CS 168: Blockchain and Cryptocurrencies

Bitcoin Transactions and Merkle Trees

Prof. Tom Austin
San José State University

Lab Review

"Bitcoin is just Git"

(comment overheard in grad school)

Bitcoin Blocks

- Collections of transactions
- Fixed size
- Collectively, form a *blockchain*
- *Genesis block* – the very first block

Block Information

- Version
- Timestamp
- Previous block hash
- Proof-of-work (PoW) target
- Nonce (the "proof")
- Merkle root

Block Information

- Version
- Timestamp
- **Previous block hash**
- **Proof-of-work (PoW) target**
- **Nonce (the "proof")**
- Merkle root

Reviewed another day

Block Information

- Version
- Timestamp
- Previous block hash
- Proof-of-work (PoW) target
- Nonce (the "proof")
- **Merkle root**

Determines transactions in block

Merkle Trees

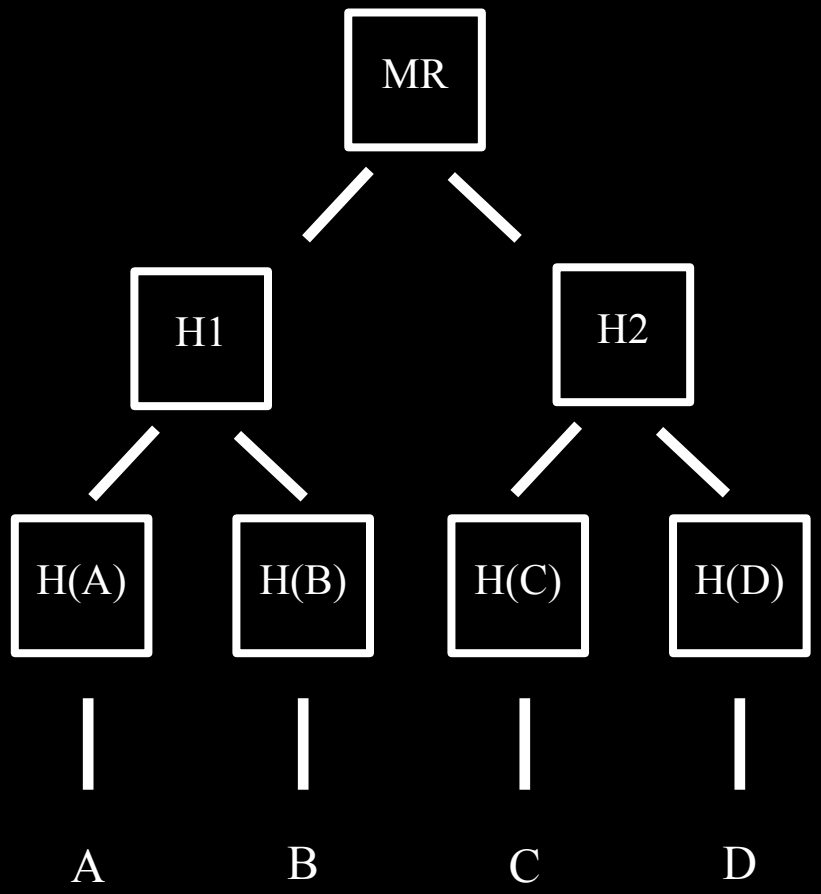
- Binary tree
- All nodes are hashes
  - Leaves: hashes of the data
    - Transactions, for Bitcoin
  - Inner nodes: hashes of children nodes
- Definitions
  - Merkle root: root of a Merkle tree
  - Merkle path: nodes needed to reconstruct Merkle root

Merkle Trees

H1 = H(H(A),H(B))

H2 = H(H(C),H(D))

MR = H(H1,H2)
(Merkle root)

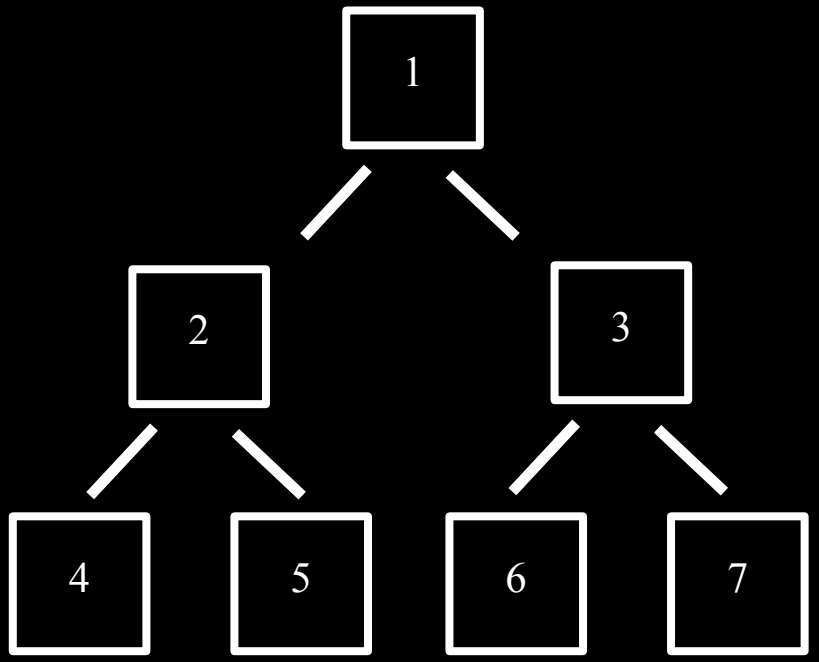


Storing Merkle Trees

More efficient to store in an array.

Left child = n*2

Right child = n*2+1



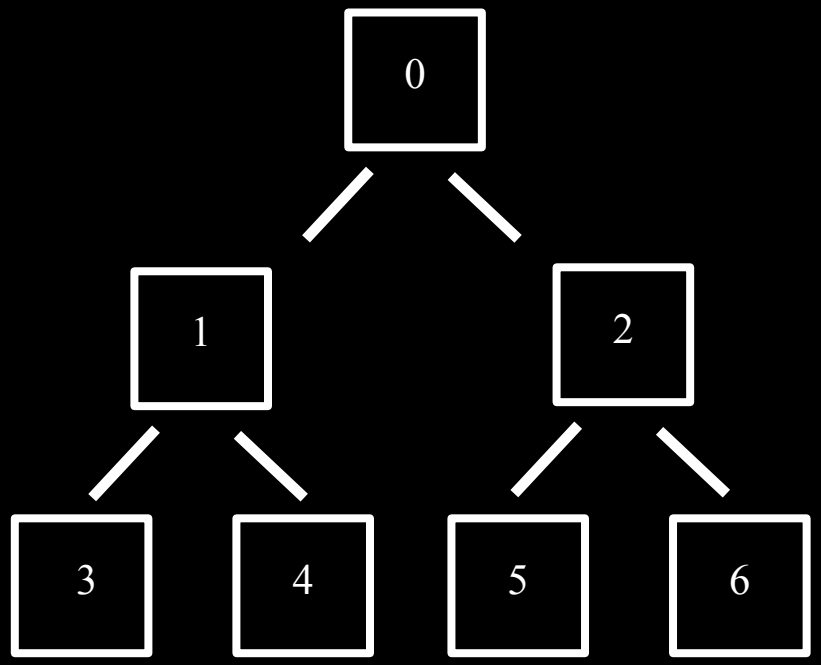
Storing Merkle Trees

More efficient to store in an array.

Left child = (n+1)*2-1

Right child = (n+1)*2

(A little adjustment is needed when indexing from 0).



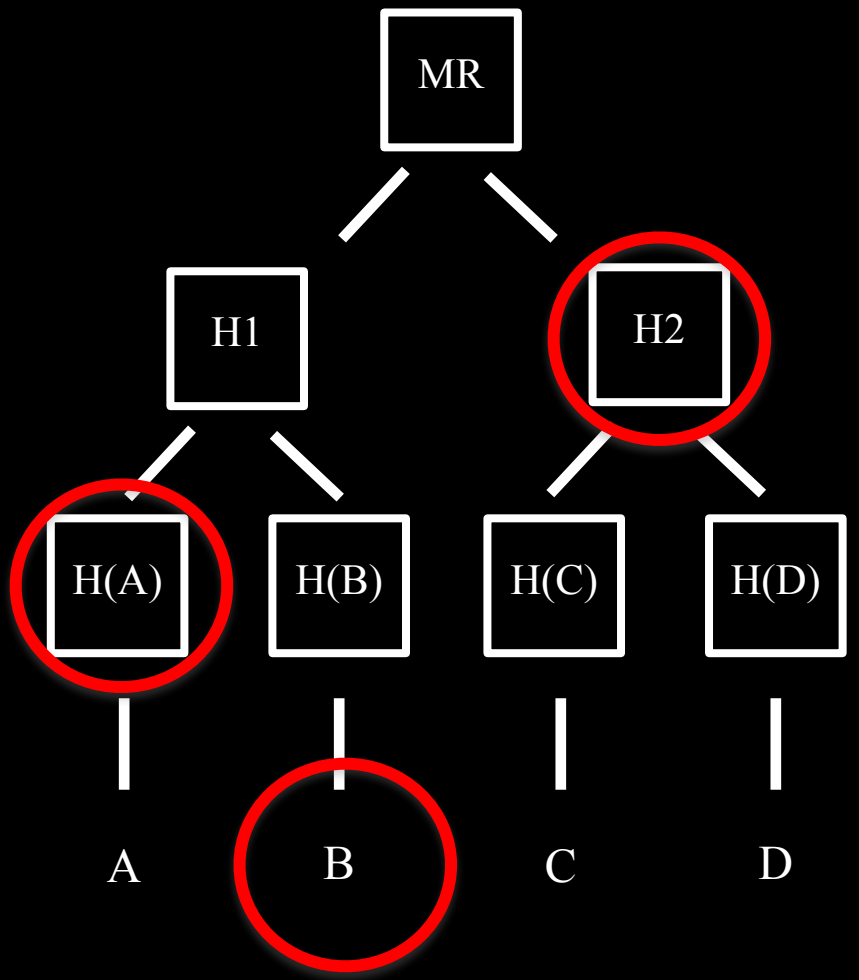
Using Merkle Trees

- Merkle root is known
- Validator requests specific transaction
- Miner provides Merkle path
  - Pieces needed to reconstruct Merkle root

Merkle Path

Merkle path for transaction B:

- Transaction B
- H(A)
- H2



Why a Merkle Tree?

- Log n hashes to verify a transaction
- Minimal data needed to transmit across the network
- Old transactions may be pruned

Reading for Upcoming Classes

- Mastering Bitcoin, Chapters 1-2
  - Bitcoin overview and history
- Mastering Bitcoin, Chapter 9
  - Reviews the blockchain
- Mastering Bitcoin, Chapter 10
  - Reviews mining and consensus

Lab: Implement a Merkle Tree

Details in Canvas and course website.