Deep into Blockchain Series

Cryptography & Peer2 Peer Networks

Presenter(s): Founding Team

Event Organizers

dcentrum Community

Connect | Collaborate | Create

Venue Sponsor

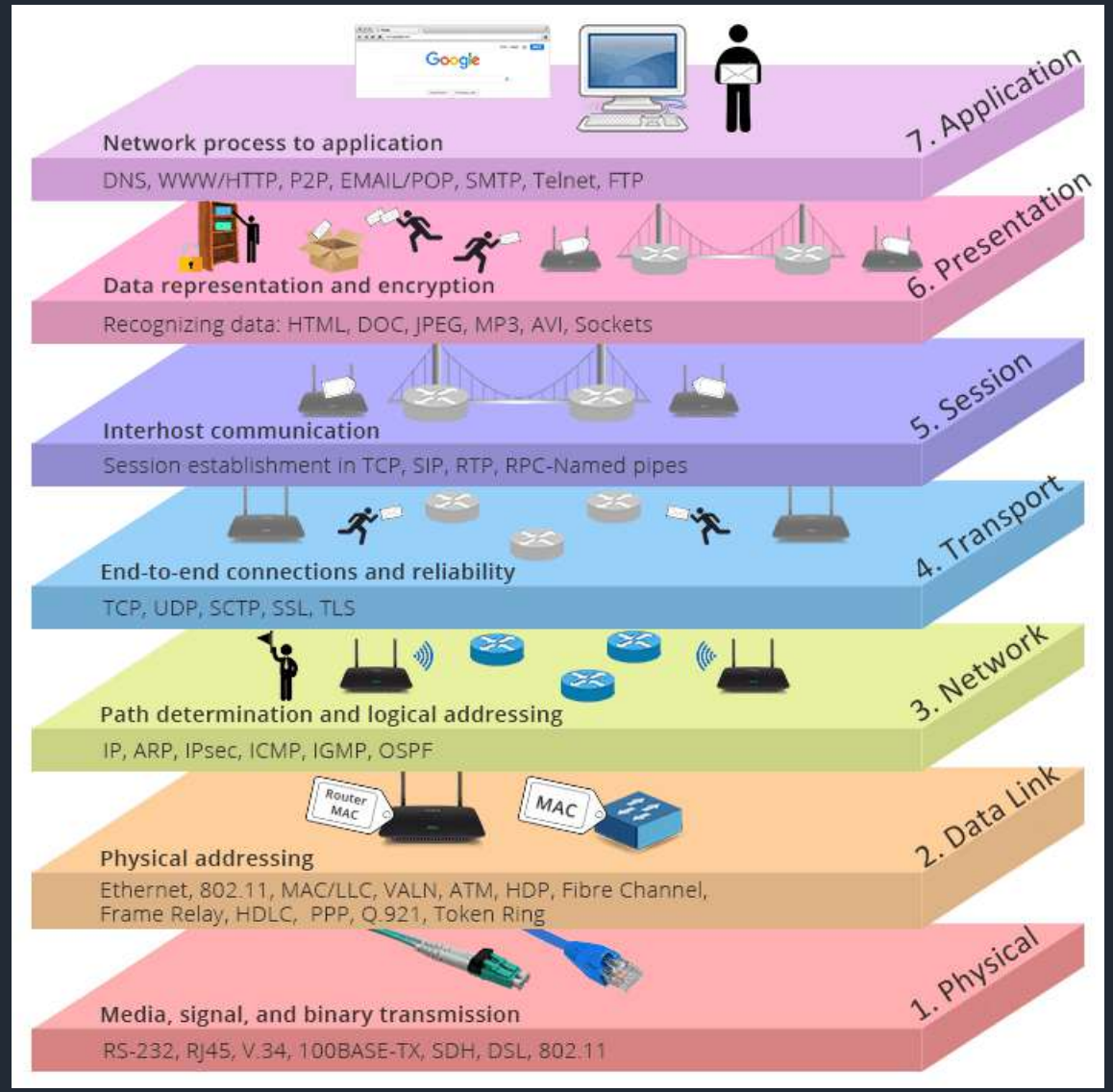
nagarro

Peer2Peer Networks Agenda

- OSI – 7 Primary Layers of Network
- Distributed Systems – Properties, Considerations and Constraints
- Peer2Peer Networks
  - Distributed Hash Tables
    - Kademlia
  - Gossip
- Code walkthrough of some of the implementations

OSI – Open Systems Interconnection Model

Layer	Protocol	Data Protocol Unit	Addressing
Application	HTTP,SMTP	Messages	N/A
Transport	UDP / TCP	Segments	Port #
Network	IP	Datagrams	IP Address
Datalink	Ethernet, WiFi	Frames	MAC Address
Physical	10BaseT, 802.11	Bits	N/A



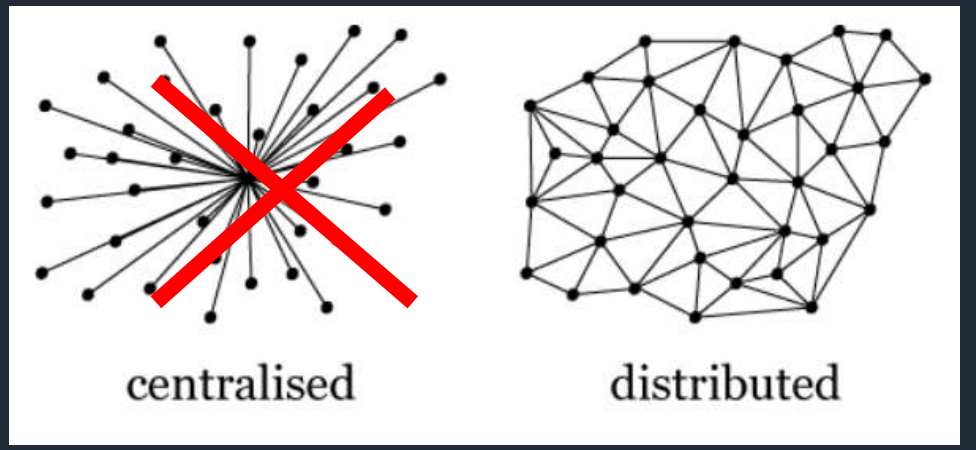
Distributed Systems

What is a Distributed System?

Distributed Systems are a set of independent nodes (processes) connected via channels for information to move between the nodes, establishing a network

Purpose:

To achieve a common goal and avoid a single point of failure.



Distributed Systems: Characteristics & Constraints

Basic Characteristics:

- ❑ Autonomous
- ❑ Asynchronous
- ❑ Failure Prone

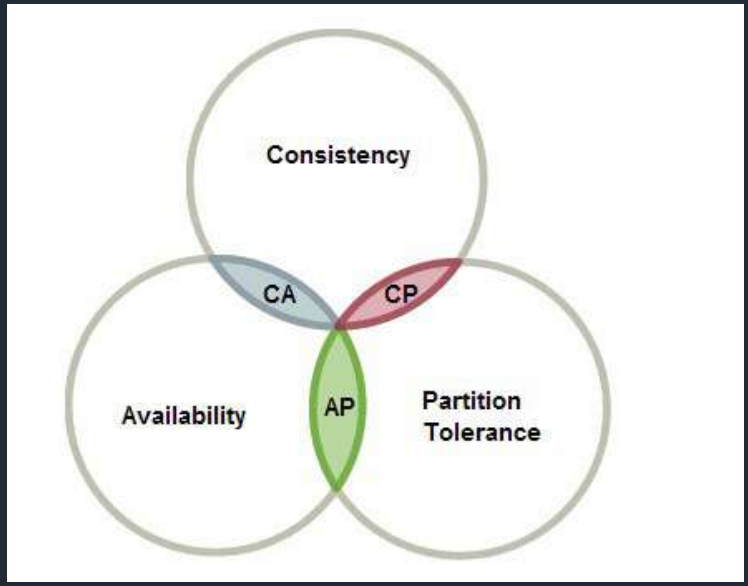
Constraints:

- ❑ CAP Theorem

CONSISTENCY – AVAILABILITY – PARTITION NETWORK

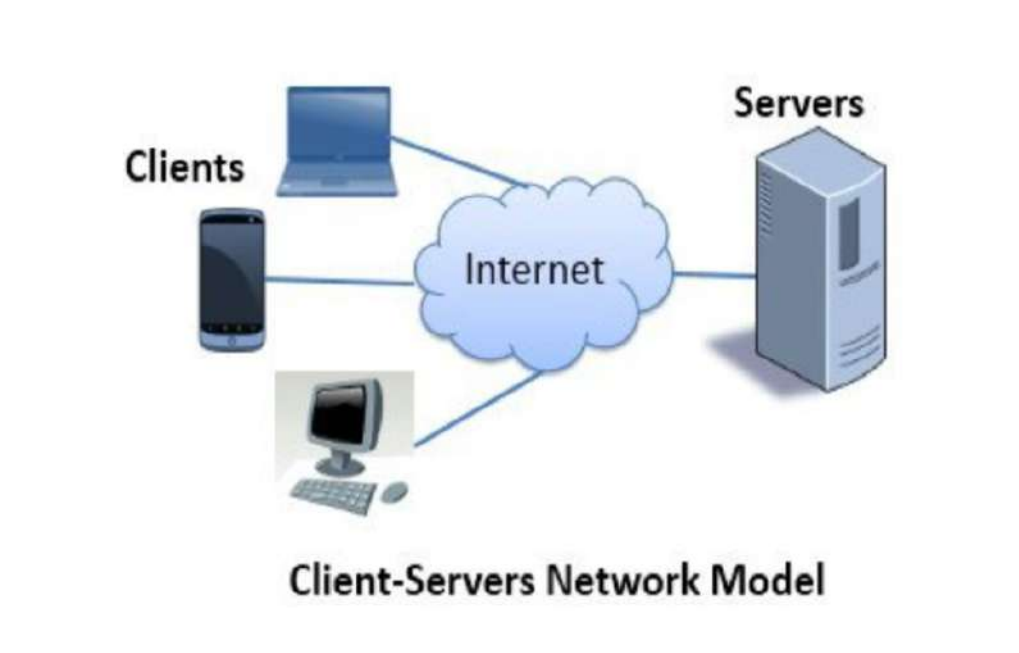
- ❑ FLP Theorem

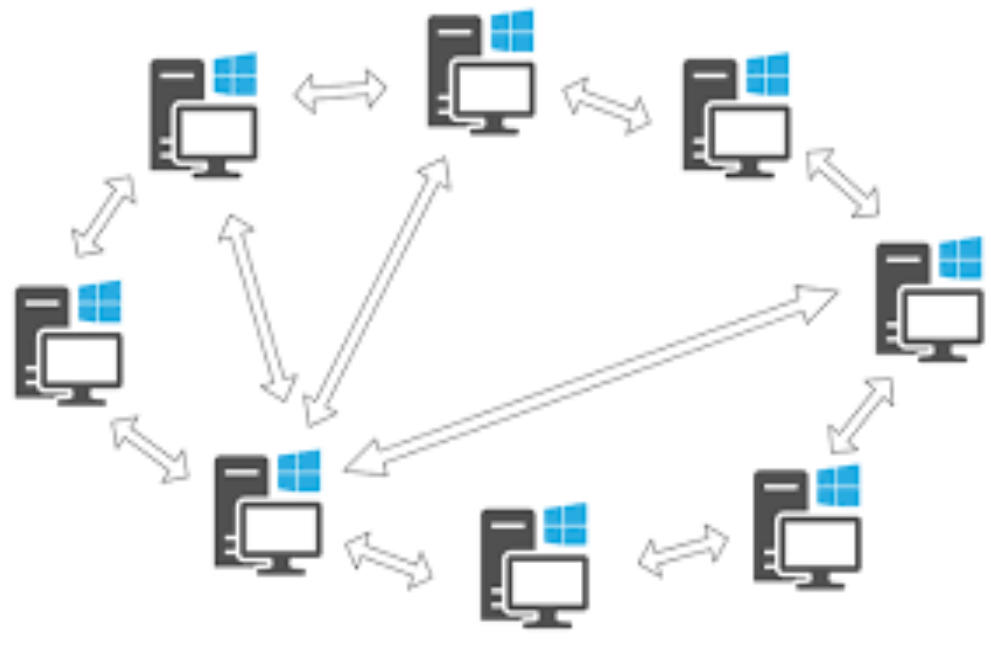
”In a purely distributed system, the consensus problem is impossible(with a deterministic solution) to solve if in a presence of a single crash failure”



Peer-To-Peer Networks

Peer-To-Peer Network is a network of computer systems known as peers or nodes connected to each other to store and share the content like messages, files or a stream of media etc. or to perform a most common computational work as well.

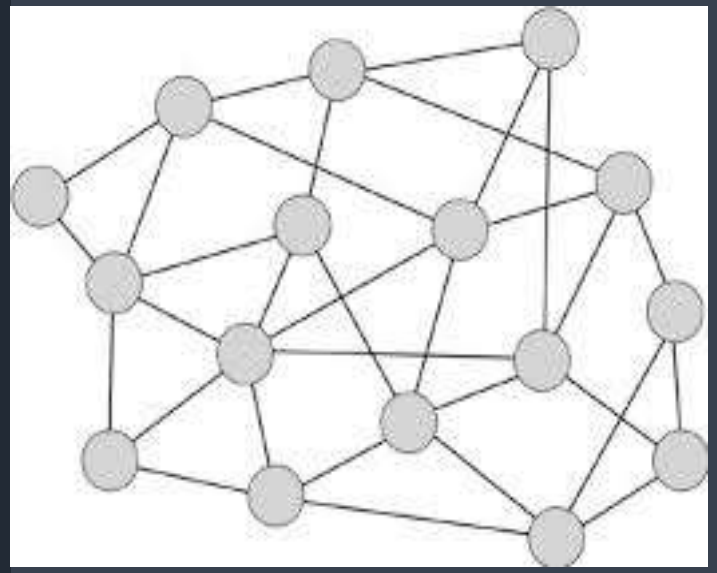




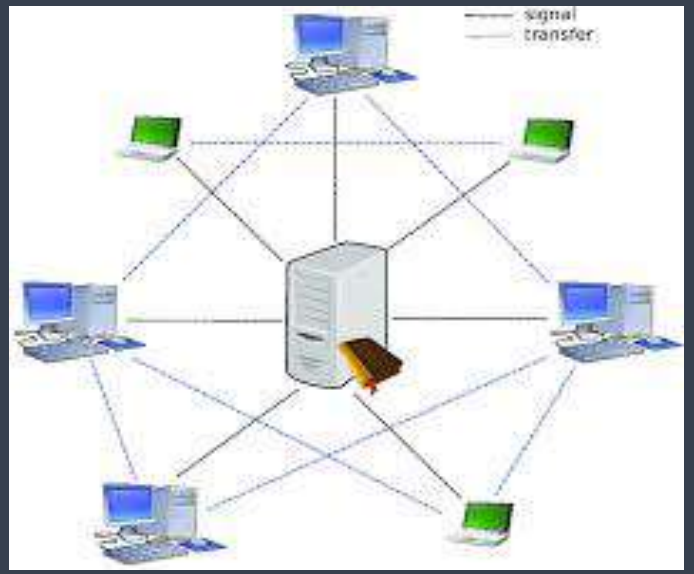
Peer-To-Peer Networks - Type

P2P Networks are three types in terms of how they maintain peer discovery and content management

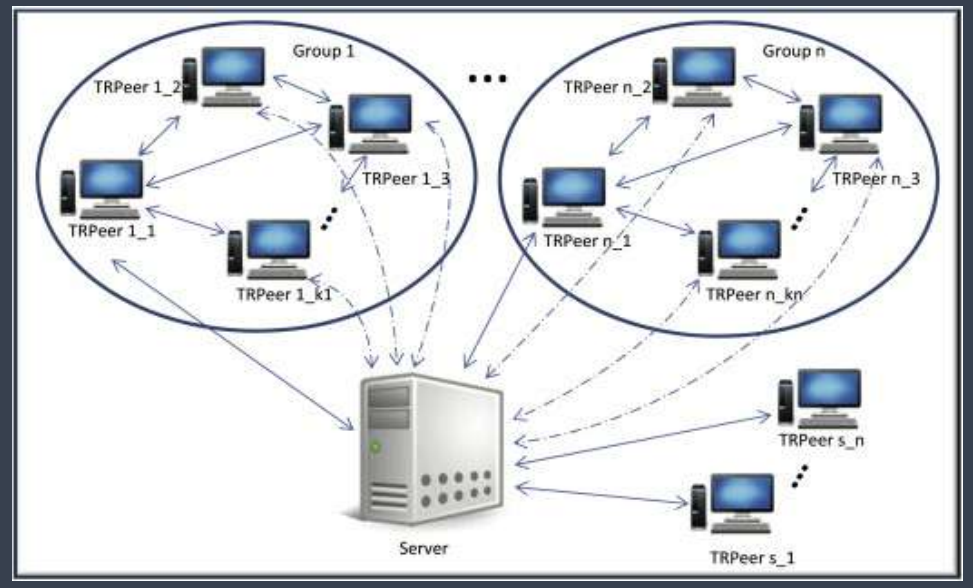
Pure P2P



Centralized P2P

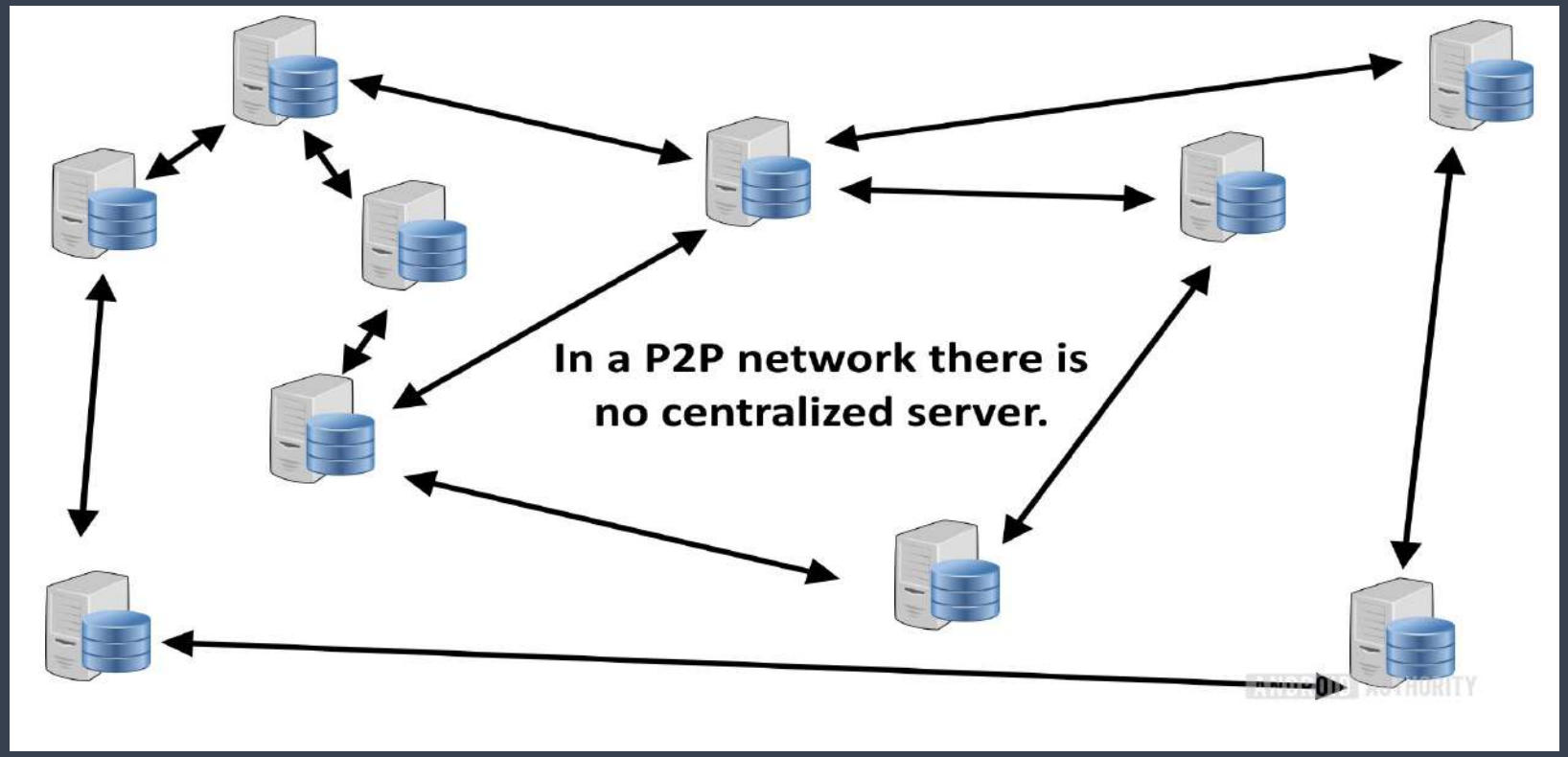


Hybrid P2P



Peer-To-Peer – Why in Blockchain / DLTs

Blockchain or DLT platforms depends on p2p networks , because these platforms store data, share data and execute smart contracts or script in decentralized manner to achieve the decentralization of computing & data.



Peer-To-Peer Networks - Functions

- Peer Discovery – Every peer to discover other peers
- Execute the business logic – Execute smart contracts
- Exchange of data – Exchange of membership of nodes and Network active status
- Synchronize the data – Synchronize of ledgers

Peer-To-Peer Networks – Peer Discovery

A new peer will join the network with initial endpoint information

Platform	Nodes	Default nos	Who Maintains
Bitcoin	Hardcoded / DNA Seeds	8	Bitcoin community members
Ethereum	Bootstrapping nodes	3	maintained by Eth Foundation
IOTA	Neighbour Nodes	5	IOTA Foundation
Hyperledger	Endorsement / Orderers / Anchor Peers / Committing	Depends on no of Organizations	Channel Config
ipfs	bootstrap list	Around 10	

https://github.com/bitcoin/bitcoin/blob/d882f635898fe036ef7be6b30bac31d29ec03ae3/src/chainparams.cpp#L116

Peer-To-Peer Networks – Exchange of data

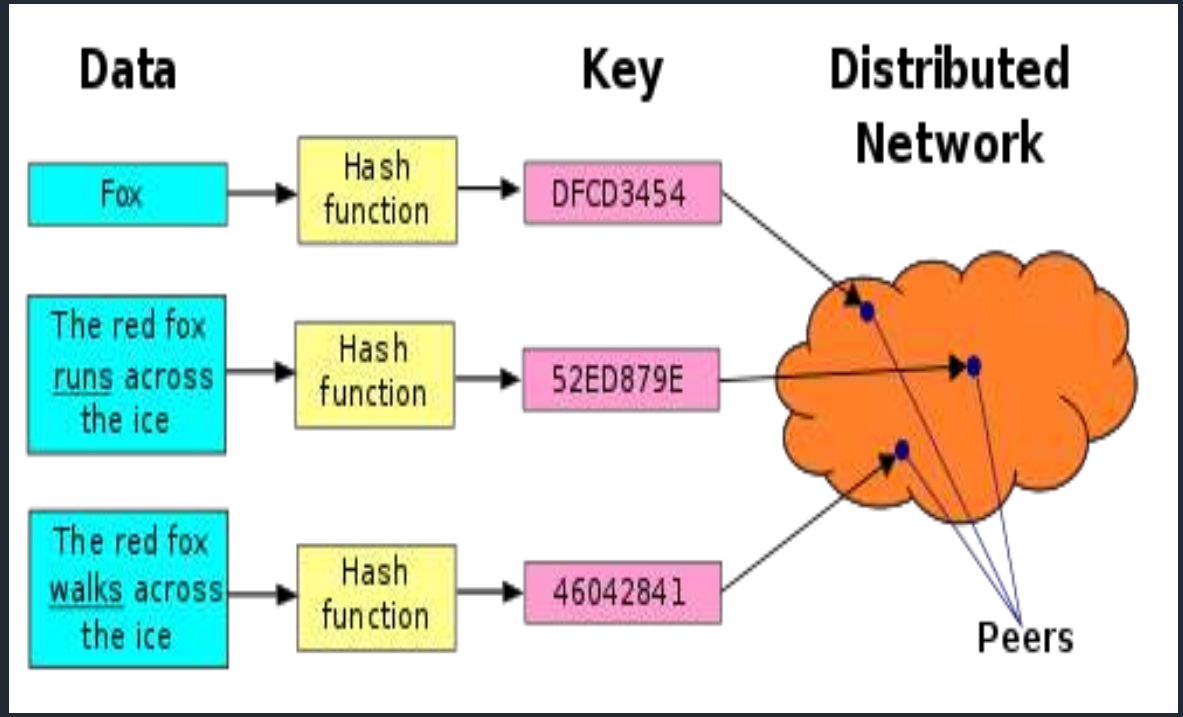
Peers communicate with other peers using different protocols for exchange of data.
Peers exchanges the meta data & latest ledgers.

Platform	Protocol
Bitcoin	TCP messages like by addr, version, getdata etc
Ethereum	RLNx, DevP2P
IOTA	Gossip
Hyperledger	Gossip
IPFS	DHT
StorJ	DHT

Peer-To-Peer – Kadamlia (DHT)

Kadamlia is one of the most popular algorithm based on Distributed Hash Tables.

1. Each peer has 160-bit NodeID
2. Each peer contains node lookup table
3. Peers communicate with UDP
4. It uses Routing table called k-buckets to store all node ids, IP addresses and ports
5. It prefers longest lived & short distant nodes
6. Communicates via UDP messages like Ping, FindNode, FindValue, Store etc.
7. Apps used: IPFS, Ethereum, StorJ etc.



Gossip Protocol

Gossip protocol is a communication layer between network peers on top of standard network protocols like TCP or UDP

1. Randomly picks some known peers and send its own new message received from other peers or
2. Application can configure this protocol to do messaging either with an interval based or on- no of transactions basis

3. Application can use this protocol for aggregations of Flooding messages.

Apps used: Hyperledger, IOTA, Cassandra, Dynamo

Gossip - Demo