COPENHAGEN
INTERNATIONAL
SOFTWARE DEVELOPMENT
CONFERENCE 2014

goto; conference

HOW THE BITCOIN PROTOCOL ACTUALLY WORKS

Jan Møller
Mycelium

Follow us @gotocph

Training: Sept 23-24 // Conference: Sept 25-26, 2014

How Does Bitcoin Actually Work?

- This talk is **not** about the political or economical impact of Bitcoin.
- This talk is **not** about how to buy, sell, spend, or secure your bitcoins.
- This talk is about how Bitcoin actually works. …you know… nerdy stuff!

How it Started

- White paper published November 2008 by Satoshi Nakamoto

"Bitcoin: A Peer-to-Peer Electronic Cash System"

- Working implementation published 3 months later as an open source project.

What is Bitcoin?

- Bitcoin is the name of a p2p protocol

  Allows a network of computers to govern all
  the rules of Bitcoin

- Bitcoin is a unit of account

  Like Euro, Danish Kroner, or gold coins

- Bitcoin is a payment System

  You can send value between accounts in the Bitcoin network

Properties of Common Digital Payment Systems

- No Counterfeiting

  YOU can't increase money supply at will

- No Double Spending

  YOU can't spend the same value more than once

- Transaction irreversibility

  YOU can't undo a transaction

Properties of Bitcoin

- No Counterfeiting

  NOBODY can increase money supply at will

- Transaction irreversibility

  NOBODY can undo a transaction

- No Double Spending

  NOBODY can spend the same value more than once

Bitcoin Solves Two Things

- Eliminates trust in a central authority

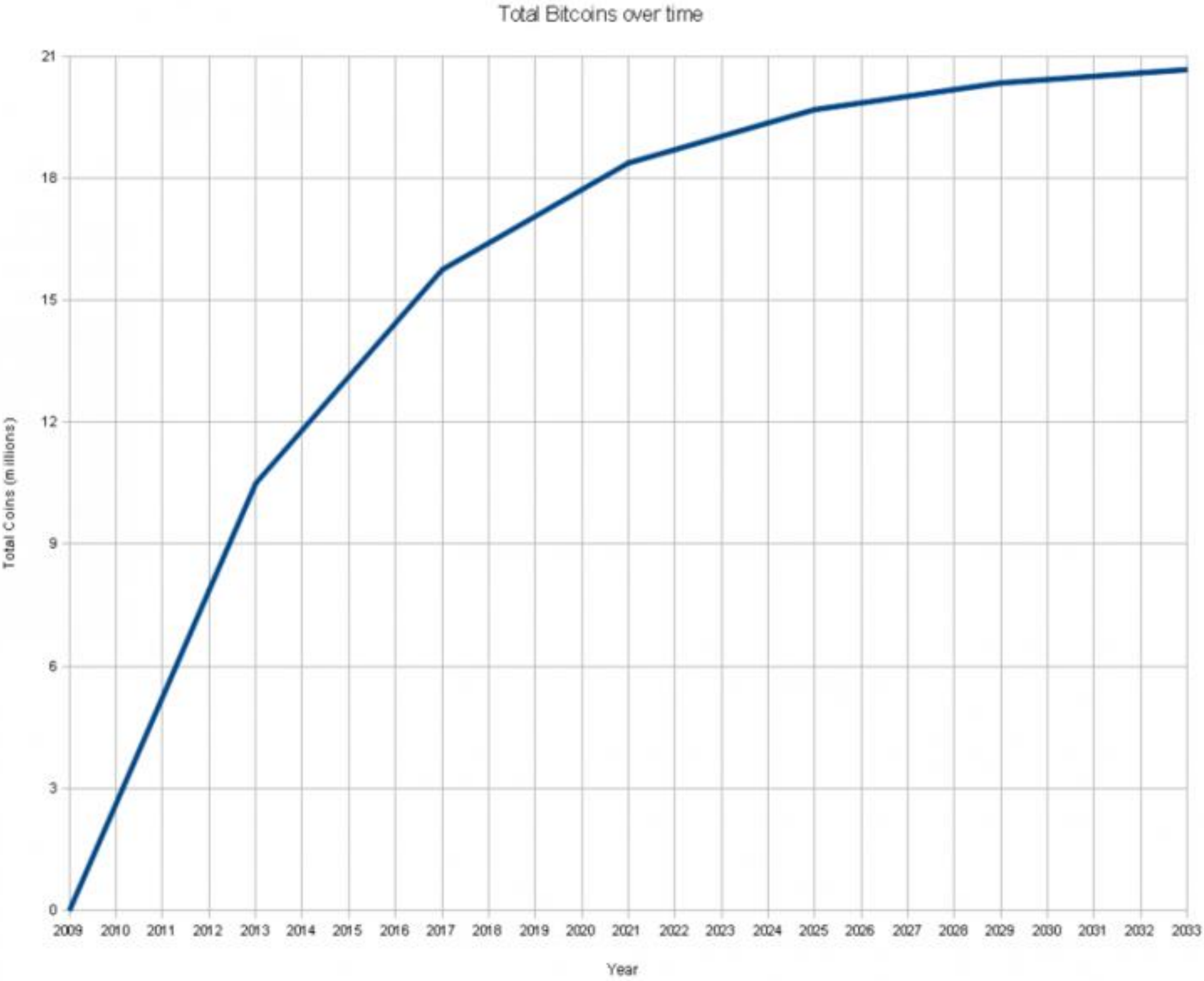
  You trust the rules of a protocol enforced by mathematics and cryptography

- Distribution of funds

  How to distribute value when you create a new currency?

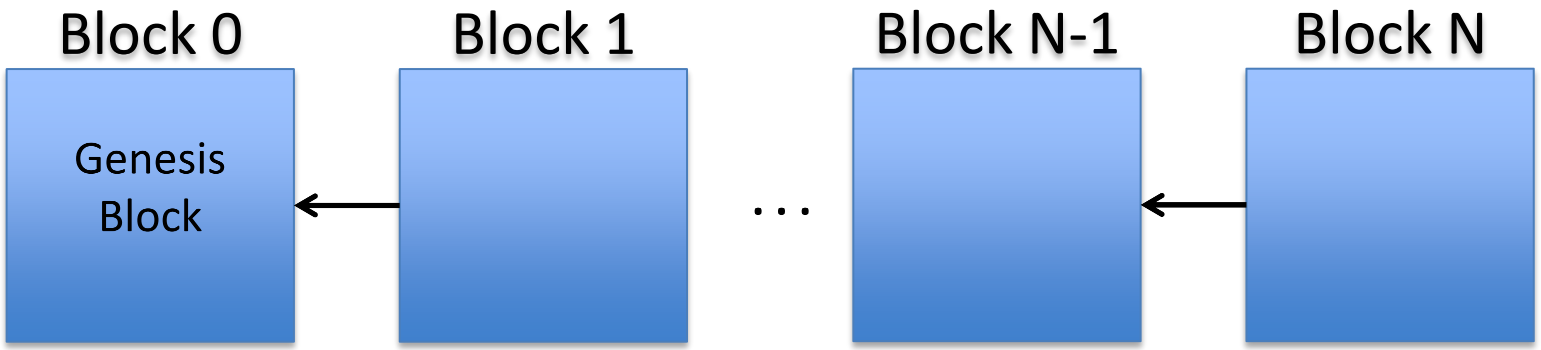
Distribution of Funds

- Every 10 minutes since inception a “random” node in the Bitcoin network receives a reward.
- The reward started at 50 bitcoins, and halves every 4 years


Total Bitcoins over time
Total Coins (millions)
21
18
15
12
9
6
3
0
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
Year

The Block Chain

- The big invention that makes Bitcoin work
- The block chain is a database containing historical records of all the transactions that ever occurred in the network.
- Every full node in the network has a copy that they keep up to date and verify.
- Some nodes extend the block chain, they are called miners.



Think of it as a big accounting book.
Every block is a page in the book.

Anyone can try to add a page to the book to get a reward
… but it is computationally hard to do so

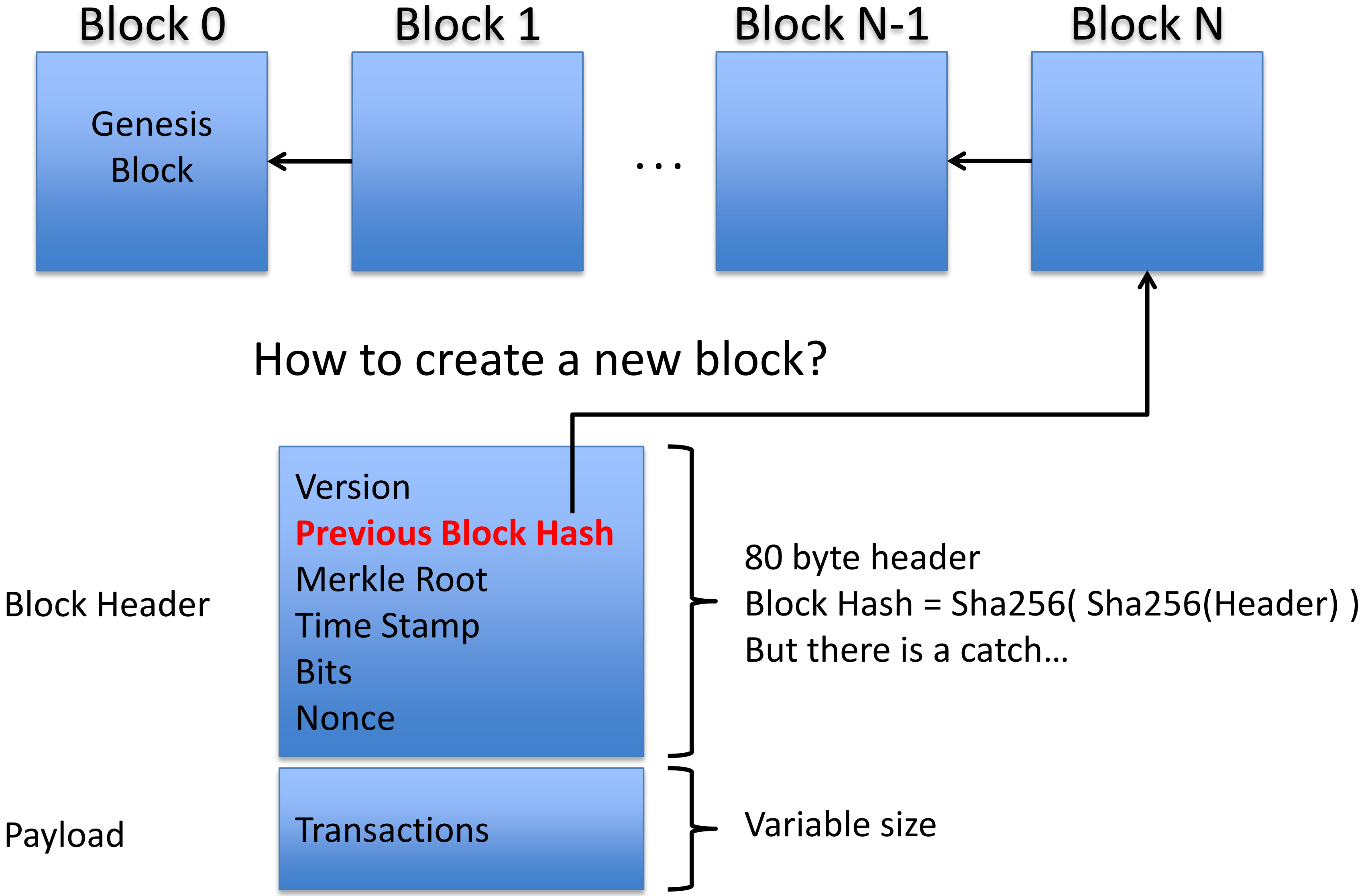
Problem: We want a new block to appear every 10 minutes on average.

Introducing SHA-256

- Cryptographically secure one-way hash function.
- Takes any input and produces a 32 byte output.
- Flipping one bit in the input gives a different randomly distributed output.

```
Sha256(“GOTO”) = e38c772d4940e4e059430cd25b797923
                 bfe139db8b74831e062b409a97ca63ff

Sha256(“TOGO”) = 52031acdcfba3318c4daafcd3bc30a56
                 be3a455dfa59128d72bcf74ef52491bb
```



Block 0

Genesis Block

Block 1

. . .

Block N-1

Block N

How to create a new block?

Block Header

Version
Previous Block Hash
Merkle Root
Time Stamp
Bits
Nonce

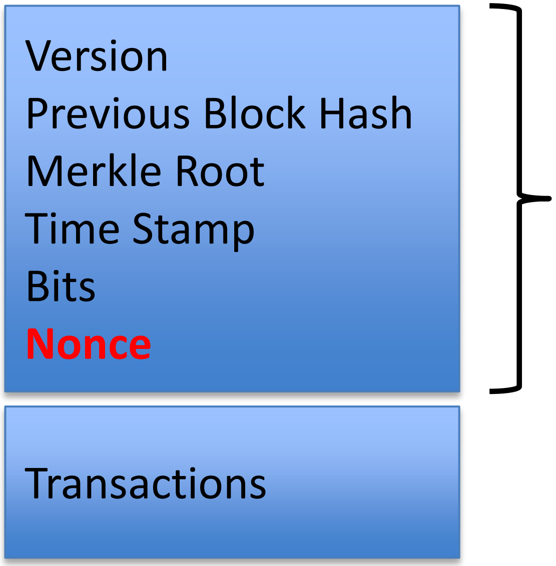
80 byte header
Block Hash = Sha256(Sha256(Header))
But there is a catch…

Payload

Transactions

Variable size

Block hash must be below the target difficulty


Version
Previous Block Hash
Merkle Root
Time Stamp
Bits
Nonce

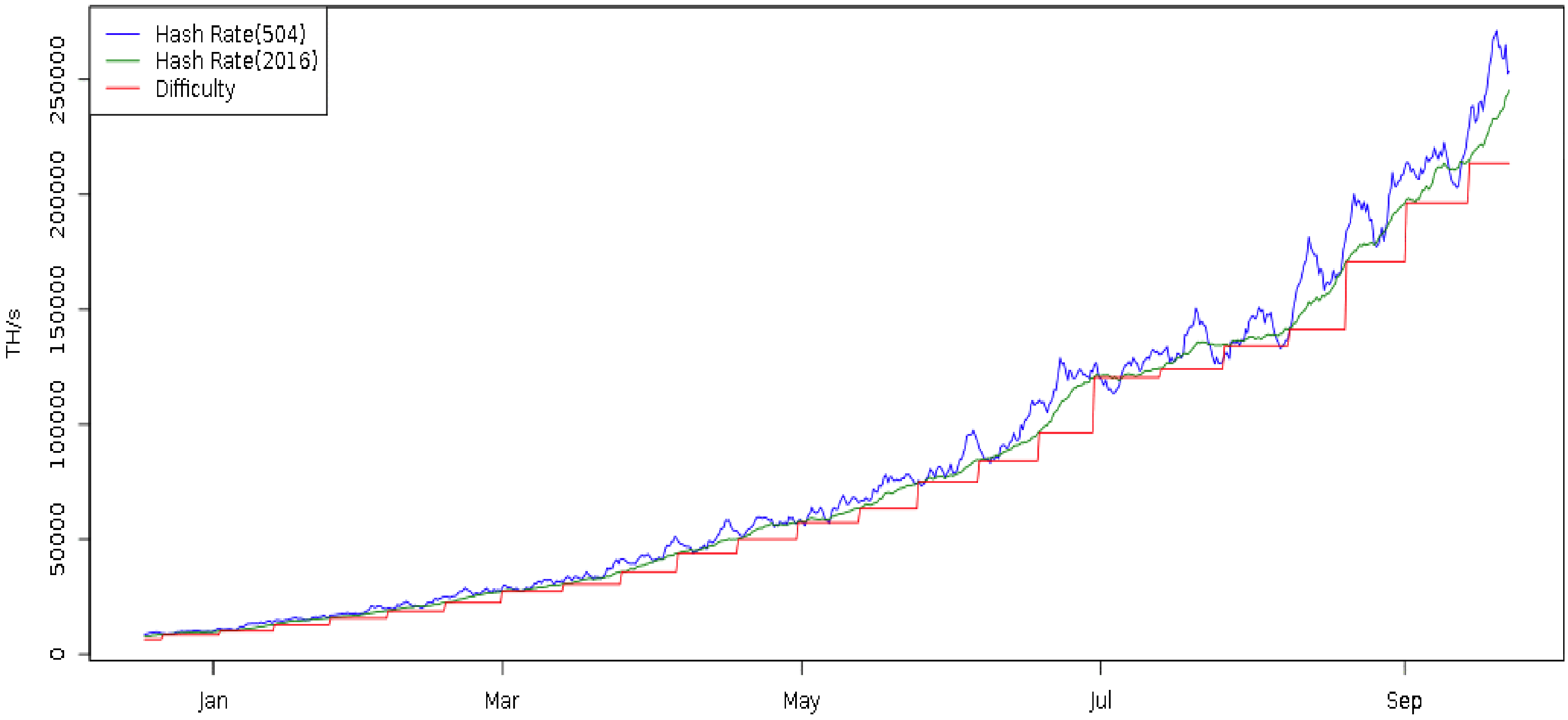
Transactions

1 create header
2 make nonce random
3 calculate block hash
4 is it below the target?
5 ☺ we are done
6 ☹ goto 2

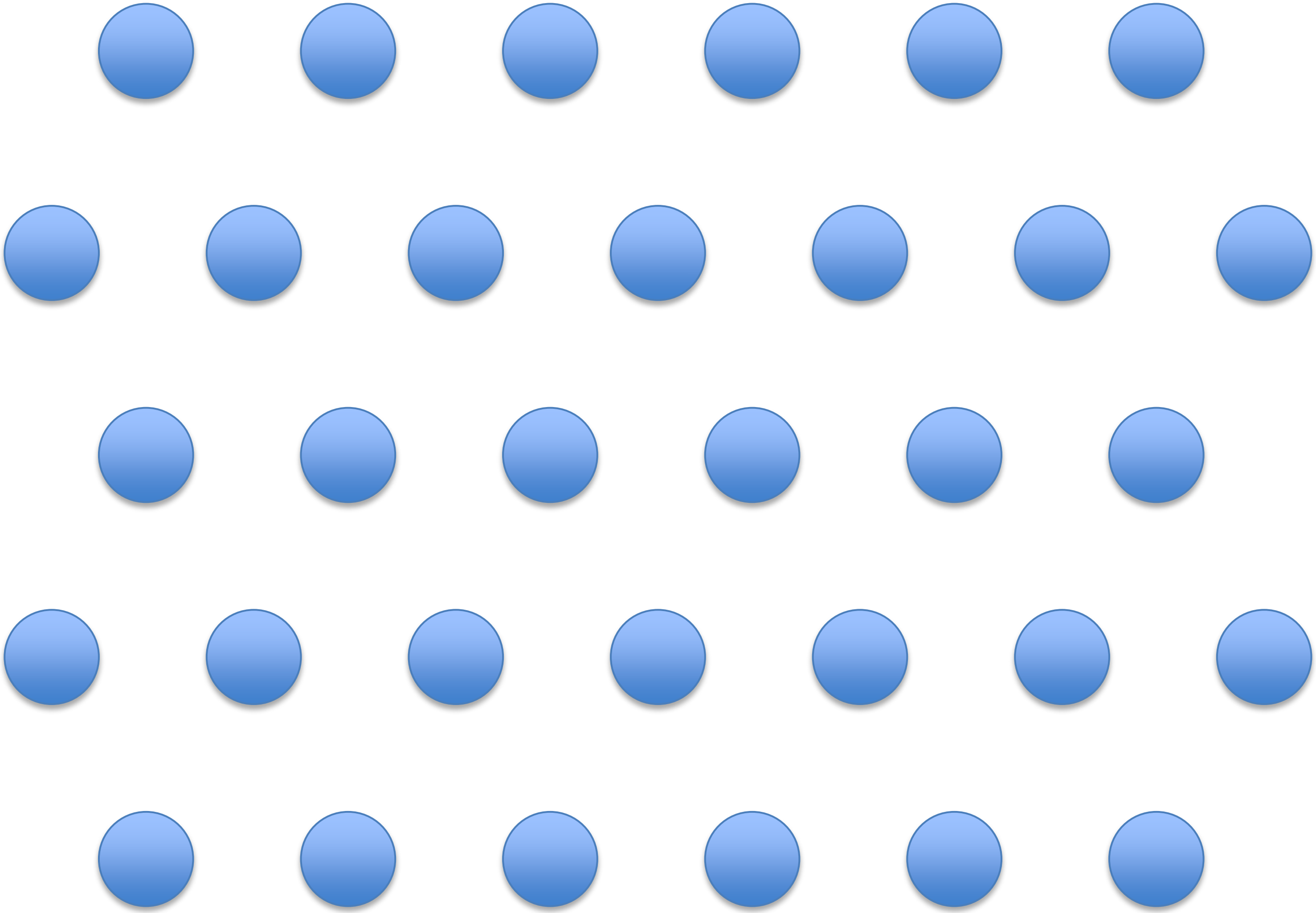
Block# 321511 ~ 250,000,000 GH/s

00000000000000001fb68313c9728ec3728686a632ad36c31fe9a9bf4b112362

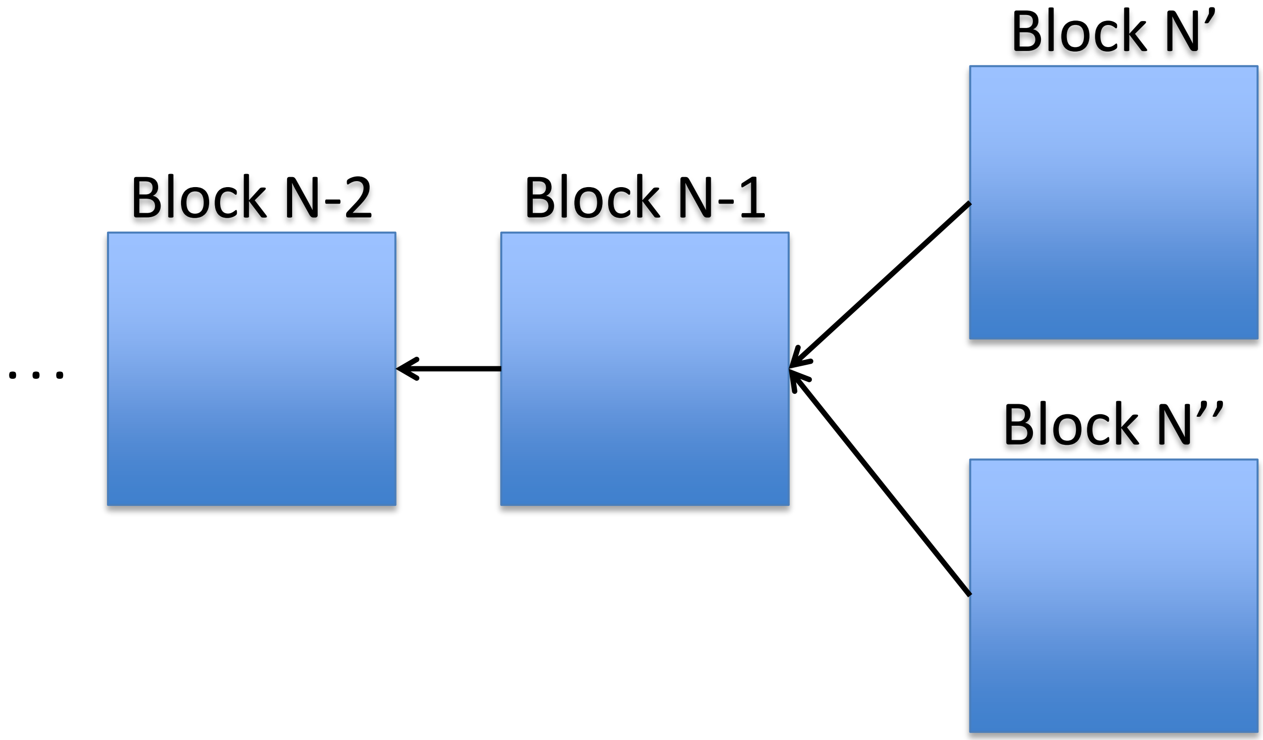
The Difficulty Adapts



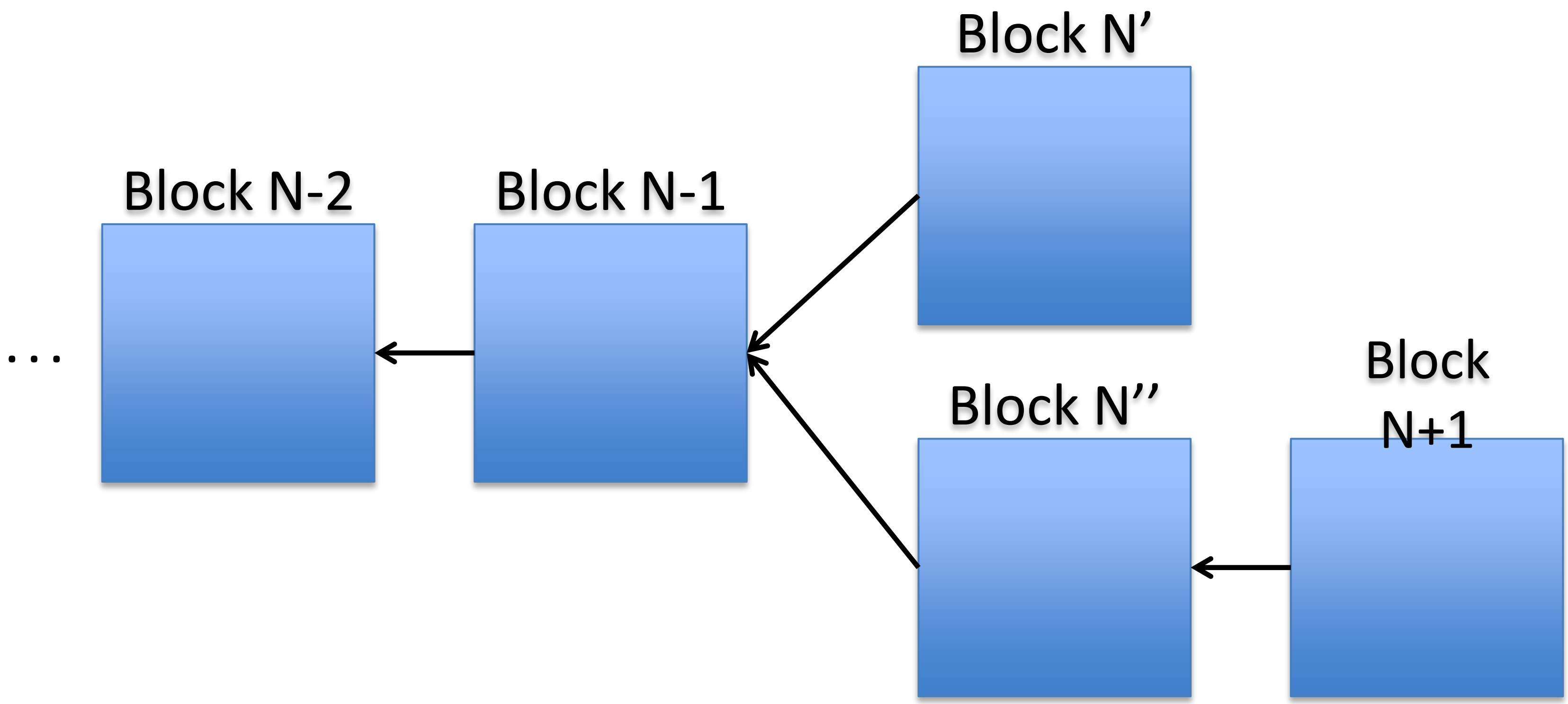
Block Propagation



Forks are Normal (1)



Forks are Normal (2)



The longest chain wins!

Bitcoin Public/Private Keys

- A Bitcoin uses Elliptic Curve cryptography
- A private key is 32 random bytes
- A public is computed from a private key
- There is no encryption in Bitcoin, only signing

Bitcoin Addresses

- A Bitcoin addresses is a bit like a bank account. **`1Kk18SN6WRPTEXbXBm3dZSzEw7NdbChyc9`**

- Calculated from a public key

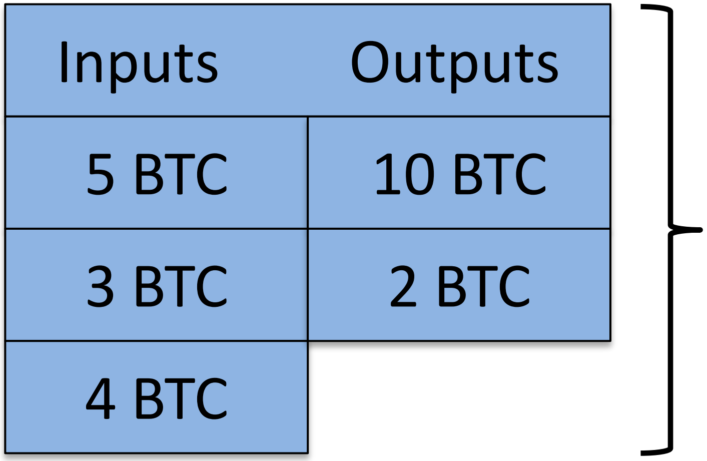
  RIPEMD-160(Sha256(public key))

- Nobody knows who owns which addresses

- Value is moved between addresses using transactions.

Transactions (simplified)

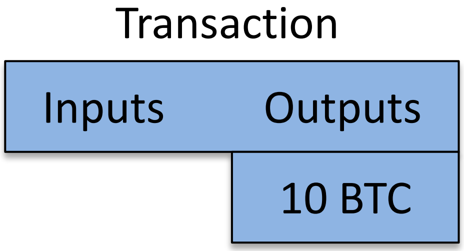
- A Bitcoin transaction sends value from one set of addresses to another



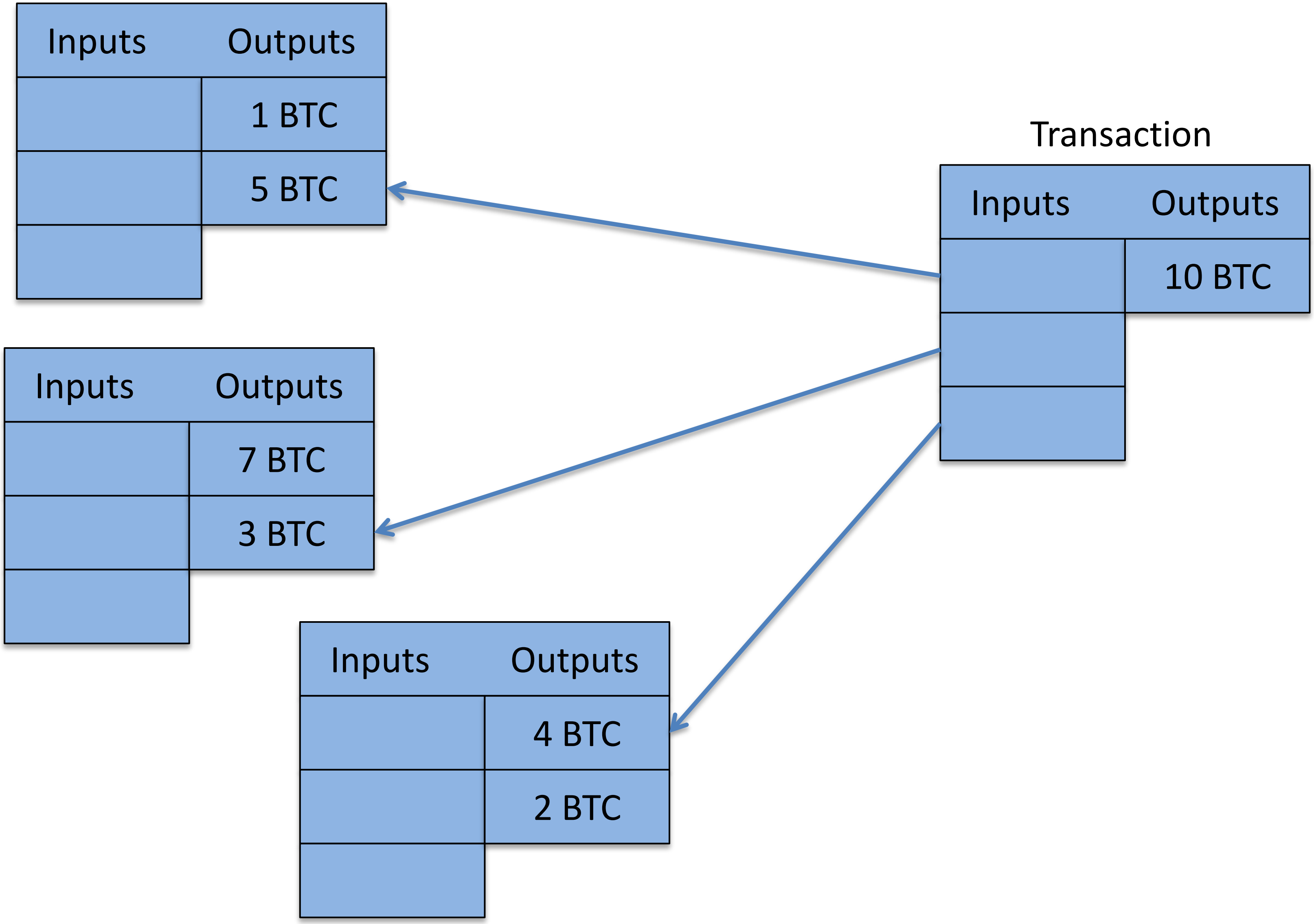
Inputs	Outputs
5 BTC	10 BTC
3 BTC	2 BTC
4 BTC	

Transaction Hash =
Sha256(Transaction Data)

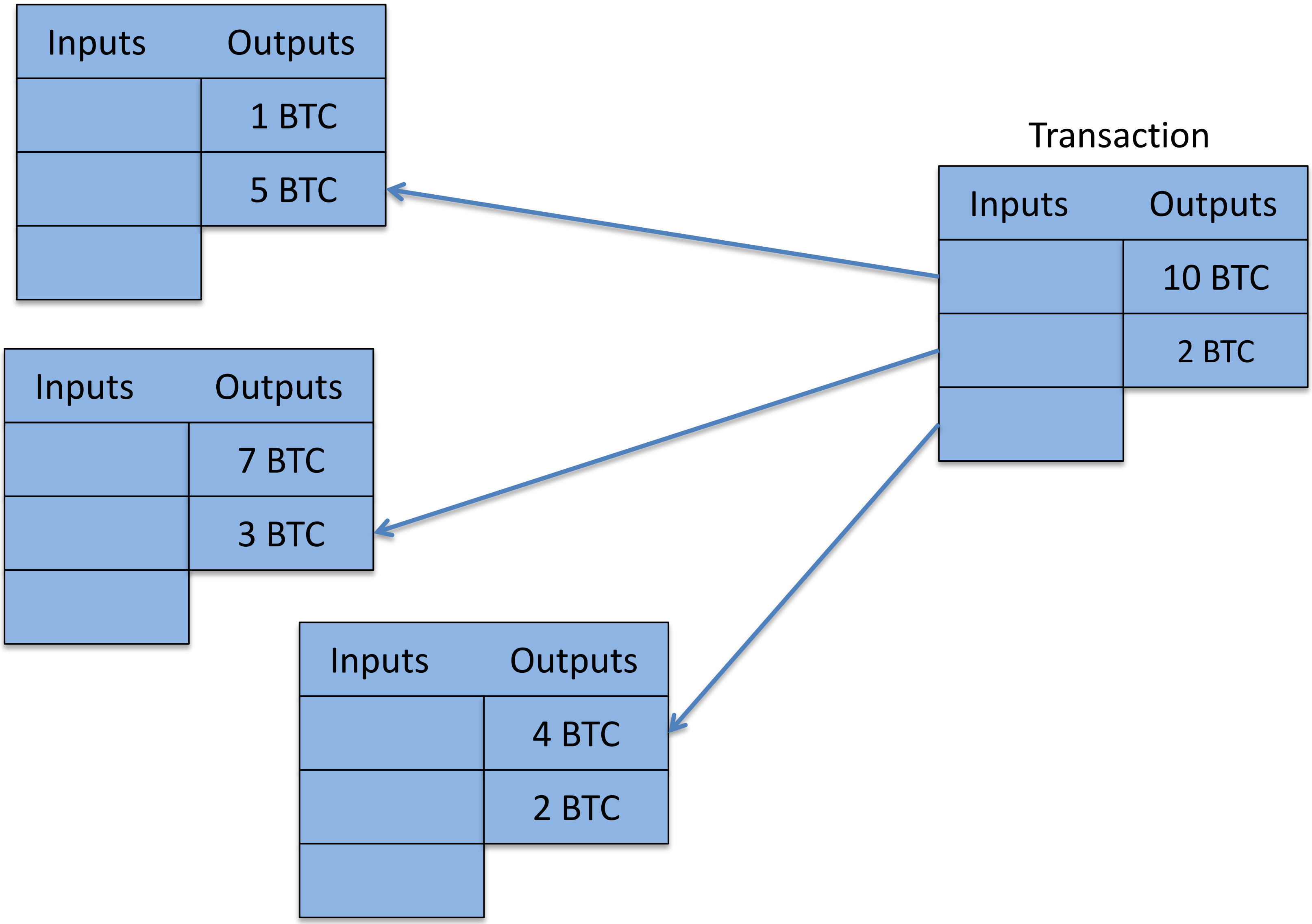
Creating a Transaction (1/7)



Creating a Transaction (2/7)



Creating a Transaction (4/7)



Inputs	Outputs
	1 BTC
	5 BTC

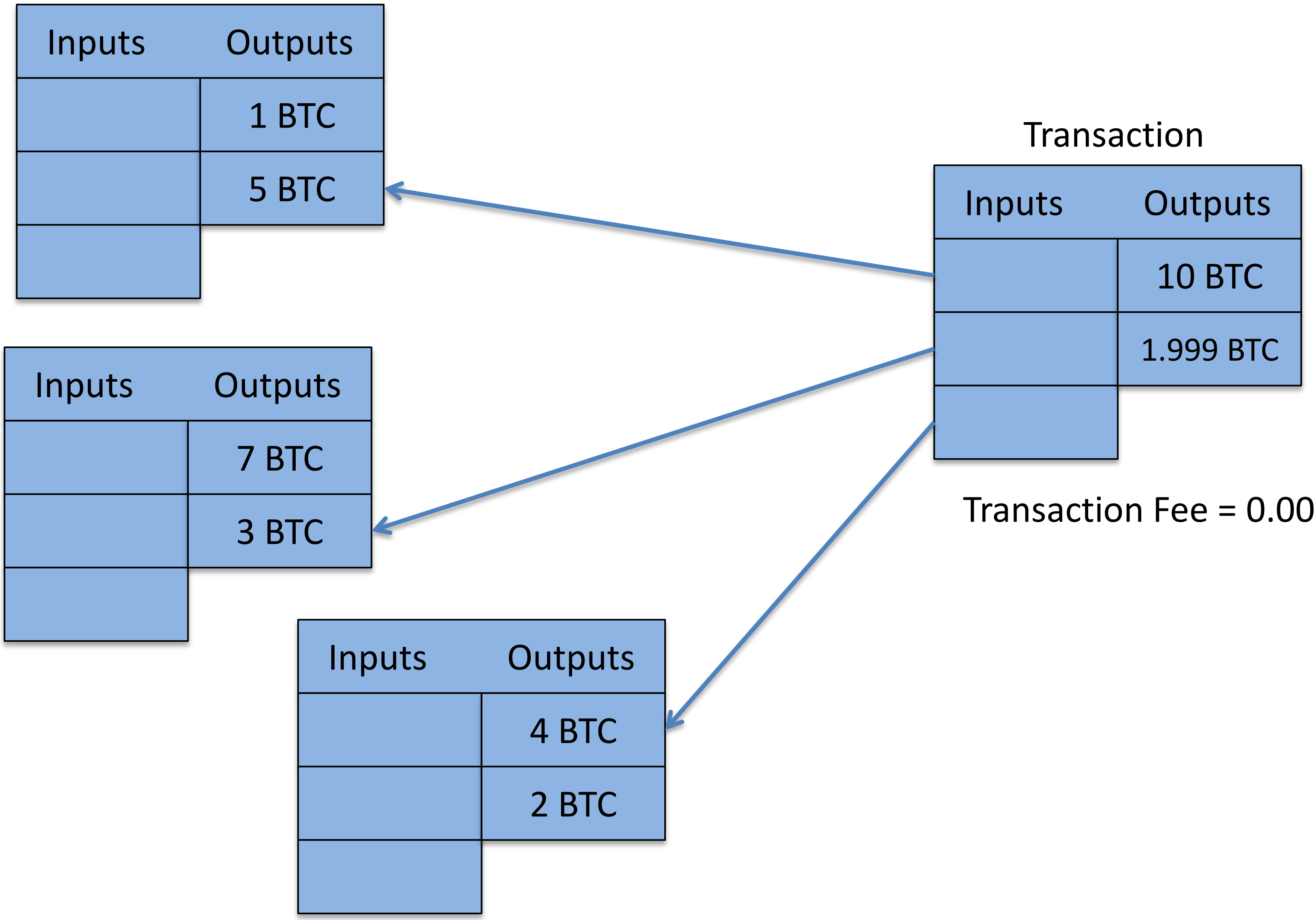
Inputs	Outputs
	7 BTC
	3 BTC

Inputs	Outputs
	4 BTC
	2 BTC

Transaction

Inputs	Outputs
	10 BTC
	2 BTC

Creating a Transaction (4/7)



Inputs	Outputs
	1 BTC
	5 BTC

Inputs	Outputs
	7 BTC
	3 BTC

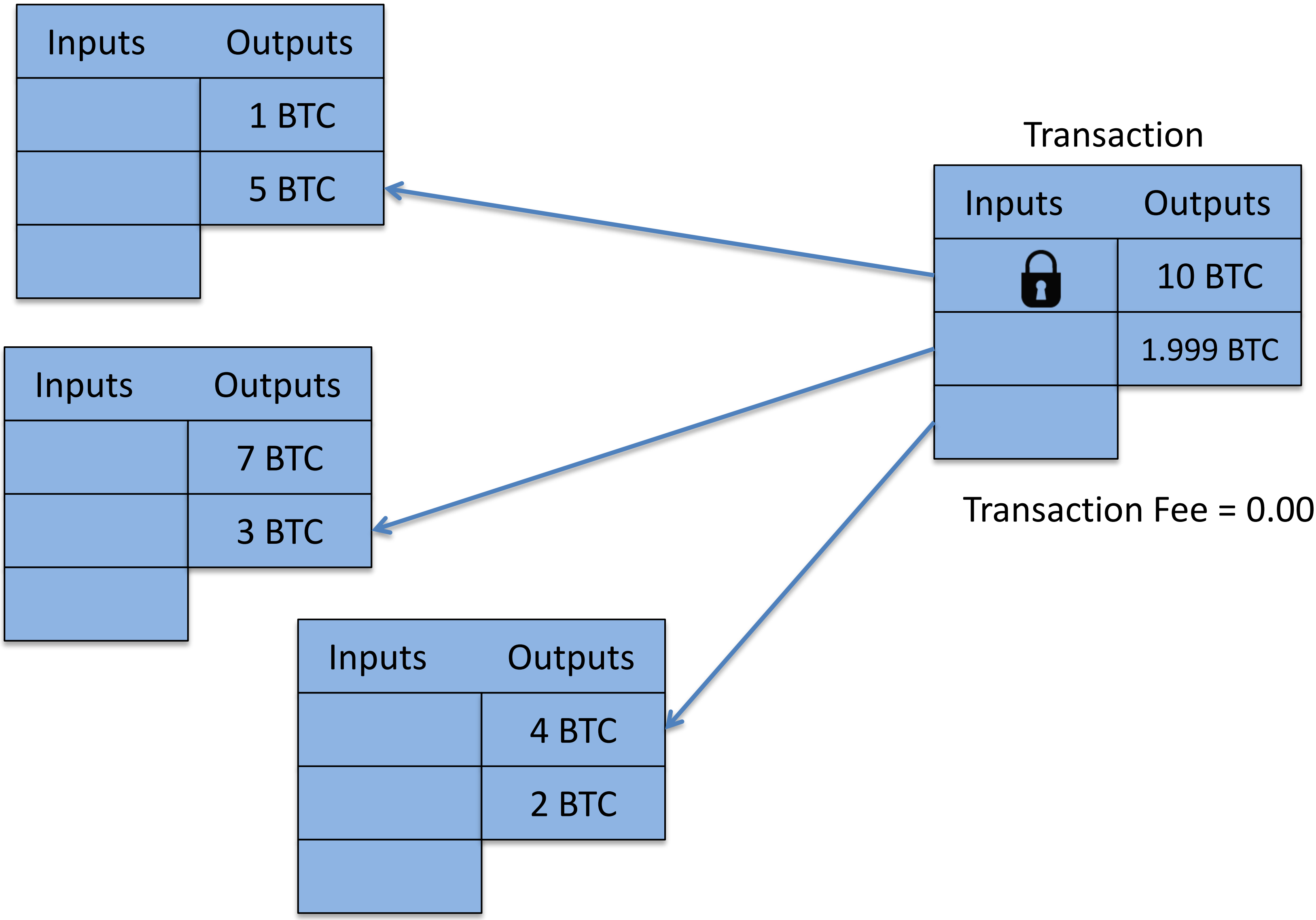
Inputs	Outputs
	4 BTC
	2 BTC

Transaction

Inputs	Outputs
	10 BTC
	1.999 BTC

Transaction Fee = 0.0001 BTC

Creating a Transaction (5/7)



Inputs	Outputs
	1 BTC
	5 BTC

Inputs	Outputs
	7 BTC
	3 BTC

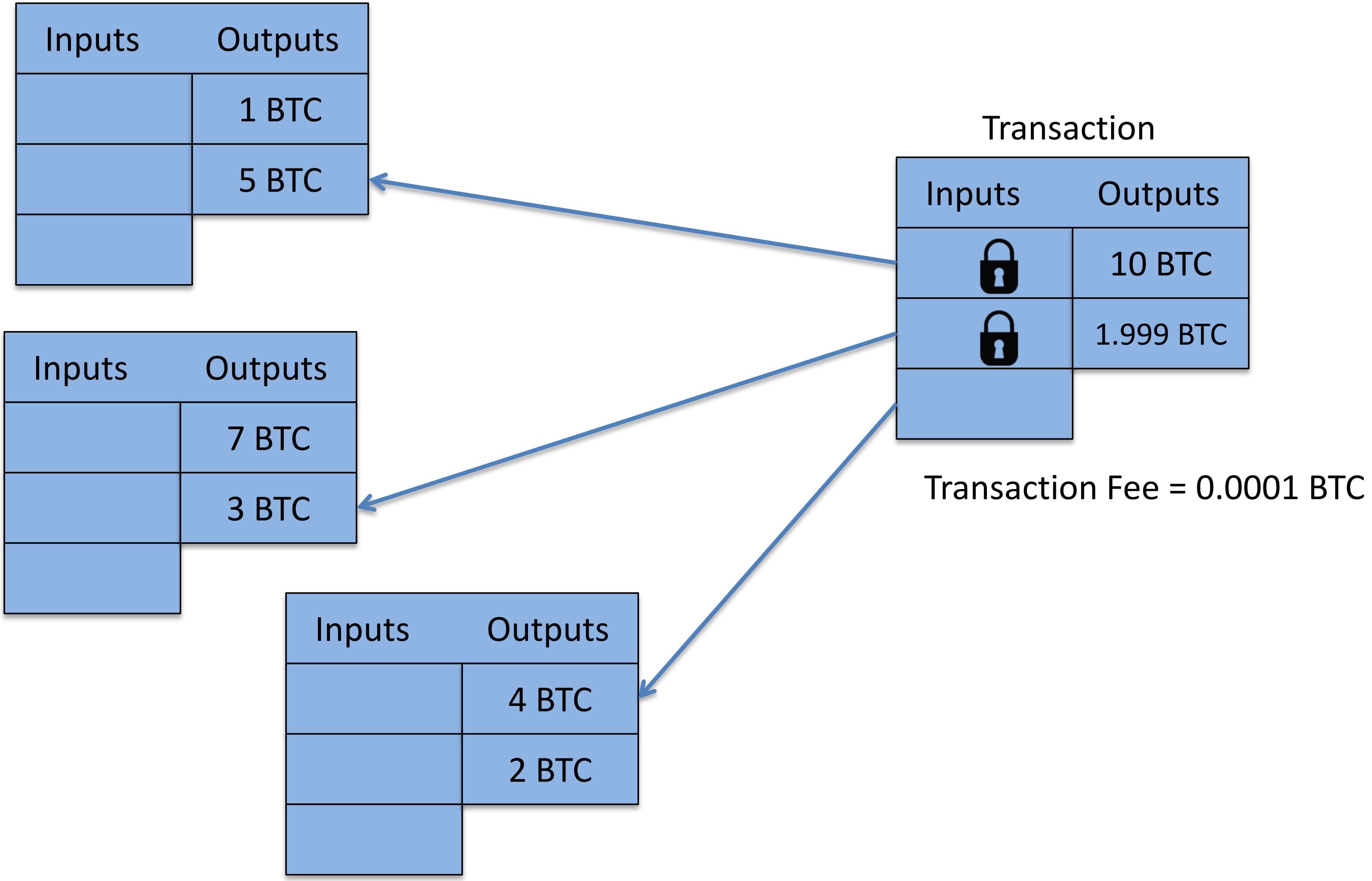
Inputs	Outputs
	4 BTC
	2 BTC

Transaction

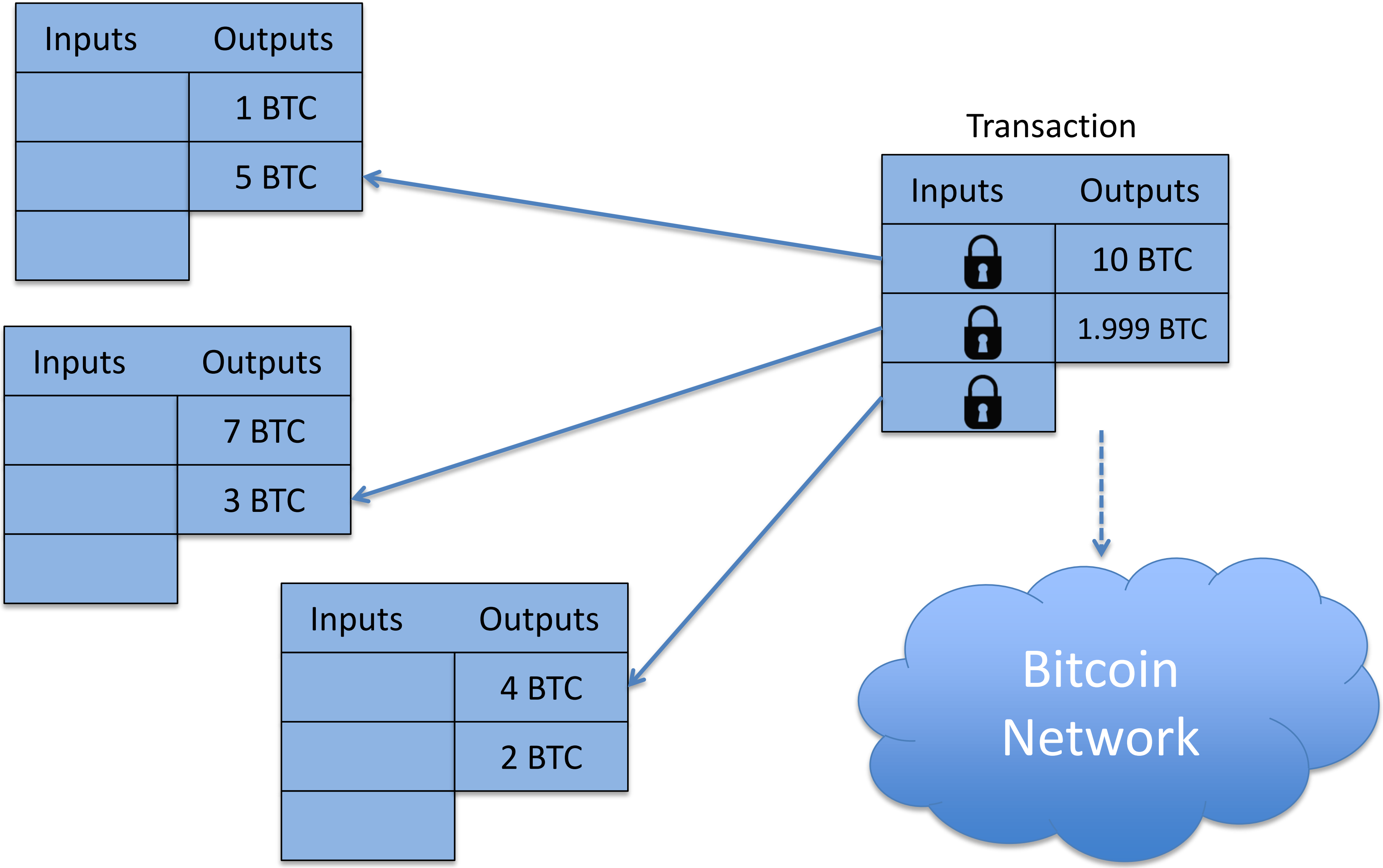
Inputs	Outputs
🔒	10 BTC
	1.999 BTC

Transaction Fee = 0.0001 BTC

Creating a Transaction (6/7)



Creating a Transaction (7/7)



Inputs	Outputs
	1 BTC
	5 BTC

Inputs	Outputs
	7 BTC
	3 BTC

Inputs	Outputs
	4 BTC
	2 BTC

Transaction

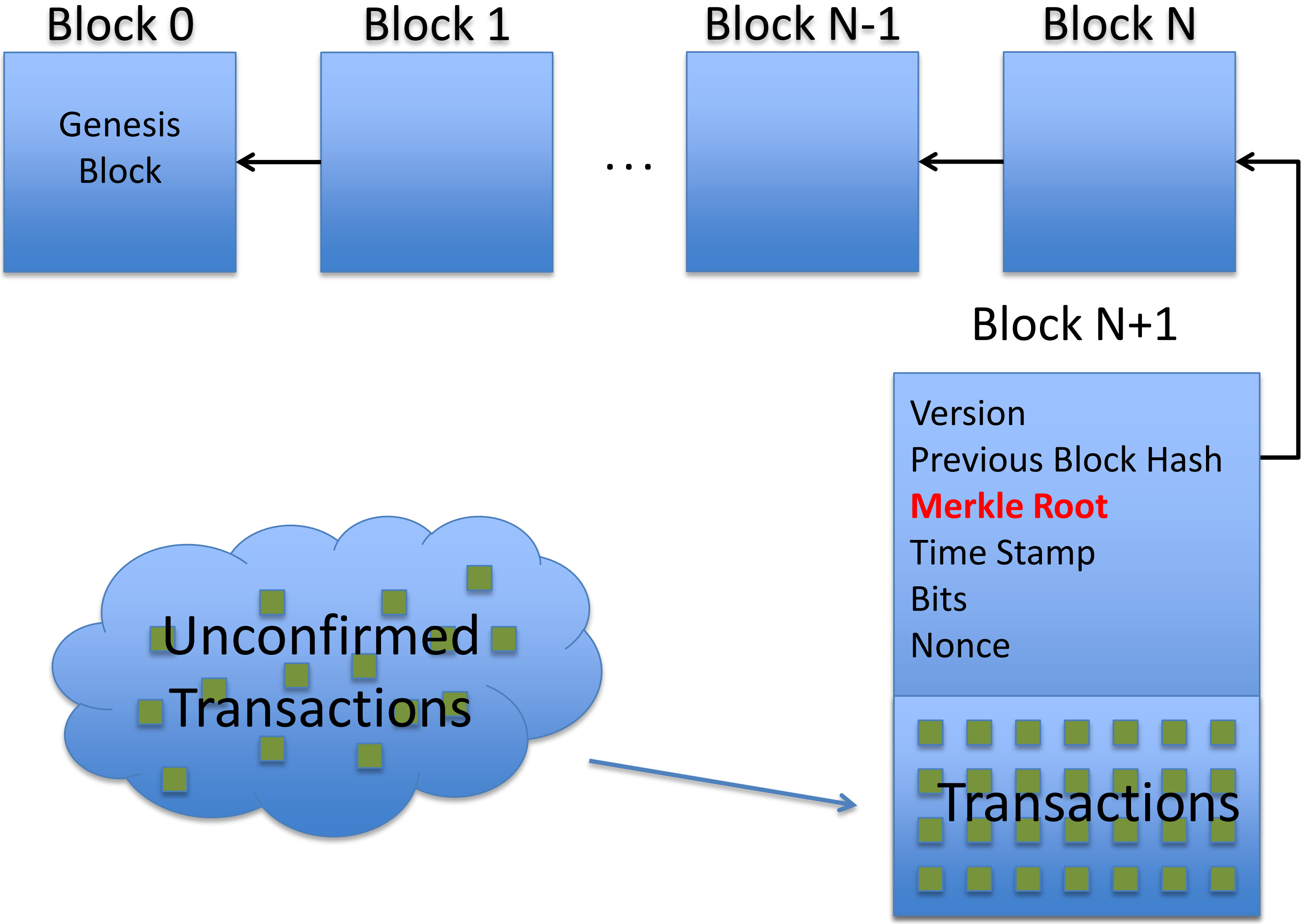
Inputs	Outputs
🔒	10 BTC
🔒	1.999 BTC
🔒	

Transaction Relaying

- Receive transaction from peer

- Verification (simplified):
  - Verify that the signatures are sound
  - Verify that the inputs are unspent
  - Verify that the sum of outputs <= sum of inputs

- Relay transaction to other peers



Block 0

Genesis Block

Block 1

. . .

Block N-1

Block N

Block N+1

Version

Previous Block Hash

Merkle Root

Time Stamp

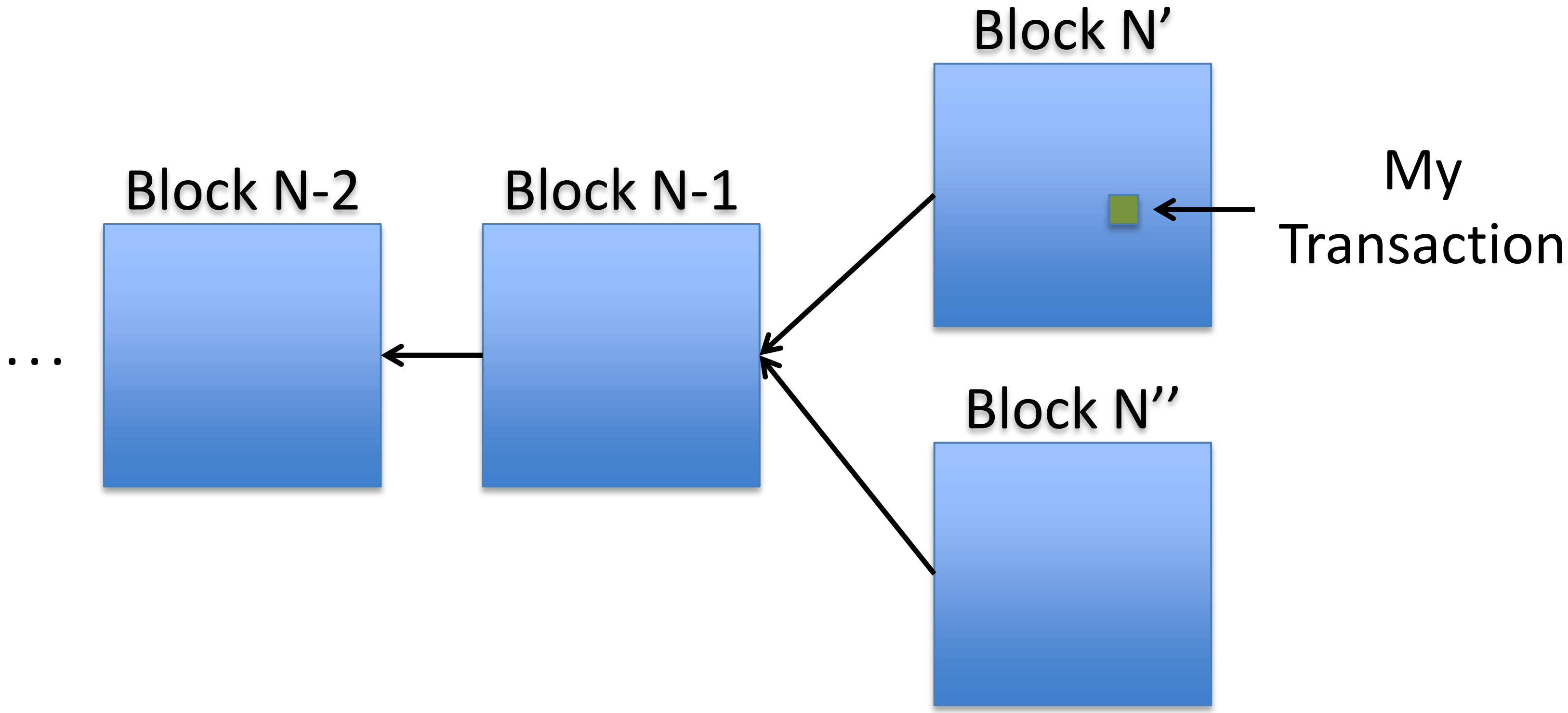
Bits

Nonce

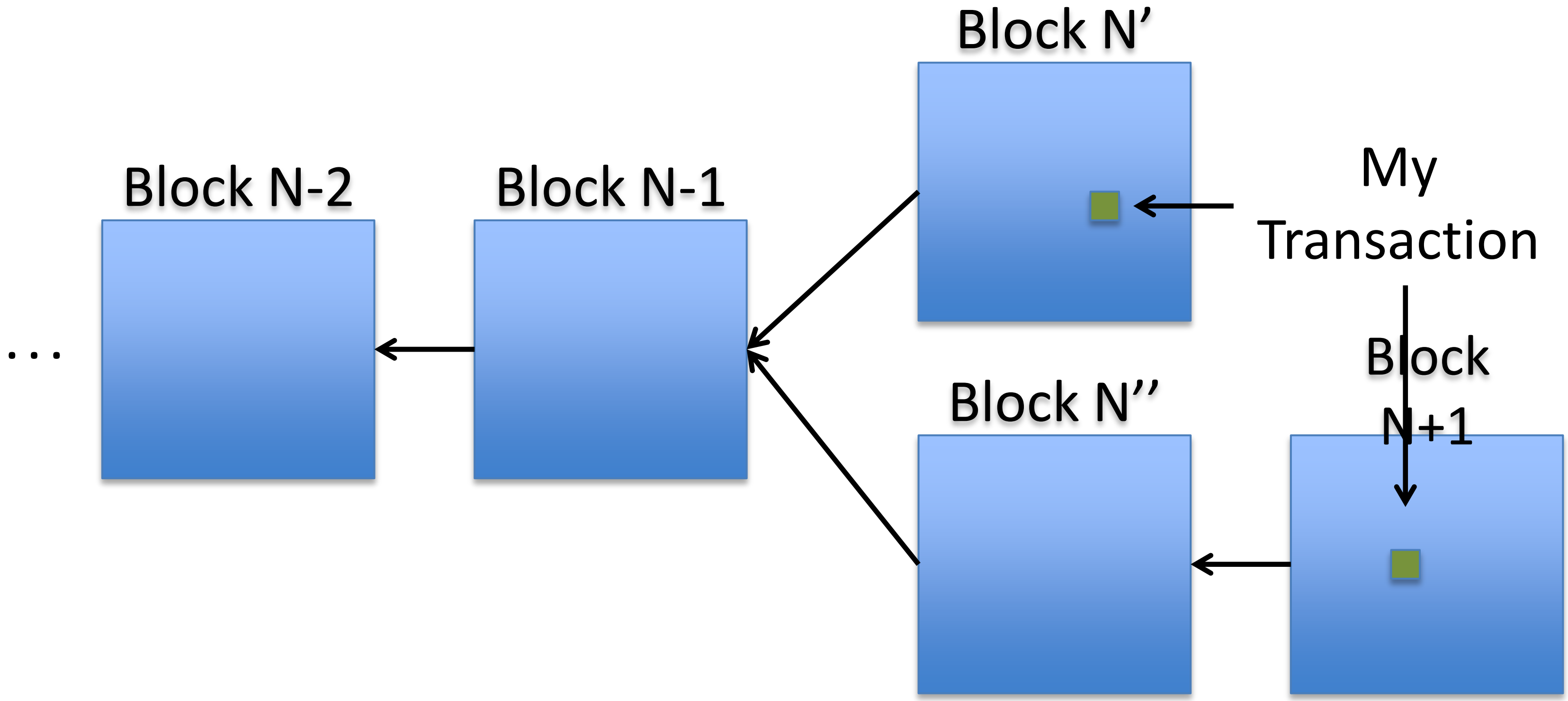
Transactions

Unconfirmed Transactions

Transactions in Forks (1)



Transactions in Forks (2)

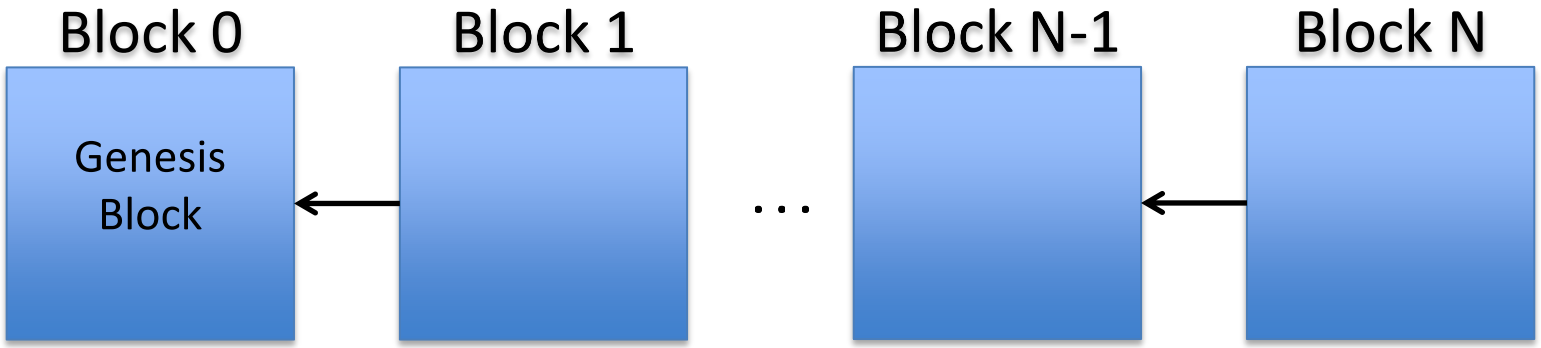


The longest chain wins!

Properties of Bitcoin (1/3)

No Counterfeiting

“NOBODY” can increase money supply at will



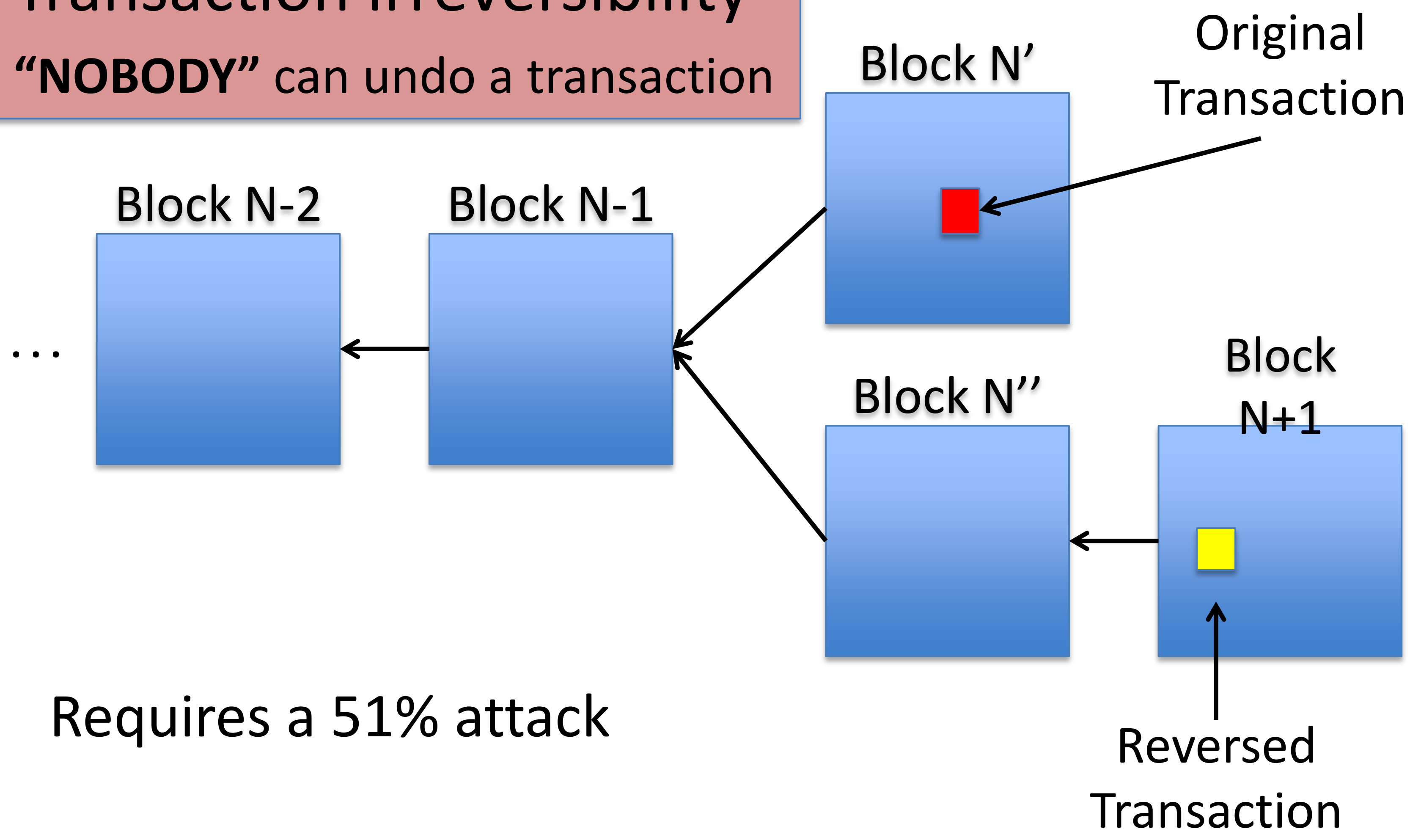
You are competing with the biggest distributed computer the world has seen.

If you can beat it, it just gets harder.

Properties of Bitcoin (2/3)

Transaction irreversibility

“NOBODY” can undo a transaction

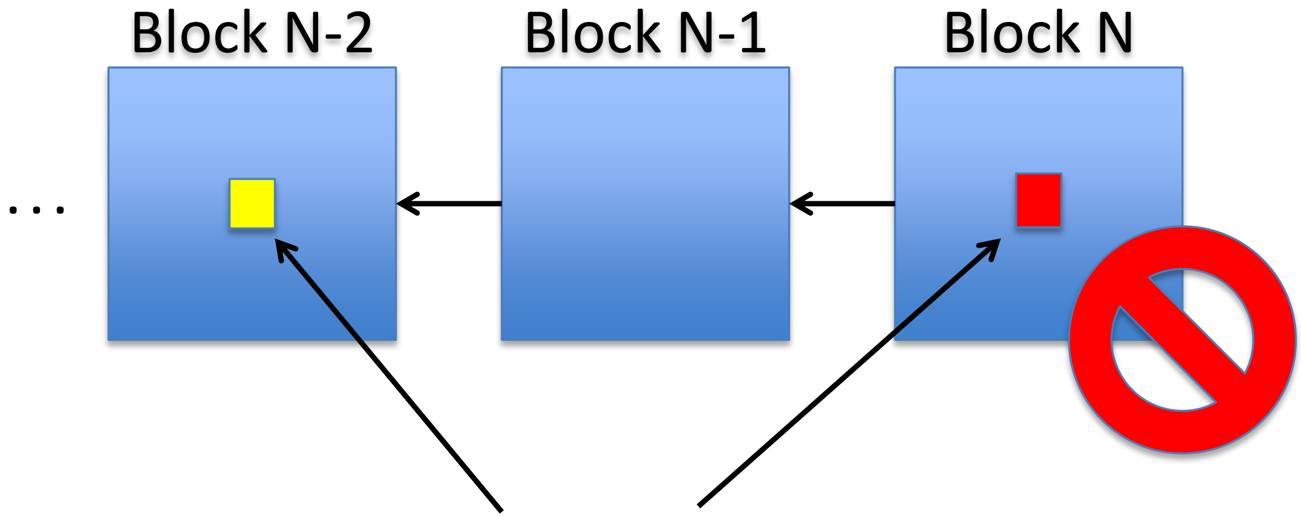


Requires a 51% attack

Properties of Bitcoin (3/3)

No Double Spending

NOBODY can spend the same value more than once



Two transactions spending
the same outputs

Block Chain Tech is New

Trustless decentralized ordering of events

- Decentralized DNS with **Namecoin**
  - A decentralized open source information registration and transfer system.
- Decentralized voting with **Votecoin**
  - The Liberal Alliance party in Denmark announced they were in favor of a block chain-based vote.

We can do stuff that wasn’t possible before