Tor, Bitcoin

Question 1 ***True/false***

Q1.1 Assume you've set up a 3-relay Tor circuit to access some websites over HTTPS. A malicious adversary takes control of the entry relay, but the other two are honest and uncompromised.

TRUE or FALSE: The adversary can now learn your identity.

○ TRUE ○ FALSE

Q1.2 Assume you've set up a 3-relay Tor circuit to access some websites over HTTPS. A malicious adversary takes control of the middle relay, but the other two are honest and uncompromised.

TRUE or FALSE: The adversary can now learn which website you are visiting.

○ TRUE ○ FALSE

Q1.3 Assume you've set up a 3-relay Tor circuit to access some websites over HTTPS. A malicious adversary takes control of the exit relay, but the other two are honest and uncompromised.

TRUE or FALSE: The adversary can now learn your identity.

○ TRUE ○ FALSE

Q1.4 TRUE or FALSE: In Bitcoin, once your transaction is successfully added to a block that lives on the longest chain, you can be guaranteed that it will never be lost.

○ TRUE ○ FALSE

Q1.5 TRUE or FALSE: If you had 70% of the hashing power in Bitcoin, you would be able to add spoofed transactions to the blockchain

○ TRUE ○ FALSE

Q1.6 TRUE or FALSE: In Bitcoin, including the hash of the previous block is only useful for ensuring immutability and append-only properties

○ TRUE ○ FALSE