Bitcoin

What We Know So Far

- Consensus

- Cryptographic Primitives

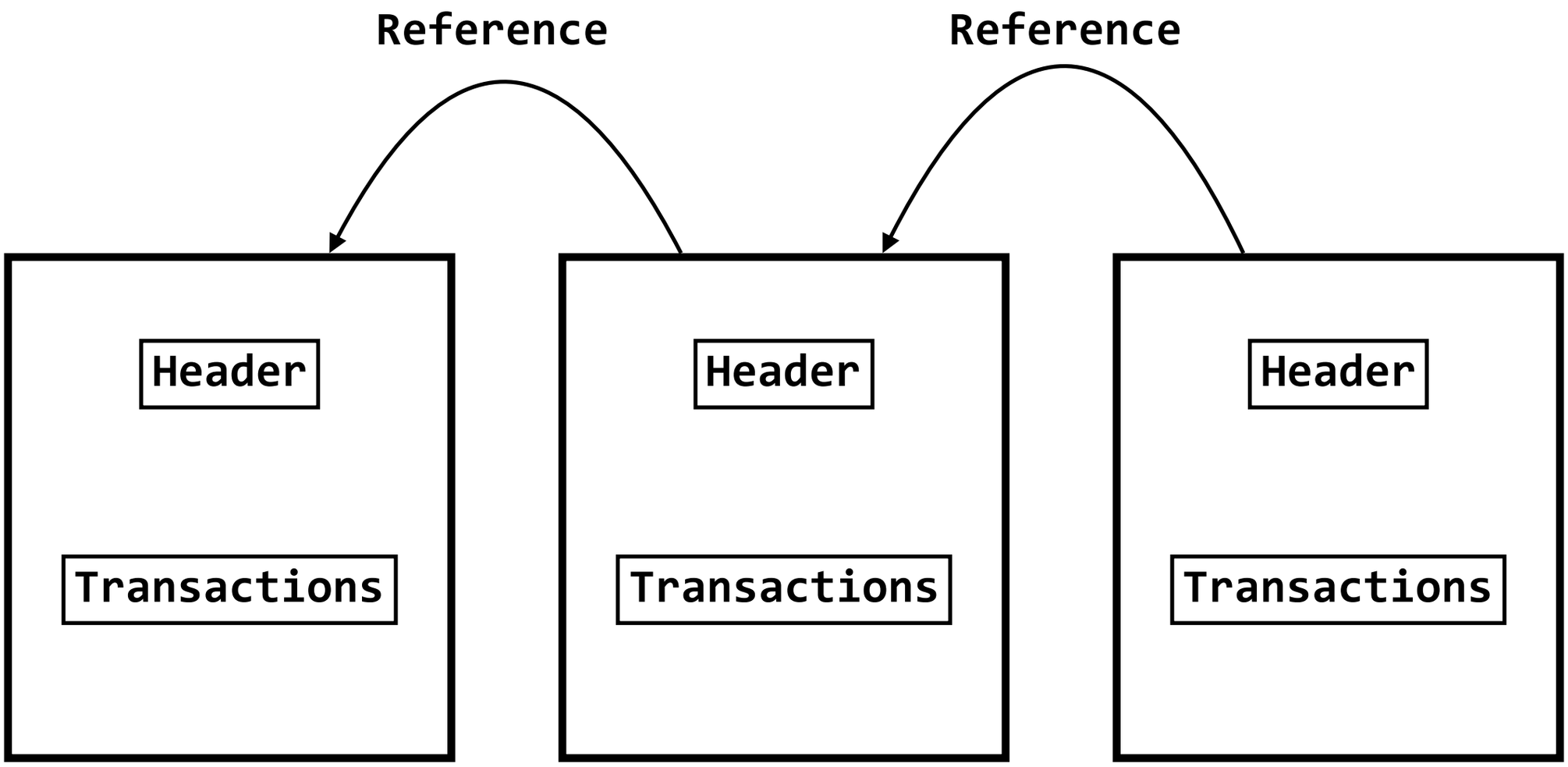
Today

- Putting It All Together

- The Bitcoin System

The First Primitive

Data Structure


Reference
Reference
Header
Header
Header
Transactions
Transactions
Transactions

How Do You Communicate?

- Broadcast
- Relay

Growing This Thing

- Add blocks
    - Which include transactions

Growing This

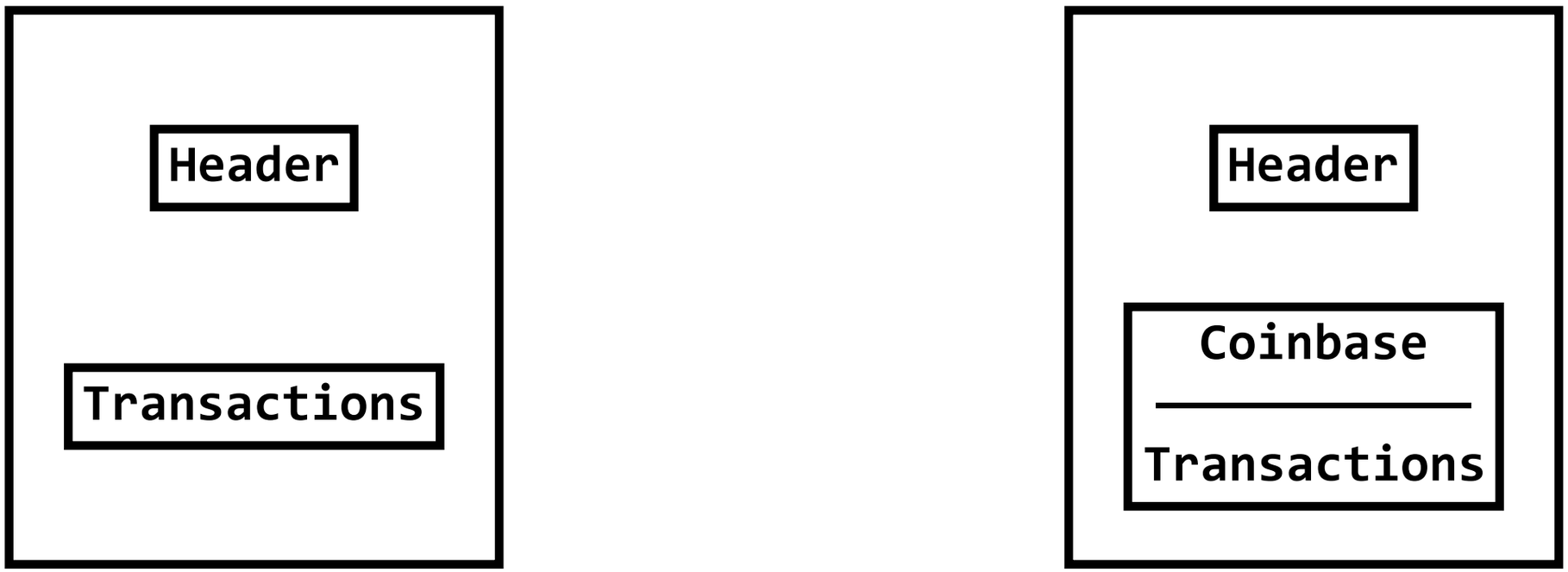
- Incentive to add blocks
- Miners
  - Full Node
- Block subsidy

The Subsidy

- 12.5 BTC

- Halves again mid-2020-ish

The Coinbase Transaction



Malicious?

- Give yourself BTC
- All manner of invalid transactions

How Do You Deter This?

Impose a Cost

- What kind of cost?
  - Computational

Ingredients

- A Preimage-Attack Resistant Hash Function
  - SHA-256
- An Evolving Challenge
  - Evolve in response to network realities

The Challenge

- $H(x) < TARGET$

X?

- Checksum of block header
  - Current protocol version
  - A reference to a prev block
  - A timestamp
  - ....
  - **NONCE**

Nonce?

- A one-time use value

Mining

- Miner can set this nonce
  - (note the rest are pretty much pre-determined)

The Challenge

- Pick that nonce

- So that the block hash < TARGET

SHA-256

- Output looks random
- Preimage attack resistant
  - One-way

TARGET

- 00000FFFFF….
- Hex string
- Probability of leading zeros?

TARGET

- SHA-256?

Proof Of Work

Some Algebra

- P = (TARGET+1) / 2^256
  - Likelihood of getting your value right
- Expected value:
  - 2^256 / (TARGET+1)

Protocol

- Approx 10 minutes per block
- So Given The Total Hash Rate (TH/s)
- Compute Expected Time for block to be mined by the network

Estimating THR

- Look at previous 2016 blocks
- Update every 2016 blocks
- DIFFICULTY

Target

- DIFFICULTY = (Difficulty target) / (current target)

An Evolving Challenge

- Total Hashing Power
- GPUs
- ASICs
- 80e6 TH/s

Protocol Limits

- 10 minutes per block
- So total # of potential hashes:
  - 60 x 10 x 80e6 hashes in this period
  - Pick a target so that expected # of trials aligns with this hash rate

Commit?

Commit

- Other miners build on top of this block

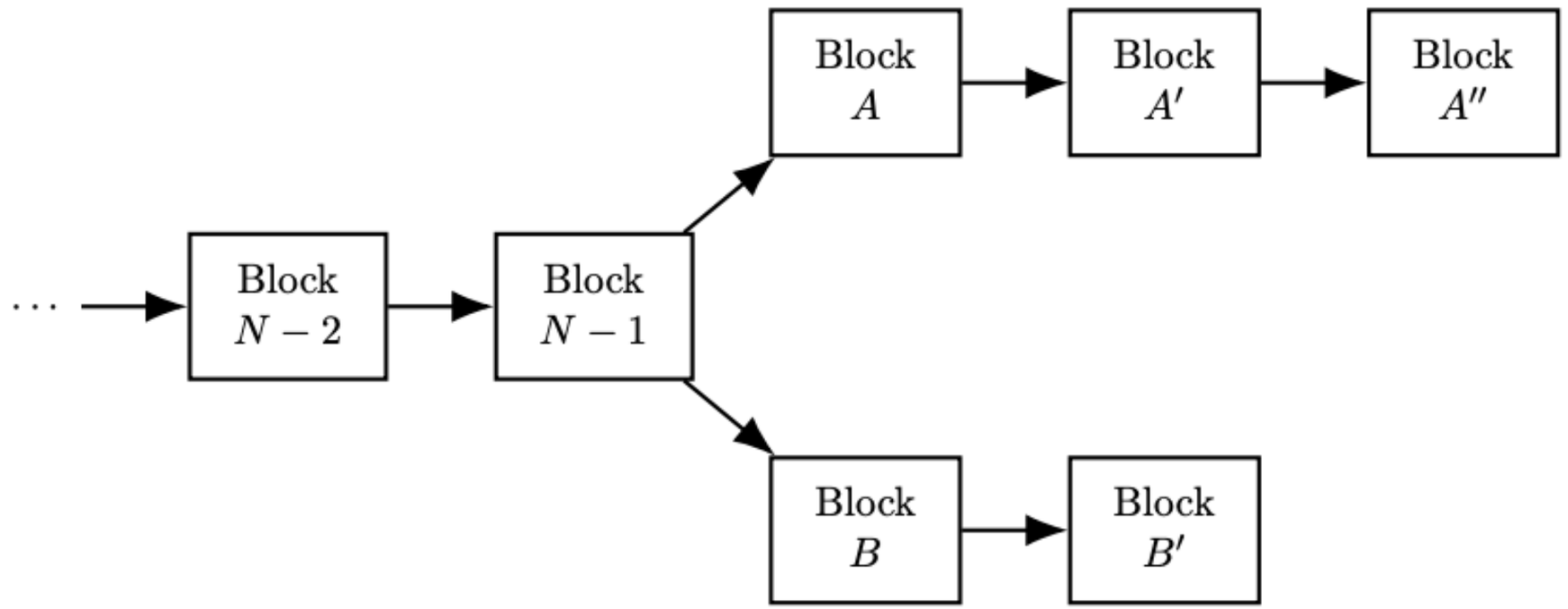
Race Conditions

2 Miners

- Both mine valid blocks
- Both broadcast their blocks to the network
- People accept both and start building on them

Fork

- It is unlikely:
  - Both branches will grow indefinitely equally
  - Someone in 1 branch will see a block from the other branch
  - PROTOCOL: Longest branch must be honored


Block
A
Block
A'
Block
A''
$\cdots$
Block
$N-2$
Block
$N-1$
Block
B
Block
B'

Fork

- Stale blocks
- All coinbase transactions are discarded
- Other transactions are part of the next pool to build blocks from

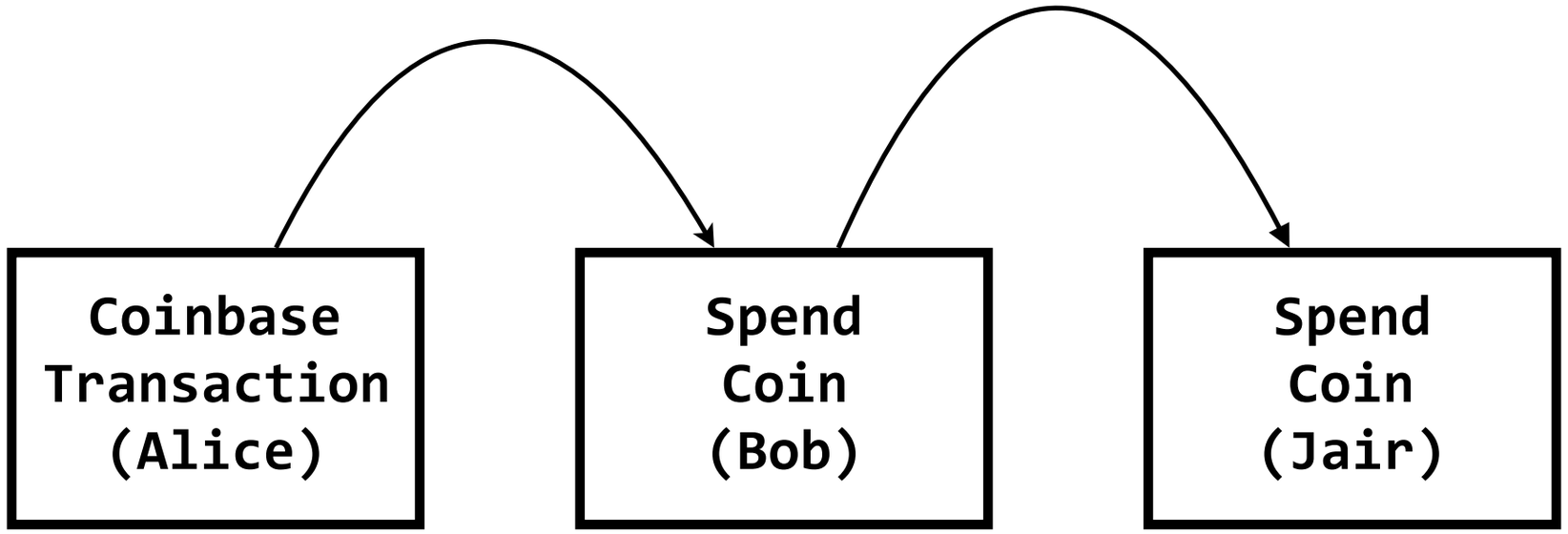
Fees

- Block Reward:
  - Block subsidy
  - Transaction Fees

Higher Fee

- Miners likelier to include your transaction
- How do you estimate what fee is good?
  - Records time of listen -> time to include
  - Reliable estimates

Tale Of A Bitcoin



Transaction Data Structure

- Input (zero or more)
- Output (one or more)

A Coinbase Transaction

- No inputs

A Regular Transaction

- (Signature (with pubkey), Amount)

Alice Gives X BTC To Bob

- (Sign_Pubkey(bob_pubkey), X)
- (One of) the output

Referencing A Txn

- Double SHA-256(txn)

Bob Spends X

- Point to where X is:
  - Txn id
  - Point to the output that contains the BTC
- Satisfy the conditions
  - (priv key)

Transaction State

- Spent
- Unspent

You Can Only Spend

- The unspent
  - UTXO

Block Header

- Merkle Tree Root: Checksum of Transactions

Double Spend

- Alice, Bob
- Alice pays Bob bitcoin
- Alice creates 2 blocks:
  - Bitcoin x paid to Bob: t1
  - Bitcoin x paid to Alice: t2

What Happens

- Only 1 of these can be in the blockchain
- Alice broadcasts t1
- Hides t2
- t1 is included in a block

And Then

- Alice begins working on t2
- Broadcasts t2 out

2 Cases

- Alice controls >= 50% of the hash rate

- Alice controls < 50% of the hash rate

Case I

- If Alice controls > 50% of the hash rate
- Alice can exclusively mine blocks assuming the block (Containing t2) is the right one
- And Alice will win

Case II

- Depends on how much compute power Alice has
- The longer you wait (i.e. more blocks built on top of the block containing t1)
  - the lower the likelihood of getting hoodwinked

Waiting

- Confirmations:
  - # of blocks passed since “the one”

Altering The Chain

- How?