Blockchain

Contents

[Introduction 2](#_Toc102585706)

[Problem 2](#_Toc102585707)

[What is it? 2](#_Toc102585708)

[Key Points 3](#_Toc102585709)

[Ledgers, Transactions and Contracts 3](#_Toc102585710)

[How does Blockchain work? 3](#_Toc102585711)

[Types of Blockchains 4](#_Toc102585712)

[Public Blockchains 4](#_Toc102585713)

[Private Blockchains 4](#_Toc102585714)

[Hybrid Blockchains/ Consortiums 4](#_Toc102585715)

[Sidechains 5](#_Toc102585716)

[What Is the Difference Between Bitcoin and Ethereum Blockchains? 5](#_Toc102585717)

[Bitcoin Basics 5](#_Toc102585718)

[Ethereum Basics 5](#_Toc102585719)

[Ethereum vs. Bitcoin Blockchains 6](#_Toc102585720)

[Glossary 6](#_Toc102585721)

[Block 6](#_Toc102585722)

# Introduction

## Problem

**Business Networks** benefit from connectivity:

* Participants are customers, suppliers, banks, partners
* Cross geography and regulatory boundary

**Wealth** is generated by the flow of goods and services across business network in transactions and contracts

**Markets** are central to this process:

* Public (fruit market, car auction), or
* Private (supply chain financing, bonds)

**Two fundamental types of assets**

* Tangible, e.g., a house
* Intangible, e.g., a mortgage
* Intangible assets subdivide
  + Financial, e.g., bond
  + Intellectual, e.g., patents
  + Digital, e.g., data
* Cash is also an asset which has a property of anonymity

# What is it?

As the word describes, blockchain is essentially a chain of blocks containing information. The original intention of blockchain was to avoid backdating digital documents by timestamping them however, it was not really used until it was adapted to create the digital cryptocurrency Bitcoin. Blockchain was initially developed to increase efficiency in businesses. Previously, most business networks captured financial transactions of the companies they interacted with by keeping records, ledgers, etc which led to a lot of duplication of documents and wasted time which in turn incurred extra costs to which the solution of blockchain was derived.

Block chain is a method of storing data (information) in such a way that changing, hacking, or cheating it is difficult or impossible. The records are supervised by a large community rather than a single central authority, such as a bank, and no single person has power over them. Each block in the chain contains several transactions, and each participant's ledger is updated every time a new transaction occurs on the block chain. The block chain is a software protocol (just how SMTP for email) that consists of numerous components, including a database, software application, and a network of connected computers.

## Key Points

* A block chain is a series of read-only (irreversible) transactions tracked by a group of computers using special computer techniques.
* These irreversible recordings are not owned by a single entity.
* A block chain is a decentralised peer-to-peer (P2P) network of computers known as nodes. Simply put, a database which stores information in the form of transactions.
* In a block chain, each node possesses the same copy of data, which is referred to as the digital ledger.

# Ledgers, Transactions and Contracts

**Ledger:** a ledger is a book or collections of records which describes the inputs and outputs of the business. Account transactions are documented in a ledger.

**Transaction:** an asset transfers between participants.

For example, Tadas gives a car to John - simple.

**Contract:** the conditions for a transaction to occur.

For instance, if John pays Tadas some money, then the car passes from Tadas to John - simple. However, if the car fails to start, the funds do not pass to Tadas (as decided by a third-party authority) - more complex.

## Blockchain Transactions

When a transaction is completed on a blockchain and enough confirmation is received, the transaction becomes irreversible.

Diagram

Description automatically generated

# How does Blockchain work?

Blockchain acts as a distributed ledger, open to anyone and a key feature of it is that once data is recorded inside a blockchain, it is harder to change it. The blocks itself consists of 3 key points:

* Data,
* Hash,
* Hash of the previous block.

The data stored within the block will depend on the type of blockchain, for example, the Bitcoin blockchain data stores transaction details like sender, receiver and how many coins.

A block’s hash is its unique identifier, like a fingerprint, and is used to identify a block and its contents. On the block’s creation, its hash is also generated so if any changes are made to the block, a new hash would be generated.

To create the chain between the blocks, each block has the hash of the previous block which it will link to. Since the first block has no other blocks before it, it is often referred to as the genesis block. Noting the hash of the previous block in each following block is what makes tampering with data in blockchain difficult; if the data in a previous block is modified it will generate a new hash, so the hash it used to have and was persisted to the blocks following it would become invalid which is why changing a single block would make all the blocks after it worthless.

# Types of Blockchains

There are four types of blockchains:

## Public Blockchains

Anyone who wants to request or validate a transaction can use public blockchains, which are open, decentralised networks of computers (check for accuracy). Those who validate transactions (miners) get rewarded.

Proof-of-work or proof-of-stake consensus procedures are used in public blockchains (discussed later). The Bitcoin and Ethereum (ETH) blockchains are two popular examples of public blockchains.

## Private Blockchains

Private blockchains aren't public, and access is restricted. The system administrator must give permission to everybody who wants to join. They are usually centralised and managed by a single entity. Hyperledger, for example, is a permissioned, private blockchain.

## Hybrid Blockchains/ Consortiums

Consortiums are a hybrid of public and private blockchains with both centralised and decentralised functionality. Energy Web Foundation, Dragonchain, and R3 are just a few examples.

Keep in mind that there isn't universal agreement on whether these concepts are synonymous. Some people distinguish between the two, while others believe they are interchangeable.

## Sidechains

A sidechain is a blockchain that runs in the opposite direction from the main chain. It enhances scalability and efficiency by allowing users to transport digital assets across two blockchains. The Liquid Network is one example of a sidechain.

# What Is the Difference Between Bitcoin and Ethereum Blockchains?

## Bitcoin Basics

The Bitcoin network is a decentralised, public peer-to-peer payment system that allows users to send and receive bitcoins without the involvement of a bank. The digital currency, also known as a bitcoin token, is the only cryptocurrency traded on the Bitcoin network and has the ticker symbol BTC.

Nodes verify that the PoW consensus technique is followed by recording transactions in a digital ledger (or that mining happens). Bitcoin may appear complicated to some, but it isn't when you look at it as a combination of three things:

* A peer-to-peer payment system: Without the use of a bank, you can send money (BTC) from one person or company to another. Utilizing this approach to send money is faster, more secure, and less expensive than using traditional ways.
* A decentralised system, such as the internet, in which no single entity controls it and it cannot be halted by a third party.
* A store of value like gold (often called digital gold), but much easier to transfer than gold.

## Ethereum Basics

Vitlaik Buterin wanted to build on the Bitcoin blockchain in 2013 after travelling, meeting with bitcoin developers, and understanding Bitcoin's limits.

The Ethereum network is a decentralised peer-to-peer network that is open to the public. It uses nodes, like Bitcoin, and allows users to transmit and receive cryptocurrency—in this case, Ether.

The network was designed to deploy decentralised applications (dapps) and smart contracts, not just as a payment mechanism.

Decentralized apps, or computer programmes that communicate with the Ethereum blockchain, are known as Dapps. Smart contracts, on the other hand, run on the Ethereum blockchain and are contracts that execute without the need for a middleman whenever specific conditions (written into computer code) are met. For example, a smart contract may be configured to deliver a percentage of the proceeds to a specific person.

## Ethereum vs. Bitcoin Blockchains

Essentially, the Bitcoin and Ethereum networks are public, decentralised peer-to-peer networks with their own currency, bitcoins, and ether, respectively. Both use digital ledger technology and rely on encryption.

However, their functions and capabilities are vastly different. Bitcoin is a digital currency and a decentralised payment mechanism. Its blockchain is a database that keeps track of all bitcoin transactions and who owns them. Ethereum is more than just a payment system; it also allows for the creation of smart contracts and apps, making it a more advanced blockchain.

# Glossary

## Block

Blocks are files that exist on the block chain network and are used to permanently store data. Any or all recent transactions that haven't been logged in any of the prior blocks are kept in a block. As a result, a block resembles a ledger sheet or a book of records. A block is also a permanent record store that cannot be edited or erased after it has been published. As a result, a block is like a ledger page or a record book. Once published, a block is likewise a permanent record storage that cannot be modified or erased.