

European Stability Mechanism



Wholesale central bank digital currency – the safe way to debt capital market efficiency

In this paper we analyse the usefulness of digital currencies for wholesale financial transactions in Europe. Currently, several risks impede any broad adoption of distributed ledger technology, but this sovereign debt issuance case study demonstrates the potential widespread efficiency gains from smart contracts run on distributed ledger technology. A wholesale central bank digital currency on a private permissioned blockchain could overcome existing risks and impediments and lead to significant efficiency gains in the financial system across debt capital markets.

Josselin Hebert*
Edmund Moshhammer
Herbert Barth**

March 2023



The authors are grateful for the insightful comments from Kalin Anev Janse, Rolf Strauch, Niels Hansen, Jürgen Klaus, George Matlock, Raquel Calero, Stefano Finesi, and Stéphane Vincent.

Disclaimer: The views expressed by external authors in this discussion paper do not necessarily represent those of the ESM or ESM policy. The ESM accepts no responsibility or liability for the accuracy or completeness of the information, including any data sets presented in this paper.

* j.hebert@esm.europa.eu

** Herbert Barth contributed to this paper when employed at the ESM.

PDF	ISBN 978-92-95223-29-5	ISSN 2467-2025	doi:10.2852/615824	DW-AC-23-001-EN-N
-----	------------------------	----------------	--------------------	-------------------

More information on the European Union is available on the Internet (<http://europa.eu>). Luxembourg: Publications Office of the European Union, 2023

© European Stability Mechanism, 2023

All rights reserved. Any reproduction, publication, and reprint in the form of a different publication, whether printed or produced electronically, in whole or in part, is permitted only with the explicit written authorisation of the European Stability Mechanism.

Table of contents

Foreword	2
Executive summary	4
Introduction	6
1. Background	7
Disruption and innovation: where it all started	8
Stablecoins and tokenised commercial bank money	9
A European central bank digital currency	10
Tokenisation of bonds	11
The legal framework for a central bank digital currency	11
2. Benefits of a wholesale digital euro	13
Increased speed of execution	14
Transparency	14
Financial stability	17
Scalability	18
Risk reduction and risk mitigators	18
Cost savings	21
3. Benefits demonstrated by sovereign and supranational issuance	23
Next-generation automation experiments for post-trade	24
Pre-trade automation in case of auction-based debt issuance	26
Pre-trade automation for syndication-based issuance and related limitations	29
Setup proposal – a private permissioned blockchain	29
Implications for primary and secondary markets	34
4. Conclusion	36
References	38
Acronyms & Glossary	42

Foreword



KALIN ANEV JANSE

Chief Financial Officer and Management Board Member

A digital euro would offer an electronic means of payment and settlement for European Central Bank issued money. Early discussions on the creation of a European central bank digital currency (CBDC) led the European Central Bank to investigate the potential design for a digital euro¹ and the Bank for International Settlements to conduct experiments, albeit mainly focused on providing a retail version CBDC. The benefits of a retail digital euro, including strengthening the international role of the currency, have been widely discussed. The ESM fully supports the European Central Bank in this process which it drives. But little has been said on the benefits of a wholesale digital euro. In this paper, the authors address this gap in and explore the possible benefits of a wholesale digital euro for debt capital markets from an ESM perspective.

The ESM sees the wholesale digital euro as a game changer for future developments. Indeed, a broad stakeholder community of professionals across financial markets has made a strong case for a wholesale digital euro, considering “a digital central bank money issued by the Eurosystem to be a cornerstone to support wholesale payments, security settlement,² and collateral management [...] enabling next-generation automation through smart contracts, reduced friction and [this] would also further support the EU’s Capital Markets Union.”³

The ESM’s mandate is to support the financial stability of the euro area by providing loans to countries in financial distress. The ESM finances these loans by issuing bonds on capital markets, both for new loan disbursements and refinancing of outstanding loans.⁴ Costs and execution of these funding transactions directly impact the borrowing countries. The ESM also invests capital that is the basis of its prime credit quality and low funding costs, a process that necessitates efficient capital markets. Thus, enhancing efficiency results in lower funding costs, better return on investments, broader availability of funding, and reduced execution risks closer to zero.

¹ European Central Bank, [Digital euro](#), (accessed 14 November 2022).

² Such as distributed ledger technologies, including but not limited to blockchain technologies.

³ International Capital Market Association, [International Capital Market Association's response to the European Central Bank questionnaire on financial market stakeholders' potential interest in the Eurosystem providing a euro central bank money settlement of wholesale transactions in the payments, securities settlement, and collateral management domains](#), p 1. (accessed 28 November 2022). The International Capital Market Association represents around 600 members from all stakeholder communities in financial markets.

⁴ Past loans generally have substantially longer maturities, beyond 40 years, than the corresponding bond issues. Therefore, bonds are refinanced until the final loan matures.

A wholesale euro issued by the European Central Bank would increase the speed of executions, foster transparency in record keeping, encourage global scalability, and enable purpose-bound money with a strong use case in environmental, social, and governance (ESG)-related finance. Risk reduction and cost savings would contribute to efficiency gains, reducing financial stability risks and supporting part of the ESM mandate.

At present, 105 countries are exploring CBDC issuance. Ten emerging market economies have already officially launched their CBDC,⁵ and central banks in major economies are laying the groundwork for their own digital currency.⁶ Notably, Singapore has already chosen the direction to pursue a wholesale CBDC, as Monetary Authority of Singapore Governor Ravi Menon announced in summer 2022.⁷

These developments point to the arrival of globally available CBDCs in one form or another, particularly for wholesale transactions. Therefore, the time is right to design the digital on-chain euro for international success. In the ESM's view, wholesale use cases merit due attention.

⁵ Atlantic Council, [Central Bank Digital Currency Tracker](#), (accessed 28 November 2022).

⁶ Bank for International Settlements, [Chang Yong Rhee: Central bank digital currency - what we have learned from a recent hands-on experiment](#), (accessed 28 November 2022).

⁷ Monetary Authority of Singapore, ["Yes to Digital Asset Innovation, No to Cryptocurrency Speculation" - Opening Address by Mr Ravi Menon, Managing Director, Monetary Authority of Singapore, at Green Shoots Seminar on 29 August 2022](#), (accessed 28 November 2022).

Executive summary

Digital enhancements increase efficiency and reduce risks.

Distributed ledger technology, powered by smart contracts, has the potential to greatly increase operational efficiency and reduce capital market risks. A distributed environment where transparent records are maintained allows for novel features such as purpose-bound money and greater auditability would enhance financial stability. Programmability reduces counterparty risks in transactions and increases scalability and interoperability through flexible interfaces. Controlled by supervised entities, risks related to know your customer, money laundering, terrorist financing, and cyber security become more manageable.

Cost savings stem from a wholesale digital euro.

These benefits carry potentially significant cost savings, particularly given today's tremendous volume of wholesale transactions. Automation should reduce staff costs and instant settlements can eliminate hedging and liquidity costs. Limiting risks such as counterparty risk will shrink associated costs, while expanding settlements in central bank money would reduce costs associated with credit risks in commercial bank money settlements. For ESG-labelled bonds, increased transparency could reinforce the greenium.

Hurdles remain on the road to broader use of distributed ledger technology.

Though given such benefits, why is distributed ledger technology not already more broadly adopted? There are three explanations. First, many central banks are working on related time-consuming projects. Second, private market solutions lack the availability of stable central bank money and are paralysed by reputation shocks. And third, several design choices remain undefined, such as the necessary legal framework, infrastructure governance, access management, how to ensure privacy, exception management, etc.

A realistic technical setup for sovereign debt issuance.

In this paper, we outline the setup of a private permissioned blockchain that could address these hurdles and demonstrate the benefits of automation tools for sovereign debt issuance. For auction type debt issuance, smart contracts would facilitate end-to-end automation, and bidders could lock their wholesale digital euro funds on-chain while the system would perform the allocation and exchange for on-chain debt instrument tokens.

Table 1

Summary of benefits and risks of a natively on-chain wholesale digital euro for debt capital markets

Theme	Benefits	Risks and mitigators
Speed of execution	Programmability enables automation of complex use cases such as end-to-end automation of debt issuance.	<u>Risk</u> : faulty smart contracts, including metamorphic smart contracts. <u>Mitigation</u> : code audit, metamorphic code detection methods.
Transparency	Immutability and transparency of records ensure high auditability.	<u>Risk</u> : smart contracts cannot be cancelled unless specifically programmed, creating a ‘fat finger’ risk. <u>Mitigation 1</u> : technical setup to allow for a modification or cancellation until a defined moment in time.
	Transparency on the use of proceeds for ESG-related bonds, linking the use of funds to auditable data sources.	<u>Mitigation 2</u> : sandbox environment to test smart contracts before deployment.
	Technical solutions to comply with privacy requirements of market participants and overall auditability.	<u>Mitigation 3</u> : exception management system for private blockchain.
Financial stability	Extending access to central bank money to additional capital market participants for increased stability through reduced credit and liquidity risk and real time oversight to operations by regulators.	<u>Risk</u> : broader access to central bank money could decrease access for commercial banks and increase the risk of bank runs. <u>Mitigation 1</u> : variable wholesale CBDC interest rate below commercial bank deposit rate would disincentivise digital euro as a store of value. <u>Mitigation 2</u> : smart contract switches and breaks.
Scalability	Smart contracts offer technical solution for interoperability of blockchains, overcoming fragmentation.	
Risk reduction	Settlement in central bank money is risk-free.	<u>Risk</u> : enforcing anti-money laundering and countering financing of terrorism may be challenging in an open, distributed environment. <u>Mitigation 1</u> : in a public blockchain (e.g. Ethereum) technical standards allow the enforcement of applicable regulations.
	Automation erodes human error in daily operations.	<u>Mitigation 2</u> : private, permissioned blockchain allows for regulated gatekeepers in charge of applying regulations.
	Instant settlement shrinks open positions between legal commitment and execution.	

Source: authors' compilation

Introduction

In this discussion paper, we argue that a shift to the use of distributed ledger technology and smart contracts would increase capital markets' efficiency and that an on-chain wholesale CBDC could enable that transition while also mitigating risks.

We lay out three main factors that currently limit broad use of distributed ledger technology as an infrastructure for financial transactions:

- First, while distributed ledger technology reduces some existing risks, it remains vulnerable to other risks that are well managed with the current infrastructure. Legal uncertainty and how to ensure know your customer compliance are two examples.
- Second, financial transactions always comprise a payment leg and a settlement leg. Settling transactions with distributed ledger technology, in the absence of central bank money available on-chain, introduces inefficiencies and risks such as the necessity of pre-funding and credit risk on the issuer of tokens for payment. The private creation of payment tokens would not allow to benefit from all the costs and time savings, nor ensure all the risk reductions identified for wholesale CBDC.
- Third, the threat of fraud and value volatility are two large barriers. Cryptocurrency's reputation suffered a huge blow with the recent fraud and subsequent collapse of FTX, with the market value of all cryptocurrencies tumbling by over USD 2 trillion since early 2021.⁸

However, as will be shown in this paper, the technology offers huge efficiency gains across financial transactions, provided these shortcomings can be overcome. The issue is therefore how to overcome these challenges and affect a broader roll-out of distributed ledger technology and ensure it outperforms legacy infrastructures in wholesale finance.

We therefore argue that on-chain wholesale central bank money for certain use cases would represent the best solution to mitigate the obstacles and reap the maximum benefits of financial transactions agreed and executed on chain, enabling smart contracts.

In Section 1 of this paper, we provide some context for the debate. In Section 2 we make the case for a purposeful wholesale CBDC that applies next-generation automation tools in a distributed environment to increase efficiency and reduce operational risks. We further discuss features any such wholesale CBDC would need to offer. In Section 3, using the example of sovereign debt issuance, we propose a potential high-level design of such a system. Our conclusions, laid out in Section 4, apply and are constrained to the specific use cases analysed in this paper.⁹

⁸ [The failure of FTX and Sam Bankman-Fried will leave deep scars](#), The Economist 17 November 2022 (accessed 17 November 2022).

⁹ It would go beyond the resources available for this paper to provide an overall analysis of wholesale CBDC as compared to all legacy infrastructures. For a broader picture of use cases, see [the International Capital Market Association's response to the Banque de France](#).



1. Background

Disruption and innovation: where it all started

On 31 October 2008 the whitepaper “Bitcoin: A Peer-to-Peer Electronic Cash System” (Nakamoto, 2008) served as a manifesto laying out a radical disruption of the then-existing financial system and proposing a system with no need for banks to act as middlemen for transactions. The paper put forward the application of blockchain-style distributed ledger technology and ‘mining’ as a consensus protocol. The public blockchain, the immutable database of all transactions across all accounts, is transparent and accessible to everyone, and ‘mining’ cryptographically ensures the integrity of transactions. Blockchain platforms allow instant peer-to-peer transactions, removing the need for banks to verify a personal account balance, and money supply is governed by computer algorithms rather than by central bankers.

Over the next decade, the blockchain-based platform Ethereum added smart contract functionality to blockchains. Rather than cash transactions, this technology allows for the representation of any asset, physical or digital, in the form of a cryptographic token, as well as the creation of decentralised applications that run autonomously on a peer-to-peer network. This is a generalisation to Bitcoin; smart contracts in Ethereum can be the foundation to an electronic currency such as Bitcoin, but they can stretch far beyond.

Entities that connect blockchains to external systems, called oracles, completed the toolkit by creating the potential to connect smart contract-enabled distributed ledger technology with any external data source, unlocking and multiplying automation capabilities. Two smart-contract parties could then, for instance, agree on a future payment based on the development of an exchange rate.

Distributed ledger technology, smart contracts, and the technical capabilities of oracles led to the emergence of decentralised finance. This deregulated and open-source environment drastically reduced entry barriers and attracted software developers and investors alike to establish decentralised alternatives for trading, lending, and investment functions. Eliminating middlemen and an inherent high degree of automation reduced service costs and transaction times substantially. New instruments, like cryptocurrencies whose price is designed to be pegged to a reference asset (called stablecoins), emerged as additional tools that allowed for the exchange of cryptoassets against a somewhat stable instrument.

A European Securities and Markets Authority report noted that decentralised finance shares many risks with traditional finance, such as market, credit, and liquidity risks, which might be exacerbated by the close interconnectedness and automaticity of smart contracts (European Securities and Markets Authority, 2022). However, decentralised finance also introduces new kinds of risks. Bugs or exploits in smart contracts can lead to theft, and often the governance of key services bears centralisation risks (Aramonte, Huang, & Schrimpf, 2021). In many cases, services are governed by a minority with the power to abruptly change the rules, potentially leading to front running or theft. Despite the transparency in all transactions, decentralised finance is complex to regulate given its low entry barrier, and as such is an increasing systemic risk to financial stability. At its peak at end-2021, the market value of cryptocurrencies totalled nearly USD 3 trillion, with roughly USD 150 billion directly related to decentralised finance. Both numbers fell by about two thirds in 2022 due to macroeconomic developments such as rising interest rates and inflation – along with the collapse of the algorithmic stablecoin platform terraUSD and major cryptoassets exchange FTX. The terraUSD collapse was due more to the malfunctioning and risks of stablecoins used rather than to the functionality of decentralised finance, and the FTX collapse was related to fraudulent management and a lack of regulation.

Figure 1

Market capitalisation of crypto and decentralised finance

(in USD million)



Source: CoinGecko.com

While decentralised finance does pose certain risks, the automation capabilities developed by distributed ledger technology, smart contracts, and oracles driving this nascent industry could positively impact numerous industries, including debt capital markets.

Stablecoins and tokenised commercial bank money

Asset trades typically include two legs, the asset leg and the cash leg. In a world where assets are represented by tokens on a distributed ledger, the asset leg materialises in the transfer of tokens on the distributed ledger, whereas the cash leg might occur on- or off- ledger. On ledger cash allows for all the benefits of programmability by remaining on-chain while avoiding disruptions to the process.

Cryptocurrencies were natural candidates for the cash leg in decentralised finance, but they are too volatile for a settlement instrument. More stable instruments were needed, such as stablecoins and tokenised commercial bank money.

Stablecoins “... aim to maintain a stable value relative to a specified asset (typically US dollars), or a pool or basket of assets, and provide perceived stability when compared to the high volatility of unbacked cryptoassets.” (Financial Stability Board, n.d.). Describing all types of stablecoins goes beyond the remit of this paper, so we only mention fiat-collateralised stablecoins. These are issued by corporates who claim to hold commercial bank money reserves to back each stablecoin one-to-one, which could be considered as a potential on-ledger cash instrument to settle tokenised asset transactions. However, in today’s environment they present a number of risks: mainly legal risks because stablecoins are currently unregulated; credit risks against the stablecoin issuer; and counterparty performance risk involving the ability of the stablecoin issuer to maintain a reliable system.

Tokenised commercial bank money, another on-ledger cash instrument, aims to offer value stability for the cash leg of transactions. These are issued by commercial banks and backed by

assets held by the issuer, but credit risks remain given the liability to the commercial bank issuing it.

Synthetic CBDC is another option that private actors may offer to facilitate digital asset transaction settlements. This consists of a financial institution issuing an on-chain token backed by reserves it holds at a central bank, though counterparty performance risks would remain if such actors were to be regulated.

A European central bank digital currency

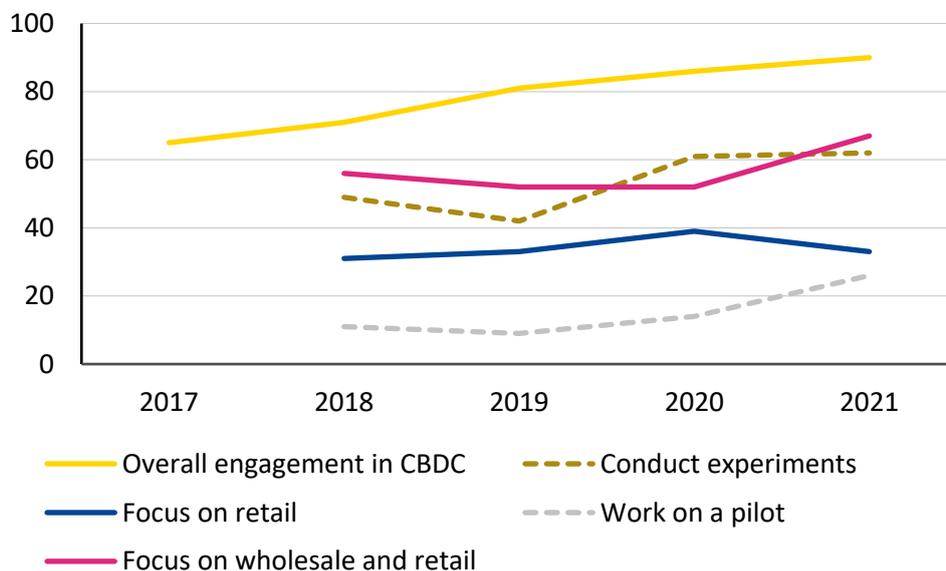
There is currently no European CBDC accessible for retail use. The only form of the euro that is a direct liability of the central bank for retail use is the physical bank notes or coins. Central bank money has, however, been digitally available for wholesale transactions for decades (Panetta, 2022). Though no accessible on-chain version of that exists today. The European Central Bank is investigating a digital euro project focusing on retail use while also studying for wholesale use the best technical answer to meet market participants expectations in a managed, less risky environment.¹⁰

A growing number of central banks around the world are exploring – and at times even rolling out – both retail and wholesale CBDC.

Figure 2

Survey results for central bank involvement in CBDC

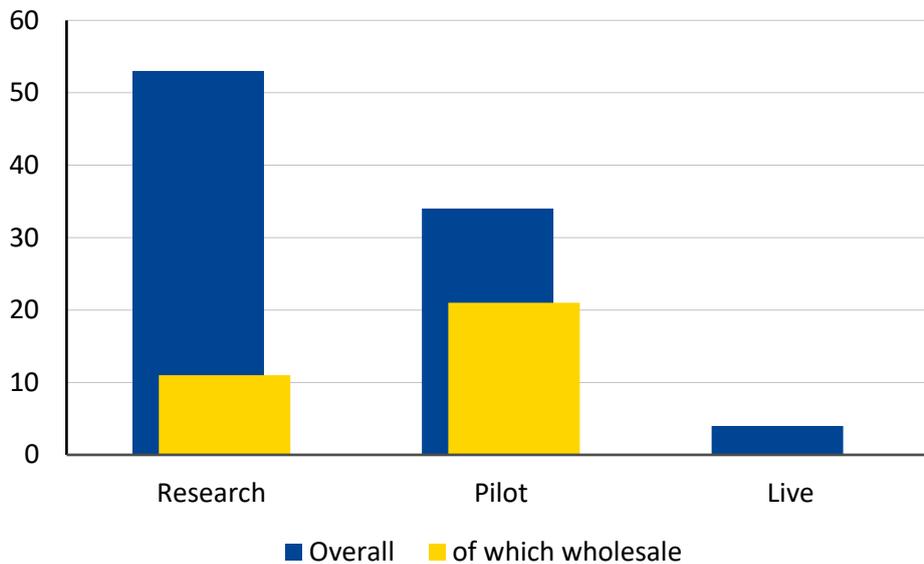
(share of respondents)



Source: 2021 Bank for International Settlements central bank survey on CBDCs and digital tokens

¹⁰ European Central Bank, [Digital euro](#), (accessed 14 November 2022).

Figure 3
Survey results of central bank involvement in CBDC in 2022
(number of central banks)



Note: Updated dataset on CBDC projects, speeches, and search interest, as of 13 January 2023.
Source: Auer, Cornelli, & Frost, 2020

We find that there are two key features a CBDC needs to facilitate wholesale use – tokenisation and legal clarity on its functionality. Endowing a wholesale digital euro with such features would facilitate the effective modernisation of Europe’s capital markets.

Tokenisation of bonds

Asset tokenisation consists of converting the rights of an asset into a digital token, i.e. a representation of the asset on a distributed ledger.

In the case of a debt instrument, the bondholder will have a digital wallet on a distributed ledger with a record of tokens assigned to the bondholder’s wallet.

For example, when issuing a tokenised bond for a notional value of €1 billion with a minimum denomination of €1 million, an issuer would issue 1,000 tokens – each with a nominal value of €1 million. These would then be allocated to primary market buyers using a delivery versus payment settlement before being traded on-chain on the secondary market.

Each token grants rights to its holder, the type and breadth of which depend on the specificity of the issue. At a minimum, it grants the holder the right to receive the nominal value at redemption date and any coupon payments attached to the bond.

The legal framework for a central bank digital currency

The introduction of CBDC requires legal certainty about its status and functionality as a basis for trust in the currency. Therefore, the introduction of a CBDC calls for a legal framework that defines the central bank’s mandate to issue CBDC and the legal status of such CBDCs. It is often

argued that legislation enabling CBDCs should also ensure they are fully fungible with fiat currency and their treatment when held by intermediaries. The prudential treatment of CBDC should also be the same as for other forms of central bank money.

Moreover, wholesale CBDC legal frameworks should also recognise settlement finality and netting for payments made with wholesale CBDC.

The legal status and implications of CBDCs depend on the design features according to a global overview provided by the Bank for International Settlements. While account-based designs are well understood in law, the legal status of digital tokens is often unclear. Among the 171 central banks within the International Monetary Fund membership, 61% of central bank laws limit the authority of currency issuance to banknotes and coins – and therefore do not support token-based CBDC interpretations. Wholesale applications are more straightforward, with 85% of central bank laws supporting the issuance of account-based CBDC to a restricted group of stakeholders – such as the state and banks – but exclude the general public (Bossu, et al., 2020). Furthermore, a 2021 Bank for International Settlements survey across 81 central banks found 10% were changing legislation to render it more friendly to CBDC (Kosse & Mattei, 2022).



2. Benefits of a wholesale digital euro

A wholesale digital euro is mostly about efficiency gains. More automation implies increased speed of execution, interoperability, and cost savings. Because transactions can be instantly settled and rely on central bank money, this reduces counterparty risks and adds real time regulatory oversight, thereby potentially considerably strengthening financial stability. Furthermore, the distributed ledger offers new tools such as purpose-bound money.

Increased speed of execution

Programmability is of the essence

Financial transactions today imply a great number of different actors executing and verifying contractually required steps for payments and settlements. Smart contracts fundamentally change this multi-tiered and error-prone process. They would be essential to reap the full benefits in cases such as sovereign issuance, as demonstrated in Section 3.

A key step for bidders would be locking funds into a smart contract that would automatically execute upon the closing of a deal, either by being transferred to the issuer or released should the bid be too low. A smart contract cryptographically resolves the counterparty risk of bidders failing to stand by their bid, at very little cost. Both issuers and bidders can trust in a smooth operation governed by the smart contract, which is transparent to everyone and executed by a trusted system. Initially, this would apply to auctions, but it is possible to imagine the application for syndicated issuance if the allocation rules and related investor qualities are established and coded – while remaining private to the issuer.

A programmable on-chain wholesale digital euro would foster end-to-end automation of debt issuance, thus accelerating the speed of execution. We examine such a potential use case in more detail in Section 3.

Transparency

Record keeping and immutability

One key novelty promised by blockchain is the transparency of records at any point along the process. Immutability of records ensures that transparency cannot be blurred by retroactive interventions.

The transparency and immutability features provide a remarkably high auditability of the code and the process, with on-chain code replacing legacy written contracts. Generally, such code is also provided in a non-technical format so it is easily understood by all stakeholders. All actions required by the code in smart contracts are readable and checkable at any point in time by all authorised participants in the financial transaction.

However, this immutability comes with a ‘fat finger’ risk, whereby a user incorrectly inputs information and, once submitted, a smart contract cannot be cancelled unless programmed otherwise.

We demonstrate that this risk can be largely eliminated in the use case of an on-chain debt issuance system, since the technical parameters could allow investors to update or cancel bids up to a certain point, either at the user interface or at the smart-contract level pre-defined and established by the issuers in the system. It would then be clear to participants that bids would be final beyond this set time limit.

A sandbox environment, whereby participants can test their smart contracts prior to deployment would offer a level of protection against any risk of deploying faulty smart contracts in a live environment.

In addition, an exception management system could be considered. A private blockchain, involving a limited number of nodes with regulated and trusted operators, seems more appropriate than a public blockchain in such a case.

Purpose-bound money and environmental, social, and governance

A potential specific new use case of wholesale CBDC lies in the transparent use of proceeds from ESG-related bonds.¹¹ These bonds, often referred to as ‘green’ or ‘social’ bonds, commit the issuer to use the funds from investors for specified ESG purposes. An on-chain wholesale CBDC would allow for the programming of the intended use of proceeds directly within the money raised from investors. The use of funds as committed by the issuer could be traced on-chain until the final disbursement for the intended and committed purpose. This would mitigate risks of green washing, improve reporting and thus support trust and transparency in the labelled ESG bond market.¹²

The Monetary Authority of Singapore has published a report on the potential uses of purpose-bound money for their economy.¹³ Though that report delineates retail use cases, such as purpose-bound vouchers or government payouts, the same technical logic could be applied to wholesale purpose-bound money. In this case, the purpose would be defined as the intended use of proceeds for ESG.

As it has been successfully tested by the Monetary Authority of Singapore that “purpose-bound money enables senders to specify conditions, such as validity period and types of shops, when making transfers in digital Singapore Dollar”,¹⁴ so at the wholesale level an ESG loan provider would send to the borrower under the loan CBDC a communication specifying for which ESG expenditures the loan can be used. This should strengthen both the issuer’s ESG-funding credibility and the overall credibility of ESG-related bond markets.

The control and reporting of fund usages could be linked technically to auditable data sources using oracles, so promoting the implementation of smart contracts that establish the conditions for the use of funds agreed for a specific instrument. The Japan Exchange Group intends to issue such a digitally-tracked green bond to finance its transition to 100% renewable electricity consumption, using solar panel output data in reporting linked to the green bond token.¹⁵

Project Genesis, an initiative by the Bank for International Settlements Innovation Hub and the Hong Kong Monetary Authority, has demonstrated how a private permissioned distributed ledger technology can help build an environment that offers investors a way to easily invest in green bonds using a stablecoin for the on-chain settlement of transactions and an extensibility

¹¹ Purpose-bound money can be used in wholesale and retail transactions. Our use case of ESG-related bonds starts at the wholesale level where an issuer raises money from investors and commits them to ESG use of funds. The tracking of the disbursements would be partially in the wholesale area (if funds are disbursed to agencies or financial institutions as intermediaries) and partially, as in the example from the Monetary Authority of Singapore, in the retail area, provided retail CBDC is available as well.

¹² We acknowledge that infrastructures such as programmable payments without CBDC can provide an alternative and should be further analysed for their comparative credentials.

¹³ Monetary Authority of Singapore, [MAS Report on Potential Uses of a Purpose-Bound Digital Singapore Dollar](#) (accessed 18 January 2023).

¹⁴ Monetary Authority of Singapore, [MAS Report on Potential Uses of a Purpose-Bound Digital Singapore Dollar](#) (accessed 18 January 2023).

¹⁵ Japan Exchange Group, [JPX Begins Research on “Digitally Tracked Green Bonds” Utilizing Security Tokens](#), (accessed 19 October 2022).

to CBDC. This project focused on retail investors, but the findings could also be applied to a wholesale CBDC platform.

Beyond the example ESG-related finance, we can consider many other potential uses and even conclude that the technology is use-case agnostic. In fact, the Monetary Authority of Singapore stated that “purpose-bound money refers to a protocol that specifies the conditions upon which an underlying digital currency can be used.”¹⁶

One major example might be spending programmes by governments and agencies. The disbursement of European Union funds under regional, sectorial, or other programme conditions¹⁷ could merit an experiment studying programmable payments with wholesale CBDC and its alternatives, such as bridge solutions using existing TARGET2 infrastructures.

Programmability does not guarantee that central banks issuing CBDC would provide purpose-bound money, e.g. in cases where some euros could only be spent for specific purposes. Programmability is rather a design feature allowing private users of CBDC to programme purpose-bound conditionality into the use of their funding.

Privacy considerations

While transparency is an important efficiency gain, some information privacy¹⁸ is essential for many use cases and would need management.

In a competitive market, parties would prefer to not disclose their interests to competitors. For instance, they might not want to be associated with particular transactions. In an issuance example, a bidder might not want to reveal his or her bid to other bidders. Investors in financial instruments generally do not want their holdings to be known to market competition.

Other use cases strictly require at least selective transparency while complying with anti-money laundering/combating financing of terrorism rules (see section on Risk reduction and risk mitigators). The underlying logic of smart contracts needs to be transparent to the parties involved, even if certain inputs (such as auction bids or the issuer’s chosen allocation key) are not. Parties may need to reveal their identity or specific identification features relevant for participation in restricted environments. For example, access today is restricted for many sovereign auctions, when applying for an undercollateralised loan, or when an entity must publicly report certain holdings.

Different implementation options exist for managing privacy requirements.

A system based on a public blockchain such as Ethereum would both promote transparency and offer some privacy because only public addresses are visible to the typical user, ensuring pseudonymity. However, this carries the risk that investors may discover each other’s transactions were they to know the public address of competing investors from, for example, having transacted together in the past. This could be overcome by establishing a unique public address for each action, i.e. setting up a new wallet, though the transfer of funds to the new address could still be traced.

Strict privacy could be implemented either through information technology (IT) solutions or cryptography. The IT solution is based on trusted execution environments, as demonstrated by the public blockchain protocol Oasis.¹⁹ Cryptographic solutions include designated verifier ring

¹⁶ Monetary Authority of Singapore, Project Orchid, (accessed 5 December 2022).

¹⁷ Such as the Next Generation European Union programme.

¹⁸ Privacy beyond regulatory purposes (see section on anti-money laundering and know your customer regulations).

¹⁹ The Oasis Protocol Foundation, [Oasis Network](#) (accessed 1 June 2022)

signature and zero-knowledge proofs, and have been demonstrated for anonymous sealed-bid auctions on public blockchains (Sharma et al., 2021).

A system based on a private or permissioned distributed ledger technology would allow for arbitrary degrees of privacy. Node operators, notably regulated entities, and regulators would have full visibility. It would then be a separate decision as to whether regular participants would see all transactions, similar to a public blockchain, or be limited to only viewing a participant's own transactions and those explicitly shared with the participant.

Financial stability

Mitigation of financial stability risks

Wholesale CBDC would foster financial stability, a core concern for central banks – including the robustness of financial market infrastructures and payment systems.

If wholesale CBDC was designed so that access was restricted to today's TARGET2 users, the introduction impact would centre on operational efficiency gains that add robustness to the system. However, should access be broadened to participants who want to exchange commercial bank deposits for wholesale CBDC, that would enhance financial stability. Wholesale CBDC would increase financial stability by avoiding credit and liquidity risks, and broadening access to wholesale CBDC would accommodate more participants in this low-risk instant-settlement environment. For example, investors today often need to engage in sovereign issuances through intermediaries with TARGET2 access. However, broadening access could crowd out commercial banks and render them more dependent on volatile wholesale funding sources, thereby increasing liquidity risk across the banking sector.²⁰

Different solutions have been postulated to protect financial institutions' balance sheets, including holding limits for a retail central bank digital euro. In a world of well-integrated commercial bank money and digital euro wallets, holding limits would not constrain transaction size, with incoming CBDC funds instantly transformed into commercial bank money and outgoing transactions splittable at limited cost. However, wholesale CBDC applications where tokens need to be locked (see Pre-trade automation in case of auction-based debt issuance section) would be hindered. More useful for wholesale CBDC would be a variable interest rate below the commercial bank deposit rate, so that bank deposits remain competitive, or alternatively a refinancing approach (Brunnemeier & Niepelt, 2019), whereby commercial bank deposits would be substituted by central bank lending.

Although broader access to central bank money holdings may increase the risk of bank runs in times of crisis, the implementation would give regulators real-time access to platform operations and allow them to take timely action during shocks and readjust protective rules such as margin requirements. Smart contracts could also be equipped with switches or breaks should too many commercial bank deposits of a single bank be converted in short time into wholesale CBDC. The ledger could play a major role in improving the ability of later audits. In this way, overall, on-chain wholesale CBDC has the potential to make the euro financial system

²⁰ High demand for digital euros may have a negative impact on financial stability, given the key role of the banking sector in financial intermediation. Following an increase in funding costs, banks might have to deleverage and reduce the supply of credit, thus hindering the optimal level of aggregate investment and consumption. This could ultimately lead to higher costs for borrowers and less economic activity.

more resilient.

Scalability

Smart contracts, given their generalist scripting language, are the means to ensure forward compatibility and scalability of distributed ledger technology-based platforms. We do not know how many different digital currencies will emerge over time, but we can ensure interoperability at low cost through smart contracts. For instance, hashed timelock contracts²¹ are a type of smart contract used in blockchain applications, that reduces counterparty risk by creating a time-based escrow that requires a cryptographic passphrase for unlocking. These can be used as cryptographic solution to atomic swaps between arbitrary blockchains. These blockchains may even be run in fully decoupled ecosystems, potentially using different programming languages and interfaces.

Today, cross-border payments entail significant transaction costs. The Bank for International Settlements Innovation Hub demonstrated in its Project mBridge that a multi-CBDC platform upon which multiple central banks could issue and exchange their respective CBDCs is a particularly promising solution for reducing these costs: “To achieve this, mBridge adopts a single-platform, direct-access CBDC model – a common technical infrastructure hosting multiple CBDCs, on which local and foreign financial institutions can directly hold and transact in CBDCs issued by central banks, irrespective of jurisdiction.” (Bank for International Settlements, 2022). In a world where both euros and dollars are tokenised on programmable blockchains, hashed timelock contracts would allow two actors to exchange these tokens using different platforms without exchanges or intermediaries. Though, some specific risks arising from timeouts in hashed timelock contracts – such as when one party could have both the asset and cash available – require proper management built into the system (Bech et al., 2020).

Risk reduction and risk mitigators

An on-chain digital euro could eliminate or at least substantially shrink certain risks inherent in the current financial market infrastructure:

- Settlement in central bank money is risk-free. Any alternatives, such as payment tokens, incur risks ranging from counterparty risks (credit and performance risks) to process risks.
- On-chain records are immutable, including their payment legs. This protects against intentional or unintentional changes to records without the consent of parties concerned.
- On-chain contracts and assets, including payments in CBDC, are a sequence of codes. Once approved, human error is eradicated from the process.
- Instant²² settlement removes open positions between legal commitment and execution,

²¹ The person receiving the funds in a transaction must perform two actions to access the funds: enter the correct passphrase and claim payment within a specific timeframe. If they enter an incorrect passphrase or do not claim the funds within the timeframe, they lose access to the payment.

²² Instant can mean within hours, minutes, or even seconds. Atomic settlement refers to settlement within seconds and is technically possible but doesn’t offer human decision makers time to perform verifications or corrections, and thus may not be adequate in all cases (e.g. with large financial transactions).

reducing the implied market risk and required hedging that adds counterparty risk.

However, on-chain financial transactions and payments also incur new risks. In our view, these can be efficiently mitigated using digital technologies that have evolved with the changes of risk patterns. Consequently, the net effect in risk reduction from using wholesale CBDC should be positive.

Enforcement of regulation on anti-money laundering and combatting financial terrorism

The European Union has adopted legislation to combat money laundering and terrorist financing.

Anti-money laundering and anti-terrorist financing rules apply to different potential users of wholesale CBDC. In the case of sovereign debt issuance, these rules would apply through the debt instrument issuance and lifecycle from the issuer to investors in the primary and secondary markets.

Issuer checks function in a similar way, whatever the technology, with banks acting as intermediaries and regulated actors in charge of performing the checks.

Investor checks on the primary markets have banks play the role of instrument distributors, which is the case no matter the issuance method chosen. In syndication, banks collect investor interest through book-building, while in auction they place bids themselves before acting as sellers and market makers with the investors.

However, on the secondary market, money laundering and financial terrorism risks arise with an on-chain process because investors could sell the instruments they hold in their wallet to any other investor without intermediary intervention. But this can be circumvented in several ways.

First, one could trust an intermediary custodian with the private key to the investor wallet. Without access to their own wallet, investors cannot initiate transactions without the custodian's involvement. The custodian must be a regulated actor, in charge of ensuring know your customer and anti-money laundering checks of those who want to purchase the security from the investor.

Second, technical standards can limit the ability to sell or purchase a token, making it possible to implement know your customer standards. Ethereum employs three such standards, one of which – considered the trading industry standard – ensures whitelisting of investors and compliance with selling restrictions.²³

Third, the distribution of the security and wholesale CBDC tokens on a private permissioned blockchain would create a secure environment in which investors could transfer security tokens. In such a technical design, regulated entities could operate the nodes, ensuring know your customer checks for all participants in a distributed way. Operating one common private distributed network engender additional efficiency because know your customer checks could be performed only once for the whole network instead of the number of times it's performed today. The Bank for International Settlements Innovation Hub's experiment on the use of wholesale CBDC across borders offers a variety of technical designs that leverage on the advantages of permissioned blockchains for anti-money laundering and know your customer considerations (Bech et al., 2022). Banque de France and the Monetary Authority of Singapore also demonstrated the added value of permissioned distributed ledger technology

²³ ERC1400, ERC1404 and ERC1462 standards allow the implementation of know your customer. ERC1400 (The Security Token Standard, n.d.) is the most complete standard for Security Tokens, whereas ERC1404 and ERC1462 offer simpler yet less complete approaches. ERC1404 ensures whitelisting of investors and compliance with selling restrictions and is considered by the industry as a relevant standard (Luxembourg Capital Markets Association, 2022)

environments for anti-money laundering, know your customer, and privacy concerns with the use of on-chain wholesale CBDC (Liquidity Management in a Multi-Currency Corridor Network, 2021).

We find that these solutions would ensure the full respect of anti-money laundering and combatting financial terrorism rules for both the holding of wholesale CBDC and tokenised debt instruments.

Box 1. Disintermediation and money laundering and terrorism financing risks

Decentralised finance applications make it technically possible to eradicate the middlemen. The suppression of intermediaries would reduce, if not remove, the need for financial transaction identity checks.

Traditional stakeholders in wholesale financial markets like the ESM do not support disintermediation. Neutral intermediaries like banks continue to play the key role in the protection of the general public against criminals laundering money and terrorism financing. Any financial infrastructure, legacy or on-chain, needs to ensure proper enforcement of applicable anti-money laundering and combatting financial terrorism rules, both at the time of any issue in the primary market and during its lifetime in the secondary market.

Tackling cybersecurity risks

Security is key when establishing any IT system for financial transactions, especially given the large amounts of money at stake in wholesale capital markets. Investors are institutional investors, and the unit of amount of issued debt is either billions of euros or US dollars, as illustrated in Table 2.

Table 2

Auction-based debt issuance volumes for a selection of sovereigns, supranationals, and agency issuers in 2021

Issuer	Bid amount	Total issued through auctions	Number of auctions	Average bid per auction	Average issued per auction
Agence France Trésor	€554 billion	€266 billion	103	€5.4 billion	€2.6 billion
Deutsche Bundesbank	€663 billion	€495 billion	155	€4.3 billion	€3.2 billion
US Treasury	N/A	USD 17,791 billion	445	N/A	USD 39.9 billion

Sources: Agence France Trésor, Deutsche Finanzagentur, U.S. Department of the Treasury.

This generates an extremely high incentive for potential hackers, demanding an especially robust system that can counter any unwarranted incursion.

Some security risks are specific to proof-of-work blockchains, such as 51% attacks – which do not exist for private permissioned blockchains with a trusted notary – with others common to all systems, such as phishing or routing attacks. All these risks are widely covered in the literature.

The risk of a faulty smart contract is another, more specific risk that would need to be addressed by any on-chain debt issuance system. As wholesale CBDC would be locked into smart contracts, a poorly written smart contract could lead to huge losses much higher than what has already

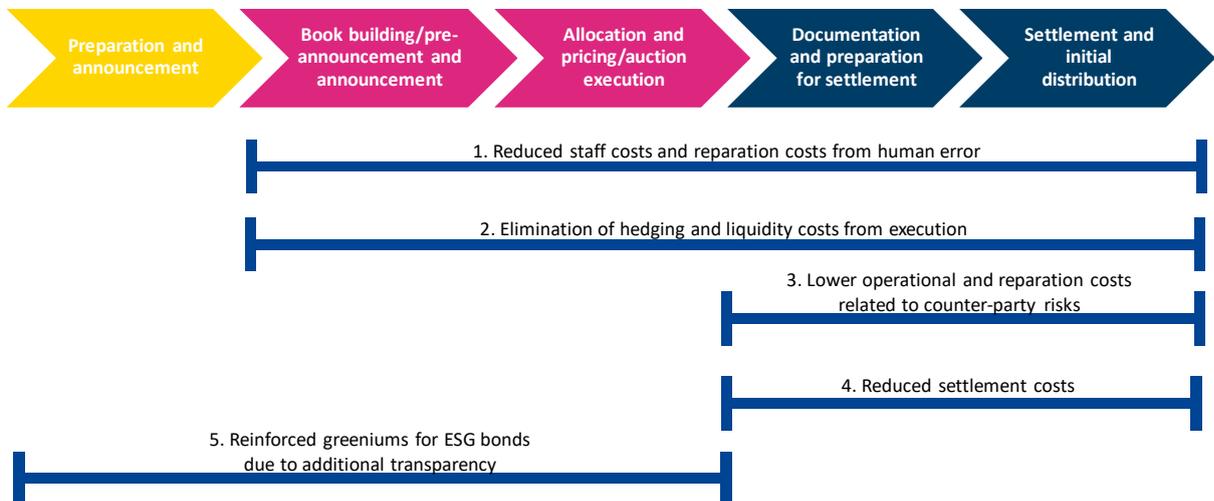
been seen in previous cases.²⁴ This risk could be mitigated through classic information security measures, such as code audit and penetration tests.

In addition, malicious actors could also develop so-called metamorphic smart contracts that would allow them to change the code in a smart contract after it has been deployed. Though, some methods do exist to detect such metamorphic smart contracts (Blau, 2022).

Cost savings

Cost savings flow from efficiency gains and impact the whole value chain of debt issuance, as illustrated in Figure 4. Even smaller cost savings span the entire life of a debt instrument because the settlement of debt service benefits from the same cost advantages as the initial settlement.

Figure 4
Cost savings of on-ledger wholesale CBDC in the case of sovereign bond issuance



Source: Authors' compilation

Real-time execution of financial transactions through smart contracts removes the risk of human error, which could incur reparation costs. Costs implied by the 'fat finger' risk can be managed by sandbox testing and an exception management system.

Reducing execution times, ideally through atomic settlement, could ultimately eliminate liquidity and hedging costs.

Reducing risks, such as counterparty risks, implies lower operational costs and reduces the costs that would be incurred if those risks materialised.

The availability of a wholesale digital euro would increase settlements in central bank money, thereby reducing the risks and associated costs of settlements in commercial bank money.²⁵

Issuers of ESG-labelled bonds enjoy reduced funding costs because investors accept a slightly lower yield for a good cause. Increasing transparency by technically linking the bonds to relevant

²⁴ Tech Monitor, [Top 10 biggest cryptocurrency thefts are estimated to amount to USD 3.1 billion](#) (accessed 16 June 2022)

²⁵ However, we acknowledge that international central securities depositories have been working with the European Central Bank on ways to provide T2S settlement as an option for bond settlements in central bank money.

data would reinforce this greenium.²⁶ Given the transparency and immutability of use-of-funds records, the cost of allocation reporting could be reduced by translating machine records into readable formats. Automated and trusted use-of-funds records could further facilitate any subsequent impact reporting and reduce related cost.

A cost increase is implied in the event of the technically feasible 24/7/365 service for a decentralised infrastructure with wholesale CBDC, but such service would only be provided on the strong assumption that the benefits of such around the clock-service would more than outweigh such operating costs.

In the current experimental and research phase, the magnitude of cost savings remains uncertain since it will depend on the choices of operating models and their design features (Kiff et al., 2020).²⁷ In Section 3 we describe a proposed infrastructure that leverages a private permissioned blockchain that would secure most benefits listed in this section.

²⁶ The term greenium has been derived from the standard term premium, meaning that an investor pays to issuer a difference to the market price. This is mainly the case for a new debt issuance when an investor pays up or an on-the-run-liquid new bond and for ensuring allocation to the investor.

²⁷ The logic of this article can be also applied to wholesale CBDC.

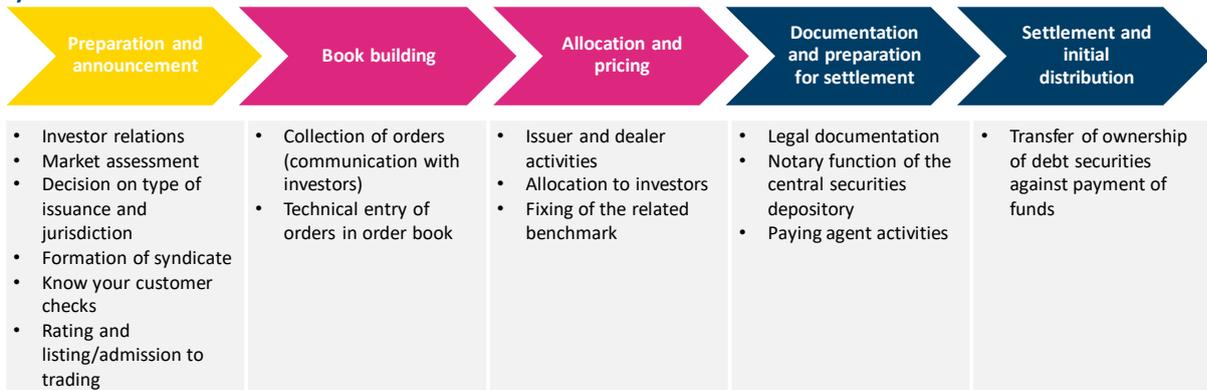


3. Benefits demonstrated by sovereign and supranational issuance

Next-generation automation experiments for post-trade

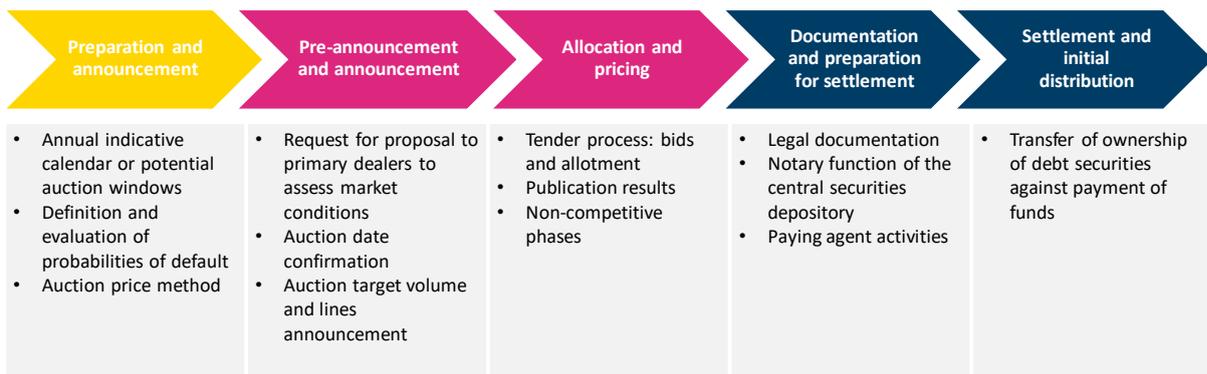
Today, sovereigns, supranationals, and agencies issue debt on the capital markets using two main issuance methods: syndication and auctions. These represent different approaches to trade preparation, or pre-trade steps, as illustrated in Figure 5 and Figure 6.

Figure 5
Syndication issuance model



Source: (European Central Bank Debt Issuance Market Contact Group, 2021)

Figure 6
Auction issuance model



Source: (European Central Bank Debt Issuance Market Contact Group, 2021)

In a syndication, the debt issuer selects a group of investors to sell a new offering. Book building and order consolidation are dematerialised, leveraging on software from the market, but order collection from investors is not automated and strongly based on personal relationships between investors, issuers, and bankers.

In an auction, banks that have an established relationship with the issuer are invited to an auction online, employing well-established methodology that may differ from one issuer to another (see Box 2 below). In some cases, the general public may also participate directly.

However, post-trade steps are the same for both syndications and auctions, i.e. documentation, settlement preparation, and final distribution.

Numerous recent experiments on private, permissioned, and public blockchains have explored the feasibility and potential added value of tokenised bonds and on-chain settlements. The objectives of some of these experiments were to demonstrate the feasibility of blockchain technology in issuing tokens representing debt instruments; the added value of representing debt with on-chain tokens; the feasibility of settling primary market (sell and buy positions for a

new issuance) and secondary market trades with wholesale CBDC; and the feasibility of settling such on-chain trades with traditional forms of central bank money.

The World Bank was the first to issue a bond on a private, permissioned blockchain, using an ad-hoc version developed by their Blockchain Innovation Lab, and targeting “faster, more efficient, and more secure transactions”.²⁸

The European Investment Bank was the first to issue a bond on a public blockchain. It issued a two-year €100 million bond on Ethereum in April 2021. The issuance was settled with wholesale digital euro, a wholesale CBDC issued intra-day by Banque de France for the specific purpose of this experiment, and was motivated by a “reduction of intermediaries and fixed costs, better market transparency through an increased capacity to see trading flows and identity of asset owners, as well as a much faster settlement speed.”²⁹ As the bond has not yet matured, learnings about secondary market trades have not yet been published, though some trades have been disclosed publicly.³⁰

The European Investment Bank also issued a two-year €100 million bond on a private permissioned blockchain, with two banks acting as custodians. Wholesale CBDC issued by Banque de France and Luxembourg Central Bank issued wholesale CBDC for settlement. This issuance implemented a same day settlement and a cross-chain delivery versus payment.³¹

Deutsche Bundesbank demonstrated the feasibility of triggering a payment in the conventional real-time gross settlement system from a distributed ledger technology environment, mentioning “more efficient securities settlement and securities digitalization”.³²

Banque de France, together with the French Debt Management Office Agence France Trésor, Euroclear, and major French banks experimented the on-chain settlement of French government bonds. This experiment relied on a permissioned blockchain with nodes deployed in the cloud, proving that transferring securities and CBDC tokens between different blockchains can be managed easily, and that settling bonds using wholesale CBDC can reduce the settlement time. It also found that such settlements removed more frictions than using a bridge solution to trigger a real-time gross settlement payment from a blockchain environment.³³

The Bank for International Settlements Innovation Hub conducted a series of projects exploring various aspects of wholesale CBDC:

- Project Helvetia, in collaboration with the Swiss National Bank and SIX Swiss Exchange Group explored how wholesale CBDC could be used to settle transactions involving tokenised financial assets. It demonstrated how wholesale CBDC would be integrated into the core banking systems of the central and commercial banks and simulated various trades.³⁴
- Project Jura, in collaboration with the Swiss National Bank and Banque de France experimented with the settlement of tokenised euro commercial paper and foreign

²⁸ The World Bank, [World Bank Prices First Global Blockchain Bond, Raising A\\$110 Million](#), (accessed 8 June 2022).

²⁹ European Investment Bank, [EIB issues its first ever digital bond on a public blockchain](#), (accessed 8 June 2022).

³⁰ Hedgeweek.com, [Generali carries out first market transaction based on blockchain infrastructure](#), (accessed 8 June 2022).

³¹ European Investment Bank, [EIB innovates further with Project Venus, the first euro-denominated digital bond on a private blockchain](#), (accessed 29 November 2022).

³² Deutsche Bundesbank, [DLT-based securities settlement in central bank money successfully tested](#), (accessed 8 June 2022).

³³ Banque de France, Euroclear, [Experimenting settlement of French government bonds in Central Bank Digital Currency with blockchain technology](#) (accessed 14 June 2022)

³⁴ Bank for International Settlements, Swiss National Bank, SIX Swiss Exchange, [Project Helvetia: A multi-phase investigation on the settlement of tokenised assets in central bank money](#), (accessed 14 June 2022).

exchange transactions. It demonstrated how central banks could allow access to CBDCs for regulated non-resident financial institutions.³⁵

- Project Mariana, in collaboration with Banque de France and the Monetary Authority of Singapore, investigated the use of automated market makers to automate foreign exchange markets and settlement. The objective is to demonstrate how cross-border payments may be improved.³⁶

The Monetary Authority of Singapore has been investigating on-chain CBDC since 2016 with Project Ubin.³⁷ The experiments successfully covered decentralised cross-border inter-bank payments and settlements, delivery versus payment settlement finality, and inter-ledger interoperability. In phase five of the Ubin project, the Monetary Authority of Singapore showcased many use cases across various industries, including atomic delivery versus payment of tokenised bonds and payments.

We find that these experiments all focused on the post-trade steps of debt issuance due to three main factors:

1. pre-trade steps are traditionally considered as relying heavily on investor relationships;
2. post-trade steps are the same no matter the issuance method; and
3. these are operational steps that are transparent for the investor.

These last two factors are an incentive to streamline and automate the process as much as possible.

Pre-trade automation in case of auction-based debt issuance

An auction system could be designed to use next-generation automation tools, unlocking end-to-end automation and conditional triggering brought forward by smart contracts.

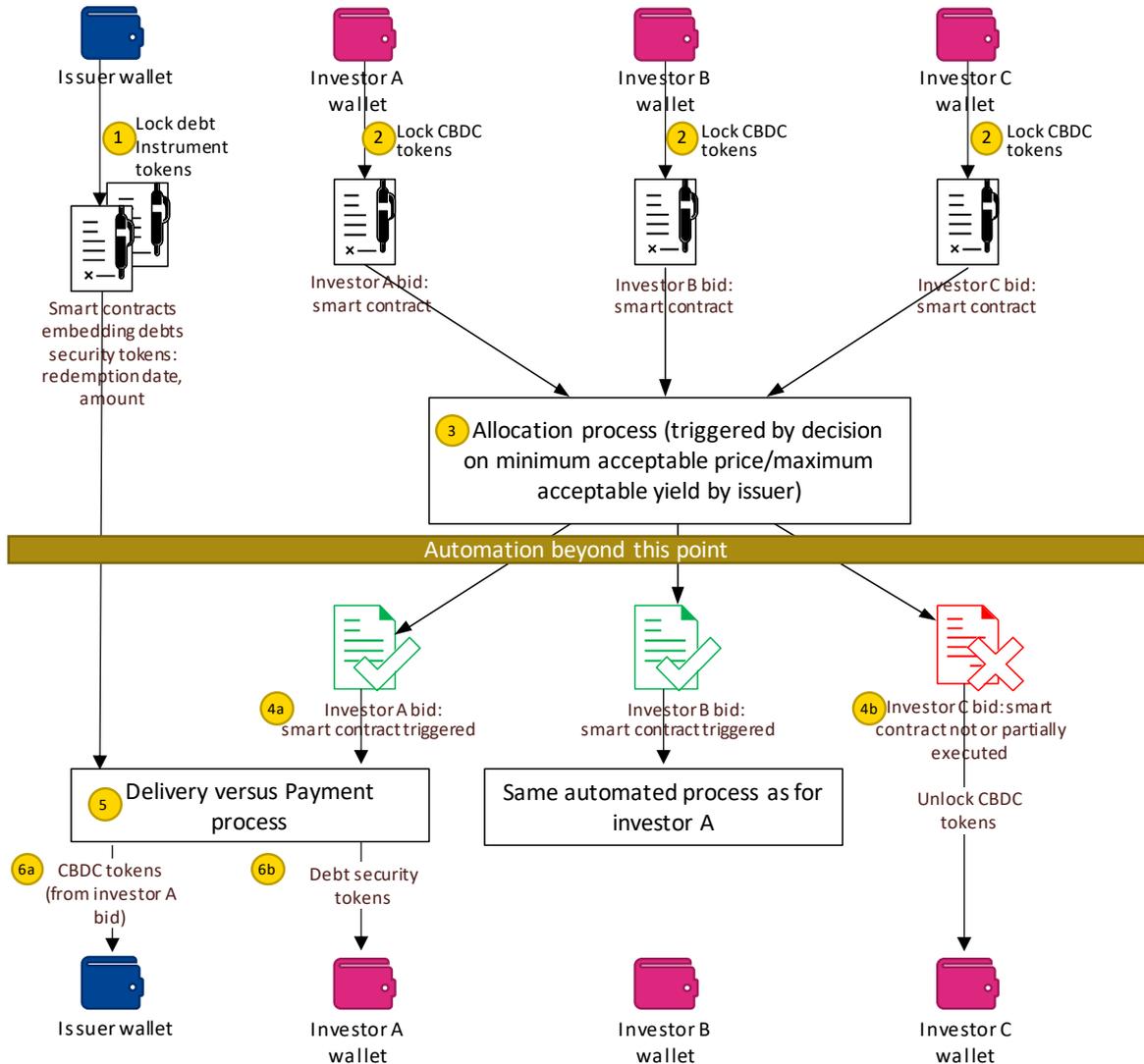
07 below sketches out a potential on-chain auction process that assumes the availability of on-chain wholesale CBDC within the design.

³⁵ Bank for International Settlements, [Press release: BIS, Bank of France and Swiss National Bank conclude successful cross-border wholesale CBDC experiment](#), (accessed 15 September 2022).

³⁶ Bank for International Settlements, [Project Mariana: CBDCs in automated market-makers](#), (accessed 1 February 2023).

³⁷ Monetary Authority of Singapore, [Project Ubin: Central Bank Digital Money using Distributed Ledger Technology](#), (accessed 21 December 2022).

Figure 7
End-to-end automation of debt issuance via auctions thanks to smart contracts



Source: authors' compilation

Once the auction is announced, an off-chain step, the process works as follows:

- Step 1. The issuer, or a technical third-party acting on its behalf, issues the debt instrument tokens and places these in the issuer wallet. This allows an automatic triggering of the settlement upon auction closure. The tokens are locked into smart contracts that allow for an automated execution of the instrument's corporate actions, notably coupon payments and redemption.
- Step 2. In parallel of step 1, investors interested in bidding at the auction place their bid in the form of a smart contract. They can modify (increase/decrease) or cancel their order up until a certain moment in time defined in advance by the issuer. The smart contracts are pre-funded, meaning that investors must commit their money at the moment of bidding. This reduces settlement risk, the risk that an investor might not provide the cash in time for the transaction settlement. This approach is similar to the one described by Schlegel & Mamageishvili (2021). It also allows the automatic triggering of the delivery versus payment process (step 5). However, pre-funding of smart contracts may add friction to the process, which could be mitigated by operating

intra-day or employing solutions taken from decentralised finance, such as short-term collateralisation provided by third parties.

Throughout the process, the bids of each bidder should only be visible to the bidder itself and to the issuer.

- Step 3. The allocation process can then proceed based on a set of rules defined by the issuer and not publicly available. In today's auction issuance process, this step is manual because it requires a decision by the issuer in accordance with its yield curve strategy and depending on market conditions at the time of allocation. In the system we define here, this step could remain manual or be automated based on a target maximum acceptable yield set by the issuer before the auction launch. This would support full end-to-end automation and could be adapted to both syndication-based issuance and to different auction methods chosen by issuers (Box 2).
- Step 4a. For successful bids, the 'auction' smart contract is triggered to launch the delivery versus payment settlement.
- Step 4b. For unsuccessful bids, the smart contract releases any CBDC tokens that were locked into the process back into the investor wallet.
- Step 5. The delivery versus payment process of successful bids involves a simultaneous exchange of tokens.
- Step 6a and 6b. While CBDC tokens are released from the investor's auction smart contract and transferred into the issuer's wallet (step 6a), the debt tokens are released from the smart contract set up by the issuer in step 1 for an amount equivalent to the investor's bid and transferred into the investor's wallet (step 6b). These steps are executed automatically and simultaneously in the process known as instant atomic settlement.

Such on-chain auctioning systems add value by eliminating the manual steps that exist between trade and settlement. The end-to-end integration we propose fosters automated settlement immediately after any allocation, condensing the process and thereby cutting costs and reducing risks.

Box 2. Different types of auctions in capital markets and beyond

Several auction methods exist for issuing debt on capital markets, offering variants of most common auction types: English auction, Dutch auction, first-price sealed-bid auctions, and second-price sealed-bid auctions.

Table 3

Auction characteristics for a selection of issuers from the sovereigns, supranationals, and agency sector

Issuer	Auction type	Frequency	Participants
Agence France Trésor	Auction with several prices and sealed prices	Weekly	15 primary dealers
Deutsche Bundesbank	Auction with several prices and non-competitive bids	Variable, depending on the securities. Approximately weekly.	32 primary dealers
US Treasury	Competitive and non-competitive bids. Same yield granted to all bidders.	More than daily: 445 public auctions in 2021	Individuals and various types of entities including trusts, estates, corporations, partnerships, etc.

Sources: Agence France Trésor, Deutsche Finanzagentur, U.S. Department of the Treasury

Auction prototypes exist on different distributed ledger technologies that overcome the implementation challenges of the different types of auctions (Sambare et al., 2022).

Traditional art auction house Christie’s recently announced its move to fully on-chain auctions on Ethereum for non-fungible token sales, using bids in the form of smart contracts locking ETH.³⁸

Pre-trade automation for syndication-based issuance and related limitations

The mechanism we present to automate auction-based debt issuance using smart contracts could be adapted to syndication.

- Step 1 would remain unchanged.
- Step 2 would be adapted to collect investor orders, thus building a book of orders in the form of smart contracts.
- Step 3, the allocation, is more challenging to fully automate as it would depend on the issuer’s investor relations strategy. In the case of a syndication, the issuer can view investors’ orders and decide which investor will be allocated the instrument. Some investors will be served in full, others may be only partially served or not served at all. This decision belongs to the issuer and can only be made once the book building phase is completed. However, if an issuer clearly defines its allocation rules across pre-determined investor categories, the allocation process could be coded into smart contracts as done for an auction.
- Steps 4, 5, 6a, and 6b would remain unchanged because, as mentioned above, post-trade steps are issuance method-neutral.

Setup proposal – a private permissioned blockchain

A programmable on-chain wholesale CBDC

We propose that any trade settlement mechanism using on-chain auction or book building should consider both a technical and risk requirement. The pre-funding of any bid smart contracts would be a pre-requisite for end-to-end automation (auction) or optimal automation (syndication). In capital markets, settling transactions with central bank money would offer the highest standard for both issuers and investors because it would eliminate the credit risk for both parties.

In the absence of on-chain central bank money, one alternative would be a form of wholesale stablecoin backed by central bank money, as developed for instance by Fnality International in their Narrative³⁹ or considered by the Bank of England “central banks could allow private sector players that have access to central bank reserves a greater ability to transact those reserves, allowing those firms to organise connectivity to other ledgers amongst themselves” (Cunliffe, 2022). However, this solution would inject a counterparty performance risk in the process, i.e. against the issuer of the so-called wholesale stablecoin.

³⁸ Christie’s, [Christie’s 3.0: Revolutionary Platform Established Christie’s as First Global Auction House to Host Fully On-Chain Sales](#), (accessed 5 October 2022).

³⁹ Fnality, [The Fnality Narrative](#), (accessed 1 June 2022)

A second alternative would be tokenised commercial bank money like the JPM Coin.⁴⁰ The downside of this solution would be the creation of both a counterparty risk and a credit risk against the commercial bank issuing the token.

A third and much discussed alternative to on-chain wholesale CBDC is a bridge solution between distributed ledger technology hosting digital assets and real time gross settlement system. The Eurosystem TARGET2 payment platform has proven itself a robust payment infrastructure, and several stakeholders have proposed linking distributed ledger technology to TARGET2 through trigger solutions as a substitute to maintaining central bank currencies on chain. TARGET2 would offer interfaces that may be contacted through smart contracts to trigger the execution of payments. While trigger solutions may be a readily implementable interim solution that would cover many of today's use-cases, there is a risk that implementation could introduce additional intermediaries, lack key functionalities (e.g. conditional time-locking of funds), higher transitional infrastructure costs,⁴¹ or slow responses to innovations. In the example of an on-chain debt issuance discussed in this paper, this bridge solution might potentially not support pre-funding of smart contracts. Some workarounds, such as using an intermediary to manage escrow accounts, would facilitate the process flow but implant complexity. Thus, more experimentation on such bridge solutions would deepen understanding of the exact potential and limitations.

At this stage, an on-chain wholesale CBDC appears the best solution for reducing risks and reaping the most benefits of smart contracts.

Intermediaries as node operators

Financial institutions could be authorised to adopt new roles as regulated actors to operate nodes to a private permissioned distributed ledger technology that take advantage of the benefits of smart contracts set forward in this paper. This approach offers many advantages.

First, markets participants would need know your customer approvals only once by one node operator, a significant efficiency gain for regulated actors in charge of know your customer checks.

Second, privacy could be enforced by limiting node operators' view to only the public addresses of market participant's wallets.

Third, it would be easier to protect a private network against cyber-attacks, either generic or specific to distributed ledger technology.

Fourth, establishing an exception management system could define a process to override record immutability in special cases.

Fifth, programmability would be ensured by choosing underlying technology from among the wide range of solutions available. Each node operator could deploy new applications on the network as smart contracts, for instance an auctioning or book-building system as described in this paper.

Finally, the central bank could play a significant role in this network by issuing wholesale central

⁴⁰ J.P. Morgan, [Digital solutions enabling instant transfer and clearing of multi-bank, multi-currency assets on a permissioned distributed ledger](#), (accessed 17 June 2022).

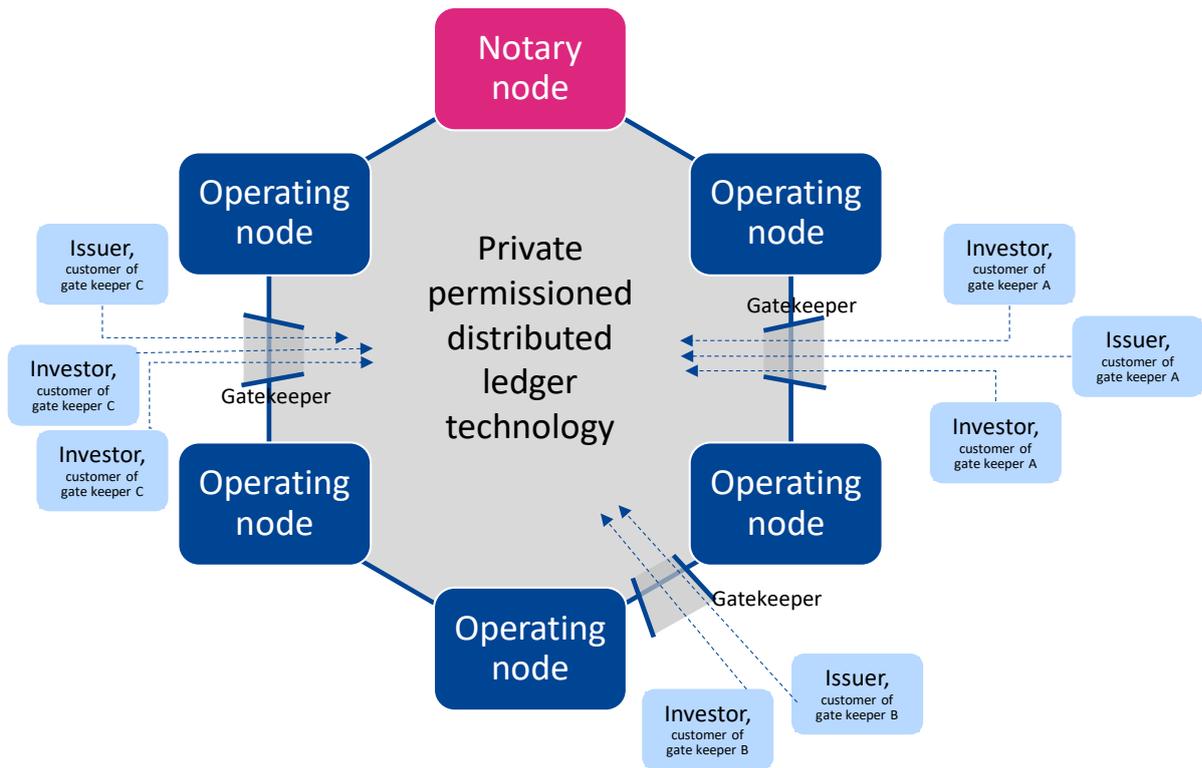
⁴¹ International Capital Market Association, [International Capital Market Association's response to the European Central Bank questionnaire on financial market stakeholders' potential interest in the Eurosystem providing EUR central bank money settlement of wholesale transactions in the payments, securities settlement and collateral management domains](#), p 2, (accessed 28 November 2022).

bank money on this private permissioned distributed ledger technology, and by operating a notary node as detailed in project Helvetia (Bank for International Settlements, Swiss National Bank, SIX Swiss Exchange, n.d.).

The governance specificities of such a private permissioned distributed ledger technology operated by a central bank and regulated entities would demand an in-detail study that stretches beyond the scope of this discussion paper. Among the key features the governance should ensure are: preventing nodes from censoring transactions and eliminating the risk of front running. Also, a common standard should be established for frequently used smart contracts, not at least to specify the terms of central bank money issued on the chain. In our view, a solution to one of the key problems in public blockchains would be central banks operating as a notary and regulated intermediaries operating node.

Figures 8, 9, and 10 below illustrate this approach.

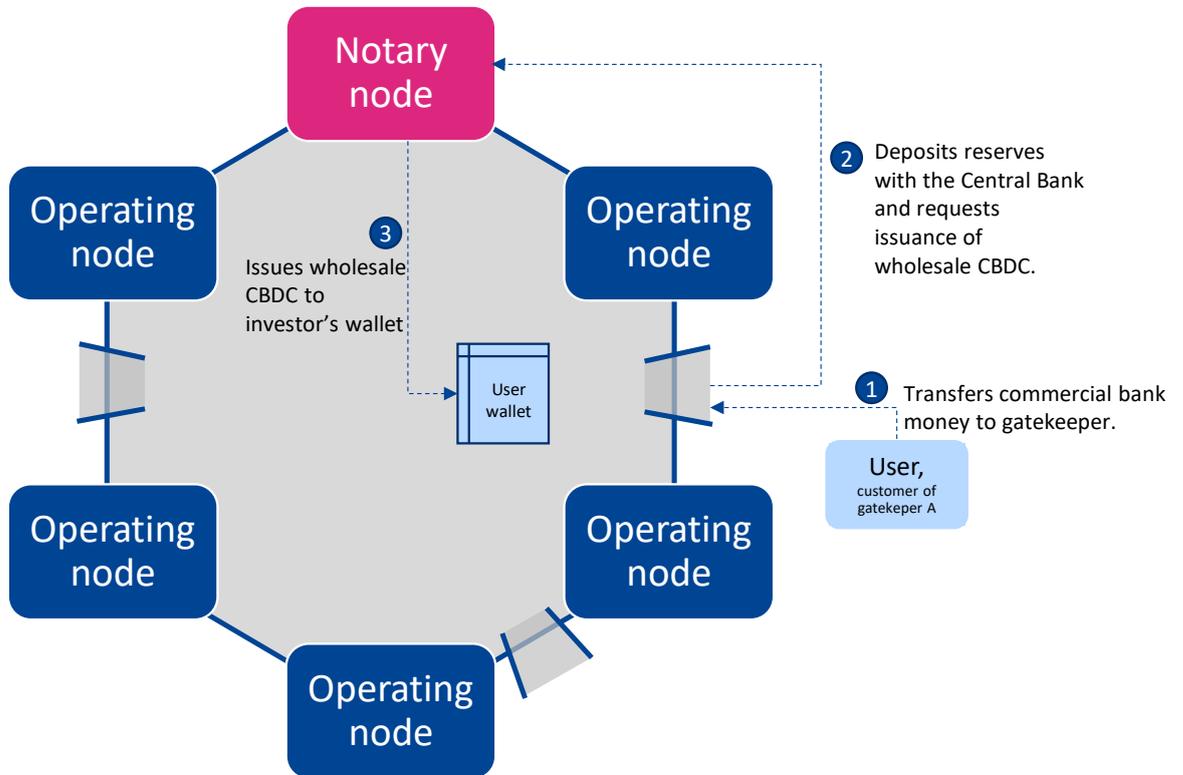
Figure 8
Private permitted distributed ledger technology operated by regulated actors



Notary node	Run by a central bank, provides uniqueness consensus and validates the transactions and maintains a record of the transactions.
Operating node	Run by regulated actors such as banks, traditional central clearing counterparties, etc. that provide a part of the distributed ledger technology and maintain a running record of transactions. The addition of a node is subject to notary nodes' authorisation.
	Gate keepers are regulated actors and grant users access to the distributed ledger technology and its decentralised applications, performing know your customer as a pre-requisite.
User	Users are market participants such as issuers, investors, banks, etc. They are white-listed by at least one gatekeeper.

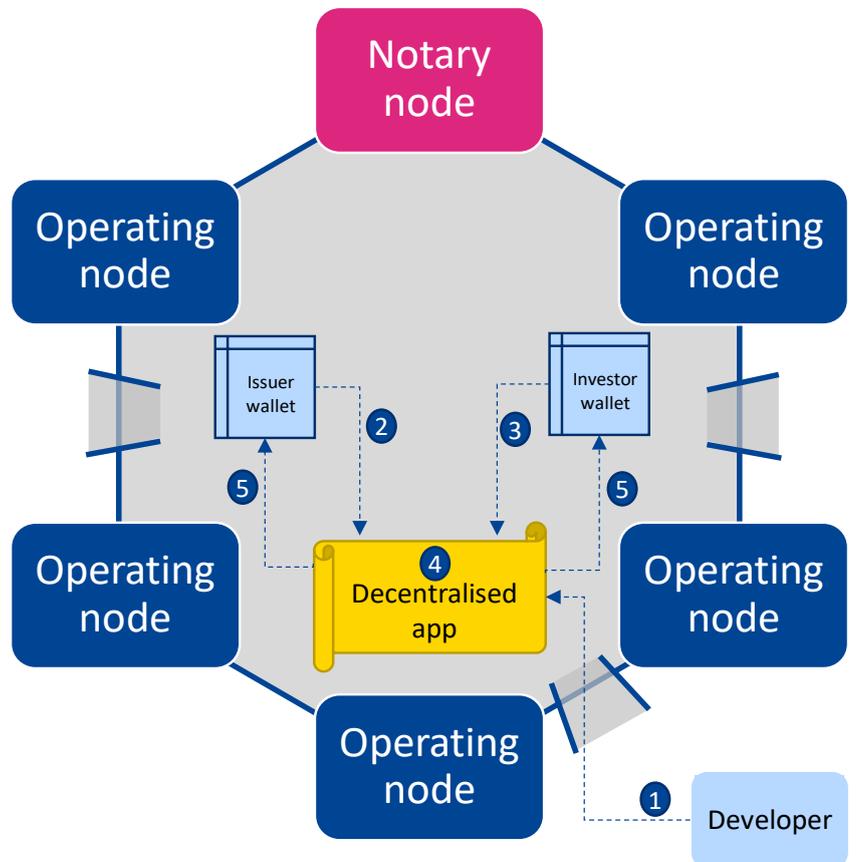
Source: authors' compilation

Figure 9
Wholesale CBDC issuance process in the proposed private permitted distributed ledger technology network



Source: authors' compilation

Figure 10
Wholesale CBDC issuance process in the proposed private permitted distributed ledger technology network



Developer	<p>Can be a bank, issuer, or central bank that develops and deploys a decentralised app for a specific purpose, e.g. auction issuance or book building.</p> <ol style="list-style-type: none"> 1 Developer develops and deploys an issuance app. 2 Issuer issues bond or bill tokens in the form of smart contracts linked to the decentralised app placed in their own wallet. 3 Investor (which can also be a bank), locks in wholesale CBDC by placing an auction or order. 4 Allocation via decentralised app. 5 Delivery versus payment process where issuer receives wholesale CBDC and investor receives bond or bill tokens.
------------------	---

Source: authors' compilation

Implications for primary and secondary markets

Market participants need to be whitelisted by a gatekeeper to access the network. This will allow for the application of anti-money laundering and combatting financing terrorism regulations by

trusted, regulated actors. Once whitelisted, market participants will have direct access to their wallet, meaning they could technically be autonomous in posting orders or auctions for primary market issuances, should regulations authorise it and issuers take this option. However, we believe that the role of intermediaries in the primary market reaches well beyond the role of technical operators and will remain unchallenged because of the added value they provide. Banks advise issuers on numerous elements, including size, maturity, and pricing guidance. They play a key role in supporting long-term investor relations of issuers and contact investors when a deal is announced, so generating appropriate market interest. The digitalisation that would accompany the system we propose may require intermediaries to adjust their business models but would not disrupt them.

On the secondary market, the direct access of market participants to their wallet could lead them to directly transfer a security in exchange for wholesale CBDC. It is worth consideration to build marketplaces that help market participants find trade counterparties leveraged on their technical ability to transfer their tokens. Such marketplaces could potentially transform current over-the-counter markets, drastically changing the way markets function. But, these changes would only materialise over the longer term, so the market-making role of banks will remain strong for the time being.

4. Conclusion

In this paper, we have explored the potential of next-generation automation tools, i.e. distributed ledger technology, smart contracts and oracles, the issuance of wholesale CBDC, and how they could increase the efficiency of debt issuance and trading.

The processing of securities and cash transfer within an integrated distributed ledger technology-based infrastructure is expected to accelerate execution thanks to programmability, and offer additional transparency while respecting market participants' privacy expectations, while also contributing to financial stability. Currently available technology offers scalable, interoperable solutions.

This new approach would help reduce existing risks within the legacy financial market infrastructures, but would introduce new risks. These could be mitigated by applying the right design choices, particularly regarding the application of anti-money laundering and combatting financial terrorism regulations and the prevention of cyber-security risks.

All these factors together should lead to cost savings. We have demonstrated that for sovereign debt issuances not only post-trade activity could be designed to benefit from this.

The new system should offer programmable features and reduce risks. On-chain wholesale CBDC with programmability features do seem to be the missing piece that could further the emergence and use of tokenised capital markets at scale in this market segment.

A private permissioned blockchain with nodes operated by regulated entities, with the central bank operating a notary node, would appear to be an architecture for developing digital assets in capital markets within a safe and controlled environment. Experience gained from recent or upcoming debt issuances on private blockchains by the European Investment Bank and others could be leveraged to further this proposition.

We see several challenges and room for research based on this proposal.

First, a detailed technical analysis would be needed to ensure the best choice of technology to meet the high-level requirements set out in this discussion paper.

Second, this paper does not analyse the aspect of competition and anti-trust regulation, and it should be determined if competitors would be ready to operate nodes in a common distributed infrastructure.

Third, governance rules should be elaborated to establish the decision and financing arrangements needed for progressing towards a permissioned private network.

The paper does not cover the implications of our proposals for central banks and regulators, in particular governance considerations and the need to control central bank money on distributed ledger technology. These are fundamental factors that any central bank would wish to consider in depth before issuance of a wholesale CBDC on distributed ledger technology.

Finally, experiments around on-chain, end-to-end debt issuance automation would allow market participants to confirm the gains we foresee in this paper, explore further bridge solutions as a potential intermediary setup, and share experiences with the community. This would contribute to employing digitalisation as a means to enhance capital market efficiency.

References

- Agence France Trésor. (n.d.). *Issuance techniques* | Agence France Trésor. Retrieved June 08, 2022, from Agence France Trésor: <https://www.aft.gouv.fr/en/issuance-techniques>
- Agence France Trésor. (n.d.). *Key figures*. Retrieved June 20, 2022, from Agence France Trésor: <https://www.aft.gouv.fr/en/principaux-chiffres-oat>
- Aramonte, S., Huang, W., & Schrimpf, A. (2021, December). DeFi risks and the decentralisation illusion. *BIS Quarterly Review*, pp. 21-36.
- Atlantic Council. (n.d.). *Central Bank Digital Currency Tracker*. Retrieved November 28, 2022, from Atlantic Council: <https://www.atlanticcouncil.org/cbdctracker/>
- Auer, R., Cornelli, G., & Frost, J. (2020, April 24). *Rise of the central bank digital currencies: drivers, approaches and technologies*. Retrieved January 15, 2023, from Bank for International Settlements: <https://www.bis.org/publ/work880.htm>
- Bank for International Settlements. (2022, October). *Project mBridge: connecting economies through CBDC*. Retrieved November 14, 2022, from Bank for International Settlements: <https://www.bis.org/publ/othp59.htm>
- Bank for International Settlements. (2021, December 8). *Bank for International Settlements, Bank of France and Swiss National Bank conclude successful cross-border wholesale CBDC experiment*. Retrieved September 15, 2022, from Bank for International Settlements: <https://www.bis.org/press/p211208.htm>
- Bank for International Settlements, Swiss National Bank, SIX Swiss Exchange. (2022). *Project Helvetia Phase II - Settling tokenised assets in wholesale CBDC*. Retrieved June 14, 2022, from Bank for International Settlements: <https://www.bis.org/publ/othp45.pdf>
- Bank for International Settlements. (n.d.). *Project Mariana: CBDCs in automated market-makers*. Retrieved February 1, 2023, from Bank for International Settlements: <https://www.bis.org/about/bisih/topics/cbdc/mariana.htm>
- Bank for International Settlements, Swiss National Bank, SIX Swiss Exchange. (n.d.). *Project Helvetia: A multi-phase investigation on the settlement of tokenised assets in central bank money*. Retrieved June 14, 2022, from Bank for International Settlements: <https://www.bis.org/about/bisih/topics/cbdc/helvetia.htm>
- Banque de France. (2021). *Experimenting settlement of French government bonds in Central Bank Digital Currency with blockchain technology*. Retrieved June 14, 2022, from Euroclear: <https://www.euroclear.com/content/dam/euroclear/news%20&%20insights/Format/Whitepapers-Reports/settlement-french-government%20bonds-in-cbdc-with-blockchain.pdf>
- Banque de France, Monetary Authority of Singapore. (2021). *Liquidity Management in a Multi-Currency Corridor Network*. Retrieved October 27, 2022, from Banque de France: https://www.banque-france.fr/sites/default/files/media/2021/11/15/bdf-mas-onyx_liquidity_management_in_a_multi-currency_corridor_network_vfinal_-_12112021_0.pdf
- Bech, M. et al. (2022, June 21). *Using CBDCs across borders: lessons from practical experiments*. Bank for International Settlements, Innovation Hub. Retrieved October 18, 2022, from Bank for International Settlements: <https://www.bis.org/publ/othp51.pdf>
- Bech, M. et al. (2020). *On the future of securities settlement*. Bank for International Settlements. Retrieved September 27, 2022, from Bank for International Settlements:

- https://www.bis.org/publ/qtrpdf/r_qt2003i.htm
- Blau, M. (2022, June 24). *A Tool for Detecting Metamorphic Smart Contracts*. Retrieved July 13, 2022, from a16z crypto: <https://a16zcrypto.com/metamorphic-smart-contract-detector-tool/>
- Bossu, W., Itatani, M., Margulis, C., Rossi, A., Weenink, H., & Yoshinaga, A. (2020). Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations. *IMF Working Paper WP/20/254*. Retrieved October 18, 2022, from International Monetary Fund: <https://www.imf.org/en/Publications/WP/Issues/2020/11/20/Legal-Aspects-of-Central-Bank-Digital-Currency-Central-Bank-and-Monetary-Law-Considerations-49827>
- Brunnemeier, M. K., & Niepelt, D. (2019). On the equivalence of private and public money. *Journal of Monetary Economics* 106, 27-41.
- Christie's. (2022, September 27). *Christie's 3.0: Revolutionary Platform Established Christie's as First Global Auction House to Host Fully On-Chain Sales*. Retrieved October 5, 2022, from Christie's: <https://www.christies.com/about-us/press-archive/details?PressReleaseID=10648&lid=1>
- Cunliffe, S. J. (2022, September 28). *Innovation in post trade services - opportunities, risks and the role for the public sector – speech by Sir Jon Cunliffe*. Retrieved October 2, 2022, from Bank of England: <https://www.bankofengland.co.uk/speech/2022/september/jon-cunliffe-keynote-speech-at-the-afme-operations-post-trade-technology-innovation-conference>
- Deutsche Bundesbank. (2021, March 24). *DLT-based securities settlement in central bank money successfully tested*. Retrieved June 8, 2022, from Deutsche Bundesbank: <https://www.bundesbank.de/en/press/press-releases/dlt-based-securities-settlement-in-central-bank-money-successfully-tested-861444>
- Deutsche Bundesbank. (n.d.). *Auction procedure | Deutsche Bundesbank*. Retrieved June 08, 2022, from Deutsche Bundesbank: <https://www.bundesbank.de/en/service/federal-securities/auction-procedure/auction-procedure-619048>
- Deutsche Finanzagentur. (n.d.). *Auction Results*. Retrieved June 20, 2022, from Deutsche Finanzagentur: <https://www.deutsche-finanzagentur.de/en/institutional-investors/primary-market/auction-results/>
- European Central Bank. (2023). *Digital Euro*. Retrieved November 14, 2022, from European Central Bank: https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html
- European Central Bank Debt Issuance Market Contact Group. (2021). *Advisory report on debt issuance and distribution in the European Union*. European Central Bank. Retrieved June 14, 2022, from European Central Bank: <https://www.ecb.europa.eu/pub/pdf/other/ecb.advisoryreportdebtissuancedistributionEU202112~3da04b818a.en.pdf>
- European Investment Bank. (2022, November 29). *European Investment Bank innovates further with Project Venus, the first euro-denominated digital bond on a private blockchain*. Retrieved November 29, 2022, from European Investment Bank: <https://www.eib.org/en/press/all/2022-448-eib-innovates-further-with-project-venus-the-first-euro-denominated-digital-bond-on-a-private-blockchain>
- European Investment Bank. (2021, April 28). *European Investment Bank issues its first ever digital bond on a public blockchain*. Retrieved June 8, 2022, from European Investment Bank: <https://www.eib.org/en/press/all/2021-141-european-investment-bank-eib-issues-its-first-ever-digital-bond-on-a-public-blockchain>

- European Securities and Markets Authority. (2022, October). *Crypto-assets and their risks for financial stability. ESMA Report on Trends, Risks and Vulnerabilities Risk Analysis*. Retrieved November, 7, 2022, from European Securities and Markets Authority: https://www.esma.europa.eu/sites/default/files/library/esma50-165-2229_trv_2-22.pdf
- Financial Stability Board. (n.d.). *Crypto-assets and Global 'Stablecoins'*. Retrieved November 14, 2022, from Financial Stability Board: <https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/crypto-assets-and-global-stablecoins/>
- Fnlity International*. (n.d.). Retrieved June 1, 2022, from Fnlity: <https://www.fnality.org/home>
- Generali carries out first market transaction based on blockchain infrastructure*. (2022, April 13). Retrieved June 8, 2022, from Hedge Week: <https://www.hedgeweek.com/2022/04/13/313762/generali-carries-out-first-market-transaction-based-blockchain-infrastructure>
- International Capital Market Association. (n.d.). *ICMA's response to the ECB questionnaire on financial market stakeholders' potential interest in the Eurosystem providing EUR central bank money settlement of wholesale transactions in the payments, securities settlement and collateral management domains*. Retrieved November 28, 2022, from International Capital Market Association: <https://www.icmagroup.org/News/news-in-brief/icmas-response-to-the-ecb-questionnaire-on-financial-market-stakeholders-potential-interest-in-the-eurosystem-providing-eur-central-bank-money-settlement-of-wholesale-transactions-in-the-payments-securities-settlement-and-collateral-management-domains-usi/>
- J.P. Morgan. (n.d.). *Coin Systems | Onyx by J.P. Morgan*. Retrieved June 17, 2022, from J.P. Morgan: <https://www.jpmorgan.com/onyx/coin-system.htm>
- Japan Exchange Group. (2022, February 14). *JPX Begins Research on "Digitally Tracked Green Bonds" Utilizing Security Tokens*. Retrieved October 19, 2022, from Japan Exchange Group: <https://www.jpx.co.jp/english/corporate/news/news-releases/0010/20220214-01.html>
- Kiff, J. et al. (2020, June 26). *A Survey of Research on Retail Central Bank Digital Currency*. Retrieved November 12, 2022, from International Monetary Fund: <https://www.imf.org/en/Publications/WP/Issues/2020/06/26/A-Survey-of-Research-on-Retail-Central-Bank-Digital-Currency-49517>
- Kosse, A., & Mattei, I. (2022). *Bank for International Settlements Papers No 125 Gaining momentum - Results of the 2021 BIS survey on central bank digital currencies*. Bank for International Settlements. Retrieved September 17, 2022, from Bank for International Settlements: <https://www.bis.org/publ/bppdf/bispap125.pdf>
- Luxembourg Capital Markets Association. (2022). *Proof of Concept - Structuring a DLT debt issuance in Luxembourg*. Retrieved June 15, 2022, from Luxembourg Capital Markets Association: https://www.luxcma.com/images/events/2022/20220329_DLT/20220330_LuxCMA - DLT proof of concept - final.pdf
- Monetary Authority of Singapore. (2022, October 31). *MAS Report on Potential Uses of a Purpose-Bound Digital Singapore Dollar*. Retrieved January 18, 2023, from Monetary Authority of Singapore: <https://www.mas.gov.sg/news/media-releases/2022/mas-report-on-potential-uses-of-a-purpose-bound-digital-singapore-dollar>
- Monetary Authority of Singapore. (2022, October 31). *Project Orchid*. Retrieved December 5, 2022, from Monetary Authority of Singapore: <https://www.mas.gov.sg/schemes-and-initiatives/project-orchid>

- Monetary Authority of Singapore. (n.d.). *Project Ubin: Central Bank Digital Money using Distributed Ledger Technology*. Retrieved December 21, 2022, from Monetary Authority of Singapore: <https://www.mas.gov.sg/schemes-and-initiatives/Project-Ubin>
- Monetary Authority of Singapore. (2022, August 29). "Yes to Digital Asset Innovation, No to Cryptocurrency Speculation" - Opening Address by Mr Ravi Menon, Managing Director, Monetary Authority of Singapore, at Green Shoots Seminar on 29 August 2022. Retrieved November 28, 2022, from Monetary Authority of Singapore: <https://www.mas.gov.sg/news/speeches/2022/yes-to-digital-asset-innovation-no-to-cryptocurrency-speculation>
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved June 1, 2022, from Bitcoin: <https://bitcoin.org/bitcoin.pdf>
- Panetta, F. (2022, September 26). *Demystifying wholesale central bank digital currency*. Retrieved October 18, 2022, from European Central Bank: <https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220926~5f9b85685a.en.html>
- Sambare, S. et al. (2022). A Survey of E-bidding System using Blockchain. *Fourth International Conference on Smart Systems and Inventive Technology* (pp. 250-255). IEEE. Retrieved June 1, 2022, from Institute of Electrical and Electronics Engineer: <https://ieeexplore.ieee.org/document/9716443>
- Schlegel, J., & Mamagishvili, A. (2021). On-Chain Auctions with Deposits. Retrieved June 1, 2022, from Cornell University: <https://arxiv.org/abs/2103.16681>
- Sharma, G. et al. (2021). Anonymous Fair Auction on Blockchain. *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)* (pp. 1-5). IEEE. Retrieved June 1, 2022, from Institute of Electrical and Electronics Engineer: <https://ieeexplore.ieee.org/document/9432664>
- Tech Monitor. (2022, March 17). *The ten biggest crypto hacks of all time*. Retrieved June 16, 2022, from Tech Monitor: <https://techmonitor.ai/technology/cybersecurity/biggest-cryptocurrency-hacks-of-all-time>
- The Oasis Protocol Foundation*. (n.d.). Retrieved June 1, 2022, from Oasis Protocol: <https://oasisprotocol.org/>
- The Security Token Standard*. (n.d.). Retrieved October 3, 2022, from Security Token Standard: <https://thesecuritytokenstandard.org/>
- The World Bank. (2018, August 23). *World Bank Prices First Global Blockchain Bond, Raising A\$110 Million*. Retrieved June 08, 2022, from The World Bank: <https://www.worldbank.org/en/news/press-release/2018/08/23/world-bank-prices-first-global-blockchain-bond-raising-a110-million>
- U.S. Department of the Treasury. (n.d.). *Auctions*. Retrieved July 13, 2022, from Treasury Direct: https://www.treasurydirect.gov/indiv/products/prod_auctions_glance.htm
- U.S. Department of the Treasury. (n.d.). *Investor Class Auction Allotments*. Retrieved June 20, 2022, from US Department of the Treasury: <https://home.treasury.gov/data/investor-class-auction-allotments>
- Yong Rhee, C. (n.d.). *Chang Yong Rhee: Central bank digital currency - what we have learned from a recent hands-on experiment*. Retrieved November 28, 2022, from Bank for International Settlements: <https://www.bis.org/review/r221028b.htm>

Acronyms & Glossary

Anti-money laundering		The laws, regulations, and procedures aimed at uncovering efforts to disguise illicit funds as legitimate income. Money laundering seeks to conceal crimes ranging from small-time tax evasion and drug trafficking to public corruption and the financing of groups designated as terrorist organisations.
Atomic settlement		Whenever two financial market participants agree to trade an asset, the act of transferring the ownership of the asset from the seller to the buyer, and the associated payment, is called the trade settlement. In traditional financial markets, trading and settlement are separate processes. Atomic settlement refers to simultaneously performing both processes.
Bank for International Settlements	BIS	International financial institution owned by central banks that fosters international monetary and financial cooperation and serves as a bank for central banks.
Banque de France	BdF	The Bank of France, headquartered in Paris, is the central bank of France.
Bitcoin		A decentralised digital currency that can be transferred on a peer-to-peer bitcoin network. Bitcoin transactions are verified by network nodes using cryptography and recorded in a public distributed ledger called a blockchain.
Blockchain		A type of distributed ledger technology that consists of a growing list of records, called blocks, that are securely linked by cryptography.
Bridge solution		Linking tools that bridge the universe of central bank digital currency and legacy payments networks.
Central bank digital currency	CBDC	Digital tokens, similar to cryptocurrency, issued by a central bank, which are pegged to the value of that country's fiat currency.
Central clearing counterparty	CCP	Also referred to as a central counterparty, a financial institution that takes on counterparty credit risk between parties to a transaction and provides clearing and settlement services for trades in foreign exchange, securities, options, and derivative contracts.
Central securities depository	CSD	Responsible for the registration and safekeeping of securities as well as the settlement of securities in exchange for cash through their securities settlement system. They track how many securities have been issued, by whom these securities have been issued, and who is their owner.
Collateralisation		The use of a valuable asset as collateral to secure a debt instrument.
Combatting the financing of terrorism		Laws, regulations, and other practices intended to restrict access to funding and financial services for those the government designates as terrorists. By tracking down the source of funds that support terrorist activities, law enforcement may be able to prevent such activities.

Cryptoasset		A digital or virtual asset secured by cryptography, which makes it nearly impossible to counterfeit or double-spend.
Cryptocurrency		See Cryptoasset.
Decentralised apps	dApp	Digital applications or programs that exist and run on a blockchain or a peer-to-peer network of computers instead of a single computer. Decentralised apps are outside the purview and control of a single authority. Often built on the Ethereum platform, they can be developed for a variety of purposes including gaming, finance, and social media.
Decentralised finance	DeFi	An emerging financial technology based on secure distributed ledgers such as those used by cryptocurrencies.
Delivery versus payment	DvP	This transaction stipulates that securities be delivered to a specified recipient only after a payment is made. It is a settlement method that ensures the transfer of securities only when payments are executed.
Digital euro		An electronic means of payment that anyone could use across the euro area. It would be secure and user-friendly, like cash today. As central bank money issued by the European Central Bank, it would be different from private money, but a card or a phone apps could be used to pay with it.
Distributed ledger technology	DLT	The technological infrastructure and protocols that support simultaneous access, validation, and record updating in an immutable manner across a network extending across multiple entities or locations.
Environmental, social, and governance	ESG	A set of standards for a company’s behaviour used by socially conscious investors to screen potential investments. For example, environmental criteria consider how a company safeguards the environment, including corporate policies addressing climate change. Social criteria examine how it manages relationships with employees, suppliers, customers, and the communities within which it operates. Governance deals with a company’s leadership, executive pay, audits, internal controls, and shareholder rights.
ERC Security Token Standard	ERC1400	A proposed standard for security tokens – incorporating differentiated ownership, error signaling, document references, gatekeeper (operator) access control, and issuance/redemption semantics.
ERC Simple Restricted Token Standard	ERC1404	The ERC-1404 standard allows shareholders to interoperate with the Ethereum ecosystem with added functionality that allows the fund to enforce transfer restrictions within the share's smart-contract.
ERC Base Security Token	ERC1462	An extension to ERC-20 standard token that provides compliance with securities regulations and legal enforceability.
Ether/Ethereum	ETH	Ethereum is a blockchain-based platform best known for its cryptocurrency, ether. It supports smart contracts, an essential tool behind decentralised applications. Many decentralised finance and other

		applications use smart contracts together with blockchain technology.
European Central Bank	ECB	The prime component of the Eurosystem and the European System of Central Banks. One of seven European Union institutions.
European Securities and Markets Authority	ESMA	An independent European Union authority that contributes to safeguarding the stability of the European Union's financial system by enhancing the protection of investors and promoting stable and orderly financial markets.
Eurosystem		The monetary authority of the euro area, the collective of European Union Member States that have adopted the euro as their sole official currency. The European Central Bank has, under Article 16 of its Statute, the exclusive right to authorise the issue of euro banknotes.
Exception management		Exception management is the process of responding to unwanted or unexpected events when a computer program runs.
Fat finger risk		A fat finger error is a human error caused by pressing the wrong key when using a computer to input data.
Financial Stability Board	FSB	An international body that monitors and makes recommendations about the global financial system. It was established after the G20 London summit in April 2009 as a successor to the Financial Stability Forum.
FTX cryptocurrency exchange	FTX	A Bahamas-based cryptocurrency exchange. The exchange was founded in 2019 and, at its peak in 2021, had over one million users and was the third-largest crypto exchange by volume. Since 11 November 2022, FTX has been in Chapter 11 bankruptcy proceedings in the US court system following a liquidity crisis.
Gatekeepers		Part of a technical and organisational approach to digital euro service provision. The main difference between a direct and intermediated model is the role of the private sector. In a direct model, supervised intermediaries are only gatekeepers, in an intermediated model they would play a more prominent role, including that of settlement agents. Gatekeepers would authenticate end users and deal with activities such as know your customer, anti-money laundering, and combatting financial terrorism requirements; they may also provide the technical connectivity between users and the Eurosystem infrastructure. The basic functions of gatekeepers are therefore similar to those of commercial banks in the primary provision of cash to the economy.
Hashed Timelock Contract	HTLC	A hashed timelock contract is a type of smart contract used in blockchain applications. It reduces counterparty risk by creating a time-based escrow that requires a cryptographic passphrase for unlocking. In practical terms, this means that the person receiving the funds in a transaction has to perform two actions to access the funds: enter the correct passphrase and claim payment within a specific timeframe. If they enter an incorrect passphrase or do not claim the funds within the timeframe, they lose access to the payment.

Immutability		Decentralised blockchains are immutable, which means that the data entered is irreversible. For Bitcoin, this means that transactions are permanently recorded and viewable to anyone.
International Capital Market Association	ICMA	Association that represents financial institutions active in the international capital market worldwide.
International Monetary Fund	IMF	International organisation providing financial assistance and advice to member countries. The IMF came into formal existence in 1944 following the Bretton Woods Conference held a year earlier. Along with its sister organisation, the World Bank, it was created to prevent economic crises such as the Great Depression. It is a specialised agency of the United Nations and is run by its 190 member countries.
Know your customer		Standards used in the investment and financial services industry to verify customers and know their risk and financial profiles.
Locking/unlocking tokens		See hashed timelock contracts.
Metamorphic smart contracts		Smart contracts developed by malicious actors that allow them to change the code inside a smart contract after it has been deployed.
Mining		Refers to solving a specific cryptographic puzzle. See proof of work.
Monetary Authority of Singapore		The central bank and financial regulatory authority of Singapore. It administers statutes pertaining to money, banking, insurance, securities and the financial sector in general, as well as currency issuance.
Non-fungible token	NFT	A unique digital identifier that cannot be copied, substituted, or subdivided and is recorded in a blockchain and used to certify authenticity and ownership.
Notary node		A well-known and trusted node inside a network that provides uniqueness and consensus.
On-chain transactions		Cryptocurrency transactions that occur on the blockchain and remain dependent on the state of the blockchain for their validity. On-chain transactions are considered valid only when the blockchain has been updated to reflect the transactions on the public ledger. On-chain transactions offer security and transparency since they cannot be altered once verified and recorded on the network.
On-ledger transactions		See on-chain transactions.
Oracle		Blockchain oracles are entities that connect blockchains to external systems. This could for example be an impartial financial data provider. Two smart-contract parties could then for instance agree on a future payment based on the development of the exchange rate.
Over-the-counter	OTC	The process of trading securities via a broker-dealer network as opposed to on a centralised exchange like the New York Stock Exchange.
Peer-to-peer	P2P	A distributed application architecture that partitions tasks or workloads between peers. Peers are equally

	privileged, equipotent participants in the network and are said to form a peer-to-peer network of nodes.
Penetration test	Also known as a pen test or ethical hacking, this is an authorised simulated cyberattack on a computer system, performed to evaluate the security of the system; this is not to be confused with a vulnerability assessment.
Pre-funding	Future obligations are guaranteed by risk-free securities in an escrow account.
Primary market	A source of new securities. Often on an exchange where companies, governments, and other groups go to obtain financing through debt-based or equity-based securities. Primary markets are facilitated by underwriting groups consisting of investment banks that set a beginning price range for a given security and oversee its sale to investors. Once the initial sale is complete, further trading is conducted on the secondary market, where most daily trading occurs.
Private permissioned blockchain	Public blockchains allow anyone access, whereas private blockchains are only available to selected users. Permissioned blockchains are a hybrid of public and private blockchains; anyone can access them as long as they have permission from the administrators to do so.
Programmability	See smart contract.
Proof of work	A system that requires a not-insignificant but feasible amount of effort to deter frivolous or malicious uses of computing power. The concept was subsequently adapted to securing digital money by Hal Finney in 2004 through the idea of reusable proof of work using the SHA-256 hashing algorithm. Following its introduction in 2009, Bitcoin became the first widely adopted application of Finney's PoW idea. It also forms the basis of many other cryptocurrencies, allowing for secure, decentralised consensus.
Public blockchain	See Private permissioned blockchain.
Purpose-bound-money	A form of digital money that enables senders to specify conditions, such as validity period and types of shops, when making transfers.
Real-time gross settlement	Specialist funds transfer systems where the transfer of money or securities takes place from one bank to any other bank on a real-time and on a gross basis.
Secondary market	A market where investors buy and sell securities they already own. This is what most people typically think of as the stock market, though stocks are also sold on the primary market when first issued. National exchanges, such as the New York Stock Exchange and the NASDAQ, are secondary markets.
Securities settlement system	An entity that enables securities to be transferred and settled by book entry according to a set of predetermined multilateral rules. Such systems allow transfers of securities either free of payment or against payment.
Smart contract	A self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements

		contained therein exist across a distributed, decentralised blockchain network. The code controls the execution, and transactions are trackable and irreversible.
Sovereigns, Supranational, and Agencies	SSA	This sector includes governments, government-owned or guaranteed corporates, central banks, development banks, regions, provinces and local authorities. The acronym is typically used by investment banks to define the remit of an operation or desk focused on servicing a specific market. The term is used in contrast with financial institutions group and corporate markets.
Stablecoin		Cryptocurrencies where the price is designed to be pegged to a reference asset. The reference asset may be fiat money, exchange-traded commodities, or a cryptocurrency.
Supervised entities		The European Central Bank maintains a list of all significant banks under its direct supervision and less significant banks under its indirect supervision. The list of supervised entities is updated regularly and reflects all decisions on bank significance that entered into force before the relevant cut-off date. In the Single Supervisory Mechanism Framework Regulation, the types of supervised banks are referred to as: 1) credit institutions established in participating Member States, 2) financial holding companies established in participating Member States, 3) mixed financial holding companies established in participating Member States, 4) branches established in participating Member States by credit institutions established in non-participating Member States.
Syndicated government bond		In syndicated bond offerings, a government debt office will appoint a panel of underwriters, banks and broker-dealers. Syndicated transactions are so defined because the banks form a debt syndicate, a group of underwriters, usually investment banks, who will manage the debt offering.
Synthetic CBDC		An organisational choice for providing CBDC services. Contrary to a pure CBDC in which the central bank creates tokens or offers accounts to the public. Synthetic CBDC is an indirect, two-tier form, whereby the liability is issued by a commercial bank but is fully backed by central bank liabilities. A hybrid form would consist of direct claims on the central bank, with intermediaries handling payments.
TARGET2		TARGET2 is the real-time gross settlement system for the euro area and is available to non-euro area countries. TARGET2 is based on an integrated central technical infrastructure, called the Single Shared Platform.
TerraUSD	UST	Terra is a blockchain protocol and payment platform for algorithmic stablecoins. The project was created in 2018. It is most known for its Terra stablecoin and the associated Luna reserve asset cryptocurrency.
Token		Tokens connect smart contracts with the real world. A token is a uniquely identifiable digital representation of an asset defined in a smart contract. Today any interested software developer can create tokens. Stablecoins are such tokens, and they derive their value

		<p>from a peg to a real-world currency such as the US dollar or a commodity. Supervised financial companies offer reserve-services to guarantee the token price stability, with the inherent credit-risk on the company committed under the service. Once digitalised, tokens can be transferred and traded, or used in more complex applications such as option-contracts.</p>
Trusted execution environments	TEE	<p>A secure area of a main computer processor that guarantees the confidentiality and integrity of the code and data loaded inside. Code within the trusted execution environment cannot be replaced or modified by unauthorised entities, which may also be the computer owner itself. This is done by implementing unique, immutable, and confidential architectural security such as Intel Software Guard Extensions (Intel SGX) which offers hardware-based memory encryption that isolates specific application code and data in the memory.</p>
Wallet		<p>A cryptocurrency wallet is a device, physical medium, program, or service that stores the public and/or private keys for cryptocurrency transactions. In addition to this basic function of storing keys, a cryptocurrency wallet often also offers the functionality of encrypting and/or signing information.</p>
Wholesale CBDC	w-CBDC	<p>The settlement of interbank transfers and related wholesale transactions in central bank reserves. Wholesale CBDC, involves a narrow set of stakeholders that already use digital central bank settlement infrastructures today, such as banks or central securities depositories. In the future, new stakeholders could take part in the wholesale settlement chain using new technologies such as distributed ledger technology. Retail CBDC in contrast involves a wide range of stakeholders: legislators, the retail payments ecosystem and the broader public.</p>
Yield curve strategy		<p>A yield curve is a line that plots yields (interest rates) of bonds having equal credit quality but differing maturity dates. The slope of the yield curve gives an idea of future interest rate changes and economic activity. Yield curve strategies are used by investors who hope to achieve capital gains by anticipating differences in interest rates for different terms of bonds.</p>

Sources: Bank for International Settlements, Ethereum Improvement Proposals, European Central Bank, International Monetary Fund, Investopedia, Monetary Authority of Singapore, New York Fed, The Security, Tokensoft, Token Standard, Wikipedia