Tutorial 6 Solutions

1. What is the difference between a peer-to-peer network and a centralised network? What things are harder to do with a peer-to-peer network?

A peer-to-peer system is made up of a number of different nodes, all with equal status. It is a lot harder to reach an agreement among nodes, especially when some of them might be malicious.

2. Why do digital coins have a unique ID while pound coins do not? Is this similar to the unique ID on bank notes?

It is very easy to forge anything digital and so each different digital coin needs a unique ID to tell them apart. Using them involves searching all possible transactions, which is CPU intensive.

Each pound coin is a different physical object, making them somewhat harder to copy. If they each had unique ID's then these ID's would have to be recorded with each transaction, which is much too much effort.

Bank notes have unique ID's to determine where and when they were printed. This can be useful in some crimes involving new notes. Apart from that, they are like pound coins and so the reason for ID's is different.

3. What is a crypto-coin ledger and why is it important?

It is a record of all transactions. It is used to prove ownership since coins can be traced to their creation. It also prevents double spending.

4. How can you get change when you spend your crypto-coin?

Each transaction destroys one coin and creates two new coins. One is the payment and the other is your change.

Several small value coins can be combines if they are all destroyed in a transaction and one new coin with the same value is created.

5. What is a blockchain and a Merkle tree? Why are they useful?

A block chain is a linked list, where each block contains a hash of the previous block as well as a pointer to it. It is created in time order so that it is impossible to insert a fraudulent transaction into an existing blockchain.

A Merkle tree is a sorted binary tree which also stores hashes as well as links to sub-blocks. It is used to create all the transactions forming a block. It is more efficient to search than if all transactions were in a linked list.

6. What cryptographic algorithms are used by bitcoin?

SHA-256 for the hashes and Elliptic Curve Digital Signatures for the signatures.

7. What is distributed consensus and how is it achieved with bitcoin?

A distributed consensus arrives when all honest nodes agree to the structure of a new block that is proposed by an honest node.

All nodes get copies of all transactions and keep a list of pensing transactions that have not made it into the blockchain. When a new node is proposed, they check to make sure that it only used valid transactions before adding it to their copy of the ledger.

8. Does it matter if some nodes have different versions of the blockchain? Will this happen even if all nodes are honest?

This is bound to happen because of network latency. A valid transaction may arrive late at some nodes, while being part of a proposed new block. Thes nodes will reject the new block and not add it to their version of the blockchain. They will eventually add the new block later on.

So it doesn't matter if two nodes differ in a few newer nodes. Honest nodes will agree on all older blocks.

9. A merchant should wait for a crypto currency to clear before parting with his goods, but how long should he wait?

A rule of thumb is wait for 1 hour. This is protection against double spending.

10. What is bitcoin mining? What does it involve? What does the winner do and what is their reward? Why does it pay for the winner to be honest?

Miners solve a hard computational puzzle, a hash puzzle with bitcoin mining.

The winner gets to propose a new block containing all the current transactions.

An extra transaction awarding him 25 bitcoins (currently) is included.

They only get this reward if the new block is accepted by the majority of other nodes. If they are dishonest then they don't get the bitcoins because it won't be accepted.

11. How often are new blocks created? How is this time interval kept constant?

Every 10 minutes on average. The hardness of the puzzles is adjusted to keep the interval to 10 minutes.

12. What is a transaction fee and how is it useful?

Transactions can award some of the bitcoins spent to the successful miner. This may eventually replace the mining award.

13. What are stored in wallets? List some different types of wallets.

14. How do bitcoin exchanges work and what are some of the dangers in using them?