Peer to Peer Network

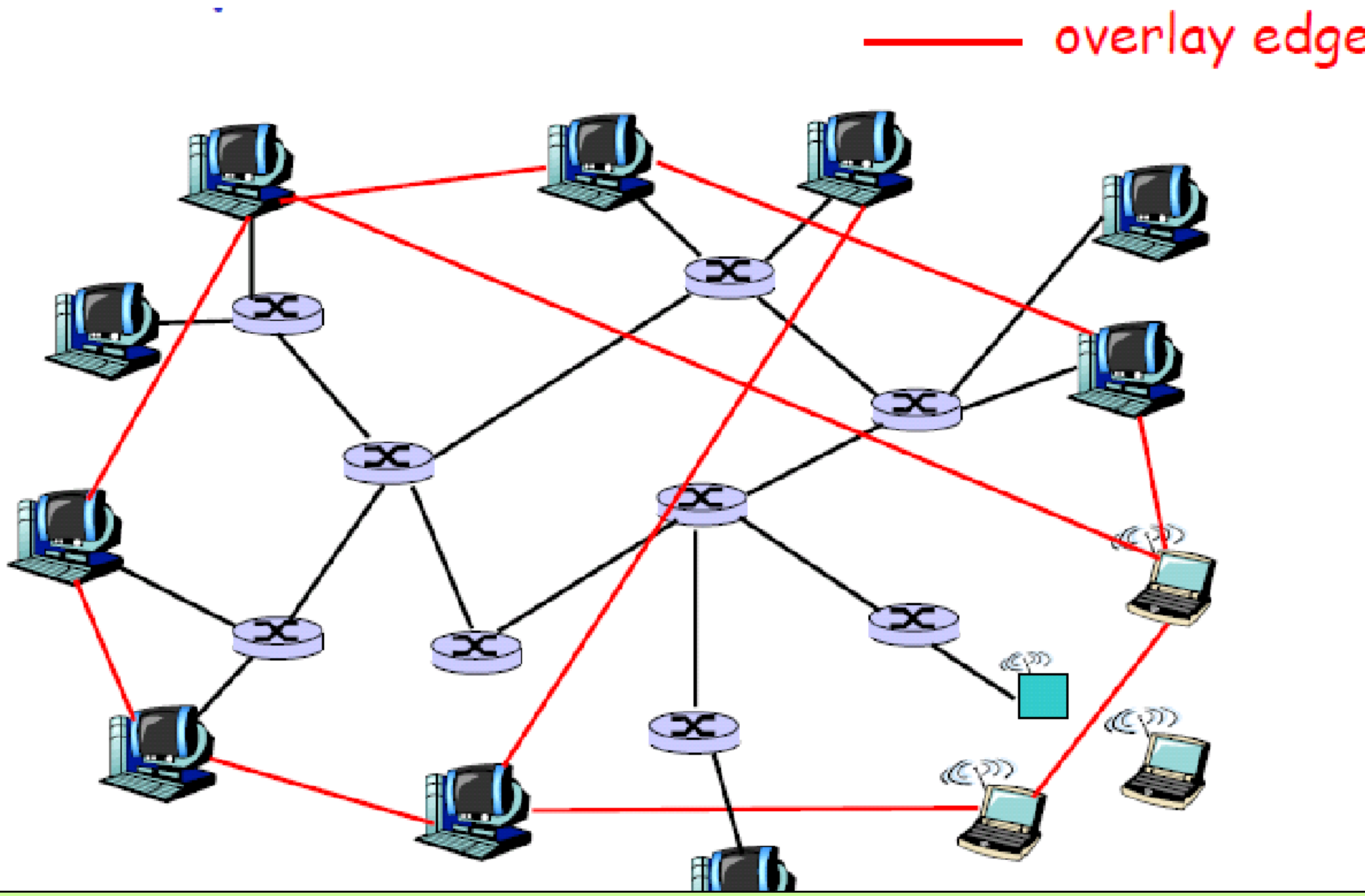
Peer to Peer (P2P) System Overview

- Significantly autonomous from a centralized authority.
  - Each node can act as a Client as well as a Server.
- Use the vast resources of machines at the edge of the internet.
  - Storage, content, CPU power, Human presence.
- Resources at edge have intermittent connectivity, being added & removed.
  - Infrastructure is untrusted and the components are unreliable.

P2P properties

- Massive scalability
- Autonomy : non single point of failure
- Resilience to Denial of Service
- Load distribution
- Resistance to censorship

Overlay Network



A P2P network is an **overlay network**. Each link between peers consists of one or more IP links.

Overlay Graph (continue)

- Virtual edge
  - TCP connection
  - or simply a pointer to an IP address
- Overlay maintenance
  - Periodically ping to make sure neighbor is still alive
  - Or verify aliveness while messaging
  - If neighbor goes down, may want to establish new edge
  - Could be a challenge under high churn rate

Setup P2P Network

- Gather the necessary resources like two computers connected the same network.
- Install P2P software like Downloa56ude BitTorrent, eMule, and Limewire.
- Configure firewall settings to allow P2P traffic
- Connect to the P2P network
- Share files
- Test and troubleshoot (if required)

Distributed Network

Overview

- Collection of multiple nodes,
- Independently run networks that are collectively managed
- Every participant can communicate with one another without going through a centralized point
- **Importance**
  - Provide better reliability
  - Multiple entry points
  - Centralized management and monitoring
  - Uniform policy across the network infrastructure

Types of Distributed Network

- Client-Server: a central server providing services to multiple clients
- Peer-to-Peer: each device can act as both client and server
- Hybrid: combination of client-server and peer-to-peer

Use Cases of Distributed Network

- Secure Access Service Edge (SASE)
- Globally distributed SaaS architectures
- Growing in popularity due to remote workforces
- Provides network security services for all business traffic flows
- Redirects users to alternative head-end locations
- Edge computing for IoT
- Low-latency network access for collection and analysis of IoT data
- Multiple edge compute nodes are required

Distributed Network Application

- File sharing: allows multiple users to access and share files over the network
- Cloud computing: allows users to access and store data remotely
- Streaming services: deliver audio and video content in real-time
- Online gaming: allows multiple players to play together in a virtual environment

Hardware Used in Distributed Network

- Computers: Desktop computers, laptops, and servers
- Smartphones: Many distributed networks, such as blockchain networks, allow users to participate using their smartphones
- Internet of Things (IoT) devices: Distributed networks can also be run on small devices like sensors and smart home appliances
- Cloud servers: Distributed networks can also be run on servers located in data centers, which are connected to the Internet and can be accessed remotely.

Distributed Network Architecture

- Components of a distributed network: multiple networks, communication protocols, routing algorithms
- Communication protocols: responsible for transmitting data between the different networks
- Routing algorithms: determine the most efficient path for data to travel through the network
- Distributed systems all nodes have to trust each others or at least trust a "master" node, where as P2P systems doesn't assume trust between nodes

Distributed Network Architecture

- Components of a distributed network: multiple networks, communication protocols, routing algorithms
- Communication protocols: responsible for transmitting data between the different networks
- Routing algorithms: determine the most efficient path for data to travel through the network

Consensus Algorithm

PoW (Proof of Work)

Consensus algorithm used to **secure and validate transactions** on a blockchain network. The idea behind PoW is that it requires network participants, known as "**miners**", to solve complex mathematical problems in order to add new blocks to the blockchain. The process of solving these problems is known as "**mining**".

PoW (Continue)

- Very secure and resistant to malicious actors
- Quite energy-intensive
- May not be the best solution for all types of networks
- Algorithm is designed to be computationally expensive and time-consuming, making it difficult for a malicious actor to control a majority of the network's computing power and manipulate the blockchain.

How PoW Works

- A new transaction is broadcasted to the network and added to a pool of unconfirmed transactions, known as the "mempool".
- Miners take the transactions from the mempool and group them into a block.
- The miner must then solve a complex mathematical problem, known as a "hash puzzle", that is specific to the current block. This puzzle is designed to be difficult to solve, but easy to verify.
- Once a miner solves the puzzle, they broadcast their solution (known as the "nonce") to the network.
- Other miners will then verify the solution and, if it is valid, add the block to the blockchain. The miner who solved the puzzle is rewarded with a certain amount of cryptocurrency for their efforts.
- The new block is added to the blockchain and the transactions in it are considered confirmed.

PoS (Proof of Stake)

Consensus algorithm used to secure and validate transactions on a blockchain network. Instead of using computational power to validate transactions, PoS **uses the amount of cryptocurrency held by network participants**, known as "validators", to determine who is eligible to add new blocks to the blockchain.

PoS (Continue)

- Designed to be more energy-efficient than PoW, as it doesn't require computational power to validate transactions.
- Incentivizes validators to have a stake in the network, as it is in their best interest to keep the network secure.
- More vulnerable to a situation called a "nothing at stake" problem, where validators can validate multiple blocks at the same time which can lead to forks

How PoS Works

- When a new transaction is initiated, it is broadcasted to the network and added to a pool of unconfirmed transactions, known as the "mempool".
- Validators, who have a certain amount of cryptocurrency "staked" as collateral, are chosen to create a new block. The selection process is based on the validator's stake and sometimes additional factors like randomization.
- The chosen validator then adds the transactions from the mempool to a new block and broadcasts it to the network.
- Other validators verify the block and, if it is valid, add it to the blockchain. The validator who created the block is rewarded with a certain amount of cryptocurrency for their efforts.
- The new block is added to the blockchain and the transactions in it are considered confirmed.

PoA (Proof of Authority)

Consensus algorithm used to secure and validate transactions on a blockchain network. It is similar to Proof of Stake (PoS) in that it uses a set of **designated network participants**, known as "validators" or "authorities", to validate transactions and add new blocks to the blockchain. However, unlike PoS, the validators are **known and pre-approved identities**, rather than chosen based on the amount of cryptocurrency they hold.

PoA (Continue)

- Designed for private or consortium blockchain where the identity of the validators is known and controlled by a specific entity or group.
- Can provide a higher level of security and trust, as the validators are known entities that can be held accountable.
- Also less decentralized and may not be suitable for certain use cases, such as public blockchains.

How PoA Works

- When a new transaction is initiated, it is broadcasted to the network and added to a pool of unconfirmed transactions, known as the "mempool".
- The designated validators, who have been pre-approved and vetted by the network, are chosen to create new blocks.
- The chosen validator then adds the transactions from the mempool to a new block and broadcasts it to the network.
- Other validators verify the block and, if it is valid, add it to the blockchain. The validator who created the block is rewarded with a certain amount of cryptocurrency for their efforts.
- The new block is added to the blockchain and the transactions in it are considered confirmed.

Comparing PoW, PoS, PoA

Consensus Algorithm	Proof of Work (PoW)	Proof of Stake (PoS)	Proof of Authority (PoA)
How it works	Miners solve complex mathematical problems to add new blocks to the blockchain	Validators are chosen based on the amount of cryptocurrency they hold to add new blocks to the blockchain	Validators are pre-approved identities to add new blocks to the blockchain
Security	High	High	High
Decentralization	High	Medium	Low
Energy consumption	High	Low	Low
Environmental Impact	High	Low	Low
Scalability	Medium	High	High
Use cases	Public blockchains	Public & Private blockchains	Private & Consortium blockchains