

CompSci 661 Week 2

✓ Blockchain Primitives

- ✓ Cryptographic hash functions
- ✓ Merkle trees
- Attack of the week!
- Blockchain diagram
- Double-spend Attack
- HW1

↓
 $Pub = F(priv)$
⇒ Pub/priv key crypto
⇒ AES
↓
 $Ciphertext = F'(secret, message)$
 $F'(H(priv), message)$

Cryptographic hash functions

Key property

#1: preimage resistance (one way hash) $x = H(y)$

hash
↓
 $x = H(y)$
Preimage
↓

Given an x you can't come up with y

→ #2: 2nd preimage resistance $H(y \oplus 4) = x$

#3: collision resistance (Birthday attack) $H(y \oplus 1)$

it is infeasible to find y & y' s.t. $H(y) = H(y')$

⇒ #4: Random oracle Property (avalanche property)

if 1 bit changes in the preimage $\sim \frac{1}{2}$ bits change in hash

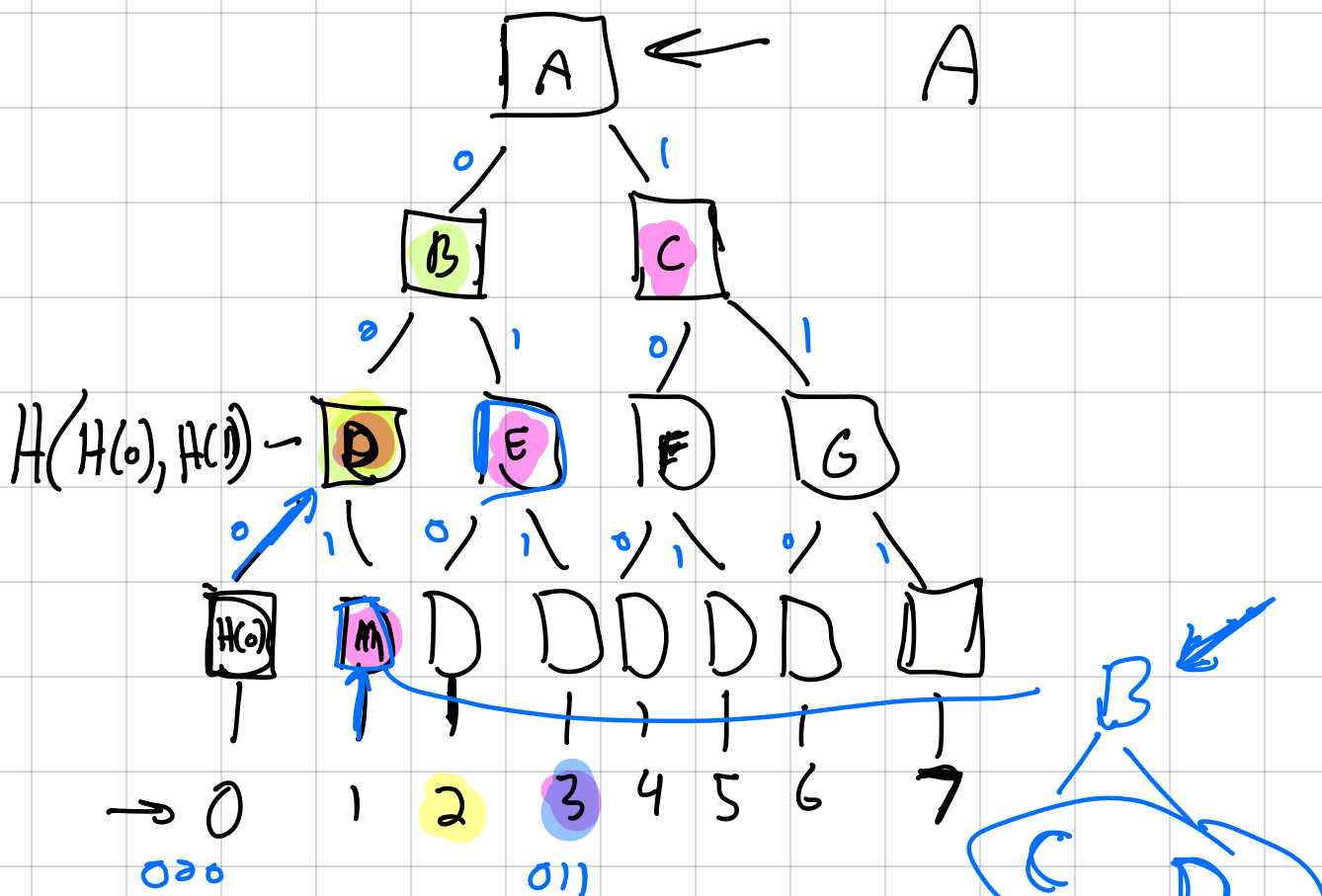
Cool Uses!

- Global pointer (SHA256) blake2b
- Bittorrent, IPFS
- Deduplication - remove redundant data in datacenters
- TOTP time-based one time Password (google Authenticator)

$$H(\underbrace{\text{time}}_{30}, \text{secret})$$

- Not storing passwords as plaintext
- $$H(\text{secret}, \text{nonce})$$
- $\uparrow$ $\uparrow$

Merkle Tree



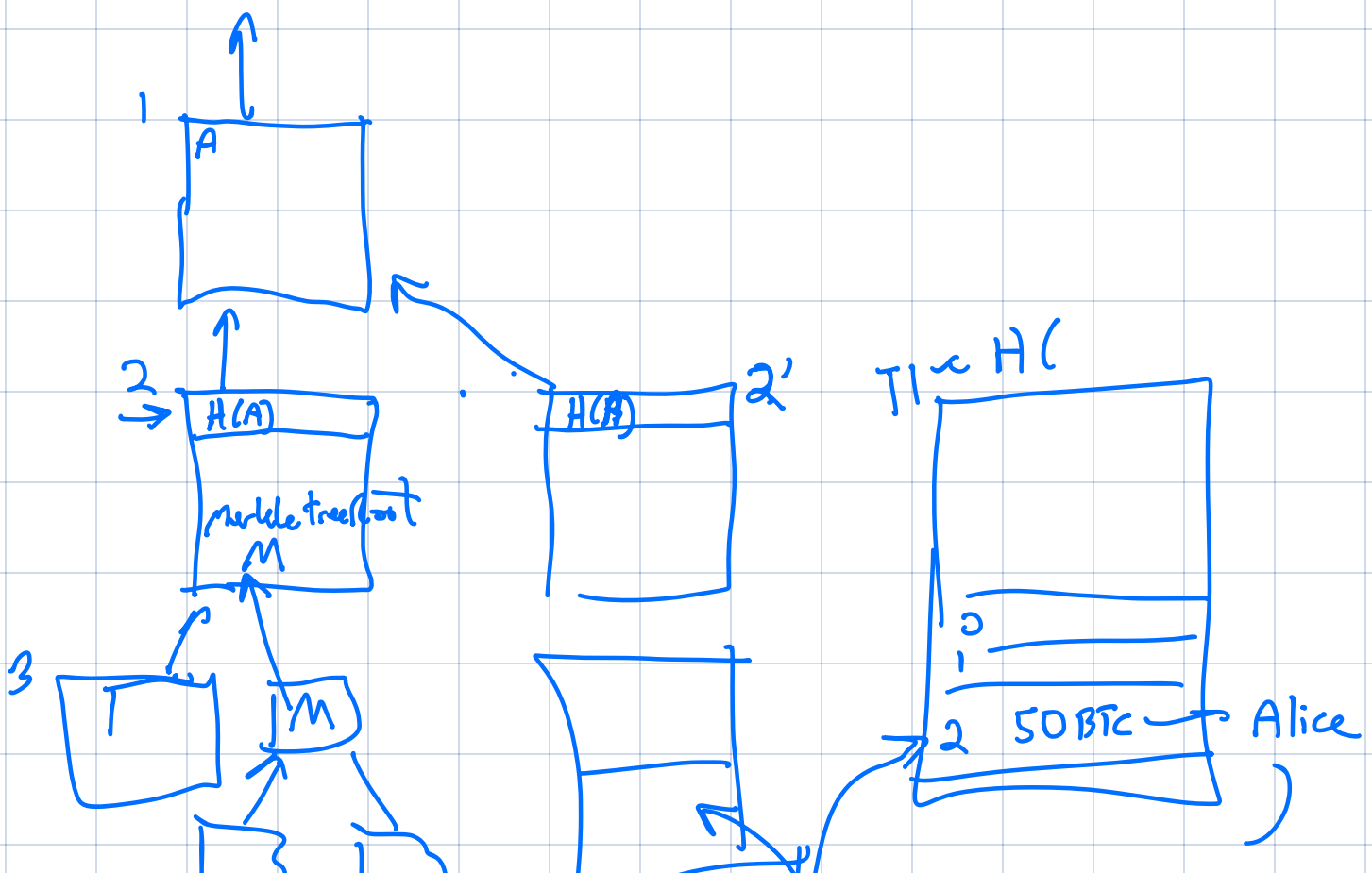
$\circ \overset{\circ}{H}(1), \overset{\circ}{E}, \overset{\circ}{C} \Leftarrow \text{Proof}$

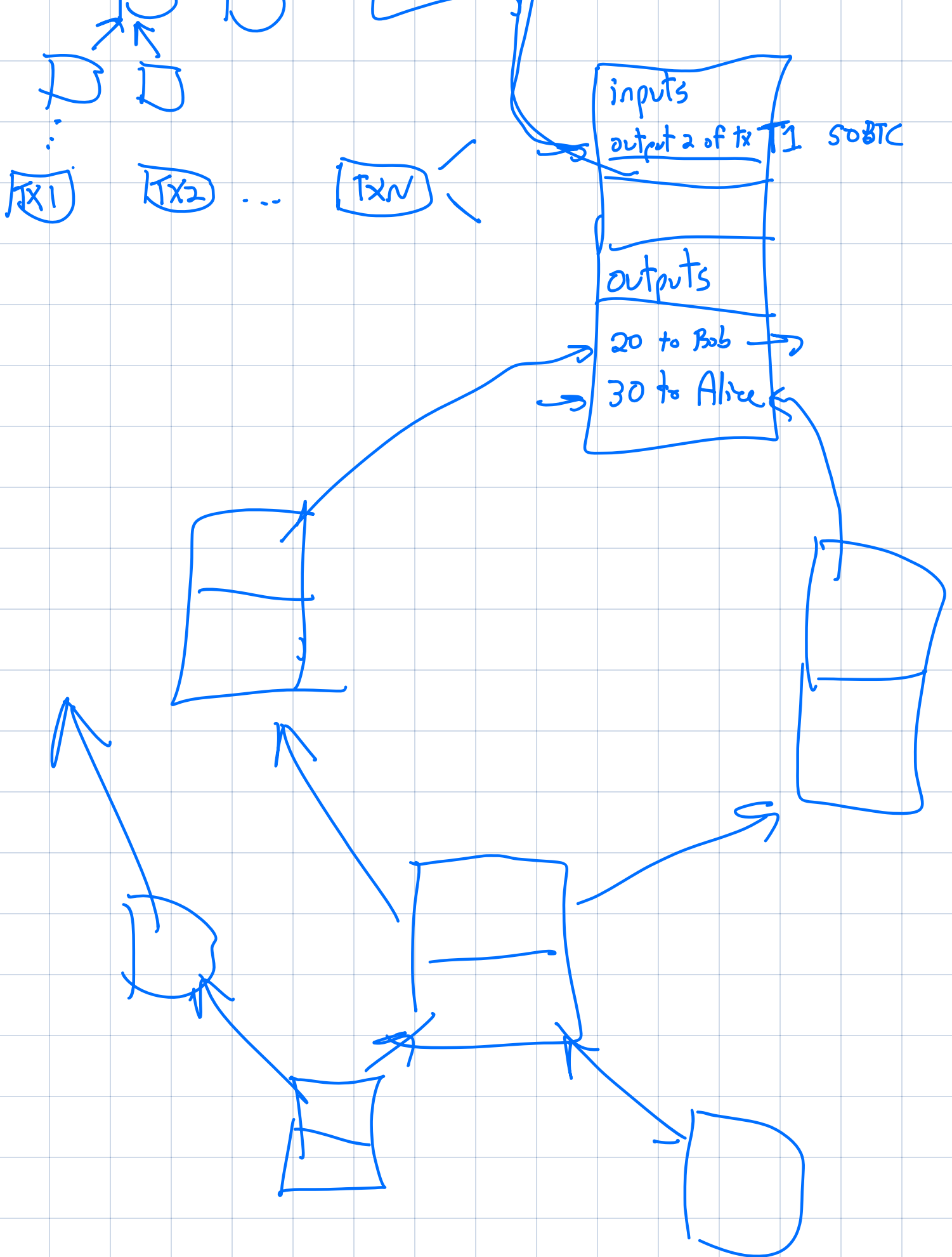
$\overset{H}{H}(H(\overset{H}{H}(0), H(1)), E), C) \Leftarrow \text{expression}$

$\exists \quad 2^R, D^R \subset F^{0/1}$

$\overset{H}{H}(H(H(3), H(2)), D), C)$

Blockchain Diagram





Txes form a DAG!