

Exercise 2

A. Blockchain

1. Name the three key properties of the Bitcoin Blockchain according to the lecture and explain them.

Solution:

- The Blockchain is trust-free. This means that we do not need to trust a third party which maintains the platform. The decentralized network ensures the validity of the contents of the Blockchain.
- The Blockchain is tamper-proof. No entity can single-handedly manipulate the data after it is stored in the Blockchain.
- The Blockchain is transparent. All contents of the Blockchain can be seen by any node of the network.

2. Decide if changing the following contents of the block alters the hash of the block header.

- Transaction ordering (Tx stay the same)
- Transaction add/removal
- Difficulty
- Previous blocks
- Nonce

Solution:

- Transaction ordering (Tx stay the same) **Yes**
- Transaction add/removal **Yes**
- Difficulty **Yes, but you cannot change it (defined by the network)**
- Previous blocks **Yes, but you should not change it (results in invalid blocks)**
- Nonce **Yes**

3. Explain how chaining is implemented in a Blockchain.

Solution:

Blocks are chained through adding the hash of the previous block (n-1) to the current block (n).

B. Genesis Block

Solution:

The headline you intend to use is an advertisement. Therefore, it would be possible for you to know of this text ahead of time and actually create the first Block before that date.

C. Network

6. Name and briefly explain three roles in the Bitcoin network.

Solution:

Wallet Owner:

- The wallet owner owns different private keys to unspent transaction outputs (UTXOs)
- He is the owner of all stored currencies on these addresses
- He sends money by signing and publishing new transactions to a connected light node, full node or miner

Light Node:

- The light node can act as a relay for transactions of one wallet owner
- It validates whether a single transaction of the wallet owner was executed correctly
- The light node also requires a full node to connect to the network
- Almost no relevance in practice today. Today, centralized services are used to create transactions.

Full Node:

- The full node maintains the complete blockchain. Its record of the chain is complete, it contains every single transaction and block until the genesis block.
- Is connected to other full nodes and exchanges information. Namely:
- Validates every transaction and block it receives
- Relays all new transactions and blocks

Miner:

- The miner needs the same record as a full node in order to work properly. He also is connected with other nodes and maintains the network.
- Additionally, the miner is responsible for creating new blocks by trying to solve the mining puzzle.
- The miner gets rewarded by creating new blocks.

(Taken from the lecture notes)

7. Explain the function of the memory pool.

Solution:

The memory pool stores all transactions which are not contained in a block yet. Each full node maintains the list of these transactions and updates it when 1) a new block arrives and 2) new transactions arrive.

8. Alice wants to send 1.0 BTC to Bob. What steps does her transaction take until being completed?

Solution:

1. The transaction is created and signed by Alice.
2. The signed transaction is sent to a full node for validation.
3. If the transaction is valid, the full node publishes the transaction to the network and is added to the memory pool.
4. A miner includes Alice's transaction from the memory pool to its block. The miner solves the puzzle and publishes the block to the network.
5. Other nodes receive the mined block and validate all contents.

D. Storing Bitcoins

9. What is the difference between a hot storage and cold storage? Give an example for both types. Which type do exchange wallets fit in?

Solution:

A hot storage wallet is immediately available to use. An example is a wallet software on your PC connected to the internet. A cold storage is a method of storing private keys in an isolated environment. These wallets are not immediately available but provide higher security. An example is a printed paper wallet.

Exchange wallets resemble hot wallets, as (depending on limitations and security) funds are immediately available. However, transferring coins to an exchange wallet means handing the possession of your coins to the exchange. You no longer own the private key, but the exchange does. In many cases exchanges got hacked and users lost their funds.