**Blockchain Trilemma:**

**Introduction**

* In basic terms, a **blockchain is a distributed digital database**. Blocks of **data are organized in chronological order**. The blocks are **linked and secured by cryptographic proofs**.
* **The idea is that decentralized and secure blockchains allow for a world where we don’t need to rely on third parties for networks or markets to function**. However, if this tech is to be more widely adopted there’s a core problem is “**blockchain trilemma**”.
* This term was popularized by **Ethereum co-founder Vitalik Buterin**.
* The blockchain trilemma refers to the idea that it’s **hard for blockchains to achieve optimal levels of all three properties** (**decentralization**, **security**, and **scalability**. ) simultaneously. **Increasing one usually leads to a weakening of another.**

## What is decentralization?

* **Bitcoin and similar blockchain networks are decentralized by design**. The whole structure is such that there is **no one person or organization in charge**. Rather, it is decentralized. The **network layer is open to anyone** who wants to participate. As a result, **control is fully distributed** rather than held by one single entity. **Everyone has access to the same data**. If anyone tries to cheat the system by changing the records in their favor, then the rest of the participants will reject the faulty data.
* This can get quite technical, but let’s take the Bitcoin network as an example. There is no third party in control. Compare this with the need for banks in the financial system. The banks enforce trust between people transacting, and ensure all records are kept correctly. The Bitcoin blockchain, however, shares all that data with everyone on the network, so that it can be **checked and confirmed, before being added to the digital database**. **The result is a system that can exist without the need for third parties.**
* **Decentralization offers the possibility of what is known as** [**Web3**](https://academy.binance.com/en/articles/the-evolution-of-the-internet-web-3-0-explained). Right now we have Web2 — the internet of today. It’s full of sites and apps controlled by companies, but featuring content made by the users. **Web3 is the next step. An internet where decentralized blockchain tech lets people control their own data and online lives.**
* One thing to note, however, is that because of how these **distributed systems work — with a need for a wide range of participants to agree on the validity of any data** — **transaction times can be slow due to the way information needs to be shared and processed**.
* And so, **blockchains need to scale, which is to say be capable of handling more data at faster speeds.**

## What is blockchain security?

* It doesn’t matter how decentralized a blockchain is if it lacks security. **A good blockchain network should be resistant to attacks from malicious entities**. Centralized systems derive their security from the fact that the system is closed. Whoever is in control can guarantee the data is free from interference. But how is this achieved in a decentralized system where anyone can take part?
* It’s a complicated topic, but we can return to Bitcoin as an example of decentralized blockchain security. **The Bitcoin blockchain uses a combination of cryptography and a network consensus mechanism called** [**Proof of Work (PoW)**](https://academy.binance.com/en/articles/proof-of-work-explained).
* In terms of cryptography, each block has a kind of digital signature (or [hash](https://academy.binance.com/en/glossary/hash)). Each block of data is connected in a way that can’t be tampered with because any changes would alter a block’s hash. Any attempt to change the data would be quickly identified by the rest of the network.
* **The PoW consensus mechanism is another part of the puzzle. It helps secure the cryptocurrency’s ledger**. Understanding Proof of Work is a whole article in itself, but for our purposes, note that **members of the network can only verify new transactions and add them to the ledger through an activity known as** [**mining**](https://academy.binance.com/en/glossary/mining)**.** This involves using computational power to solve a mathematical puzzle. Part of the process requires these computers to perform numerous hashing functions. This plays into the issue of scalability, as **the PoW mechanism is secure but relatively slow**.
* Also note that the more participants (nodes) there are in the network, the more secure it is. **The greater the number of parties, the harder it becomes for one bad actor to take control of the system**. This relates to what is known as the [51% attack](https://academy.binance.com/en/articles/what-is-a-51-percent-attack). As an overview: if a single entity (or group of bad actors) can control more than 50% of a blockchain’s total network hashing rate, then they would be able to override consensus and change the chain’s data to benefit themselves, such as [double spending](https://academy.binance.com/en/glossary/double-spending) tokens.

***In short, security is a fundamental requirement for a blockchain to be successful because, without it, attackers can take control of the chain, rendering it useless.***

## What is scalability?

* Scalability refers to the goal of building a blockchain that **can support more and more transactions per second**.
* **Scale is required if blockchain tech is to serve wider society and possibly billions of users. But this is where a lot of blockchains still struggle.**
* This is **because decentralization and security are so fundamental to blockchain that they tend to be focused on first**. However, by prioritizing decentralization and security, scalability becomes a challenge.
* The number of transactions a chain can handle can be severely limited. A centralized payment system such as Visa states that it’s able to support 24,000 transactions per second. This is because the network is closed, and free from considerations such as public nodes and consensus. Compare this with some of the best-known blockchains.
* According to Bloomberg in 2022: “As of September, Bitcoin was unable to handle more than seven transactions per second and Ethereum, the second-most popular network, was limited to about 15 per second — a lifetime compared to conventional exchanges.”
* As mentioned, these **blockchain transaction speeds are limited due to the way the information needs to be processed by the different participants that make up the decentralized network, and the nature of the PoW consensus mechanism itself.** If more and more people in society begin to use blockchain technology, the networks will become jammed due to the limited number of transactions they can handle.

## Why the blockchain trilemma exists

* The most obvious and basic solution to the problem outlined above is to **reduce the number of participants confirming and adding to the network data in exchange for greater scale and speed.** But doing so **would lead to a weakening of decentralization with control handed to a smaller number of participants**. And it **would also lead to a weakening of security as fewer players means a higher chance of attacks.**
* So here lies the trilemma: given the **connection between the desired properties of decentralization and security, the fundamental design of how blockchain works makes it hard to scale**. Increase one, and you weaken another. How do you push scalability without damaging decentralization, security, or both?

## Solving the blockchain trilemma

There is **no one golden solution to the trilemma**. But given the importance of solving this problem, there have been **several different approaches** within the community with interesting results. Let’s run through an overview of some of the most popular developments to give you an understanding of what’s happening in the space:

### **1. Sharding**

* This is a method of **splitting** [**blockchains**](https://academy.binance.com/en/articles/what-is-blockchain-technology-a-comprehensive-guide-for-beginners) (or other types of databases) **into smaller, partitioned blockchains that manage specific data segments**. This setup takes the stress off a single chain dealing with all transactions and interactions on a network.
* **Each partitioned blockchain is known as a shard and has its specific** [**ledger**](https://academy.binance.com/en/glossary/ledger#:~:text=A%20ledger%20may%20be%20defined,in%20the%20form%20of%20credits.). These shards can then process their own transactions, but a beacon blockchain or main chain manages interactions between shards. This makes sharding a [Layer 1 network scalability upgrade](https://academy.binance.com/en/articles/blockchain-layer-1-vs-layer-2-scaling-solutions), as it’s a change to the mainnet of a blockchain.

### **2. Different consensus mechanism**

* **One of the reasons the trilemma exists in the Bitcoin network is because of the way PoW works to ensure security**. The need for miners, crypto algorithms, and huge amounts of decentralized computing power leads to a secure system, but a slow one.
* **Finding a different way to secure consensus is one approach to solving the trilemma.** This was one of the reasons behind Ethereum's move from PoW to [Proof of Stake](https://academy.binance.com/en/articles/proof-of-stake-explained) (PoS).
* **In PoS blockchains**, **participants involved in validating transactions must stake (lock) their tokens**. There’s no need for highly specialized mining machines. Adding more validators to the network is simpler and more accessible. PoS is just one of many different approaches to consensus mechanisms with scalability in mind.

### **3. Layer-2 solutions**

* Both **sharding and different consensus mechanisms are what are known as Layer-1 solutions**. They look to change the fundamental design of the underlying network. But other developers seeking to solve the trilemma have been working on solutions that build on top of an existing network structure. In other words, they think the answer lies in a second layer, or Layer 2. Examples of this include [sidechains and state channels](https://academy.binance.com/en/articles/blockchain-scalability-sidechains-and-payment-channels).
* **A sidechain is basically a separate blockchain connected to the main chain**. It’s set up in a way that assets can flow freely between the two. Importantly, **the sidechain can operate under different rules, allowing for greater speed and scale**.
* Similarly, state channels are another way of taking transactions off the main chain and easing pressure on [Layer 1](https://academy.binance.com/en/articles/what-is-layer-1-in-blockchain). **A state channel uses a smart contract**, rather than a separate chain, **to enable users to interact with each other without publishing their transactions to the blockchain. The blockchain only records the start and end of the channel.**