Blockchain Technology and Applications

CS 731

Merkle Trees

Dr. Ir. Angshuman Karmakar

IIT Kanpur

Teaching assistants

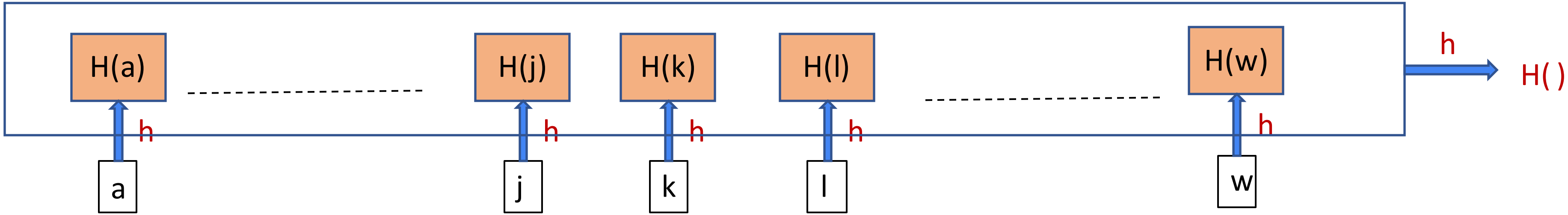
- **Sumit Lahiri** (sumitl@cse.iitk.ac.in)
- **Chavan Sujeet** (sujeetc@cse.iitk.ac.in)
- **Indranil Thakur** (indra@cse.iitk.ac.in)

Merkle trees

- Blockchain --> linked list with hash pointers?
- Binary trees?
  - Merkle trees
- There are many transactions in a block
  - How will you prove that a transaction exists in a block?
- How to stop tampering transactions in the blockchain?
- We want to get a single hash for all the transactions

Merkle trees

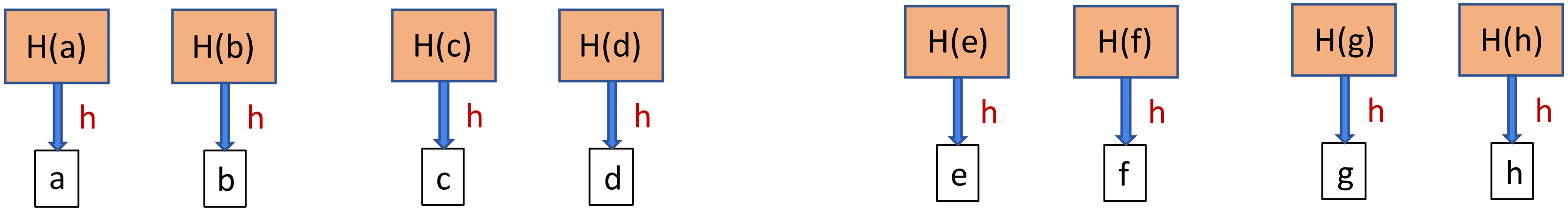
- Naïve way



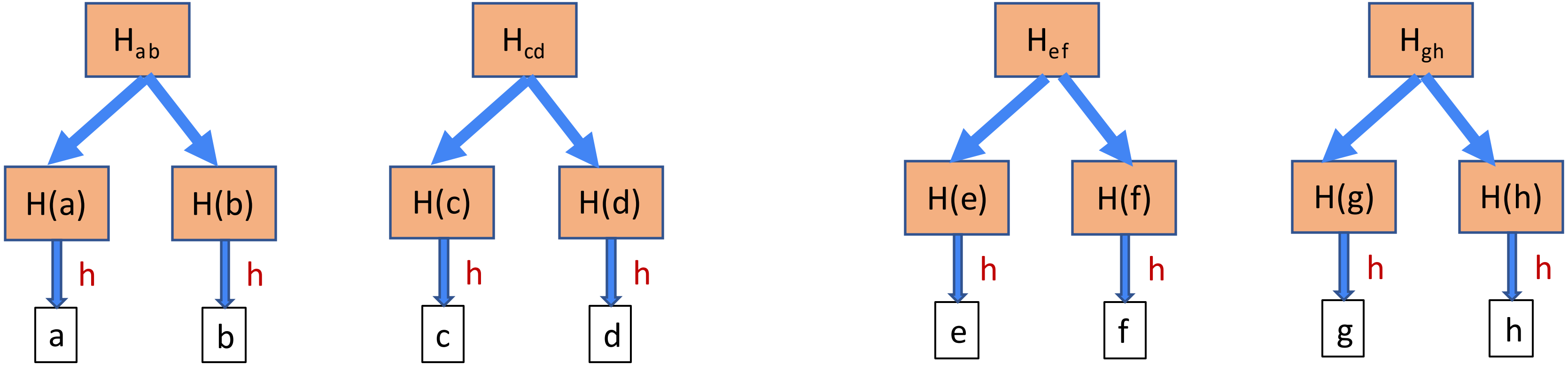
- Proof-of-membership
- Proof of non-tampering
  - O(n)
- Lots of operations
- Have to download the full block

Merkle trees

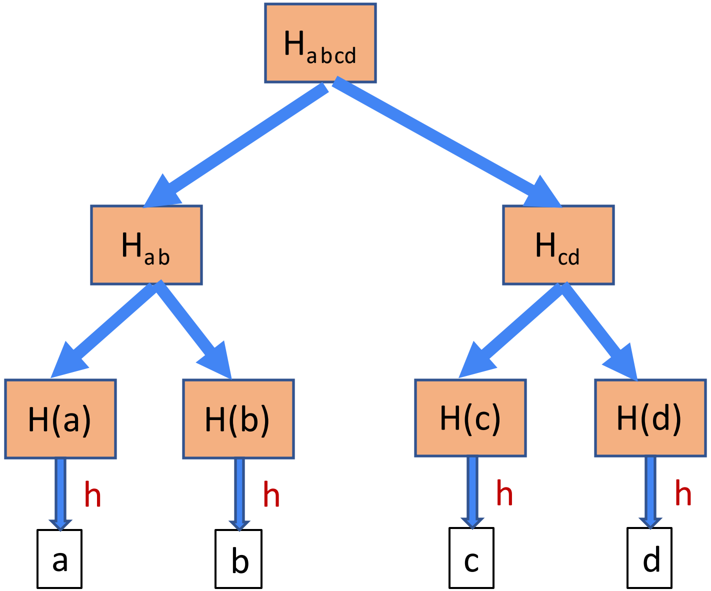
- Binary tree using hash pointers
  - Named after its inventor Ralph Merkle

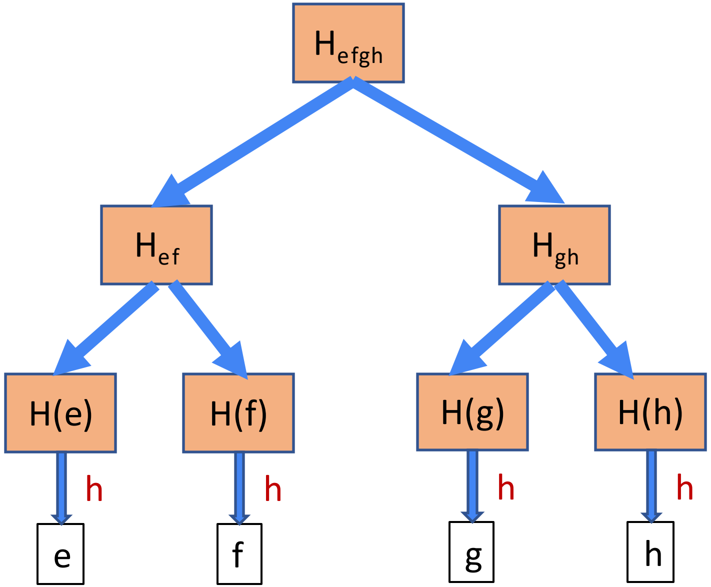


Merkle trees

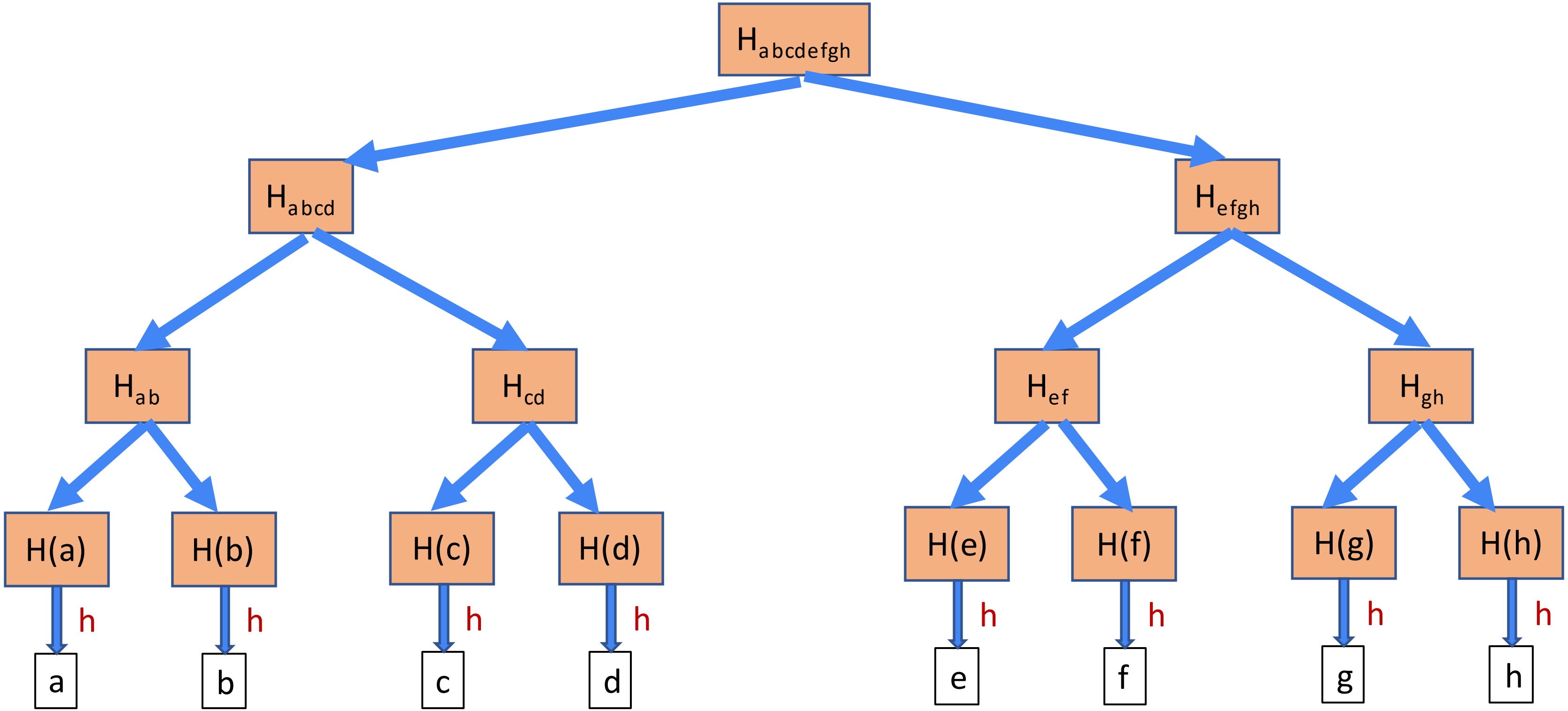


Merkle trees



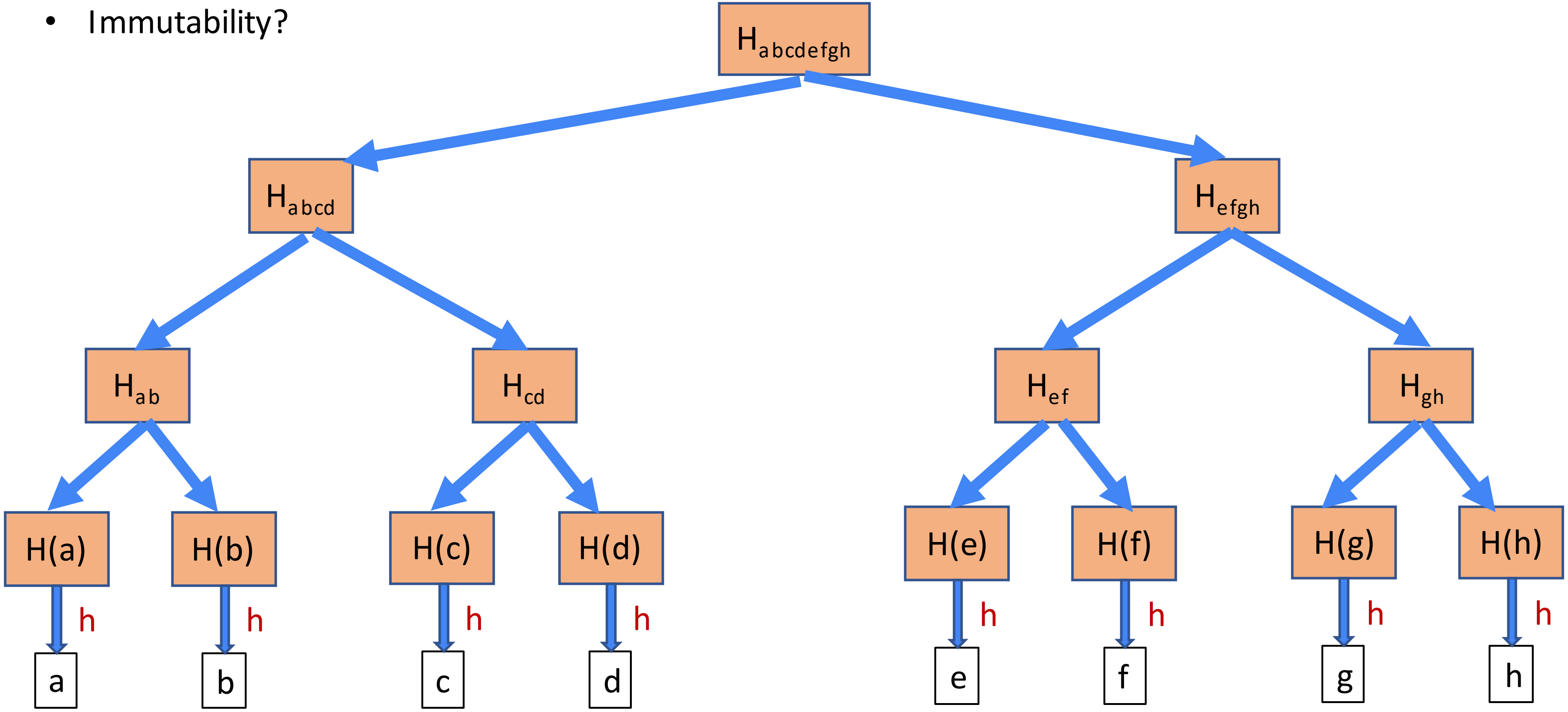


Merkle trees



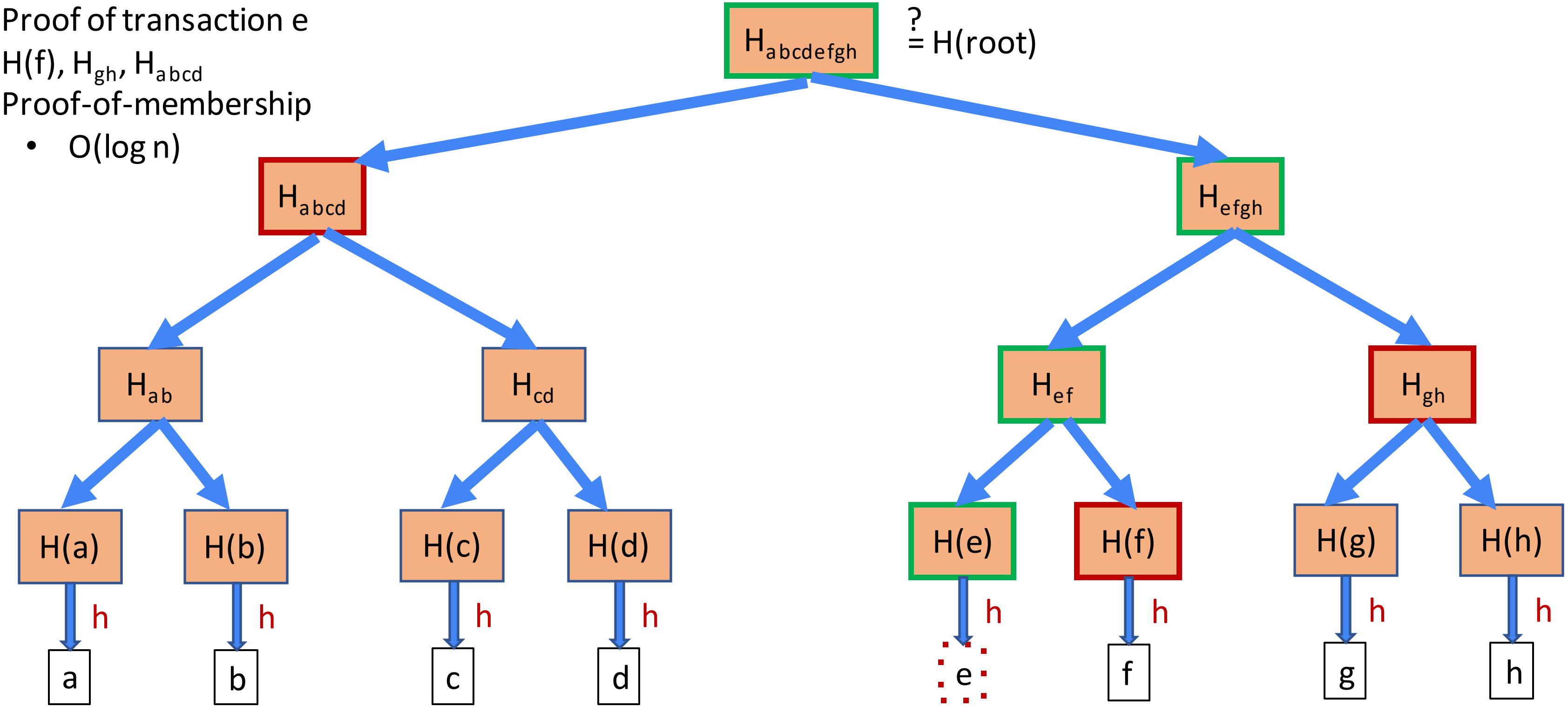
Merkle trees

- Immutability?



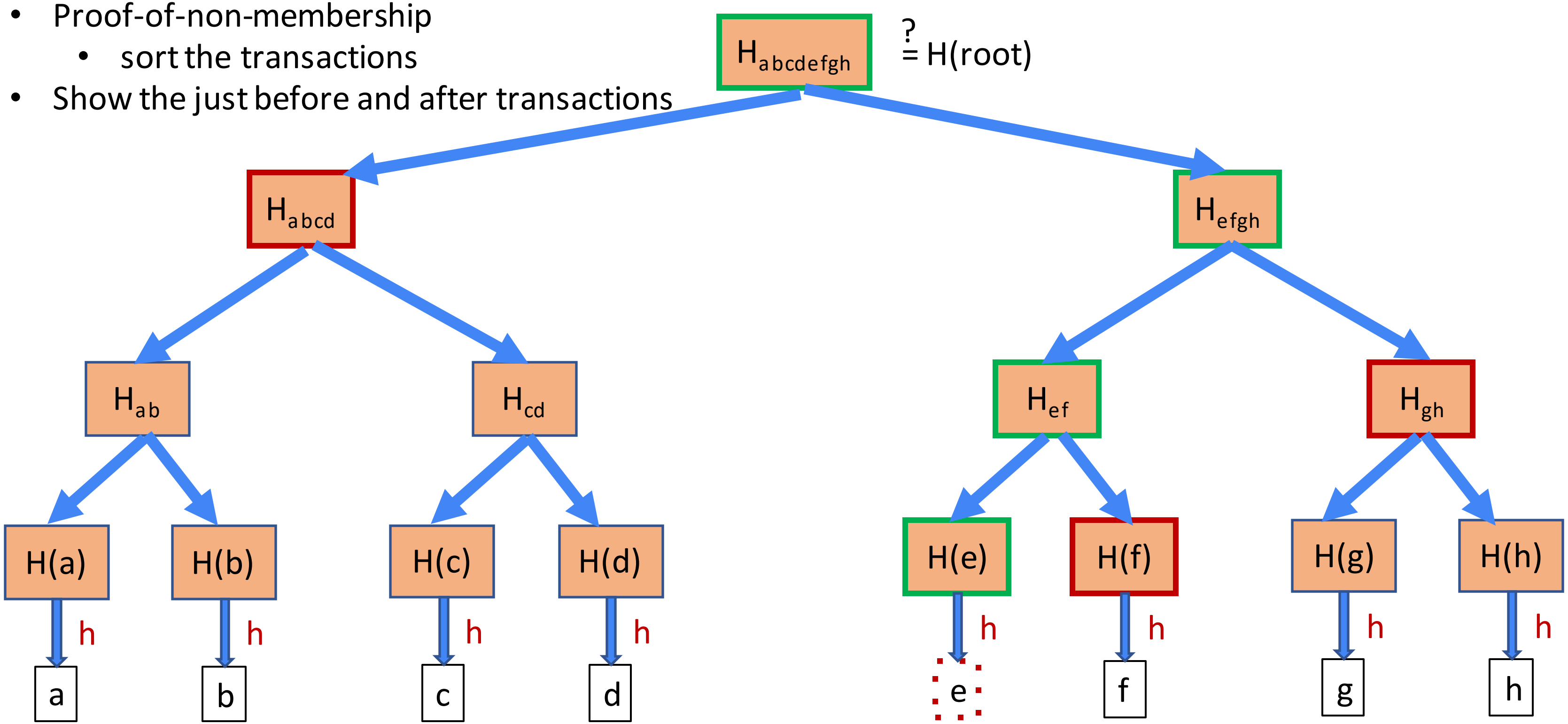
Merkle trees

- Proof of transaction e
- H(f), H_{gh}, H_{abcd}
- Proof-of-membership
  - O(log n)



Merkle trees

- Proof-of-non-membership
    - sort the transactions
- Show the just before and after transactions



Extensions

- Hash pointers
  - Can be used in any pointer-based data-structure
  - Acyclic (why?)
- Graphs?

Questions ?