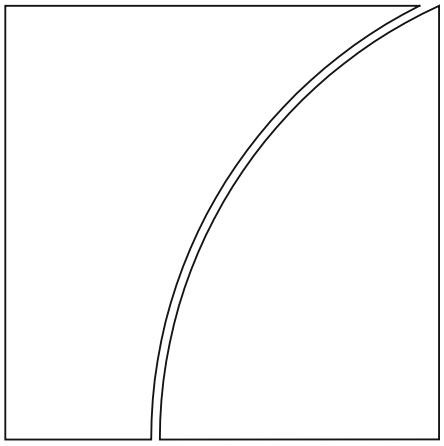
Committee on Payments and Market Infrastructures



Distributed ledger technology in payment, clearing and settlement

An analytical framework

February 2017

BANK FOR INTERNATIONAL SETTLEMENTS

This publication is available on the BIS website (www.bis.org).

ISBN 978-92-9259-031-4 (online)

Foreword

Distributed ledger (or blockchain) technology has captured the attention of many in the financial sector, including those active in payment, clearing and settlement, with its promise of greater efficiency and higher resiliency. Over the past months, there have been numerous public announcements and news articles about a new project, partnership, a round of investment funding or a white paper on distributed ledger technology (DLT). Central banks have also announced DLT-related research or initiatives in support of private sector development of this technology.

This report provides an analytical framework for central banks and other authorities to review and analyse the use of this technology for payment, clearing and settlement. Market participants and other interested parties may also find this report useful. The main aim of the framework is to help understand the uses of DLT and, in doing so, identify both the opportunities and challenges associated with this technology in a critical part of the financial system. Through this framework, central banks and other interested parties can better determine the technology's potential to provide operational efficiencies and to make financial markets more robust and resilient.

Developments to date suggest that DLT bears promise but that there is still a long way to go before that promise may be fully realised. Much work is needed to ensure that the legal underpinnings of DLT arrangements are sound, governance structures are robust, technology solutions meet industry needs, and that appropriate data controls are in place and satisfy regulatory requirements. It also seems clear that changes and related efficiency gains are more likely to be incremental than revolutionary.

Innovation in payment, clearing and settlement has been at the heart of the Committee on Payments and Market Infrastructures (CPMI) since its establishment. The Committee has played a critical role in reducing market inefficiency and improving the safety of payment, clearing and settlement systems through, among other things, the promotion of technological innovation. More recently, the CPMI published reports on digital currencies and fast payment developments. This report will hopefully contribute to the dialogue on how industry can use innovation to support robust, efficient and safe payment, clearing and settlement systems.

The Committee thanks Klaus Löber and the working group for their efforts in articulating an analytical and structured approach to this technology.

Benoît Cœuré, Chairman
Committee on Payments and Market Infrastructures

Table of contents

1. Introduction

Distributed ledger technology (DLT) is viewed by many as having the potential to disrupt payment, clearing, settlement and related activities. DLT, including blockchain technology, draws upon both well-established and newer technologies to operate a set of synchronised ledgers managed by one or more entities. In many markets, financial market infrastructures (FMIs) are entrusted by their participants with updating and preserving the integrity of a central ledger and, in some cases, managing certain risks on behalf of participants. DLT could reduce the traditional reliance on a central ledger managed by a trusted entity for holding and transferring funds and other financial assets.

DLT may radically change how assets are maintained and stored, obligations are discharged, contracts are enforced, and risks are managed. Proponents of the technology highlight its ability to transform financial services and markets by: (i) reducing complexity; (ii) improving end-to-end processing speed and thus availability of assets and funds; (iii) decreasing the need for reconciliation across multiple record-keeping infrastructures; (iv) increasing transparency and immutability in transaction record keeping; (v) improving network resilience through distributed data management; and (vi) reducing operational and financial risks.[1] DLT may also enhance market transparency if information contained on the ledger is shared broadly with participants, authorities and other stakeholders.

The use of DLT, however, does not come without risks. In most instances, the risks associated with payment, clearing and settlement activities are the same irrespective of whether the activity occurs on a single central ledger or a synchronised distributed ledger.[2] That said, DLT may pose new or different risks, including: (i) potential uncertainty about operational and security issues arising from the technology; (ii) the lack of interoperability with existing processes and infrastructures; (iii) ambiguity relating to settlement finality; (iv) questions regarding the soundness of the legal underpinning for DLT implementations; (v) the absence of an effective and robust governance framework; and (vi) issues related to data integrity, immutability and privacy. DLT is an evolving technology that has not yet been proven sufficiently robust for wide scale implementation.

This report aims to provide an analytical framework for central banks and other authorities to review and analyse DLT arrangements – in the conceptual, experimental or implementation phases – with the objective of understanding the use cases, and identifying opportunities and risks. Market participants may also find the report useful. The framework focuses on the potential implications for efficiency and safety, and for financial markets more broadly. The framework is directed primarily at arrangements that involve restricted ledgers (access to which is for approved users only), reflecting the main types of arrangement currently being developed in the financial sector, which are of particular interest to the relevant authorities.

[1] D Mills, K Wang, B Malone et al, "Distributed ledger technology in payments, clearing, and settlement", Federal Reserve Board *Finance and Economics Discussion Series*, no 2016-095, December 2016, p 17, www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf.

[2] A framework for addressing risks inherent in FMIs generally is set out in the Committee on Payment and Market Infrastructures (CPMI) and the International Organization of Securities Commissions' (IOSCO's) report on *Principles for financial market infrastructures* (PFMI). Some risks specific to digital currency aspects of DLT are discussed in the CPMI report on *Digital currencies*. See CPSS-IOSCO, *Principles for financial market infrastructures*, April 2012, www.bis.org/cpmi/publ/d101a.pdf, and CPMI, *Digital currencies*, November 2015, www.bis.org/cpmi/publ/d137.pdf.

2. Distributed ledger technology

There is some variance in the use of the term "distributed ledger technology", reflecting the evolving nature of the technology and the marketplace, as well as the spectrum of emerging applications. For this report, DLT refers to *the processes and related technologies that enable nodes*[3] *in a network (or arrangement) to securely propose, validate and record state changes (or updates) to a synchronised ledger that is distributed across the network's nodes*. In the context of payment, clearing, and settlement, DLT enables entities, through the use of established procedures and protocols, to carry out transactions without necessarily relying on a central authority to maintain a single "golden copy" of the ledger.

The report uses "arrangement" as a generic term for any DLT-based application or implementation. An arrangement can be described in terms of its technical design and institutional structure. There is limited standardisation of terminology in the industry – emerging arrangements include systems, platforms and layers. Without seeking to establish specific definitions, a *system* is designed to stand alone and to fulfil its functions without interacting with any other arrangement. Another type of arrangement might be a *platform*, with applications being built on top of a common foundation to leverage functionality across multiple arrangements. Still other implementations of the technology might seek to act as a *layer*, with the emphasis on providing interconnectivity between arrangements.

2.1 Background

In 2008, a person or persons using the pseudonym Satoshi Nakamoto published a paper[4] that outlined the mechanics of a new cryptocurrency, bitcoin, and a peer-to-peer solution for online transfers to be sent from one party to another without the need for known and trusted third parties. The solution combines a number of well-established technologies to verify and add transactions into a "block". This block (or batch of transactions) is added to a chain comprising a history of transactions (known as a blockchain) following a series of procedures and protocols. The new block is broadcast to the network so that nodes can agree on the new blockchain and update their copies of the ledger. This process of agreement, or consensus, across nodes involves cryptographically linking the new block to the previous block in the blockchain to help preserve the integrity of the ledger.

Since the introduction of blockchain technology, the industry has been exploring ways of leveraging the technology beyond bitcoin, beginning with platforms that could be programmed to store and manage records, and transfer any digital asset, instrument or information on a shared ledger. This generalised use has garnered significant attention in the financial sector, reflecting its traditional reliance on multiple ledgers to maintain transactional information and balances. The use of DLT is being explored, in particular, for payment, clearing and settlement activities because of potential efficiency gains arising from the technology. These potential gains include simplifying the settlement and related reconciliation processes required of actors participating in payment, clearing and settlement arrangements.[5]

As experimentation with DLT continues, real-world applications have highlighted some of the challenges associated with using the technology for payment, clearing and settlement. These include having safe, secure and scalable systems, among other industry needs. To address these challenges, arrangements have customised their application of DLT for the financial sector. Based on an analysis of

[3] In computer science, a node is the basic computing unit of a network. In the context of this report, a node refers to a computer participating in the operation of a DLT arrangement.

[4] See S Nakamoto, "*Bitcoin: a peer-to-peer electronic cash system*," October 2008, bitcoin.org/bitcoin.pdf.

[5] For example, in clearing and settlement arrangements, these actors could include banks, broker-dealers, custodians, registries, a central securities depository, a securities settlement system, a central counterparty, a trade repository and a payment system.

arrangements that are in use or under consideration, developments in the financial sector have often involved some common design elements, along technical and institutional dimensions. For example, arrangements are more likely to maintain a level of trust in the system through a closed set of participants[6] or the establishment of a system administrator.

2.2 Technical design elements

DLT arrangements can be designed in a number of ways and can support some or all parts of a transaction flow. Such arrangements typically involve several key technical design concepts that specify the information to be kept on the ledger and how the ledger is to be updated.

2.2.1 Maintaining information on the ledger

Ledgers that maintain records and other information are at the core of DLT arrangements. In payment, clearing and settlement use cases, a distributed ledger is employed to record ownership or balances of digital assets or digital representations of physical assets. Digital assets that originate on the ledger are typically referred to as "native assets" (also known as "native tokens"), while assets that are represented electronically on the ledger are typically referred to as "non-native assets" (also known as "non-native tokens"). The exact form of record keeping varies by arrangement but all specifications employ a digital ledger that includes a summary of transactions or balances corresponding to participants.[7]

Ledgers maintain either a history of all transactions or a set of account balances. One example of a ledger that maintains a history of transactions is a blockchain. As previously noted, in a blockchain implementation, transactions are recorded in batches, known as blocks. Once a block is confirmed as valid, it is linked (or chained) to all previous transactions on the ledger. However, a blockchain is just one type of distributed ledger, not all distributed ledgers necessarily employ blocks or chain transactions. An alternative approach might be more similar to standard bookkeeping which updates only the balance of users' accounts.

In some cases, a ledger may be used to retain more than the ownership records of assets. For example, a distributed ledger may act like a central repository for financial contracts by retaining the terms of an actual contract or a copy of it. Some DLT arrangements go a step further and allow for "automated contract tools" which permit users to include self-executing code on the ledger to automate the fulfilment of contract terms. Examples include the execution of interest and principal payments on certain dates, collection or distribution of funds based on certain events occurring or automatic termination of contracts based on agreed upon terms. This type of functionality is often referred to by the industry as a "smart contract".[8]

2.2.2 Updating the ledger

A notable property of DLT is the distribution of responsibilities for updating the ledger by multiple nodes. These nodes can be deployed across multiple sites, institutions or even jurisdictions, as discussed later. Figure 1 provides a stylised depiction of the multiple nodes that update a ledger. In this example, all the nodes are connected and have their own identical copy of the ledger. Depending on the arrangement's rules, changes to the ledger can be reflected in all copies within a certain time span (latency).[9]

[6] The term "participants" is used in this report to broadly describe users of a DLT implementation. Participants do not necessarily need to operate a node supporting the processing of transactions.

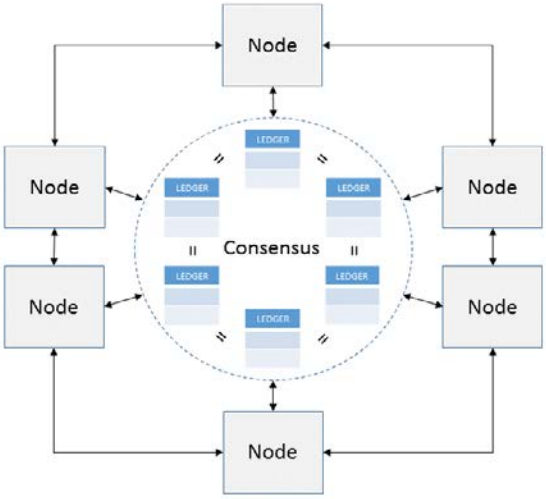
[7] See also A Pinna and W Ruttenberg, "Distributed ledger technologies in securities post-trading", *European Central Bank Occasional Paper Series*, no 172, April 2016, www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf.

[8] A smart contract will often not be a "contract" in the legal sense.

[9] This is true for fully distributed ledgers. Certain solutions also allow restrictions on the distribution of information.

Figure 1

Ledgers distributed across multiple nodes



2.2.2.a Validation and consensus

In order to update a synchronised distributed ledger, an arrangement typically uses a number of protocols for communication between nodes and for facilitating consensus among nodes about the current state of the ledger as well as its historical record.

Cryptography. Cryptographic tools, such as public key cryptography and public key infrastructure,[10] play an important role in DLT by identifying and authenticating approved participants, confirming data records and facilitating consensus on ledger updates. Participants proposing changes to the ledger, authenticate themselves by providing their cryptographic digital signatures for the proposed change. Validators will use cryptographic tools to verify whether the participant has the proper credentials to do so. Cryptographic tools may also be used to restrict access to data so that only approved parties can see the information.

Consensus. The consensus mechanism is the process by which the nodes in a network agree on a common state of the ledger. This process typically relies on cryptographic tools, a set of rules or procedures reflected in the protocol, and either economic incentives (applicable to any network configuration) or governance arrangements. Consensus generally involves two steps:

- Validation: each validator identifies state changes that are consistent according to the rules of the arrangement (that is, assets are available to the originator, and the originator and beneficiary are entitled to exchange the assets). In order to do so, each validator needs to rely on a record of previous states, either as a "last agreed state" or as a "chain of previous states".
- Agreement on ledger updates: nodes agree to state changes to the ledger. This stage of the consensus process involves mechanisms or algorithms that resolve conflicting changes to the

[10] Public key cryptography is used to share securely encrypted data and to sign digital documents. Public key infrastructure (PKI) is a set of rules, policies and procedures needed to create, manage, distribute, use, store and revoke digital certificates that associate cryptographic public keys to real entities. Both tools could be applied to DLT to grant approved users access to the arrangement and to sign transactions.

ledger.[11] The key challenge is to ensure that valid changes are made once and only once, by ensuring that state changes are synchronised across the distributed ledger.

2.2.2.b Technical roles of nodes (differentiated or not differentiated)

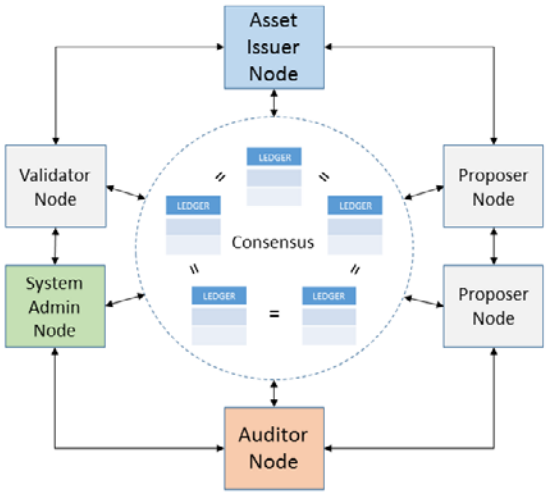
Nodes in the network may play a variety of technical roles. Examples of those roles, which are not mutually exclusive, include:[12]

- System administrator: the gatekeeper that controls access to the system and provides certain services for the arrangement, including the notary function, dispute resolution, standard-setting and regulatory reporting.
- Asset issuer: node permissioned to issue new assets.
- Proposer: node permissioned to propose updates to the ledger.
- Validator: node permissioned to confirm the validity of proposed state changes.
- Auditor: node permissioned to view the ledger but not make updates.

Further, nodes may vary in their ability to see the records stored on the ledger. For example, it is possible that a node is permissioned to see only the transactions to which it is a counterparty or one of its clients has a relevant interest, even if it maintains a copy of the complete encrypted ledger.[13] Figure 2 shows an example of a ledger distributed across multiple nodes with varying roles or permissions.

Figure 2

Ledger distributed across multiple nodes with varying roles or permissions



[11] For example, because of the distributed nature of the arrangement, it is possible that a participant transfers an asset it holds to another participant while simultaneously attempting to transfer the same asset to a third participant. Without a mechanism for agreeing which transaction to post to the ledger, the arrangement would enable participants to "double-spend" assets.

[12] Other potential roles of nodes and other participants in an arrangement include: i) wallet providers that safeguard private keys and assist in asset management; ii) protocol developers that develop the underlying technology and may manage the technology and protocol; and iii) end-users who use proposer nodes to submit transactions.

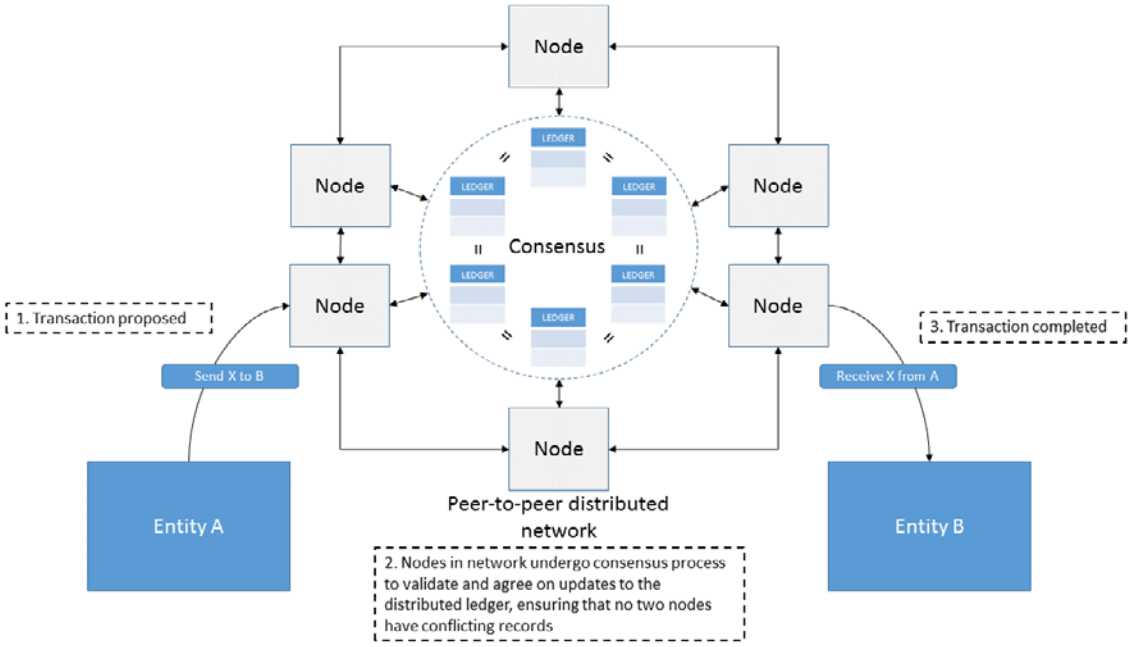
[13] The ledger may be encrypted so that nodes only view, in a decrypted form, the elements of the ledger they are permissioned to see.

2.2.3 Process flow

DLT for payment, clearing and settlement activities can be designed in a number of ways and perform different functions. To highlight how the concepts of distributed node, ledger and consensus could be used in a payment transaction, Figure 3 provides a stylised process flow for a distributed ledger transfer system.

Figure 3

Stylised process flow of a DLT-based payment system



In this example, the transaction process involves three broad steps:

(a) To initiate a payment, entity A uses cryptographic tools to digitally sign a proposed update to the shared ledger that would transfer funds from its account on the ledger to entity B's account.

(b) Upon receiving the transfer request, other nodes authenticate entity A's identity and validate the transaction by checking to make sure that entity A has the necessary cryptographic credentials to make an update to the record in question. Validation would include, among other things, verifying that entity A has sufficient funds to make the payment. Nodes also take part in the consensus process to agree on the payments that should be included in the next update to the state of the ledger.[14]

(c) After the update has been accepted by the nodes, the properties of the asset are modified such that all future transactions regarding the asset must be initiated using the cryptographic credentials of entity B.

[14] For example, the consensus process may take place in rounds where one node is given the right to propose an update in each round. Next, the non-proposing nodes vote on whether to include the update or move on to a second round. Assuming the update does not conflict with the states of the ledger distributed to each node, the update is approved through a simple voting process according to a pre-defined threshold.

2.3 Institutional design elements

A DLT arrangement's technical configuration is complemented by its institutional design. Arrangements typically involve decisions regarding what roles the various institutions play, including responsibility for operation of and access to the arrangement.

2.3.1 Operation of the arrangement

A key institutional design element of a DLT arrangement is what entity or entities are responsible for managing the arrangement, including modifying or updating the protocol and source codes, granting access and assigning permissions for other entities to perform certain roles. At one extreme, a single entity could host and operate all the nodes in an arrangement on behalf of participants and be the sole entity responsible for the maintenance of the ledger. Alternatively, maintenance could be shared across many entities, each responsible for having a copy of the ledger and performing prescribed tasks.

2.3.2 Access to the arrangement (unrestricted or restricted)

Arrangements can be designed to accommodate any number of participants. Unrestricted arrangements are designed in such a way that there are no restrictions concerning access to the arrangement or to the roles of nodes within the arrangement. In arrangements where access is completely open, the entities operating the nodes are not likely to know each other. Such arrangements may be difficult to govern and the entire set of rules governing interactions among nodes needs to be primarily "on-ledger" (encoded in the computer protocol).[15] By contrast, restricted platforms allow control over participants' access to the arrangement. Because access is controlled, the set of rules governing interactions can also be "off-ledger".[16, 17]

The preceding figures 1 and 2 do not map entities to the participation, ownership or operation of the nodes in an arrangement. As noted before, arrangements considered by the industry are typically characterised by a range of institutional configurations that map nodes and their accompanying roles to entities. Figure 4 provides one example of a restricted DLT arrangement where the authority for validating transactions and issuing assets is concentrated in a single entity. In this example, entity A serves as the system administrator and operator of all of the arrangement's validator and asset issuer nodes. Entity B and entity C operate proposer nodes, which gives them the ability to suggest new changes to the state of the ledger but not to unilaterally make such changes without entity A's approval. It is important to note that this is one of many different possible mappings of nodes and entities that the industry could consider.

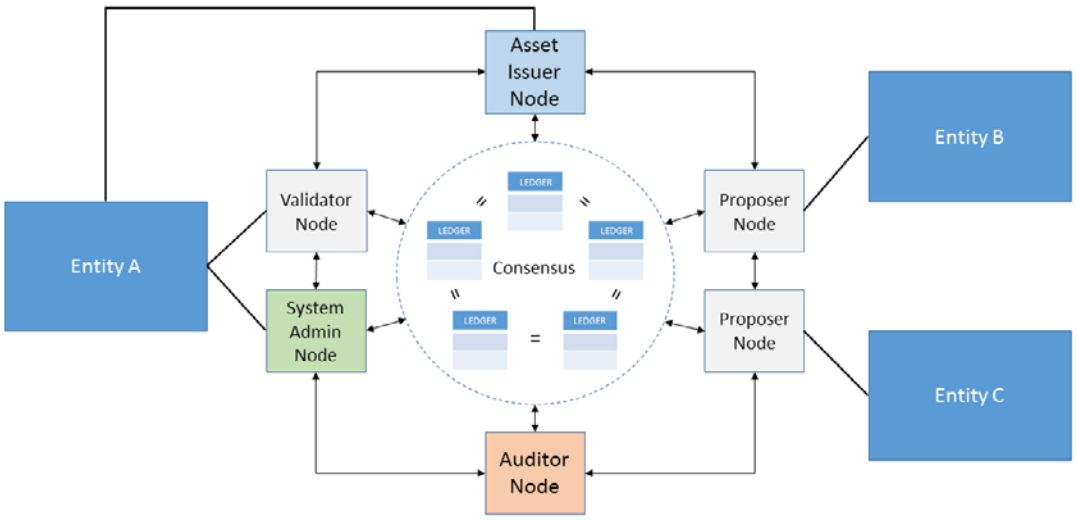
[15] One example of an on-ledger governance rule is a fine denominated in an arrangement's native asset and levied as part of the computer protocol. Because participants in an unrestricted arrangement are often anonymous, this type of mechanism may be necessary to subject participants to pecuniary sanction in order to deter inappropriate behaviour.

[16] An off-ledger governance rule may be a legal sanction or a fine that can be invoked against a specific participant because the identity of participants is known in a restricted arrangement.

[17] See also UK Government Office for Science, *Distributed ledger technology: beyond block chain*, December 2015, www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

Figure 4

An example of a restricted DLT arrangement with differentiated technical roles



2.4 Potential configurations and trade-offs

Table 1 below highlights some of the potential combined institutional and technical design configurations that an arrangement may take. It also shows the degree of change relative to today's financial ecosystem. There is likely to be a multitude of different arrangements, depending on the specific purpose they are designed to fulfil. The arrangements are not only customisable according to their technological elements, such as the number of nodes, but also by the roles played by each of the nodes.

Potential configurations of DLT arrangements — Table 1

Description of arrangement	One entity maintains and updates the ledger (for example, a typical FMI)	Only approved entities can use the service; entities can be assigned distinct restricted roles	Only approved entities can use the service; entities can play any role	Any entity can use the service and play any role
Operation of the arrangement	Single entity	Multiple entities		
Access to the arrangement	Restricted			Unrestricted
Technical roles of nodes	Differentiated		Not differentiated	
Validation and consensus	Within a single entity	Within a single entity or across multiple entities	Across multiple entities	

At the most basic level, an arrangement needs to balance the pros and cons of having unrestricted versus restricted access. For instance, unrestricted arrangements could open up services to new types of participant and reduce the tiering of relationships in payment, clearing and settlement processes. However, unrestricted access might cause scalability and information security issues because of the inherent challenges of reaching consensus between large numbers of participants that are unknown to each other. Anonymous participation also calls for security measures mitigating cyber-attacks or illicit activities to be incorporated into the design and rules of the arrangement (that is, to be resolved "on-ledger"). These issues are significant enough that current DLT implementations for payment, clearing and settlement activities are focused on restricted arrangements, which more closely fit within existing legal and regulatory frameworks.

Assigning particular roles to a broad range of entities and their nodes may introduce other important issues. For example, if only certain nodes are delegated to achieve consensus, it may be easier (and faster) to reach consensus on the state of the ledger; however, it may also be easier for any one of these nodes to compromise the integrity of the ledger. Thus, it is important that such an entity is known and trusted by participants. Increasing the number of nodes may improve the overall resilience of the network but it may also lengthen latency. DLT arrangements characterised by a larger number of distributed roles may raise important questions related to governance, settlement and operational risk management. As a result, the choice of specific protocols for validation and consensus are driven primarily by access rules and the defined roles played by entities and their nodes.

The range of approaches to DLT is an indication that a one-size-fits-all approach is not appropriate to address the broad range of challenges in payment, clearing and settlement. Arrangements such as the ones in the first column of Table 1 represent change that is more incremental in nature and reflect opportunities to record information through a single entity, much as is done today. This contrasts with the final column of Table 1, which represents bitcoin-like arrangements. Models such as these would represent more radical changes because of their completely decentralised nature. In the middle is a variety of other possible arrangements. The ongoing experimentation of different design choices reflects attempts to realise some of the benefits of DLT while recognising the specific constraints of a particular use case.

3. Analytical framework

This framework is designed to help central banks and other authorities understand DLT arrangements for payment, clearing and settlement activities by providing a structured approach to analysing their potential benefits and risks. The framework is based on four core components: (i) **scope**: understanding the arrangement (see Section 3.1), which includes its functionality and nature of service, and the factors for its effective implementation; (ii) **efficiency**: analysing the arrangement's implications for efficiency (see Section 3.2); (iii) **safety**: analysing the arrangement's implications for safety (see Section 3.3); and (iv) **broader implications**: analysing the arrangement's broader financial market implications (see Section 3.4).

The framework should be viewed as a starting point for understanding DLT arrangements to identify a range of issues that are of interest to authorities and other stakeholders. The framework is neither comprehensive nor exhaustive; nor does it address every possible DLT or payment-, clearing- and settlement-related issue. For arrangements at an early stage of development, which may not have concrete answers to some questions, the framework is intended to identify areas where further work is required. In addition, the framework does not prescribe or suggest particular design elements.

3.1 Understanding the arrangement

DLT arrangements vary significantly based on their functionality, nature of service, design, technology and processes. In order to analyse these types of arrangement, it is useful to apply a structured approach to understand the functionality and nature of a given service, and the key factors for its effective implementation.

3.1.1 What is the functionality and nature of the arrangement?

At the core of DLT is a ledger that maintains information. An arrangement will typically perform one or more of the following functions relating to maintenance of the ledger: (i) record keeping; (ii) transfer of assets or updating of balances; and (iii) use of automation tools. Other ancillary services or functions such as data lookups, screening and analytics may also be incorporated as features. In understanding the functionality and nature of the service, it may be useful to understand the improvement the arrangement is trying to effect, what part (or parts) of the value chain is affected, how it is designed and which participants and users will be impacted by it.

3.1.1.a Identifying problems, inefficiencies or improvements that it is addressing

Part of understanding the functionality and nature of the arrangement requires understanding how DLT can facilitate a solution to a problem or improve upon existing services or processes. For example, the arrangement could simplify processes, improve information flows, reduce operational costs, expand access to financial services and improve financial inclusion.[18] As discussed below, the arrangement may reduce the need for human involvement through automation, thus increasing efficiency and accuracy. This exercise should also identify the primary benefits that the arrangement can realise while taking into account its costs and newly introduced risks. The arrangement may need to balance resilience and efficiency benefits to achieve a particular outcome. In doing so, it is important to understand the potential trade-offs involved.

3.1.1.b Identifying the affected part or parts of the value chain

Identifying which part or parts of the value chain the arrangement is affecting and to what extent it brings a new concept to the marketplace (disruptive innovation) or improves current offerings (incremental innovation) will bring greater clarity on the functionality and nature of the service. The value chain can be categorised in a number of ways, including:

- Customer identification: processes associated with digital identities and compliance with know-your-customer rules, anti-money laundering requirements and counter-terrorist financing regulations.
- Pre-transaction: processes associated with creating, validating and transmitting payments, transfer instructions or other obligations, including verifying asset holdings and linking data for clearing and settlement.
- Clearing: processes associated with transmitting, reconciling and, in some cases, confirming transactions as well as potentially including the netting of transactions and the establishment of final positions for settlement.

[18] In April 2016, the CPMI and the World Bank Group published a report on *Payment aspects of financial inclusion* that sets out guiding principles to assist countries seeking to advance financial inclusion in their markets through payments. The report tackles barriers to the adoption and usage of transaction accounts (including both deposit and e-money accounts). The CPMI-World Bank task force on financial inclusion will closely follow developments in the use of DLT to analyse their implications for promoting financial inclusion. See www.bis.org/cpmi/publ/d144.pdf.

- Settlement: processes associated with transferring an asset or financial instrument, or the discharge of an obligation by the FMI or its participants in accordance with the terms of an underlying contract.
- Post-settlement: processes related to certain actions taken after settlement, including reconciliation, recording and reporting activities, asset servicing (for example, principal and interest payments), and enforcement of contract terms (for example, smart contracts).

Some arrangements may impact only one or two steps in the process. For example, some DLT arrangements being considered by the industry focus on clearing and may involve new ways of sharing information across relevant parties to a transaction but do not involve the specific settlement of transactions. Others may create a new way of processing transactions from end to end. For example, some DLT arrangements may not only involve the exchange of information, but also the exchange of value in the form of assets on a ledger.

3.1.1.c Understanding the design, technology and associated processes

The design, technology and associated processes of arrangements vary significantly. These differences reflect the nature of services provided, technological development, organisational structure of the arrangement, local market structure and practices, and other jurisdictional factors. Understanding these factors is important in relating the specific problem or improvement being addressed.[19]

3.1.1.d Identifying the affected market participants

Identifying which market participants and users are affected by the arrangement helps in recognising the potential implications for efficiency and safety of the financial system. For example, the efficiency gains that an arrangement generates for a specific group of market participants might have implications for the risk profile of another group. Potential categories of market participants to consider include FMIs, banks, other financial institutions, their customers and the relevant authorities. Affected market participants may be located in multiple jurisdictions given the global nature of financial markets.

3.1.2 What are the key factors for effective implementation?

It is important to consider and specify the factors that may influence the development and use of the arrangement. Some arrangements involve a single entity or a small group of entities. Others require widespread adoption by the industry because potential efficiency gains and other benefits may be network-dependent. That is, a critical mass of participants in the arrangement may be required before the industry can realise any potential efficiency gains. In addition, implementation may require more fundamental and structural changes in the market, including changes to market conventions and practices. The following environmental, technological and financial factors may play a part in the implementation of an arrangement:

- Environmental factors: these include institutional acceptance of new technology, market factors such as size, market structure and practices, regulatory and legal conditions, and level of industry coordination.
- Technological factors: considerations such as the maturity of the technology and its interoperability with existing systems and processes are an element in technological adoption.
- Financial factors: projects offering better returns on investment through cost savings, revenue potential, or both, are more likely to be adopted by institutions and markets.

[19] Other potential resources to help understand an arrangement's design, technology and associated policies include CPMI reports on *Fast payments – Enhancing the speed and availability of retail payments* (see www.bis.org/cpmi/publ/d154.pdf), *Non-banks in retail payments* (see www.bis.org/cpmi/publ/d118.pdf), *Digital currencies* and the PFMI.

3.2 Potential implications for efficiency

DLT is viewed by many as having the potential to improve market efficiency. Efficiency is a broad concept that encompasses the arrangement's design, functionality and resource needs. Efficiency, in this context, is gauged by the speed and cost of the entire asset transfer cycle and how well the arrangement is meeting the needs of the markets it serves. In considering both speed and cost implications, reconciliation (Section 3.2.3), credit and liquidity management (Section 3.2.4), and automation (Section 3.2.5) will be important features.

3.2.1 Speed of end-to-end processing

DLT is often promoted as enabling faster settlement of transactions in a single arrangement. DLT could simplify existing process flows by reducing friction to information sharing among participants. It is important to consider that potential improvements in the speed of end-to-end processing are being referred to at the ecosystem level (ie across the value chain), and that the speed of transaction settlement within the infrastructure itself may be slower. For example, DLT arrangements may take longer to achieve settlement when compared with real-time gross settlement (RTGS) systems because, from a technical point of view, the process for validating a transaction and reaching consensus in DLT is potentially more complex than with a central entity. See also Section 3.3.2 on settlement.[20]

Key question:

- How does the arrangement affect (or compare to) existing payment, clearing and settlement processes with regards to the speed of end-to-end processing?

3.2.2 Cost of processing

The overall costs of maintaining and updating a distributed ledger would need to be compared to the costs of current practices and other viable alternatives. In principle, industry is exploring a variety of DLT arrangements for their potential to reduce costs in certain parts of the value chain. In addition, the impact on market-wide and social costs should also be considered. Further, DLT arrangements can lead to changes in the way costs are allocated among participants. For example, a distributed arrangement in which participants contribute to maintaining and updating a shared ledger allows for the sharing of maintenance across participants rather than such costs being borne directly by one entity, such as an FMI, which then charges fees to participants. In this sharing of responsibilities, participants operating certain nodes in an arrangement could see increased direct costs for contributing to the operation of the arrangement.

Key questions:

- Does the arrangement allow for an overall cost reduction compared to existing processes? How are costs redistributed among participants?
- What social costs might arise from operating the arrangement in a distributed environment?

[20] From a payment system perspective, real-time or near real-time settlement has been available in interbank and wholesale markets for a number of years with the widespread adoption of RTGS systems in wholesale payments and its more recent adoption in retail payments by some countries. On the latter, see CPMI report on *Fast payments – Enhancing the speed and availability of retail payments*.

3.2.3 Speed and transparency in reconciliation

Reconciliation is about ensuring that internal records relating to a transaction are matched across the relevant parties. This is typically a time-consuming and labour-intensive process as it involves the reconciliation of information on different ledgers and the recording and storing of that information in different formats. By allowing information that is in a common format to be shared across participants to a transaction, the use of DLT may reduce data discrepancy, facilitate quicker reconciliation and eliminate or reduce burdensome back office activities.[21] All or part of the reconciled data may also be shared across other market participants to enhance market transparency or with the relevant authorities to facilitate reporting. However, information sharing that improves the speed and cost of reconciliation should be balanced against data protection and privacy (see Section 3.3.5).

Key questions:

- What effect does the arrangement have on the reconciliation processes of participants?
- What transaction information is available to other participants, the market and relevant authorities? How does each party gain access to the information?

3.2.4 Cost of credit and liquidity management

Enhancements such as faster processing and reduced reconciliation work may lead to more transactions occurring in real-time or near real-time in certain markets. This development may affect the credit and liquidity needs associated with payment, clearing and settlement activity. As with RTGS systems, real-time or near real-time transfers allow for a reduction in credit exposures. It, however, also places higher demand on liquidity. Faster transfers suggest that participants will also receive funds and securities more quickly, freeing up liquidity that could be tied up in collateral as is the case in today's FMIs. Of course, not all DLT arrangements being considered will necessarily lead to real-time or near real-time transactions. For those arrangements, it will be important to understand their impact on credit- and liquidity-saving features. The net impact on credit and liquidity will depend on how the arrangement is designed and on the associated behavioural changes it induces.

Key question:

- What are the credit and liquidity implications of the arrangement on participants, the system and the broader market? How do these compare with existing arrangements?

3.2.5 Efficiency gains from automated contract tools

A key feature of DLT technology is its programmability to automate certain functions. Automated contract tools (including smart contracts) can facilitate, execute or enforce the performance of certain parts of an agreement (for example, reaching a certain date and executing a principal and interest payment on a loan contract). Another example could be that certain data feeds could be used as input to the ledger with a threshold triggering a margin call or other event-driven action. DLT allows information to be embedded in the ledger, allowing for self-executing applications. Automation of contract terms could improve efficiency by eliminating the need for human intervention in executing a transaction and thus reduce the

[21] A participant's ability to reduce or eliminate reconciliation activities depends on having access to the information maintained on the distributed ledger; however, it is not certain whether constraints on access to information on the ledger would affect a participant's decision to maintain separate internal records (and thus avoid the need for reconciliation).

probability of human error. The addition of automated contract tools, among other value-added features, could significantly simplify back office processes and records management.

At the same time, self-executing applications may create new challenges and risks for the financial ecosystem. Automated contract tools, for example, are not immune to malicious or faulty code. In cases where this code is executed, the integrity of the data on the ledger could be questioned and the ramifications could be significant. Moreover, simultaneous automated execution between contracts (and codes) could cause adverse and unpredictable behavioural patterns in the financial ecosystem. Likewise, interdependencies between contracts (and codes) could result in a transmission channel for unforeseen risks (see Section 3.4).

Key questions:

- For arrangements that allow automated contract tools, what elements are being automated and how?
- How does the arrangement mitigate the introduction of malicious or faulty codes?
- What procedures or mechanisms can the arrangement use to prevent, detect, and address quickly the execution of such malicious or faulty codes?

3.3 Potential implications for safety

A key public policy objective for payment, clearing and settlement arrangements is to identify, monitor and manage material risks that may arise from their use. Technology and system designs can help an arrangement become more operationally and financially sound but can also be a source of risk. In addition, in a stress scenario, arrangements may act as channels that transmit instability and uncertainty, contributing to financial contagion.

3.3.1 Operational and security risk

DLT arrangements have the capacity to enhance the safety of payment, clearing and settlement activities while also presenting new risks. The ultimate implications for safety would require weighing the advantages and disadvantages of the technology and associated process changes.

Resilience and reliability. One of the key drivers of DLT implementation is its potential to strengthen an arrangement's resilience and reliability. The distributed nature of its design, with the use of multiple synchronised ledgers and multiple processing nodes, has the potential to reduce the risk from a single point-of-failure.[22] If a ledger or node in the arrangement is inoperable or compromised, the other nodes can allow for the continued processing of transactions. Enhanced operational resilience and reliability are of particular interest to the authorities given the importance of protecting against cyber–threats. However, having many nodes in an arrangement creates additional points of entry for malicious actors to compromise the confidentiality, integrity and availability of the ledger.

Security. The security of an arrangement is central to the safety and soundness of the financial system. Cryptographic tools, such as public key cryptography, play a central role in ensuring the security of existing systems and are of critical importance in DLT arrangements. While current cryptographic tools are considered effective and are widely used today, future technological advancements could render existing cryptographic tools less secure and effective. This issue is of particular concern for an arrangement

[22] A single point-of-failure is defined as any point in a system, whether a service, activity, or process, that, if it failed to work correctly, would lead to a failure of the entire system.

with a weak governance structure, which may not be able to react quickly enough to emerging security issues and threats. Integration of DLT in existing infrastructures or transition from current systems to DLT-based ones could also generate security breaches that are not inherent in the new technology but could have a strong operational impact. Thus, arrangements are likely to not only rely upon cryptographic tools themselves but could also take a layered approach to security and leverage additional tools.

Operational capacity and scalability. A payment, clearing and settlement arrangement typically needs to handle significant fluctuations in transaction volumes and, as a consequence, needs to be operationally scalable. Operational capacity has two primary components: (i) processing large volumes on a daily basis; and (ii) handling potential peak volumes, including in times of market stress or volatility. An arrangement that fails to meet these requirements may weaken the safety of the payment, clearing or settlement activity. The scalability of an arrangement depends on several factors, including the type of data maintained in the records, the consensus mechanism used and the degree of centralisation.

Key questions:

- What are the key operational risks for the arrangement, particularly those that could affect its resilience and reliability, security, and operational capacity and scalability? How does the arrangement generally manage these risks?
- How do these risks and their management differ from traditional arrangements, if at all?
- How does the arrangement layer security that goes beyond the reliance on cryptography?

3.3.2 Settlement issues

An often-cited benefit of DLT is the ability to shorten the end-to-end processing of financial transactions (see Section 3.2.1 on speed of end-to-end processing). In addition to affecting the efficiency of payment, clearing and settlement, DLT also has the capacity to affect safety. In this respect, it is useful to consider key components of settlement: the settlement asset, how settlement is achieved operationally and how settlement finality is achieved for legal purposes.

Settlement asset. Some arrangements are based on updating balances in the ledger (that is, the ledger is recording positions through debits and credits). Some arrangements are based on transferring digital assets in the ledger (that is, the ledger is recording the transfer of ownership of a specific digital asset that exists only on the ledger). Yet other arrangements are based on transferring digital representations of a physical asset that is held in custody (ie the ledger is recording transfers of assets held elsewhere). In the context of a payment system, for example, an arrangement could be updating a balance, transferring digital currency or updating an account balance reflecting monies held at a custodian bank.

Operational settlement. In some DLT arrangements, it can take some time to update and synchronise state changes to a ledger. The first instance of an update, for example, may not represent operational settlement because it may take time for consensus to be achieved across the nodes in the synchronisation of ledgers. In arrangements that use a proof-of-work[23] model, settlement is probabilistic. That is, the more times the transaction is confirmed in the ledger, the less likely it will be revoked. Operational settlement becomes more complex if it involves the delivery of one asset against another, for example, the exchange of securities against the corresponding cash amounts or exchange of one currency

[23] Proof-of-work is a common form of consensus that requires nodes to agree on the transactions being added to the ledger. In general, the mechanism waits for a majority of nodes to agree on a transaction before adding it to the ledger.

for another. In many arrangements involving an exchange of value, another financial market infrastructure is typically involved.

Legal settlement finality. Settlement finality is the legally defined moment at which the transfer of an asset or financial instrument, or the discharge of an obligation, is irrevocable and unconditional and not susceptible to being unwound following the bankruptcy or insolvency of a participant. In traditional systems, settlement finality is a clear and well-defined point in time, backed by a strong legal basis. For DLT arrangements, settlement finality may not be as clear. In arrangements that rely on a consensus algorithm to effect settlement finality, there may not necessarily be a single point of settlement finality. Further, the applicable legal framework may not expressly support finality in such cases.

Key questions:

- What state changes are being recorded on the ledger (for example, balances, transfers of digital assets, transfers of digital representations of a physical or immaterial asset)?
- What is the legal nature of assets or records reflected in the arrangement?
- How is operational settlement achieved on the ledger and by whom? How does it differ from traditional systems?
- How is settlement finality provided for by the applicable legal framework?
- For exchange-of-value settlement, how is delivery versus payment, delivery versus delivery and payment versus payment achieved, including where relevant across autonomous ledgers or between a ledger and a traditional FMI?

3.3.3 Legal risk

Having a well-founded, clear, transparent, and enforceable legal basis is a core element of payment, clearing, and settlement arrangements. DLT can increase legal risks if there is ambiguity or lack of certainty about an arrangement's legal basis. Because the application of this technology to payment, clearing and settlement activity is new, the legal underpinning for certain activities may not be as well established as that for traditional systems (for example, in terms of identifying the applicable jurisdiction or relevant laws). Conversely, DLT can be used to help reduce certain legal risks. For example, automating certain terms and conditions of legally binding agreements (such as automating interest payments as outlined in a contractual agreement) may reduce the risk that contract terms are not enforced as specified in the agreement within the agreed time period.

An arrangement's legal basis consists of a legal framework that includes general laws and regulations governing property, contracts and liability, among other things. It also includes the arrangement's rules, procedures and contracts. There are certain legal issues, such as proprietary rights and settlement finality (see Section 3.3.2), that should be articulated clearly by the arrangement, understood by participants and supported by applicable law. For example, the legal basis regarding the ownership or transfer of assets or the rights and obligations of the relevant parties may not always be clear. An arrangement typically attempts to use standardised rules or contracts to define rights, obligations and processes. In such cases, it is important to consider the soundness of these legal arrangements and their enforceability. This can be further complicated by transactions that take place across borders or in multiple jurisdictions, in which case the law underpinning the activity would need to be confirmed or adopted in multiple jurisdictions in ways that are mutually compatible.

Key questions:

- Does the arrangement have a clearly established, sound and enforceable legal basis for its activities, in particular if it operates in a multijurisdictional environment?
- How are potential conflicts of laws identified and addressed?
- What are the rights and obligations of the participants? How are they specified (for example, in rules, contracts or code)? What is the dispute resolution mechanism (for example, for liability issues)?

3.3.4 Governance

Governance structures can improve the safety of an arrangement (for example, by enhancing decision-making pertaining to the arrangement's design and technological evolution or by the involvement of a broad spectrum of stakeholders) or weaken it (for example, by slowing incident responses related to operational issues in the case of highly complex governance structures). An arrangement that involves the sharing of information and of ledger maintenance will need to have an especially well thought-out governance structure. Recent governance challenges relating to several unrestricted DLT use cases have highlighted the critical importance of having a clear understanding of the governance arrangements surrounding change and incident management, and of the enforcement of governance decisions.

Key questions:

- What type of governance structure does the arrangement have? Does it support sound decision-making, risk management, incident and emergency response, and provide robust management oversight?
- Does the arrangement involve the sharing of information or maintenance of the ledger across entities? If so, who are the various stakeholders in the arrangement (including direct and indirect participants), and how does the governance structure define their respective responsibilities?
- Is there a clear mechanism for decision-making or agreeing on alterations to the arrangement?

3.3.5 Data management and protection

How an arrangement records, maintains and shares data has implications for the safety of payment, clearing and settlement activity. A fundamental requirement for any record-keeping system is to have records structured and maintained in such a manner that any legitimate entity[24] can verify the relevant history of the record. In other words, the system should allow for traceability of the data. Further, traceability requires that the data not be subject to loss, damage or tampering. The integrity of the data is vital to the safety of the arrangement. Moreover, traceability may be an important requirement for compliance with know-your-customer rules, anti-money laundering requirements and counter-terrorist financing regulations. Traceability, however, should be weighed against privacy and the need to keep certain information confidential.

[24] The term "legitimate entity" may have different meanings depending on the context. In some cases, the configuration of DLT implementation will require all participants to have equal access to information. However, other configurations may require a higher level of privacy of transactional information, such that only the counterparties to a transaction have the right to know its details.

Different levels of privacy may be required depending on the design of an arrangement. In some arrangements, all nodes have access to a copy of the ledger and may, if allowed, see all transactional history. However, in applying DLT in the financial sector, participants may not want or be permitted to provide full visibility of the data. In such cases, access to information may be restricted. For example, data may be encrypted so that nodes only see the elements of the ledger that they are permissioned to see, even if it maintains a copy of the complete ledger. In some cases, nodes may only hold data that are relevant to them. Regardless of the level of privacy required, it is important to have adequate controls in place that restrict access to data as intended while allowing the nodes to reach agreement over the state of a ledger and the validity of transactions.

A possible benefit of DLT arrangements is the immutability of data recorded in the ledger, meaning that data cannot be unilaterally changed once recorded. Immutability is crucial to the safety of an arrangement as it relates to data integrity. Despite the need for immutability, there may be a need to change data in certain, limited circumstances, such as in the case of inadvertent errors, fraud and other events.[25] The ledger may merit correction or reversal of transactional data, including through the creation of new transactions. This issue may be of particular concern for self-executing codes whereby mistakes in coding or other events may need to be corrected quickly. As such, governance and operational procedures are needed to address exceptions processing.

Key questions:

- How does the arrangement guarantee data integrity, including the traceability of data?
- Are the data considered immutable? If yes, how are data, transaction or processing errors addressed?
- How does the arrangement handle data privacy and confidentiality?

3.4 Potential broader financial market implications

As DLT arrangements develop and potentially reach the production stage, they may also have broader market implications. The financial system as a whole contains numerous interlinkages. For example, financial institutions may participate in multiple payments systems and in other FMIs. Additionally, securities settlement typically requires multiple systems such as a payment system for the transfer of value and a separate securities settlement system for the transfer of a security. Further, financial institutions, payments systems and other FMIs may cross jurisdictional boundaries.

3.4.1 Connectivity issues and standards development

Industry is experimenting with a number of potential DLT arrangements, and multiple DLT arrangements are likely to emerge providing different, similar and complementary functionality. As such, one technical challenge would be to enable arrangements to communicate or connect with one another and with legacy systems in order to facilitate the conduct of a variety of financial transactions. The development of technical interoperability standards can facilitate this by providing a base layer of connectivity that also helps lower implementation and integration costs. Successful development of standards may encourage broader adoption of DLT in the financial system, which could potentially bring network scale efficiencies.

[25] Other events include the right to delete specific person-related data.

Key questions:

- What system, platform, layer, or combination thereof is being considered or used in the arrangement?
- What protocol is being considered or used in the arrangement?
- Is the protocol code open source or proprietary? If proprietary, how flexible is the code in working with other arrangements?

3.4.2 Financial market architecture

A DLT arrangement may have possible effects on the overall financial market architecture. In some implementations, the arrangement can be seen as more of an incremental upgrade over current arrangements, and one that does not change significantly current business practices. In other implementations, such as an unrestricted arrangement, DLT may lead to disintermediation of certain functions or certain entities. Such a change in business practices may affect the competitive balance in financial markets and have implications for financial market architecture. It may also introduce new, non-bank players that are not currently covered by or contemplated in existing regulatory regimes.

Key questions:

- How does the arrangement change the role of existing intermediaries or involve new actors?
- How could the arrangement change existing market and regulatory practices?

3.4.3 Broader financial market risks

A DLT arrangement could have implications for broader financial market risks.[26] One possible benefit of DLT in an interconnected system is that data shared across key entities may lead to greater market transparency and more effective risk management across systems. On the other hand, DLT could also have negative implications. For example, in a possible future configuration with many automated contract tools, macroeconomic conditions could automatically trigger margin calls across FMIs, leading to severe liquidity demand across the financial system and creating a systemic event. Thus, it would be important to better understand how some of the possible automation tools are correlated across the financial system and to assess whether additional protections are needed to prevent contagion.

Key questions:

- Does the arrangement pose broader financial market risks at this stage of development and implementation? What risks could it pose in the future?
- What interconnections does the arrangement have with other systems, including other DLT arrangements?

[26] The interconnectedness of financial institutions, FMIs and other entities raises concerns that should problems arise in one area of the financial system, those problems could cascade to other market segments and financial institutions, potentially leading to financial instability.

Annex A: Summary of key questions in the framework

This analytical framework is for central banks and other entities interested in reviewing and analysing DLT arrangements with the objective of understanding their use cases, and identifying opportunities and risks. The framework uses key questions to focus on potential implications for efficiency and safety and for the broader financial markets. The key questions summarised below are neither comprehensive nor exhaustive. Rather, they should be used as foundational questions in identifying issues for further exploration and analysis.

1. Understanding the arrangement

1.1 What is the functionality and nature of arrangement?

- Identifying problems, inefficiencies or improvements it is addressing
- Identifying the affected part or parts of the value chain
- Understanding the design, technology and associated processes
- Identifying the affected market participants

1.2 What are the key factors for effective implementation?

- Environmental factors
- Technological factors
- Financial factors

2. Potential implications for efficiency

2.1 Speed of end-to-end processing

- How does the arrangement affect (or compare to) existing payment, clearing and settlement processes with regards to the speed of end-to-end processing?

2.2 Cost of processing

- Does the arrangement allow for an overall cost reduction compared to existing processes? How are costs redistributed among participants?
- What social costs might arise from operating the arrangement in a distributed environment?

2.3 Speed and transparency in reconciliation

- What effect does the arrangement have on the reconciliation processes of participants?
- What transaction information is available to other participants, the market and relevant authorities? How does each party gain access to the information?

2.4 Cost of credit and liquidity management

- What are the credit and liquidity implications of the arrangement on participants, the system and the broader market? How do these compare with existing arrangements?

2.5 Efficiency gains from automated contract tools

- For arrangements that allow automated contract tools, what elements are being automated and how?
- How does the arrangement mitigate the introduction of malicious or faulty codes?
- What procedures or mechanisms can the arrangement use to prevent, detect and address quickly the execution of such malicious or faulty codes?

3. Potential implications for safety

3.1 Operational and security risk

- What are the key operational risks for the arrangement, particularly those that could affect its resilience and reliability, security, and operational capacity and scalability? How does the arrangement generally manage these risks?
- How do these risks and their management differ from traditional arrangements, if at all?
- How does the arrangement layer security that goes beyond the reliance on cryptography?

3.2 Settlement issues

- What state changes are being recorded on the ledger (for example, balances, transfers of digital assets, transfers of digital representations of a physical or immaterial asset)?
- What is the legal nature of assets or records reflected in the arrangement?
- How is operational settlement achieved on the ledger and by whom? How does it differ from traditional systems?
- How is settlement finality provided for by the applicable legal framework?
- For exchange-of-value settlement, how is delivery versus payment, delivery versus delivery and payment versus payment achieved, including where relevant across autonomous ledgers or between a ledger and a traditional FMI?

3.3 Legal risk

- Does the arrangement have a clearly established, sound and enforceable legal basis for its activities, in particular if it operates in a multijurisdictional environment?
- How are potential conflicts of laws identified and addressed?
- What are the rights and obligations of the participants? How are they specified (for example, in rules, contracts or code)? What is the dispute resolution mechanism (for example, for liability issues)?

3.4 Governance

- What type of governance structure does the arrangement have? Does it support sound decision-making, risk management, incident and emergency response, and provide robust management oversight?
- Does the arrangement involve the sharing of information or maintenance of the ledger across entities? If so, who are the various stakeholders in the arrangement (including direct and indirect participants), and how does the governance structure define their respective responsibilities?
- Is there a clear mechanism for decision-making or agreeing on alterations to the arrangement?

3.5 Data management and protection

- How does the arrangement guarantee data integrity, including the traceability of data?
- Are the data considered immutable? If yes, how are data, transaction or processing errors addressed?
- How does the arrangement handle data privacy and confidentiality?

4. Potential broader financial market implications

4.1 Connectivity issues and standards development

- What system, platform, layer, or combination thereof is being considered or used in the arrangement?
- What protocol is being considered or used in the arrangement?
- Is the protocol code open source or proprietary? If proprietary, how flexible is the code in working with other arrangements?

4.2 Financial market architecture

- How does the arrangement change the role of existing intermediaries or involve new actors?
- How could the arrangement change existing market and regulatory practices?

4.3 Broader financial market risks

- Does the arrangement pose broader financial market risks at this stage of development and implementation? What risks could it pose in the future?
- What interconnections does the arrangement have with other systems, including other DLT arrangements?

Annex B: Members of the working group

Chairman	Klaus Löber (European Central Bank)
Reserve Bank of Australia	David Emery
National Bank of Belgium	Filip Caron
Central Bank of Brazil	Daniel Gersten Reiss
Bank of Canada	Wade McMahon
European Central Bank	Dirk Bullmann
Bank of France	Paul Capocci
Deutsche Bundesbank	Johannes Klocke (until October 2016) Heike Winter (from October 2016) Marcus Härtel (from October 2016)
Hong Kong Monetary Authority	Shu-pui Li (until November 2016) Nelson Chow (from November 2016)
Reserve Bank of India	Supriyo Bhattacharjee
Bank of Italy	Michela Tocci Giuseppe Galano
Bank of Japan	Shuji Kobayakawa Akiko Kobayashi
Bank of Korea	Dong sup Kim
Bank of Mexico	Angel Salazar Sotelo
Netherlands Bank	Kirsten van Driel
Central Bank of the Russian Federation	Vadim Kalukhov
Saudi Arabian Monetary Authority	Mohsen Al Zahrani
Monetary Authority of Singapore	Tze Hon Lau
South African Reserve Bank	Arif Ismail
Sveriges Riksbank	Björn Segendorf
Swiss National Bank	Marco Cecchini Nino Landerer
Bank of England	Simon Scorer
Board of Governors of the Federal Reserve System	David Mills Brendan Malone
Federal Reserve Bank of New York	Wendy Ng (until November 2016) Ray Fisher (from November 2016) Vanessa Lee
Secretariat	Paul Wong Emanuel Freire

Significant contributions were also made by Andrea Pinna (European Central Bank); Bas Koolstra (Netherlands Bank); and Ayse Sungur, Pankaj Setiya and Mario Griffiths (Secretariat).