# Blockchain

## Defn

- A **blockchain** is a type of distributed ledger technology (DLT) that consists of growing lists of records, called *blocks*, that are securely linked together using cryptography
- Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree, where data nodes are represented by leaves)
- The timestamp proves that the transaction data existed when the block was created
- Since each block contains information about the previous block, they effectively form a *chain* (compare linked list data structure), with each additional block linking to the ones before it. Consequently, blockchain transactions are irreversible in that, once they are recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks.

- Blockchains are typically managed by a peer-to-peer (P2P) computer network for use as a public distributed ledger
- where nodes collectively adhere to a consensus algorithm protocol to add and validate new transaction blocks. Although blockchain records are not unalterable, since blockchain forks are possible, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance

## Structure and design

- A blockchain is a decentralized, distributed, and often public, digital ledger consisting of records called *blocks* that are used to record transactions across many computers so that any involved block cannot be altered retroactively, without the alteration of all subsequent blocks
- This allows the participants to verify and audit transactions independently and relatively inexpensively
- A blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server.

## Logical blockchain layers

- infrastructure (hardware)
- networking (node discovery, information propagation and verification)
- consensus (proof of work, proof of stake)
- data (blocks, transactions)
- application (smart contracts/decentralized applications, if applicable)

## **Blocks**

- Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree
- Each block includes the cryptographic hash of the prior block in the blockchain, linking the two. The linked blocks form a chain
- This iterative process confirms the integrity of the previous block, all the way back to the initial block, which is known as the *genesis block*

## Block time

- The *block time* is the average time it takes for the network to generate one extra block in the blockchain. By the time of block completion, the included data becomes verifiable. In cryptocurrency, this is practically when the transaction takes place, so a shorter block time means faster transactions.

## Hard forks

- is a rule change such that the software validating according to the old rules will see the blocks produced according to the new rules as invalid. In case of a hard fork, all nodes meant to work in accordance with the new rules need to upgrade their software. If one group of nodes continues to use the old software while the other nodes use the new software, a permanent split can occur.

## TYPES OF BLOCKCHAIN NETWORKS

**Public blockchains**

- A public blockchain has absolutely no access restrictions. Anyone with an Internet connection can send transactions to it as well as become a validator (i.e., participate in the execution of a consensus protocol)
- Usually, such networks offer economic incentives for those who secure them and utilize some type of a Proof of Stake or Proof of Work algorithm.

## Private blockchains

- A private blockchain is permissioned
- One cannot join it unless invited by the network administrators. Participant and validator access is restricted. To distinguish between open blockchains and other peer-to-peer decentralized database applications that are not open ad-hoc compute clusters, the terminology Distributed Ledger (DLT) is normally used for private blockchains.

## Hybrid blockchains

- A hybrid blockchain has a combination of centralized and decentralized features.[1]
- The exact workings of the chain can vary based on which portions of centralization and decentralization are used.

## Sidechains

- A sidechain is a designation for a blockchain ledger that runs in parallel to a primary blockchain
- Entries from the primary blockchain (where said entries typically represent digital assets) can be linked to and from the sidechain; this allows the sidechain to otherwise operate independently of the primary blockchain (e.g., by using an alternate means of record keeping, alternate consensus algorithm

## Uses of Blockchain

- **Cryptocurrencies**
- **Smart contracts**
- **Financial services**
- **Games**
- **Supply chain**
- **Domain names**

## How Blockchain is Improving Business Operations

- **Audits :** Blockchain offers what is essentially a permanent record of transactions, which creates an easy-to-follow paper trail for audits, both internal and governmental. It guarantees accuracies and solves the problem of pulling in records from a number of disparate sources.

- **Quality assurance :** Blockchain also has potential when it comes to quality assurance, especially when something goes wrong. Since companies can link every facet of the supply chain, if there is the need for a recall or investigation into where something went wrong, blockchain offers a definitive, contiguous ledger to immediately identify the problem.

- **Securities and commodities trading :** Blockchain promises quicker trading on stock exchanges, whether in securities or commodities. The distributed nature of the technology ensures that a process previously undertaken over the course of several days is affirmed and finalized in just several minutes, greatly streamlining the entire experience.

- **Smart contracts :** Smart contracts enable a way for organizations to handle large amounts of transactions, such as those that run across supply chains, automatically. They can be used to integrate services across different businesses without divulging sensitive or proprietary information.

## Supply chain management

- Blockchain can track goods and materials within an organization, as well, such as throughout the supply chain of a manufacturing company. As a product leaves the factory, blockchain could be used to record its arrival at a warehouse and then its shipment out to a retail store, for example.

- **Voting :** Just like currency, votes can be moved along a blockchain in a neutral, accurate and secure way. Using blockchain as a mechanism for consensus-building in communities and even nations could radically alter modern notions of democracy and strengthen the validity of election results.

## DISCUSSION QUESTION

- What are the differences between blockchain and cryptocurrency?

## CRYPTOCURRENCY

- is a digital currency designed to work as a medium of exchange through a computer network that is not reliant on any central authority, such as a government or bank, to uphold or maintain it.

## Key concepts of Cryptocurrency

- **Transferability :** makes transactions with people on the other side of the planet as seamless as paying with cash at your local grocery store.
- **Privacy** When paying with cryptocurrency, you don't need to provide unnecessary personal information to the merchant. Which means your financial information is protected from being shared with third parties like banks, payment services, advertisers, and credit-rating agencies. And because no sensitive information needs to be sent over the internet, there is very little risk of your financial information being compromised, or your identity being stolen.

- **Security** Almost all cryptocurrencies, including Bitcoin, Ethereum, Tezos, and Bitcoin Cash are secured using technology called a blockchain, which is constantly checked and verified by a hu
- **Portability** Because your cryptocurrency holdings aren't tied to a financial institution or government, they are available to you no matter where you are in the world or what happens to any of the global finance system's major intermediaries. ge amount of computing power.

- **Transparency** Every transaction on the Bitcoin, Ethereum, Tezos, and Bitcoin Cash networks is published publicly, without exception. This means there's no room for manipulation of transactions, changing the money supply, or adjusting the rules mid-game.
- **Irreversibility** Unlike a credit card payment, cryptocurrency payments can't be reversed. For merchants, this hugely reduces the likelihood of being defrauded. For customers, it has the potential to make commerce cheaper by eliminating one of the major arguments credit card companies make for their high processing fees.
- **Safety** The network powering Bitcoin has never been hacked. And the fundamental ideas behind cryptocurrencies help make them safe: the systems are permissionless and the core software is open-source, meaning countless computer scientists and cryptographers have been able to examine all aspects of the networks and their security.

## cryptocurrency is a system that meets six conditions

- The system does not require a central authority; its state is maintained through distributed consensus.
- The system keeps an overview of cryptocurrency units and their ownership.
- The system defines whether new cryptocurrency units can be created. If new cryptocurrency units can be created, the system defines the circumstances of their origin and how to determine the ownership of these new units.
- Ownership of cryptocurrency units can be proved exclusively cryptographically.
- The system allows transactions to be performed in which ownership of the cryptographic units is changed. A transaction statement can only be issued by an entity proving the current ownership of these units.
- If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs at most one of them.

## How Does Cryptocurrency Work?

- A cryptocurrency is a digital, encrypted, and decentralized medium of exchange. Unlike the U.S. Dollar or the Euro, there is no central authority that manages and maintains the value of a cryptocurrency. Instead, these tasks are broadly distributed among a cryptocurrency's users via the internet.
- You can use crypto to buy regular goods and services, although most people invest in cryptocurrencies as they would in other assets, like stocks or precious metals. While cryptocurrency is a novel and exciting asset class, purchasing it can be risky as you must take on a fair amount of research to understand how each system works fully.
- Bitcoin was the first cryptocurrency, first outlined in principle by Satoshi Nakamoto in a 2008 paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System." Nakamoto described the project as "an electronic payment system based on cryptographic proof instead of trust."