Part D

Security analysis: Discuss why the PW can prevent double spending in the Bitcoin network and identify two possible attacks on PW.

Two transactions must be performed to attempt double spending – the second transaction will have the same origin as the first and can therefore be easily identified as an attack. When a miner finds the corresponding pre-image, broadcasts it, and has it verified by other miners, the hash-chain will add a block with the signed transaction and the pre-image. In other words, the transaction data is stored permanently in the blocks. Without a pre-image, a block cannot be added to the pre-existing chain. If this were not the case, an attacker would be able to create another transaction using the bitcoins from previous transactions and there would be no way of verifying whether or not the next transaction was previously processed.

51% attack: In the bitcoin system, any group of miners who control greater than 50% of the computing power of the network are in possession of majority control. Consequently, they are able to interrupt the addition of new blocks by preventing other miners from completing them.

MITM: an attacker can intercept a miner’s broadcasted pre-image and replace it with an invalid pre-image, keeping the valid pre-image for themselves to broadcast instead.