Byzantine Generals Problem

Objectives

Objective

Describe the Byzantine Generals Problem

Objective

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

1982 Publication

The Byzantine Generals Problem

LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE
SRI International

Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors. Applications of the solutions to reliable computer systems are then discussed.

Categories and Subject Descriptors: C.2.4. **[Computer-Communication Networks]**: Distributed Systems—*network operating systems*; D.4.4 **[Operating Systems]**: Communications Management—*network communication*; D.4.5 **[Operating Systems]**: Reliability—*fault tolerance*

General Terms: Algorithms, Reliability

Additional Key Words and Phrases: Interactive consistency

1. INTRODUCTION

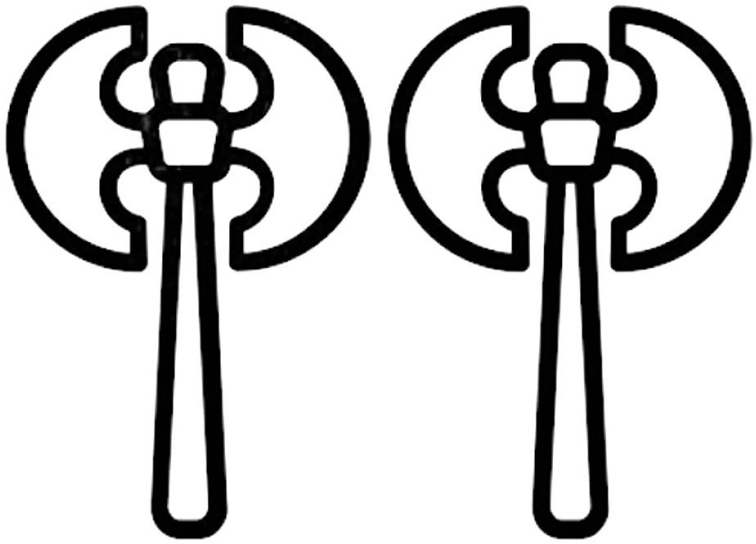
A reliable computer system must be able to cope with the failure of one or more of its components. A failed component may exhibit a type of behavior that is often overlooked—namely, sending conflicting information to different parts of the system. The problem of coping with this type of failure is expressed abstractly as the Byzantine Generals Problem. We devote the major part of the paper to a discussion of this abstract problem and conclude by indicating how our solutions can be used in implementing a reliable computer system.

We imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger. After observing the enemy, they must decide upon a common plan of action. However, some of the generals

This research was supported in part by the National Aeronautics and Space Administration under contract NAS1-15428 Mod. 3, the Ballistic Missile Defense Systems Command under contract DASG60-78-C-0046, and the Army Research Office under contract DAAG29-79-C-0102.
Authors' address: Computer Science Laboratory, SRI International, 333 Ravenswood Avenue, Menlo Park, CA 94025.

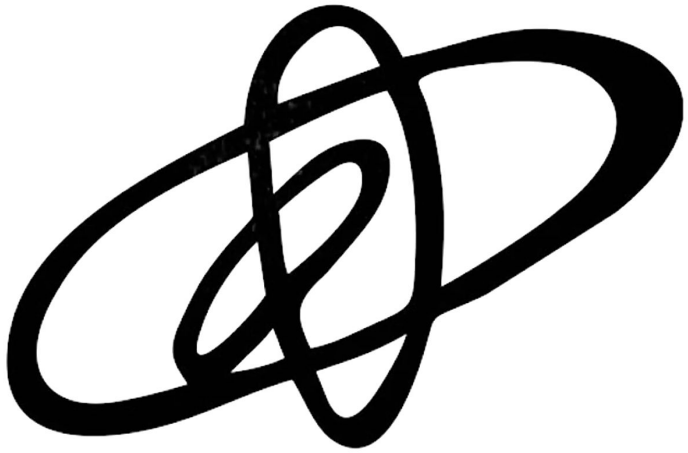
The Risk of Conflicting Information

- The Byzantine Generals Problems
  - Communicating only be messenger, the generals must agree upon a common battle plan.
  - One or more of them may be traitors who will try to confuse the others.
  - The problem is to find an algorithm to ensure that the loyal generals will reach agreement.
- A problem common to any computer system relies on teh ability to come to consensus on a decision over an unreliable and distributed communication/computer network
- Extremely relevant to blockchain technology



The Risk of Conflicting Information

- The generals represent the nodes within a computer system
- Traitors represent faulty nodes
- Messages corrupted during transport between the generals represent faulty communication channels



The Goal

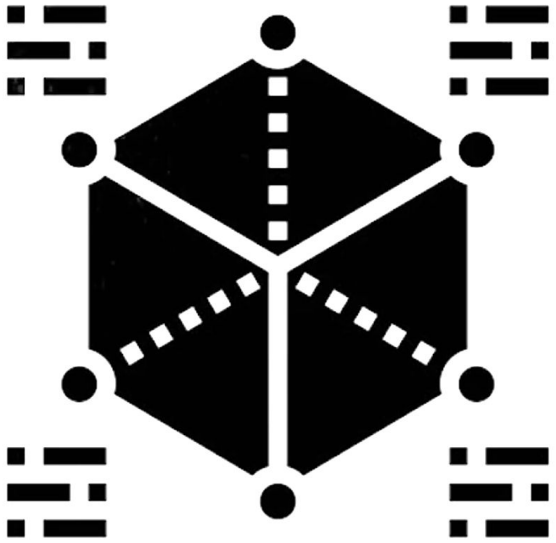
Design an algorithm/consensus protocol that guarantees two conditions

A.

B.

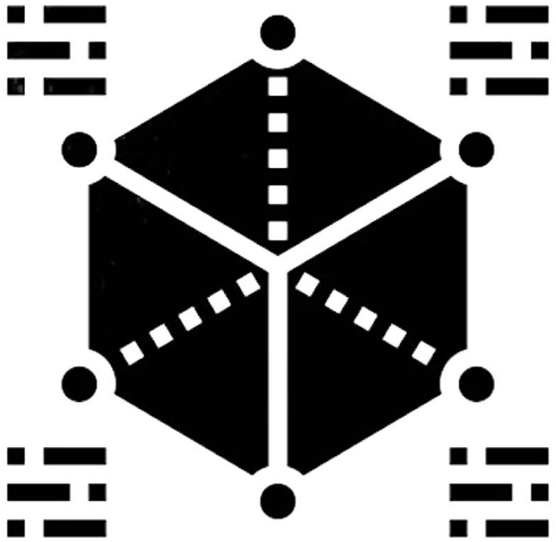
Algorithm Guarantees - Condition A

- All loyal generals decide on the same plan of action:
  - In every scenario, all loyal generals will carry out the plan of action the algorithm specifies for that scenario.
  - Any and all traitorous generals may carry out any plan they wish regardless of what the algorithm suggests.
  - Regardless of what the traitorous generals do the algorithm must guarantee this condition.



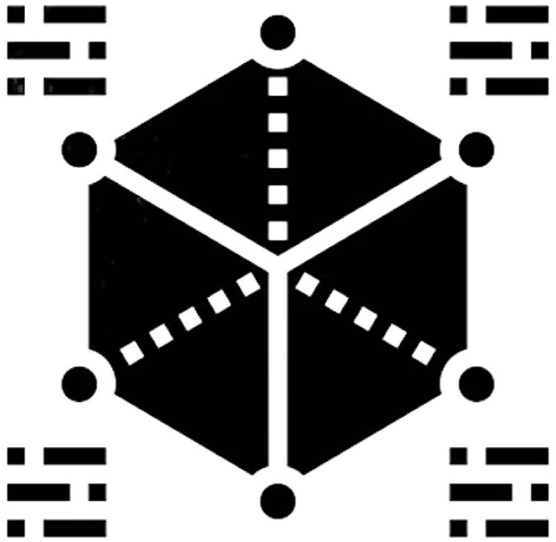
Algorithm Guarantees - Condition B

- A small number of traitors cannot cause the loyal generals to adopt a bad plan:
  - Unlike Condition A, this condition is had to formalize with respect to the definition of what a bad plan is.



Algorithm Guarantees, continued

- Let v(i) be the information communicated by the i^{th} general.
- Condition A will be achieved if each general uses the same method when combining the information.
- Decision choice is limited to “attack” or “retreat”
- Condition B can be achieved by each loyal general following the majority decision.



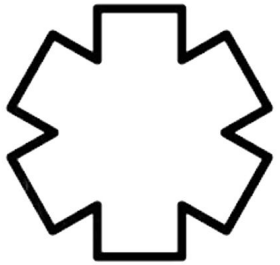
Question

Is there a key assumption being made in this solution?

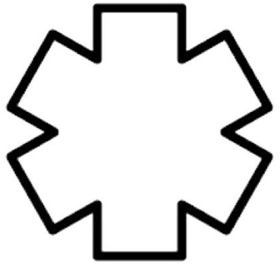
About that assumption…

Algorithm Guarantees, continued

- **Requirement 1.** Any two loyal generals use the same value of v(i).



- **Requirement 2.** If the i^{th} general is loyal, then the value that he sends must be used by every loyal general as the of v(i)



Reduction to Byzantine Generals Problem

- Restrict our consideration of the problem to how a single general sends his value to the others.

A General Sending Orders to Subordinates

- IC1: All loyal lieutenants obey the same order.
- IC2: If the commanding general is loyal, then every loyal lieutenant obeys the order he sends.
- IC1 and IC2 are known as the interactive consistency conditions.

NOTE: If the commanding general is loyal, then IC2 implies IC1

- To solve the original problem, the ith general sends his value v(i) using a solution to the Byzantine Generals Problem while considering the other generals as lieutenants.