Homework10

Read the following materials about IOTA.

1. IOTA White paper: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf
2. About IOTA Coordinator: https://medium.com/@ercwl/iota-is-centralized-6289246e7b4d

Then answer the following questions.

1. How does IOTA protect against a double spending attack? Hence are transaction confirmations guaranteed (like in Algorand) or probabilistic (like in Bitcoin)?

2. What is a parasitic tangle and how can it be created? Is this a problem in IOTA?

3. Is IOTA a truly decentralized protocol? Discuss issues facing The Coordinator and IOTA's Incentive mechanism. (open ended question)

4. Consider the fact that people contribute to the network hash rate only when they send transactions and for each transaction they only compute 150M SHA256 hashes. Consider the speed of the current SHA256 ASIC miner speed as 13.5TH/s, how many TPS IOTA would require for it to turn off coordinator so that a single SHA256 ASIC miner cannot do double spending?