Discussion Week 3

Definitions

▽ **Cryptographic Hash Functions (i.e. What are 3 properties of a hash function?)**

▽ **Hash Puzzles (i.e. What 3 requirements should a hash puzzle have?)**

Discussion Questions

▽ **What is the purpose of a Merkle tree? How can we tell if a block has been tampered with?**

▽ **Say Alice and Bob are separated and don't trust one another. Alice wants to give Bob a commitment to her guess without revealing her guess before Bob flips the coin. How could Bob cheat Alice with the commitment scheme? How could Alice cheat Bob?**

▽ **Does block difficulty strictly increase over time? If not, what does it depend on? How do we determine the block difficulty (i.e. What formula helps us calculate the difficulty)? How often does the global network difficulty change?**

▽ **Bonus/Optional: How are Bitcoin addresses generated?**

▽ **Bonus/Optional: What's the difference between pub-key hash and pub-key script?**