

Master of Financial Technology

Prepared by Dr. Omar Al-kasasbeh

FNT628

Blockchain and Cryptocurrencies

Lecture 2



Blockchain and Cryptocurrencies

FNT 628

Blockchain and Cryptocurrencies

Prepared by
Dr. Omar Al-kasasbeh



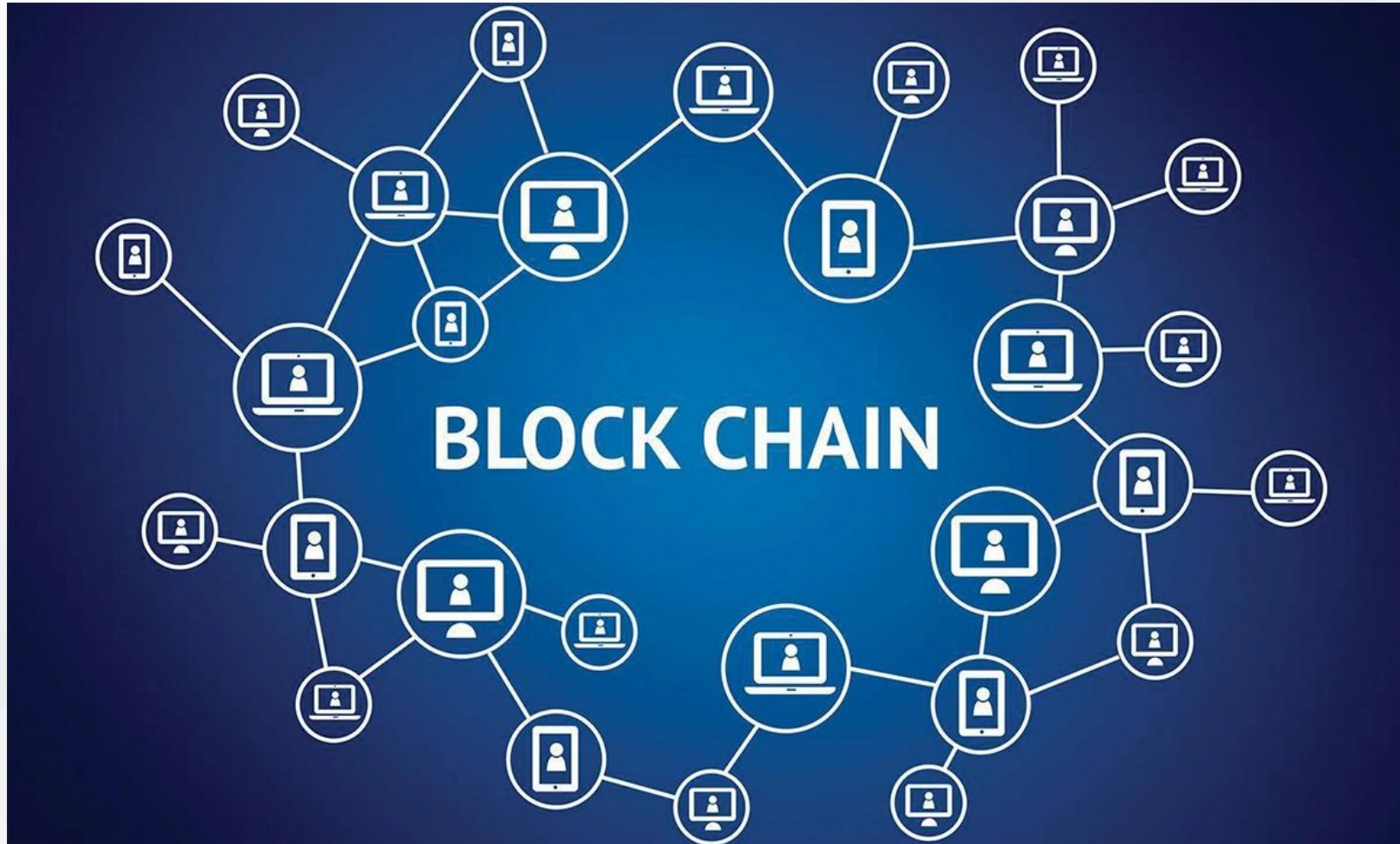
<https://midocean.edu.km>

Chapter
02

Table of Contents

1. Introduction.
2. How does blockchain technology work?
3. Permissionless networks.
4. Blockchain Applications and Benefits.
5. Blockchain Challenges.





Chapter 02

Introduction

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.

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. Interest in the technology continues to grow in the financial technology and broader financial services communities. In this course, we provide a brief overview of what blockchain technology is, how it works, and some potential applications and challenges.



Chapter

02

Blockchain Technology: Conceptual Foundations and Evolution



Chapter
02

Blockchain technology has emerged as one of the most significant technological innovations of the 21st century, fundamentally altering how digital systems manage trust, data integrity, and value exchange. Initially introduced as the underlying infrastructure for cryptocurrencies, blockchain has since evolved into a general-purpose technology with applications spanning finance, supply chain management, healthcare, governance, digital identity, and beyond. At its core, blockchain represents a paradigm shift from centralized trust models to decentralized, cryptographically enforced trust mechanisms.





Chapter 02

Traditional information systems rely heavily on centralized authorities such as banks, governments, or corporations to validate transactions, maintain records, and enforce rules. While effective, these centralized systems introduce several limitations, including single points of failure, high operational costs, vulnerability to corruption or cyberattacks, and limited transparency. Blockchain technology addresses these challenges by enabling distributed consensus, immutable record-keeping, and peer-to-peer coordination without requiring a trusted intermediary.



01

The Problem of Trust in Digital Systems



Trust is a foundational requirement in any system that facilitates exchange whether of money, data, or assets. In traditional digital systems, trust is enforced through institutional intermediaries. For example, banks verify financial transactions, governments issue identity documents, and centralized databases store and control sensitive information.

However, this trust model presents several structural weaknesses:

- Centralization of Power: Control is concentrated in a single authority or a small group of entities.
- Single Point of Failure: System failure, cyberattacks, or insider misconduct can compromise the entire system.
- High Costs: Intermediaries increase transaction costs through fees, delays, and administrative overhead.



-Limited Transparency: Users must trust that records are accurate without independent verification.

-Restricted Access: Participation is often limited by geographic, political, or institutional barriers.

Blockchain technology was conceptualized as a response to these systemic limitations, proposing a new trust model where trust is embedded in code, cryptography, and distributed consensus rather than centralized authority.



Chapter
02

Blockchain and Data Ownership

The concept of data ownership has become increasingly complex in the digital age. In traditional information systems, ownership of data is rarely defined in a strict legal sense for end users. Instead, it is usually understood as control over data who stores it, who can access it, who can modify it, and who can delete it. In most conventional systems, this control lies not with individuals, but with centralized institutions such as companies, governments, or service providers. Blockchain technology introduces a fundamentally different model that reshapes how data ownership, control, and authority are understood.



To appreciate the significance of blockchain in this context, it is essential to first understand how data ownership operates in traditional centralized systems. When users interact with online platforms such as social media, banking systems, or educational portals their data is typically stored in centralized databases managed by a single organization. Although users may be described as the “owners” of their data, the actual power to manage, restrict, or remove that data often rests with the platform provider. This creates a situation where ownership is more symbolic than practical, as users depend on intermediaries to access or control their own information.

Blockchain challenges this model by separating data control from centralized ownership. Instead of relying on a single authority, blockchain systems distribute records across a network of independent nodes. No single entity has unilateral power to alter the data once it has been validated and recorded. This architectural shift has profound implications for how ownership is defined and enforced in digital environments.



In blockchain-based systems, ownership is not primarily about possessing data files or databases. Rather, it is about possessing cryptographic authority. Control over assets, identities, or records is typically established through public private key cryptography. The private key functions as proof of authority: whoever controls the private key associated with a blockchain address has the ability to initiate transactions or assert rights recorded on the blockchain. In this sense, blockchain replaces institutional trust with mathematical proof.

This leads to an important conceptual distinction for students to understand: blockchain does not necessarily store all data directly on the ledger. Due to limitations related to scalability, cost, and privacy, most blockchain systems store only references, hashes, or proofs of data rather than the data itself. The blockchain acts as a verification layer, not a traditional data storage system. Ownership, therefore, refers to the ownership of rights, claims, or attestations rather than raw information.



A clear example can be found in the case of digital academic certificates. In a traditional system, a university stores student records in its internal database. Employers must contact the university to verify a degree, and students rely on the institution to reissue documents if they are lost. In a blockchain-based system, the university can issue a digital certificate and record a cryptographic hash of that certificate on the blockchain. The student holds the certificate, while the blockchain provides a permanent, tamper-resistant proof of its authenticity. The university retains authority over issuance, but it no longer controls verification. Ownership here is shared in a new way: the student controls access to the certificate, and the blockchain guarantees its integrity.

This illustrates a critical shift: blockchain enables verifiable ownership without centralized control. The truth of ownership does not depend on a database administrator or institutional approval at the time of verification. Instead, it is embedded in the blockchain's consensus rules and cryptographic structure.



However, blockchain does not eliminate all challenges related to data ownership. One common misconception is that blockchain automatically guarantees privacy. In reality, many blockchains especially public ones are highly transparent. Transactions and records can be visible to all participants, even if identities are pseudonymous. This creates tension between transparency and data protection, particularly in sensitive domains such as healthcare, education, or personal identity.

As a result, modern blockchain-based data ownership models often rely on hybrid architectures. Sensitive data is stored off-chain in secure databases or decentralized storage systems, while the blockchain stores proofs, permissions, or access logs. Ownership, in this context, means the ability to grant, revoke, or verify access to data rather than physically hosting the data itself. This approach allows blockchain to support data ownership while respecting privacy and regulatory constraints.



Another important dimension of blockchain and data ownership concerns immutability. Once data or proofs are recorded on the blockchain, they cannot easily be altered or deleted. While this strengthens trust and accountability, it also raises legal and ethical questions. For example, data protection laws in many jurisdictions recognize the “right to be forgotten,” which conflicts with blockchain’s permanent record structure. This highlights that blockchain ownership is not purely a technical matter but also a legal and governance issue.

Furthermore, ownership in blockchain systems is closely tied to responsibility. Since users control their assets and data through private keys, they also bear the risk of key loss or compromise. Unlike traditional systems, there may be no central authority capable of restoring access. This model empowers users but also places greater responsibility on them, redefining the relationship between individuals and digital infrastructure.



In practice, data ownership in blockchain systems is often distributed among multiple actors. The user controls cryptographic keys, the protocol defines the rules of ownership, and applications built on top of the blockchain may still manage interfaces, metadata, or off-chain storage. True decentralization, therefore, depends not only on blockchain technology itself but also on how systems are designed and governed.

From an academic perspective, blockchain transforms data ownership from a centralized, institution-driven concept into a cryptographically enforced, user-centric model. It does not eliminate intermediaries entirely, but it reduces their power to unilaterally control or alter records. Ownership becomes verifiable, transferable, and resistant to manipulation, while simultaneously introducing new challenges related to usability, regulation, and governance.





Chapter 02

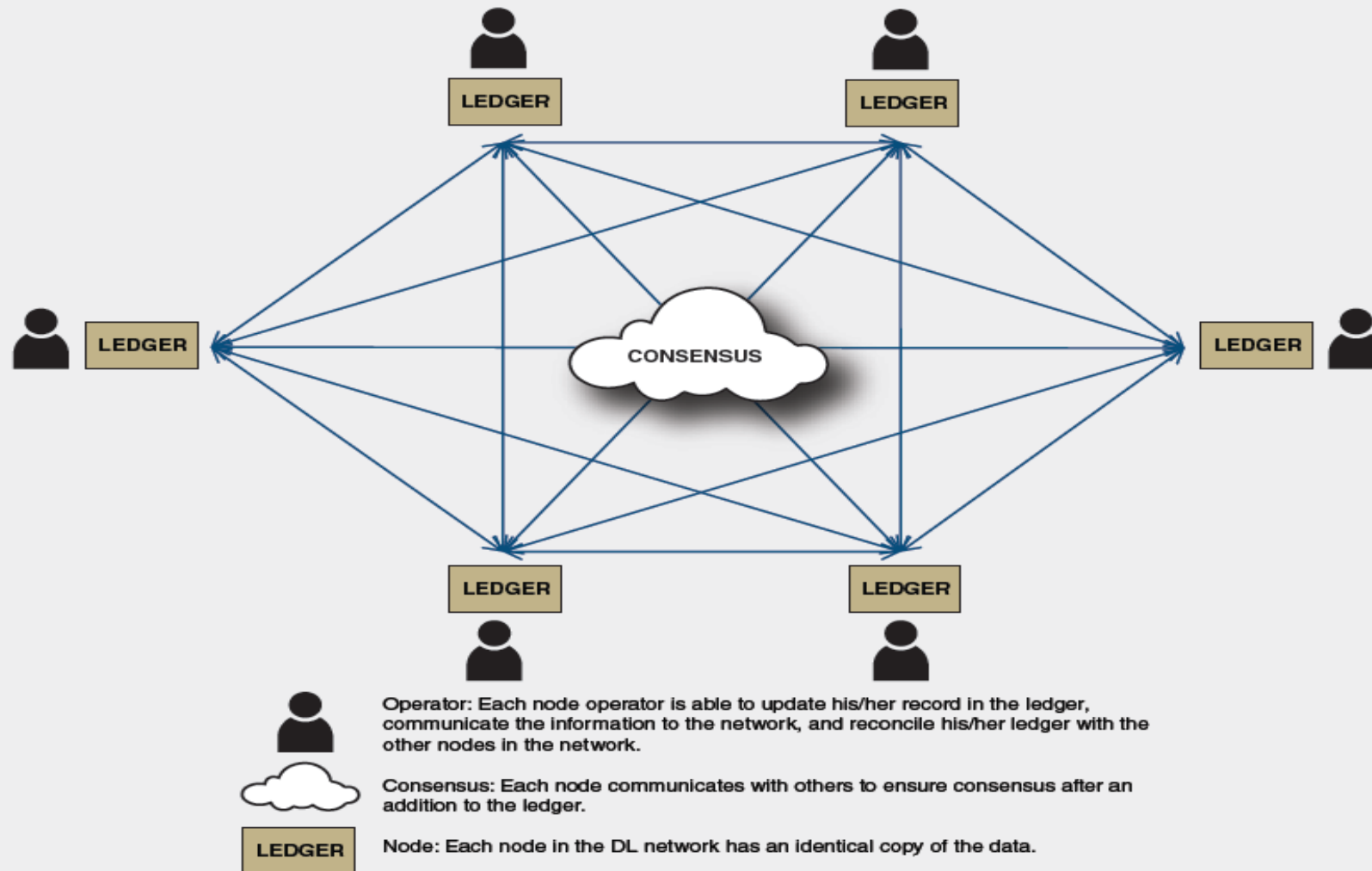
What is a blockchain database?

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



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.” 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. 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.



Chapter
02

How does Blockchain Technology Works?





Chapter 02

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.



Chapter
02

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.

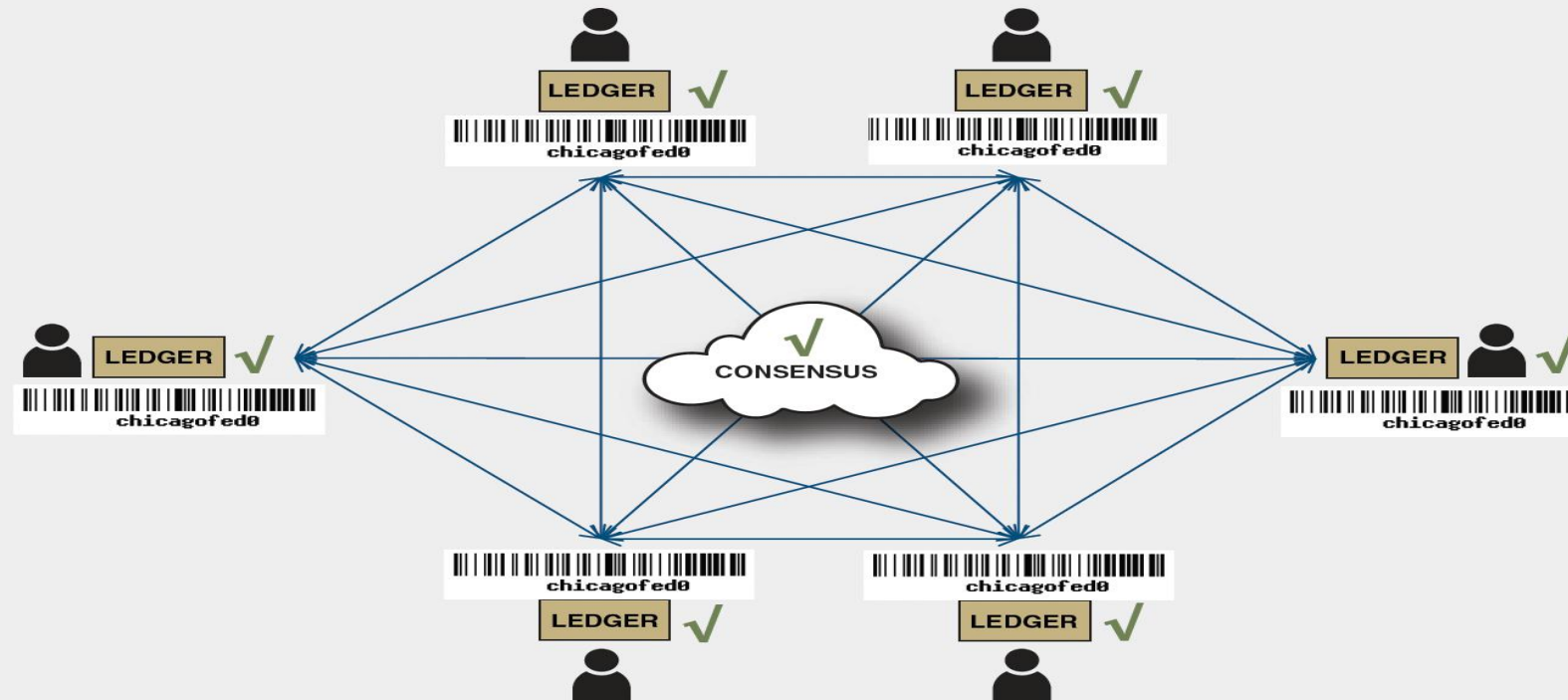
In the example in figure 2, all the node operators have the same version of the ledger ("chicagofed0"). Since all the versions of the ledgers are the same, consensus is achieved and the records are final.

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 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.

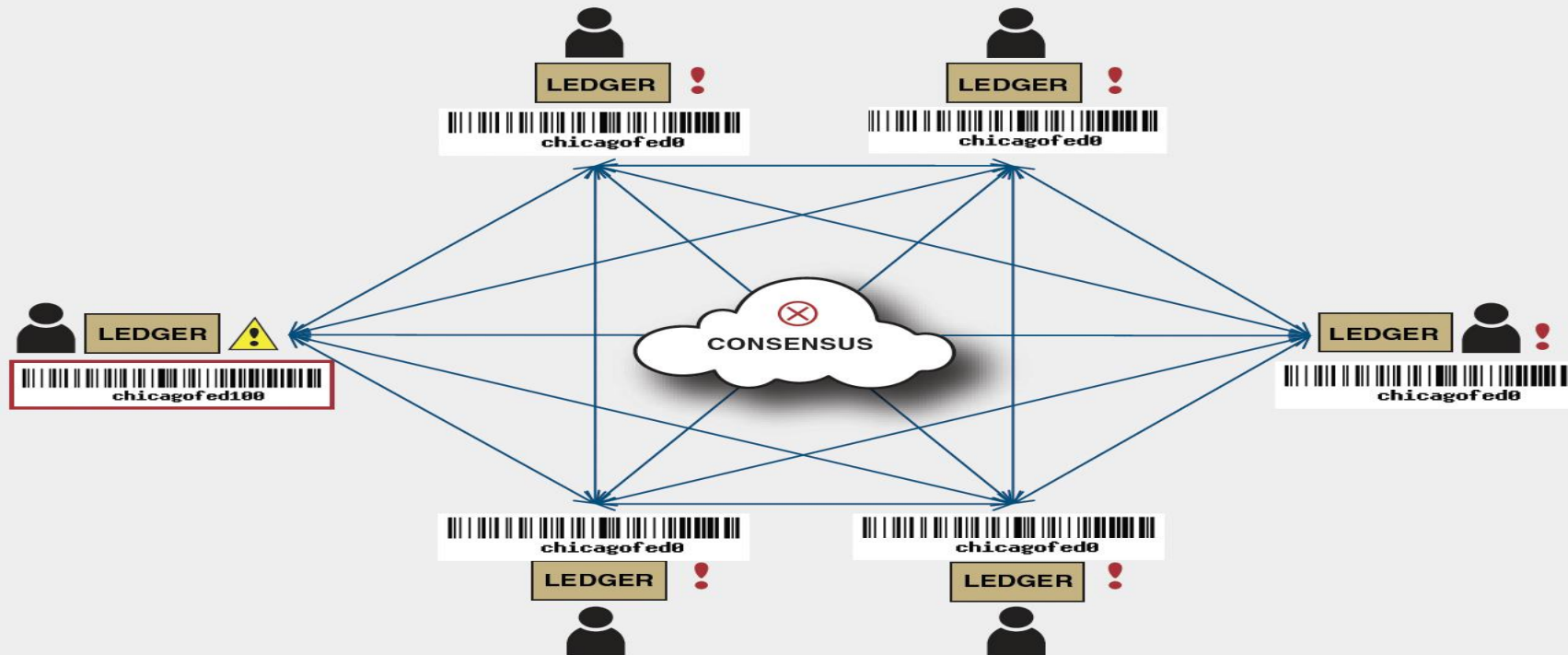
 This represents the current state of the ledger.
chicagofed0

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



FIGURE 3

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



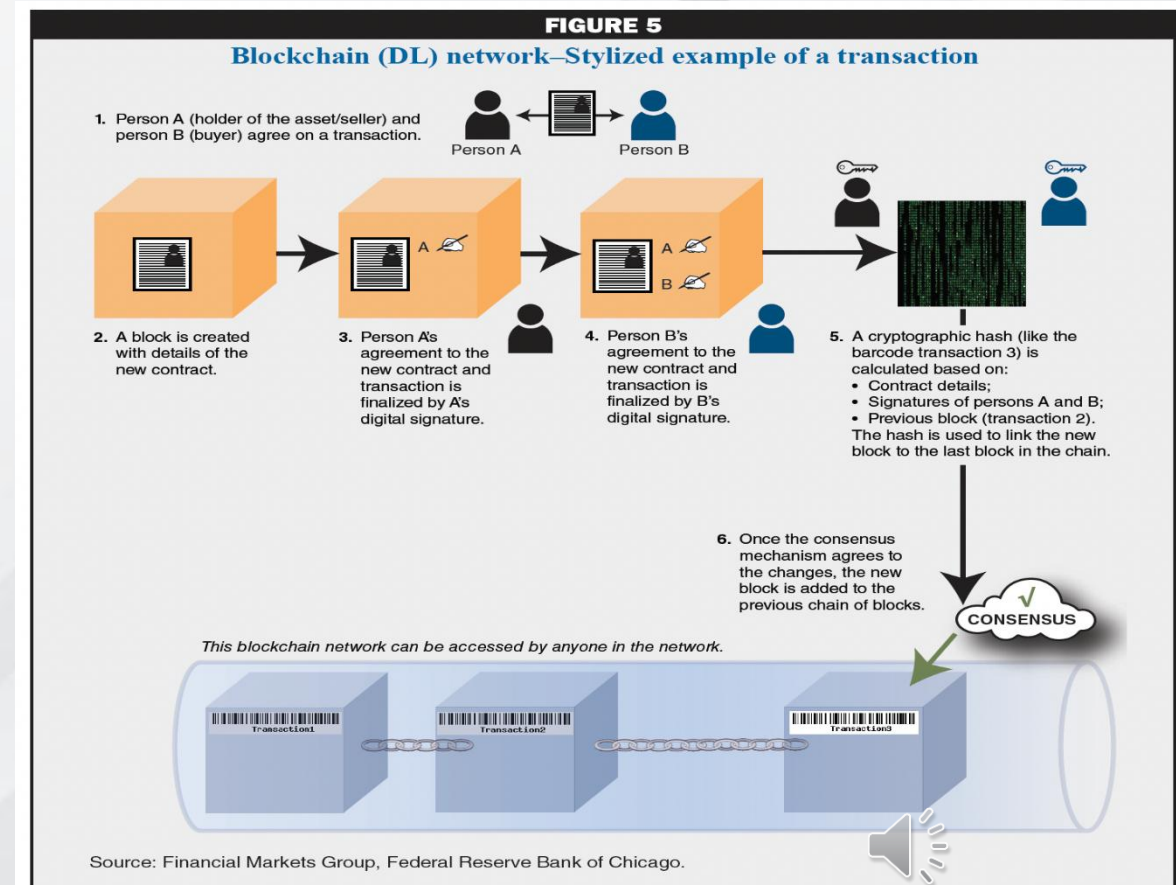
-  When a node operator updates his/her records and digitally signs the ledger, it will invoke a reconciliation/consensus fail alert.
-  Represents a change in the state of the ledger. In this example, the state of the ledger changes from chicagofed0 to chicagofed100.
-  When the states of the ledgers 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).



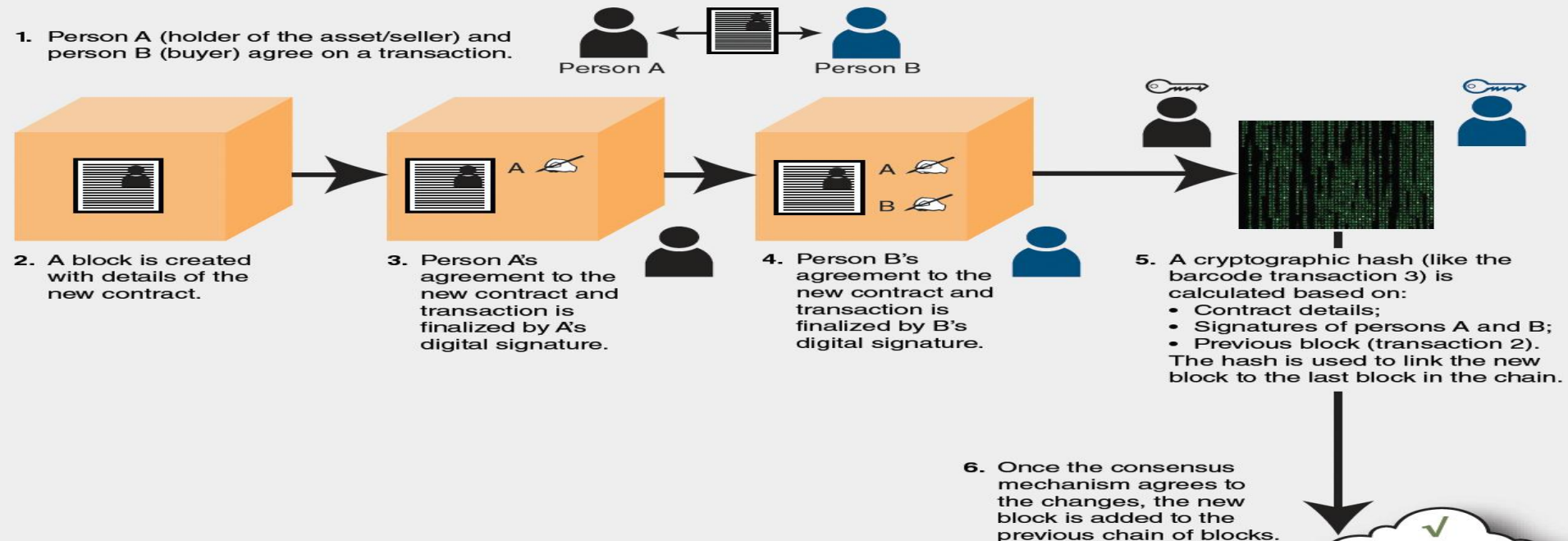
The cryptographic hash is a string of characters associated with a given block that is difficult to calculate but easy to verify. This makes it simple to verify a legitimate block, but difficult to engineer and insert into the chain a block recording illegitimate transactions.

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.

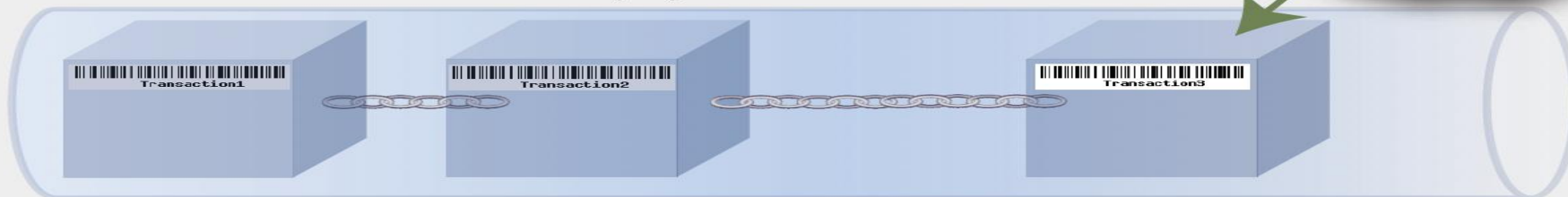


FIGURE 5

Blockchain (DL) network—Stylized example of a transaction



This blockchain network can be accessed by anyone in the network.



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.

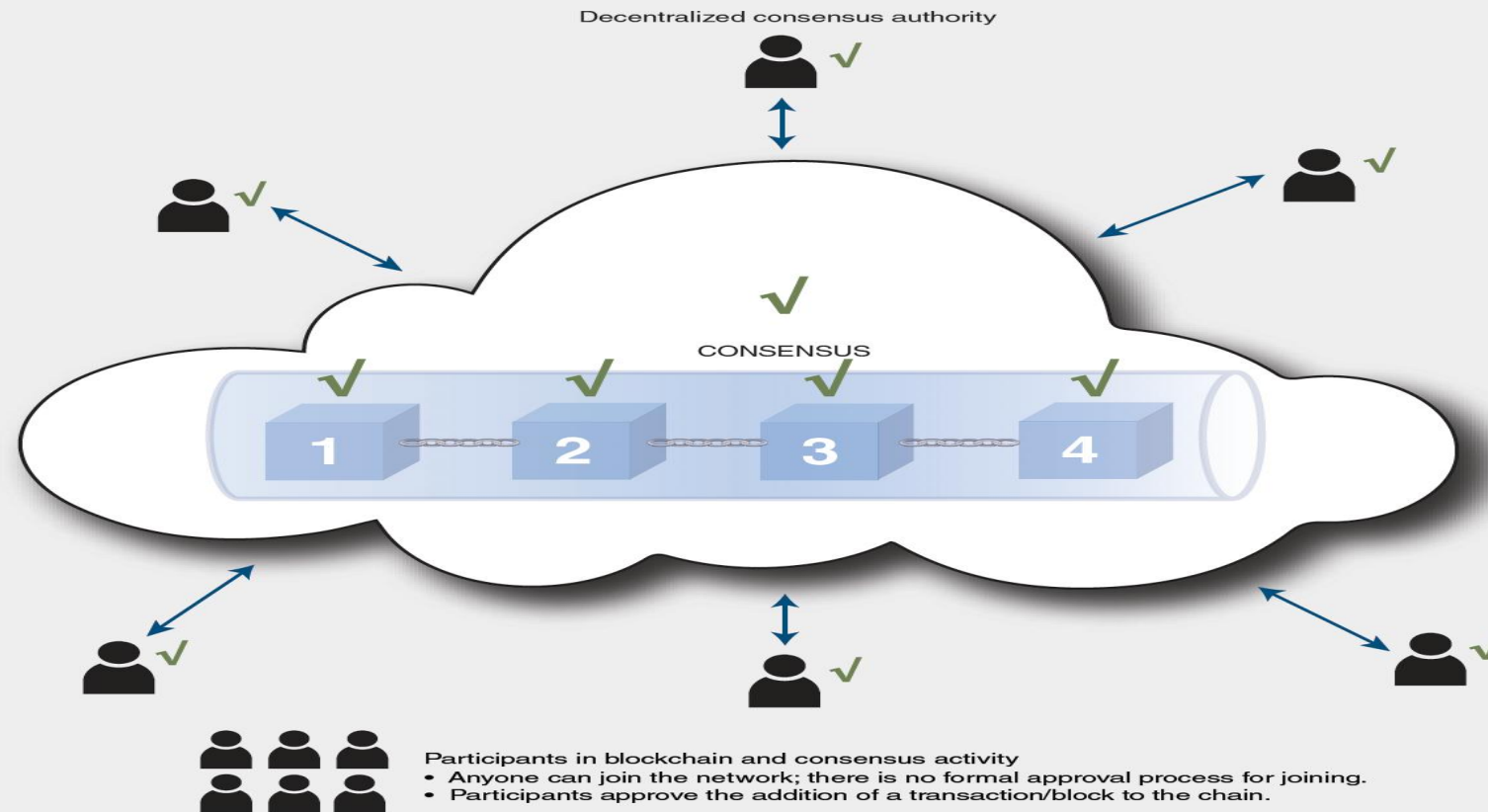
Instead, all transactions are recorded on a single database. Each user stores a copy of the database, so there is no single point of failure as exists with traditional relational databases.

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 6
Permissionless/public blockchain network



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



Permissioned networks

Chapter

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.

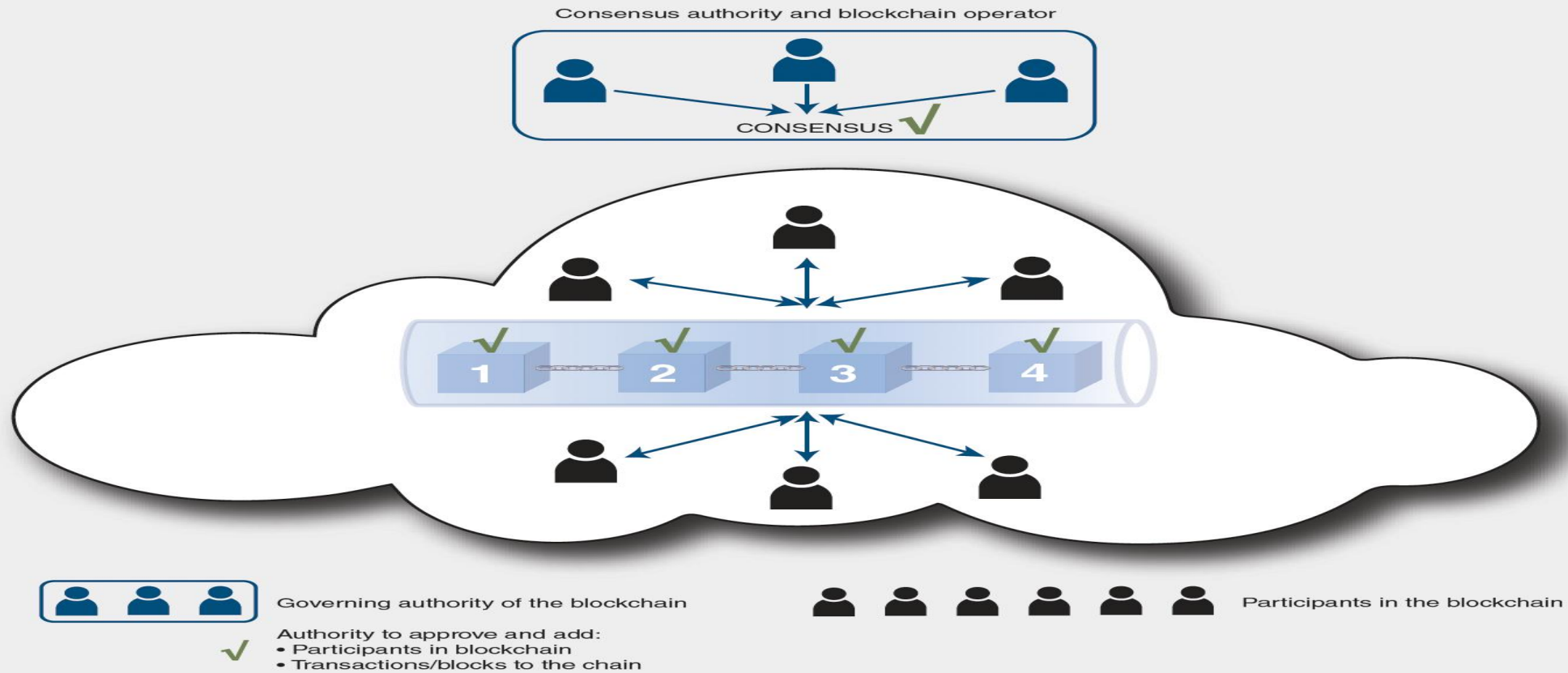
Permissioned blockchains allow certain members to control the confirmation of transactions. These permissioning members (consensus authorities) can exert control in various ways depending upon the network design.

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 7
Permissioned/private blockchain network



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



Permissioned networks

Chapter

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.

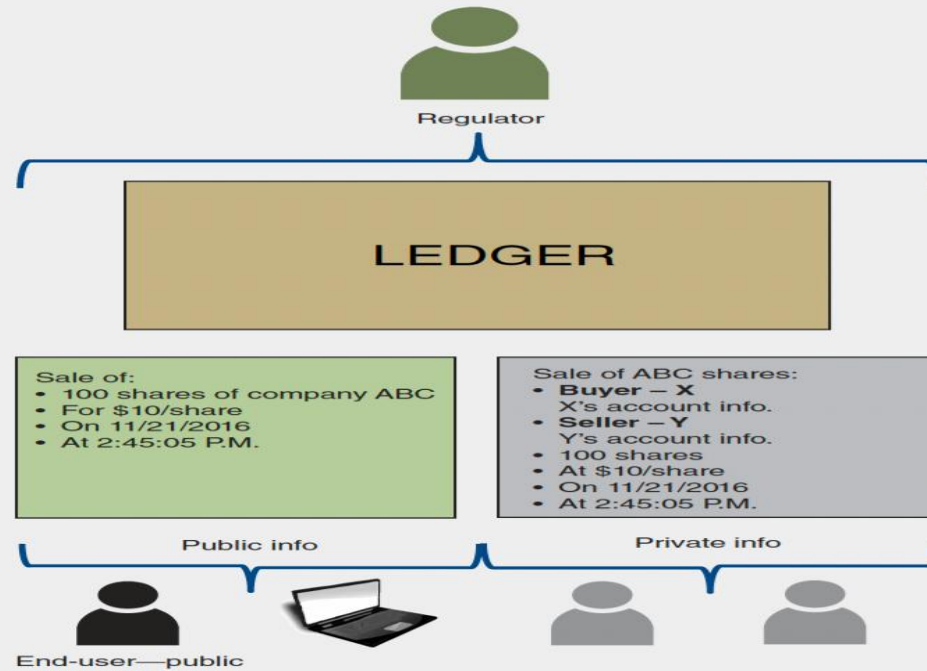
In permissioned blockchains, it is also possible to put controls in place to allow varying levels of access to the information in the ledger. For example, regulators could be allowed to view all the details of a transaction in the ledger but not add any transactions, while users might be allowed to view selective details of the transactions depending on their access level (see figure 8).



FIGURE 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

Chapter

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. 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.



Chapter

01

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



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.





Chapter 02

(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.

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. 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.

Chapter
01

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