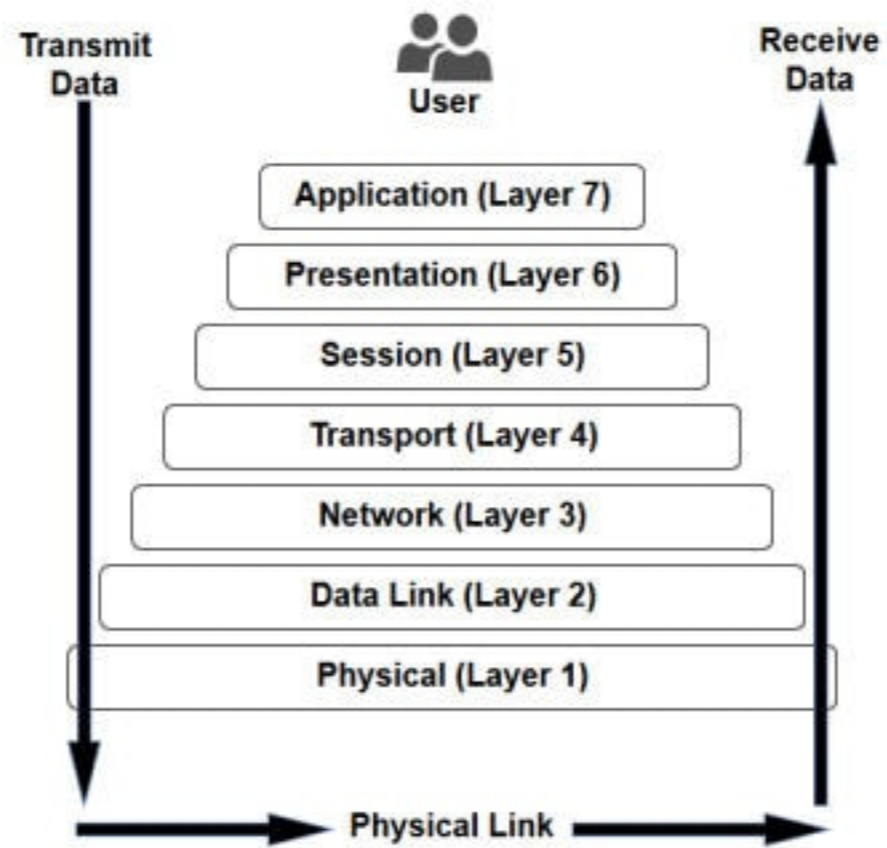


# Network Layer

October 2, 2019

# The 7 Layers of OSI



Layer 2: Protocol atop Layer 1  
(Lightning, Plasma, etc.)

Layer 1: Coin protocol (Bitcoin, Ethereum, etc.)

Layer 2: Protocol atop Layer 1  
(Lightning, Plasma, etc.)

Layer 1: Consensus (Bitcoin, Ethereum, etc.)

Layer 0: Networking

# Gossip Network

- Neighbors forward messages to other neighbors
- Used by almost all public blockchain protocols
- Security?

# P2P File Sharing (~2000)



Generation 1: Central server (Napster)

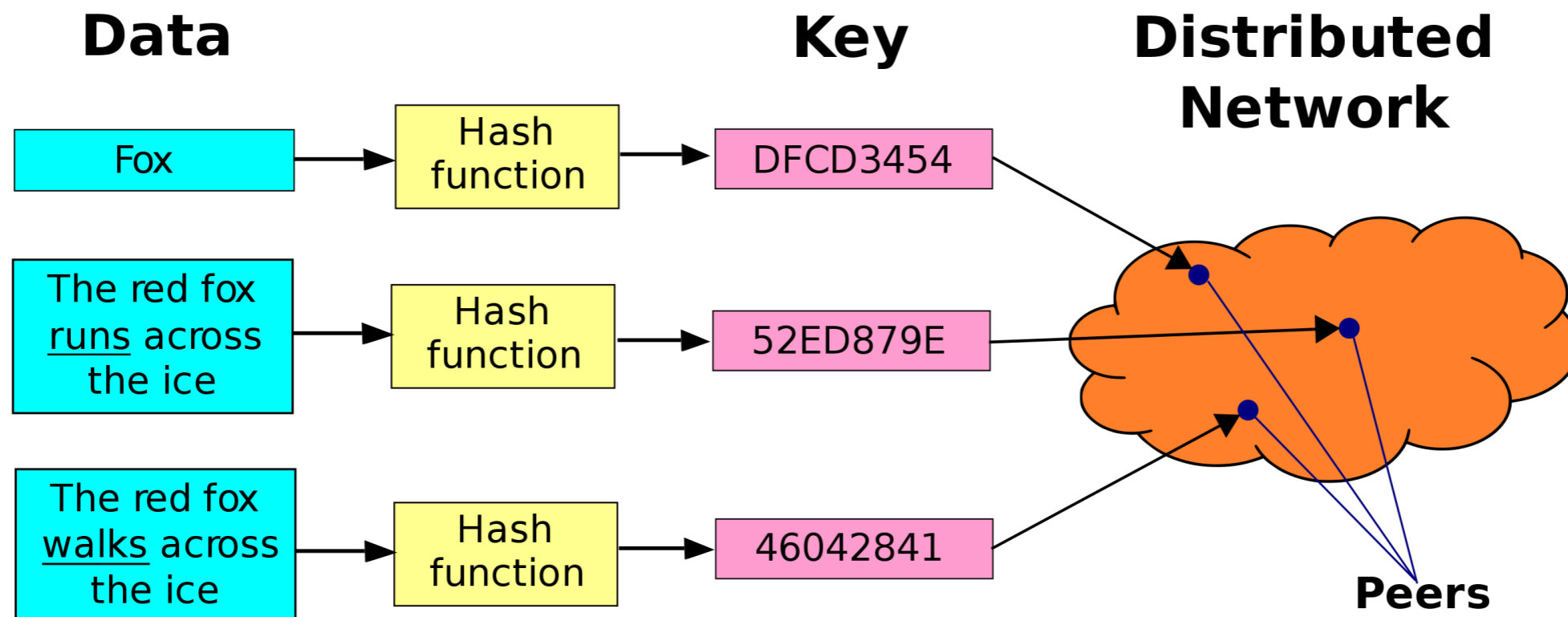


Generation 2: Flooding (Gnutella)

Then DHTs...

# Distributed Hashtables

- DHTs are hashtables, but the data is distributed. Any participating node should be able to efficiently retrieve the value for any key (even if it doesn't have it locally already)
- Purpose is to handle addressing over a large number of frequently changing nodes
- Useful for file addressing (in distributed file storage) or routing



# DHT Attributes to Consider

- Autonomy and decentralization
- Fault tolerance
- Scalability



# Kademlia

- Most widely used DHT
- Designed by Petar Maymounkov and David Mazières in 2002
- Each node has an ID and the distance between them is the xor of the IDs
- Each search brings you one bit closer
- Contact  $O(\log n)$  nodes (common for DHTs)
- Used by BitTorrent, Gnutella (which adopted it after earlier using flooding), Ethereum, IFPS, and much more

# Network Attacks

- How can you tell if a protocol is susceptible to a denial of service attack?
- What about network partitions?
  - What would happen if an undersea cable was cut?
- What can you do to mitigate?



# Final Projects

- Poster session and brief report
- Work alone or group of up to 3
  - All members of a group get the same grade
  - More expected from groups
- Choose something you find interesting
  - But ask for help if you struggle getting an idea
- You have many options
  - Implement a system, for example an interesting smart contract, a protocol, a game, a key management system, etc.
  - Conduct research, for example design an algorithm, design a protocol, benchmark existing systems, perform cryptographic analysis, write a specification, formally verify some open source code, etc.
  - Survey some area of technology
- Check your project ahead of time in office hours to verify appropriateness of scope