Question 1 *The Byzantine Generals Algorithm[6 marks]*

In the Byzantine Generals Algorithm, suppose that there is exactly 1 (one) traitor and that Ivan's data structures are:

Ivan					
General	Plan	Reported by			Majority
		Basil	John	Leo	
Basil	R		A	R	?
John	R	A		A	?
Leo	R	R	R		R
Ivan	A				A
					?

1.1 Who is the traitor? Justify your answer (explain why this general is the traitor and why none of the other generals can be the traitor).

Answer:

1.2 What does Ivan decide about Basil's and John's plans? What does Ivan decide about the overall majority plan?

Answer:

1.3 Using DAJ, construct a minimal scenario leading to the shown data structure for Ivan. In this minimal scenario, the traitor's only incorrect messages should be the ones in Ivan's data structure above. Provide a screenshot of the main window in DAJ.

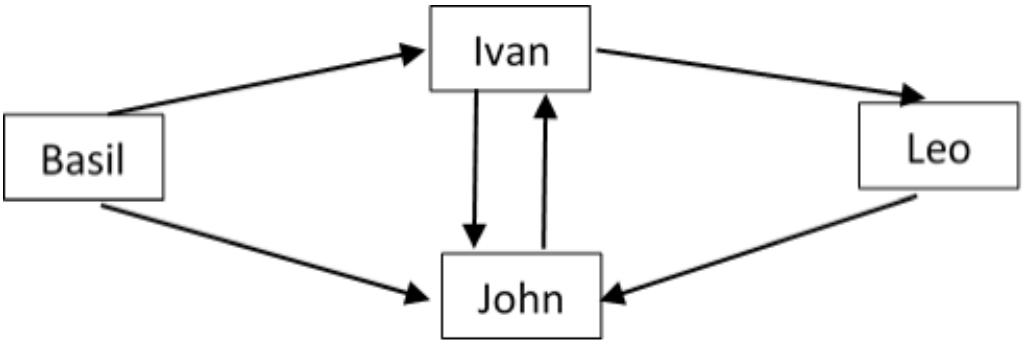
Answer:

1.4 For the scenario constructed in the previous question, provide screenshots of the 4 (four) knowledge trees that DAJ constructs about each of the generals. Note that knowledge trees are called "message trees" in DAJ. Which of these knowledge (message) trees indicate the traitor's incorrect messages?

Answer:

Question 2 *The Dijkstra-Scholten Algorithm[4 marks]*

A distributed system with 4 (four) nodes including 1 (one) environment node is depicted with the following directed graph:



Using DAJ, construct a scenario for each of the 4 (four) different spanning trees in the above directed graph. These scenarios differ in the order of the sent messages (but note that some orders of sent messages result in the same spanning tree, while you have to find all different spanning trees). For each of these scenarios, only provide a screenshot of the spanning tree that DAJ constructs.

Answer:

Question 3 *Permissionless consensus[3 marks]*

Bitcoin uses what's called *proof-of-work* consensus, where the first node to solve a computationally expensive puzzle gets to pick the next block.

How does Bitcoin mitigate the problem of two nodes solving the puzzle at roughly the same time, causing a split decision? Skim the Bitcoin white paper for the answer. Explain informally and in your own words.

Answer: