Blockchain

Codification of Trust

Goal: Collaboration without a middle man (i.e. no Trusted Third Party).

Problem: Reach consensus in a peer-to-peer network (i.e. solve the Byzantine Generals Problem)

- Subproblems: authenticity, integrity, consistency

Approach:

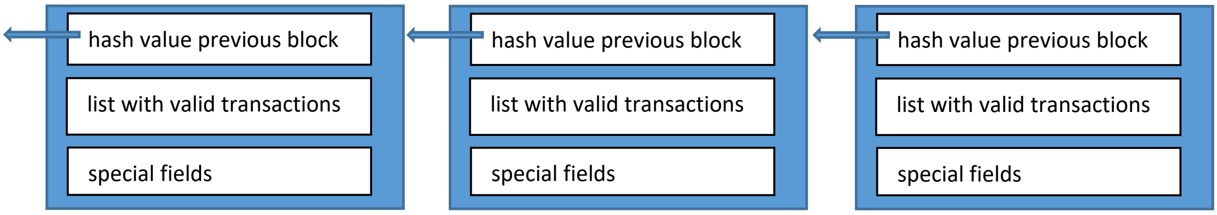
- Use public private key encryption for sender authenticity
- Use cryptographic hashing for data integrity
- Create a linked list of data blocks with cryptographic hash values as pointers, to prevent inconsistency (i.e. no double spending)

Solution:

- Transactions (data) are cryptographically signed, and then collected in new data blocks by miners
- Valid data blocks are linked into a chain: each block holds the hash value of its predecessor
- A data block is valid if:
    - All transactions (data) in the block are valid
    - The block has a certain property (consensus mechanism)
- If multiple chains exist (due to forks) the longest chain is the valid chain

Consensus mechanisms:

- Proof-of-work: the hash value of the block meets some criteria. Challenge: energy consumption
- Proof-of-stake: the block is created by a miner who meets some criteria. Challenge: nothing at stake


hash value previous block
list with valid transactions
special fields
hash value previous block
list with valid transactions
special fields
hash value previous block
list with valid transactions
special fields

Special fields: used for timestamps, miner information etc. In proof-of-work also used by miners to create a block which meets the hash value criteria (simply by trying rondom values to meet the criteria).

Changing data in a block leads to a changed hash value, breaking the chain.

<u>Incentive to reach consensus</u>: the miner of a new block gets a reward (e.g. transaction fee). This reward (as all data) is clearly only usefull if the chain is valid.

Nothing at stake: if there are multiple (longest) chains then the miner can attach a new block at the end of each chain, there is no incentive to choose a single chain. This in contrast to proof-of-work, where the miner has to choose a chain where he puts his computational power in.

Research Center for Data Intelligence

Jan Beumers, Roger Bemelmans