Introduction

Blockchain @ uninsubria

Roberto Vicario

2024/2025

Contents

1 Blockchain

Blockchain is a special kind of database that stores information in a chain of blocks. Each block contains a list of transactions, and these blocks are linked together in the order they were added like a digital ledger.

1.1 Key Components

Component	Description
Transaction	A record of an action or event, like sending money.
Block	A container for a list of transactions.
Chain	A series of blocks linked together.

> **Definition:** *Genesis Block* is the first block in a blockchain and serves as the foundation of the chain. It is unique because it has no previous block, and its previous_hash is set to zero. This block is crucial for establishing the integrity and immutability of the blockchain.

> **Definition:** The process of creating a new block and adding it to the blockchain is called *Mining*. In a real-world blockchain, this process involves solving complex mathematical problems to validate transactions and secure the network.

2 Decentralization

Decentralization means that control and decision-making aren't held by a single entity, like a company or government. Instead, power is distributed across a network of independent participants.

2.1 The Consensus Problem

In decentralized systems, no single person or computer is in charge, so how do all the independent nodes agree on what's true? That's the *Consensus Problem*:

> **Problem:** *How can a group of participants, who don't fully trust each other, agree on a single version of the truth?*

2.2 State Machine Replication (SMR)

```
# TODO
```

• A Blockchain is a replicated, write-only ledger that has very peculiar safety and liveness properties • Safety: the copies of the ledger stay in sync • Liveness: when something new information arrives, it is (eventually) written on the ledger

The blockchain stack • Layer 0 (the Internet): • Semi-reliable, point-to-point communication • Layer 1 (Consensus layer): • Keep in sync many independent machine across the globe • More general Blockchains: Consensus + Compute • Layer 2 (Scaling layer): • Exports the same same functionalities of L1 • Executes much more of them than L1 • Layer 3 (Application layer): • Exchanges (e.g. Uniswap) • NFT marketplaces (e.g. Opensea)