Federal Reserve Bank of Chicago

Blockchain and Financial Market Innovation

Rebecca Lewis, John McPartland, and Rajeev Ranjan

June 2017

PDP 2017-03

[*] *Working papers are not edited, and all opinions and errors are the responsibility of the author(s). The views expressed do not necessarily reflect the views of the Federal Reserve Bank of Chicago or the Federal Reserve System.*

Blockchain and Financial Market Innovation

By Rebecca Lewis, John McPartland, and Rajeev Ranjan

Introduction

Blockchain technology is likely to be a key source of future financial market innovation. It allows 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.

While all are in the early stages of development, there are many promising applications of blockchain technology in financial markets. This paper seeks to give the reader an overview of what the technology is, how it works, and some potential applications for and challenges posed by blockchain technology.

Part I: What it is and how it works

What is a blockchain database?

A database using blockchain technology has a network of users, each of which stores its own copy of the data, giving rise to another term for this new database architecture: 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 **Fig - 1** for the network set up). Generally speaking, DLT and blockchain are used interchangeably in position papers and popular media.

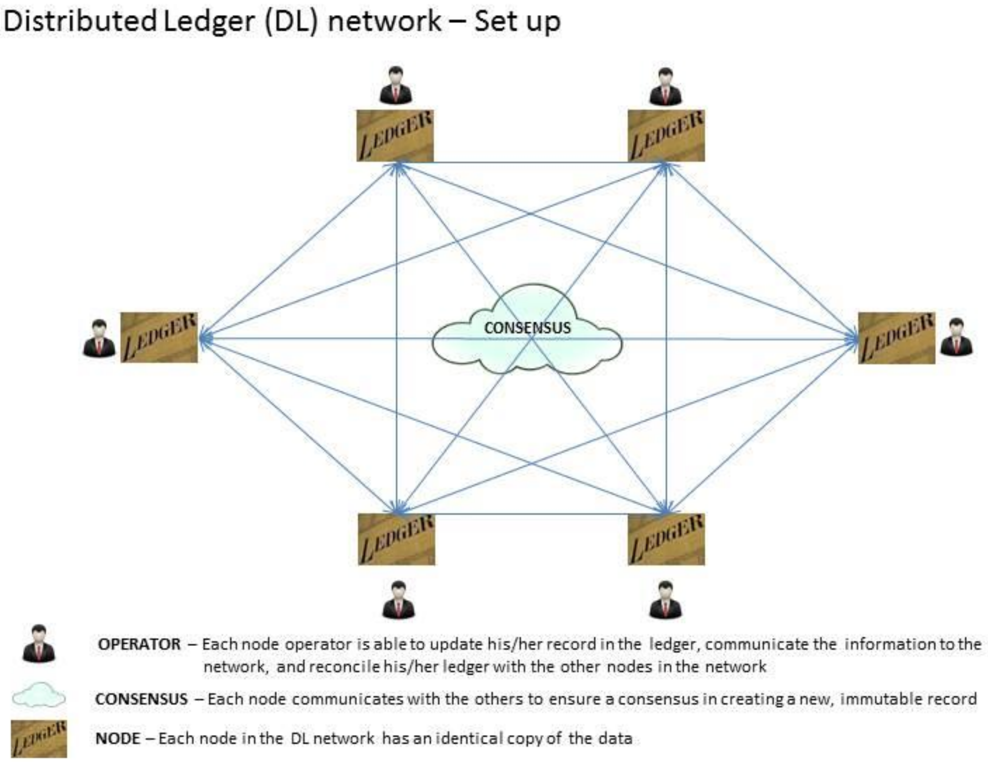
As one industry participant involved in developing blockchain technology described it, blockchain technology is "nothing more than a new…approach to database architecture… Fundamentally, [it is] an improvement over the way that, traditionally, databases have been designed and used in the past."[1]

A database is "a usually large collection of data organized especially for rapid search and retrieval."[2] While there are various ways of organizing and storing data for rapid search and retrieval, traditionally, the vast majority of databases have been relational, organizing data in tables that users can update and search.[3] Relational databases are centralized, with a master copy controlled by a central authority. Actors 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. Actors that do not trust one another must maintain separate databases that they periodically reconcile against one another.

[1] "Global Financials/FinTech: Global Insight: Blockchain in banking: Disruptive Threat or Tool?," Morgan Stanley Global Insight, April 20, 2016, p. 28.

[2] "Database." Merriam-Webster. Merriam-Webster, Web. 15 June 2017. <https://www.merriam-webster.com/dictionary/database>.

[3] Meunier, Sebastien. "Blockchain Technology - a Very Special Kind of Distributed Database." Medium. 29 Dec. 2016. Web. 15 June 2017. <https://medium.com/@sbmeunier/blockchain-technology-a-very-special-kind-of-distributed-database-e63d00781118>.



OPERATOR – Each node operator is able to update his/her record in the ledger, communicate the information to the network, and reconcile his/her ledger with the other nodes in the network

CONSENSUS – Each node communicates with the others to ensure a consensus in creating a new, immutable record

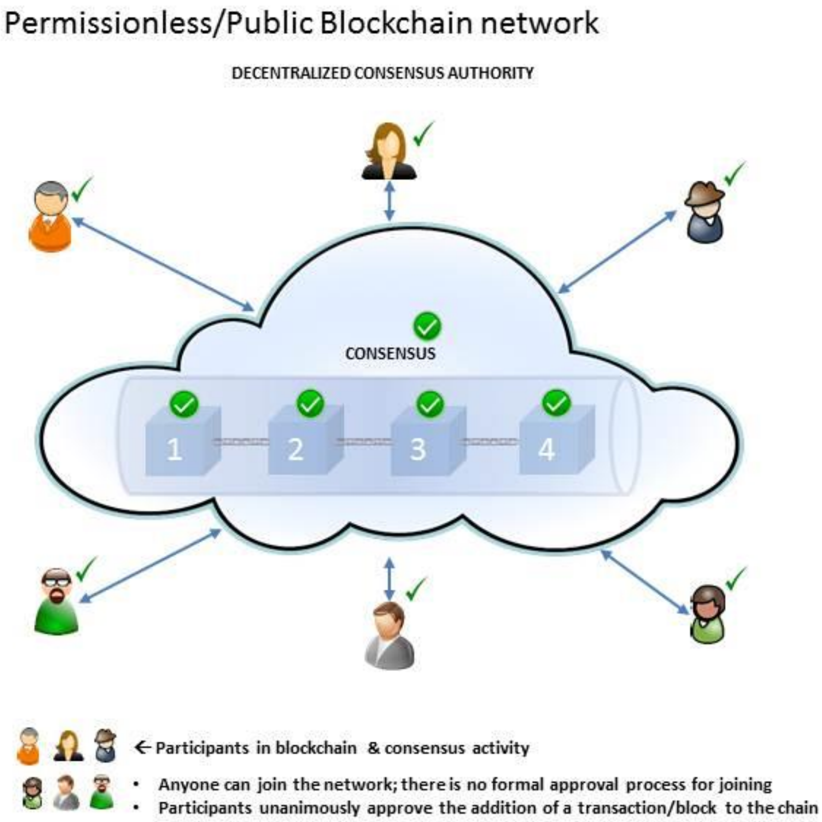
NODE – Each node in the DL network has an identical copy of the data

Source – Financial Markets Group, Federal Reserve Bank of Chicago

Fig – 1

Initial blockchain implementation: Permissionless networks

Blockchain technology was first used 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, trusting the consensus mechanism, which we discuss below, to ensure the ledger's accuracy. This avoids the need for each actor to have its own database that it periodically reconciles against those of its counterparties. Instead, all transactions are recorded on a single database. Each actor stores its own copy of the database, so there is no single point of failure as exists with traditional relational databases. Once added to the blockchain, transactions cannot be undone, making the ledger an immutable record of all previous transactions. **Fig - 2** provides an illustration of a permissionless and public blockchain network.

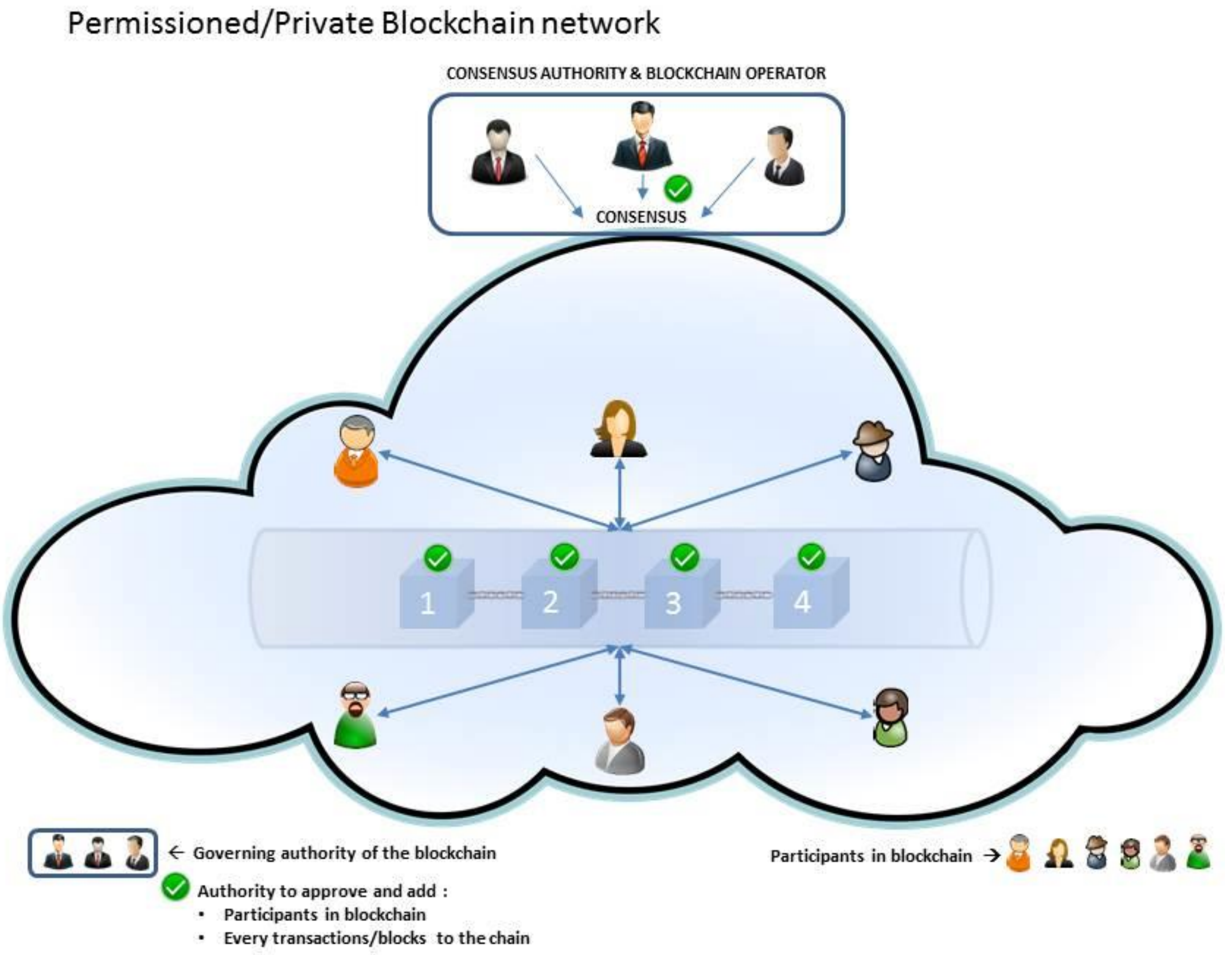

Permissionless/Public Blockchain network
DECENTRALIZED CONSENSUS AUTHORITY
CONSENSUS
1
2
3
4
← Participants in blockchain & consensus activity
• Anyone can join the network; there is no formal approval process for joining
• Participants unanimously approve the addition of a transaction/block to the chain

Source – Financial Markets Group, Federal Reserve Bank of Chicago

Fig - 2

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/or 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 control over 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. **Fig - 3** provides an illustration of a permissioned and private blockchain network.


Permissioned/Private Blockchain network
CONSENSUS AUTHORITY & BLOCKCHAIN OPERATOR
CONSENSUS
1
2
3
4
← Governing authority of the blockchain
Authority to approve and add :
• Participants in blockchain
• Every transactions/blocks to the chain
Participants in blockchain →

Source – Financial Markets Group, Federal Reserve Bank of Chicago

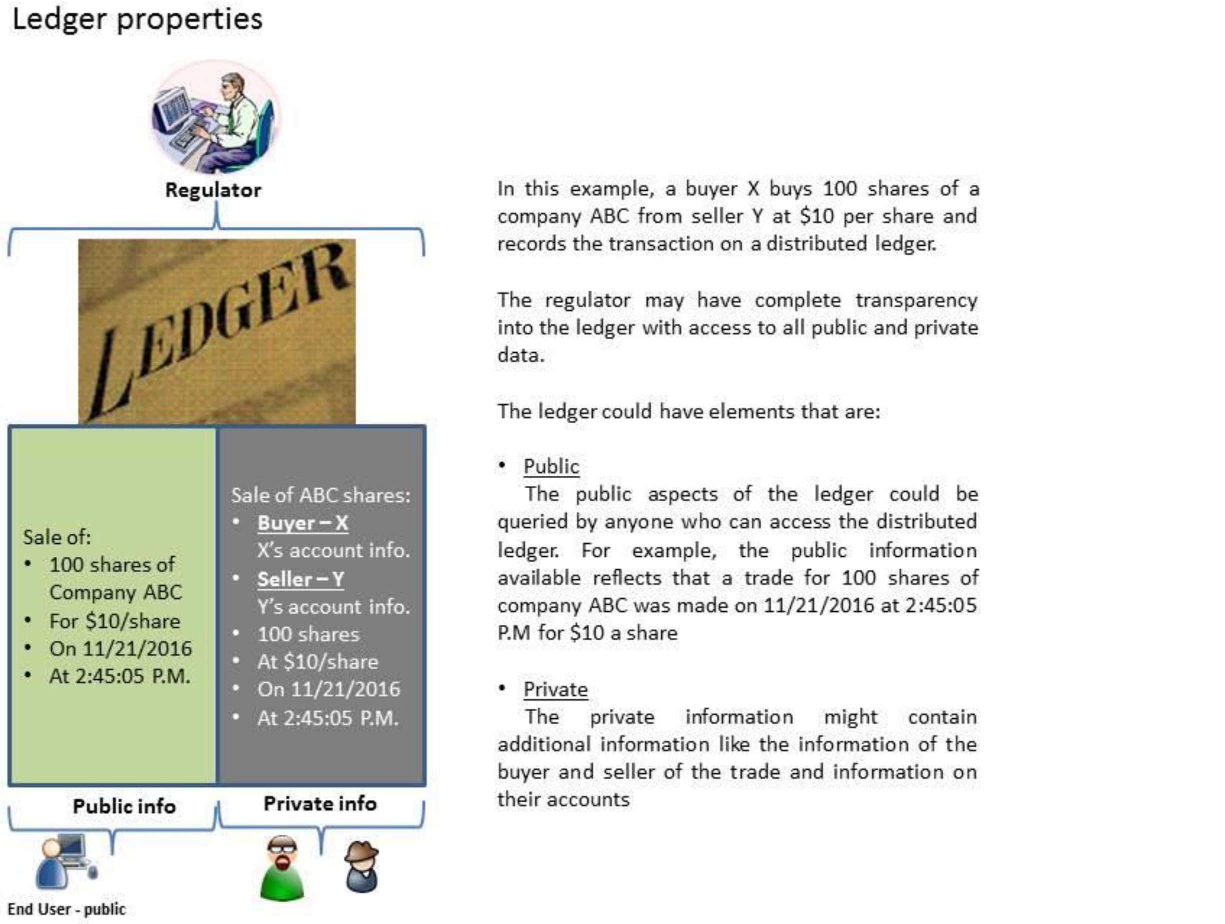
Fig - 3

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?"[4] However, permissioned blockchains retain many key features and benefits of permissionless blockchain architecture 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.

[4] Credit Suisse, quoted in Kaminska, Izabella, "How I learned to stop blockchain obsessing and love the Barry Manilow," *Financial Times*, August 10, 2016. < https://ftalphaville.ft.com/2016/08/10/2172380/how-i-learned-to-stop-blockchain-obsessing-and-love-the-barry-manilow/>.

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 **Fig - 4**).



In this example, a 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 regulator may have complete transparency into the ledger with access to all public and private data.

The ledger could have elements that are:

- Public
  The public aspects of the ledger could be queried by anyone who can access the distributed ledger. For example, the public information available reflects that a trade for 100 shares of company ABC was made on 11/21/2016 at 2:45:05 P.M for $10 a share

- Private
  The private information might contain additional information like the information of the buyer and seller of the trade and information on their accounts

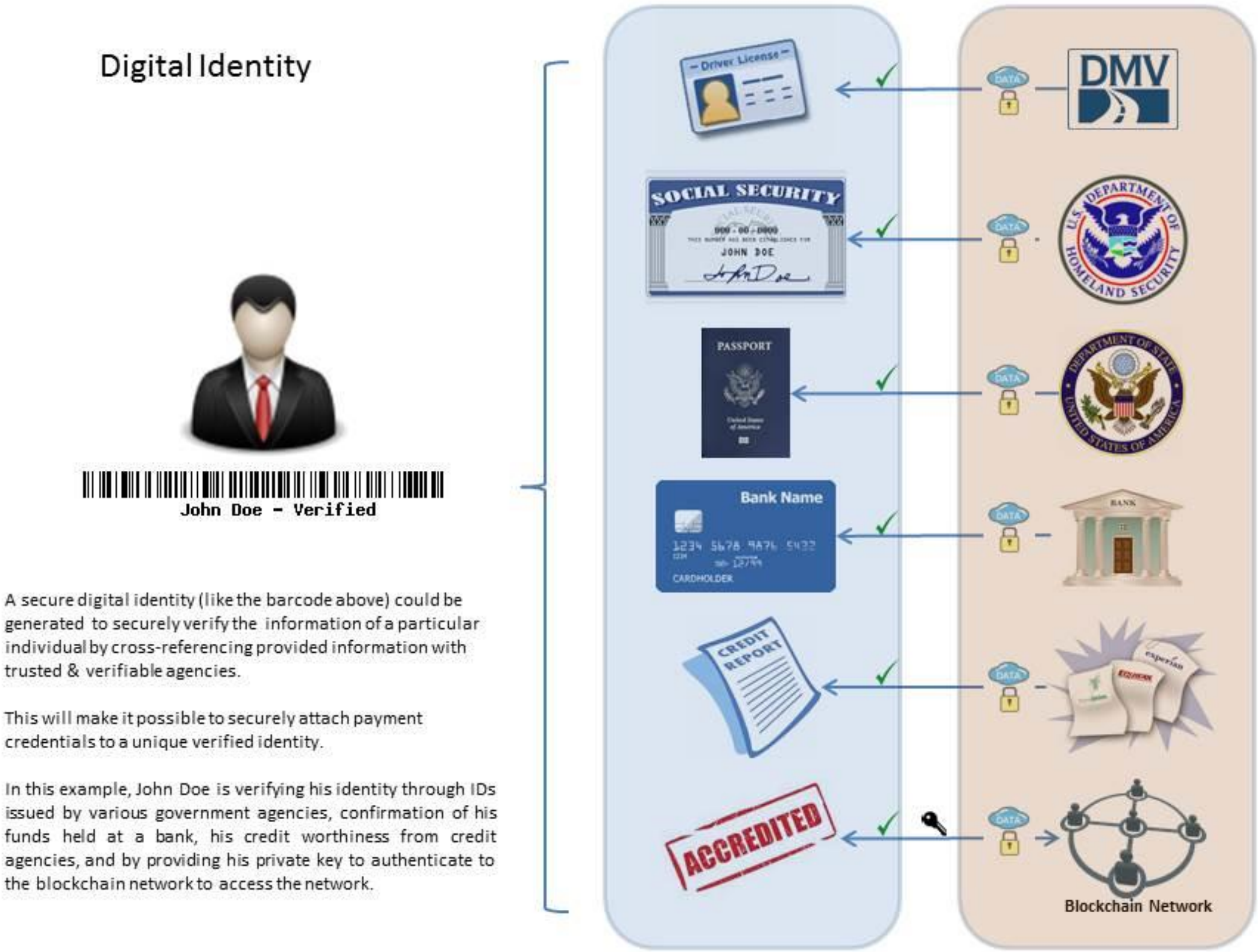
Source – Financial Markets Group, Federal Reserve Bank of Chicago

Fig – 4

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 its policy implications.

Before any transaction can occur on a blockchain, there must be a way to verify the identities of those wishing to transact. This can be achieved through the creation of digital identities. These unique digital identities are connected to private keys that allow users to confirm transactions involving their assets on a blockchain (see **Fig - 5**).



A secure digital identity (like the barcode above) could be generated to securely verify the information of a particular individual by cross-referencing provided information with trusted & verifiable agencies.

This will make it possible to securely attach payment credentials to a unique verified identity.

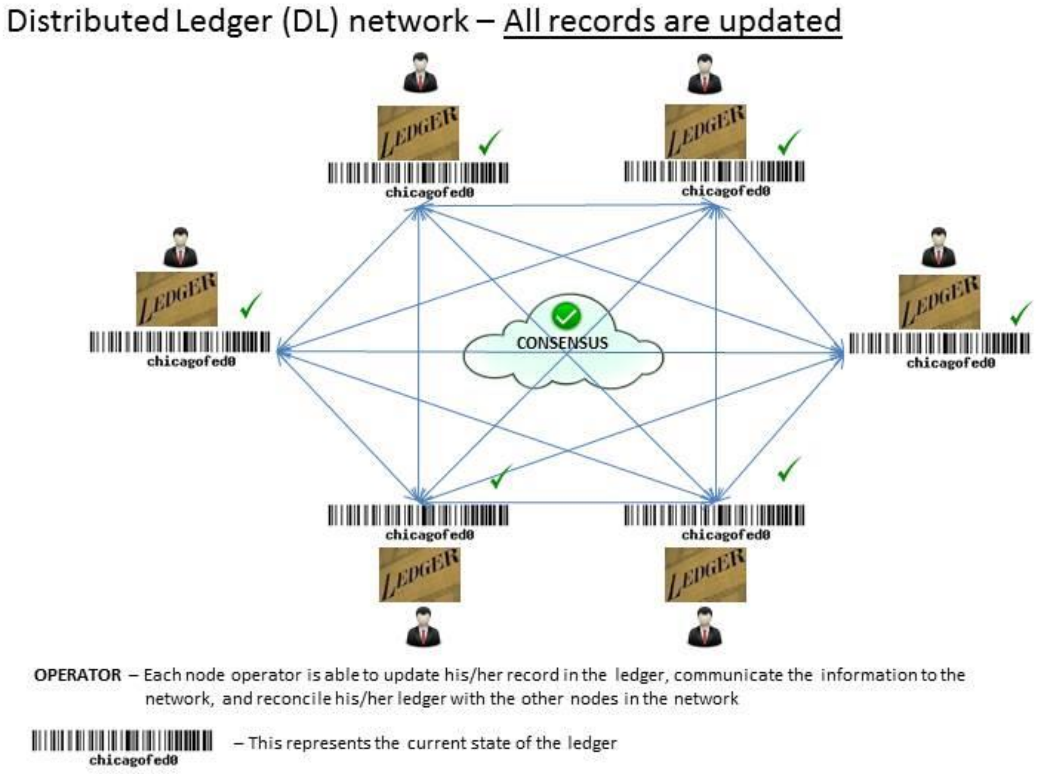
In this example, John Doe is verifying his identity through IDs issued by various government agencies, confirmation of his funds held at a bank, his credit worthiness from credit agencies, and by providing his private key to authenticate to the blockchain network to access the network.

Source – Financial Markets Group, Federal Reserve Bank of Chicago

Fig - 5

Basic distributed ledger set-up

In its simplest form, each user can read from and write to the database; 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 **Fig - 6** below).



Distributed Ledger (DL) network – All records are updated

OPERATOR – Each node operator is able to update his/her record in the ledger, communicate the information to the network, and reconcile his/her ledger with the other nodes in the network

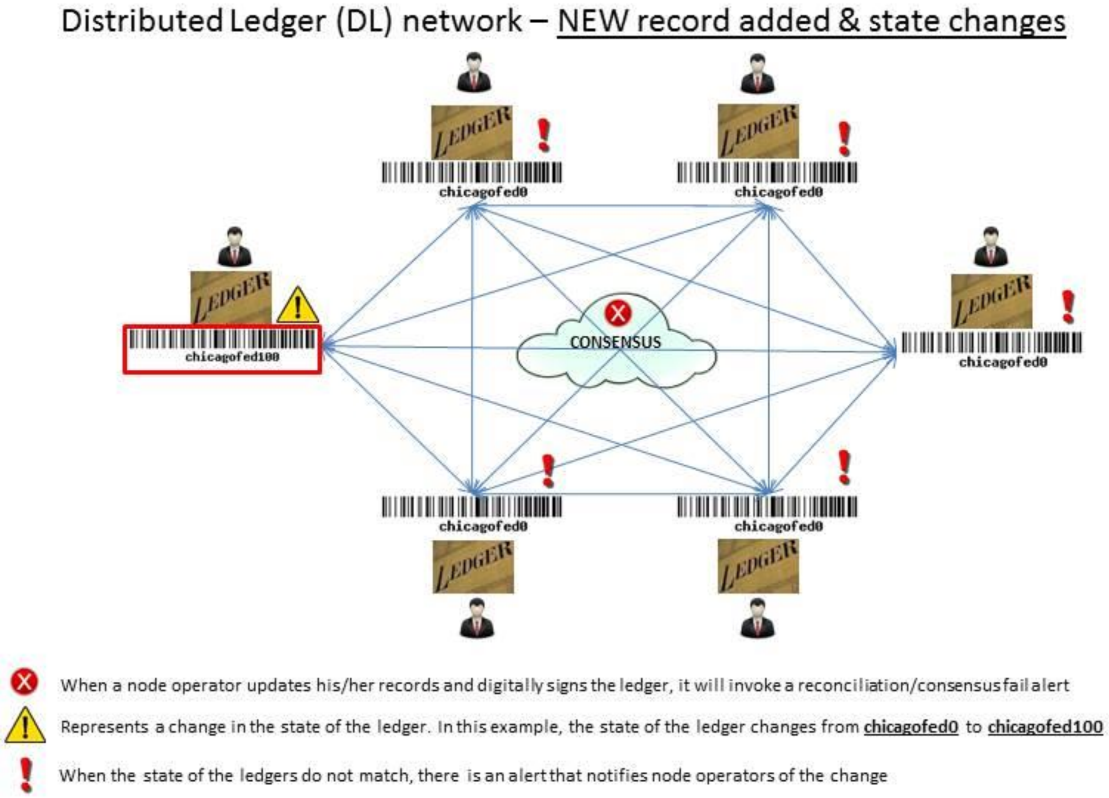
chicagofed0 – This represents the current state of the ledger

Source – Financial Markets Group, Federal Reserve Bank of Chicago

Fig - 6

In the example above, 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 **Fig - 7**). 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.


Distributed Ledger (DL) network – NEW record added & state changes
LEDGER
chicagofed0
chicagofed100
CONSENSUS

⊗ 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 state of the ledgers do not match, there is an alert that notifies node operators of the change

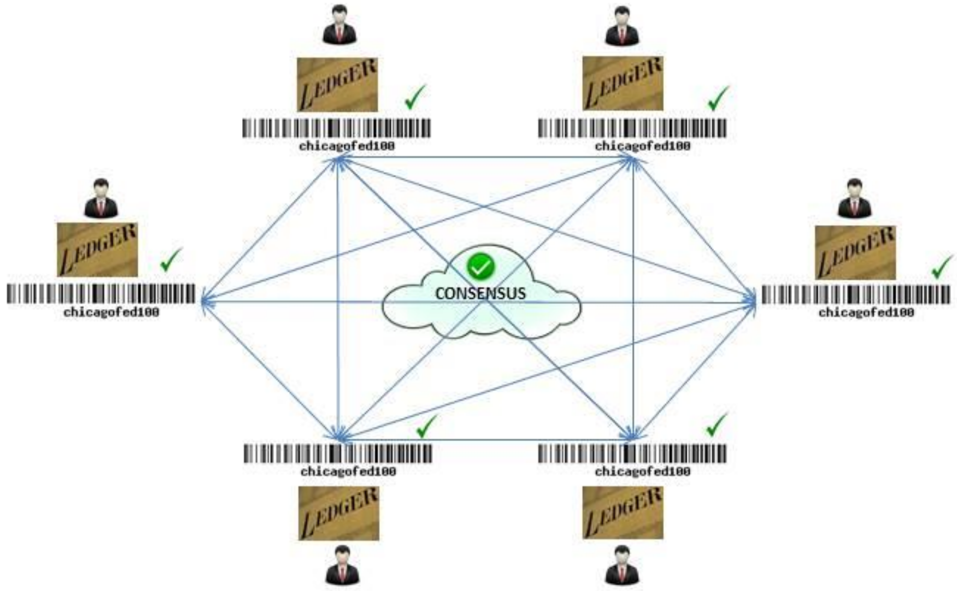
Source – Financial Markets Group, Federal Reserve Bank of Chicago

Fig – 7

There are various consensus methodologies including Proof-of-work (POW), Proof-of-stake (POS), fault tolerance algorithms that can be used in distributed computing systems like blockchain.

Once the consensus mechanism confirms the submitted transaction as valid, all ledgers are updated to reflect the new state (see **Fig - 8**).

Distributed Ledger (DL) network – Reconciliation & Consensus achieved



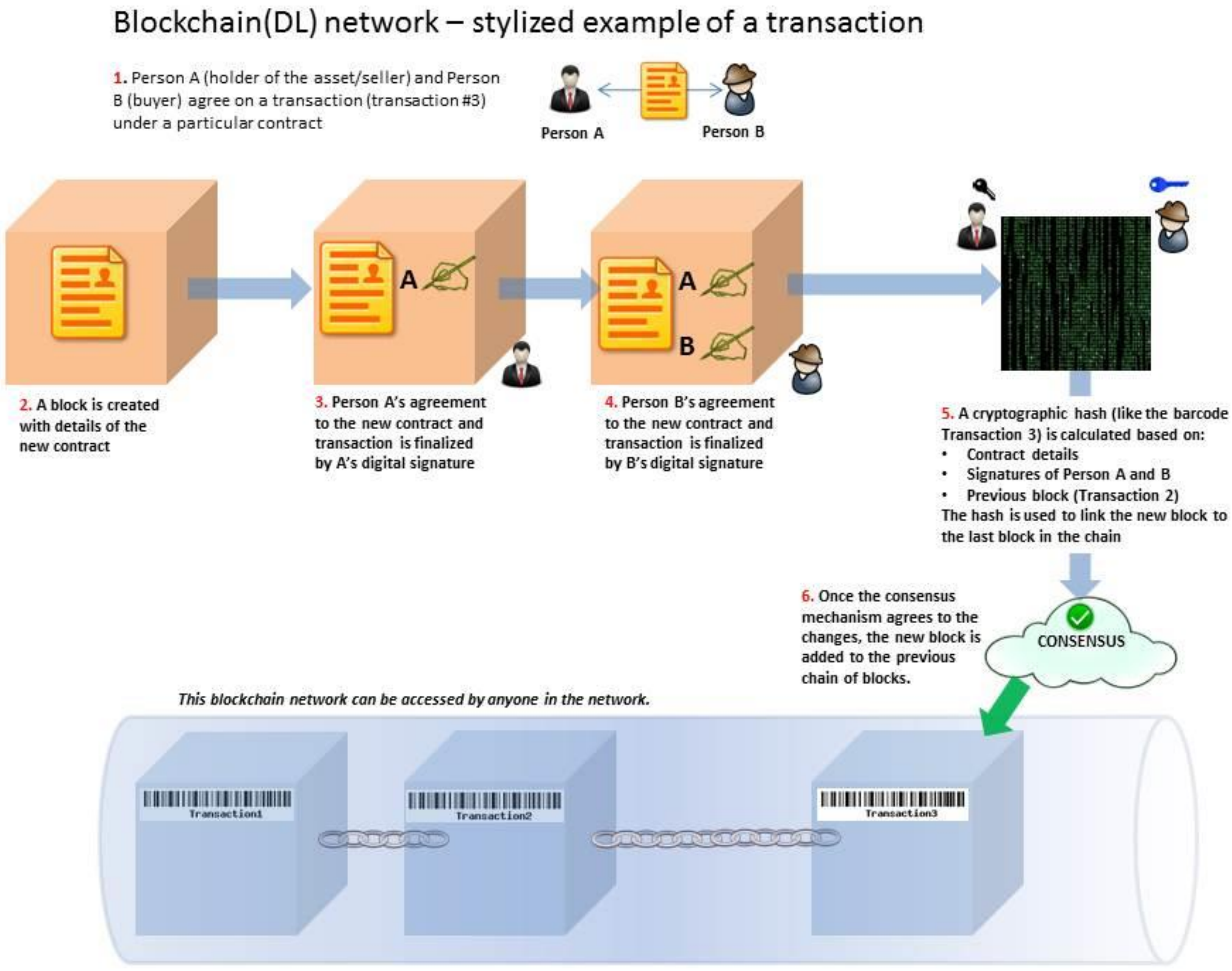
When all node operators agree to the new data change and consensus is achieved, the entire network will update their own ledgers. A state of reconciliation is reached. This ensures the immutability of records for network participants and end users.

Source – Financial Markets Group, Federal Reserve Bank of Chicago

Fig – 8

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 **Fig - 9**.


Blockchain(DL) network – stylized example of a transaction
1. Person A (holder of the asset/seller) and Person B (buyer) agree on a transaction (transaction #3) under a particular contract
Person A
Person B
A
A
B
2. A block is created with details of the new contract
3. Person A's agreement to the new contract and transaction is finalized by A's digital signature
4. Person B's agreement to the new contract and transaction is finalized by B's digital signature
5. A cryptographic hash (like the barcode Transaction 3) is calculated based on:
• Contract details
• Signatures of Person A and B
• Previous block (Transaction 2)
The hash is used to link the new block to the last block in the chain
6. Once the consensus mechanism agrees to the changes, the new block is added to the previous chain of blocks.
CONSENSUS
This blockchain network can be accessed by anyone in the network.
Transaction1
Transaction2
Transaction3

Source – Financial Markets Group, Federal Reserve Bank of Chicago

Fig – 9

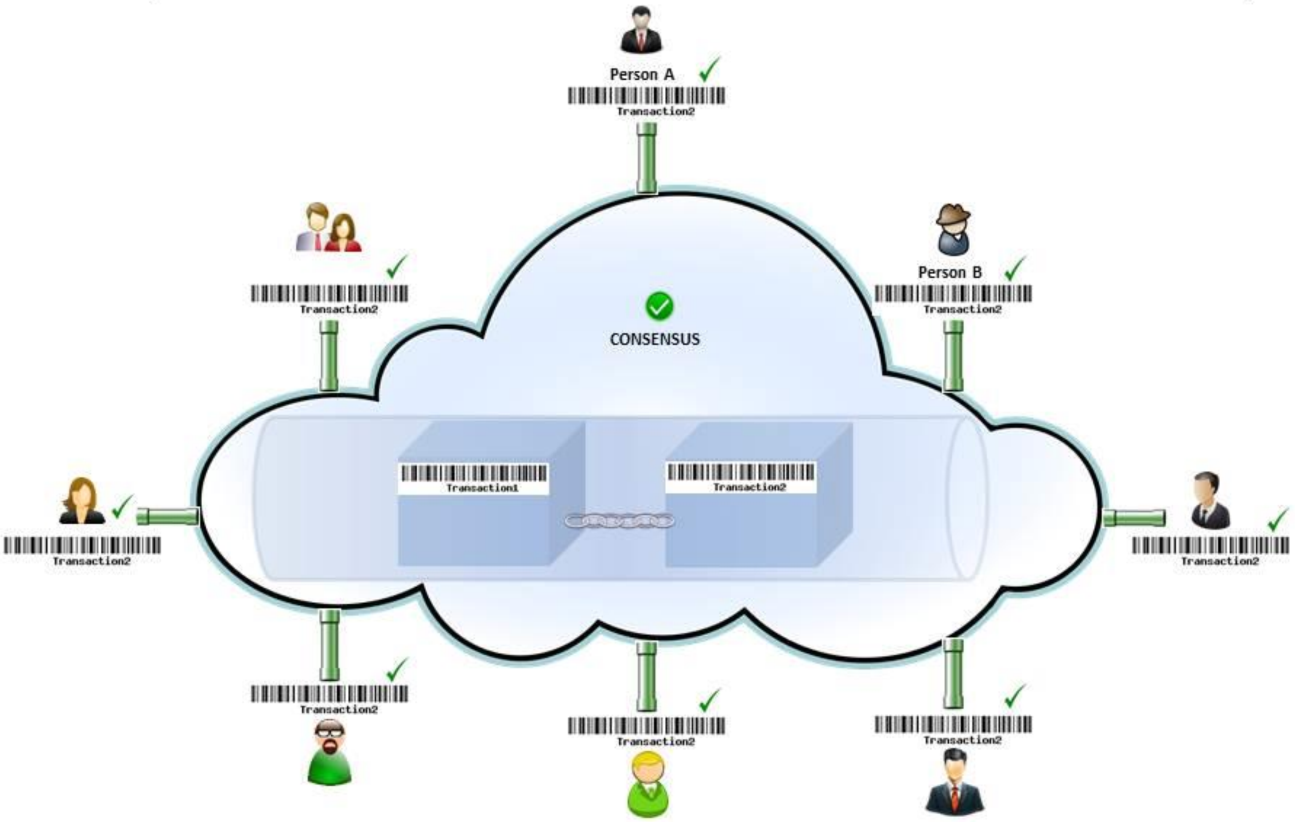
For person A to transfer an asset to person B, it is first necessary to determine if A is the rightful owner of that asset. This can be done by referencing past transactions in the blockchain and finding that at some point, A received the asset and has not yet sold it. Once this is done, A and B can agree to the transaction (step 1). A block is created with the details of the new contract (step 2), and then A and B each 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).

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 be transmitted to all participants in the network so that everyone had a matching copy of the master ledger.

The consensus mechanism will differ depending upon the design of the blockchain, but **Fig – 10** provides a general overview of how a consensus mechanism functions.

Blockchain(DL) network – Set up

0. Original state of the blockchain network. The last block of the network has the current information about an asset and a reference to its history

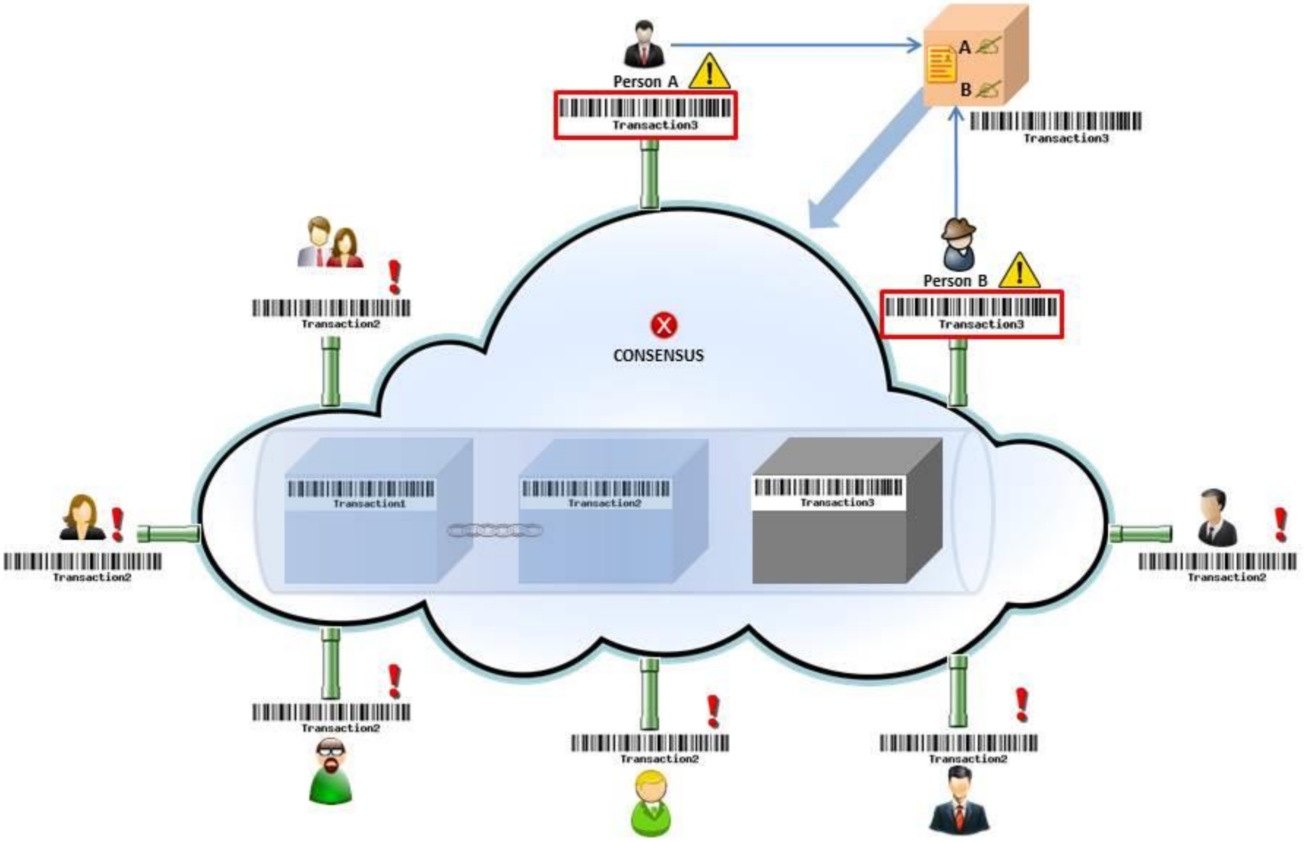


Source – Financial Markets Group, Federal Reserve Bank of Chicago

Fig – 10a

Blockchain(DL) network – Adding the new block

1. When a new block (transaction) is agreed upon and the hash calculation matches the other block's, the new block is added to the previous chain of blocks, once the consensus mechanism approves the new block

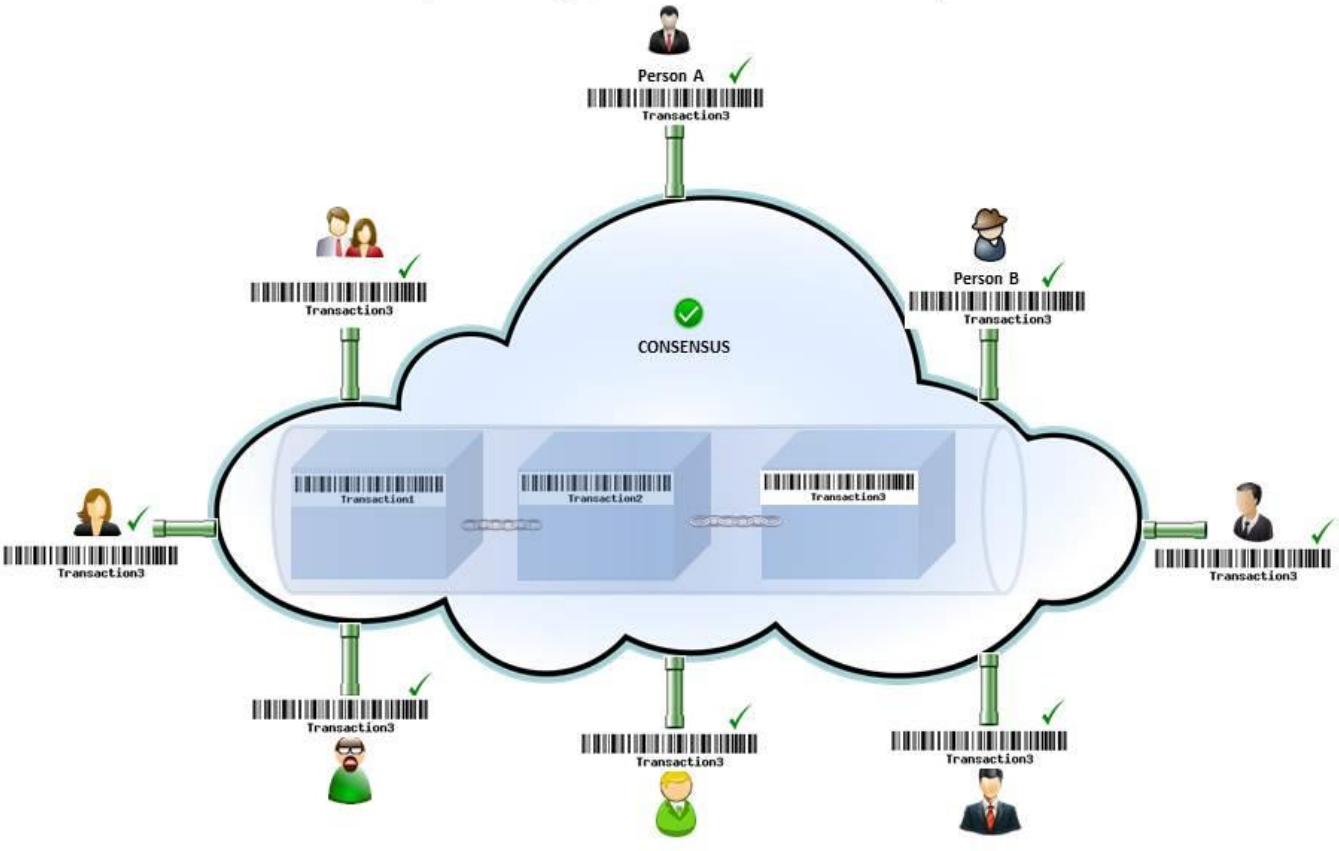


Source – Financial Markets Group, Federal Reserve Bank of Chicago

Fig – 10b

Blockchain(DL) network – Consensus achieved and block added to the network

2. Once the consensus mechanism agrees to the changes, the new block is added and chained to the previous block.



Source – Financial Markets Group, Federal Reserve Bank of Chicago

Fig – 10c

The nature of the consensus mechanism depends upon whether or not 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 mechansim. 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.

In one implementation of an unpermissioned blockchain, the Bitcoin blockchain, individuals known as miners compile submitted transactions into blocks. Miners race to solve a difficult computer problem; the first miner to solve the problem confirms the block that that miner created by adding it to the blockchain. They are awarded a certain number of bitcoins as a reward. Trust in transactions is maintained because the reward for submitting transactions is greater than the potential reward for fraud given the low probability of one’s fraudulent block winning the race. This system could break down if a user, or consortium of users, gained a majority of the computing power. They could then submit fraudulent transactions that had a high probability of being confirmed since the block they compile would be more likely than not to win the race to be added to the chain.

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 would be to fraudulently change; such a change would require updating the block with the transaction itself as well as every subsequent block in the same order in which the blocks were created.

Part II: Applications and Challenges

Blockchain technology has the potential to provide large efficiency gains. There are many potential use cases for blockchain in businesses that currently require costly intermediation, including financial services. While there are many potential applications of blockchain technology, 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.[5]

APPLICATIONS

Possible applications of blockchain technology include:

- Digital Information
    - Digital Identities – With the creation of a digital identities and blockchain's integration with various payment systems and bank networks, Identity Management and Fraud Protection will be achieved with greater speed and efficiency. This may enable faster KYC and AML checks, which are regulatory mandates for most financial institutions.

    - Digital Assets – Physical assets (real estate, stock certificates, gold, etc.) require a great deal of verification and examination every time they transact. This prolongs the transaction time and settlement time of a transaction. 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 as the owner of the asset as 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 (China, U.K, South Africa, Netherlands) around the world are experimenting with issuing digital state-sponsored fiat currencies backed by the central government.

    - Digital Wallets – Digital wallets are essentially a non-physical, digital version of a payment system. Popular examples include Apple Pay, Google Wallet, and PayPal,

[5] "Distributed ledger technology in payment, clearing, and settlement," Committee on Payments and Market Infrastructures, February 2017. <http://www.bis.org/cpmi/publ/d157.pdf>.

    which are linked to traditional bank account or credit cards. The next generation of digital wallets may carry digitized assets and currencies newly created using DLT. These digital wallets may have the unique feature of authentication via digital identities and transactional capabilities using cryptographic signatures. A use case for this has been demonstrated with bitcoin wallets carrying bitcoins and other crypto-currencies.

    - Digital Record Keeping – One of the key benefits of DLT is that it keeps an audit trail of each and every transaction and details of the parties involved. Adding an entry to the ledger or a block to the chain is depended on a consensus mechanism and if designed and executed in the right format, the record keeping process will be standardized, immutable, less prone to mistakes, and easy for interested parties to query.

- Automated Regulatory Compliance – The distributed nature of DLT can help achieve greater operational efficiencies in implementing and monitoring internal controls at an enterprise level.

- 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 its attestation by an official source. This may foster greater liquidity in certain types of trades that currently face lengthy settlement cycles and may promote better capital usage.

    - Easier title transfer of assets – With the creation of digital identities and digital assets, the time taken to settle the process of ownership and transfer of ownership may significantly decrease. For example, the title transfer of a home to the buyer from the seller is currently a multi-day process. It requires many middlemen (Title Company, escrow accounts at banks, loan originators, credit agencies, banks, inspectors, property assessor) and a multi-step approval process. DLT can reduce the processing time significantly and improve 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 – The 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 for movement of currencies. A DLT service with digital identities for the parties involved in a trade could be used to shorten the settlement time while still complying with regulations.

- 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.

CHALLENGES

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

Technical & Business challenges include:

- The 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.

- Lack of standardization of blockchain network designs – A lack of standardization can cause major issues in implementation and acceptance by businesses. Many national and international organizations are trying to establish generally accepted technical standards.

- Interoperability with legacy systems – Current businesses will face the issues of interoperability of blockchain platforms with their existing legacy systems internally. Externally, it remains to be seen how blockchains from multiple businesses might operate with each other.

- Increasing the scale of distributed ledger systems – This is especially a problem 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 and raising questions about scalability. All networks, permissioned or permissionless, will require a large amount of storage resources, as each node in the network will have and store its own copy of the distributed ledger.

- Balancing the tradeoffs between the efficiency of the 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 has the advantage of not needing everyone in the network to agree to trust certain parties.

- The immutability of transactions – 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.

- The distributed nature of blockchain systems – While the reduced reliance on a central authority and 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 cyber-criminals to target. If cyber-criminals are able to steal the information of a user necessary to submit a trade, they could create fraudulent, and immutable, transactions.

- Liquidity concerns during title transfers – While the use of a blockchain for title transfers could drastically reduce the risk associated with current settlement conventions, it does increase the importance of liquidity; funds and assets must be in proper form and location for such expedited settlement.

- The confidentiality of information and the speed of information about the record changes – In finance, the acquisition and analysis of data are key to a firm's competitive advantage. With distributed nature of the ledgers many incumbent firms will be hesitant to participate in a shared database as there might be information leakage which could cost the firms business.

- Intellectual property rights – Industry participants involved in blockchain research are increasingly patenting blockchain-related technologies; the number of blockchain-related patents filed has doubled between January and November 2016.[6] The patents could make firms working with blockchain technologies vulnerable to legal challenges which may slow down innovation and prevent new firms from entering the market.

Regulatory challenges include:

- Uncertainty over rules across various regulatory agencies. Existing regulations may be major hurdles for DLTs. The first step in improving the regulatory environment is to create a regulatory sandbox to allow DLT firms to work alongside the regulatory agencies in testing new products and services.

- Maintaining central bank controls 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 provides 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, which are likely to enable better cooperation between the public sector and private sector, improving transparency, trust, information sharing, and historical audit trails. Normally, technology is thought of as the means to implement a solution to a preexisting problem. With DLT, we may have to take a bottom-up approach and think of potential problems that it can solve.

[6] Kharif, Olga. "Who Owns Blockchain? Goldman, BofA Amass Patents for Coming Wars." Information Management. 21 Dec. 2016. Web. 15 June 2017. <http://www.information-management.com/news/data-management/who-owns-blockchain-goldman-bofa-amass-patents-for-coming-wars-10030542-1.html?CMP=OTC-RSS>.