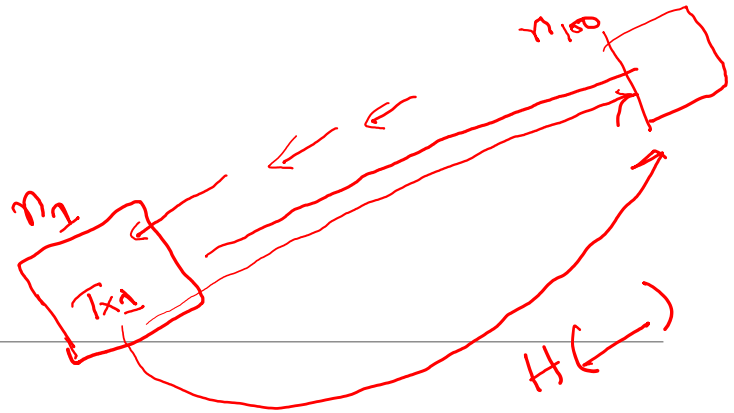
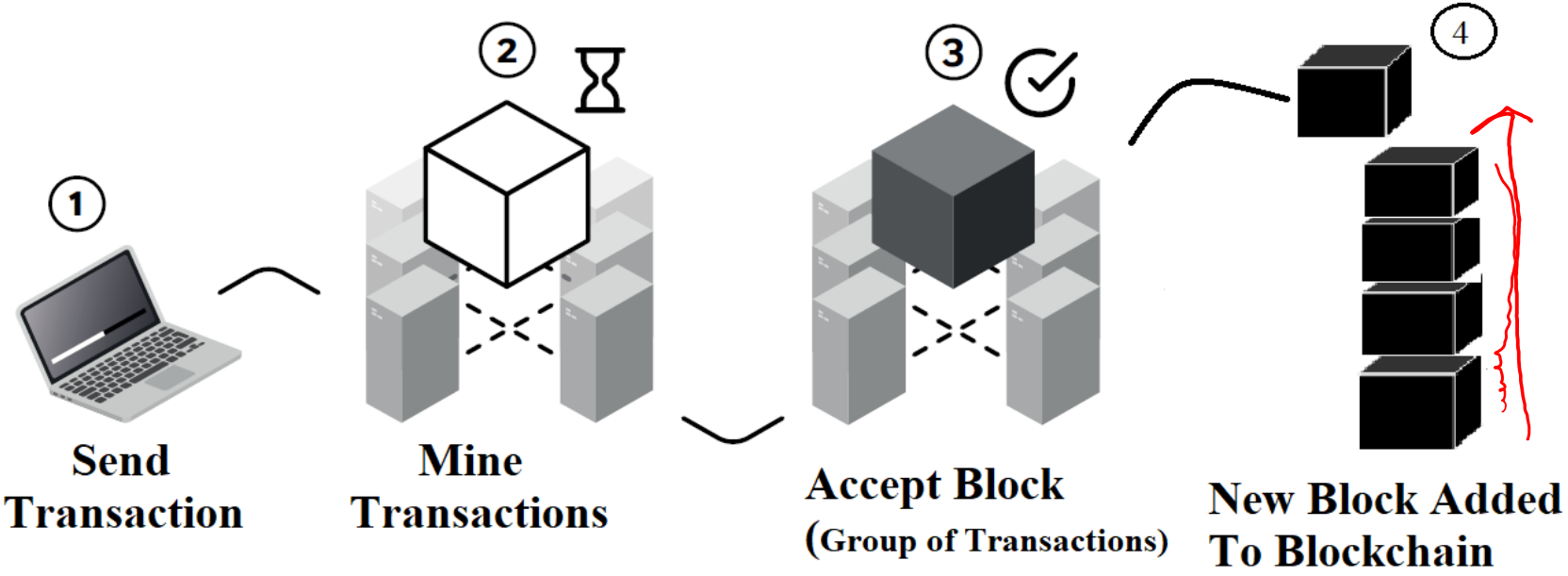
Merkle Tree

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY SRI CITY

CHITTOOR, INDIA

Bitcoin Network

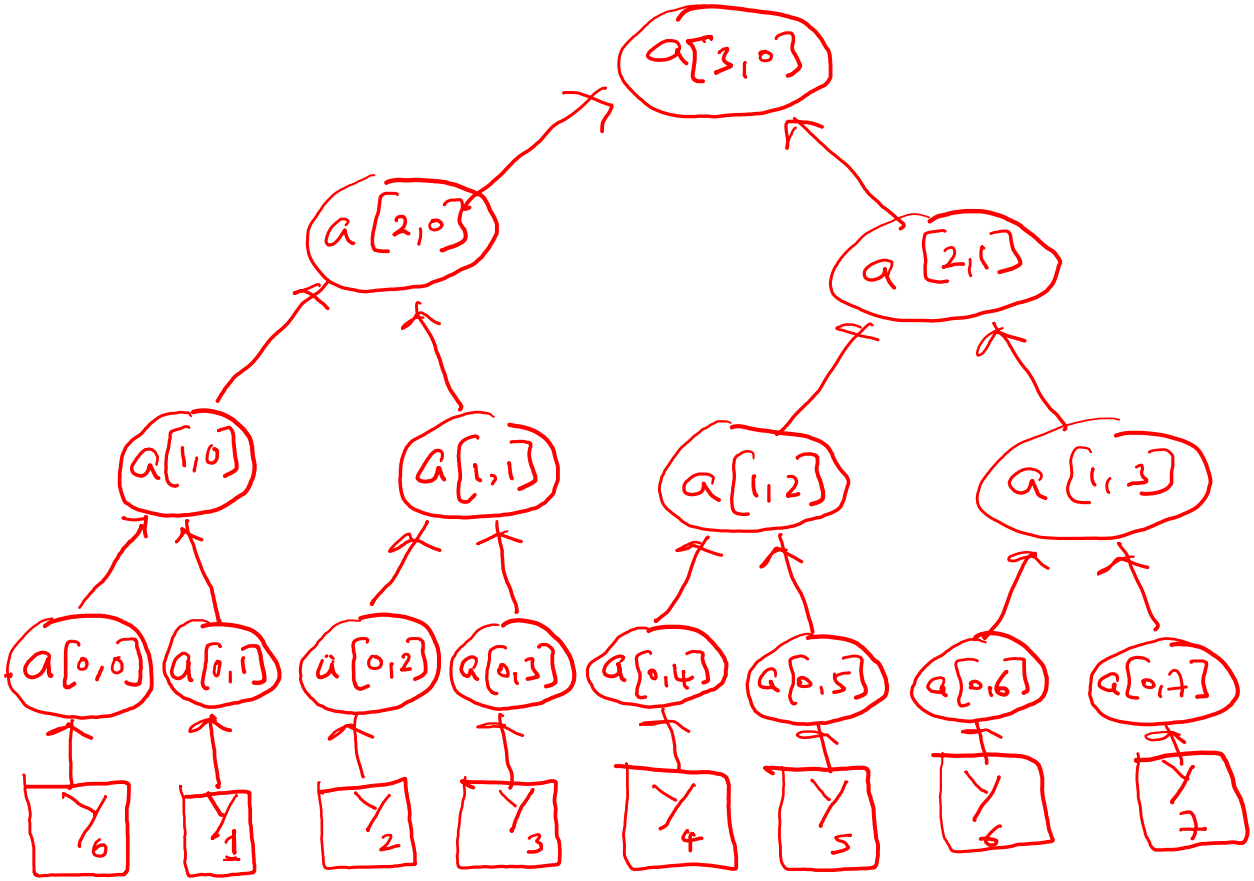




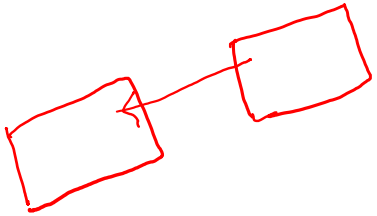
Merkle Tree

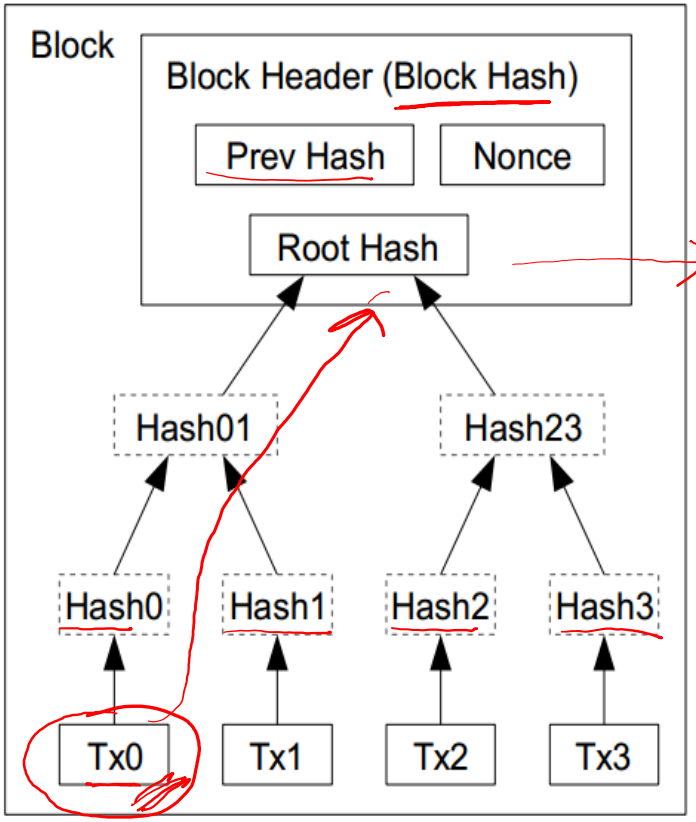
8 leafs

key merkle pubkey:

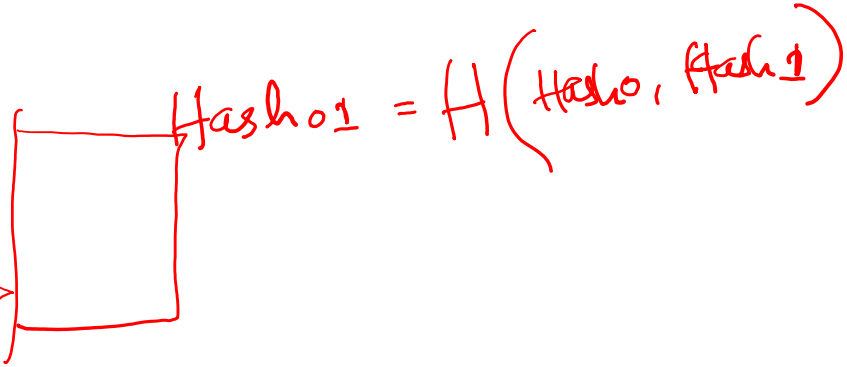


Block (Bitcoin)





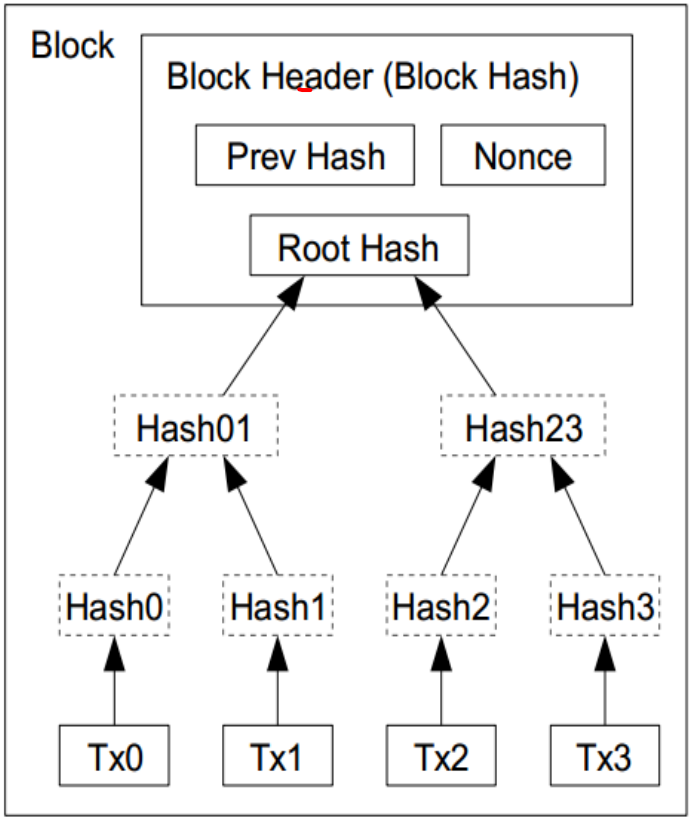
Transactions Hashed in a Merkle Tree



Optimizations

Merkle Tree

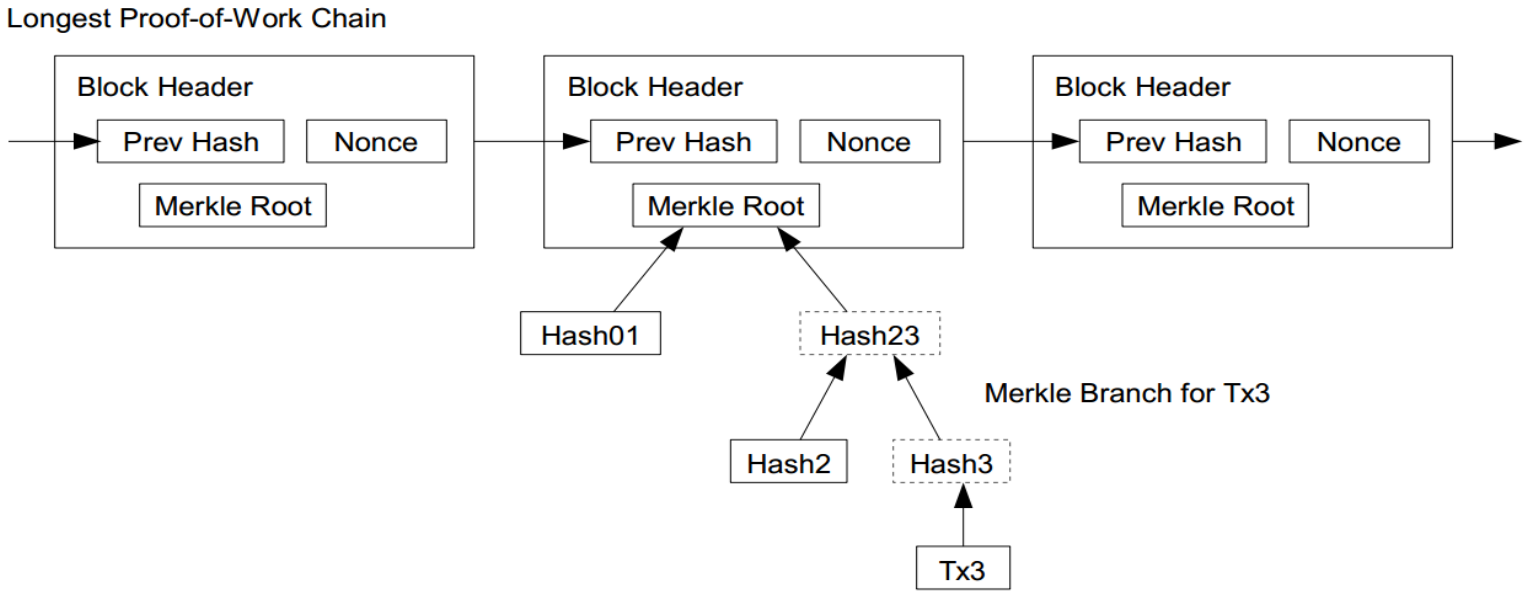
- Only keep the root hash
  - Delete the interior hash values to save disk
  - Block header only contains the root hash
  - Block header is about 80 bytes
  - **80 bytes * 6 per/hr * 24 hrs * 365 = 4.2 MB/year**
- Why keep use a Merkle tree?



Transactions Hashed in a Merkle Tree

Simplified payment verification

- Any user can verify a transaction easily by asking a node.
- First, get the longest proof-of-work chain
- Query the block that the transaction to be verified (Tx3) is in.
- **Only need Hash01 and Hash2 to verify; not the entire Tx's.**



THANK YOU