EECS 575: Advanced Cryptography
Fall 2021
Lecture 24

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- Cryptocurrencies: an overview
- Merkle trees, authenticated data structures
- Append-only logs

Agenda for this lecture

- Announcements
- Recap from last time
- Cryptocurrencies: an overview
- Merkle trees, authenticated data structures
- Append-only logs

Announcements

- Take-home exam 2 is due next Monday 12/6

Recap from last time

* Secure 2PC, Yao's garbled circuits
  - See more in 498/598
* Collision-resistant hash functions

$$h_s : \{0,1\}^* \to \{0,1\}^n \text{ is CR}$$

if

$$\Pr_{s \leftarrow \{0,1\}^\lambda}\left[x, x' \leftarrow \mathcal{A}(s) : x \neq x' \wedge h_s(x) = h_s(x')\right] = \text{negl}(n)$$

SHA-256

Recap from last time

* Digital sigs

SIG = (Gen, Sign, Ver)

  * Gen: outputs (vk, sk)
  * Sign(sk, m): outputs σ
  * Ver(vk, m, σ): outputs 0/1

UF-CMA: can't forge new signatures, even given sigs on other messages.

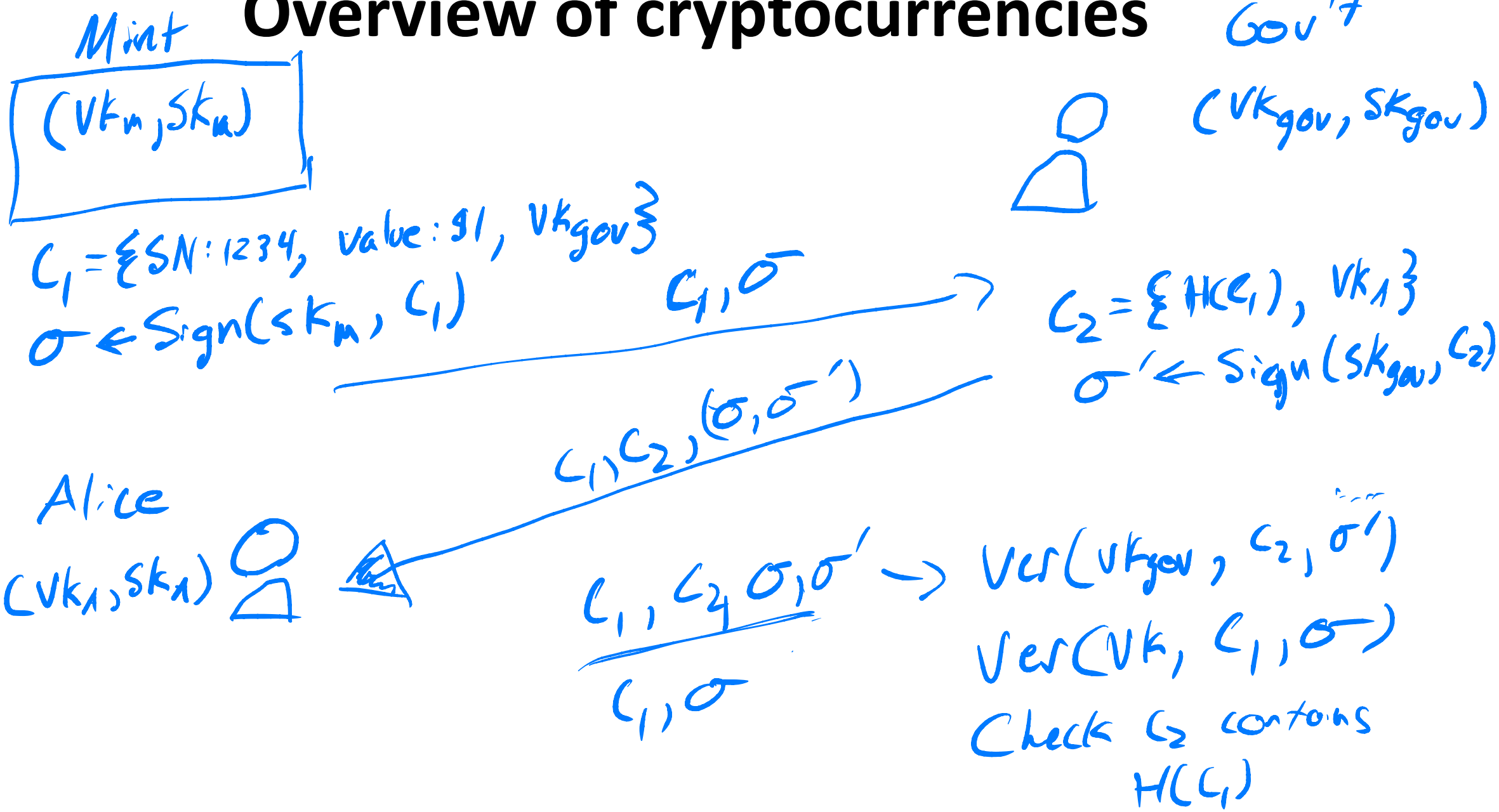
* FDH in class; not used in cryptocurrencies

Schnorr, ECDSA (exists b/c of patent)

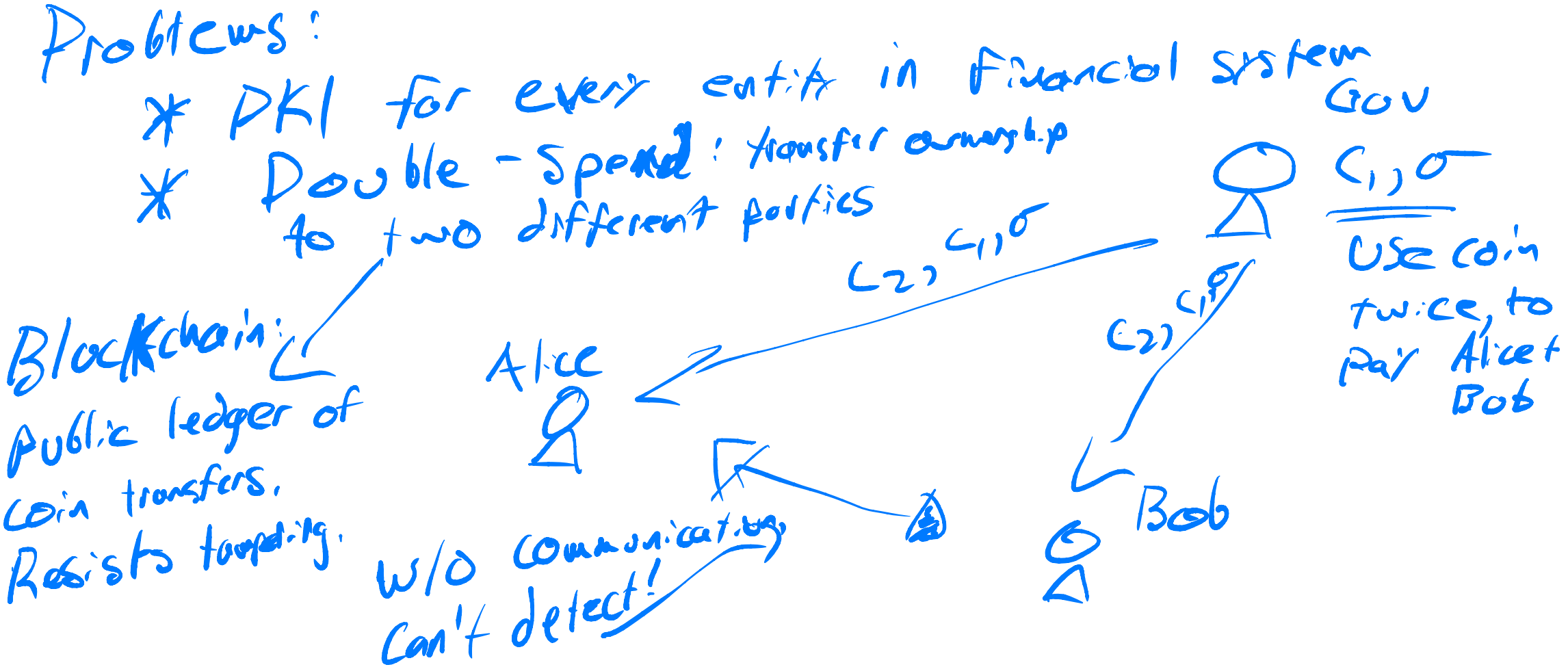
Agenda for this lecture

- Announcements
- Recap from last time
- Cryptocurrencies: an overview
- Merkle trees, authenticated data structures
- Append-only logs

Overview of cryptocurrencies



Overview of cryptocurrencies



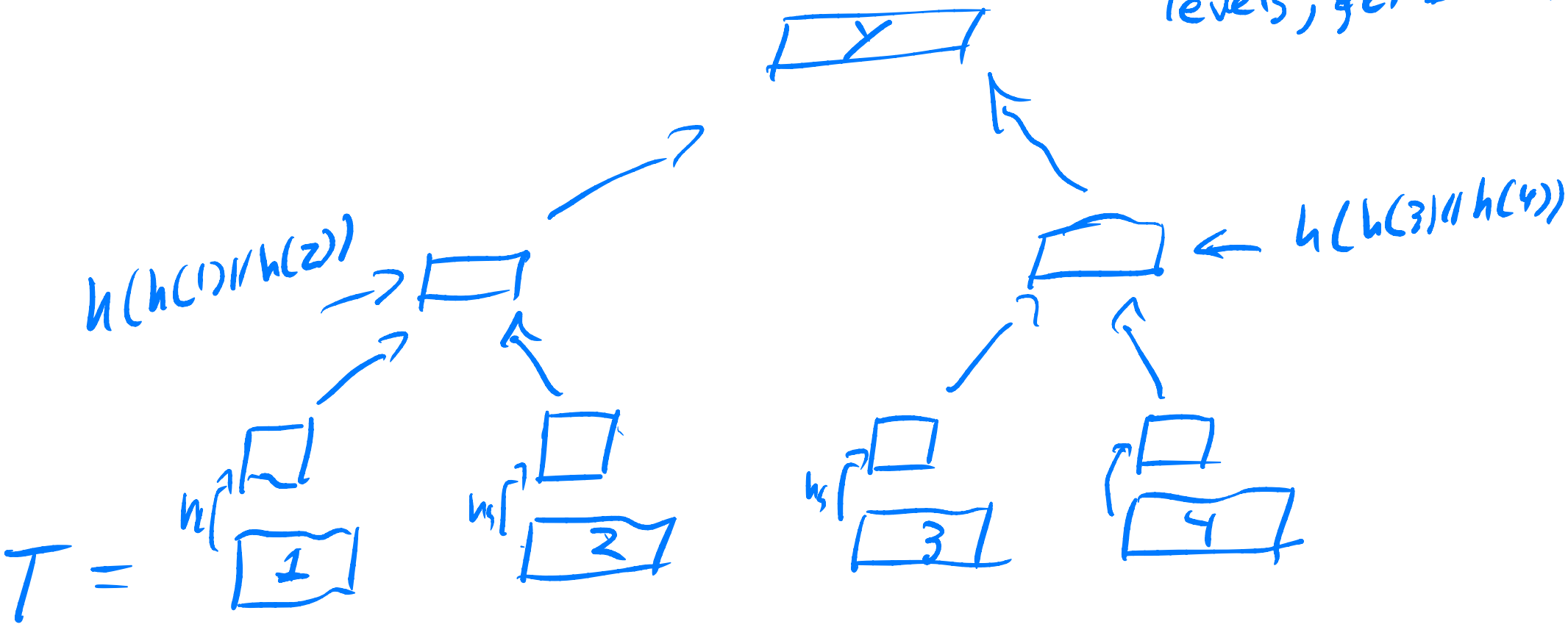
Agenda for this lecture

- Announcements
- Recap from last time
- Cryptocurrencies: an overview
- Merkle trees, authenticated data structures
- Append-only logs

Merkle trees

$h_S : \{0,1\}^{2n} \to \{0,1\}^n$

Make tree of hashes, after $\log(N)$ levels, get 1 hash.



Crucial property: short inclusion proofs

Merkle trees

$T = (X_1, \ldots, X_n)$

$\gamma = \text{MerkleTree}(T)$

"Hash"

T →

Give me X_B →

"prove"

Compute π:

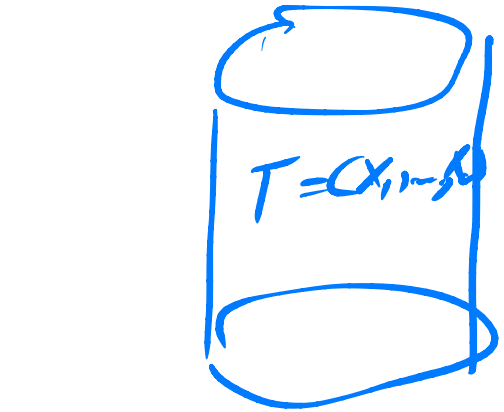
X is $T[B]$

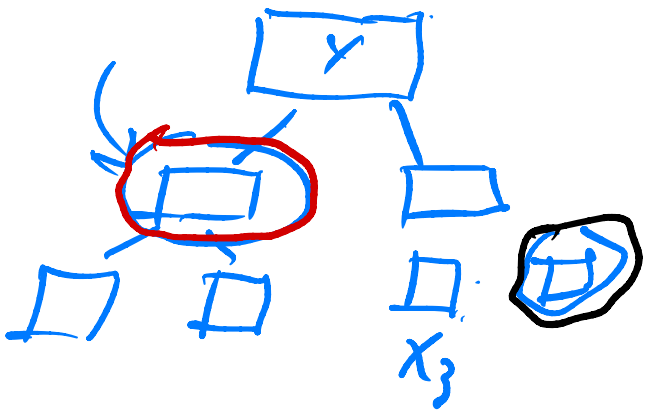
← $X, \pi = (x_4, H(H(x_1)\|H(x_2)))$

Verify proof

"verify"

In general: siblings $_T$ = of nodes on path to root From x_i





Authenticated Data Structures

An ADS $\mathcal{D} = (H, P, V)$. Algs. defined $\mathcal{X}^n, \mathcal{Y}, \mathcal{P}$

* $H: \mathcal{X}^n \to \mathcal{Y}$
  $H(T) = y$
* $P: [n] \times \mathcal{X} \times \mathcal{X}^n \to \mathcal{P}$
  $P(i, x, T) = \pi$
  Proves, e.g., x is $T[i]$.
* $V: [n] \times \mathcal{X} \times \mathcal{Y} \times \mathcal{P} \to 0/1$
  $V(i, x, y, \pi) = 0/1$

ADSSec$^{\mathcal{D}}_{\mathcal{A}}$:

$y, i, (x, \pi), (x', \pi') \leftarrow \mathcal{A}$

Ret $x \neq x'$
$\wedge\ V(i, x, y, \pi) = 1$
$\wedge\ V(i, x', y, \pi') = 1$

Exercise:

Express Merkle tree as ADS, prove

Theorem: If h_s is CR, Merkle tree is ADSSec.

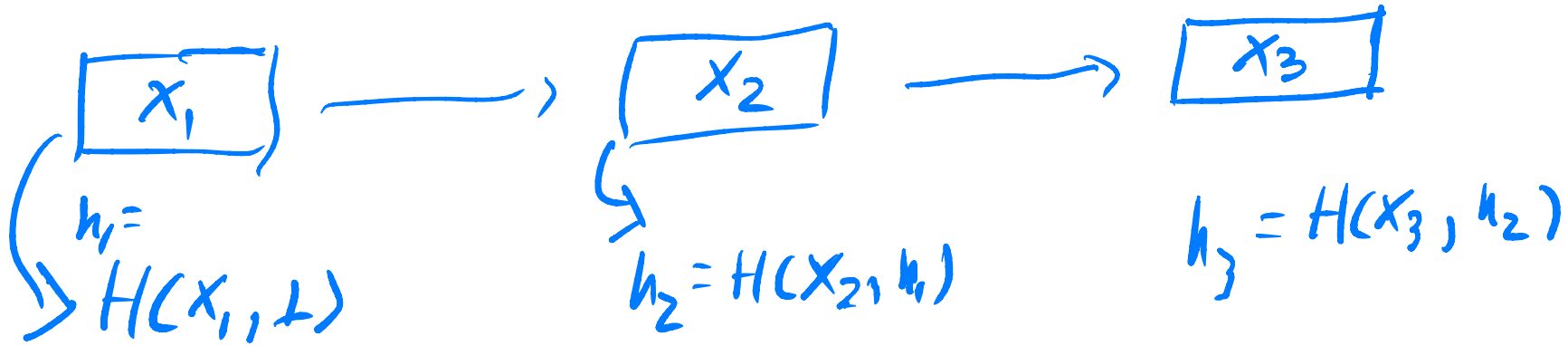
Compare to collision-resistance for hash fn

Agenda for this lecture

- Announcements
- Recap from last time
- Cryptocurrencies: an overview
- Merkle trees, authenticated data structures
- Append-only logs

Append-only logs

Authenticated linked list



Idea:

head hash is digest; each block contains hash of previous one. If H is CR then this auth. linked list; append-only.

Blockchain: append-only log of blocks of transactions. Each transaction similar to sig-based currency; block contains Merkle digest of transactions

Still need PoW to give permission to append to log.