<https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/>

**Blockchain basics: Introduction to distributed ledgers**

What is a distributed ledger?

* A distributed ledger is a type of database that is shared, replicated, and synchronized among the members of a decentralized network.
* The distributed ledger records the transactions, such as the exchange of assets or data, among the participants in the network.
* Participants in the network govern and agree by consensus on the updates to the records in the ledger.
* No central authority or third-party mediator, such as a financial institution or clearinghouse, is involved.
* Every record in the distributed ledger has a timestamp and unique cryptographic signature, thus making the ledger an auditable, immutable history of all transactions in the network.

The role of business ledgers

Business networks typically come together at marketplaces where the ***participants***, such as

* producers,
* consumers,
* suppliers,
* partners,
* market makers/enablers, and
* other stakeholders

own, control, and exercise their rights, privileges, and entitlements on objects of value known as ***assets***.

Tangible and physical assets

* Car
* Home

 Intangible and virtual assets

* Deeds
* Patents
* Stock certificates

Asset ownership and transfers are the **transactions** that create value in a business network.

Problems with current business ledgers

Current business ledgers in use today are deficient in many ways. They are

* inefficient,
* costly,
* subject to misuse and tampering.
* Lack of transparency, as well as
* susceptibility to corruption and fraud

These risks and uncertainties contribute to missed business opportunities.

What is blockchain, exactly?

A blockchain is a

* tamper-evident,
* shared digital ledger

that records transactions in a public or private peer-to-peer network.

Distributed to all member nodes in the network, the ledger permanently records, in a sequential chain of cryptographic hash-linked **blocks**,

All the confirmed and validated transaction blocks are linked and chained from the beginning of the chain to the most current block, hence the name **blockchain**.

Blockchain is the digital and decentralized ledger technology that records all transactions without the need for a financial intermediary like a bank.

How does a blockchain network work?

Instead of relying on a third party, such as a financial institution, to mediate transactions, member nodes in a blockchain network use a consensus protocol to agree on ledger content, and cryptographic hashes and digital signatures to ensure the integrity of transactions.

**Consensus** ensures that the shared ledgers are exact copies, and lowers the risk of fraudulent transactions, because tampering would have to occur across many places at exactly the same time.

***Cryptographic hashes***, such as the SHA256 computational algorithm, ensure that any alteration to transaction input — even the most minimal change — results in a different hash value being computed, which indicates potentially compromised transaction input.

***Digital signatures*** ensure that transactions originated from senders (signed with private keys) and not imposters.

The decentralized peer-to-peer blockchain network prevents any single participant or group of participants from controlling the underlying infrastructure or undermining the entire system.

Participants in the network are all equal, adhering to the same protocols. They can be individuals, state actors, organizations, or a combination of all these types of participants.

How blocks are added to the chain?

1. A cryptographic puzzle must be solved thus creating the block.
2. The computer that solves the puzzle shares the solution to all the other computers on the network. That is called proof-of-work.
3. The network verifies the proof-of-work.
4. If correct the block will be added to the chain

What are the business benefits of blockchain?

In legacy business networks, all participants maintain their own ledgers with duplication and discrepancies that result in disputes.

However, by using blockchain-based shared ledgers, where transactions cannot be altered once validated by consensus and written to the ledger, businesses can *save time and costs while reducing risks*.

Immutability mechanisms of blockchain technologies lead to lowered cost of audit and regulatory compliance with improved transparency.

No more intermediaries which can save both time and money.

Five of the biggest advantages of Blockchain technology.

**Transparency**

One of the prime reasons blockchain is intriguing to businesses is that this technology is almost always open source. That means other users or developers have the opportunity to modify it as they see fit. But what's most important about it being open source is that it makes altering logged data within a blockchain incredibly difficult. After all, if there are countless eyes on the network, someone is probably going to see that logged data has been altered. This makes blockchain a particularly secure technology.

**Reduced transaction costs**

As noted, blockchain allows peer-to-peer and business-to-business transactions to be completed without the need for a third party, which is often a bank. Since there's no middleman involvement tied to blockchain transactions, it means they can actually reduce costs to the user or businesses over time.

**Faster transaction settlements**

When it comes to traditional banks, it's not uncommon for transactions to take days to completely settle. This is due to protocols in bank transferring software, as well as the fact that financial institutions are only open during normal business hours, five days a week. You also have financial institutions located in various time zones around the world, which can delay processing times. Comparatively, blockchain technology is working 24 hours a day, seven days a week, meaning blockchain-based transactions process considerably more quickly.

**Decentralization**

Another central reason blockchain is so exciting is its lack of a central data hub. Instead of running a massive data center and verifying transactions through that hub, blockchain actually allows individual transactions to have their own proof of validity and the authorization to enforce those constraints. With information on a particular blockchain piecemealed throughout the world on individual servers, it ensures that if this information fell into unwanted hands (e.g., a cyber-criminal), only a small amount of data, and not the entire network, would be compromised.

**User-controlled networks**

Lastly, cryptocurrency investors are tending to be really encouraged by the control aspect of blockchain. Rather than having a third party run the show, users and developers are the ones who get to call the shots. For instance, an inability to reach an 80% consensus on an upgrade tied to bitcoin's blockchain is what necessitated a fork into two separate currencies (bitcoin and bitcoin cash)

What's a good blockchain use case?

* In finance, blockchain networks allow securities trades to be settled in minutes rather than days.
* In supply chains, blockchain networks allow the flow of goods and payments to be tracked and logged in real time.

To determine whether your use case is a good fit for blockchain, ask yourself these questions:

1. Is a business network involved?
2. Is consensus used to validate transactions?
3. Is an audit trail, or provenance, required?
4. Must the record of transactions be immutable, or tamper proof?
5. Should dispute resolution be final?

If you answered yes to the first question and to at least one other, then your use case would benefit from blockchain technology.

A network always needs to be involved for blockchain to be the right solution

What is Hyperledger?

* [Hyperledger](http://www.hyperledger.org/) is an open source effort to advance cross-industry blockchain technologies for business use.
* It's a global collaboration, hosted by The Linux Foundation.
* These 183+ diverse members and 9 ongoing projects, including Hyperledger Fabric and Hyperledger Composer, work in concert to create distributed ledger framework and code base.

The [**Hyperledger Fabric**](https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/IBM%20Blockchain:%20From%20farm%20to%20table) framework supports distributed ledger solutions on permissioned networks, where the members are known to each other, for a wide range of industries.

[Hyperledger Composer](https://www.hyperledger.org/projects/fabric) is a set of free, open source tools for quickly prototyping, defining, and testing a Hyperledger Fabric blockchain network and writing applications to interact with it.

Types of Blockchain

Blockchain is a type of technology not a single network. It can be implemented in many different ways.

1. Public Blockchain – Open to everyone to view and access
2. Private Blockchain – Access to a select group of authorized users.
3. Hybrid Blockchain – combination of both private and public Blockchain

A permissionless blockchain is also known as a public blockchain, because anyone can join the network. A permissioned blockchain, or private blockchain, requires pre-verification of the participating parties within the network, and these parties are usually known to each other.

The supply chain management is an ideal use case for permissioned blockchains.

Bitcoin blockchain, is a permissionless blockchain.

Projects on which domains

****