7
2017
Economic perspectives

Blockchain and financial market innovation

Rebecca Lewis, John McPartland, and Rajeev Ranjan

Introduction and summary

Blockchain technology is likely to be a key source of future financial market innovation. It allows for the creation of immutable records of transactions accessible by all participants in a network. A blockchain database is made up of a number of blocks "chained" together through a reference in each block to the previous block. Each block records one or more transactions, which are essentially changes in the listed owner of assets. New blocks are added to the existing chain through a consensus mechanism in which members of the blockchain network confirm transactions as valid. The technology allows the creation of a network that is "fully peer to peer, with no trusted third party," such as a government agency or financial institution.[1]

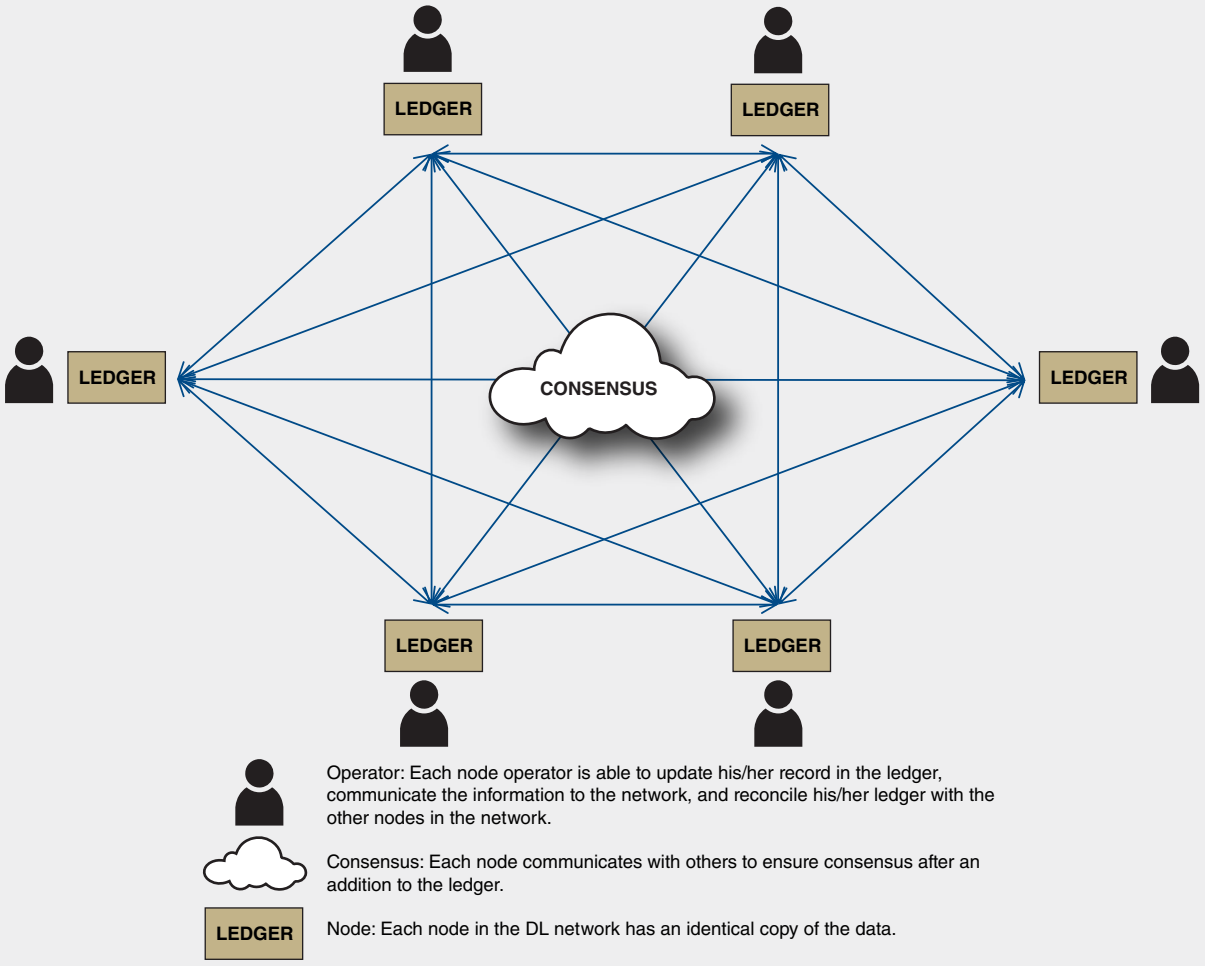
While all are in the early stages of development, there are many promising applications of blockchain technology in financial markets. The bitcoin ecosystem represents the largest implementation of blockchain technology to date.[2] Interest in the technology continues to grow in the financial technology and broader financial services communities. In this article, we provide a brief overview of what blockchain technology is, how it works, and some potential applications and challenges.

What is a blockchain database?

A blockchain database has a network of users, each of which stores its own copy of the data, giving rise to another term for blockchain technology: distributed ledger technology (DLT). Basic elements of a DLT network are: a digital ledger, a consensus mechanism used to confirm transactions, and a network of node operators (see figure 1 for the network setup). Generally speaking, the terms DLT and blockchain are used interchangeably in position papers and popular media, though DLT is considered by some to be a more general term.

FIGURE 1

Distributed ledger (DL)–Setup



Source: Financial Markets Group, Federal Reserve Bank of Chicago.

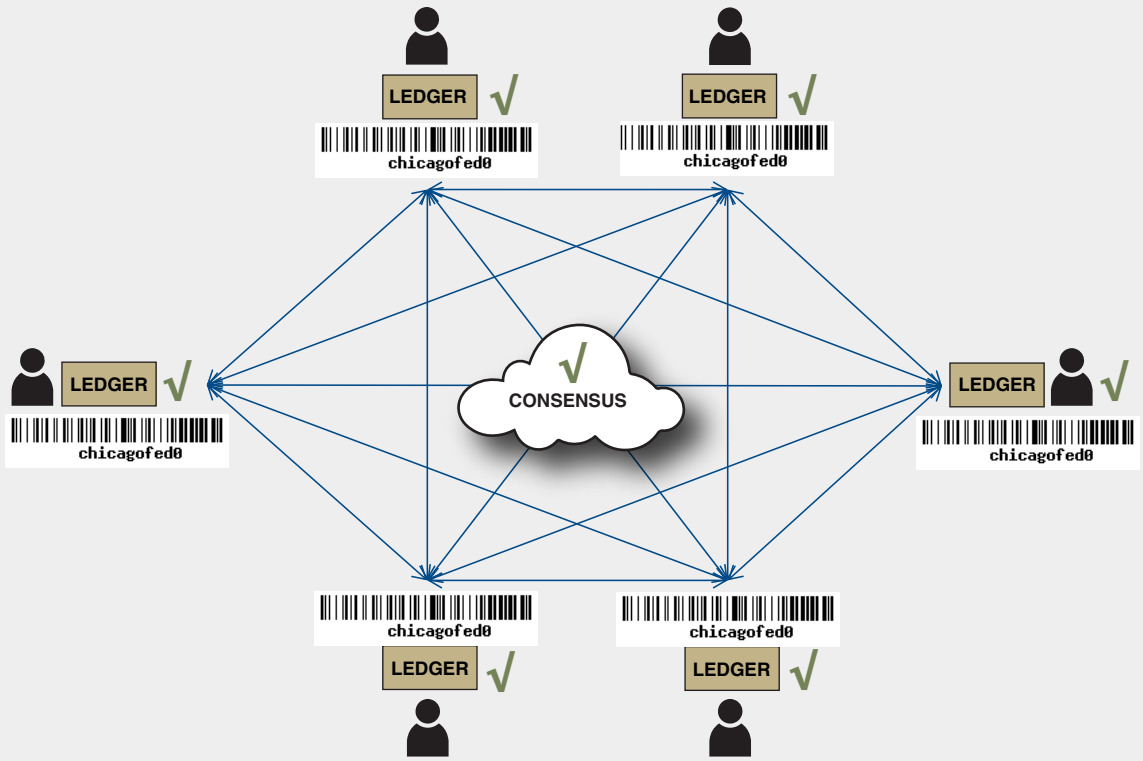
As one industry participant involved in developing blockchain technology described it, blockchain technology is essentially a new approach to database architecture. "Fundamentally, [it is] an improvement over the way that, traditionally, databases have been designed and used in the past."[3] A traditional database is a large collection of data organized for rapid search and retrieval. While there are various ways of organizing data, traditionally, the vast majority of databases have been relational, storing data in tables that users can update and search.[4] Relational databases are centralized, with a master copy controlled by a central authority. Users sharing a database must trust the central authority to keep the records accurate and maintain the technological infrastructure necessary to prevent data loss from equipment failure or cyberattacks. This central authority represents a single point of failure; if the central authority fails, the database is lost. Users who do not trust one another must maintain separate databases that they periodically reconcile.

How does blockchain technology work?

The key elements of a blockchain-based ledger, those that will enable future efficiency gains, are the distributed nature of the ledger, its immutable character, and the existence of an agreed-upon consensus mechanism. These make it possible to automate transactions, providing for close to real-time settlement, while maintaining

FIGURE 2

Distributed ledger (DL) network–All records are updated



Operator: Each node operator is able to update his/her record in the ledger, communicate that information to the network, and reconcile his/her ledger with the other nodes in the network.

chicagofed0 This represents the current state of the ledger.

Source: Financial Markets Group, Federal Reserve Bank of Chicago.

strong controls against fraud. These benefits do not depend on the exact technical implementation of any given blockchain—implementations will continue to be worked out in the coming years. However, a high-level overview of how a blockchain works helps to inform discussions about potential applications of blockchain and challenges that may arise.

A simple distributed ledger

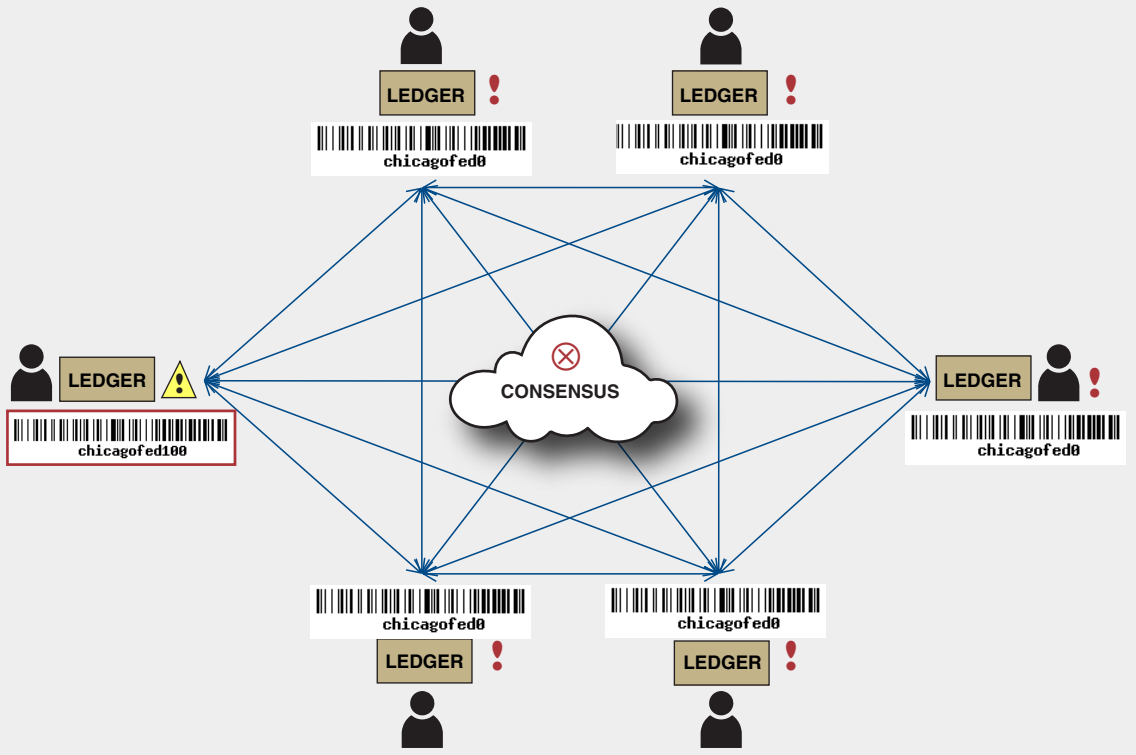
In its simplest form, each user can read from and write to the database; and each user's copy is updated to reflect the new state of the ledger after a transaction is confirmed through a previously agreed-upon consensus mechanism (see figure 2). Once a transaction is added, it cannot be updated or deleted.

In the example in figure 2, all the node operators have the same version of the ledger ("chicagofed0"). Since all the versions of the ledgers are the same, consensus is achieved and the records are final.

When a member of a blockchain network engages in a transaction, they submit the transaction to the network (see figure 3). The submission of the new transaction changes the state of the ledger (here to "chicagofed100"), which is now in conflict with the state of other copies of the ledger. Once the new transaction is discovered by the network, the consensus breaks, forcing other operators to either validate and update their records with the latest change or reject the new addition to the ledger.

FIGURE 3

Distributed ledger (DL) network–New record added and state changes



Source: Financial Markets Group, Federal Reserve Bank of Chicago.

A consensus mechanism then confirms the submitted transaction as valid. There are various methods of achieving consensus on a blockchain, as we discuss below. At this point, it is simply important to understand that a blockchain database must have a mechanism through which participants agree to a change in the state of the ledger. Once consensus is achieved, all ledgers are updated to reflect the new state (see figure 4).

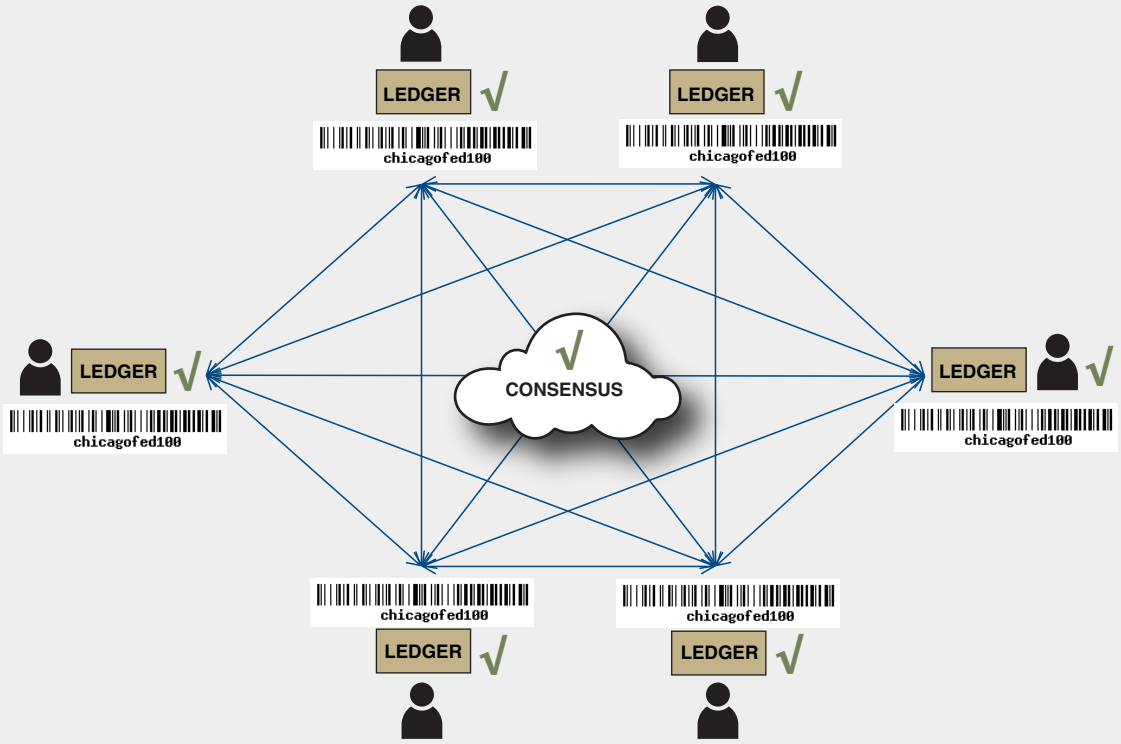
How are transactions added to a blockchain?

At its most basic level, a transaction on a blockchain is simply a change in the registered owner of an asset. The process through which transactions are created and added to the blockchain is illustrated in figure 5.

For person A to transfer an asset to person B, it is first necessary to determine if A is the rightful owner of that asset. This can be done by referencing past transactions in the blockchain and finding that, at some point, A received the asset and has not yet sold it. Once this is done, A and B can agree to the transaction (step 1). A block is created with the details of the new contract (step 2), and then A and B agree to the contract by adding their unique digital signatures (steps 3 and 4). Once both parties have signed the transaction, a cryptographic hash is calculated that will be used to link this new transaction to the chain of previous transactions (step 5). The cryptographic hash is a string of characters associated with a given block that is difficult to calculate but easy to verify. This makes it simple to verify a legitimate block, but difficult to engineer and insert into the chain a block recording illegitimate transactions.

FIGURE 4

Distributed ledger (DL) network–Reconciliation and consensus achieved



When all node operators agree to the change and consensus is reached, the entire network will update their own ledgers. This ensures the immutability of records for network participants and end-users.

Source: Financial Markets Group, Federal Reserve Bank of Chicago.

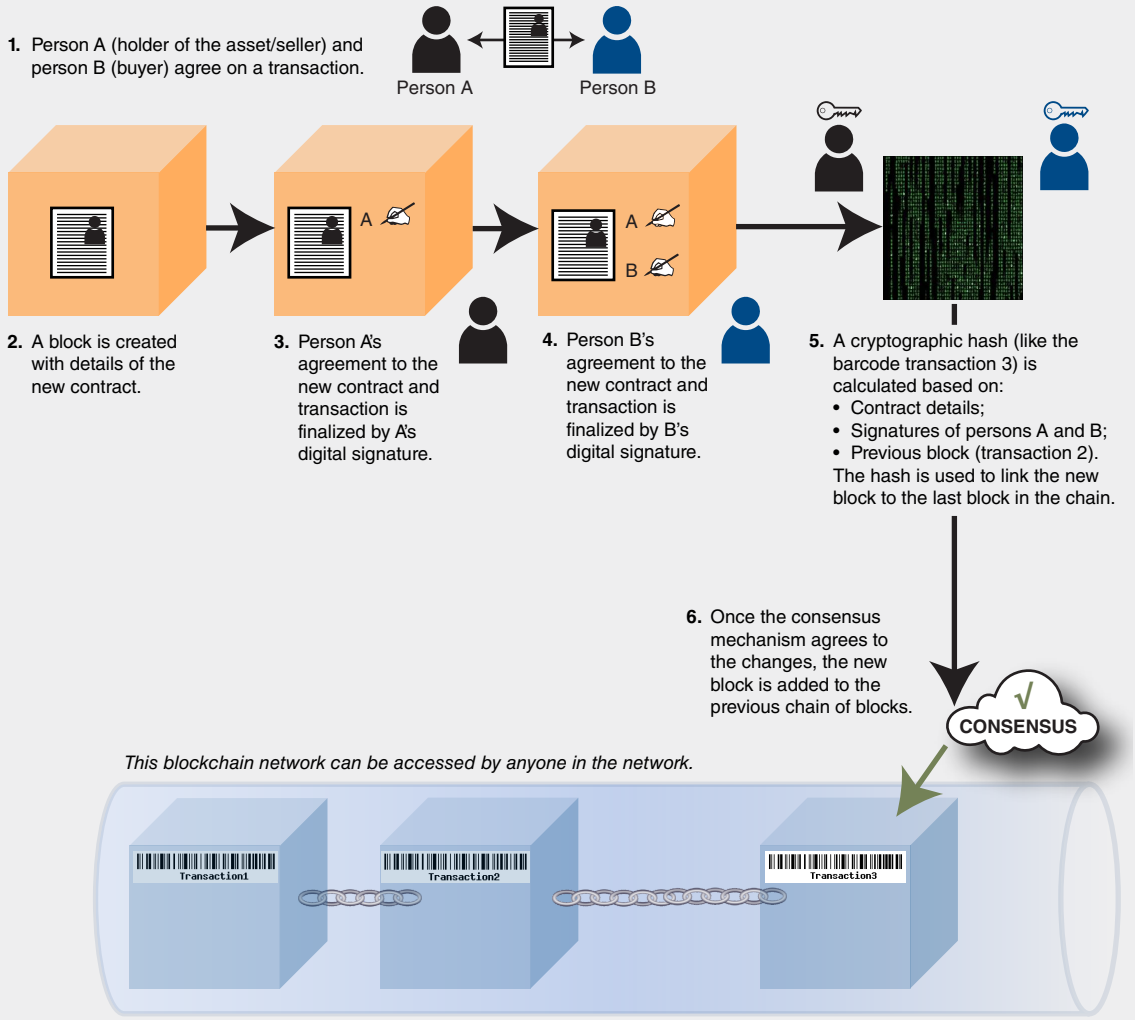
Next, the transaction is confirmed using the blockchain's consensus mechanism (step 6). After confirmation, the transaction is added to a block of recent transactions. This block is then "chained" to the previous blocks of transactions through a reference to the most recently created block in the chain. The updated blockchain would then be transmitted to all participants in the network so that everyone has a matching copy of the master ledger.

Permissionless networks

Blockchain technology was first used in 2009 to implement the digital currency bitcoin. The bitcoin blockchain is an example of a public network: It is open to any user who wishes to transact, and all users can see all transactions on the blockchain. The network is also permissionless: New transactions are added to the blockchain through a cryptographic consensus mechanism requiring vast amounts of computing power to confirm transactions. The chief advantage of a permissionless network is that it does not require a central authority to confirm or deny specific transactions; individuals who do not trust one another or any single central authority can transact on the permissionless network, relying on a consensus mechanism to ensure the ledger's accuracy. This avoids the need for users to have their own database that they periodically reconcile against those of their counterparties. Instead, all transactions are recorded on a single database. Each user stores a copy of the database, so there is no single point of failure as exists with traditional relational databases. Once they are added to the blockchain transactions cannot be undone, making the ledger an immutable record of all previous transactions. Figure 6 provides an illustration of a permissionless and public blockchain network.

FIGURE 5

Blockchain (DL) network–Stylized example of a transaction



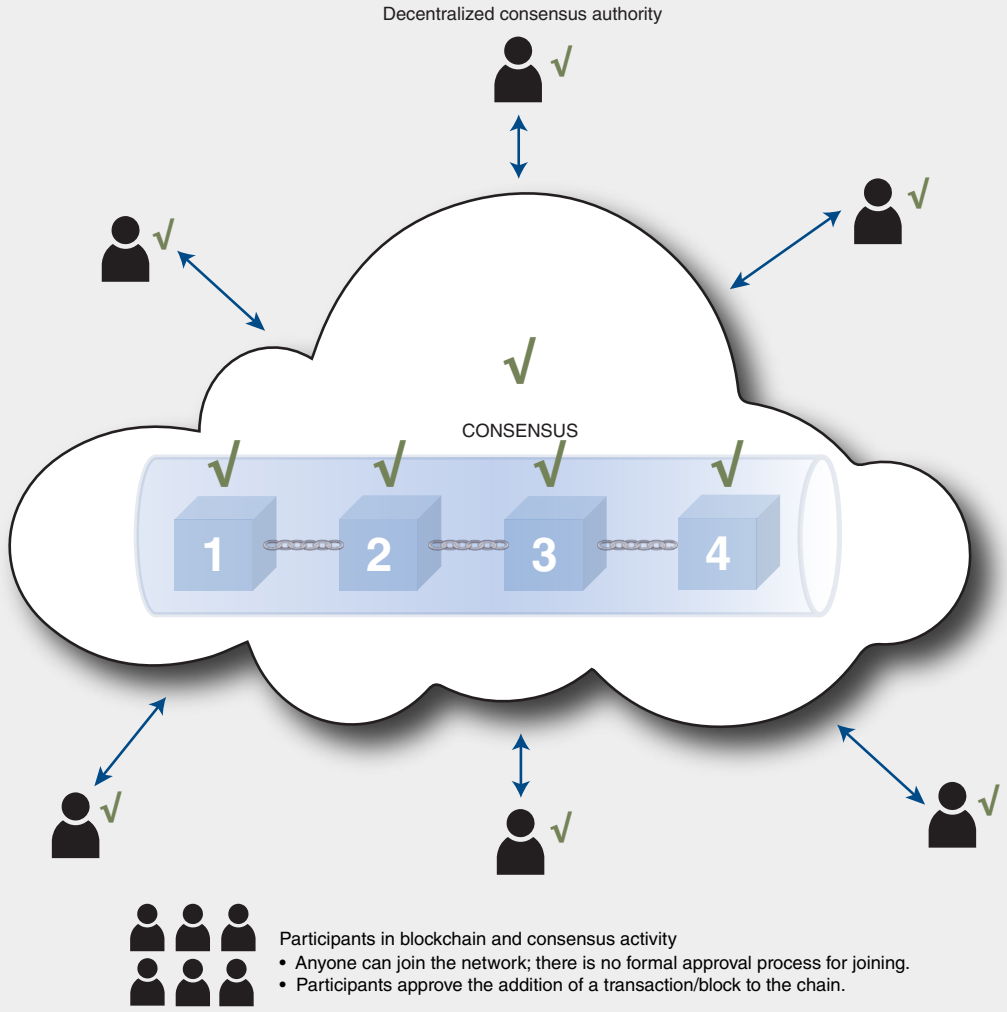
Source: Financial Markets Group, Federal Reserve Bank of Chicago.

Permissioned networks

Many see broad accessibility and a lack of a need for centralized control as two of blockchain's key benefits relative to traditional database architectures. However, for applications in financial markets where 1) there are trusted intermediaries, 2) complete transparency is not always desirable, and 3) participants must comply with regulatory requirements, this decentralized system has shortcomings. It is likely that applications of blockchain technology in financial markets will instead use private and permissioned blockchains. Private blockchains are only open to those participants that meet the membership criteria of the network, in contrast to public blockchains in which anyone is able to participate. Permissioned blockchains allow certain members to control the confirmation of transactions. These permissioning members (consensus authorities) can exert control in various ways depending upon the network design. They could be responsible for explicitly approving transactions. Another option would be to designate the permissioning members as the sole members of the network able to participate in a cryptographic consensus mechanism. Figure 7 provides an illustration of a permissioned and private blockchain network.

FIGURE 6

Permissionless/public blockchain network



Source: Financial Markets Group, Federal Reserve Bank of Chicago.

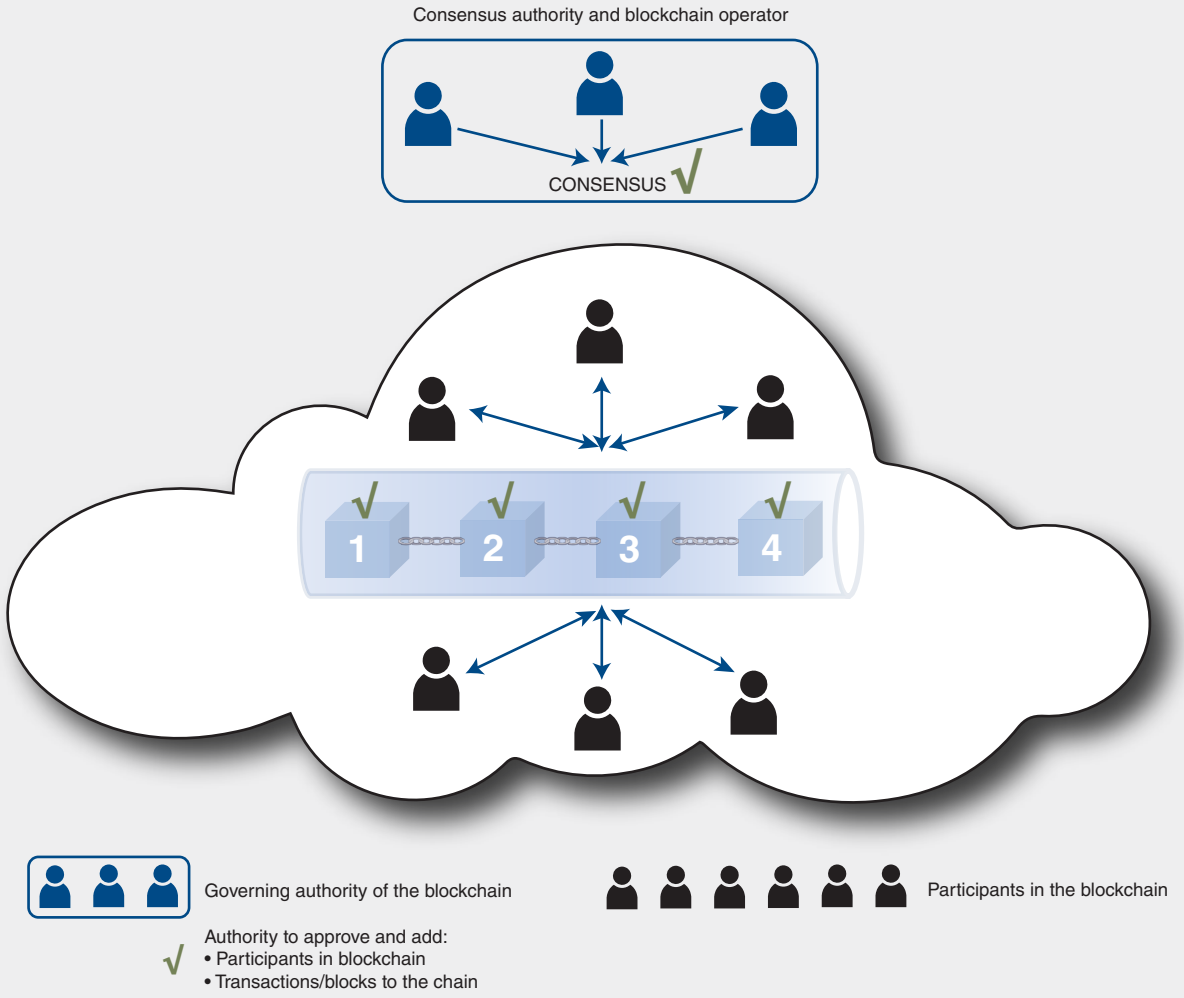
Some argue that a permissioned blockchain removes "a major benefit of the blockchain system: the system works between parties that do not need to trust each other. If the concept is to implement permissioned distributed ledgers between trusted [parties] … why would you use blockchain technology when more efficient alternatives are available?"[5] However, permissioned blockchains retain many key features and benefits of permissionless blockchains, including the decentralized storage of the database and the (near) real-time reconciliation of all copies of the database. They also alleviate some of the problems posed by the permissionless system, including its need for substantial computing resources to confirm transactions.

Regulatory imperatives such as Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements provide further reasons to prefer permissioned blockchains for financial applications, as transactions on a fully public, permissionless blockchain are anonymous and open to all, while private systems can limit participants to those who are pre-approved and trusted.

In permissioned blockchains, it is also possible to put controls in place to allow varying levels of access to the information in the ledger. For example, regulators could be allowed to view all the details of a transaction

FIGURE 7

Permissioned/private blockchain network



Source: Financial Markets Group, Federal Reserve Bank of Chicago.

in the ledger but not add any transactions, while users might be allowed to view selective details of the transactions depending on their access level (see figure 8).

Consensus mechanism

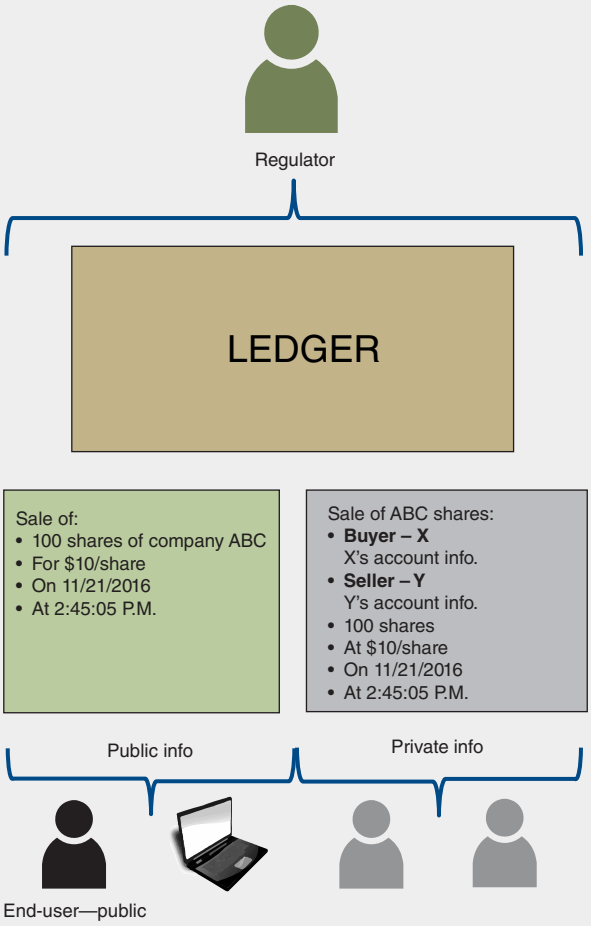
All blockchains have a consensus mechanism that is used to add new blocks to the database. The consensus mechanism will differ depending upon the design of the blockchain, especially whether the blockchain is permissioned or permissionless. If the blockchain is permissioned, the degree to which participants in the network are willing to trust one another also has an effect on the consensus mechanism. In a permissioned blockchain, once the transaction is submitted by the two parties involved, it would then be confirmed by a permissioning member of the blockchain or by some cryptographic consensus mechanism accessible only by permissioning members. Trust in transactions is maintained because users trust the network member(s) with the power to confirm transactions.

FIGURE 8

Ledger properties

In this example, buyer X buys 100 shares of a company ABC from seller Y at $10 per share and records the transaction on a distributed ledger.

The ledger has some elements that are public and can be viewed by all with access to the ledger. Other elements are private; only some users (such as the regulator) have access to those elements.



Source: Financial Markets Group, Federal Reserve Bank of Chicago.

Permissionless blockchains rely on their network of participants to confirm transactions, using a variety of algorithms to ensure the validity of transactions. One implementation of a permissionless blockchain, the bitcoin blockchain, uses a Proof of Work consensus mechanism. On the bitcoin blockchain, individuals known as miners compile submitted transactions into blocks. They confirm that those spending bitcoins in each transaction received those bitcoins from some earlier transaction recorded on the blockchain and race to solve a difficult computer problem; the first miner to solve the problem confirms their block and adds it to the blockchain. The miner is awarded a certain number of bitcoins in return. Because every user on the blockchain has access to the entire ledger, users can confirm for themselves that the latest block of transactions added to the chain records valid transactions, that is, that the users spending bitcoins in the latest round of transactions received them in some earlier transaction and have not yet spent them.

A relatively automated consensus mechanism allows for the near-instantaneous update of every copy of the ledger—once a transaction is added to the blockchain, all ledgers reflect this change. There is no need for further post-trade reconciliation. The way in which blocks are added to the ledger also creates an essentially immutable database. Since blocks of transactions are chained together, the older the transaction is, the more difficult it becomes to fraudulently change it. To fraudulently change a block, an actor would have to replace that block with a new block and regenerate all of the subsequent blocks in the chain. The consensus mechanisms ensure that regenerating blocks is difficult, either due to the oversight of permissioning members or to the time and energy required to create a block (in a permissionless system). The farther back in the chain a block is, the more difficult a change becomes because the number of blocks that an actor would have to regenerate increases. Thus, network members' confidence that a transaction will never be changed increases as the number of transactions following it increases.

Blockchain's applications, benefits, and challenges

Blockchain technology has the potential to provide large efficiency gains in businesses that currently require costly intermediation, including financial services. However, any implementation will also face a number of challenges. Regulators and policymakers, including the Committee on Payments and Market Infrastructures, are currently looking into both the potential applications of blockchain technology and the challenges that may arise.[6]

Applications and benefits

Possible applications of blockchain technology include:

Digital assets—Physical assets (real estate, stock certificates, gold, etc.) require a great deal of verification and examination every time they are traded, which prolongs the transaction and settlement time for each trade. DLT has the potential to transform the physical assets into a digital form for transactional and record-keeping purposes. Such digitized assets could essentially function as online financial instruments that change hands each time the owner of the asset recorded in a ledger changes.

Digital currencies—We are already in the era of online banking, payments, and transactions, all of which are carried out with little use of physical currencies. In recent years, various forms of cryptocurrencies have been adopted for real-world transactions. Cryptocurrencies rely on encryption techniques to generate, transact, and verify their value. They operate independently of a central bank's authority and are not backed by the central bank. Some central banks around the world (for example, China, the UK, South Africa, and the Netherlands) are experimenting with issuing digital state-sponsored fiat currencies backed by the central government.

Digital record keeping—One of the key benefits of blockchain is that it keeps an audit trail of each and every transaction and the details of the parties involved. If designed and executed well, blockchain databases will create records that are standardized, immutable, and easy for interested parties to query.

Smart contracts—In order to achieve their full potential, implementations of blockchain technology will likely be accompanied by smart contracts. Smart contracts are legal contracts written in computer code that execute automatically once certain conditions, specified in the contract, are fulfilled. Smart contracts can be added to distributed ledgers to self-execute on the basis of information in the ledger. This will allow for the automation of processes that currently require manual interventions.

Benefits that may arise from the use of blockchain technology include:

Reduction in settlement period (post-trade)—Settlement periods (the time between the execution of a trade and the performance of all duties necessary to satisfy all parties' obligations) can be drastically reduced with the swift record of submissions and their confirmation on a blockchain. This may foster greater liquidity in certain types of trades that currently face lengthy settlement cycles and may promote better capital usage. At present, the title to most financial assets can only be settled against payment when banks are open for business. If there were one blockchain that accounted for the ownership of money and another that accounted for the ownership of securities, then, assuming that buyers had sufficient funds and sellers had sufficient shares, a settlement versus payment of funds could occur at any time on any date in a matter of seconds, with legal finality and certainty.

Faster payments—Global payments systems require multiple regulatory checks and lengthy settlement cycles. The foreign exchange industry is one of the most intermediated markets in the world, requiring settlement banks and commercial banks to facilitate movement of currencies. A DLT service with digital identities for the parties involved in a trade could be used to shorten settlement times.

Challenges

The challenges posed by blockchain technology fall into two broad categories: technical and business; and regulatory.

Technical and business challenges

Achieving consensus—There is a need for consensus among a blockchain network's members. Since the ledger is distributed among all participants in the blockchain, any protocol changes must be approved by all. A potential solution, possible in a permissioned network, would be to allow one or a few participants the authority to make protocol changes that were binding upon the entire network. This, however, requires significant trust in the authorized participants.

Standardization—There is also a lack of standardization of blockchain network designs, which can cause major issues in their implementation and acceptance by businesses. Many national and international organizations are trying to establish generally accepted technical standards.

Interoperability—Current businesses will face challenges related to interoperability of blockchain platforms with their existing internal systems. Externally, it remains to be seen how blockchains from multiple businesses might operate with each other.

Scalability—The need to increase the scale of distributed ledger systems also represents a challenge, especially for permissionless blockchains that use a race to solve a computer problem in order to confirm a transaction. The race takes a large amount of computing power, limiting the speed with which new transactions can be confirmed. All networks, permissioned or permissionless, will require a large amount of storage resources, as each node in the network will maintain its own copy of the distributed ledger.

Efficiency—There will be trade-offs between the efficiency of a blockchain and its ability to avoid relying on trusted parties. A complex computational system to confirm transactions is less efficient than a system more reliant on the discretion of permissioning nodes in the network but offers the advantage of not needing everyone in the network to agree to trust certain parties.

Immutability—Once added to the blockchain, a transaction is permanent. "Fat-finger" trades, or trades that regulators demand be reversed, can only be changed by submitting an equal and offsetting trade, which the parties involved in the original trade will both need to accept.

Legal uncertainty—Currently, firms do not have clarity over the laws and regulations that will apply to DLT implementations in cases of fraud, bankruptcy, and other failure scenarios. This is especially a problem for firms that operate in multiple jurisdictions.

Security—While the reduced reliance on a central authority and the fact that copies of the ledger are stored in more than one place ameliorate the single point of failure problem present in many legacy systems, blockchain's distributed nature also creates security concerns. The more participants in the network, the more points of attack there are for cybercriminals to target. If cybercriminals are able to steal the information of a user necessary to submit a trade, they could create fraudulent, and immutable, transactions.

Liquidity—The use of a blockchain for title transfers could drastically reduce the risk associated with current settlement conventions, but it will increase the importance of liquidity; funds and assets must be in proper form and location for such expedited settlement.

Privacy—Blockchain's potential impact on the confidentiality and speed of information transfer about record changes may also be of concern to some users. For example, in finance, the acquisition and analysis of data are key to a firm's competitive advantage. Some firms may be reluctant to participate in a shared database in case of information leakage that could cost the firm's business.

Intellectual property—Blockchain technology may be subject to legal challenges and costs that could impede innovation. Industry participants involved in blockchain research are increasingly patenting blockchain-related technologies; the number of blockchain-related patents filed doubled between January and November 2016.[7] The patents could make firms working with blockchain technologies vulnerable to legal challenges and prevent new firms from entering the market.

Regulatory challenges

Uncertainty—There is currently uncertainty over rules across various regulatory agencies. Existing regulations may be major hurdles for DLTs. To enable innovation, regulatory agencies should work alongside DLT firms as they test new products and services.

Currency control—Central banks will have to find ways to maintain control over digitized currencies. If central banks were to allow commercial banks to place money in special accounts and then digitize the money on the bank's blockchain, regulators would need a mechanism for overseeing its use and ensuring that the digital currency issued did not exceed the amount held as central bank reserves.

Conclusion

While much work remains to be done, blockchain represents a promising source of future innovation in financial markets. DLT technology possesses the capability to improve the efficiency and security of financial markets, provided it is implemented in the right way. In the near future, we will see the development of specific applications of DLT that are likely to enable better cooperation between the public sector and private sector and improve transparency, trust, information sharing, and audit trails.

NOTES

[1]Details online, https://www.economist.com/news/special-report/21650295-or-it-next-big-thing.

[2]Details online, http://mitsloan.mit.edu/newsroom/articles/blockchain-explained/.

[3]Morgan Stanley, 2016, "Global insight: Blockchain in banking: Disruptive threat or tool?," Global Financials/FinTech, *Morgan Stanley Global Insight*, April 20, p. 28, available online, http://www.the-blockchain.com/docs/Morgan-Stanley-blockchain-report.pdf.

[4]Sebastien Meunier, 2016, "Blockchain technology—a very special kind of distributed database," *Medium*, December 29, available online, https://medium.com/@sbmeunier/blockchain-technology-a-very-special-kind-of-distributed-database-e63d00781118, accessed on June 15, 2017.

[5]Izabella Kaminska, 2016, "How I learned to stop blockchain obsessing and love the Barry Manilow," Alphaville, *Financial Times*, August 10, available online by subscription, https://ftalphaville.ft.com/2016/08/10/2172380/how-i-learned-to-stop-blockchain-obsessing-and-love-the-barry-manilow/.

[6]Bank for International Settlements, Committee on Payments and Market Infrastructures, 2017, "Distributed ledger technology in payment, clearing and settlement: An analytical framework," report, Basel, Switzerland, February, available online, http://www.bis.org/cpmi/publ/d157.pdf.

[7]Olga Kharif, 2016, "Who owns blockchain? Goldman, BofA amass patents for coming wars," *Information Management*, December 21, available online, http://www.information-management.com/news/data-management/who-owns-blockchain-goldman-bofa-amass-patents-for-coming-wars-10030542-1.html?CMP=OTC-RSS, accessed on June 15, 2017.

Rebecca Lewis is a financial markets analyst and John McPartland is a senior policy advisor in the Financial Markets Group at the Federal Reserve Bank of Chicago. Rajeev Ranjan is a senior vice president for operational risk in the Institutional Clients Group at Citigroup.

Economic Perspectives is published by the Economic Research Department of the Federal Reserve Bank of Chicago. The views expressed are the authors' and do not necessarily reflect the views of the Federal Reserve Bank of Chicago or the Federal Reserve System.

ISSN 0164-0682