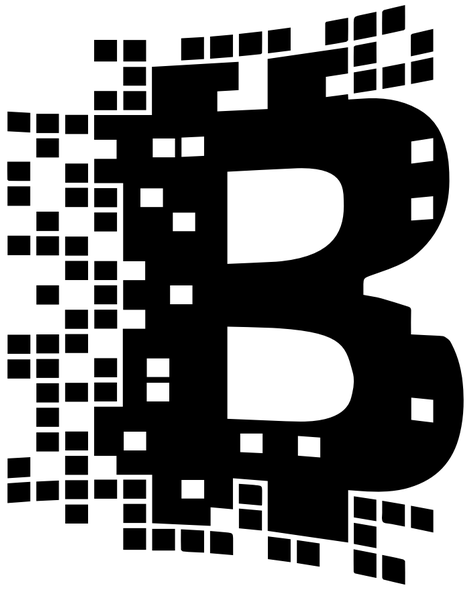
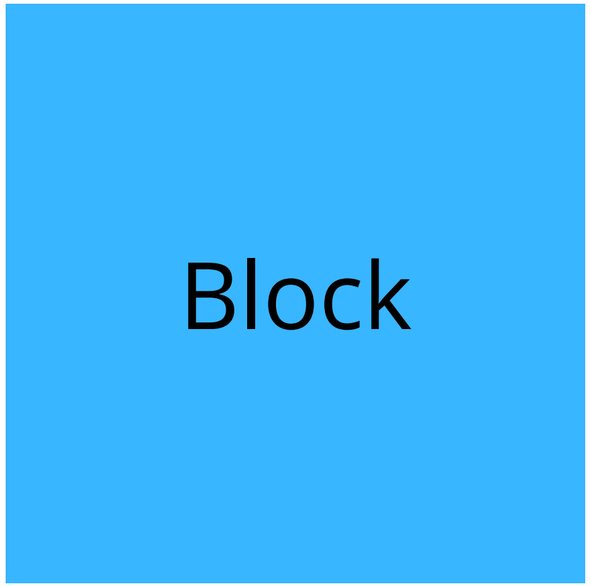


Blockchain: What, Why and How?

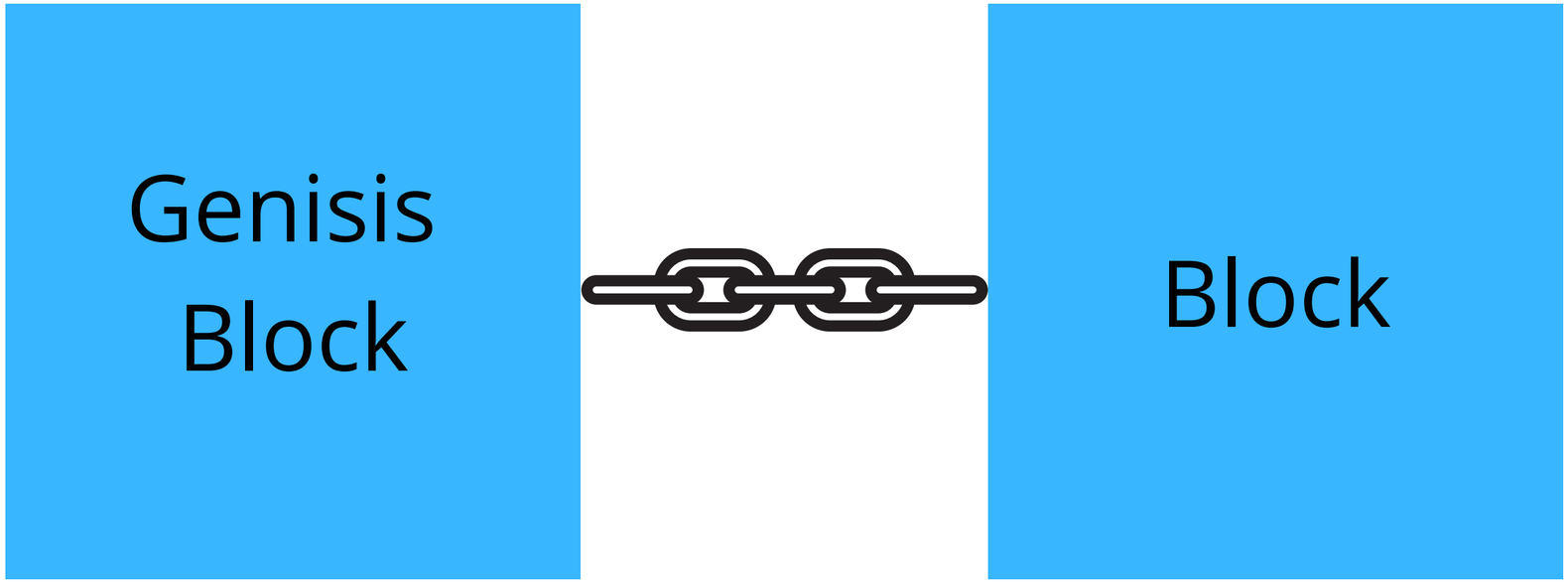
A **blockchain**,[1][2][3] originally **block chain**,[4][5] is a growing list of records, called *blocks*, that are linked using cryptography.[1][6] Each block contains a cryptographic hash of the previous block,[6] a timestamp, and transaction data (generally represented as a Merkle tree).

A Block



1. Data "trxs, records"
2. Prev. Hash: 14AB578C
3. Hash: 468EA5BA

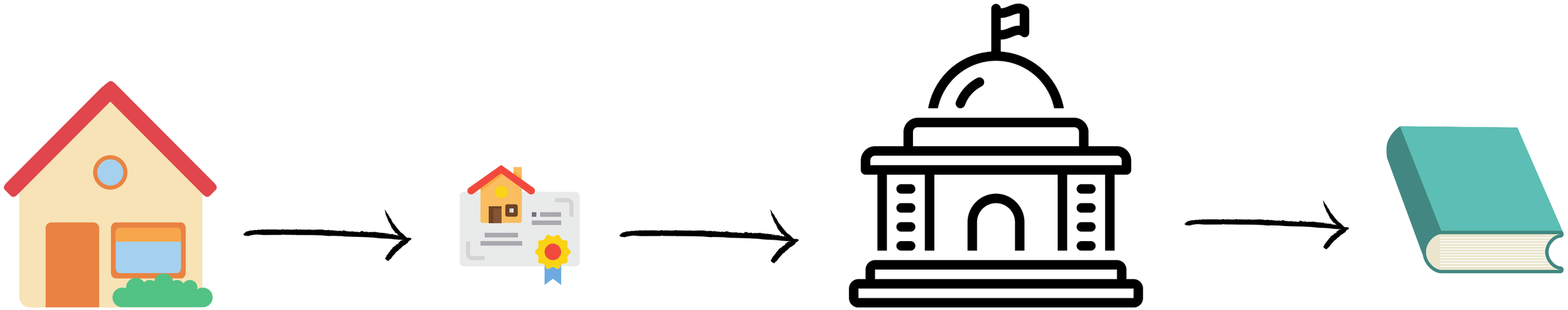
A Blockchain



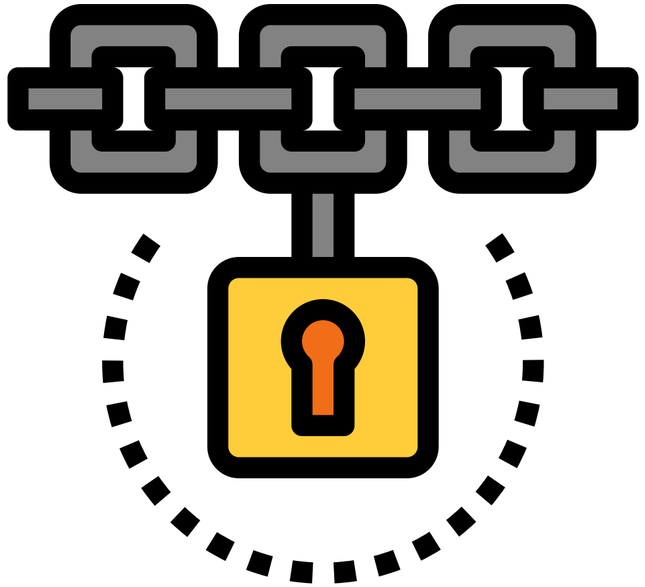
SHA256 HASH

3fc9b689459d738f8c88a3a48aa9e33542016b7a4052e001aaa536fca74813cb

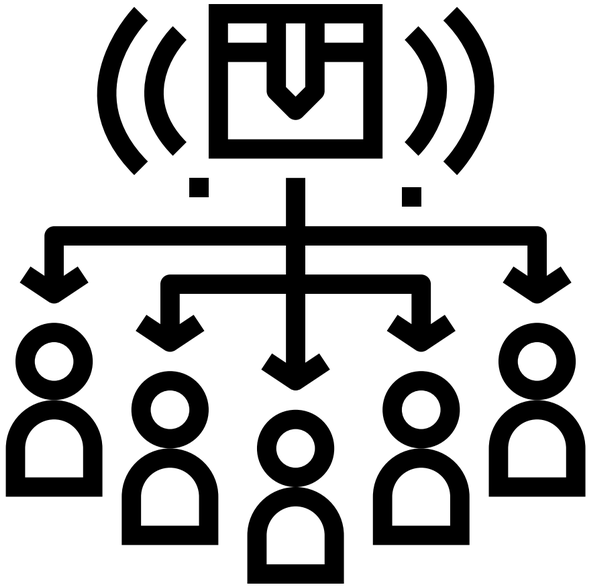
Why?



How?

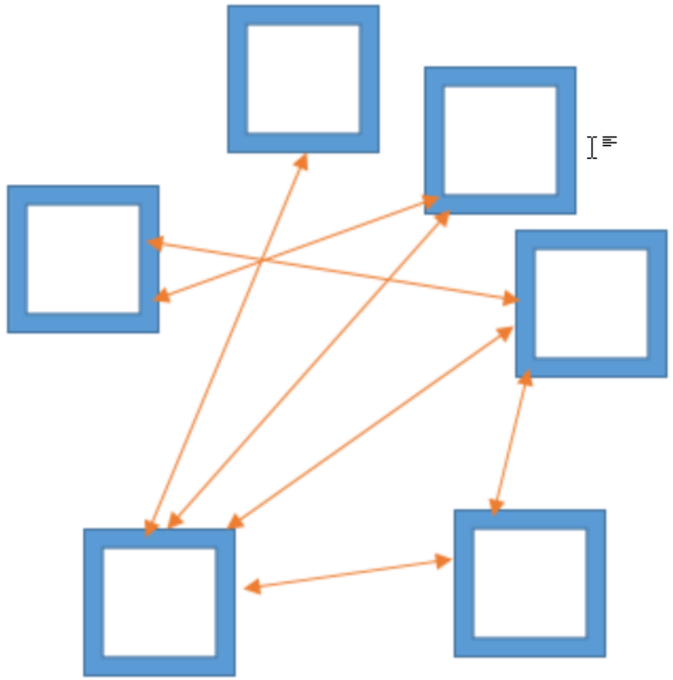


cryptographically linked



Distributed

Distributed P2P Networks



Mining

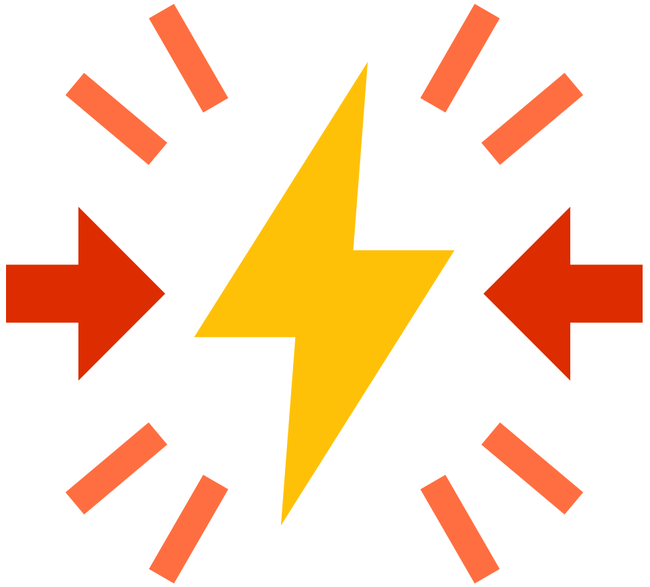
Block:	# 2
Nonce:	35230
Data:	Transactions: A -> B 5 Coins B -> D 10 Coins A -> C 2 Coins
Prev:	000015783b764259d382017d91a36d206d0600e2cbb35677
Hash:	5f1053bc0516ea1956fa0ce570b14fa6eae1be27047f6ed9c5

Flow

1. Transactions broadcast
2. Nodes maintain a pool of transactions
3. Take up some transaction (say 2000) and try to mine a block
4. Find the correct **nonce**
5. Block is mined
6. Block broadcast
7. Verified by other nodes
8. Other nodes add the new block to their local copy

Conflicts

1. What if 2 nodes mined a block at same time?
2. What if someone tries to add malicious block?



Let's build a blockchain in Julia