Blockchain technology's potential in the financial system

David Yermack
Albert Fingerhut Professor of Finance and Business Transformation
NYU Stern School of Business
National Bureau of Economic Research
European Corporate Governance Institute

Prepared for the Federal Reserve Bank of Atlanta
2019 Financial Market's Conference
Amelia Island, FL
May 20, 2019

Blockchain technology’s potential in the financial system

This essay evaluates the potential for blockchain technology to bring value to the financial system, with a special focus on wholesale financial markets. Discussing this topic at a research conference organized by a U.S. Federal Reserve Bank seems ironic. The first application of blockchains to finance occurred ten years ago when Nakamoto (2008) launched the Bitcoin payment system, introducing to the financial world the innovation of Haber and Stornetta (1991) of a blockchain database that is shared widely among users in the form of a “distributed ledger.” Nakamoto famously encoded the original block of the Bitcoin blockchain with the headline of that morning’s *Times* of London, “Chancellor on brink of second bailout for banks.” This gesture indicated an ambition to compete with and surpass the legacy global payments network.

While Bitcoin and successor cryptocurrencies have grown remarkably, data indicates that many of their users have not tried to participate in the mainstream financial system. Instead they have deliberately avoided it in order to transact in black markets for drugs and other contraband (Foley, Karlsen, and Putniņš, 2019) or evade capital controls in countries such as China (Ju, Lu and Tu, 2016). However, the potential benefits of blockchain for improving data security and solving moral hazard problems throughout the financial system have become widely apparent as cryptocurrencies have grown. By

2015 exploratory uses of blockchains had begun in dozens of prominent stock exchanges, insurance companies, payment processors, banks, and other institutions. Today, many financial industry participants have become promoters of blockchain technology, with many routinely publishing descriptions of the underlying business opportunities such as J.P. Morgan (2018). Central banks in some countries have become involved in coordinating and building blockchain platforms intended for use in the interbank settlement market, among other applications.[1]

Section 1 of this essay presents a brief overview of blockchain technology. Section 2 highlights differences between open or public blockchains, such as those used in Bitcoin and other cryptocurrencies, and private or permissioned blockchains, the model that is clearly favored by regulators and industry participants. Section 3 discusses potential use cases of blockchains in the wholesale financial system, with subsections examining interbank settlements, investment markets, real estate, and trade finance. Section 4 states conclusions.

1. How do blockchains work?

The word "blockchain" refers to a ledger that arranges its entries sequentially. Each entry includes an encryption of new data, such as a financial payment, which is merged with the encryption of the prior entry. The joint encryption of these two pieces in turn becomes the first part of the subsequent entry (Figure 1). This sequential encoding and merging of information creates a high degree of security, because a retroactive change in one transaction entry, perhaps by a hacker or thief, causes a change in all

[1] For an example see Khatri (2019).

subsequent entries which would be immediately obvious to those with access to the ledger. The blockchain thus provides a robust form of time-stamping, so that the user can know the order in which transactions occurred or contracts were executed.

"Blockchain" has become short-hand for the use of a sequential ledger in a context in which it can be read and perhaps updated by multiple parties, in some cases the entire community of users. In nearly all cryptocurrency applications, the ledger is distributed to all users, and this wide distribution effectively crowd-sources the auditor function. This decentralization of data and transparency was first proposed by Haber and Stornetta (1991) for validating the creation and ownership of digital property. It completely inverts classical ideas about cyber security, which typically have required data to be hidden and tightly controlled by a trusted third party, such as a clearinghouse that ratifies trades on a stock exchange.[2]

The idea of eliminating the trusted third party and creating a "trustless" financial system has animated much of the entrepreneurial work on improving decentralized blockchains. In addition to cryptocurrencies, blockchains now host protocols such as self-executing "smart contracts" (Szabo, 1996), which require second-generation blockchains such as Ethereum that convey value based upon contingencies and the resolution of uncertainty. Initial coin offerings, which are purpose-built tokens tied to one product or service, represent the most widely used smart contracts to date, and some

[2] Like many intellectual breakthroughs, the blockchain and distributed ledger draw upon numerous prior innovations in cryptography and accounting. The first usage of the word "blockchain" appears to have occurred among adherents of Bitcoin. Nakamoto's (2008) white paper does not use the term, though it uses phrases such as "the next block in the chain" and "blocks are chained." A 1976 patent awarded to IBM researchers was titled, "Message verification and transmission error detection by block chaining."

of these reside on their own blockchains as well as on Ethereum, EOS, and other blockchain platforms.

While rapid innovation continues across thousands of decentralized blockchain projects, most of them share a set of common design principles. Data are typically encrypted using hash codes, a widely used innovation in cryptography that originated in the late 1970s. Value is stored in the form of digital tokens, such as the Ether tokens native to Ethereum, and tokens move between digital wallets with pseudonymous addresses that rely on double-key cryptography, an invention that also emerged during a fruitful wave of cryptography advances in the 1970s.

The most controversial – and creative – aspect of decentralized blockchains arises from the assignment of responsibility for adding new blocks to the chain. This typically occurs as the outcome of a “mining” competition between users, for which Nakamoto (2008) proposed a reward scheme that both attracts computing power to the network while also providing incentives for the participants to behave honestly. This clever application of mechanism design in a “proof of work” system has resulted in a hitherto unimaginable degree of data security for Bitcoin, which has never been hacked in more than ten years of continuous use despite the opportunity for anyone at all to compete for the right to update the ledger.

While blockchain mining protocols solve longstanding problems in data security, they create new ones that are anathema to legacy providers of financial services. The wide availability of transaction data to absolutely anyone violates widespread legal norms and regulations that require confidentiality and data privacy for clients. Mining has become costly, due to the high demands for energy to power the computers that compete by trying to discover integers that solve cryptographic puzzles. In competitive mining, a possibility exists for near-ties among miners in a global communications network that is subject to communications bottlenecks, a problem known as latency. These deadlocks, which occur with some frequency, result in disagreements about whose block becomes part of the ledger, creating "forks" in the blockchain. Forks take time to resolve through further competition (Biais *et al.*, 2019), and the possibility that secret forks may exist causes blockchain transaction confirmations to be probabilistic rather than certain. In extreme cases involving policy disputes, a minority of miners can create a deliberate "hard fork" of a blockchain, resulting in a schism that requires the set of miners to choose between two versions of the ledger, such as Ethereum vs. Ethereum Classic or Bitcoin vs. Bitcoin Cash. Threats of hard fork attempts can create uncertainty about future liquidity of blockchain networks and thereby discourage potential users from participating.

2. Public and permissioned blockchains

In the financial services industry, the problems enumerated above have made the use of "open" or "public" blockchains impractical, for reasons connected to both business strategy and regulatory compliance. Nevertheless, many financial institutions have been attracted by the data security provided by blockchains, as well as the possibility for shared ledgers to solve moral hazard problems by inducing better behavior by market participants.[3] Industry has therefore gravitated toward a "permissioned" model of the blockchain, in which access is controlled by a gatekeeper, who typically assumes responsibility for creating new blocks in the blockchain as well. Figure 2 illustrates the

[3] For the interested reader, these possibilities are explored in Yermack (2017).

different designs of open and permissioned blockchains. Of course, the permissioned blockchain reintroduces the critical role for a trusted third party, which Nakamoto (2008) had designed out of public blockchains in the belief that no third party is worthy of unconditional trust. Nevertheless, most banks, stock exchanges, and clearinghouses have no compunction about asserting that they are trustworthy, and the willingness of other firms to opt into permissioned blockchains implicitly validates this point of view.

Permissioned blockchains have begun to take many different forms, and their creation and governance appears to be an important research topic for academics as well as an emerging area of concern for regulators. Some blockchains operate internally to one organization, while others follow a membership model that might be overseen by a lead bank or an industry association. A high profile contemporary example is the food safety blockchain announced by Wal-Mart in 2018 for its produce suppliers. Still other blockchains are based on common technologies championed by consortiums such as R3, whose Corda architecture has become widely used, Hyperledger, and the Ethereum Enterprise Alliance, among others.

3. Applications of blockchains in financial markets

This section surveys the progress to date of blockchain technology in the mainstream financial system. In principal, blockchains might add value to any industry in which data security is important, and there are numerous applications beyond the financial system for blockchains to enhance data security in areas such as healthcare, government vital statistics, food safety, academic transcripts, and an endless list of other possibilities. Due to the focus of this conference I will restrict my observations mainly to banking and investment markets, with some attention to closely related areas such as real estate and trade finance.

3(a). Interbank settlements and reconciliations

Blockchains appear to have great potential for improving the efficiency and security of routine transfers, payments, and reconciliations across the banking system. Over the past two years, numerous leading financial institutions and consortiums have launched market tests of different blockchain-based settlement systems.

Most of these projects are aimed at the wholesale banking market and not necessarily customer facing products. The benefits come from reducing error rates, eliminating inconsistencies that arise when multiple ledgers are used to record the same transaction, and moving information more quickly and transparently. Often, a digital token is involved, so that one participant can settle its debts to another by acquiring an adequate supply of the token and conveying it over the network to the address of the counterparty, who may choose to retain the tokens for future settlement transactions of its own or simply convert the tokens into fiat currency balances within the host bank.

One of the most ambitious projects is the CLS Group's CLSNet service, which uses an IBM Hyperledger blockchain platform to calculate offsets between its 79 member financial institutions. CLS processes more than half of the world's foreign exchange transactions and typically has volume of more than $5 trillion per day. In launching CLSNet, the organization stated, "The initial blockchain opportunity focuses on backoffice operations between market participants; the opportunity to strip out the frictions and redundancies that impede efficiencies and speed."

A similar project launched in early 2019 is JPM Coin, a blockchain-based, digital "stable coin" that was launched to replicate the U.S. dollar but will be extended by J.P. Morgan to a range of fiat currencies. The JPM Coin is intended to be used inside the bank to transfer value instantaneously between institutional account holders, who can acquire, send, and redeem the coins over a blockchain. The intent of the JPM Coin is to speed up settlement times while reducing errors and disputes. J.P. Morgan is also the sponsor of the Interbank Information Network, a blockchain-based, peer-to-peer network to exchange messages in connection with cross-border payments. Begun in 2017 with 75 banks, the IIN had grown to more than 220 institutions by 2019.

These initiatives of J.P. Morgan compete, in principle with other emerging blockchain projects such as the Utility Settlement Coin, sponsored by a consortium of mostly European money center banks, and existing private market entrants such as the Ripple digital currency, which has grown to play a prominent disrupter role in the remittances market.

How large are the potential savings from these initiatives? Nobody really knows, because market tests remain in early stages and regulatory engagement has been incomplete. However, many utopian estimates are circulating. A Wall Street Journal article in 2015, written around the launch of the Utility Settlement Coin project involving UBS and other major banks, quoted a consulting firm report that projected savings of $20 billion per year by 2022 in a market where the aggregate operating costs amount to $65 to $80 billion a year (Irrera, 2015).

3(b). Blockchains in the capital markets

Blockchains have been proposed as solutions to numerous problems in securities trading, clearing, settlement, and antecedent activities such as shareholder voting and the enforcement of covenants via smart contracts. A wide range of pilot programs have occurred in applying blockchains to capital markets, ranging from the issuance of bonds over blockchain platforms by Daimler Benz, the World Bank, and Societe Generale, to holding shareholder voting on a blockchain for companies listed on the Estonian stock exchange.

The potential for using blockchains and distributed ledgers to modernize stock markets has probably received the most public attention among the large set of such initiatives underway across the investments industry. Blockchains have appeal for clearing and settlement in the equity markets due to the extreme complexity of current systems. To settle an equity trade in the United States today requires two days, due to the large number of offsets, error checks, and redundancies built into the process (Figure 3). This complexity appears to be an artifact of the overlapping and asynchronous system of share ownership ledgers kept by companies, brokers, and clearinghouses, none of which has a complete, up-to-date view of the true ownership of a company's circulating shares.

A number of start-up companies have attempted to create new capital and derivative markets using blockchains with the goal of near-immediate settlement of trades; one of the most visible has been the t0 exchange created by the firm overstock.com. While none of these market entrants poses an immediate threat to the major market exchanges, a large number of the most prominent stock markets have begun to experiment with blockchain projects with an eye toward the innovative efforts of these new market entrants.

The most visible and ambitious of these efforts has been the transition of the entire ASX market in Sydney, Australia, to a distributed ledger platform. The project, which was first announced in January 2016, is currently set to launch in the second quarter of 2021 after a lengthy validation and on-boarding process. In the U.S., the Depository Trust Clearing Corp., the clearinghouse for numerous equity and derivatives markets, is engaged in a similar validation program for blockchain platforms that are scheduled to go into use for some products in mid-2019. Broadridge, the company that tabulates proxy voting for the large majority of U.S. shareholder elections, is also building out blockchain platforms for streamlining and securing its processes. A related project has been undertaken by The Vanguard Group, one of the largest U.S. asset management firms, which has partnered with Symbiont to track the composition of equity market indexes on a blockchain platform; these data are critical to Vanguard's famous portfolio of indexed equity funds, which require accurate and secure reflection of the underlying index memberships.

Nearly all of these capital market initiatives take a business-to-business rather than business-to-customer approach, meaning that they are opaque to end users. They seek to improve the "plumbing" of the capital markets by enhancing the speed, reliability, and security of the client experience without disturbing the way in which clients interact with the platform.

3(c). Blockchains in real estate

Real estate represents the largest source of worldwide wealth, and it relies on ledger systems in which titles to property are kept by political authorities. In much of the world, these systems are incomplete, inconsistent, vulnerable to political manipulation, or even non-existent. Recording real estate titles on blockchains has the potential to clarify and secure property rights, which in turn could promote the use of real estate as collateral for financing business investment and economic growth. The absence of secure real estate systems is cited by de Soto (2000) as a leading cause of underdevelopment in much of the Southern hemisphere, and the weaknesses of real estate ledgers create large transaction costs and frictions even in wealthy economies such as the United States.

A number of underdeveloped countries such as Honduras, Ghana and Georgia have proposed national blockchain real estate ledgers and in some cases begun to build them. To date, the most comprehensive attempts at a blockchain title system have occurred in Sweden, where the Lantmäteriet national land registry has built and successfully tested a blockchain platform for real estate transfers. The company responsible for Sweden's system, ChromaWay, in late 2018 was engaged to build a similar pilot program in the Australian state of New South Wales.

At least two major challenges have not yet been solved in the introduction of blockchain real estate ledgers. First, if the current allocation of property is disputed at the time that a blockchain based registry is launched, the new ledger may validate an arrangement of ownership that faces principled objections from those without access to political power. Second, real estate is an inherently complex asset, with many encumbrances such as easements and covenants, some of which are contingent or time-limited. Recording this diverse data in a manageable form seems challenging, and the applications of blockchains to recording ownership of real assts may be more promising with more homogenous goods such as automobiles or heavy machinery.

3(d). Blockchains in trade finance

Providing short-term financing for goods and raw materials in transit is among the most complex and multi-faceted markets in the financial world. Among other obligations, payments must be made to numerous transport companies, import-export duties must be paid when goods cross national borders, and various liens and letters of credit expire when goods are delivered to various intermediate or final destinations. Many different ledgers are kept independently by transporters, lenders, and other parties connected to the movement of freight, and the entries in these ledgers will not always agree for at least two reasons. The first is the possibility of innocent record-keeping errors, which can lead to disagreements about payments that may be resolved only by the lengthy mailing of paper documents back-and-forth. Second, many participants in the supply chain will have incentives to falsify entries in their own journals, such as representing the arrival of a delivery truck as occurring earlier than it actually did in order to reduce the carrying cost of a loan or avoid performance penalties. In a significant number of cases, these problems are so severe that trade finance cannot be obtained at all, and export orders are cancelled as a result according to Jessel and DiCaprio (2018).

A distributed ledger, shared and updated by all parties, appears to be a tailor-made solution to these problems. Figure 4 illustrates the essential logic, illustrating the interactions in a simple transaction involving a shipper, recipient, and two finance companies., In the current system, represented on the left, separate documents are created and exchanged back-and-forth in all directions. In the distributed ledger system, shown on the right, one ledger is kept and viewed by all parties with authorization.

Keeping these ledgers in a blockchain environment would enhance their security by eliminating the opportunity for any one party to edit, backdate, or otherwise change the history of the ledger. Given the moral hazard problems connected to mis-reporting, using a blockchain seems particularly opportune The opportunity for potential savings is vast, given that the trade finance market is currently worth up to $12 trillion annually (Jessel and DiCaprio, 2018).

A prominent example of a successful trade finance blockchain, as described by Morris (2018), is we.trade, a consortium of approximately a dozen prominent European banks that uses a shared ledger built by IBM on Hyperledger Fabric to facilitate timely payments tied to the movement of goods.

4. Conclusions

Blockchain and distributed ledger technology represents a significant innovation in record-keeping. While applications of blockchains may become important in diverse areas such as healthcare data or government vital statistics, the finance industry unquestionably represents the source of the largest number of potentially high-value use cases.

Today some of the largest financial institutions in the world, including major commercial banks, stock exchanges, and central banks, have launched ambitious projects to use blockchains in both wholesale and retail applications. For regulatory reasons the wholesale applications, nearly always in the form of permissioned blockchains, appear to be the furthest along. However, significant disruptions to the legacy financial system still appear to be years away, and the scale of potential savings, while potentially eye-popping, remains mostly a matter of speculation among market participants.

References

Biais, B., C. Bisère, M. Bouvard, and C. Casamatta, 2019, “The blockchain folk theorem,” Review of Financial Studies 32, 1662-1715.

de Soto, H., 2000, *The mystery of capital: Why capitalism triumphs in the west and fails everywhere else.*

Foley, S., J.R. Karlsen, and T.J. Putniņš, 2019, “Sex, drugs and Bitcoin: How much illegal activity is financed through cryptocurrencies?” Review of Financial Studies 32, 1798-1853.

Haber, S. and W. S. Stornetta, 1991, “How to time stamp a digital document,” in *Advances in Cryptology - CRYPT0’ 90*, Lecture Notes in Computer Science 537, 437–455.

Irrera, Anna, 2015, “UBS building virtual coin for mainstream banking,” The Wall Street Journal, September 3, available at https://blogs.wsj.com/digits/2015/09/03/ubs-building-virtual-coin-for-mainstream-banking/.

J.P. Morgan, 2018, *Blockchain and the decentralization revolution.* Available at https://www.jpmorgan.com/global/cfa/blockchain.

Jessel, B., and A. DiCaprio, 2018, “Can blockchain make trade finance more inclusive?” Journal of Financial Transformation 47, 35-50.

Ju, L., J. Lu, and Z. Tu, 2016, “Capital flight and Bitcoin regulation,” International Review of Finance 16, 445-455.

Khatri, Yogita, 2019, “Thai central bank builds blockchain solution for digital currency project,” Coindesk, May 7, available at https://www.coindesk.com/thai-central-bank-builds-blockchain-solution-for-digital-currency-project.

Morris, N., 2018, “Trade finance blockchain race is about to start,” Ledger Insights, available at https://www.ledgerinsights.com/wetrade-trade-finance-blockchain-race/.

Nakamoto, S., 2008, “Bitcoin: A peer-to-peer electronic cash system,” unpublished manuscript.

Szabo, N., 1996, “Smart contracts: Building blocks for digital markets” Extropy: The Journal of Transhumanist Thought, 16.

Yermack, D., 2017, “Corporate governance and blockchains,” Review of Finance 21, 7-31.

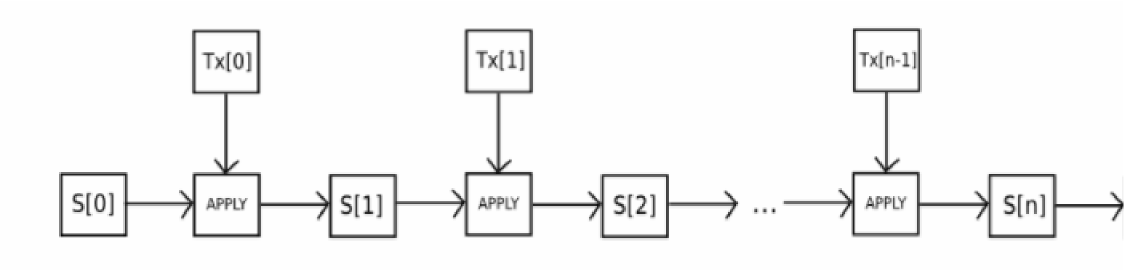
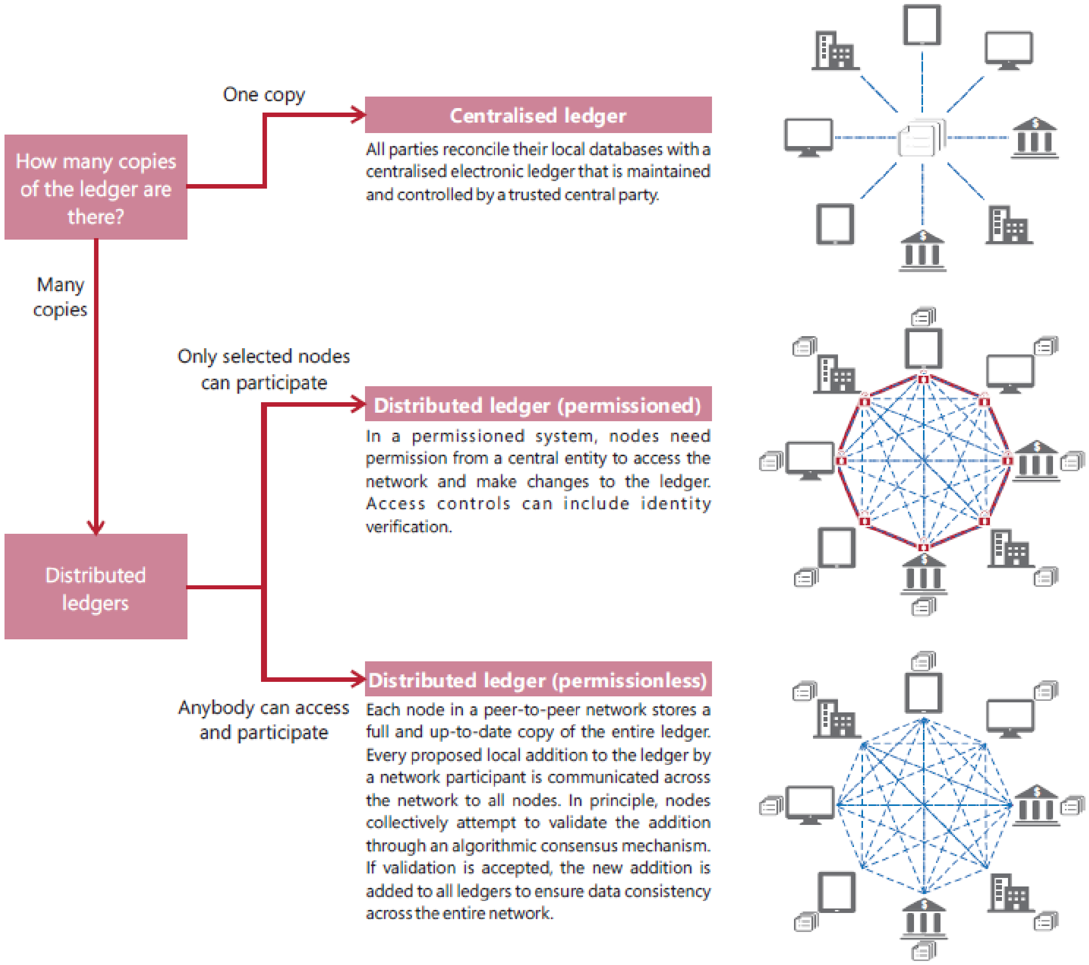


Figure 1
Arrangement of data in a blockchain ledger

In each block *n* the data for a new transaction, Tx(*n*), is merged with the encryption of the prior block, S(*n*-1), to create the encrypted output S(*n*). This in turn becomes an input to the subsequent block *n*+1. If a prior transaction is changed, this data structure causes all subsequent blocks to change, allowing anyone with access to the ledger to realize not only that data had been tampered with, but also the precise point in the ledger where the tampering had occurred.

Source: Ethereum White Paper,
https://github.com/ethereum/wiki/wiki/White-Paper


How many copies of the ledger are there?
One copy
Centralised ledger
Many copies
Distributed ledgers
Only selected nodes can participate
Distributed ledger (permissioned)
Anybody can access and participate
Distributed ledger (permissionless)

All parties reconcile their local databases with a centralised electronic ledger that is maintained and controlled by a trusted central party.

In a permissioned system, nodes need permission from a central entity to access the network and make changes to the ledger. Access controls can include identity verification.

Each node in a peer-to-peer network stores a full and up-to-date copy of the entire ledger. Every proposed local addition to the ledger by a network participant is communicated across the network to all nodes. In principle, nodes collectively attempt to validate the addition through an algorithmic consensus mechanism. If validation is accepted, the new addition is added to all ledgers to ensure data consistency across the entire network.

Figure 2
Permissioned and Permissionless ledgers

Source: BIS Annual Economic Report 2018, p. 96, https://www.bis.org/publ/arpdf/ar2018e5.pdf

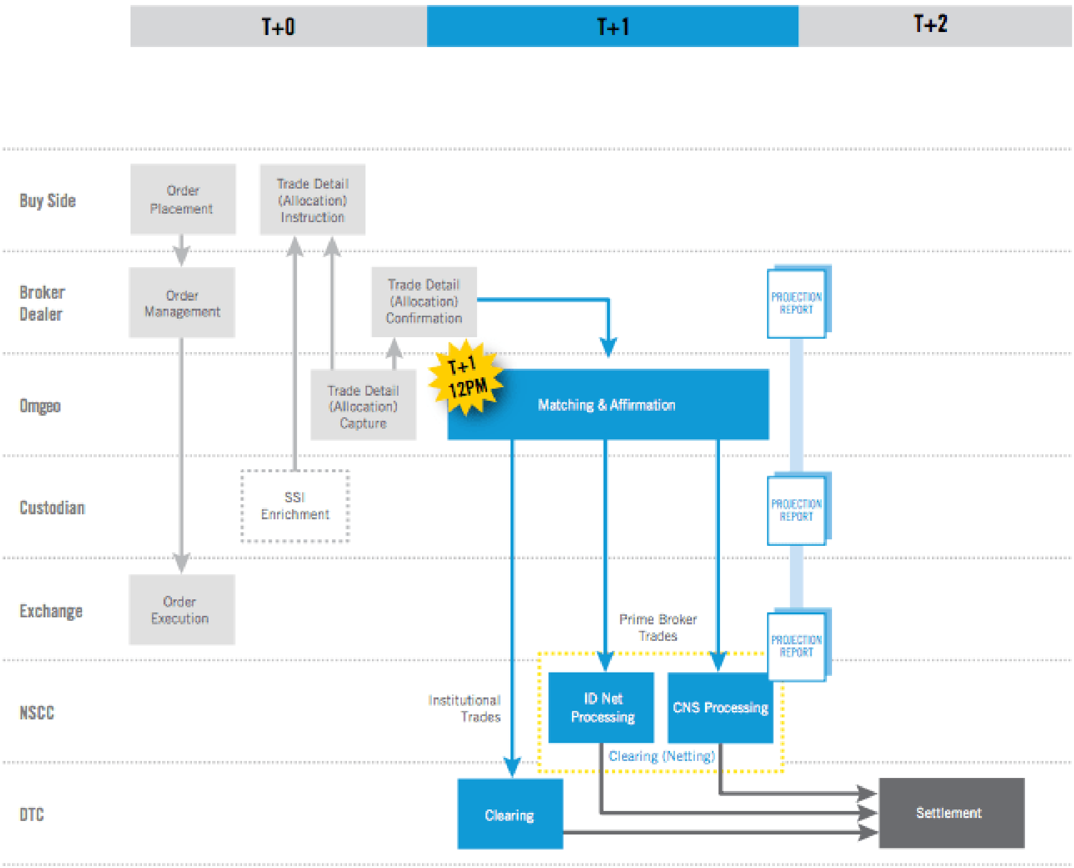


Figure 3
Schematic of equity trade clearing and settlement in the U.S. markets

Source: Depository Trust Clearing Corp.

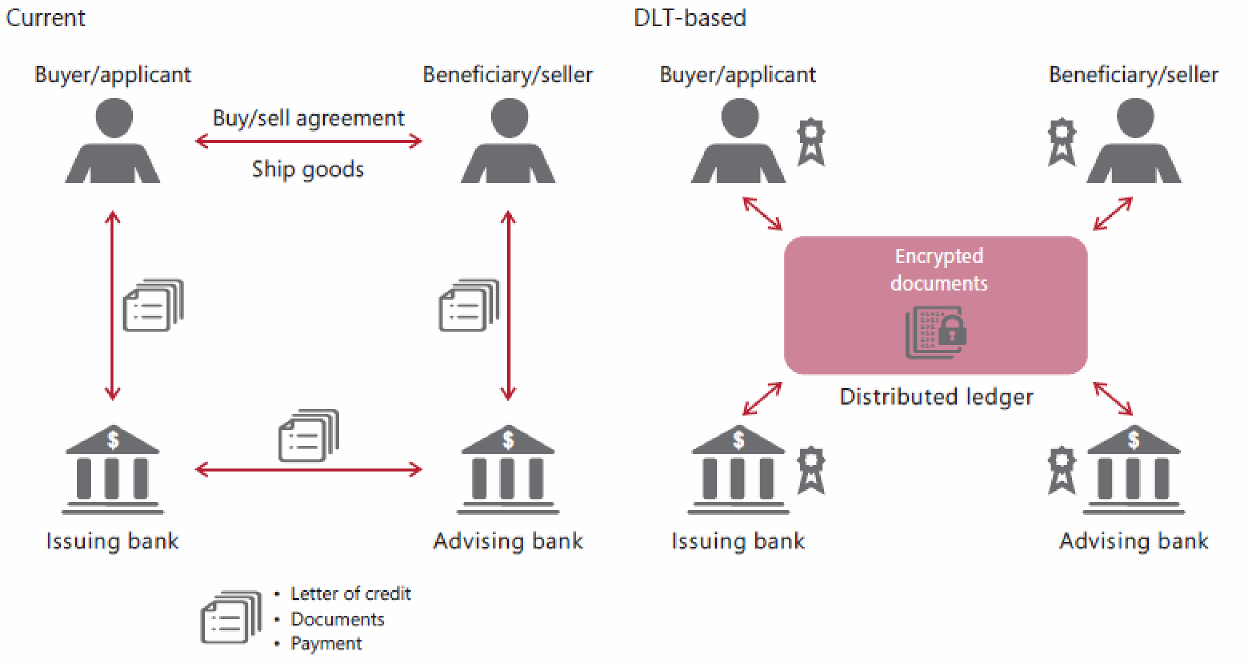


Figure 4
Reorganization of trade finance using a distributed ledger

Source: BIS Annual Economic Report 2018, p. 106,
https://www.bis.org/publ/arpdf/ar2018e5.pdf