eCommerce – Chapter 07

Bitcoin – Basic Approach

- Cryptocurrency and payment system
- Distributed pee-to-peer without a central server o point of control
- Participants conduct consensus mechanisms to accept or decline transactions and to update the blockchain.
- Number of bitcoins is controlled by mining process. Prevents fraudulent manipulation of the blockchain.

Transactions as Double-Entry Bookkeeping

- **Transactions:** Move value from inputs to outputs
- **Inputs:** Refer to transactions from where the value is coming from.
- **Outputs:** Assign new owners to a value by associating it with a destination key.
- **Transaction fee:** When inputs and outputs don't match.

A chain of Transactions

- Outputs from one transaction can be used as inputs in a new transaction, creating a chain of ownership.
- Contains a digital signature for each amount of inputs.
- **Spending money:** Signing a transaction that transfers value from previous transactions over to a new owner identified by bitcoin address.
- The blockchain is a huge collection of unspent transaction outputs.

Common Transaction Forms

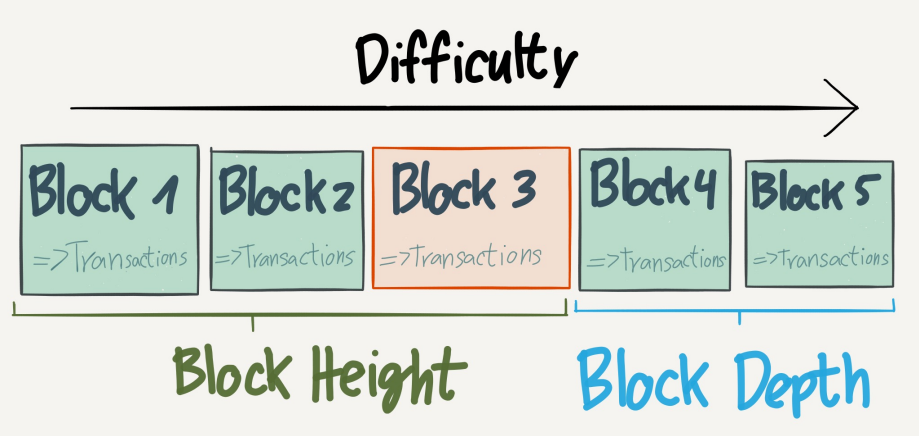
- **Common transaction:** Simple payment from address to another.
- **Aggregating Transaction:** Several inputs can be aggregated to one input *(Clean up wallet)*
- **Distributing Transaction:** Distribute one input to multiple outputs**.** *(Pay Employees)*

Block Depth and Height

- Transaction are not verified until they become part of the blockchain
- New transactions are collected and stored in a pool
- Every 10 minutes, mining nodes start generating new blocks by adding transactions from the pool.
- A new block is filled with transactions and a fingerprint (the result of a hash function) of the last block thereby chaining the new block to its predecessor.
- To protect the blockchain from subsequent manipulation, mining nodes have to solve a computational intensive problem (*proof- of-work*)

- The *height* of a block refers to its position in the blockchain counted from its beginning, i.e., block #0 (genesis block)

- The *depth* of a block refers to its distance measured from the block on the top of the blockchain



Elliptic Curve Multiplication (ECM)

- Private key is built by a random number generator that produces a 256-bit value
- The public key is calculated form the private using elliptic curve multiplication, which is irreversible.
- Reverse operation can only be done with brute-force
- Much more efficient than RSA. 160 bit similar to 1024.

Creating of Bitcoin Addresses

- Ownership of Bitcoins is established through digital keys, bitcoin addresses and digital signatures.
- **Digital Keys:** Are given by a pair of private and public key, which belong to a user's account.
- **Public key:** Used to generate a Bitcoin Address (*Bank Account Number*)
- **Private key:** Used for digital signatures, sign transactions (*PIN*)

Nondeterministic Wallets

Wallets: Are containers for private keys.

- Collections of randomly generated private keys.
- Generates 100 random private keys when first started and add more on demand
- Each key is only used once
- Funds are irrevocably lost if the wallet becomes inaccessible

Deterministic Wallets

- Contain keys that are all derived form a common seed through use of a one-way hash function
- All keys can be derived from seed, allowing for easy migration of all the user's keys between different wallet implementations

Hierarchical Deterministic Wallets

- Most advanced form of deterministic wallets
- Generate keys in a tree structure, such that a parent key can derive a sequence of children keys.
- Can be used to express additional organizational meaning.

Mnemonic Code Words

- Word sequences that represent (encode) a random number used as a seed to derive deterministic wallet
- Sequence of words is sufficient to re-create the seed and the wallet with all derived keys.

Paper Wallets

- Are Bitcoin private keys printed on paper.
- Often also contain the Bitcoin address
- Funds on a paper wallet should be withdrawn completely with one transaction
- No re-useable

Transactions

Creating Transactions:

- Online or offline
- Once it has been created, it is signed by the owner of the source funds (input)

Sending Transactions:

- Sender of a node should send to a transaction to multiple nodes to make sure that it propagates
- Need to be delivered to the bitcoin network for propagation and inclusion in the blockchain
- It can be broadcast using underlying network technology

Propagating:

- Each bitcoin node is connected to a few other bitcoin nodes that it discovers during start-up through the peer-to-peer-protocol
- Messages are propagated from each node to all peers to which its connected
- Once a transaction is sent to any node connected to the network, it will be validated by that node

- If valid, the node will propagate it and return confirmation. If not, it will reject it and return a rejection message

Structure

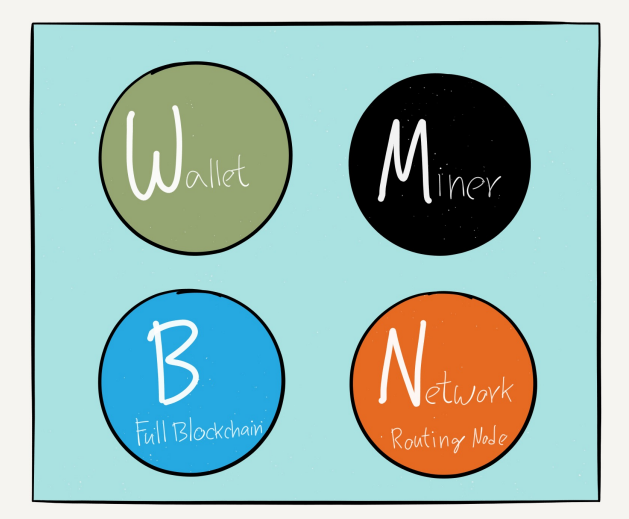
Field	Description
Version	Specifies which rules this transaction follows
Input Counter	How many inputs are included
Inputs	One or more transaction inputs
Output Counter	How many outputs are included
Outputs	One or more transaction outputs
Locktime	A Unix timestamp or block number

Locktime: Defines the earliest time a transaction is valid and can be relayed on the network or added to the blockchain

Script Construction: Bitcoin wallets validate transactions by executing a script, written in a Forth-like programming language.

Node Types

- **Routing nodes:** Used to send transactions and flood transactions within the network
- **Full blockchain nodes:** Maintain a complete up –to-date copy of the entire blockchain
- **Mining nodes:** Participate in the creating of new block of the blockchain
- **Wallet nodes:** Enable users to create and receive transactions, manage a user's bitcoin addresses and store related public and private keys
- **Core Client:** Implement the four functions mentioned above
- **Full Nodes:** Implement all but mining



The Bitcoin Network

- Initial Handshake between peers
- Address propagation and discovery
- Getting the blockchain: Synchronizes with lock
- SPV (Simple Payment Verification) Nodes download the block headers (approx. 1000 smaller than the hole blockchain)
- Bloom filters are probabilistic filters that allow SPV nodes to receive a subset of transactions without revealing precisely which Bitcoin address they are interested in

The Blockchain

- Is an ordered, back-linked list of blocks of transactions
- It can be stored in file or database
- Each block is identified by a *Block Hash*.
- Each block references its parent block through the previous *Block Hash* field in the block header
- **Genesis Block:** The first block created
- **Merkle root:** Summary of all transactions contained in the block
- **Merkle tree:** A binary hash tree used for efficiently summarizing and verifying the integrity of large sets of data

Mining & Consensus

- Is the process by which new Bitcoins are added to the money supply
- Two types of rewards:
    - **Proof-of-work:** Solving a difficult mathematical problem
    - **Transaction fees:** Superplus between inputs and outputs
- **Emergent Consensus:**
    - Applied by full and mining nodes
    - Tasks:
        1. Verification of transaction
        2. Mining blocks
        3. Verification of blocks
        4. Assembling and selecting chains of blocks

- **Blockchain Fork:** When two candidate blocks compete to form the longest blockchain. Usually occurs when two miners solve the proof-of-work simultaneously.