# Mining

## Network Attacks

Ira A. Fulton Schools of Engineering
Arizona State University

# Objectives

**Objective**

Explain how a 51% Attack works

**Objective**

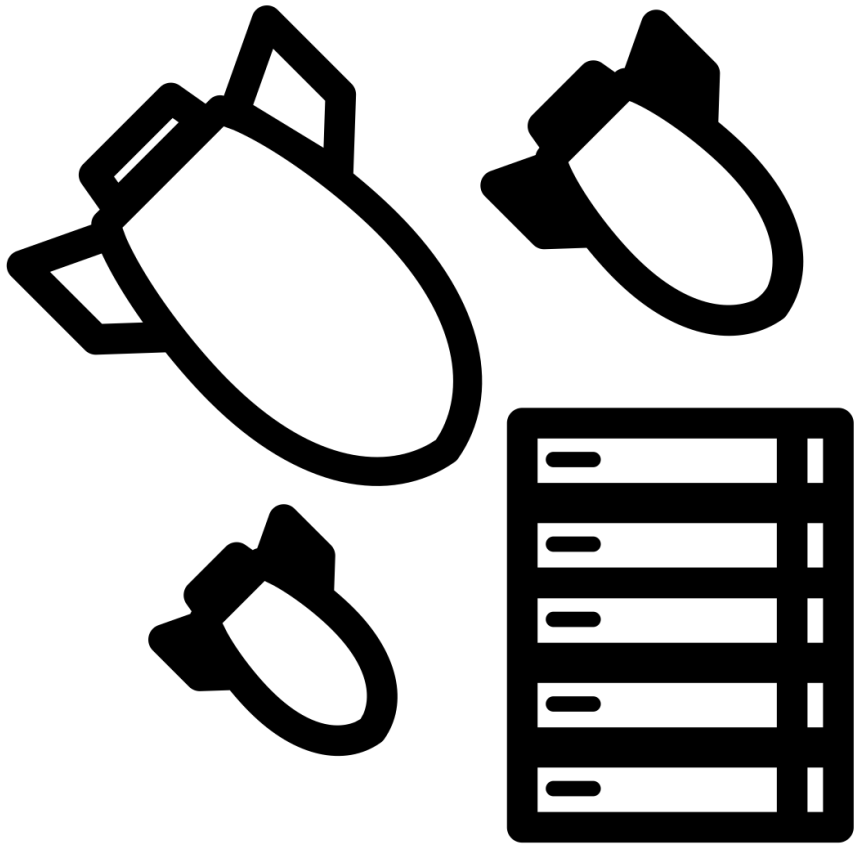
Explain how a Selfish Miner Attack works

**Objective**

Explain how a Social Attack works

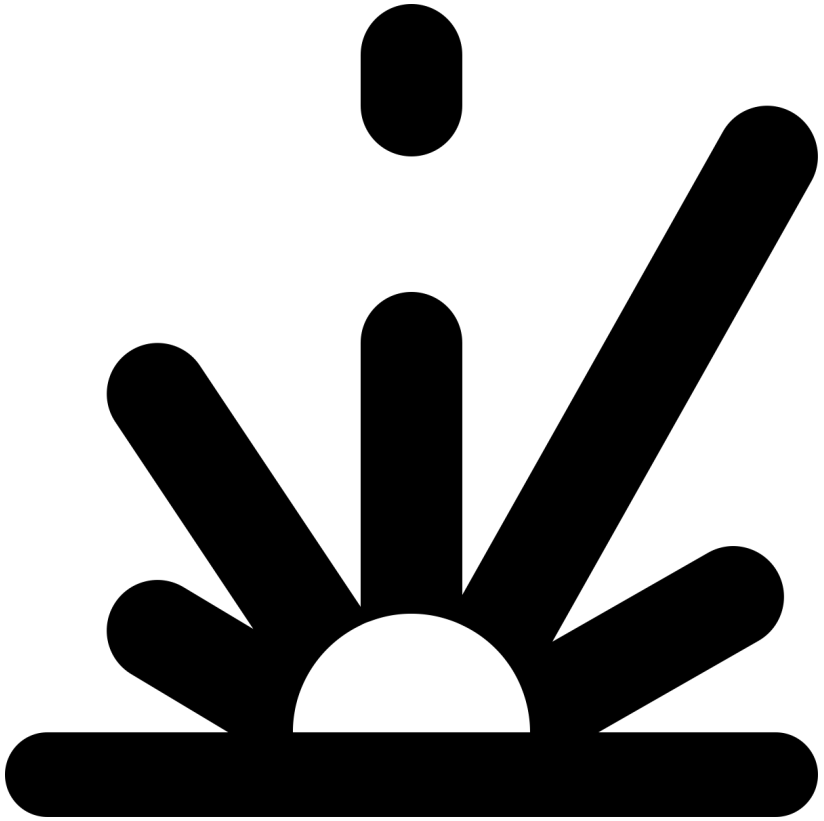
# 51% Attack

- Identified by Bitcoin whitepaper
- Requires one miner to have more than 50% of the network's hashing power
- Would require *a lot* of energy/financial resources
- More theoretical than practical
- Secretly produce a valid chain that would overrule an existing chain if published
- If published and accepted by nodes, can undo/reverse original transactions



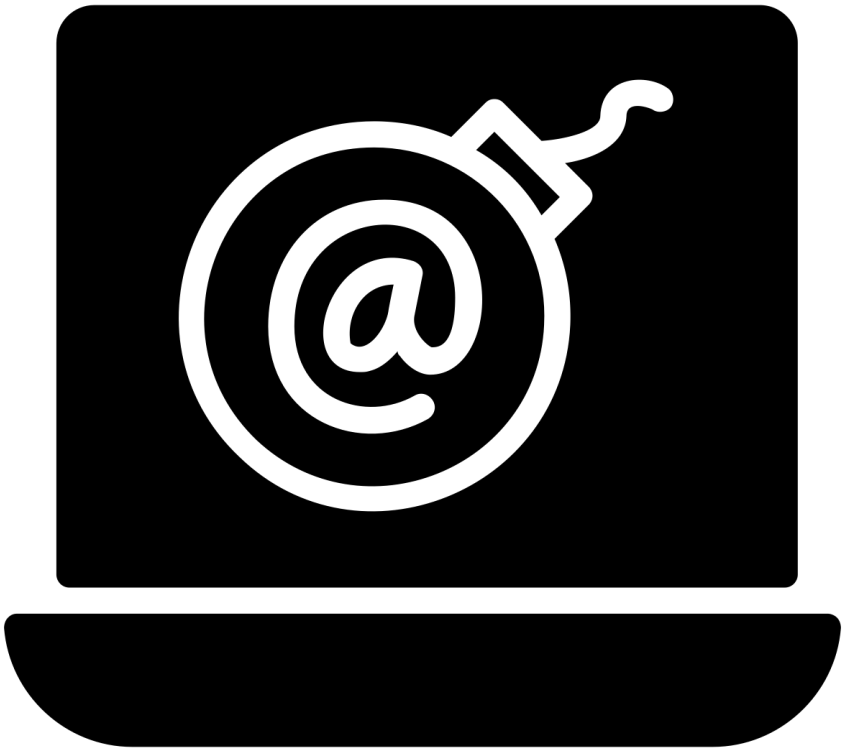
# Selfish Miner Attack

- Can be achieved when a miner has one-third (33%) or more of the hash power
- Requires gaming the network for increased rewards—e.g., mine a block but delay announcing it to the network
- Drives down other miners' profits
- One miner profiting more than expected may drive other miners off the network
- Fewer miners on the network can increase risk of a 51% Attack



# Social Attack

- Broad class of attacks
- For example, a website mimicking an official site that asks for user name and password
- Targets individual users



# Final Note

- Think about these attacks when designing a blockchain application
- Permissioned blockchains offer more security
  - Only allow certain actors
  - Do not rely on proof of work (provides energy savings)
  - Does not require the creation of new tokens
- 51% Attack almost impossible on a permissioned blockchain