# Peer to Peer Systems
# Master Degree in Computer Science and Computer Science and Networking
# 6 CFU

## Objectives of the Course

This course introduces the basic principles and tools to define and develop a peer to peer (P2P) system, with a focus on Distributed Hash Tables and the distributed technology of blockchains and on the cryptocurencies.

The first part of the course introduces the general concepts underlying any P2P system (topology, information diffusion,...). This part also present several case studies (Bittorrent, the KAD network,..).

Cryptocurrencies and, more in general, blockchains, are a recent "killer application" in the area of P2P systems. The second part of the course presents and discusses the blockchain technology and the decentralized digital currencies (cryptocurrencies) such as Bitcoin. The course introduces both the theory and principles at the basis of cryptocurrencies operations and practical examples of their use. This part introduces the cryptocurrency ecosystem and discusses the existing and potential interaction of cryptocurrencies with the banking, financial, legal and regulatory environment. Lastly the course details how innovative applications exploit blockchain technology

## Syllabus

- **P2P Topologies**
  - Peer to Peer (P2P) systems: general concepts
  - Unstructured Overlays: Flooding, Random Walks, Epidemic Diffusion
  - Structured Overlays: Distributed Hash Tables (DHT), Routing on a DHT
  - Case Studies:
    - Bittorrent as a Content Distribution Network: KAD implementation of the Kademlia DHT, game-based cooperation
- **Complex Network for the analysis of P2P systems**
  - Network models
    - Random Graphs and Small Worlds
    - Small World navigability: Watts Strogatz and Kleinberg.
    - Complex networks navigability
- **Cryptocurrencies and Blockchains**
  - basic concepts:

    - review of basic cryptographic tools (digital signatures, cryptographic hash, Merkle trees.,..)
    - blockchains: definitions
    - distributed consensus: definitions
- the Bitcoin blockchains
    - Nakamoto consensus
    - Bitcoin mining mechanism
    - pseudoanonymity: traceability and mixing
    - the Bitcoin P2P Network
    - Bitcoin ecosystem
    - scalability issues
    - Bitcoin Extensions/alternatives: altcoins, sidechains, the StellarConsensus Protocol
- Applications of blockchains
    - Ethereum: programming smart contracts
    - Blockchain 1.0: cryptocurrencies
    - Blockchain 2.0: financial instruments built on cryptocurrencies
    - Blockchain 3.0: applications beyond cryptocurrencies (DNS, lotteries, voting, IoT...)