestic data regulations.

These benefits could be further enhanced by leveraging **tokenisation** and the dual nature of tokens encompassing both identifying information and the rules governing transfer. In the case of payments, for example, supervisory compliance requirements that depend, among other things, on the transacting parties, their location and the type of transfer could be directly embedded into the token.[26] While not undertaken in the context of a unified ledger, the BIS Innovation Hub's Project Aurora is exploring how privacy-enhancing technologies and advanced analytics might be leveraged to combat money laundering across financial institutions and borders.

The combination of smart contracts, information and tokenisation could also improve the issuance of and investment in securitised assets and bonds. One example is mortgage-backed securities (MBS), which pool mortgage loans into tranches of debt that are subsequently purchased by investors. Yet even in the deeply liquid $12 trillion US MBS market, the process of securitisation involves over a dozen intermediaries.[27] Automation through smart contracts could eliminate time lags in information and payment flows, streamlining the securitisation process. A token could integrate real-time data on borrower repayments and how they are pooled and distributed to investors, further reducing the need for intermediaries.

Another use case is in green finance. The BIS Innovation Hub's Project Genesis illustrates some of the benefits of tokenisation and smart contracts. The project involves a platform from which an investor can download an app and invest any amount into tokenised government bonds that fund a green investment. Over the bond's life cycle, smart contracts allow the investor not only to see accrued interest, but also to track in real time how much clean energy is being generated and how far

carbon emissions are being reduced as a result of the investment. Moreover, the investor can sell the bond in a transparent secondary market.

Taken together, these examples show how applications of the unified ledger have the potential to enhance the current monetary and financial system. For existing processes, a unified ledger could seamlessly automate and integrate transactions. And by leveraging the benefits of tokenisation and providing a secure environment for sharing data, a unified ledger could enable altogether new types of transaction.

Guiding principles for a unified ledger

Any application of the unified ledger concept should adhere to a number of high-level guiding principles. First and foremost, any application should be fully integrated with the two-tiered structure of the monetary system. In this way, the central bank could continue to support the singleness of money by providing settlement in wholesale CBDC, and the private sector could continue to innovate to the benefit of households and firms. In addition, there are important principles related to its scope and governance. These will specify how best to ensure a level playing field and foster competition, as well as how to ensure data privacy and operational resilience. The concrete implementation of these principles ultimately depends on the needs and preferences of each jurisdiction as well as the details of the specific application.

Scope, governance and competition

The first important question regards the **scope** of the ledger. As discussed above, the concept of a unified ledger does not exclude a multiplicity of coexisting ledgers, each with a specific use case. In practice, the concept is likely to be applied first to specific applications where benefits are more immediate (Box E). For example, one ledger could aim at improving securities settlement, involving only the relevant parties, while another could pertain to trade finance in, say, the shipping industry. Starting from specific use cases, the ledger's scope could expand over time as it includes additional assets and entities. Ultimately, the scope of the ledger will depend on the specific needs and constraints of each jurisdiction.

Irrespective of its scope, a unified ledger would effectively be a new type of FMI or a combination of multiple FMIs. As such, a natural starting point for drawing up standards would be the *Principles for financial market infrastructures*,[28] which, in addition to setting out requirements for access, safety and operational resilience, state that FMIs should provide clear and certain final settlement (Principle 8) in central bank money where practical and available (Principle 9). These principles apply to a wide range of infrastructures such as payments systems, central securities depositories, securities settlement systems, central counterparties and trade repositories.

The scope of the ledger has direct implications for its governance arrangements, competitive design and the incentives to participate.

Governance of a unified ledger could follow existing arrangements, whereby central banks and regulated private participants take part in governance under established rules. For example, when money and payments are involved on a ledger, the central bank will necessarily play a role as the provider of the ultimate settlement asset. Its specific involvement in governance arrangements could take various forms, much as it does in the case of traditional payment systems, where public ownership, regulation and oversight, as well as private mutual ownership are all viable options.[29] To ensure integrity, regulated and supervised private participants should remain in charge of customer-facing activities. They should also adhere to established

Box E

The tokenisation continuum

Tokenisation – the process of recording claims on real or financial assets that exist on a traditional ledger on a programmable platform – needs to overcome several economic, legal and technical challenges.

An intrinsic feature of many markets is economic friction generated by uncertainty and misaligned incentives, which can be mitigated by trusted intermediaries. For example, when a bank makes a loan to a non-financial firm, the borrower knows more about the quality of its project and the effort devoted to it. To ensure that funds are put to their intended use, lenders need to screen the quality of the borrower ex ante and monitor performance ex post. Technology alone is unlikely to overcome these market imperfections, leaving a role for intermediaries to screen borrowers.

Tokenisation efforts must also address legal issues. Rules and regulations governing tokenised assets must be aligned with those of their non-tokenised counterparts, which requires regulatory coordination to prevent unintended consequences such as shadow activities, theft and regulatory arbitrage. This task is easier for assets subject to legal frameworks and regulations that are standardised and can be easily translated into a computer algorithm. Broader issues include those pertaining to investor and consumer protection, cyber security and regulatory compliance across borders.

There are also technical challenges, especially in the design of ramps that map assets on traditional ledger systems to their tokenised counterparts. Ramps lock assets in their platform of origin as collateral for the tokens that are issued on the programmable platform. Locking and unlocking the original assets requires seamless interaction and coordination across systems. For example, to lock a property on a platform, the on-ramp would need to ensure that the property is no longer tradable outside the platform. As property titles are kept in disparate local registries, full automation could be difficult without the involvement of (offline) intermediaries. Generally, the feasibility of on-ramping and the associated benefits on the programmable platform will depend on the level of automation and harmonisation of the systems of origin.

As discussed in a recent BIS study, these aspects define a tokenisation continuum (Graph E1).[1] It highlights a trade-off: for those applications where tokenisation is easiest, per-unit gains are likely to be modest; but the gains are likely to be largest for applications where tokenisation is most difficult. Therefore, in the short term, tokenisation could focus on identifying assets that are suitable for tokenisation and traded in large volumes.

The tokenisation continuum — Graph E1

Source: Aldasoro et al (2023).

[1] See Aldasoro et al (2023).

KYC, AML and CFT regulations, as well as perform ongoing due diligence to ensure compliance with privacy regulations.

The demands on governance arrangements increase with the scope of the ledger. For example, a unified ledger for cross-border payments would require seamless interoperability across private payment service providers (PSPs) and central banks located in various jurisdictions with different regulatory and supervisory frameworks. It would hence require significant harmonisation efforts across jurisdictions. A ledger

that targets domestic securities settlement, on the other hand, would require less intensive coordination efforts.

An open and level playing field is important for competition and **financial inclusion**. From a public policy perspective, it is critical to consider how the introduction of a common platform may affect the industrial organisation of money and payments, and ultimately of the entire financial system. Promoting healthy competition between private actors through open platforms can foster innovation and lower costs for end users by reducing rents. By designing platforms and attendant regulations with these goals in mind, public authorities can help ensure that network effects work for the benefit of consumers. To this end, the use of encryption techniques such as homomorphic encryption could help prevent the concentration of data within centralised entities, and hence the emergence of dominant players.

An important challenge in promoting competition is providing the right **economic incentives** for potential participants. Without the right incentives, PSPs might decide not to join. Efforts to centralise over-the-counter (OTC) bond markets offer valuable lessons.[30] Trading government bonds on an exchange, as opposed to over the counter, can lead to lower costs through improved matching and greater liquidity, especially during stress periods.[31] However, high entry and operating costs or benefits from established investor-dealer relationships can deter some players from joining. As the main players in OTC markets, dealers also often enjoy market power and high profits, which can make them reluctant to join a common platform.[32] But unless a sufficient number of players join, there may be insufficient liquidity and virtuous network effects cannot take hold. The experience from the introduction of fast payment systems suggests that mandating participation while simultaneously providing an infrastructure that allows for private sector innovation can be key to ensuring adoption.[33] Once the benefits of network effects unfold, new players will join voluntarily.[34]

Data privacy and operational resilience

By bringing together money, assets and information on a common platform, a unified ledger raises important issues about data privacy and operational resilience.

Adequate safeguards are necessary to **protect users' privacy**. The concentration of different types of data, possibly including transaction data in combination with information on geolocation and purchased products or services, raises concerns about data theft and abuse.[35] As a fundamental right, privacy requires a conservative approach to data management on the unified ledger. Commercial secrecy is no less important. Businesses may be hesitant to participate in a unified ledger application unless they can protect confidential information such as smart contract code and transaction logs.

A key element to guaranteeing privacy is to create partitions in the ledger's data environment (Graph 5). Each entity, such as banks or the owners of tokenised assets, will see only transactions and associated data on their own partition. Updates to the data environment are initiated by the account owners through use of their private keys. These private keys are used to authenticate and authorise transactions, ensuring that only legitimate account owners can make changes to their own partition of the ledger's data environment.

In addition, encryption and other **privacy-preserving technologies** can ensure the safe sharing and use of data. When different entities interact in a transaction, information from different partitions needs to be shared and analysed in the execution environment. Secure data-sharing technologies enable mathematical computations to be performed directly on encrypted or anonymised data, without

revealing sensitive information. Some intermediaries and users may be more willing to share data in encrypted form with other parties, which could foster competition and innovation rather than market concentration and captive behaviour. Commercial secrecy can be maintained by encrypting individual smart contracts. Only the code owner, or parties designated by the code owner, would have access to the contract details.

Various privacy-preserving technologies can protect confidential and personal data in a unified ledger, each with its own benefits and costs, depending on the specific application. Table 1 summarises the key characteristics of selected technologies and the trade-offs involved in their use. Homomorphic encryption and differential privacy allow users to share their data with other parties in encrypted form. Secure multi-party computation and federated learning, on the other hand, enable entities to use common machine learning algorithms while keeping their data in their local partitions. These methods differ in terms of their degree of privacy protection, computational burden and ease of implementation.[36]

A concrete example of how encryption technology might be used is a small bank that would like to apply a big tech's advanced machine learning model to assessing the credit risk of its loan applicants. Traditionally, the bank would have to grant the larger player access to its data for this task, which requires a great level of trust that the data will not be used to competitively undermine the small bank. With homomorphic encryption or similar methods, however, the bank can send encrypted data and take advantage of the big tech's analytic services without handing over the actual data. The big tech, in turn, could further improve its algorithms as they are trained on larger data sets.

As institutions that serve the public interest with no commercial interest in personal data, central banks could play a crucial role in designing ledger applications where privacy safeguards are implemented from the ground up. The ledger could be

Different characteristics of privacy-preserving technologies — Table 1

Privacy-preserving technologies	Application use cases[1]	Computation overhead[2]	Data breach risk[3]	Challenges to implement[4]
Homomorphic encryption (HE) is a cryptographic technique that allows data to be encrypted and shared while still being usable for computations.	Secure cloud computing; patient medical data; financial services; data analytics across organisations; IoT (ie sensors and smart devices).	High	Low	High
Differential privacy (DP) is a technique that adds a controlled amount of noise or randomness to data to protect privacy.	Statistical analysis of census and survey data; public health data-sharing; machine learning across multiple organisations; personalised recommendations and online advertising.	Low to medium	Low to medium	Low to medium
Secure multi-party computation (SMPC) is a cryptographic technique that allows multiple parties to jointly perform computations on their private data.	Secure financial analysis; fraud detection; medical data analysis, supply chain management; human resources and payroll processing; data privacy compliance as GDPR.	High	Low to medium	High
Federated learning (FL) is an approach where data are kept locally on different devices or servers, and machine learning models are trained collaboratively.	Fraud detection; credit scoring; IoT applications such as smart homes; health care (eg disease detection); online advertising (eg ad recommendation and targeting); natural language processing (sentiment analysis).	Medium to high	Medium	Medium

[1] Examples where the technology can be effectively applied to protect the privacy of sensitive or personal data. [2] Computational resource requirements, such as processing power and memory. [3] Potential for unauthorised access, disclosure, theft or compromise of sensitive or confidential information. [4] Challenges, obstacles or barriers that may arise during the process of deploying, integrating or operationalising a technology.

Source: BIS.

designed to embed privacy laws directly into the programming of tokens. In many cases, data privacy laws give consumers the opportunity to grant or deny third parties consent to use their data. For example, the European Union's General Data Protection Regulation gives its citizens the "right to be forgotten" by asking firms to delete their personal data. Likewise, the California Consumer Privacy Act endows Californians with the right to know what personal information is being collected and to prevent its sale or ask for its deletion. However, it is often difficult for users to exercise their options effectively, and to verify whether firms have actually deleted their data. By embedding the option to prevent the sale of data or to delete them directly into a smart contract specific to a certain token and transaction (eg payment data should only be accessible by certain institutions), data privacy laws could be made more effective.

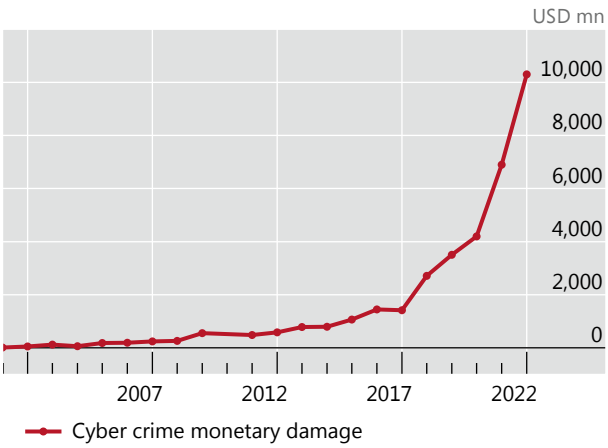
Beyond privacy protection, rising costs from cyber attacks (Graph 8.A) highlight the need for strong institutional and legal safeguards for **cyber resilience**. Safeguarding the integrity and confidentiality of the ledger's data requires multiple layers of security such as encryption, authentication, access controls, monitoring and regular security audits. A cyber attack on a critical FMI or ledger could not only entail significant monetary and reputational damage, but also lead to widespread disruption in the financial system and ultimately inflict significant societal costs.[37] The more comprehensive the ledger, the bigger the risks of a single point of failure and therefore the larger the potential associated costs. An appropriate level of investment in cyber resilience and security is therefore paramount.

A unified ledger could help ensure a sufficient level of investment in cyber security. Cyber security is a public good. If one institution spends more to protect its own infrastructure, it makes the system as a whole safer, thereby benefiting all other institutions. However, given such positive externalities, the classical problem of under-investment by private parties arises.[38] Collectively, financial institutions will spend too little on cyber security (Graph 8.B). The unified ledger, sustained by a public-private partnership that internalises these externalities, could overcome this issue. It would lead to greater investment in cyber security, increasing overall system resiliency.

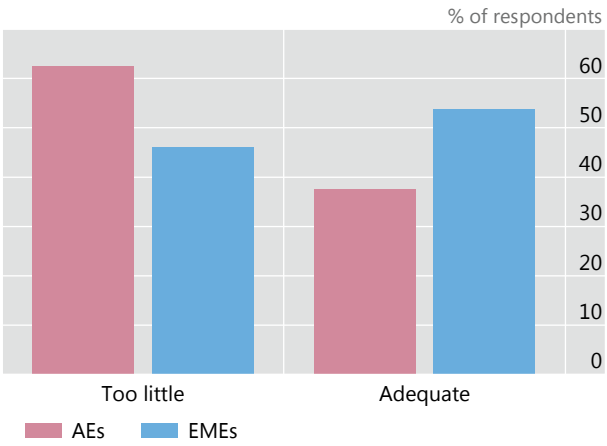
Cyber incidents are rising but spending on security is inadequate[1]

Graph 8

A. The cost of cyber attacks is rising rapidly



B. IT spending in the financial sector is deemed inadequate



[1] See technical annex for details.

Sources: Doerr et al (2022); Statista.

Conclusion

To realise the full benefits of innovation in money, payments and a broader range of financial services, it is crucial to have a vision for the future monetary system and for the role of central banks in driving innovation to meet evolving needs. Given the unpredictable nature of innovation, the focus should be on building a monetary system that is adaptable enough to support safe and sound innovation by the private sector, in any form that this may take.

This chapter has presented a blueprint for a future monetary system that harnesses the transformative potential of tokenisation to improve existing structures and open up new possibilities. This blueprint has sketched out a new financial market infrastructure – a unified ledger – that integrates CBDCs, tokenised deposits and other tokenised claims on financial and real assets in one place.

A unified ledger has two key advantages. First, it provides a venue where a broader array of contingent actions and financial transactions could be seamlessly integrated and automatically executed. In this way, it enables simultaneous and instantaneous settlement. In contrast to the crypto world, settlement in central bank money ensures the singleness of money and the finality of payments. Second, by having everything in one place, it allows new types of contingent contracts that serve the public interest by overcoming obstacles associated with information and incentive problems.

The ideas behind the unified ledger show how the future monetary system might evolve. In practice, the specific needs and constraints of each jurisdiction will dictate which applications of the concept will take root first, and on what scale. Along this journey, multiple ledgers, each catering to specific use cases, could coexist and interconnect through APIs to ensure interoperability.

Crucially, this journey requires a shift in emphasis from individual experimentation to joint innovation. Public-private collaboration is essential to develop technological solutions, establish common platforms and ensure proper oversight and supervision. Through cooperation, innovation and integration, it is possible to pave the way for a monetary system that builds on trust, enables new economic arrangements, enhances the efficiency and accessibility of financial transactions and responds to the evolving demands of households and firms.

Endnotes

[1] Schnabel and Shin (2004) provide a historical account of bills of exchange, their evolution from instruments in the payment system to sophisticated instruments of credit, and their role in fostering the growth of trade and commerce. Related discussions are also presented in Quinn and Roberds (2015, 2016) and Frost et al (2020), who also discuss how the Bank of Amsterdam took on a lender of last resort function in the 1763 panic, providing emergency liquidity by accepting a broader range of collateral, and with open market operations.

[2] For further elaboration on the structural flaws of crypto see BIS (2022) and Boissay et al (2022).

[3] See Carstens (2023b).

[4] See Carstens (2023a).

[5] Token-specific contracts also allow for the ability to transfer fractions of a token, so-called fractionalisation. Fractionalisation could lower the barriers to entry for households, thus helping to widen financial inclusion.

[6] See BIS (2022).

[7] See Cunliffe (2023).

[8] Asset-backed stablecoins are by far the most prevalent form of stablecoin. They are usually pegged to a numeraire, such as the US dollar, and backed by assets such as government bonds, short-term corporate debt or bank deposits. The issuer typically manages the underlying collateral and coordinates the coins' redemption and creation. Currently, stablecoins are used mainly within the crypto system and are typically provided by unregulated issuers.

[9] See McLeay et al (2014).

[10] This discussion is based on stablecoins of the safest possible variety, namely those fully backed by the safest and most liquid assets. Other varieties such as those backed by risky assets or algorithmic stablecoins do not represent a viable alternative (BIS (2022)).

[11] See Garratt and Shin (2023).

[12] See Garratt et al (2022).

[13] These considerations would also be relevant to retail CBDC. However, similar measures that apply to cash today, such as the Financial Action Task Force requirements, could apply to retail CBDC.

[14] For example, Lotus 1-2-3 was the standard spreadsheet program throughout the 1980s and into the early 1990s. It was widely used by financial traders, portfolio managers and analysts in investment and commercial banks, brokerage houses and money management companies. Despite various updates, technical setbacks meant that Lotus was struggling to keep pace with the rapid advances in computing power. In the early 1990s, Lotus was surpassed by Microsoft's Excel, which provided new functionalities and easier usability through a graphical user

interface. Similarly, a key reason why smartphones replaced earlier versions of the cell phone was not because they were better for making calls or sending texts, but because they let third parties use their creativity in developing new products and services through apps.

[15] Real-world information can be represented on the ledger in two ways. First, via oracles, which are third parties that enter data onto the unified ledger so that they can be directly referenced by smart contracts. Second, via application programming interfaces (APIs). The so-called oracle problem (Duley et al (2023)), which hinders the use of real-world data on decentralised platforms, would not apply, as the unified ledger would use a trusted and mutually accepted set of rules and procedures for data access and conflict resolution in the event of discrepancies.

[16] In the case of a card payment from a customer to a merchant there is an additional authentication and verification process that involves the merchant, the purchaser's bank, the acquiring bank and, in many cases, an access control service that verifies the payment instrument (eg debit/credit card).

[17] See CPMI (2023).

[18] Atomic settlement involves the reduction of settlement lags (potentially to zero, ie "instant settlement"), while extending the functionality of delivery-versus-payment (DvP) and payment-versus-payment (PvP) arrangements such that multiple linked transactions by various parties can be bundled and settled together ("simultaneous settlement"). See Bech et al (2020) and Lee et al (2022).

[19] Another improvement from the adoption of a unified ledger relates to the transaction initiation process. Most person-to-business transactions currently involve an initial validation/verification process that involves contacting an intermediary, verifying the customer's identity and the payment instrument (eg the debit card using the CVV code) and having all these checks communicated to all relevant participants (eg the buyer, the merchant, the buyer's bank and the acquiring bank). On a unified ledger, these steps are replaced by the use of private and public keys, which confirm legitimate ownership of funds.

[20] More broadly, PvP arrangements may add to funding liquidity risks, as funding is needed to carry out a transaction when required.

[21] See Costello (2019). Project Dynamo by the BIS Innovation Hub also investigates how tokenisation could improve supply chain finance.

[22] See Association of Certified Fraud Examiners (2022).

[23] See Gambacorta et al (2023).

[24] These problems became particularly acute with the entry of large technology firms into financial services. See Boissay et al (2021).

[25] See Blattner and Nelson (2021) and Doerr et al (2023).

[26] See Auer (2022).

[27] For example, the so-called servicer collects borrower repayments, pools them and forwards them to a trustee. The trustee then distributes the pooled repayment to security holders according to the structure set in the transaction documents.

[28] See CPSS-IOSCO (2012).

[29] See Manning et al (2009).

[30] Most OTC markets rely on large financial institutions (dealers) to intermediate between investors.

[31] Kutai et al (2023) argue that two main reasons can explain this: the possibility of conducting all-to-all trading, and the ability to generate efficiency gains from instant netting of bilateral settlement obligations.

[32] See Allen and Wittwer (2023).

[33] See Duarte et al (2022).

[34] Evidence from the mandate to trade index credit default swaps in swap execution facilities suggests as much; see Riggs et al (2020).

[35] See Armantier et al (2021) and Chen et al (2023).

[36] Privacy-preserving technologies are based on various methodologies. HE uses the principle of additive and multiplicative homomorphism to enable computations on encrypted data, yielding the same result as if the computations were performed on the original data. SMPC allows multiple parties to jointly compute a function without revealing their input values. However, as the number of parties increases, SMPC may entail higher communication costs. FL allows each party to train a machine learning model separately without sharing their data. Instead, parties only reveal their updated model parameters to a third or central party to collectively build a better machine learning model by aggregating the parameters. DP adds calibrated noise to the original data to protect the privacy of the data. However, there is a trade-off between accuracy and privacy in DP, as improper calibration of noise can result in inaccurate results.

[37] See Eisenbach et al (2022).

[38] See Anand et al (2022), Doerr et al (2022) and Garratt and Schilling (2022).

Technical annex

Graph 7.A: Each bar reflects the coefficient estimate of the elasticity of credit to changes in firms' transaction volume or local house prices in firm-quarter regressions.

Graph 7.B: ROC curves plot the fraction of non-defaults admitted for a given score cutoff against the fraction of defaults admitted.

Graph 8.A: Based on cyber crimes reported to the Internet Crime Complaint Center (IC3) of the Federal Bureau of Investigation (FBI).

Graph 8.B: Share of respondents who selected each respective answer to the question "Do you think that investment on cyber security has been too little/adequate/too much over the past year?".

References

Aldasoro, I, S Doerr, L Gambacorta, R Garratt and P Koo Wilkens (2023): "The tokenisation continuum", *BIS Bulletin,* no 72, April.

Allen, J and M Wittwer (2023): "Centralizing over-the-counter markets?", *Journal of Political Economy*, forthcoming.

Anand, K, C Duley and P Gai (2022): "Cybersecurity and financial stability", *Deutsche Bundesbank Discussion Papers*, no 08.

Armantier, O, S Doerr, J Frost, A Fuster and K Shue (2021): "Whom do consumers trust with their data? US survey evidence", *BIS Bulletin*, no 42, May.

Association of Certified Fraud Examiners (2022): "Occupational fraud 2022: a report to the nations".

Auer, R (2022): "Embedded supervision: How to build regulation into decentralized finance", *Cryptoeconomic Systems*, vol 2, issue 1.

Bank for International Settlements (BIS) (2022): "The future monetary system", *Annual Economic Report 2022*, June, Chapter III.

Bank for International Settlements Innovation Hub (2023): "Lessons learnt on CBDCs", report to the G20, forthcoming.

Bech, M, J Hancock, T Rice and A Wadsworth (2020): "On the future of securities settlement", *BIS Quarterly Review*, March, pp 67–83.

BIS Committee on Payments and Market Infrastructures (CPMI) (2023): "Facilitating increased adoption of payment versus payment (PvP) – final report", March.

Blattner, L and S Nelson (2021): "How costly is noise? Data and disparities in consumer credit", working paper.

Boissay, F, T Ehlers, L Gambacorta and H S Shin (2021): "Big techs in finance: on the new nexus between data privacy and competition", *BIS Working Papers*, no 970.

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

Carstens, A (2023a): "Innovation and the future of the monetary system", keynote speech at the Monetary Authority of Singapore, 22 February.

——— (2023b): "The value of trust", speech at award ceremony, King of Spain Prize in Economics, Madrid, 6 March.

Central Bank of Brazil (2023): "Motivations for the Brazilian Digital Real pilot", Voto 31/2023, 14 February.

Chen, S, S Doerr, J Frost, L Gambacorta and H S Shin (2023): "The fintech gender gap", *Journal of Financial Intermediation*, vol 54.

Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commissions (CPSS-IOSCO) (2012): *Principles for financial market infrastructures*, April.

Costello, A (2019): "The value of collateral in trade finance", *Journal of Financial Economics*, vol 134, no 1, pp 70–90.

Cunliffe, J (2023): "The shape of things to come: innovation in payments and money", speech at the Innovate Finance Global Summit, London, 17 April.

Doerr, S, L Gambacorta, T Leach, B Legros and D Whyte (2022): "Cyber risk in central banking", *BIS Working Papers*, no 1039.

Doerr, S, L Gambacorta, L Guiso and M Sanchez del Villar (2023): "Privacy regulation and fintech lending", *BIS Working Papers*, no 1103.

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.

Eisenbach, T, A Kovner and M Lee (2022): "Cyber risk and the US financial system: A pre-mortem analysis", *Journal of Financial Economics*, vol 145, no 3, pp 802–26.

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

Gambacorta, L, Y Huang, Z Li, H Qiu and S Chen (2023): "Data vs collateral", *Review of Finance*, vol 27, no 2, pp 369–98.

Garratt, R and L Schilling (2022): "Optimal data security with redundancies", working paper.

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

Garratt, R and H S Shin (2023): "Stablecoins versus tokenised deposits: implications for the singleness of money", *BIS Bulletin,* no 73, April.

Kutai, A, D Nathan and M Wittwer (2023): "Exchanges for government bonds? Evidence during COVID-19", mimeo.

Lee, M, A Martin and B Müller (2022): "What is atomic settlement?", Federal Reserve Bank of New York, *Liberty Street Economics*, November.

Manning, M, E Nier and J Schanz (2009): *The economics of large value payments and settlement: theory and policy issues for central banks*, Oxford University Press.

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

McLeay, M, A Radia and R Thomas (2014): "Money creation in the modern economy", Bank of England, *Quarterly Bulletin*, First Quarter.

Quinn, S and W Roberds (2015): "Responding to a shadow banking crisis: the lessons of 1763", *Journal of Money, Credit and Banking*, vol 47, no 6, pp 1149–76.

——— (2016): "Death of a reserve currency", *International Journal of Central Banking*, vol 12, no 4, pp 63–103.

Riggs, L, E Onur, D Reiffen and H Zhu (2020): "Swap trading after Dodd-Frank: evidence from index CDS", *Journal of Financial Economics*, vol 137, no 3, pp 857–86.

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.

Glossary

Accounts: (digital) representation of an end user's set of claims, real or financial.

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

Atomic settlement: instant exchange of assets, such that the transfer of each occurs only upon transfer of the others.

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 on a programmable platform.

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. These interfaces are built on non-programmable platforms. Not to be confused with a token wallet.

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

Delivery versus payment (DvP): A settlement mechanism that links an asset transfer and a funds transfer in such a way as to ensure that delivery occurs if and only if the corresponding payment occurs.

End users: individuals, households and firms that are not participants in a platform

Homomorphic encryption (HE): a technique that allows data to be encrypted in such a way that they can be processed by third parties without being decrypted.

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.

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.

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

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

Programmable platform: technology-agnostic platform that includes a Turing machine with an execution environment and a ledger and governance rules.

Payment versus payment (PvP): a settlement mechanism that ensures that the final transfer of a payment in one currency occurs if and only if the final transfer of a payment in another currency or currencies takes place.

Ramps: protocols that connect non-programmable platforms to programmable platforms. Ramps lock assets in their platform of origin as collateral for the tokens that are issued on the programmable platform.

Secure multi-party computation (SMPC): a cryptographic technique that allows multiple parties to jointly compute a function on their private data without revealing the data to each other.

Smart contract: self-executing applications of programmable platforms 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 programmable platform. Tokens can be tokenised, ie derived from claims in traditional ledgers, or can be issued natively in the platform, ie "native" tokens.

Tokenisation: the process of recording claims on real or financial assets that exist on a traditional ledger onto a programmable platform.

Tokenised asset: a digital representation of a claim of an asset in a programmable platform.

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