Distributed ledger technology in payments, clearing, and settlement

David Mills, Kathy Wang, Brendan Malone, Anjana Ravi, Jeff Marquardt, Clinton Chen, Anton Badev, Timothy Brezinski, Linda Fahy, Kimberley Liao, Vanessa Kargenian, Max Ellithorpe, Wendy Ng, and Maria Baird[1]

2016-095

Please cite this paper as:
Mills, David, Kathy Wang, Brendan Malone, Anjana Ravi, Jeff Marquardt, Clinton Chen, Anton Badev, Timothy Brezinski, Linda Fahy, Kimberley Liao, Vanessa Kar- genian, Max Ellithorpe, Wendy Ng, and Maria Baird (2016). "Distributed ledger technology in payments, clearing, and settlement," Finance and Economics Discussion Series 2016-095. Washington: Board of Governors of the Federal Reserve System, https://doi.org/10.17016/FEDS.2016.095.

NOTE: Staff working papers in the Finance and Economics Discussion Series (FEDS) are preliminary materials circulated to stimulate discussion and critical comment. The analysis and conclusions set forth are those of the authors and do not indicate concurrence by other members of the research staff or the Board of Governors. References in publications to the Finance and Economics Discussion Series (other than acknowledgement) should be cleared with the author(s) to protect the tentative character of these papers.

Working Papers may be quoted without additional permission.

[1] The authors would like to thank Mari Baca, Daniel Ebanks, Sarah Wright, Thomas Doheny, Robert Carper, Patrick Adler, Peter Lee, Michael Warner, and Kaushik Ashodiya for their contributions and assistance. The views expressed in this paper are solely the responsibility of the authors and should not be interpreted as reflecting the views of the Board of Governors of the Federal Reserve System, or anyone else in the Federal Reserve System.

1. Overview

Digital innovations in finance, loosely known as fintech, have garnered a great deal of attention across the financial industry. Distributed ledger technology (DLT) is one such innovation that has been cited as a means of transforming payment, clearing, and settlement (PCS) processes, including how funds are transferred and how securities, commodities, and derivatives are cleared and settled. DLT is a term that has been used by the industry in a variety of ways and so does not have a single definition. Because there is a wide spectrum of possible deployments of DLT, this paper will refer to the technology as some combination of components including peer-to-peer networking, distributed data storage, and cryptography that, among other things, can potentially change the way in which the storage, recordkeeping, and transfer of a digital asset is done.

The driving force behind efforts to develop and deploy DLT in payments, clearing, and settlement is an expectation that the technology could reduce or even eliminate operational and financial inefficiencies, or other frictions, that exist for current methods of storing, recording, and transferring digital assets throughout financial markets. The purported benefits of DLT that could address these frictions, including improved end-to-end settlement speed, data auditability, resilience, and cost efficiency, have led industry participants to investigate the application of DLT to a wide variety of PCS processes. Proponents of the technology have claimed that DLT could help foster a more efficient and safe payments system, and may even have the potential to fundamentally change the way in which PCS activities are conducted and the roles that financial institutions and infrastructures currently play.

Although there is much optimism regarding the promise of DLT, the development of such applications for PCS activities is in very early stages, with many industry participants suggesting that real-world applications are years away from full implementation.[2] Even so, given the industry momentum in developing new proofs of concept (PoCs), this timeline may accelerate. In some cases, there have already been announcements that the technology will be used within the next year or two in actual production environments. An important goal of this paper is to examine how this technology might be used in the area of payments, clearing, and settlement and to identify both the opportunities and challenges facing its practical implementation and possible long-term adoption.

The Federal Reserve's interest in DLT

In the aggregate, U.S. PCS systems process approximately 600 million transactions per day, valued at over $12.6 trillion.[3] Given that safe and efficient arrangements for conducting PCS processes are critical to the proper functioning of the financial markets, and to financial stability more broadly, the benefits and risks that may arise with any potentially transformative changes to PCS processes should be thoroughly understood and managed by the relevant stakeholders. As part of its core objective to foster the safety and efficiency of the payment system and to promote financial stability, the Federal Reserve has a public policy interest in understanding and monitoring the development of innovations that could affect the

---

[2] *For example, technology research firm Gartner, which monitors emerging technologies, estimates that it will be five to ten years until DLT achieves "mainstream adoption." See Gartner (2016), "Hype Cycle for Emerging Technologies."*

[3] *Average daily volume and value were calculated using 2014 data on U.S. retail and wholesale PCS systems and were approximated based on the number of business days in the year. See Committee on Payment and Market Infrastructures (2015), Statistics on Payment, Clearing and Settlement Systems in the CPMI Countries, http://www.bis.org/cpmi/publ/d142.htm.*

structural design and functioning of financial markets.[4] Further, as a regulator and supervisor of financial institutions involved in PCS activities, an operator of retail and large-value payment and settlement systems, and a catalyst for payments system improvement, the Federal Reserve is also in a unique position to view the different implications of payments innovations from a wide range of perspectives.

As a preliminary step to understanding the implications of DLT developments in payments, clearing, and settlement, a team of Federal Reserve staff (FR research team) held discussions with a broad range of parties that are interested in, participate in, or are otherwise contributing to the evolution of DLT.[5] The team conducted interviews and conversations with approximately 30 key industry stakeholders, including market infrastructures, financial institutions, other government agencies, technology start-ups, more-established technology firms, and industry consortia. Additionally, the team attended numerous industry conferences and symposia and continues to engage with industry participants and follow developments related to the technology. This paper is informed by this outreach.

Organization of this paper

The paper is organized as follows. Section 2 provides a description of the essential elements of payments, clearing, and settlement, including an overview of the role financial intermediaries play.[6] Section 3 describes the key technological components of DLT and how they relate to the essential elements discussed in section 2. Section 4 describes several potential uses for DLT that were identified over the course of the research team's industry engagement and summarizes the approaches the industry is taking to investigate the potential of the technology. Sections 5 and 6 introduce some of the challenges to the adoption and implementation of DLT. Section 5 focuses on business, technology, and financial design challenges, while section 6 focuses on challenges related to risk management. Section 7 provides a summary.

2. Payments, clearing, and settlement

Many proponents in the fintech community have suggested that the widespread deployment of DLT may bring fundamental changes to not only the technology architecture of financial markets but also the financial market structure. This view stems from the perceived potential for DLT to facilitate certain PCS processes in ways that are not currently achievable without the aid of financial intermediaries that are entrusted by market participants, including households and businesses, with ensuring that their transactions are settled successfully on an on-going basis. As the first step in analyzing the potential impact of DLT on how activities in payments, clearing, and settlement are conducted, this section discusses the essential elements of PCS processes and how these processes have evolved with previous innovations, including how they have shaped the roles that financial intermediaries, such as financial institutions and infrastructures, currently play.

---

[4] *The Federal Reserve Board adopted its Federal Reserve Policy on Payment System Risk (PSR policy) with the objectives of fostering the safety and efficiency of payment, clearing, settlement, and recording systems and promoting financial stability, more broadly. The PSR policy includes the Board's views on standards for the management of risks (including legal, operational, and financial risks) in these types of systems. See Board of Governors of the Federal Reserve System (2016), "Federal Reserve Policy on Payment System Risk," Board of Governors, https://www.federalreserve.gov/paymentsystems/files/psr_policy.pdf.*

[5] *The research team is a multi-disciplinary group of officers and staff from the Board of Governors of the Federal Reserve System, the Federal Reserve Bank of New York, and the Federal Reserve Bank of Chicago.*

[6] *For purposes of this paper, a financial intermediary is broadly defined to include financial institutions (such as banks, broker/dealers, and other institutions that interact with the end-users of a financial transaction) and infrastructures (such as payment, clearing, and settlement systems for funds, securities, and derivatives).*

Essential elements of a financial transaction

In its simplest form, the clearing and settlement of a financial transaction, regardless of the asset type, requires (1) a network of participants, (2) an asset or set of assets that are transferred among those participants, and (3) a transfer process that defines the procedures and obligations associated with the transaction. Typically, the set of direct participants are financial institutions such as banks or broker- dealers. Indirect participants include end users such as households or businesses. An asset can be any financial instrument, such as a monetary instrument, security, commodity, or derivative.

Communications among the participants in a network involve sending electronic messages, acknowledgements, statements, and other information between computer systems typically maintained by a network operator and its participants. Payments and post-trade securities clearing and settlement are characterized by somewhat different transfer processes and may involve different types of financial intermediaries, as described in sections 2.1.1 and 2.1.2., respectively.[7] Section 2.1.3 describes further the role(s) of financial intermediaries that facilitate today's PCS processes.

Payments processes

For a funds-only transfer, the process involves a series of four conceptual steps that are called submission, validation, conditionality, and settlement. These processes are generally facilitated by financial intermediaries, such as payment systems.[8] After a sender submits a payment message to a payment system, the message must pass through that system's validation procedures. Validation will vary by system and can include security measures, such as verification of the sender's identity and the integrity of the message. If a payment is determined by the system to be valid, the system then typically checks whether necessary conditions for settlement are satisfied, such as the availability of sufficient funds or credit for settlement. Payments that pass the conditionality test are prepared for settlement. Under some payment system frameworks, settlement finality (that is, when settlement is unconditional and irrevocable) occurs when the receiver's account is credited.

Securities, commodities, and derivatives post-trade processes

For securities, commodities, and derivatives transactions, post-trade processes provide confirmation of trade terms, clearing, and settlement. In many cases, these processes are facilitated by financial intermediaries, such as payment systems, securities settlement systems (SSSs), central securities depositories (CSDs), and central counterparties (CCPs), which specialize in particular PCS functions.[9,10]

---

[7] *The discussion in sections 2.1.1 and 2.1.2 are based on Annex D of the following: Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commissions (2012), Principles for Financial Market Infrastructures, http://www.bis.org/cpmi/publ/d101a.pdf. Effective September 2014, the Committee on Payment Settlement Systems changed its name to the Committee on Payments and Market Infrastructures.*

[8] *A "payment system" is defined in the PSR policy as a set of instruments, procedures, and rules for the transfer of funds between or among participants. Payment systems include, but are not limited to, large-value funds transfer systems, automated clearing house systems, check clearing houses, and credit and debit card settlement systems. See Board of Governors of the Federal Reserve System (2016), "Federal Reserve Policy on Payment System Risk," Board of Governors, https://www.federalreserve.gov/paymentsystems/files/psr_policy.pdf.*

[9] *A "securities settlement system" is defined in the PSR policy as an entity that enables securities to be transferred and settled by book entry and allows the transfers of securities free of or against payment. A "central securities depository" is defined in the PSR policy as an entity that provides securities accounts and central safekeeping services. A "central counterparty" is defined in the PSR policy as an entity that interposes itself between counterparties to contracts traded in one or more financial markets, becoming the buyer to every seller and the seller to every buyer. See Board of Governors of the Federal Reserve System (2016), "Federal Reserve Policy on Payment System Risk," Board of Governors, https://www.federalreserve.gov/paymentsystems/files/psr_policy.pdf.*

[10] *In some cases, one entity may perform multiple PCS functions, such as securities clearing and settlement, as well as safekeeping and custody.*

Confirmation involves counterparties agreeing to the terms of the trade and settlement date. The next step is clearing, in which an entity calculates the counterparties' obligations to make deliveries or payments on the settlement date. This entity may compute settlement obligations individually (that is, on a transaction-by-transaction basis) or on a net basis (that is, determining the net obligations of buyers and sellers for a number of transactions).

After clearing comes settlement, during which the relevant delivery and payment obligations of the counterparties to the securities, commodities, or derivatives transaction are discharged. For example, in a securities transaction, settlement occurs when securities are delivered to the buyer and funds to the seller. Depending on the commodity and terms of settlement, commodities transactions may involve settlement of only funds obligations, or it may also involve the delivery of financial instruments, other documents, or even a physical commodity (e.g., precious metals, oil, wheat, etc.). The settlement of derivatives contracts other than commodity contracts also depend on the type of derivative and terms of settlement. Finality of each leg of the transaction occurs when the transfer is irrevocable and unconditional. When there are multiple legs in a transaction, delivery versus payment (DvP) mechanisms are often used to coordinate settlement of the different legs, as well as manage the risk that one leg settles with finality when the other does not.[11]

Roles of financial intermediaries in payments, clearing, and settlement

Certain institutions serve as intermediaries in payments, clearing, and settlement and may play one or more critical roles in fostering the smooth functioning of the broader financial system. These roles generally include the provision of services as well as financial, operational, and legal risk management, and a governance structure for them, their customers, and the markets they serve.

Intermediaries such as banks and broker-dealers are typically trusted by end users, such as households and businesses, to store, maintain ownership records of, and transfer assets on their behalf. When these end users initiate a transaction, their banks or broker-dealers interact with other intermediaries, such as financial market infrastructures (FMIs), that can take the form (and function) of a payment system, SSS, CSD, or CCP.[12] FMIs centralize and facilitate the clearing, settlement, and recording of financial

transactions for the markets they serve, often on a multilateral basis. In doing so, FMIs can allow participants to manage their risks more effectively and efficiently and may reduce certain risks.[13]

The transfer process is typically organized with the FMI as a central hub through which banks or broker-dealers interact with one another. Because banks and broker-dealers may be active in multiple financial markets, they often interact with multiple FMIs. Figure 1 depicts a very simple hub and spoke system with one FMI and its participants. In the figure, the FMI has a master copy of the transactions ledger for trades that go through it. Each participating financial institution has its own ledger of transactions which may include both transactions that go through FMI A and transactions that do not. In practice, FMI A may have multiple ledgers organized by business line, operational activity, geographic area, or accounting center. The reconciliation within and among the various parties to a transaction may occur as part of the clearing process or daily balancing activities. Some reconciliation steps may take place after individual

[11] *For a description of the different models, see Annex D of the following: Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commissions (2012), Principles for Financial Market Infrastructures, http://www.bis.org/cpmi/publ/d101a.pdf. See also Committee on Payment and Settlement System (1992), Delivery Versus Payment in Securities Settlement Systems, http://www.bis.org/cpmi/publ/d06.htm.*

[12] *A "financial market infrastructure" is defined in the PSR policy as a multilateral system among participating financial institutions, including the system operator, used for the purposes of clearing, settling, or recording payments, securities,*

[13] *However, FMIs may also concentrate risks and create interdependencies between and among FMIs and participating institutions.*

transactions have been settled.

The broader financial system contains numerous hub and spoke systems that are intricately linked through, among other things, the PCS relationships between entities ranging from end-users to intermediaries. Figure 2 depicts a stylized example of how the simple hub-and-spoke structure is essentially more complex because of the interconnectedness of various participants. Financial institutions may often participate in multiple FMIs, as shown by FI 2 in figure 2. Further, participation in derivatives, or other financial transactions. See Board of Governors of the Federal Reserve System (2016), "Federal Reserve Policy on Payment System Risk," Board of Governors, https://www.federalreserve.gov/paymentsystems/files/psr_policy.pdf.

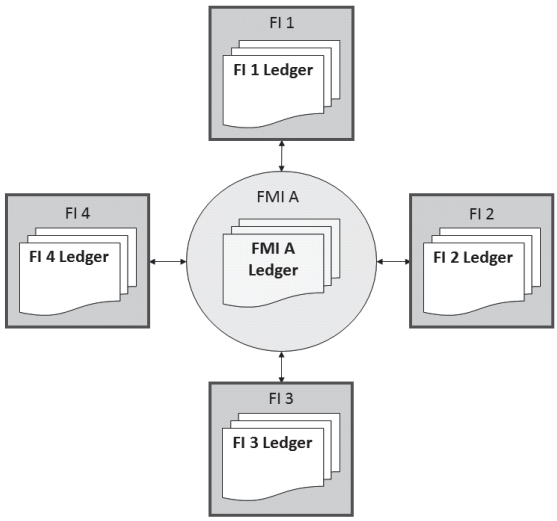

Figure 1: Simple example of a hub and spoke structure with one FMI and financial institutions (FIs) as participants

FMIs may cross jurisdictional boundaries, as shown by the connections of FI 6 and FI 7 in figure 2, which adds another layer of legal and operational complexity.[14]

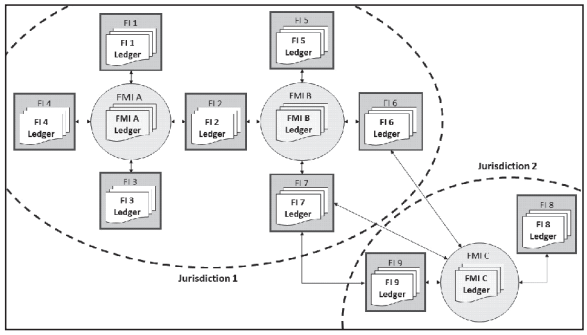

Figure 2: Example of a more-complex hub and spoke structure with multiple FMIs, FIs, and jurisdictions

Innovations in payments, clearing, and settlement

The methods for executing, clearing, and settling financial transactions have evolved over centuries.[15] As transaction volumes and the complexity of market participants increased, certain frictions emerged and increased the costs as well as the risks of transacting in financial markets. Frictions, such as operational and financial inefficiencies, prompted market participants to seek solutions that would reduce costs.

Solutions to these inefficiencies, in turn, took the form of technological development, changes in market structure (for example, formation of new intermediaries or changes to the roles of existing intermediaries), or a combination of the two.[16] The availability and maturity of technology are key factors in determining the extent to which a technological solution versus a change to the market structure would serve to address a particular friction or inefficiency.

---

[14] *For an example depiction of this complex set of linkages in the derivatives market, see figures 1 and 2 in Jerome Powell (2014), "A Financial System Perspective on Central Clearing of Derivatives," speech delivered at "The New International Financial System: Analyzing the Cumulative Impact of Regulatory Reform", a conference sponsored by the Federal Reserve Bank of Chicago and the Bank of England, held in Chicago, Illinois, November 6, 2014, https://www.federalreserve.gov/newsevents/speech/powell20141106a.pdf.*

[15] *Trade execution takes place before PCS processes, but is referenced here for illustrative purposes.*

[16] *One example in which a change in market organization and structure provided a solution to an operational inefficiency was the formation of check clearing houses. The New York Clearing House was formed in the 1850s for the purposes of interbank check collections, before computer technology was available to address the increasingly cumbersome physical settlement of checks by payment in gold among multiple banks. As a result, the settlement process itself was redesigned by introducing a new facility that centralized physical check clearing and settlement on a multilateral basis in one location. Many other local or regional check clearing houses were subsequently created around the United States. See J.S. Gibbons (1859), the Banks of New- York, Their Dealers, the Clearing House, and the Panic of 1857 (New York: D. Appleton & Co), pp. 292-295.*

Often, the introduction of a new technology necessitates a change in market structure. One such example was the introduction of advanced communications networks and electronic databases to the physical processes associated with clearing and settling paper stock certificates. This evolution reduced both the liquidity and operational costs required to complete a geographically diverse, multi-party transaction and was aided not only by the technical ability to produce digital representations of physical certificates or assets, but also by the changing roles of financial intermediaries.

New FMIs were created to play the roles of CSDs and, in some cases, CCPs. These market infrastructures assumed the responsibility and legal liability of ensuring that valid transactions submitted by banks and broker-dealers for themselves and their customers were cleared and settled. The CSDs, which often also operate as SSSs, provided the storage and recordkeeping of ownership of securities by their members and facilitated funds and securities transfers by providing trust, and in many cases, liquidity, throughout the transfer process. If CCPs were also created for a particular market, they would frequently provide the clearing function and, importantly, would typically provide a "guarantee" of settlement between shortly after the trade date until the settlement date of the transaction.[17] Broker-dealers and banks fulfilled their roles, in part, by maintaining various independent ledgers for recording and posting debits and credits to customer funds and securities accounts on those ledgers. As trusted intermediaries with sole authority to update their own electronic transactional databases (that is, ledgers) within their purview, the different financial intermediaries worked under rules and governance processes that provide the necessary integrity and reliability for end users to have confidence in the transfer process.

Opportunities for new innovations in payments, clearing, and settlement

Innovations have made way for the bulk of today's payments, clearing, and settlement in the wholesale and retail financial markets to be conducted over a set of large and complex electronic networks of participants and processes. Taken together, these comprise the financial architecture and are often broadly called the U.S. payment system. There remain, however, opportunities for improvement.

Traditional payment services, often operating on decades-old infrastructure, have adjusted slowly to changes in technology, increasing end-user expectations for speed and convenience, and increases in security threats.[18] DLT represents an opportunity to deal with existing frictions in payments, clearing, and settlement (section 4) and, as stated above, may cause market structure changes. The extent of these changes, however, depends on how the financial industry addresses certain challenges to implementation and adopts the technology. Before examining these challenges, this paper first considers the technological components of DLT and how they may be applied in the PCS context.

---

[17] *An important element of any CCP design is the legal mechanism for the CCP to become the counterparty to its participants' trades (such as through innovation and substitution of counterparties), which allows the CCP to assume the original parties' contractual obligations to each other. Other legal mechanisms that allow the CCP to guarantee obligations may also exist, such as explicit and legally binding settlement guarantees.*

[18] *Federal Reserve System (2015), "Strategies for Improving the U.S. Payment System," white paper, January 26, https://fedpaymentsimprovement.org/wp-content/uploads/strategies-improving-us-payment-system.pdf*

3. Distributed ledger technology

In the strictest sense, a distributed ledger is a type of database that is shared across nodes in a network.[19] However, because the financial industry is considering a wide range of applications for the technology, this paper considers "distributed ledger technology" in a very broad sense to be some combination of components, including peer-to-peer networking, distributed data storage, and cryptography that, among other things, can potentially change the way in which the storage, recordkeeping, and transfer of a digital asset is done. The composition of these combinations is dictated by the particular friction or inefficiency a particular implementation of DLT is designed to solve.

In order to differentiate between the broader topic of DLT and specific implementations of DLT, this paper refers to a "DLT arrangement" when describing a particular selection, combination, or configuration of these technological components. These arrangements could take a number of forms, that, when implemented, range from having a minimal to a very significant impact on how PCS processes are conducted. For example, existing financial intermediaries may adopt a few of the key components of DLT as an enhancement to their existing technical platforms. This type of incremental adoption may not change any underlying business, operational, or behavioral practices supporting the PCS process. At the other extreme, a comprehensive DLT arrangement might be implemented to replace entire functions traditionally managed by existing financial intermediaries (that is, entire PCS processes). This type of comprehensive approach might result in very significant changes to the architecture of the financial system for conducting payments, clearing, and settlement. For example, in very extreme but unlikely scenarios, the use of banks to conduct payments could become obsolete. In between these extremes lie a number of potential future states for the financial architecture.

The extent to which DLT will have an impact on the financial architecture may become clearer as the technology matures. The level of impact will depend at least in part on decisions about which components of DLT are adopted and how DLT arrangements are ultimately implemented. As the industry considers a wide variety of applications, DLT arrangements are likely to take on a range of forms, with different components of the technology being used for different purposes. Thus, this section reviews some of the key components of DLT that could be adopted in the context of payments, clearing, and settlement.

Entities can be connected on a peer-to-peer basis via nodes

In a DLT arrangement, nodes are the devices running the DLT software that collectively maintain the database records. In this design the nodes are connected to each other in order to share and validate information.[20] At its extreme, this structure enables any entity, such as end-users, financial institutions, or FMIs, with a node to share database management responsibilities directly with each other on a peer- to-peer basis. This is in contrast to traditional database architectures that operate with a central hub that acts as the single source of valid information and control. Outside of the conduct of PCS processes,

DLT also enables a single party to maintain its database records across multiple nodes, for purposes including increased operational resiliency.

[19] *One specific type of distributed ledger is a block chain, which adds changes to the database via a series of blocks of transactional data that are chronologically and cryptographically linked to one another. The terms "distributed ledger technology" and "block chain technology" are often treated as synonyms in the industry even though block chain is actually a specific type of distributed ledger.*

[20] *Communication channels between nodes may be separate from the channels used by end users to access the nodes or the institutions that maintain them.*

Figure 3 represents two examples of this peer-to-peer connectivity. In contrast to the hub-and-spoke model of figure 1, in which each entity maintains its own independent ledger, each node in figure 3 has a copy of a common ledger. Further, although the connectivity of the nodes is the same between the two panels of figure 3, the ownership and housing of the nodes are different. In the left panel, the nodes are hosted within a single entity. In the right panel, however, multiple entities are in the arrangement, and each of them hosts a node. Section 3.9 will discuss the importance of this distinction.

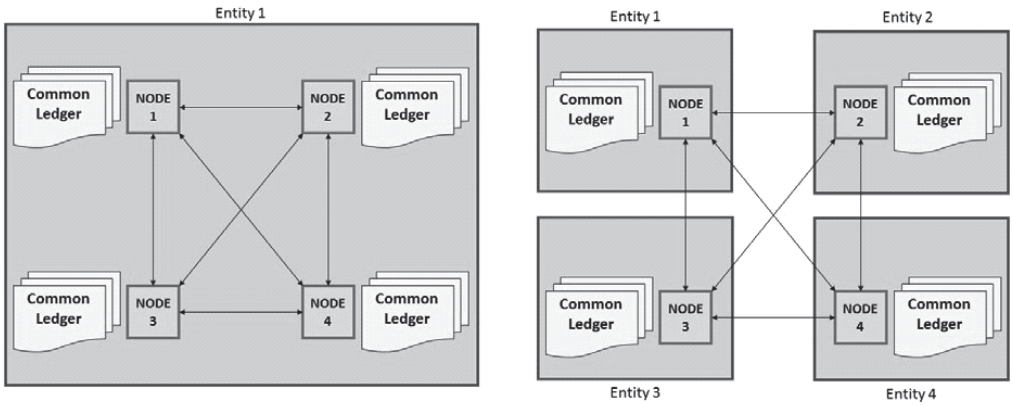

Figure 3: Two simple examples of node connectivity structure

An entity's ability to participate in a DLT arrangement, however, depends not only on that entity's computing resources (i.e., operational capabilities) for running nodes, but also on whether the arrangement is designed to be an open or closed system. Open systems are those that accept all interested entities that have the technical ability to participate. Closed systems have additional membership criteria that must be satisfied in order for an entity to be permitted to operate a node. These criteria can include financial requirements such as the entity's creditworthiness or ability to access liquidity resources, as well as legal requirements such as the entity's ability to meet any contractual obligations to the arrangement or to have proper business licenses to conduct business. Crypto currency DLTs such as Bitcoin are generally open systems. Many DLT arrangements being contemplated by the financial industry, however, are envisioned as closed.[21]

Participants in a DLT arrangement can be permitted to play different roles or functions

Regardless of whether a DLT arrangement is open or closed, participants (and therefore the nodes they maintain) may be differentiated by the roles they are permitted to play or functions they are permitted to perform. DLT arrangements in which the participants are allowed to perform all activities are often called "permissionless." Those that restrict participants' activities are often referred to as "permissioned." For example, for certain DLT arrangements, some participants may only be permitted to have nodes that send and receive asset transfers for existing assets. Other participants may have the ability to issue new assets. Still others may have permissions to validate transactions (as discussed below), while another set of participants may be able to update the history of transactions to the ledger (also discussed below).

[21] *In the context of Figure 3, the left panel is a clear example of a closed DLT arrangement, as all the nodes are hosted by a single entity. The right panel, however, could represent either an open or closed arrangement. The determining factor of which is whether the entities that host the nodes also needed to meet additional criteria to be permitted to participate in the arrangement.*

Some participants may be limited to only reading the ledger, while others may also be allowed to write to the ledger. Crypto currency DLT arrangements such as Bitcoin are examples of permissionless systems. The financial industry, however, is focused mainly on developing permissioned systems because these systems offer a way to provide controls over important functions performed in the arrangement.

Ownership of an asset can be stored on a ledger within the DLT arrangement

Assets can be designed in a variety of ways. For example, they can be issued and traded entirely within the ledger or they can be representations of assets that exist outside the ledger. Regardless, ownership information with respect to an asset can be stored on a ledger within the DLT arrangement, which maintains the ownership positions of all participants in the system. The asset owner within the DLT arrangement could be financial institutions such as banks or broker-dealers, much like today. In a more extreme scenario where services are disintermediated, these assets could be held directly by households and businesses.

DLT arrangements can use cryptography to facilitate PCS processes

DLT arrangements use cryptography for several purposes, such as identity verification and data encryption. For example, during asset transfers, a form of cryptography known as public key cryptography usually forms the foundation of the transaction validation process.[22]

To transfer an asset, a participant may create what is known as a digital signature with its non-shared cryptographic credential called a private key. To confirm that the asset in question belongs to the participant initiating the transaction, other participants of the DLT arrangement with the required permissions to act as validators of transactions can verify authenticity of the ledger entry by decrypting it with a mathematical algorithm and the asset owner's publicly available public key. As a consequence of this process, ownership of an asset, including the ability to transfer it to other parties, often depends on having access to the correct private keys.[23]

Additionally, cryptography may be used to encrypt transactional information on the ledger such that only certain participants can decrypt the details of each transaction. Since most DLT arrangements require some level of distribution of records on the ledger, cryptography employed for this purpose can be an important tool in instances where some degree of privacy is necessary.

Finally, cryptography can also be used to facilitate the consensus process discussed in 3.6.

Transactions histories and current states of ownership can be distributed across the nodes of the DLT arrangement

In a DLT arrangement, information regarding records of ownership and transaction histories can be distributed across the nodes in the network. Importantly, this distribution is the foundation of the technology, with the ledger of transaction histories

---

[22] *Public key infrastructure (PKI) is the name given to the set of entities and procedures that govern the creation, distribution, and validation of public keys. With respect to some implementations of DLT, roles and procedures played by specific entities in the traditional PKI framework may be executed by the DLT protocol and thus may not require centralized authority or control. For additional information on public key infrastructure, see U.S. Department of Commerce, National Institute of Standards and Technology (2013), Digital Signature Standards (DSS), http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf, and U.S. Department of Commerce, National Institution of Standards and Technology (2001), Introduction to Public Key Technology and the Federal PKI Infrastructure, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf.*

[23] *U.S. Department of Commerce, National Institute of Standards and Technology (2013), Digital Signature Standards (DSS), http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.*

and ownership positions shared as one common ledger that participants agree is correct. Important design choices for this ledger include the appropriate level of information that should be contained and shared on the ledger and which participants have the ability to read or write to the ledger. Typically, even if all nodes have a complete copy of the ledger, it is technologically possible that some of the data on the ledger is encrypted so that only authorized participants can decrypt and read the underlying information.

The protocol in a DLT arrangement can define the procedures necessary for the asset transfer process

For DLT arrangements intended for facilitating payments, clearing, or settlement, the PCS processes are coded into a protocol, which is a syntax and set of procedures that define how members of the arrangement interact. For a payment transfer, a DLT protocol may lay out validation checks (for example, verify ownership) and conditionality checks (for example, access to sufficient funds or credit). For a securities, commodities, or derivatives transfer, a DLT protocol could provide the conditions around confirmation, clearing, and settlement.

An important difference in these protocols and processes between today's financial architecture and a DLT arrangement is the process for settlement. Settlement in a DLT arrangement involves the updating of the common ledger with the new ownership positions of the relevant counterparties. For a distributed ledger, proposed transactions and subsequent positions are broadcast to nodes that maintain a copy of the ledger and ultimately accepted as the new version of the ledger.

The process of having nodes accept a new version of the ledger is commonly referred to as consensus, which is consequently an important part of sharing a common ledger in a peer-to-peer network.

Because multiple participants typically have the ability to write to the common ledger, it is possible that two seemingly valid transactions could be broadcast to the network at the same time. For example, a sender of funds may be able to submit a payment using funds that are already allocated to a previous payment before the sender's previous transaction is reflected in the ledger. This possibility is the so- called “double-spend problem,” which arises in an environment where settlement may not occur instantaneously and is not under a single decision maker's control.[24]

DLT arrangements use consensus algorithms or other similar processes as a way for nodes on the network to prioritize one valid transfer over another so that only one transfer is accepted and posted to the common ledger and the other is ultimately rejected.

Specific to protocols and processes for validation of transactions, the design of consensus algorithms used in a DLT arrangement can help to prevent invalid transactions from being accepted by the system and can also make the ledger more tamper-resistant. These processes may also be designed to address specific aspects of types of transactions. For example, transfers over a certain threshold could trigger additional validation steps or alternative consensus rules to be applied before the transaction is accepted in the ledger.

[24] *In both DLT arrangements and traditional payment systems, the double-spend problem may arise, for example, if identical, duplicate payments or transfers can be sent even when only one payment or transfer can be valid. In a DLT arrangement, an example would be multiple simultaneous attempts to transfer a digital asset with the same serial number or unique identifier. Note that a related but not identical problem can occur if a party attempts to make two valid transfers, but owns an insufficient amount of a digital asset to settle both transfers.*

The design of a DLT arrangement's protocols, however, can have consequences for the scalability and performance characteristics of the overall DLT arrangement. For example, the choice of consensus model may affect the rate at which transactions can be processed and considered final by the arrangement. For this reason, the industry is currently researching a number of consensus algorithms that it hopes will reduce this latency and increase the scalability of DLT arrangements.

Application programming interfaces can improve usability of DLT arrangements

Application programming interfaces (APIs) are a set of routines, protocols, and tools for building software applications. An API specifies how software components should interact, and within a DLT arrangement APIs can enable the addition of new features or enhancements not native to the distributed ledger protocol itself. For example, they could communicate directly with the underlying protocol of a distributed ledger to effect transfers and gather information. APIs can also provide user-friendly interfaces that make using the technology easier for a broader set of potential users. These applications can be customized to meet the needs of particular asset types or markets. As the number of DLT arrangements using different protocols increases, APIs may play a critical role in improving usability and interoperability between different protocols and between protocols and legacy systems.

Smart contracts may be used in DLT arrangements to automate certain transfers based on pre-specified events agreed to by counterparties to a transaction

Smart contracts are coded programs that are used to automate pre-specified transactional events based on agreed upon contractual terms. Like with traditional contracts, a smart contract depends on participants' consent to its terms. These agreed-upon smart contracts can be used in conjunction with a distributed ledger to self-execute based on information received in the distributed ledger or from other sources. For example, several companies developing DLT products are exploring the use of smart contracts to model corporate debt issuances. In these simulations, a debt-issuing company specifies the parameters of the contract, such as its par value, tenor, and coupon payment structure. Once assigned to an owner, the smart contract would automatically make the required coupon payments until the bond reaches maturity.

DLT implementation can be considered from a legal entities perspective in addition to a technology perspective

As noted in the beginning of section 3, the extent to which DLT will have an impact on the financial architecture may become clearer as the technology matures. Some proponents of DLT point to the possible use of the technology to automate and even replace functions traditionally played by financial institutions and FMIs. Nonetheless, information technology is only one factor that typically influences the function and organization of PCS processes. Other factors include business, coordination, and network economics as discussed in section 5. Legal issues, as discussed in section 6, also loom large.

From a fundamental perspective, certain types of legal entities appear necessary to carry out ordinary PCS activities even as some of their functions and operations may adjust with the advent of new technologies.

For example, CCPs for derivatives are inherently designed to be the buyer to every seller and the seller to every buyer when they are used to centrally clear either exchange traded or over-the- counter derivatives. In order to effectively carry out the CCP

function, some type of central legal entity appears to be necessary; this type of entity is essentially a financial intermediary.[25]

With respect to CCPs for cash securities trades, there is discussion of whether concepts like real-time clearing and settlement of such trades would make unnecessary, the use of CCPs to guarantee trades between trade execution and final settlement. This is a logical possibility and could be a case of technology used in a way that makes the need for a settlement guarantee obsolete. However, markets will likely need to evaluate the costs and benefits of the types of changes that financial institutions and FMIs would need to implement for real-time clearing and settlement as well as the financial issues involved in faster settlement such as liquidity management.[26]

It may also happen that if there is a business case for real-time settlement in the securities markets, DLT would be only one of the technologies considered for implementation.

Additionally, traditional financial assets such as securities are typically a liability of a legal entity, such as a government or corporation. In a DLT arrangement, decisions about what type of entities can issue what instruments on a distributed ledger may be important to provide a firm legal foundation for DLT activity. Moreover, entities such as custodians may be needed to effectively control and manage the issuance of digital assets – potentially from a significant number and wide range of issuers – onto distributed ledgers, much like how securities custodians have been used since the 1970s to immobilize securities certificates and issue book-entry securities against them. Such intermediaries may not be technologically necessary to make the use of DLT feasible, but their use could result from the economics of issuing and managing securities, including the need to meet regulatory requirements.

Financial institutions acting for their own accounts and on behalf of clients may wish to hold and trade digital assets and to manage various risks. Some of these types of intermediaries have emerged already to provide services to Bitcoin users, even though Bitcoin is an open system in which anyone may hold the crypto currency directly. More generally, third-party service providers currently provide a wide range of technology and other services to financial institutions and their clients, which creates an "ecosystem" of financial and non-financial entities that are frequently involved in producing and delivering PCS services. Overall, the economics of intermediaries will likely continue to be more complex than a simple problem of technology or technology costs.

A particularly important and traditional issue in PCS economics is the need for groups of firms and individuals to coordinate PCS activity to reduce the costs and risks of clearing and settlement. In addition to legislation and regulation, governments and the private sector have historically established rule-setting bodies, clearing houses, and specialized financial institutions to address the need for multilateral rules and functions.[27]

Depending on the era, the jurisdiction, and the problem being addressed, some of these multilateral organizations have also been given roles as financial intermediaries. Although technology has been one

[25] *Even in the pre-2008 environment of voluntary central clearing of standardized over-the-counter derivatives, CCPs existed and performed important functions such as clearing interest rate swaps for major dealers.*

[26] *For information on the issues considered by the industry on the plan to shorten the settlement cycle of U.S. equities from three days after trade date (i.e., T+3) to T+2, see Industry Steering Committee (2015), White Paper: Shortening the Settlement Cycle: The Move to T+2, http://www.ust2.com/pdfs/ssc.pdf. For additional information on the initiative to move to T+2, see the industry T+2 website at http://www.ust2.com/.*

[27] *Associations of financial institutions have also been used to establish model master agreements used in bilateral clearing.*

contributing factor in determining the design of a particular PCS arrangement, the fundamental need for coordination has often required joint action through new or existing legal entities to, at a minimum, provide organization and governance.

4 Potential opportunities for DLT in payments, clearing, and settlement

Industry participants and technology firms are increasingly exploring ways to develop and deploy DLT arrangements for use in payments, clearing, and settlement. Although the technology has the potential to provide a new way of storing, recording, and transferring digital assets, at present most industry participants are looking at ways to integrate the technology into existing systems and institutions. Many models may alter or eliminate some roles of current intermediaries in payments, clearing, and settlement but may not necessarily eliminate the need for coordination or centralization of certain functions by trusted intermediaries. These trusted intermediaries could still be needed to play important roles in addressing frictions beyond what DLT may be able to accomplish or may be able to use DLT arrangements to improve or evolve how they accomplish their respective missions.

Path to adopting new technology

The path to adoption of any new technology, including DLT, typically follows several stages of development, beginning with a "proof of concept."[28]

These PoCs are simple, experimental uses of the technology on a very small scale in a controlled environment (for example, nonproduction) and are often used to help researchers understand the potential and limits of a technology for a specific purpose. At this stage, some important aspects of the technology and operations that are critical in a production environment, such as scalability or security, may not be fully understood or addressed. Much of the industry has been working on PoCs in 2016, usually for particular asset classes and use cases. Some of these PoCs are referenced below.

PoCs that show potential may move into the pilot phase in which the technology could be used for real transactions. Pilots have a limited duration, defined objectives and milestones, and typically also limit the number of participants in order to determine how the technology works in production. Technologies that are successful in the pilot phase may then move toward the production stage. Technologies at this stage have the full set of features necessary to facilitate the storage, recordkeeping, and transfer of the asset being considered. The final stage of the development process is broad adoption of the technology by participants in the payments, clearing, and settlement system. At the time of the FR research team's interviews, most of the DLT experimentation was at the PoC stage. There have been some announcements of the intent to put distributed ledger technology into production.

Potential applications of DLT in payments, clearing, and settlement

Information collected through interviews with industry stakeholders indicates that firms have several common motivations behind efforts to develop and deploy DLT arrangements:

- Reduced complexity (especially in multiparty, cross-border transactions)
- Improved end-to-end processing speed and availability of assets and funds
- Decreased need for reconciliation across multiple record keeping infrastructures

[28] *Scott Campbell (2013), "POC vs. Pilot vs. Production," January 25, https://www.citrix.com/blogs/2013/01/25/poc-vs-pilot-vs-production/. See also National Defense Industrial Association 2008, "Engineering for System Assurance", Version 1.0, pp. 84, http://www.acq.osd.mil/se/docs/SA-Guidebook-v1-Oct2008.pdf.*

- Increased transparency and immutability in transaction record keeping
- Improved network resiliency through distributed data management
- Reduced operational and financial risks

DLT is essentially asset-agnostic, meaning the technology is potentially capable of providing the storage, recordkeeping, and transfer of any type of asset. This asset-agnostic nature of DLT has resulted in a range of possible applications currently being explored for uses in post-trade processes. The following section describes a set of "use cases" identified during the industry interviews and discusses, among other uses, post-trade clearing and settlement, cross-border payments, and financial inclusion. For each potential use, the industry has noted a set of existing frictions that might be addressed by DLT technology and developed one or more PoCs to explore major issues in developing and applying the technology further. The PoCs also suggest that DLT arrangements may introduce new challenges to potential uses, and as a result, sections 5 and 6 will discuss questions that will need to be addressed in order to transition from the PoC stage to widespread adoption.

Securities, commodities, and derivatives transactions

Many organizations are particularly interested in identifying which aspects of post-trade processing could benefit from DLT's potential to reduce information transfer times from trade execution to settlement, and thus to increase the speed and efficiency of the operations that influence the length of settlement cycles. In theory, the distributed and consensus forming aspects of DLT could allow for multiple parties to agree on the terms of trades in a fraction of the time required with existing processes. In addition, some contend that eliminating other frictions in clearing, such as reconciliation across various independently managed ledgers, would allow market participants to reduce processing delays and operational costs.Specific use cases that have received public attention include clearing and settlement in equities markets as well as international commodities markets. For example, several large exchanges are exploring DLT-based solutions to improve existing post-trade processes for clearing and settling trades made on exchanges. These exchanges are developing PoCs to track ownership of digital representations of securities in order to potentially combine the trade and post-trade processes for asset transfers into one step. For commodities markets, a DLT arrangement is in development to potentially allow for more efficient transfers of commodity "certificates" tied to specific physical assets such as precious metals.

Both examples connect with legacy payments systems for the payments leg of an asset transfer. Thus, interoperability between the DLT arrangement and legacy systems becomes an area of focus because final settlement is tied to the completion of both legs of a securities or commodities transfer (as discussed in section 6.3). The industry has been focusing on ways to make those connections, including the establishment of escrow accounts that interact with or are within a DLT arrangement. These escrow accounts would hold onto one side of the transaction until confirmation that the other side is executed.

The potential for DLT to reduce frictions in the clearing and settlement of securities has led many industry participants to explore this technology as a way of reducing middle and back office costs. For example, many such costs are driven by procedures that must be done manually or duplicated at multiple firms. During securities trades, all parties typically keep duplicative records of the trade details, requiring costly reconciliation between firms. DLT arrangements are being developed to, among other things, share the costs of maintaining such recordkeeping infrastructures.

Cross-border payments

Numerous firms have identified the slow, indirect, and expensive settlement of cross-border payments as a current point of friction that could be alleviated through the application of DLT arrangements.

Currently, electronic cross-border payments are effected by credit (and sometimes debit) transfers that convert funds from bank to bank through a series of correspondent banking relationships, often with an assessment of multiple fees.[29]

Although actual message communication between banks, using "straight- through-processing," can take place in near real time, correspondent banks may not act on messages promptly, and settlement may take longer. Exception processing can take even longer. According to one report, the settlement times for cross-border payments can take up to five days for the most common currency pairings, generally with limited clarity regarding the total amount of fees to be charged and the timing of settlement.[30]

Depending on the jurisdiction and the banks involved, costs are generally passed on to the end-users and may be deducted from the face amount of the funds transferred. For the end-user, the frictions include the predictability of settlement timing and costs, as well as the general opaqueness of correspondent banking networks. For small to medium-sized banks that offer such services to their customers but often lack the relationships to directly process cross-border payments, the frictions include the reliance on larger institutions, the associated costs of maintaining relationships, and the associated fees and timing of settlement for payments. Frictions may also include problems in exception processing and reconciliation.[31]

Some startups are attempting to alleviate some of these frictions by using DLT and more direct transacting as a replacement for intermediaries, which potentially reduces the number of steps to complete cross-border payments and enables direct relationships between counterparties. Developers argue that certain attributes of DLT, such as the ability to share ledgers across geographic distances and time-zones, could reduce the number of intermediaries needed to effect cross-border payments. By reducing the number of intermediaries, certain regional banks may be able to directly access the network, resulting in a more transparent and efficient cost structure for cross-border payments. Some of these cost savings could then potentially be passed onto their customers.

In addition, a particular industry development of note is the Inter ledger Protocol (ILP) which allows transactions to flow across different ledgers and creates connection points between two or more digital ledgers. In effect, the protocol defines a set of procedures for proposing a payments path and cryptographically escrowing funds across a series of interoperable ledgers and then subsequently executing the escrowed transactions once the recipient of the payment validates or acknowledges receipt of payment. The ILP is being developed as an open standard and is intended to improve interoperability and streamline the process for transferring digital assets by enabling entities in different countries with different payment systems to more easily transact with one another.

---

[29] *Committee on Payment and Market Infrastructures (2016), Correspondent Banking, http://www.bis.org/cpmi/publ/d147.pdf.*

[30] *McKinsey and Company (2015), "Global Payments 2015: A Healthy Industry Confronts Disruption," October, pp. 23-24, http://www.mckinsey.com/~/media/McKinsey/dotcom/client_service/Financial%20Services/Latest%20thinking/Payments/Global_payments_2015_A_healthy_industry_confronts_disruption.ashx.*

[31] *Lipis and Adams (2014), SWIFT Institute, "Cross-Border Low Value Payments and Regional Integration: Enables and Disablers," November, https://www.swiftinstitute.org/wp-content/uploads/2014/11/SWIFT-Institute-Working-Paper-No-2014-005-Cross-border-LVP-Regional-Integration-Lipis_v4-FINAL.pdf. See also The World Bank (2015), "Withdrawal from Correspondent Banking; Where, Why, and What to Do About It," November, http://documents.worldbank.org/curated/en/113021467990964789/pdf/101098-revised-PUBLIC-CBR-Report-November-2015.pdf.*

Adoption of this or a similar protocol could spur further innovation and adoption of DLT-based systems for the cross-border payments use case.[32]

Financial inclusion

Financial inclusion is another challenge both domestically and abroad that some are attempting to address with DLT. Some of the potential benefits of DLT for cross-border payments described above might also be able to help address issues involving cross-border remittances as well as challenges in providing end-users with universal access to a wide range of financial services. Access to financial services can be difficult, particularly for low-income households, because of high account fees, prohibitive costs associated with traveling to a bank.[33] Developers contend DLT may assist financial inclusion by potentially allowing technology firms such as mobile phone providers to provide DLT-based financial services directly to end users at a lower cost than can (or would) traditional financial intermediaries; expanding access to customer groups not served by ordinary banks, and ultimately reducing costs for retail consumers.

Information-sharing

According to interviews, the ability of DLT to maintain tamper-resistant records can provide new ways to share information across entities such as independent auditors and supervisors. As an example, DLT arrangements could be designed to allow auditors or supervisors "read-only access" to certain parts of the common ledger. This could help service providers in a DLT arrangement and end users meet regulatory reporting requirements more efficiently. Developers contend that being given visibility to a unified, shared ledger could give supervisors confidence in knowing the origins of the asset and the history of transactions across participants. Having a connection as a node in the network, a supervisor would receive transaction data as soon as it is broadcast to the network, which could help streamline regulatory compliance procedures and reduce costs. At the same time, however, since not all of a service provider's transactions with a customer, or information about a customer, might be on one or any distributed ledger, certain regulatory requirements could be difficult to meet by simply providing access to a ledger. Notwithstanding such questions, however, the industry is actively exploring this use case.

Industry approaches to adopting DLT

As mentioned at the beginning of this section, the financial industry's focus thus far has been on experimentation and the development of PoCs. Stakeholders have taken different approaches to developing these PoCs, all with the objective of achieving adoption of distributed ledger technologies in payments, clearing and settlement. Some firms are exploring the development of DLT solutions within specific markets or asset classes and are designing DLT arrangements that are tailored to a particular use case. Other firms are developing DLT frameworks as a general purpose, open source technology that can be configured and deployed in a wide array of settings. The strategies employed broadly fall into the following categories:

Projects by financial institutions. Many global financial institutions have at least one DLT- related initiative. Several have formed dedicated teams to study and experiment with the technology and/or established innovation labs in order to understand the potential costs and benefits of DLT arrangements, as applicable

[32] *See https://interledger.org/interledger.pdf for more details.*

[33] *Committee on Payment and Market Infrastructures and The World Bank (2016), Payment Aspects of Financial Inclusion, http://www.bis.org/cpmi/publ/d144.pdf. See also Federal Deposit Insurance Corporation (2016), FDIC 2015 National Survey of Unbanked and Underbanked Households, October, https://www.fdic.gov/householdsurvey/2015/2015report.pdf.*

to their businesses. FMIs and similar organizations are also involved to varying degrees in these efforts. Some have published papers on this topic.[34]

- **Product development by technology firms:** Technology companies are experimenting with their own DLT product offerings. For example, some firms are looking to expedite settlement, whereas others are seeking technical solutions for issuing securities in a cryptographically secured, digital form and trading them securely on a shared platform.
- **Partnerships between technology firms and financial institutions.** Several large financial institutions are investing in or collaborating directly with DLT startups in ways that are mutually beneficial. For example, financial institutions may provide the capital, regulatory expertise, and access to depositors that startups need to grow. In return, financial institutions benefit from access to innovative financial technology, with which they may experiment within or alongside their existing systems with limited disruption to operational or organizational practices.
- **Block chain-as-a-Service (BaaS) partnerships**. BaaS refers to a model for the provision of DLT systems or services where technology companies charge fees for centrally hosting the computing infrastructure, typically in a cloud environment, and codebase necessary for DLT systems, making it easy for other firms to deploy and test DLT systems with limited overhead. Established technology firms are competing to be the leading provider of BaaS services.
- **Participation in consortia.** Consortia are helping industry participants mutualize the costs and risks associated with developing DLT arrangements. In addition, these multilateral partnerships are acting as catalysts for future discussions related to common ledger operability standards and enabling the testing of PoCs. By joining consortia, firms are able to lower development costs and test solutions together instead of in silos. Some consortia have membership fees and are driven by the need to generate commercial solutions, while others are focused exclusively on developing a unified code base and open standard.
- **Hosting or supporting business development programs for startups.** By offering or co-sponsoring programs such as an accelerator or incubator, which can include providing funding, business consulting services, or even physical equipment, some financial institutions are seeking to steer the future of promising startups early on.

33As described in section 2, a complex network of participants is involved in PCS. Each of these participants plays one or more critical roles in the smooth functioning of the financial system. Any changes to the technology underlying the PCS processes, therefore, would likely affect this entire network of participants. To that end, many of the aforementioned efforts to achieve wider adoption of the technology are attempting to build acceptance among the existing network of intermediaries and their ecosystem that is at the heart of the PCS activity, including financial institutions, market infrastructures, end users, and service providers. Although the DLT community has generated much excitement, there remain certain challenges for the technology to take hold in payments, clearing, and settlement.

[34] *Depository Trust and Clearing Corporation (2016), "Embracing Disruption: Blockchain White Paper," white paper, January, http://www.dtcc.com/news/2016/january/25/blockchain-white-paper. See also SWIFT and Accenture (2016), "SWIFT on distributed ledger," April, https://www.swift.com/insights/press-releases/swift-and-accenture-outline-path-to-distributed-ledger-technology-adoption-within-financial-services. See also Euroclear and Oliver Wyman (2016), "Blockchain in Capital Markets," February, http://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2016/feb/BlockChain-In-Capital-Markets.pdf.*

5 Challenges to adoption and implementation: business, technical, and financial design issues

As noted above, the industry is at an early stage of development regarding DLT. As the industry continues to experiment, a number of business, technical, and financial design challenges must be addressed before DLT can become a practical solution for some aspects of payments, clearing, and settlement. This section summarizes some challenges the industry must address in order to reach broad adoption of DLT.

Business issues

Cost-benefit considerations of potential use cases

The previous section referenced several use cases for DLT that the industry is exploring. A key challenge is identifying appropriate use cases where the potential reduction in costs of operational and financial inefficiencies would justify the cost of the investment and operational changes needed to implement DLT. In addition, the longer term operating costs of DLT would need to be favorable relative to current or plausible alternative technologies. Some see potential in targeting markets that today have significant operational inefficiencies, such as highly decentralized and disorganized post-trade operations. Others see opportunities for spillover benefits such as an opportunity to standardize business processes alongside DLT implementation. Still others have targeted markets where the transition to a DLT arrangement may have relatively lower costs because of certain efficiencies already in place, such as markets where assets are already in digital form. Importantly, evaluations of these use cases involve a comparison of other viable alternatives to address the frictions present in the markets where DLT is being considered.

Network effects

Fundamentally, if broad adoption of DLT is to take place in payments, clearing, and settlement, the industry will need a critical mass of participants for any application of the technology to be successful. Network effects are derived from the fact that each additional user of a network increases the benefit of the network for existing users. This effect can often lead to a problem for early adoption because the net benefits for early adopters may be negative without sufficient participation, leading to a possible lack of adoption. Indeed, many of the interviewed firms explicitly recognized network effects as a critical factor that will influence the adoption of DLT for PCS processes. The industry is trying to address these effects in various ways, as mentioned in section 4. These efforts include establishing consortia to facilitate cooperation on issues related to the technology and partnerships between start-ups and established FMIs that help coordinate decision-making for a particular market segment.

Technical issues

Viable technology solutions

In addition to finding a business case, the industry must also be comfortable that the technology can achieve sufficient scale of operations and interoperability with legacy systems and other DLT arrangements. Both must be considered when developing a viable DLT solution.

Scalability

As mentioned in section 1.1, U.S. PCS systems process hundreds of millions of transactions daily. Consensus algorithms and cryptographic verification introduce latency and limit the number of transfers that some DLT arrangements can process concurrently. Additionally, ledgers that add transactional histories on top of one another, such as block chains, may challenge storage capacity over time. Design choices, such as the choice of consensus algorithm, can mitigate some of these concerns. For example, some in the industry are considering limiting permissions to write to the common ledger to only atrusted central

intermediary as in current arrangements, reducing latency by eliminating the need for consensus altogether. Nonetheless, electronic payments technology must have the scalability needed to provide fast and reliable service to the market or it is unlikely to be acceptable to financial institutions or public authorities.[35]

Interoperability

Interviews with firms suggest the future will not be characterized by a single DLT arrangement. Instead, multiple DLT arrangements will likely be developed and deployed based on the needed functionality and on the required regulatory and market stipulations of a specific business case. Certain legacy systems may also continue to exist. Given that the broader financial system will continue to have a diverse set of participants interacting within a single financial market or across different financial markets, the ability for participants to process transactions smoothly among the relevant systems will be critical to the continued efficient functioning of the broader financial system.

As now, intermediaries, businesses, and households would still need to interact with a (potentially large) number of systems to conduct their PCS activities in a DLT arrangement. Interoperability across DLT arrangements or between DLT arrangements and legacy systems is likely to be an important factor in determining the extent of DLT adoption. Intermediaries may help address this problem for businesses and households; nonetheless, frictions and costs rise as the complexity of connections to and use of different systems increase. Moreover, the likely co-existence of legacy and new DLT arrangements adds further complexity and fragmentation.

In the short run, a reasonable amount of coordination, communication, and interoperability between proposed DLT arrangements with existing systems and providers will be necessary for benefits of DLT to be realized. Standards-based APIs and interoperability protocols can serve as a needed bridge between emerging and existing systems. As DLT arrangements seek to improve the speed and efficiency of the transfer and exchange of value, it is critical that access to and interoperability with these arrangements are equally fast and efficient. As transactions are potentially processed more quickly within a given DLT arrangement, other systems that depend on information such as confirmation of transaction settlement may be exposed to risk if there are delays in or barriers to these systems' ability to access such information.

Standards development

Standards development is another critical area for the successful adoption of DLT. Standards are important for providing a base layer of interoperability across different DLT arrangements and legacy systems. If organizations eventually interact with multiple DLT arrangements, open industry standards can also help to lower implementation and integration costs and ensure consistent expectations about how information from DLT-based arrangements is structured and accessed. Indeed, the industry is contemplating ways of achieving common standards. One challenge, however, is that many applications of DLT are still being developed and tested, and the industry may not have sufficient information at this point to develop appropriate standards. This is typical of emerging technologies in the PoC stage.

Beyond interoperability, APIs may be required to enable DLT arrangements to make requests to

[35] *See generally, Federal Financial Institutions Examination Council (2004), FFIEC Information Technology Handbook, "Operations Booklet," July, http://ithandbook.ffiec.gov/it-booklets/operations/introduction.aspx. See also SWIFT and Accenture (2016), "SWIFT on distributed ledger," April, https://www.swift.com/insights/press-releases/swift-and-accenture-outline-path-to-distributed-ledger-technology-adoption-within-financial-services.*

external systems to achieve enhancements that are not core to the DLT arrangement itself. A robust set of APIs may also help organizations to realize the operational efficiencies of DLT arrangements without requiring dramatic changes to IT architecture in the short-term. From this perspective DLT arrangements are not merely an end product, but can be viewed at least in part as a platform developers can build upon. Building open APIs in common, industry-standard languages, and enhancing software development kits lowers the barriers for organizations and their development teams to enter the DLT industry, acting as a potential catalyst to interoperability.

Cryptographic key and access data management

Effective management of cryptographic keys and access credentials is a particularly important business issue in the context of DLT because, unlike many other applications of this type of cryptography, users can potentially suffer immediate and irrevocable monetary losses without recourse if keys or access credentials are lost or compromised. Key compromises may lead to economic losses associated with account takeover and fraud. Lost keys may render data unreadable or inaccessible, resulting in the permanent loss of the value secured by the cryptography. The ability to bind the identity of public keys to individual or corporate identities is also an important privacy-related aspect of digital signature arrangements in which users are subject to legal requirements such as those associated with anti-money-laundering compliance.

The ability to maintain the secret nature of private keys and achieve the desired security properties of public key encryption is a complex and challenging undertaking, which depends on a variety of factors including the strength of the cryptography and the protocols used for key generation, storage, distribution, revocation, and destruction. Reflecting these challenges, numerous standard setting and regulatory bodies have established detailed guidance and minimum requirements for enterprise use of cryptographic keys and the design of cryptographic key management systems.[36]

Applying the requirements and guidance to DLT arrangements will be an important step for such arrangements to become viable. Beyond specific key-management issues, organizations that employ DLT will still need to consider best practices in information security that extend well beyond cryptography.

Information management

The introduction of DLT brings the promise that participants share common information on a ledger with a history that is extremely difficult, if not impossible, to alter. It is fundamentally important that the common information be correct.

This requirement can be difficult to achieve if many participants can write to the ledger. For example, decisions regarding who can create new assets and how information that is input to the system is checked for accuracy are fundamental. Also, the designers of a DLT arrangement must determine how errors and known fraudulent account take-overs are handled and resolved.

---

[36] *U.S. Department of Commerce, National Institute of Standards and Technology (2013), A Framework for Designing Cryptographic Key Management Systems, August, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-130.pdf.See also U.S. Department of Commerce, National Institute of Standards and Technology (2016), Recommendation for Key Management, January, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf. See also International Organization for Standardization and International Electrotechnical Commission (2005), Information Technology - Security Techniques - Code of Practice for Information Security Management, June, http://www.slinfo.una.ac.cr/documentos/EIF402/ISO27001.pdf. See also Federal Financial Institutions Examination Council (2016), FFIEC Information Technology Handbook, "Information Security," September, http://ithandbook.ffiec.gov/media/216407/informationsecurity2016booklet.pdf.*

An additional challenge is the determination of exactly what information to share. This issue is especially challenging when information, possibly including customer information, is shared among competitors.

Relevant privacy laws and regulations must also be satisfied. Participants will have to agree on the extent of information that is shared and whether the complete set of information will still need to be entrusted to a central institution, such as a clearinghouse. Failure to agree on the level of this "differentiated privacy" could be one challenge in reaching a critical mass of users.

Financial design issues

The use of DLT technologies may raise basic issues about how financial instruments are designed and, in some cases, the role and need for financial intermediaries. The design of a DLT arrangement could take many forms and involves decisions about the nature of the digital assets in the system, the entities that can issue the digital asset and how they do so, and the roles that intermediaries will ultimately play regarding the issuance, storage, recordkeeping, and transfer of the digital assets. Some of these issues echo debates from the development of book-entry securities and electronic payments over the past five decades.

Financial instruments

As discussed in section 4, some of those interviewed are considering electronic representations of securities that can be held and transferred on DLT arrangements. Securities may be originally issued in electronic form or in paper form, and regardless of issuance method, traditional design choices are applicable to book-entry securities which are "immobilized" or "de-materialized" through the use of a securities custodian. Further, design choices need to be made to determine whether either type of book-entry security is issued directly to the ultimate holder, with transfers of the security requiring changes in the registration of the security, or whether securities can be held in a fungible form that can be held and transferred through a series of intermediaries.[37]

Over time, DLT may provide opportunities to re-visit the traditional choices for the design, holding, and transfer of securities. For example, one new development appears to be the concept of "tokenization," in which coded data are intended to represent a security on some type of ledger and to enable rapid and easy transfers by owners or their intermediaries, but not to be the security itself or the bundle of rights and obligations the security represents. One aspect that will not change is that the securities themselves will by definition continue to be liabilities of the ultimate issuer of the securities.

Intermediaries that carry electronic securities on their books will presumably continue to have rights and responsibilities with respect to those securities. If systems with tokens representing securities are developed, and the tokens are not designed or intended to be securities, then questions may arise about the status of the tokens, what they represent, and how they are treated when holdings or transfers go awry. The legal status of digital assets is discussed further in 6.1.1.1 below. Related questions exist for physical commodities, although the legal framework may be different and the role of physical underlying assets must be taken into account.

Monetary instruments

Similar points can also be made about monetary instruments. In the case of what might be called book-entry money, financial intermediaries issue deposit

[37] *Securities Transactions Settlement, 69 FR 12921 (March 18, 2004), https://www.federalregister.gov/documents/2004/03/18/04-5981/securities-transactions-settlement.*

liabilities that holders treat as assets and use to make payments and store wealth. Traditionally, each intermediary issues its own liabilities, and the completion of payments from one party to another when each holds their monetary instruments at a different institution typically involves a specific change in the amount of the account ledger (the monetary liability at each institution) held by each party. In principle, the use of DLT could involve the establishment of a common ledger for each bank, with links between ledgers designed to process payments between ledgers. However, if multiple institutions are involved in the transfer of payments, some way to settle the payments between them will be needed. The general options for conducting such settlements are well known. Either banks settle using adjustments to their claims on each other or settle using claims on a third-party financial intermediary, such as a correspondent or central bank.

Interbank settlement using a commodity such as gold is a historical possibility, but is unlikely within the current monetary regimes.

The design of monetary instruments that parallel some of the original properties of banknotes is also a possibility. Historically, commercial banks issued banknotes that were negotiable instruments, that is, they were essentially the property of the holder of the note, without a clearing and settlement process in which account balances were adjusted at a central intermediary with each payment. Certain kinds of pre-paid cards are currently designed in this way, and the debate over the design of prepaid cards and electronic money in the mid-1990s has lessons for today.[38]

In the case of DLT, each bank could presumably maintain its own ledger for its customers to use to make payments directly between one another without needing to send payment instructions through that bank. The liabilities of the bank held on the ledger could be registered to each holder individually but might also be issued in "bearer form" and owned by whoever holds the liability. Design choices would presumably be influenced by the benefits and costs of the different types of arrangements. When multiple banks are involved and have customers who want to make payments across the banks, a mechanism would be needed to communicate and settle transactions between institutions in order to complete payments.

Financial intermediaries

Another design choice for both securities and monetary instruments would be the types of institutions that would be allowed to issue these liabilities and act as intermediaries. In some cases, institutions may be needed to act as custodians. Regulatory frameworks have been established and enhanced over time to address these questions and to help foster safe and efficient systems for issuing and transferring securities and money. To the extent new entrants into these processes come forward with new types of design concepts, those entrants may need to interpret and review regulatory issues.

Some have raised the possibility that DL technology may make financial intermediaries obsolete. One cannot rule out long-run changes in the roles and responsibilities of intermediaries in financial markets and the demand for their services. However, intermediaries play important roles in matching borrowers and savers in the economy, providing safe monetary instruments that form the basis of the payment system, aggregate financial activity and more. It is far from clear that these functions will all become obsolete in the foreseeable future.

[38] *Committee on Payment and Market Infrastructures (2015), Digital Currencies, http://www.bis.org/cpmi/publ/d137.pdf.*

6 Challenges to adoption and implementation: risk management

In addition to the challenges identified above, questions also arise about the way in which the implementation of DLT would fit into the risk-management frameworks that already exist to promote safety and confidence in payments and securities transfer processes.

Legal, settlement, operational, and financial risks are inherent in the conduct of PCS activities. With the current design of the financial markets, such risks are typically concentrated at intermediaries such as banks and FMIs, which, in turn, specialize in managing and controlling these risks. For example, today's FMIs establish rules and manage risks through a centralized governance structure, help eliminate certain risks (for example, provide for legally defined settlement finality and delivery versus payment), mitigate and measure others (for example, credit and liquidity risks), reduce costs of clearing and settling transactions between and among multiple parties (for example, netting), and provide a level of transparency to the market. However, a tradeoff may arise because FMIs also typically concentrate much of the conduct of PCS activities, and therefore risks, into a single or handful of central entities.

Much of the focus of the policy and regulatory environment, therefore, has been on ensuring that these intermediaries appropriately and adequately manage risks, so that they may run effectively even in times of stressed market conditions.

A key consideration that may affect the assessment and adoption of any DLT solution is whether a change to one aspect of the PCS process, even if it is meant to increase efficiencies or to mitigate a particular risk, merely shifts the risks among actors in the PCS process or increases the overall risks in the conduct of PCS activities. The extent to which a particular solution affects the fundamental design of the financial system as well as day-to-day activities is likely to affect this assessment. For example, on the one hand, if a solution reduces the cost of clearing, but does so by shifting financial and operational risk to end-users of a system or by reducing the ability of specialized intermediaries to manage risk, difficult decisions may be needed about the trade-off between the benefits of greater efficiency and the associated costs and risks. On the other hand, if a solution unambiguously would reduce costs and risks to financial markets over the long run, it may face short-term challenges to adoption, but may also have clear long-run strategic benefits to the markets.

Legal considerations

The legal framework (for example, statutes, regulations, policy, and supervision) governing financial markets and the conduct of PCS activities is well-established. Much of the existing legal environment, however, is organized and implemented in a manner consistent with the current financial market architecture, which has a complex network of participants that perform a variety of functions and are regulated, supervised, and overseen by a diverse group of regulators. The relevant laws, regulations, andsupervisory policies are aimed at achieving broad objectives such as market transparency, safety and soundness of financial institutions, and the efficient and effective functioning of the broader financial system, and are not generally intended to favor a particular electronic technology.[39]

[39] *Some laws and regulations have been designed to reduce the use of paper in PCS systems following, for example, the "paperwork crisis" of the 1960s and 1970s. Some legal frameworks have also had implicit biases toward paper notices and other documents since these were the accepted communications or authentication technologies when the frameworks were adopted.*

Even so, the laws and regulations applicable to PCS can affect the manner in which, speed by which, and extent to which any implementation or configurations of DLT for a particular use case can be adopted by regulated entities or new entrants to the financial system. It is therefore important to consider how the legal framework may differ depending on the configurations of DLT, as the industry further develops DLT use cases.

Legal basis of certain DLT components

Distributed ledgers

As DLT matures, the legal basis for certain components of the technology, which may not be contemplated in the current legal framework for PCS activities, will merit careful consideration. One of the purported benefits of DLT is that it provides an auditable record of information that is simultaneously updated and distributed among participants.[40]

Businesses using and trusting the records that are stored on shared ledgers must consider the legal basis for these records. Users of these records will need to be assured of their reliability as an authoritative source of the underlying obligations and the enforceability of those obligations. Shared ledgers should be designed to provide these assurances under existing laws, or, alternatively, statutes and rules may need to be adjusted to accommodate DLT- enabled recordkeeping.

Digital representations of assets

Digital representations of a physical asset, such as tokens, as well as natively issued digital assets are also key components of a DLT arrangement. The ownership rights and obligations associated with digital tokens and assets may not be clearly defined in today's legal framework. Many ownership interests in assets, such as negotiable instruments and securities, are already represented using physical or book- entry records, and the corresponding legal frameworks are robust and have developed over time.

Careful legal analysis must be done to understand how ownership of digital tokens on a distributed ledger fit into the current legal frameworks and what gaps need to be filled by contractual agreements or new laws and regulations.

Smart contracts

DLT has also raised the possibility of writing terms and conditions between parties into computer code to be executed automatically. In order for these "smart contracts" to be enforceable, they must have a sound legal basis. Contract law is an established set of rules that govern the basic principles of contracting, including formation, amendment, termination, and dispute resolution. Some classic contract doctrines, such as voiding unconscionable contracts, or amending contracts due to changed circumstances, conflict with the automatic execution of smart contracts. If smart contracts proliferate, judges and juries will have to review them to determine their legal basis and evidentiary status.

Complex applications of smart contracts could potentially allow for traditional organizations, such as businesses and nonprofits, to be run through rules encoded as smart contracts. The legal status of organizations that are run on smart contracts is unclear.[41]

---

[40] *An example of how using a DLT-enabled shared ledger may be inconsistent with existing laws has been highlighted in the following article: Jenny Cieplak and Mike Gill (2016), "How Distributed Ledgers Impact Post-Trade in a Dodd-Frank World," Coindesk, July 9, http://www.coindesk.com/distributed-ledger-cftc-post-trade-dodd-frank/.*

[41] *For example, the Decentralized Autonomous Organization (DAO) was a smart contract running on the Ethereum block chain that acted as a venture capital fund. Participants pledged ether, the Ethereum block chain's native crypto currency, to the DAO in exchange for tokens, which represented voting shares in the organization. Curators (well-known members of the community) were to select projects seeking funding and put them up for a vote, with token holders receiving votes proportional to the amount of ether they pledged.*

If "management" of an organization is conducted automatically by code, legal systems will have to determine who to hold accountable if laws are broken and disputes arise. The legal frameworks around corporations and other business associations would have to adapt to the concept of distributed management.

Licensing

As discussed in section 2, PCS innovation can emerge from new technology, changes to the existing market structure, or both. The emergence of DLT is likely to augment the existing market structure to include new participants that provide PCS services. Some of these participants are specific technology firms or software companies that partner with existing financial intermediaries to implement a DLT arrangement. Others may augment or even replace the services of existing financial intermediaries. Although it is too soon to predict what corresponding change in market structure might emerge as a result of DLT, one challenge for any emergent firm that takes on a traditional financial intermediary role is the likely need to acquire some type of charter or license to provide services or conduct activities that involve the holding and transferring of assets on behalf of households and businesses. The nature and form of such charters or licenses remains an open question as lawmakers and regulators may consider whether existing financial institution licenses are sufficient, or alternative licenses may need to be developed. In the crypto currency world, the New York State Department of Financial Services' "Bit License" is one such example for institutions that play roles related to storing, recordkeeping, and transfer services.[42] In DLT arrangements, intermediaries might provide services around the storage, recordkeeping, and transfer of more-traditional financial assets but not other traditional functions of banking such as household and business lending (so-called narrow banks). It may be useful to explore the pros and cons of a special banking charter with requirements that differ from traditional banking licenses based on the more limited scope of services provided[43].

Compliance with BSA/AML

Compliance with the Bank Secrecy Act (BSA) and anti-money-laundering (AML) requirements is the responsibility of a variety of intermediaries, including but not limited to banks, money services businesses, and securities broker-dealers. AML compliance includes transaction monitoring, know your customer requirements, and reporting of suspicious activity to the U.S Department of the Treasury's Financial Crimes and Enforcement Network (FinCEN). As DLT matures and the types of intermediaries in existence potentially change, the appropriate government agencies may need to provide guidance on the application of existing law to any new intermediaries or PCS processes.[44] In fact, this process was followed when FinCEN issued new guidance with respect to the BSA's application to virtual currency exchangers.[45]

---

[42] *New York State Department of Financial Services (2015), Final Bit License Regulatory Framework, June 24, http://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm.*

[43] *The Office of the Comptroller of the Currency has sought comment on similar ideas. See Office of the Comptroller of the Currency (2016), Supporting Responsible Innovation in the Federal Banking System: An OCC Perspective, March, http://www.occ.gov/publications/publications-by-type/other-publications-reports/pub-responsible-innovation-banking-system-occ-perspective.pdf. See also Office of the Comptroller of the Currency (2016), Recommendations and Decisions for Implementing a Responsible Innovation Framework, October, https://occ.gov/topics/bank-operations/innovation/recommendations-decisions-for-implementing-a-responsible-innovation-framework.pdf.*

[44] *In the United States, the AML authority responsible for interpreting the BSA and its implementing regulations is FinCEN: https://www.fincen.gov/.*

[45] *U.S. Department of the Treasury, Financial Crimes Enforcement Network (March 18, 2013), FIN-2013-G001, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," https://fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf.*

Governance

Effective, accountable, and transparent governance arrangements are critical to the risk management of PCS systems. Ideal governance arrangements are clear and transparent, promote the safety and efficiency of the system, and support the stability of the broader financial system. Sound governance arrangements would continue to be necessary for DLT arrangements in order to determine the rules regarding functionality, risk management, and access to the network, as well as which entities are responsible for maintaining and modifying the protocol. The methods by which governance arrangements take effect may differ depending on the design of the DLT arrangement. Two extremes in the design of DLT arrangements are discussed below.

Open permissionless systems

Open and permissionless systems, discussed in section 3.1, may require distributed governance arrangements, in which consensus could be used to determine any changes to the network's protocol or functions. It is not clear, however, the extent to which such arrangements would address significant unforeseen issues or the potential need to change significant rules once they are put into motion. The potential lack of clear, transparent, and predictable governance, particularly in an open and permissionless DLT arrangement, could potentially have a negative effect on the stability of the network and broader financial system, especially if it at any point the network interacts significantly with regulated entities in the traditional financial system.

The 2016 hack of the Decentralized Autonomous Organization (DAO) demonstrated the challenges of having a decentralized governance arrangement that requires consensus of the network to deploy changes. In this example, the debate centered on whether the Ethereum community should claw back a large amount of ether that was transferred by an unknown participant from the DAO's address to a separate address. With no single accountable decision-making authority, philosophical differences arose about whether to retain a known illegitimate action in order to preserve the inalterability of the common ledger or to attempt to essentially reverse the action because it was known to be illegitimate. This debate led to a division that resulted in uncertainty for the network and volatility in the value of ether.[46]

Closed permissioned systems

Conversely, closed systems, and particularly those in which participants are differentiated based on the roles they play and functions they are permitted to perform, may involve one or more institutions that have ownership rights over the arrangement. To that end, this type of arrangement could create a more-centralized governance structure for granting access to the system arrangement, making significant decisions such as rules or technology upgrades on behalf of the arrangement, as well as determining permissions to write changes to the ledger. Such arrangements are likely to be more recognizable as traditional corporate or FMI governance arrangements than computer protocols for open and permissionless arrangements. Permissioned systems may also employ governance arrangements that allow for distributed (potentially delegated) governance for some aspects of the network and centralized governance for others. Importantly, as with the traditional corporate or FMI governance arrangements, uncertainty could be reduced around responsibility, accountability, and liability for decisions related to the system. The flexibility of the governance arrangement to adjust over time might also increase.

---

[46] For additional information on the DAO hack, see Dan Goodin (2016), "Bitcoin Rival Ethereum Fights for its Survival after $50 million Heist," June 21, http://arstechnica.com/security/2016/06/bitcoin-rival-ethereum-fights-for-its-survival-after-50-million-heist/.

Settlement finality

A key risk in entering into any financial transaction is the risk that settlement will not take place as expected. Failure to settle as expected can be due to a number of factors, such as a counterparty's default, an operational issue, or uncertainty about when settlement is considered final and irrevocable. This section discusses two types of uncertainties in settlement finality that a DLT arrangement might introduce.

In post-trade clearing and settlement, settlement finality is currently a legally defined moment, typically supported by a statutory, regulatory, and/or contractual framework underlying a given financial transaction. Parties to a transaction and their intermediaries rely on the definition and timing of finality when they update their own ledgers to effect settlement, determine the ownership of assets, and measure and monitor various risks. In contrast, in some versions of DLT arrangements, multiple parties are permissioned to update a shared ledger, and those parties must agree to a particular state of the ledger through the consensus process. Settlement finality in this world rests on probabilistic finality, whereby the longer a transaction is considered settled by the system participants, the less likely this transaction will be reversed (or dropped). This approach to finality contrasts with the traditional approach of defining an unambiguous and transparent moment of finality. With a probabilistic approach to finality, legal liability may be difficult to assign or be ambiguous in such a network, and the uncertainty has implications for the balance sheets of participants as well as the rights of their customers and creditors.

Settlement finality is even more complicated when considering both legs of a financial transaction, for example, the delivery of an asset against payment for the asset in rigorous versions of DvP. Not only must finality be clear and certain for both legs, but each leg's finality should be conditional on the finality of the other. This interdependency can be a challenge in a situation where the payment and asset delivery legs may not be occurring on the same network, platform, or ledger and where no intermediary exists to provide assurance for settlement finality. Should a counterparty default on its obligations after only one of the legs of the transaction settles, there could be an open question regarding the status of the transaction. At a minimum, such designs for DvP deserve rigorous scrutiny, and may require extra layers of risk management.

Financial risk

Counterparties to a financial transaction may also face credit or liquidity risks arising in each step of the payment, clearing, or settlement processes. Credit risk is the risk that a counterparty may be unable to fully meet its settlement obligations when due or at any point through the duration of the exposure.

Liquidity risk is the risk that a counterparty will have insufficient funds to meet its financial obligations when due but may do so at some point in the future. Although these two risks are distinct concepts, they are often related.[37]

In a financial system with financial intermediaries that have responsibilities for facilitating the payment, clearing, or settlement processes and sometimes even guaranteeing settlement of a transaction on behalf of its customers or participants, much of this credit and liquidity risk between the original counterparties is assumed and managed centrally by the intermediary. Tools for managing credit risks range from those that eliminate credit risk (for example, requirements that

[47] *Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commissions (2012), Principles for Financial Market Infrastructures, http://www.bis.org/cpmi/publ/d101a.pdf, page 19.*

payment obligations be fully prefunded) to those that mitigate and manage credit risk (for example, allowing for posting of collateral at reasonable haircuts, or discounts from market value). Whether an FMI participant is required to fully prefund a payment account or post collateral in order to complete a transaction affects the participant's own liquidity. Similarly, how a DLT arrangement is designed to handle counterparty credit risk could have a significant impact on the participants' liquidity needs.

Operational risk

The risk of operational failures or disruptions threaten the successful settlement of financial transactions, irrespective of whether the underlying payment, clearing, or settlement processes are supported or facilitated by an intermediary or through a decentralized and automated technological platform. Possible operational failures include errors or delays in processing, system outages, insufficient capacity, fraud, and data loss and leakage. Therefore, system resiliency and security are critical components of managing operational risk.

Safety and integrity in clearing and settlement is critical for broader financial stability which is a key reason that major clearing and settlement systems are regulated. Hence, a fundamental threshold test for new technologies will be whether they can be deployed and operated safely, with the requisite high degree of resiliency and security across a wide range of adverse scenarios.[38] Many of the interviewed firms suggest that the distributed data storage aspect of DLT provides greater resilience and data integrity than traditional centralized clearing and settlement systems do. If one or several entities that hold a copy of the distributed ledger experience a failure, the remaining unaffected entities would be able to maintain an accurate ledger and, therefore, continue the system's operations. Further, some interviewed firms suggested that individual firms or system might be able to employ DLT to store backup copies of data within legacy systems in a technologically diverse system in order to strengthen resilience against cyberattacks.[39]

DLT arrangements must also address the same risks as existing PCS systems and, although the current procedures and controls used to address these risks appear to be generally relevant for DLT, modifications may be required in order to make these currently used risk-mitigation strategies applicable to a distributed environment. Similar to traditional PCS systems, one of the biggest concerns with DLT solutions is endpoint security. As with any system where vulnerabilities can potentially exist within both software and hardware components, DLT may face increased exposure to cyber-attacks through its distributed network of participants, or endpoints, which are validating transactions and writing to the blockchain. Endpoint security remains an ongoing challenge for which no easy technological solution may exist.

Additionally, the strength issue of cryptography is particularly important for DLT arrangements. Cryptography can be used not only to protect data but also to serve as a way to manage rights and access to data. Although layered approaches to security, known as Defense in Depth, would be expected for any organization using DLT or any other technology, if the system's encryption is compromised, DLT arrangements may be particularly vulnerable. Not only is the strength of the encryption important, but so too are the procedures and controls surrounding the security of encryption keys and any key management

[48] *Lael Brainard (2016), "The Use of Distributed Ledger Technologies in Payment, Clearing, and Settlement," speech delivered at The Institute of International Finance Blockchain Roundtable, Washington D.C., April 14, https://www.federalreserve.gov/newsevents/speech/brainard20160414a.htm.*

[49] *Committee on Payments and Market Infrastructures and Board of the International Organization of Securities Commissions (2015), Guidance on Cyber Resilience for Financial Market Infrastructures, http://www.bis.org/cpmi/publ/d146.pdf. See also National Institute of Standards and Technology (2014), Framework for Improving Critical Infrastructure Cybersecurity, Feb 12, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.*

processes used. Furthermore, because risks and threats are continually evolving, the procedures and controls to secure DLT systems must also continually assess risk, improve, and adapt, which may be particularly challenging in an open and permissionless system. Ultimately, these and other security concerns will have to be fully addressed before DLT can achieve widespread adoption.

However, these same design properties may also help DLT address certain resiliency and security risks that are present in traditional systems. For example, some experts suggest that DLT arrangements can be created without the reliance on centralized databases that are typically susceptible to disruptive cyber-attacks. By using certain distributed ledger arrangements, it may be possible to reduce or avoid the risk of extensive and prolonged system outages (and even permanent losses of data) in a manner different from the traditional approach of systems that rely on centralized databases. Instead, identical and widely dispersed databases that are hard to impact simultaneously may be able to assist one another in recovering from a cyber-attack. Nonetheless, there are a number of important factors to consider that underlie such suggestions, including the difficulty of simultaneous attacks on all of the databases in a distributed network, the difficulty of corrupting data stored on a DLT, the ability to quickly propagate data to compromised sites, and the ability of a compromised site to quickly begin using the refreshed data. For DLT to be successful, careful and ongoing analysis of the security considerations will be critical.

7 Summary

This paper has examined how DLT can be used in the area of payments, clearing and settlement and identifies both the opportunities and challenges facing its long-term implementation and adoption. In the context of payments, DLT has the potential to provide new ways to transfer and record the ownership of digital assets; immutably and securely store information; provide for identity management; and other evolving operations through peer-to-peer networking, access to a distributed but common ledger among participants, and cryptography. Potential use cases in payments, clearing, and settlement include cross-border payments and the post-trade clearing and settlement of securities. These use cases could address operational and financial frictions around existing services. Nonetheless, the industry's understanding and application of this technology is still in its infancy, and stakeholders are taking a variety of approaches toward its development. Given the technology's early stage, a number of challenges to development and adoption remain, including in how issues around business cases, technological hurdles, legal considerations, and risk management considerations are addressed.

Finally, as a recent innovation, DLT has the potential to also drive change to the financial market structure in ways that take advantage of the new technology. Although it is too soon to predict what these changes may be, the way that the industry finds use cases and addresses the challenges identified in this paper will provide clarity over time. As the technologies and experimentation with these technologies continue to develop, it will be important to thoroughly understand how these changes apply broadly. Understanding the potential range of DLT adoption and its link to changing the financial market structure is an area for future research.

David Mills, Kathy Wang, Brendan Malone, Anjana Ravi, Jeff Marquardt, Clinton Chen, Anton Badev, and Timothy Brezinski are/were with U.S. Federal Reserve Board. Linda Fahy, Kimberley Liao, Vanessa Kargenian, Max Ellithorpe, and Wendy Ng are/were with U.S. Federal Reserve Bank of New York. Maria Baird is/was with U.S. Federal Reserve Bank of Chicago.