# Sybil Attacks

- Attacker attempts to fill the network with the clients under its control
  - Refuse to relay valid blocks
  - Relay only attacked blocks – can lead to double spending

- Solution:
  - Diversify the connections – Bitcoin allows outbound connection to one IP per /16 (a.b.0.0) IP address

# Denial of Service (DoS) Attacks

- Send lot of data to a node – they will not be able to process normal Bitcoin transactions

- Solutions:
  - No forwarding of orphaned blocks
  - No forwarding of double-spend transactions
  - No forwarding of same block or transactions
  - Disconnect a peer that sends *too many* messages
  - Restrict the block size to 1 MB
  - Limit the size of each script up to 10000 bytes
  - …

# The Monopoly Problem

- PoW depends on the computing resources available to a miner
  - Miners having more resources have more probability to complete the work

- Monopoly can increase over time (*Tragedy of the Commons*)
  - Miners will get less reward over time
  - Users will get discouraged to join as the miner
  - Few miners with large computing resources may get control over the network

# Handling Monopoly and Power Consumption - Proof of Stake (PoS)

- Possibly proposed in 2011 by a Member in Bitcoin Forum - https://bitcointalk.org/index.php?topic=27787.0
  - Make a transition from PoW to PoS when bitcoins are widely distributed

- PoW vs PoS
  - PoW: Probability of mining a block depends on the work done by the miner
  - PoS: Amount of bitcoin that the miner holds – Miner holding 1% of the Bitcoin can mine 1% of the PoS blocks.

# Proof of Stake (PoS)

- Provides increased protection

https://www.youtube.com/watch?v=M3EFi_POhps

  - Executing an attack is expensive, you need more Bitcoins
  - Reduced incentive for attack – the attacker needs to own a majority of bitcoins – an attack will have more affect on the attacker

- Variants of “stake”
  - Randomization in combination of the stake (*used in Nxt and BlackCoin*)
  - Coin-age: Number of coins multiplied by the number of days the coins have been held (*used in Peercoin*)

# Proof of Burn (PoB)

- Miners should show proof that they have *burned* some coins

  i.e. no one will be able to spend that coin

  - Sent them to a verifiably un-spendable address
  - Expensive just like PoW, but no external resources are used other than the burned coins

- PoW vs PoB – Real resource vs virtual/digital resource

- PoB works by burning PoW mined cryptocurrencies

# PoW vs PoS vs PoB

## PoW

- Do some work to mine a new block
- Consumes physical resources, like CPU power and time
- Power hungry

## PoS

- Acquire sufficient stake to mine a new block
- Consumes no external resource, but participate in transactions
- Power efficient

## PoB

- Burn some wealth to mine a new block
- Consumes virtual or digital resources, like the coins
- Power efficient

# Proof of Elapsed Time (PoET)

- Proposed by Intel, as a part of Hyperledger Sawtooth – a blockchain platform for building distributed ledger applications

- Basic idea:
  - Each participant in the blockchain network waits a random amount of time
  - The first participant to finish becomes the leader for the new block

# PoET over Trusted Environments

- How will one verify that the proposer has **really waited** for a **random amount of time?**
  - Utilize special CPU instruction set – *Intel Software Guard Extension* (SGX) – a trusted execution platform
  - The trusted code is private to the rest of the application
  - The specialized hardware provides an attestation that the trusted code has been set up correctly

i.e. complete hardware control