

Master of Financial Technology

FNT 628

**Blockchain and
Cryptocurrencies**



www.midocean.ae

Table of Contents

1. Blockchain Technology.
2. How does blockchain technology work?.
3. Blockchain Applications.
4. Blockchain Benefits.
5. Blockchain Challenges.

Blockchain Technology

Blockchain Technology

- Blockchain may still be a new term for many readers. It is, therefore, appropriate to start with a discussion on the definition of blockchain.
- A ledger is a book of permanent record. The record must be correct and tamper free.
- A blockchain is a ledger that is put together on the Internet in a decentralized manner by an indefinite number of contributors.
- Blockchain is a chain of files containing whatever needs to be permanently recorded.
- A basic blockchain connects files to form a simple string of chain.
- A more sophisticated blockchain connects files to form a net-like structure.



Blockchain and Data Ownership

- A database is like an address book in which many data elements are stored systematically and organized for easy use. Blockchain is a new technology that allows us
- to record data and sources and recipients of data exchanged on the Internet, thereby creating an accurate, permanent, and very inexpensive database.
- The first application of blockchain technology was the virtual currency called Bitcoin.
- Functionally, a virtual currency is much the same as a deposit currency that is based on bank accounts. Each bank account records debits to and credits from other accounts, which the bank keeps to be absolutely accurate and tamper-free.
- Because the record shows who owes how much to whom, and because people trust that the records are absolutely reliable, it can be used to transfer money through wire transfers; debit cards are a major means of payment nowadays.

Blockchain and Data Ownership

A virtual currency is a similar collection of accounts (called wallets) that record debits and credits.

- The difference is that the virtual currency accounts are on the Internet.
- Blockchain technology has made it possible to keep this record absolutely reliable by using algorithm without relying on a central authority like a bank.
- Blockchain accounts record digital data, which plays the role of money because people trust that they are accurate and tamper-free.
- As this shows, blockchain can assign the ownership of each data piece to an account holder.
- This is the innovation that blockchain technology has brought to society.

Distributed Computing

- Distributed computing is a revolutionary innovation in computer networks, which allows many terminal computers to perform complicated tasks independently (Holohan and Garg 2005).
- One good example is a category of games called “massively multiplayer online games” in which many different players participate and try to achieve their respective goals, which may vary from car racing to shooting to role playing.
- Blockchain technology is built on this idea of distributed computing and adds decentralization to enable individual participants to maintain a secure record of transactions, ownerships, and promises.

Distributed Computing

- The initial design of a computer network, which connects many computers to share resources, is centrally managed.
- In building a centralized network, a network administrator is chosen, a large server computer is set up, a network connecting many computers is designed, and software is installed on the server and made available for network users.
- The administrator centrally manages users' network connections, and only users with connection permission can use the network.
- The networks of companies and universities are designed in this way, and the same is true for online banking systems that connect automatic teller machines (ATMs). In a centrally managed network, the terminal computers perform very minimal tasks.
- For example, a bank ATM terminal recognizes the account number and the password, and then performs simple tasks such as deposits and withdrawals.
- As a network becomes larger, it becomes more and more difficult to maintain a centralized network.
- The load on the central server increases, and the cost of managing the server becomes very large.
- Central servers can also become very attractive targets for malicious attacks, and once these servers are compromised, the entire system can be destroyed.

Distributed Computing

- A distributed network is built by connecting various independent servers and computers.
- Various tasks are distributed to different servers, and altogether a single goal can be achieved.
- A large volume of tasks are assigned to terminal computers.
- As long as basic rules for connecting to the network are set and those rules are followed, any server and any computer can join the network.
- Such rules are called protocols. In the most immediate example, the email address is separated by the at-mark; the part after the “at mark” is an address indicating a particular computer group; the part before is an individual in that group.
- This rule is a very small part of the large Internet protocol.
- A distributed network makes it possible to utilize a large portion of the computing power of the computers in a network.
- The various computers connected to the network perform large tasks by computing independently while coordinating tasks through exchange of data.
- Having a large number of computers work independently can achieve great goals at very low cost.

Blockchain: Decentralized Ledger

- Distributed computing has evolved as a computer network construction method.
- Blockchain is a technology that builds a ledger based on distributed computing in a decentralized manner.
- This might sound simple, but, in reality, it is not.
- To create a decentralized ledger, it is necessary to devise a totally new algorithm, and such work led to the creation of Bitcoin.
- To create and maintain a secure decentralized ledger, it is not enough to use a security program; such security measures can be easily breached by experienced hackers.
- Even if many independent computers maintain ledger together with good intentions, they are still vulnerable to attacks by computers with malicious intentions.
- This is especially so if such a ledger maintains records that function as money or virtual currency, where absolute accuracy and permanence are required.

Blockchain: Decentralized Ledger

- This problem was overcome by the first blockchain, known as Bitcoin.
- In most blockchain, the database is shared by a large number of servers.
- Each server stores the entire blockchain record and carries out similar jobs in parallel.
- These servers are called full nodes of a blockchain.
- A new server that wants to join a blockchain network is free to copy the blockchain record and download the necessary software to store the records.

Blockchain: Decentralized Ledger

- Once in a while, the records on participating servers are synchronized so that only one record is produced. With more nodes, the number of copies of the blockchain's ledger throughout the world increases, which makes it extremely difficult for malicious computers to attack the blockchain.
- The decentralized ledger database is linked with user accounts called wallets.
- A wallet is a record of a particular user's transactions, which is kept on the user's terminal computer.
- Once a transaction between two accounts is agreed upon, the account owners apply to the blockchain to record the transaction.
- In most of the existing blockchains, recorders of transactions are different from users who use a blockchain as a currency.
- In some blockchains, users of a blockchain record their transactions by themselves.

Mining

- The Bitcoin blockchain uses “mining” to maintain the accuracy and reliability of transaction records.¹ Mining in the context of blockchain technology is to present a computer-generated crypto puzzle to individuals (computers), to give a prize (in Bitcoin) to the individual who solves the puzzle first, and to let the individual record the transaction.
- In competing for the prize, many people (computers) engage in solving the crypto puzzle to create transaction records.
- With only one individual out of many competitors receiving the prize, this process is similar to mining; and individuals engaging in solving puzzles are called miners.
- As soon as a mining computer solves the existing puzzle, a new file (block) is created and attached to the existing chain of blocks.
- The new block creates a new puzzle to be solved. At the same time, the solution is announced to the network of mining computers.
- Mining computers check if that solution is correct.
- If the solution is in fact correct, mining computers start working on solving the new puzzle created by the block that they have just validated.

Mining

- In this entire process, it is important that there is no single individual who is in charge of checking the validity and uniqueness of records on blockchain. Instead, many independent individuals check the validity of records, which produces a unique record (ledger). This process is completely decentralized.
- For Bitcoin blockchain, on one hand, simple records of several transactions are put together and recorded as a new block. On the other hand, for Ethereum blockchain,
- user-executable computer programs and resulting transactions of executing the programs can be written into a new block by a mining node.
- A problem with blockchains is that mining consumes computer resources not directly related to records. Many miners work on solving the puzzle posed by the blockchain. Because this puzzle can be solved by a sequence of computations, anyone can find an answer so long as he/she is prepared to spend enough computing resources.
- As a result, if there are 1,000 miners, the computational resources used by 999 miners (i.e., electricity to run computations) will be wasted.
- As the value of virtual currency soars, the number of miners has increased dramatically, and it is said that about 10,000 miners are active around the world.
- Given that the average time required to solve the puzzle is 10 min, it is possible that a huge amount of electricity is being wasted.
- To maintain the accuracy of the blockchain, a certain number of miners must be involved.
- Whether electricity is wasted is related to the number of miners required to maintain accuracy.

Advancement of Blockchain Technology

- The Bitcoin blockchain proved that a secure ledger can be created in a decentralized manner without using a trusted authority who is specialized in managing a ledger.
- Since then, different types of blockchains have been created.
- A blockchain called IOTA creates a blockchain model that is not based on mining, hence does not consume a large amount of electricity.
- The IOTA blockchain is not a linear chain of files as used by the Bitcoin blockchain.
- Instead, it has a very complicated network structure, which itself is impossible to replicate. This structure is called a directed acyclic graph (DAG).
- Each transaction file (block) is given two arms, each of which randomly grabs another file (directed from grabbing to grabbed files).
- As the number of files becomes larger, the number of arms increases by the power of 2, which soon becomes an extremely complicated structure.
- In this structure, a sequence of files is created in which a particular file grabs another file, which will grab the next, and so on.
- It has been shown that if such a sequence never contains a circle (acyclic), the structure can serve as a blockchain, which can dispense with the requirement for mining.

Advancement of Blockchain Technology

- A few years after Bitcoin was introduced, a new blockchain called Ethereum was developed.
- It was able to execute any program and to create execution records, as well as record transactions.
- Not only does Ethereum provide its own virtual currency, called Ether, it also works in conjunction with Ether to provide a “platform” for loading and executing programs.
- These programs are called smart contracts, which can program the execution of a promise between users with various contingencies.
- Once a business can be run on a blockchain, business developers seek funding to further develop the business or for future businesses.
- Such funding is also carried out over the Internet in a manner similar to crowd funding.
- This method of funding is called ICO (initial coin offering), and it sells and collects funds for business vouchers called tokens.

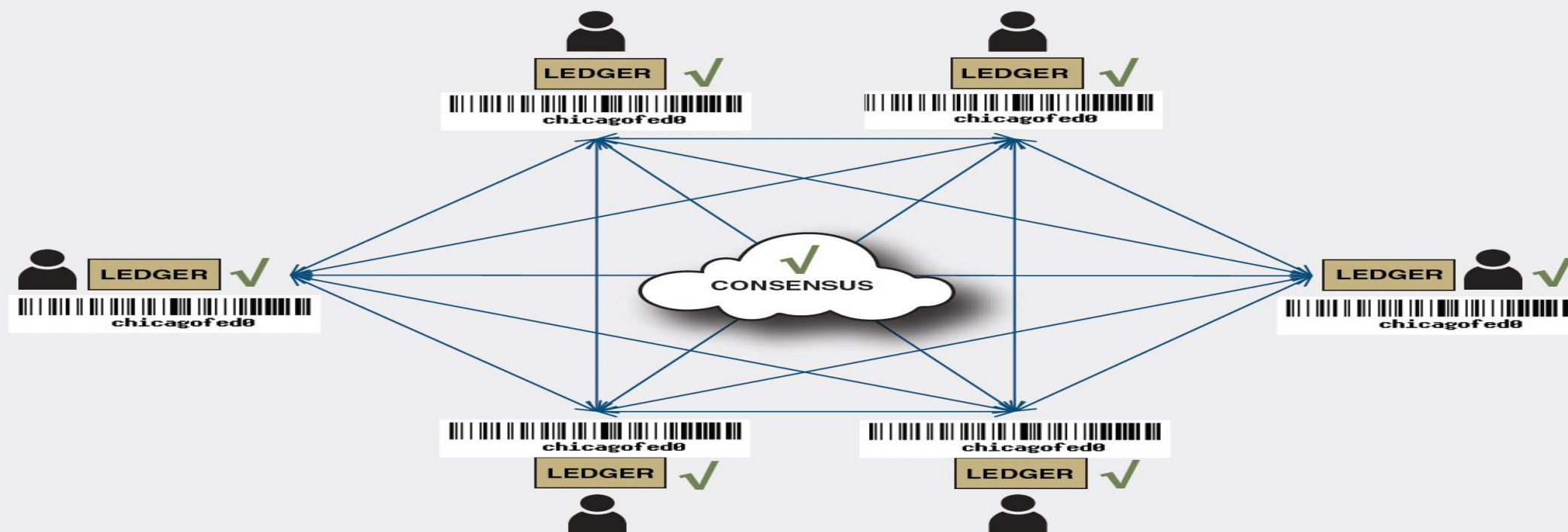
How does Blockchain Technology Works?

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 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.

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.

 This represents the current state of the ledger.

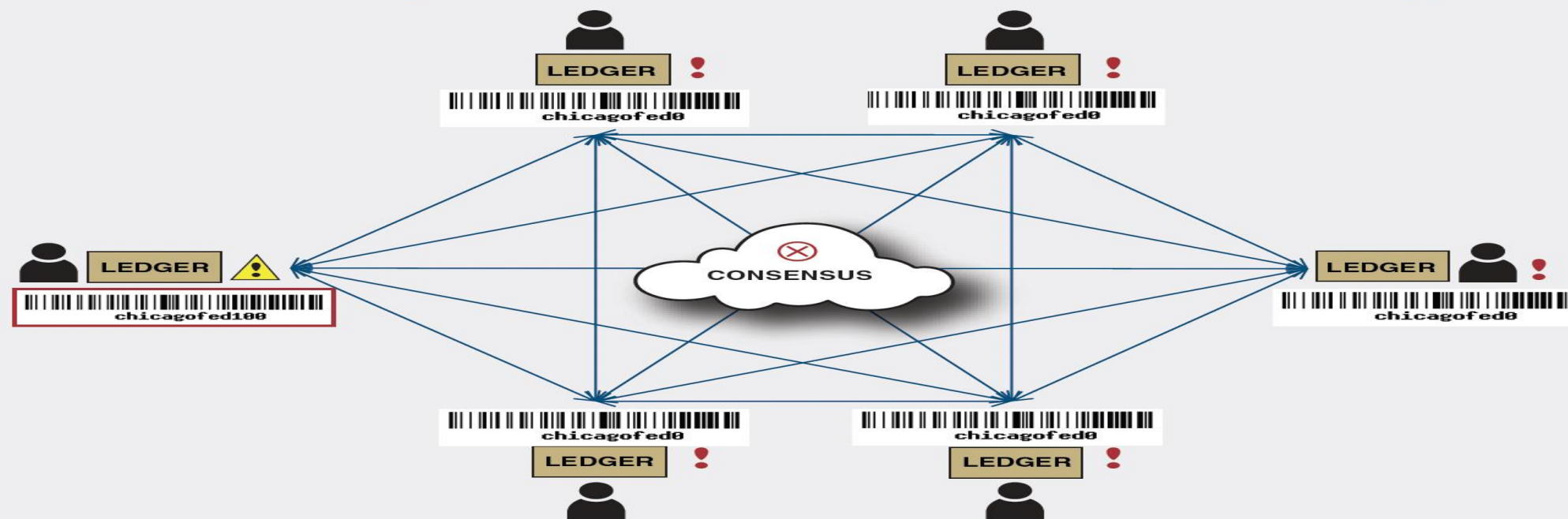
Source: Financial Markets Group, Federal Reserve Bank of Chicago.

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



-  When a node operator updates his/her records and digitally signs the ledger, it will invoke a reconciliation/consensus fail alert.
-  Represents a change in the state of the ledger. In this example, the state of the ledger changes from chicagofed0 to chicagofed100.
-  When the states of the ledgers do not match, there is an alert that notifies node operators about the change.

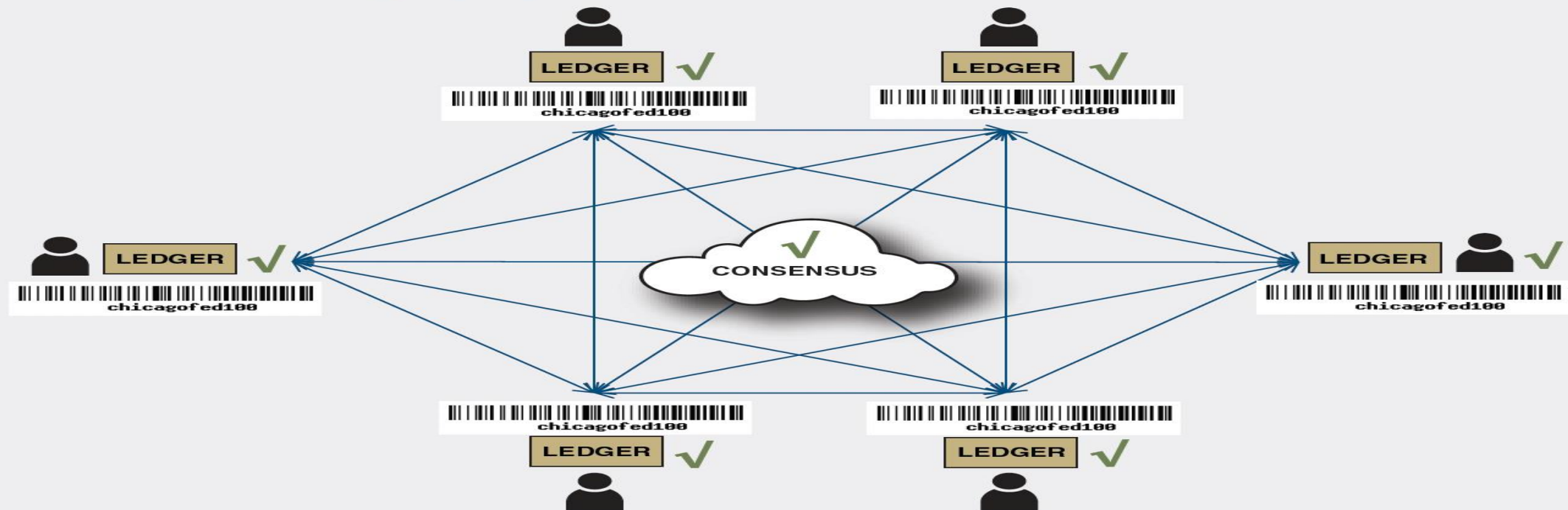
Source: Financial Markets Group, Federal Reserve Bank of Chicago.

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.
- 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.

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.

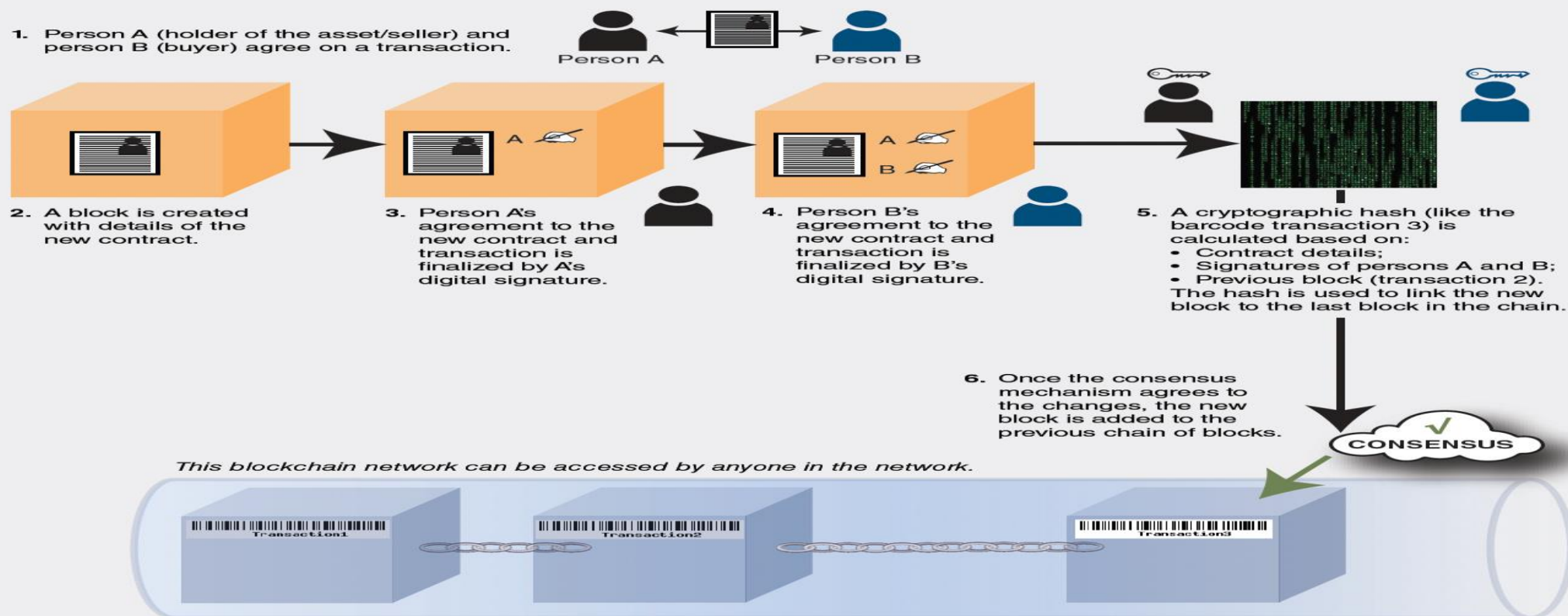
Source: Financial Markets Group, Federal Reserve Bank of Chicago.

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

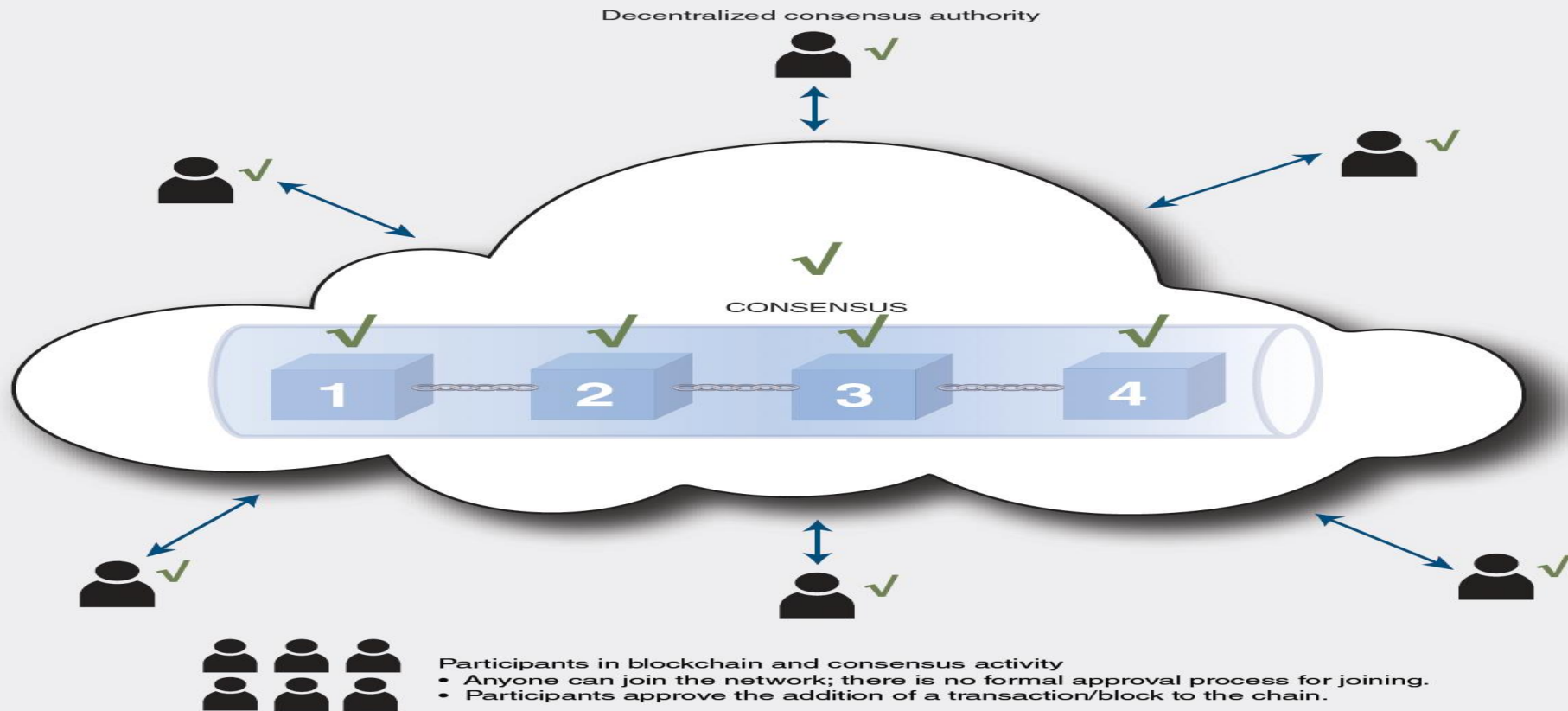


Source: Financial Markets Group, Federal Reserve Bank of Chicago.

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

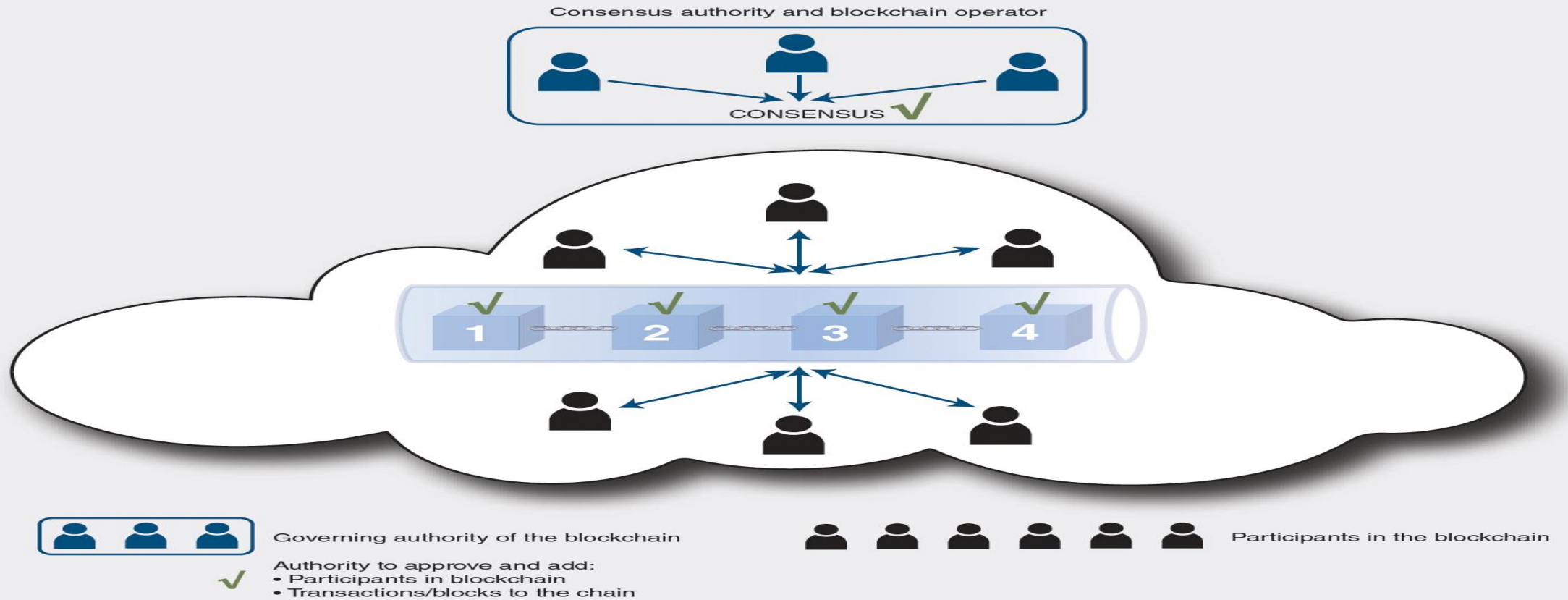


Source: Financial Markets Group, Federal Reserve Bank of Chicago.

Permissioned networks

- 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?”
- 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 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).

FIGURE 7
Permissioned/private blockchain network

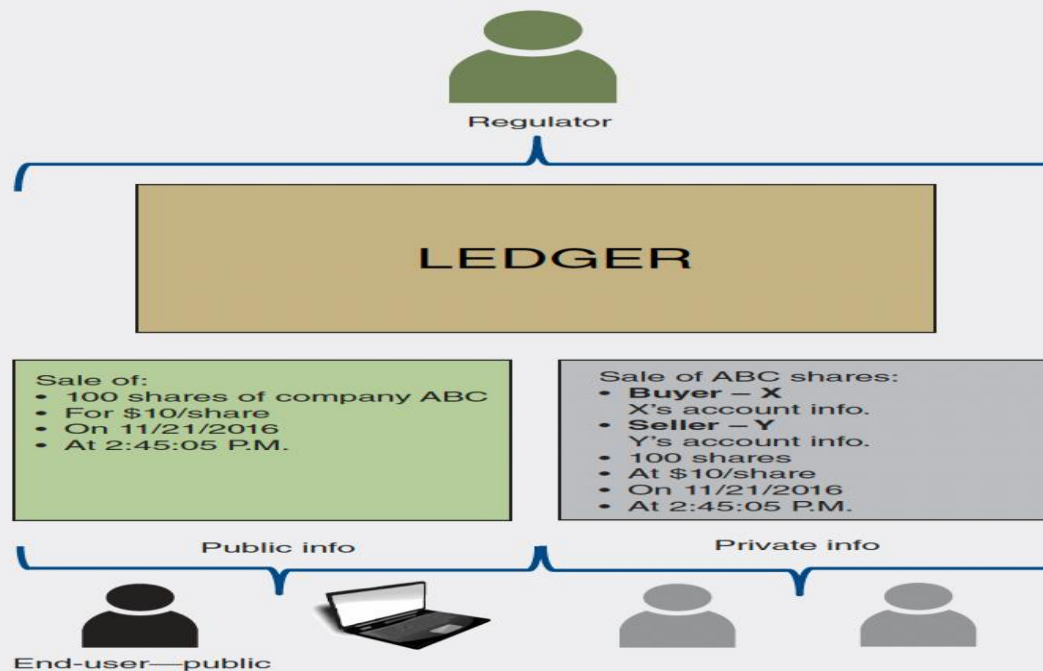


Source: Financial Markets Group, Federal Reserve Bank of Chicago.

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.

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.

Consensus mechanism

- 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.

Consensus mechanism

- 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

Blockchain Applications, Benefits and Challenges

Applications of Blockchain Technology

- **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 recordkeeping 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 of Blockchain Technology

- ***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 of Blockchain Technology

- ***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.

Challenges of Blockchain Technology

- **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.

Challenges of Blockchain Technology

- ***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.
- ***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.

References

- Rebecca Lewis, John McPartland, and Rajeev Ranjan (2017), *Blockchain and financial market innovation, Economic Perspectives, Federal reserve Bank.*
- <https://www.investopedia.com/terms/b/blockchain.asp>



Thank You