Proof-of-Work Consensus Applied to the Byzantine Generals Problem

Ira A. Fulton Schools of Engineering
Arizona State University

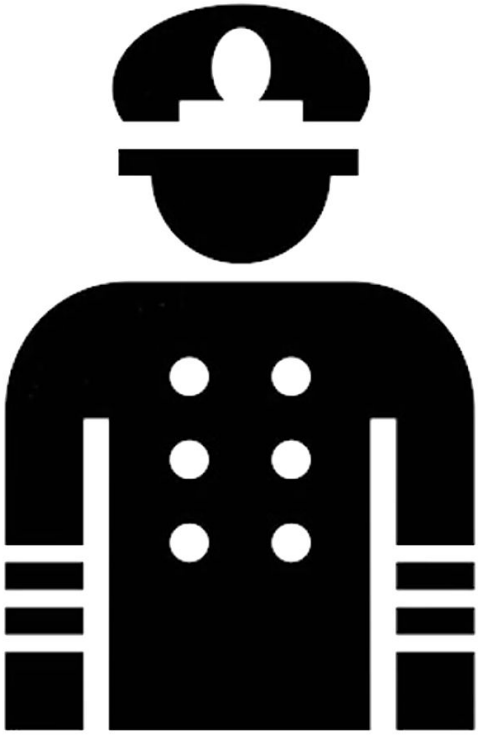
Objectives

Objective

Explain the importance of the Byzantine Generals Problem regarding consensus for blockchain networks

BGP - Recap (1/2)

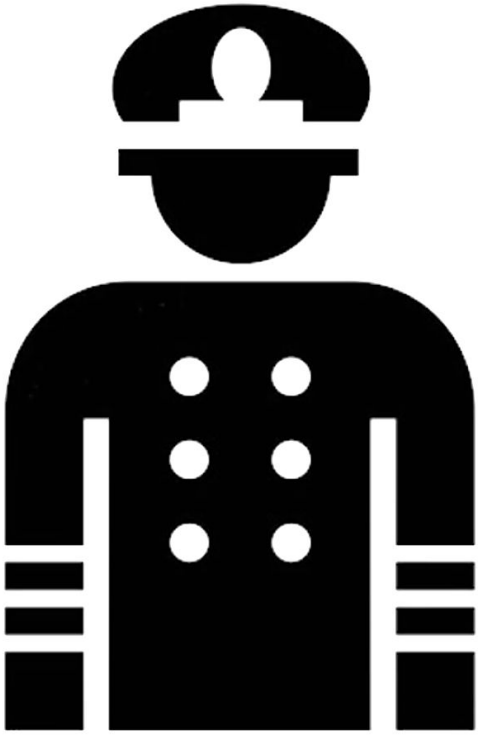
- Goal of finding an algorithm that…
  - allows a decentralized network to come to consensus
  - guarantees two properties
    1. All loyal general decide upon same plan of action
    2. Small amount of traitors cannot cause loyal generals to adopt a bad plan
- Reduce the problem to how a single node communicates his information



BGP - Recap (2/2)

- A commanding general must send an order to his n-1 lieutenant generals such that…
  - IC1: All loyal lieutenants obey the same order.
  - IC2: If the commanding general is loyal, then every loyal lieutenant obeys the order he sends.

QUESTION: How does Proof-of-Work Consensus solve the Byzantine Generals Problem?



Proof-of-Work Consensus Algorithm

- Probabilistic solution to Byzantine Generals Problem
  - Probability of a malicious node generating an alternate history quicker than honest history decreases per added block

Achieving Consensus: Abstract PoW Example (1/2)

1. Byzantine generals will agree on a specific PoW problem (calculation and verification processes)
    - First plan received with a valid solution will be the accepted plan
2. The generals begin solving the PoW problem
    - Attempt to create a block and broadcast it
3. The general who solves the problem send messengers to the other generals
    - The plan of action
    - A solution to the problem

Achieving Consensus: Abstract PoW Example (2/2)

- When a general receives a block, he will independently verify the solution and incorporate it into his block of it is valid
  - Then begins working on next PoW problem
- As the process continues and more generals solve the PoW problem, the chain grows
  - Makes clear the generals which chain has the majority contribution for all the generals

Consensus Process Outcome

- Generals can get a probability of how many other nodes are also in agreement with them
  - Results of being able to calculate the time it takes for block production for entire chain they believe to be the honest plan
- PoW prevents conflicting signals
  - Generals build PoW blocks on top of each other
  - Essentially seal/vote for information in parent block

EXAMPLE: If it takes an average of 10 minutes for a block with all generals' computational power combined, and within an hour six blocks are produced, the generals can surmise that there is consensus on the plan of attack.