Next time:
- Hash functions
- Autonhazard data structures

- How to build a ledger in a decentralized way
  - Bitcoin mechanics (block headers, scripts) way

HW 1 - out due Sep 21
Proj 2 - out soon Sep 28
Hash function

\[ H(\cdot): M \rightarrow T \quad |M| \rightarrow |T| \]

- gigabytes \rightarrow 32 \text{ byte} \ (\text{digest})

a collision: a pair \( m_1, m_2 \) \( m_1 \neq m_2 \) s.t. \( H(m_1) = H(m_2) \)

many collisions exist

Collision-resistant: CANNOT* find collisions
SHA-256 (Bitcoin) SHA-3 (Ethereum)
SHA-1 broken MD5 broken
Application: untrusted outsourced storage

\[ y = H(F) \xrightarrow{F} F' \xrightarrow{F} \text{Check } H(F') = y \]

Option 1: Store \( y = H(F, |F_1|, |F_2|, ..., |F_n|) \)

Option 2: Store \( y_1 = H(F_1), y_2 = H(F_2) \)

Option 3: Merkle Tree (Merkle 1980)
Option 3: Merkle Tree (Merkle 1980)

\[ h_1 = H(F_1) \]
\[ h_2 = H(F_2) \]
\[ h_3 = H(F_3) \]
\[ h_4 = H(F_4) \]
\[ h_5 = H(n, 11h_2) \]
\[ h_6 = H(h_3 \| h_4) \]
\[ \text{Root} = h_9 = H(h_5 \| h_6) \]

Given root, \( F_2 \), how to check integrity:

Need proof = \[ h_1, h_6 \]

Check root = \[ H(h_5 \| h_6) \]

= \[ H(H(n, 11h_2) \| h_6) \]

Proof size? \( O(n \log N) \approx 32 \text{ bytes} \)

Prove exclusion?
If sorted, show neighbors
Merkle tree is an **Authenticated Data Structure**

Take any "pointer-based data structure", replace pointers w/ hashes

\[ \Rightarrow \text{Authenticated data structure} \]

- Binary tree $\rightarrow$ Merkle tree
- FS hierarchy $\rightarrow$ ?
- Linked Prefix tree $\rightarrow$ Blockchain Merkle Prefix tree $M(x) \rightarrow y$

(root/head)
Bitcoin blockchain

- tx-root
- tx0
- tx1
- "coinbase"
- extra nonce
- mint 12.5 BTC
- tx2
- tx3
- ... tx6
- head
{  
  "hash": "000000000000000000013fa0db3570a8c7f20baabdf2e8e2a8e4dd74a6f83463ef",
  "ver": 3,
  "prev_block": "0000000000000000392392c2dd2eba4baf32281a57a1e3fdb703a427eb6bf25",
  "mrkl_root": "89463ffe9363eb2e406ea82f3d25606b462f8c029342948fb826146d57112e44",
  "time": 1443367529,
  "bits": 403867578,
  "nonce": 3763501186,
  "n_tx": 373,
  "size": 283879,
  "tx": [  
  
  ],
  "mrkl_tree": [  
  "b6c2dc5e1661072c1540a7b5b5effb3618cd316274fb97d99c86ba18b2b38f7e",
  "ccfa5a40d5fe9059330b190ef069efc5bcfc3e0929ae18d9c266e7087b6934e0f",
  "3978ecb2efbcf91ebca088cda65f5757f26fb92b843ccc6f3853854821003c47",
  ],
}

Bitcoin block header

{
  "hash": "0000000000000000013fa0db3570a8c7f20baabdf2e8e2a8e4dd74a6f83463b", 
  "ver": 3, 
  "prev_block": "00000000000000000392392c2d2eba4baf32281a57a1e3f9fb703a429cb", 
  "mrkl_root": "89463ffe9363eb2e406ea82f3d25606b462f8c029342948fb826146d57", 
  "time": 1443367529, 
  "bits": 403867578, "3" mining data 
  "nonce": 3763501186, 
  "n_tx": 373, 
  "size": 283879, 
  "tx": [ 
    ... 
  ],
  "mrkl_tree": [ 
    "b6c2dc5e1661072c1540a7b5b5effb3618cd316274fb97d99c86ba18b2b38f7e", 
    "ccfa5a405f6e9059330b190ef069efc5bfcf3e0929ae18d9c266e7087b6934e0f", 
    "3978ecb2efbcaf91ebca088cda65f5757f26fb92b843ccc6f3853854821003c47", 
    ... 
  ]
}
Blockchain Size
Source: blockchain.info
Consensus

UT signatures by a TTP (bank)

```
\[ \text{sign}(\text{key}) \rightarrow \text{sign}(\text{key}) \]
```

"Centralized Blockchain"
"Permissioned Blockchain"

Problems:
1) Easy to fork / equivocate
2) DoS / censorship / freezing
3) Bank can get hacked / go offline
4) Invalid tx?
5) Monopolist stagnation
V2 t-of-n signers

- who chooses n, t?
- who approves signers?
- how to agree on block contents?
- voting

Byzantine agreement
Paxos
U3: Rotating signers vs designated signers

Rule:
- Extend longest valid chain + honest majority

longest chain is valid
Nakamoto consensus (Bitcoin)

- no signing of blocks

but blocks are hard to find

require solving a computational puzzle
Proof-of-work assumption

"Puzzle friendliness": No faster way to find n than trial-and-error / brute force
memoryless progress-free
Bitcoin's puzzle (PoW) Proof-of-work

Given: block header $b$
Find: nonce $n$

s.t.
$$H(b || n) \leq \text{target} = 2^{256-p}$$
$$d = \text{difficulty} \approx 70$$
Nakamoto consensus

- Puzzle
- Puzzle
- Puzzle
- Puzzle
- Puzzle
- Puzzle
51% attacker 😞
Next time:
- Hash functions
- Authenticated data structures
- How to build a ledger in a decentralized way
- Bitcoin mechanics (block headers, scripts) way

HW 1 - out due Sep 21
Proj 2 - out soon Sep 28
Hash function

\[ H() : M \rightarrow T \quad |M| \rightarrow |T| \]

a collision: a pair \( m_1, m_2 \) \( m_1 \neq m_2 \) such that \( H(m_1) = H(m_2) \)

many collisions exist

Collision-resistant: cannot find collisions

SHA-256 (Bitcoin) SHA-3 (Ethereum)
SHA-1 broken MD5 broken
Application: untrusted outsourced storage

\[ y = H(F) \]
\[ F' \]

Check: \( H(F') = y \)

Option 1: Store \[ y = H(F, \ldots, F_n) \]

Option 2: Store \[ y_1 = H(F_1), y_2 = H(F_2) \]

Option 3: Merkle Tree (Merkle 1980)
Option 3: Merkle Tree (Merkle 1980)

\[ h_1 = H(F_1) \]
\[ h_2 = H(F_2) \]
\[ h_5 = H(h, 11h_2) \]
\[ h_3 = H(F_3) \]
\[ h_4 = H(F_4) \]
\[ h_6 = H(h_3 \| h_4) \]
\[ \text{Root} = h_9 = H(h_5 \| h_6) \]

Given root, \( F_2 \), how to check integrity

Need proof = \{ \( h_1 \), \( h_6 \) \}

check root = \( H(h_5 \| h_6) \)

\[ = H(H(h, 11h_2) \| 11h_6) \]

Proof size? \( O(hgN) \) \( \lceil \log_2 N \rceil \). 32 bytes

Prove Exclusion?
If sorted, show neighbors
Merkle tree is an **Authenticated Data Structure**

Take any "pointer-based data structure", replace pointers w/ hashes

\[ \implies \text{Authenticated data structure} \]

Binary tree $\implies$ Merkle tree

FS hierarchy $\implies$ ?

Linked Prefix tree $\implies$ Blockchain Prefix tree $M[x] \rightarrow y$

(root/head)

[Diagram of a Merkle tree with a root and a leaf node labeled head.]
Bitcoin blockchain

(tx-root) ← (tx-0) ← (tx-1)

(tx-2) ← ... ← (tx-6)

"Coinbase"
→ extra nonce
→ mint 12.5 BTC
Bitcoin block header

{
  "hash": "0000000000000000013fa0db3570a8c7f20baabdf2e8e2a8e4dd74a6f83463c6",
  "ver": 3,
  "prev_block": "00000000000000000392392c2dd2eba4baf32281a57a1e3fdb703a427a",
  "mrkl_root": "89463ffe9363eb2e406ea82f3d25606b462f8c029342948fb826146d57",
  "time": 1443367529,
  "bits": 403867578, 3 mining data,
  "nonce": 3763501186,
  "n_tx": 373,
  "size": 283879,
  "tx": [
    ...
  ],
  "mrkl_tree": [
    "b6c2dc5e1661072c1540a7b5b5effb3618cd316274fb97d99c86ba18b2b38f7e",
    "ccfa5a40d5fe9059330b190ef069efc5bcf3e0929ae18d9c266e7087b6934e0f",
    "3978ecb2efbcf91ebca088cda65f5757f26fb92b843ccc6f3853854821003c47",
    ...
  ]
}
{
    "hash": "0000000000000000013fa0db3570a8c7f20baabdf2e8e2a8e4dd74a6f83463ef",
    "ver": 3,
    "prev_block": "0000000000000000000000392392c2dd2eba4baf32281a57a1e3f6b703a427eb6bf25",
    "mrkl_root": "89463ffe9363eb2e406ea82f3d25606b462f8c029342948fb826146d57112e44",
    "time": 1443367529,
    "bits": 403867578,
    "nonce": 3763501186,
    "n_tx": 373,
    "size": 283879,
    "tx": [
        ...
    ],
    "mrkl_tree": [
        "b6c2dc5e1661072c1540a7b5b5effb3618cd316274fb97d99c86ba18b2b38f7e",
        "ccfa5a40d5fe9059330b190ef069efc5bcfc3e0929ae18d9c266e7087b6934e0f",
        "3978ecb2efbc91ebca088cda65f5757f26fb92b843ccc6f3853854821003c47"
    ],
}
Blockchain Size
Source: blockchain.info

MB 42,783
Consensus

UI signatures by a TTP (bank)

↓↓↓

"Centralized Blockchain"
"Permissioned Blockchain"

Problems:
1) Easy to fork / equivocate
2) DoS / censorship / freezing
3) Bank can get hacked / go offline
4) invalid tx?
5) Monopolist stagnation
V2 \( t \cdot (n - \text{signers}) \)

- who chooses \( n, t \)?
- who approves signers?
- how to agree on block contents?
  - voting

Byzantine agreement
Paxos
V3: Rotating signers vs designated signers

Rule:
- Extend longest valid chain + honest majority

longest chain is valid
V4: Nakamoto consensus (Bitcoin)

- no signing of blocks

but blocks are hard to find

require solving a computational puzzle
Proof-of-work assumption

"Puzzle friendliness"

No faster way to find $n$ than trial-and-error / brute force
memoryless progress-free
Bitcoin's puzzle (PoW) Proof-of-work

Given: block header $b$

Find: nonce $n$

s.t. $H(b || n) \leq \text{target} = 2^{256 - p}$

$d = \text{difficulty} \approx 70$
Nakamoto consensus

---

- Puzzle
- Solve
- X
- Publish
- Publish
51% attacker