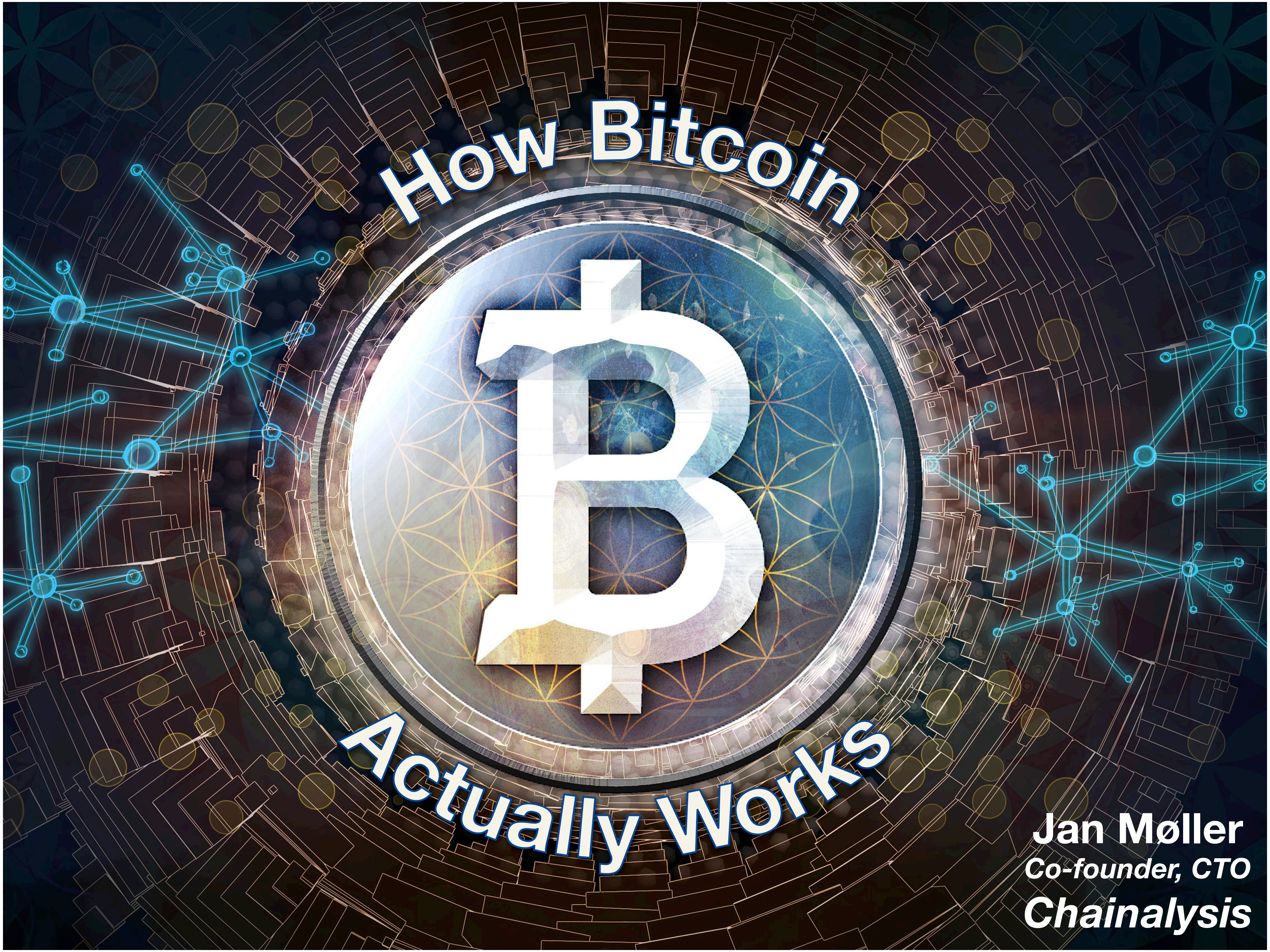
How Bitcoin Actually Works



Jan Møller

Co-founder, CTO

Chainalysis

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**”

“I've been working on a new electronic cash system that’s fully peer-to-peer, with no trusted third party.”

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

A Brief [FUN] History

First Bitcoin Transaction	January 2009
2 Pizzas 10.000 BTC	May 2010
1 BTC Suprasses USD 1	February 2011
1 Cessna Aircraft 10.000 BTC	June 2011
1 BTC Surpasses USD 100	April 2013
1 BTC Surpasses USD 200	April 2013
1 BTC Surpasses USD 1000	November 2013
1 BTC Down to USD 245	June 2015

Today 1 bitcoin is about USD 750

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, Australian Dollar, or WoW 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

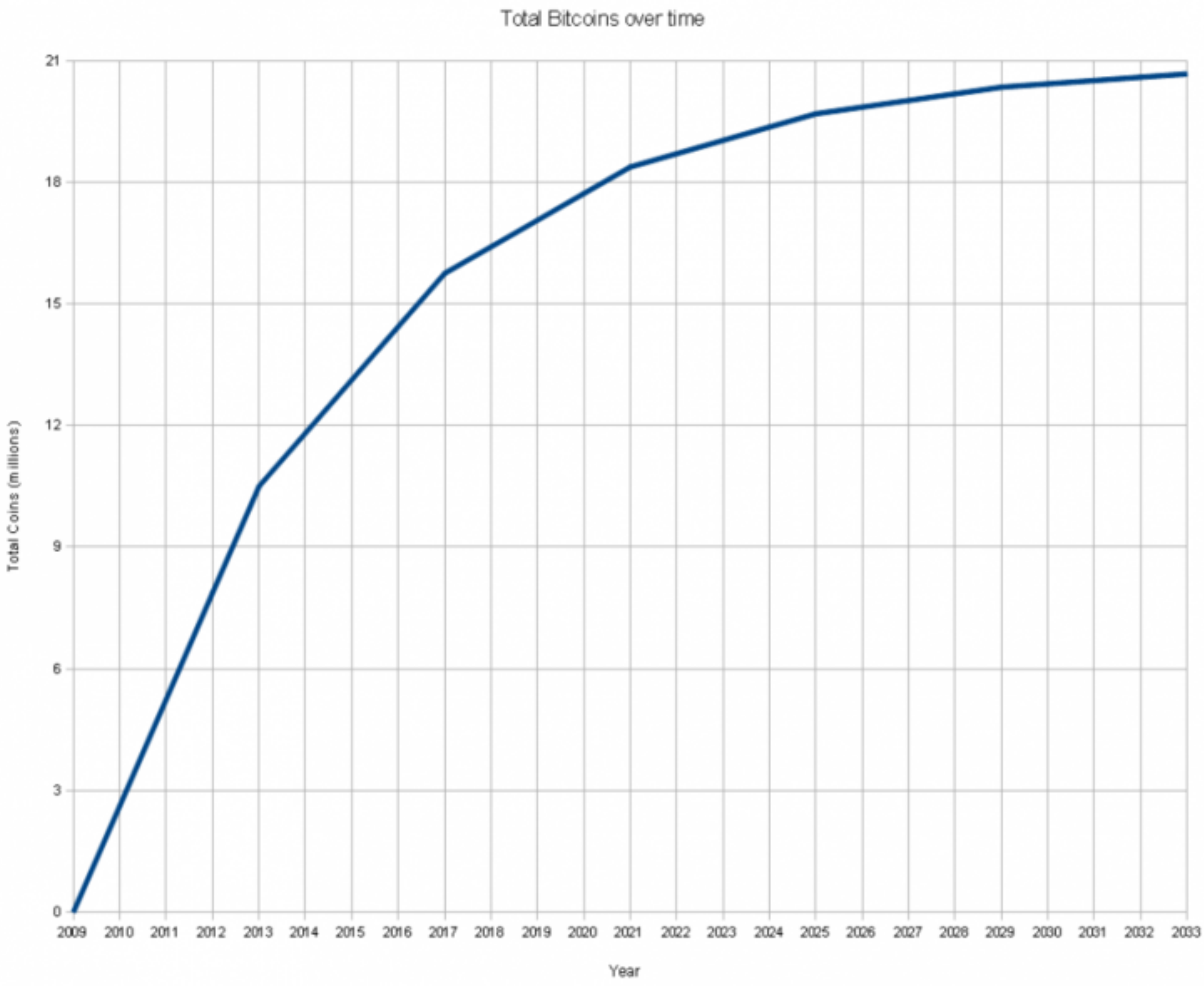
- Distribution of funds

  How to distribute value when you create a new currency?

Distribution of Funds

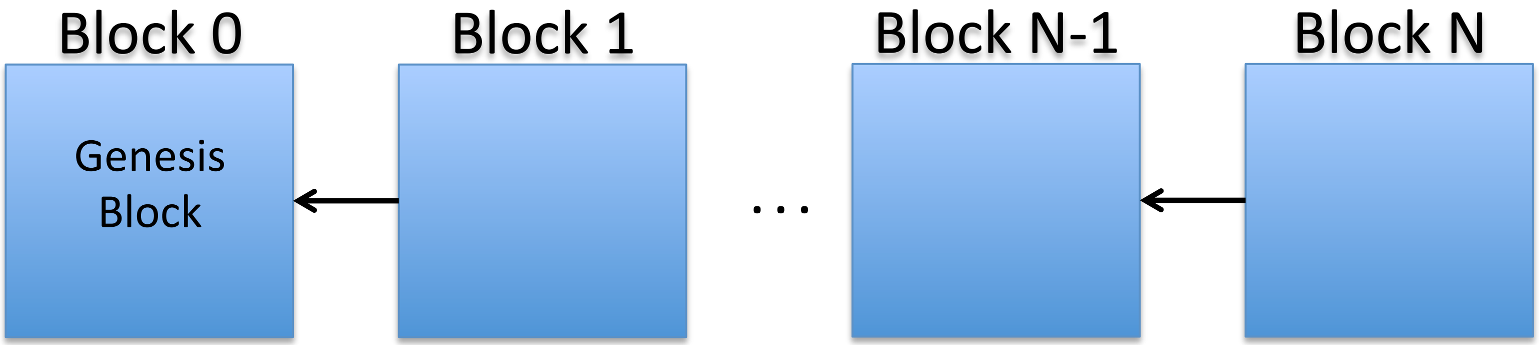
- Every 10 minutes since inception a “random” node in the Bitcoin network receives a reward.

- The reward started at 50 bitcoins, and halves every 4 years


Total Bitcoins over time
Total Coins (millions)
0
3
6
9
12
15
18
21
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 Blockchain

- The big invention that makes Bitcoin work
- The blockchain 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

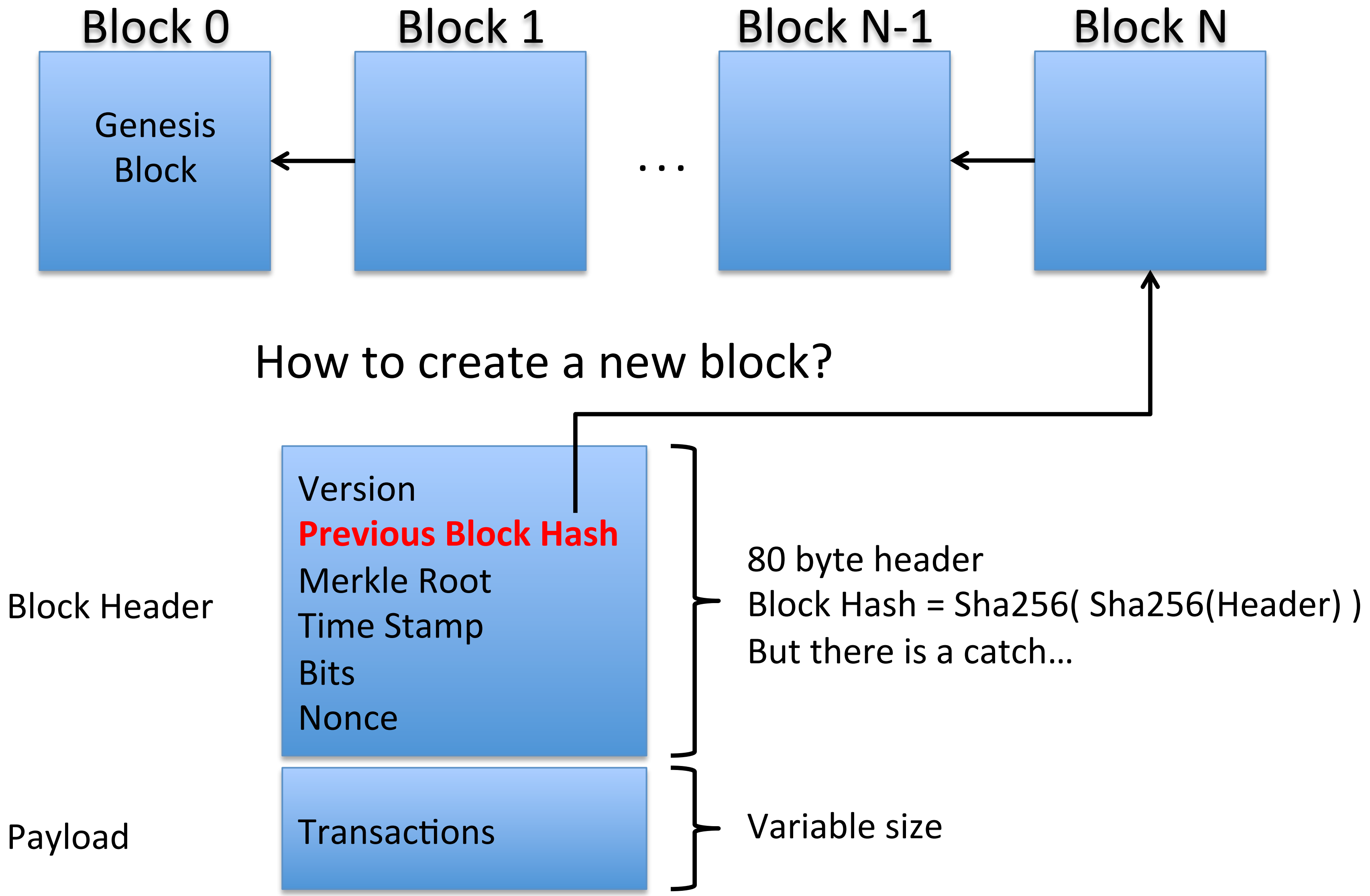
Problem: We want a new block to appear every 10 minutes on average.

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(“YOW”) =  990d7204316fe2907f55cb22d7b66fe9
                 e1f7e26dca2b61041cc3d3eec303d6a7

Sha256(“WOY”) =  cab9db6bcb5b96f48fb3e5f11cc43008
                 a9eee6b168127ee7422f7218877751ff
```



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))

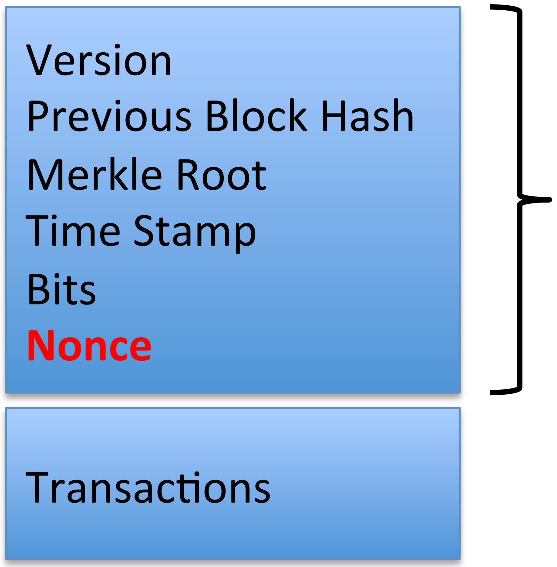
But there is a catch…

Payload

Transactions

Variable size

Block hash must be below the target difficulty



Version
Previous Block Hash
Merkle Root
Time Stamp
Bits
Nonce

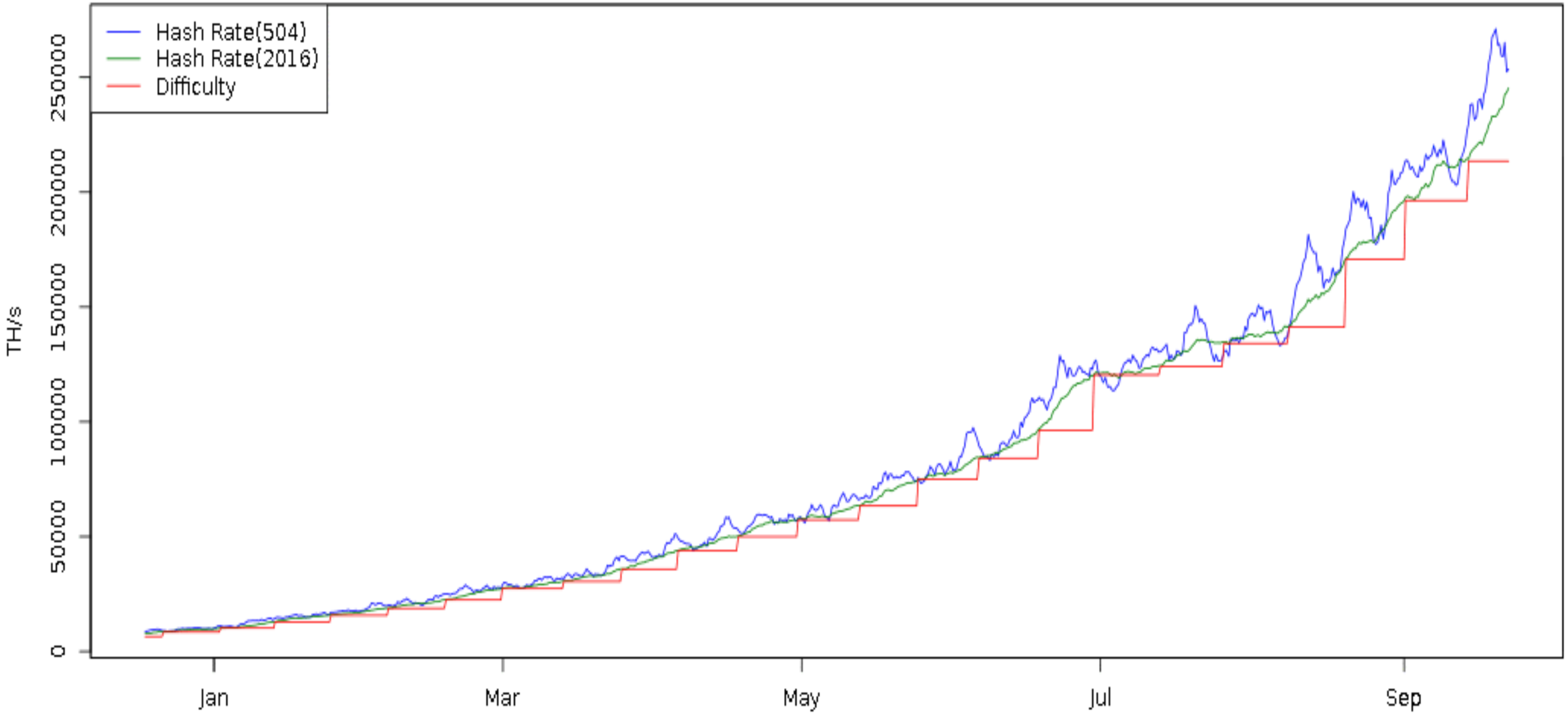
Transactions

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

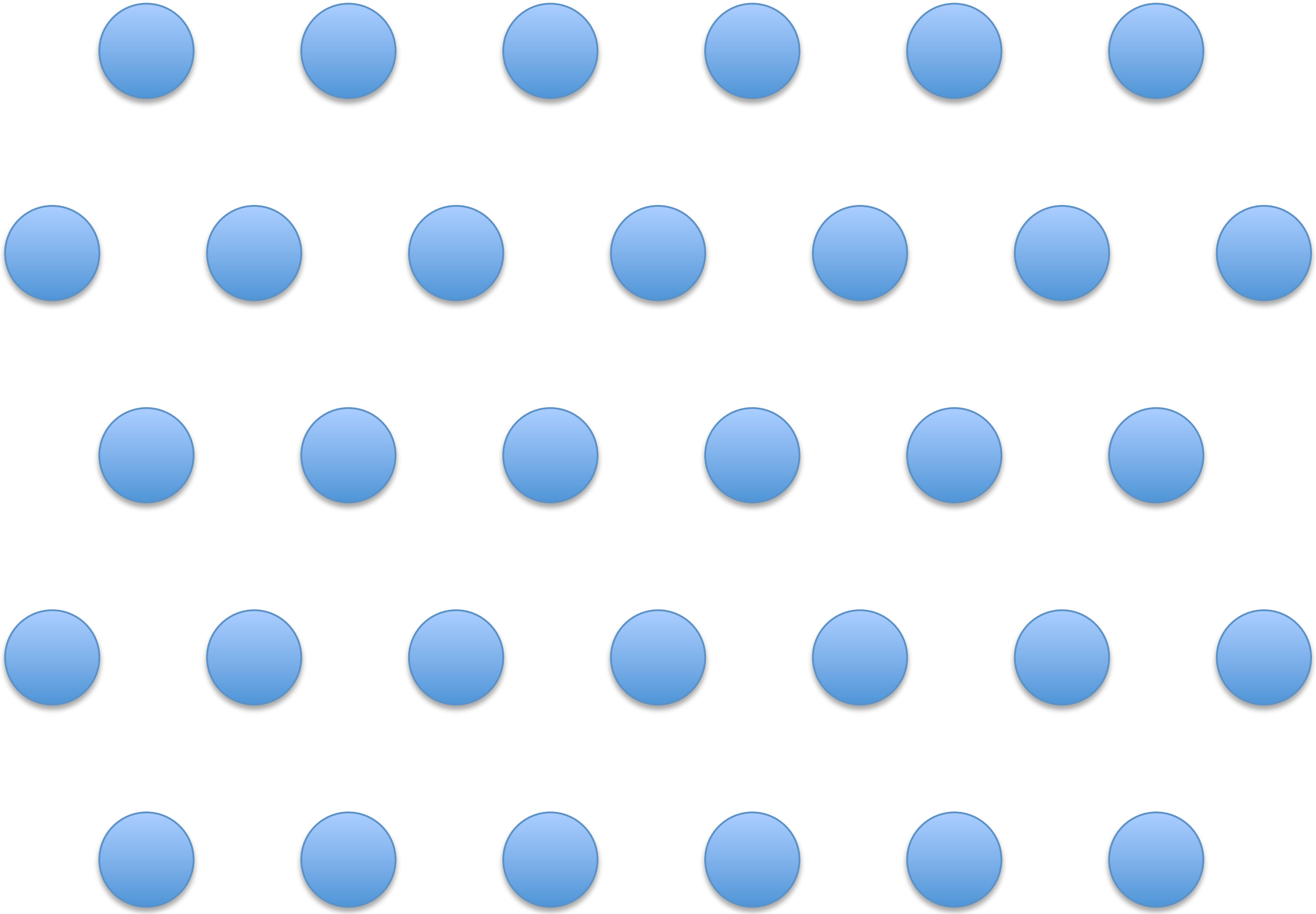
Block# 440000 ~ 2,000,000,000 GH/s

00000000000000000038cc0f7bcdbb451ad34a458e2d535764f835fdeb896f29b

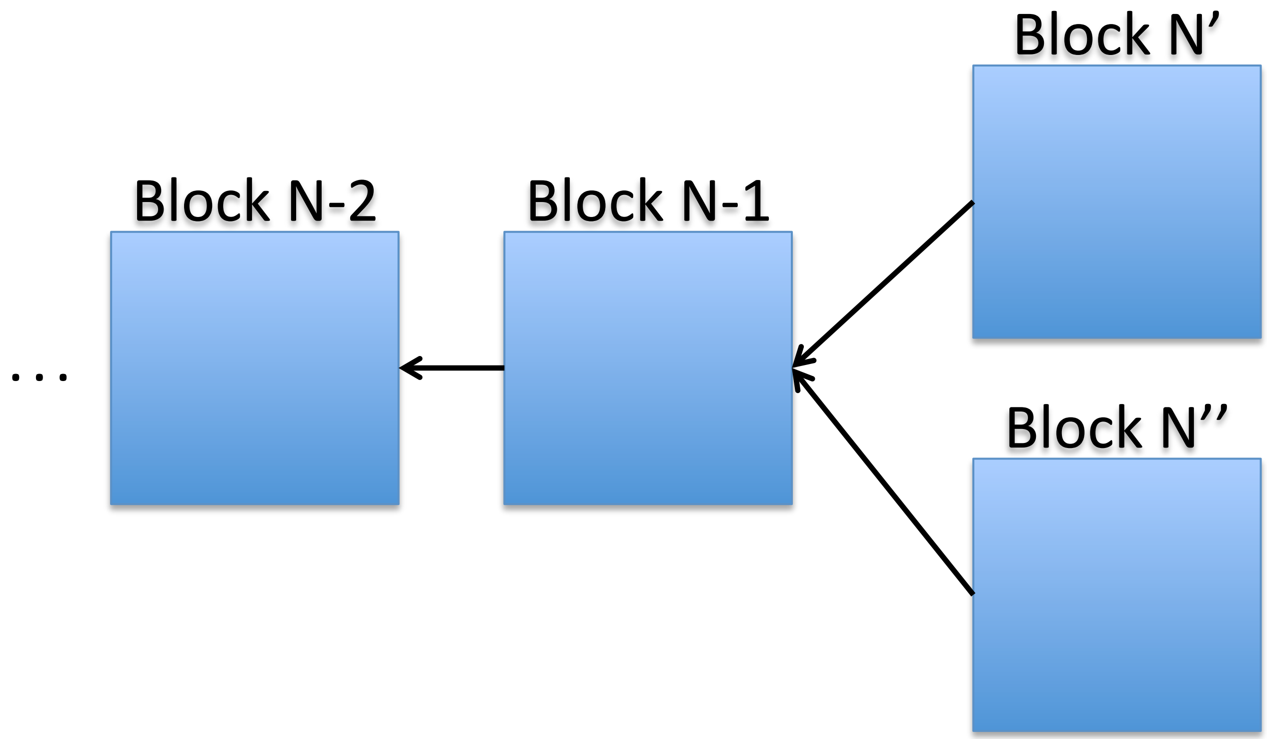
The Difficulty Adapts



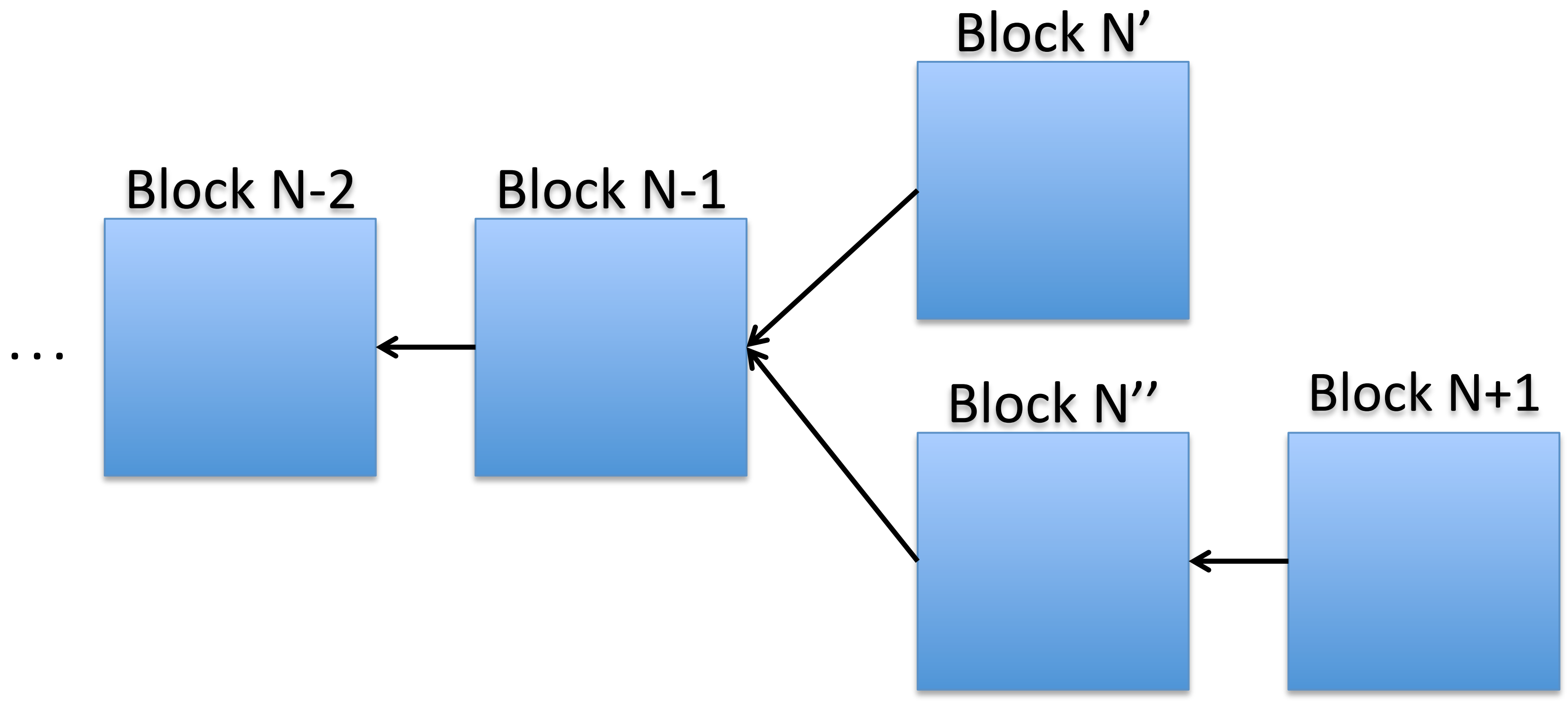
Block Propagation



Forks are Normal (1)



Forks are Normal (2)



The longest chain wins!

Distribution of Funds Summary

- Funds are distributed by solving blocks

- Difficulty adapts over time

- The longest chain wins

Bitcoin Public/Private Keys

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

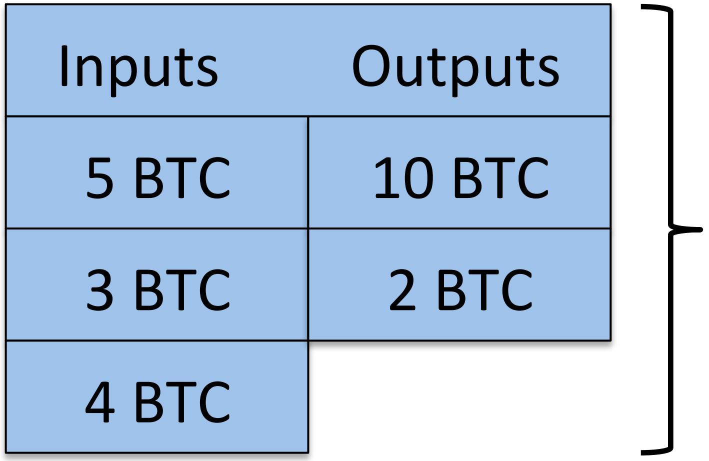
Bitcoin Addresses

- 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)

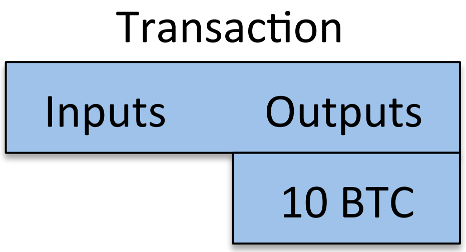
- A Bitcoin transaction sends value from one set of addresses to another



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

Transaction Hash =
 Sha256(
  Sha256(Transaction Data)
)

Creating a Transaction (1/7)



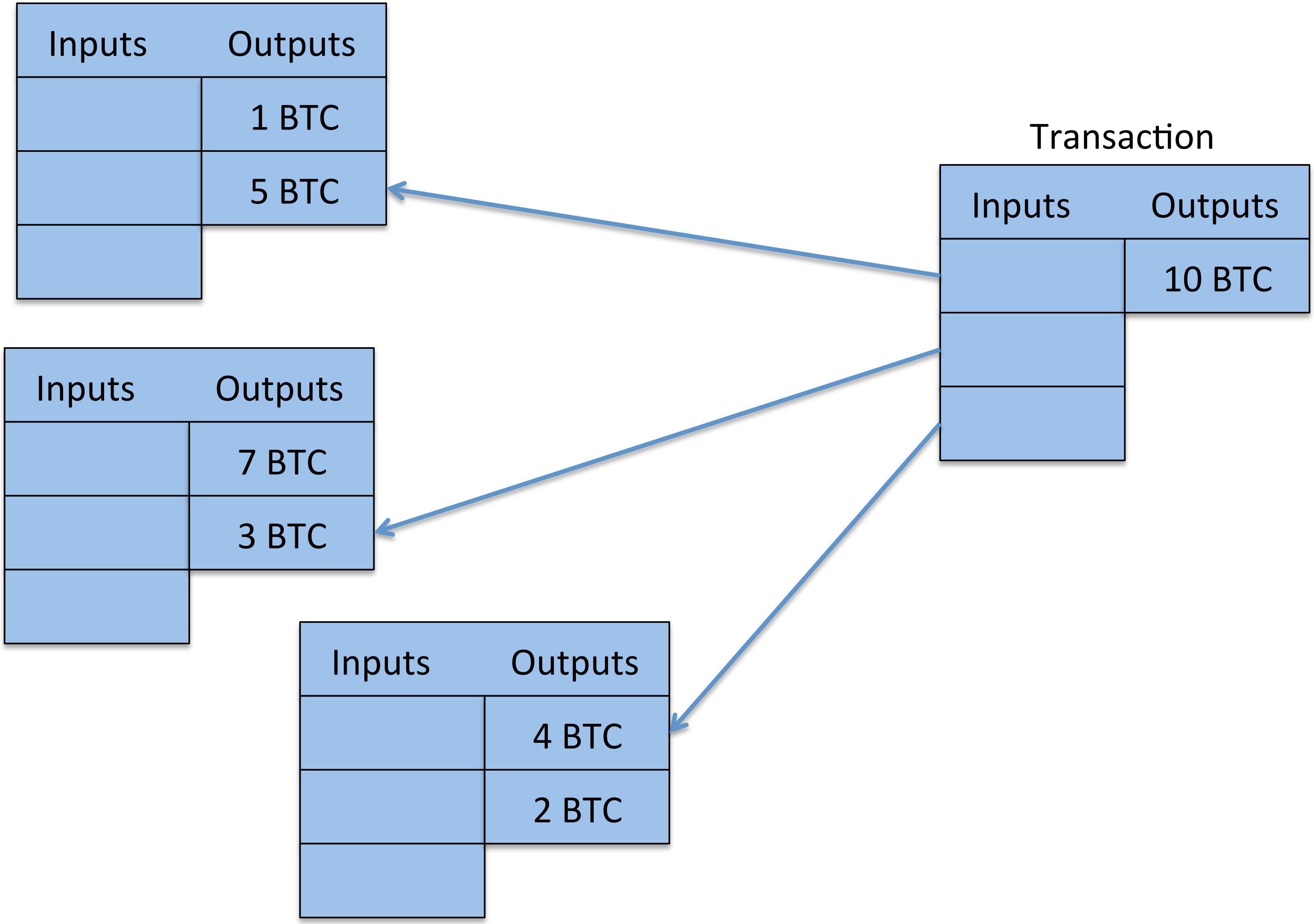
Transaction

Inputs

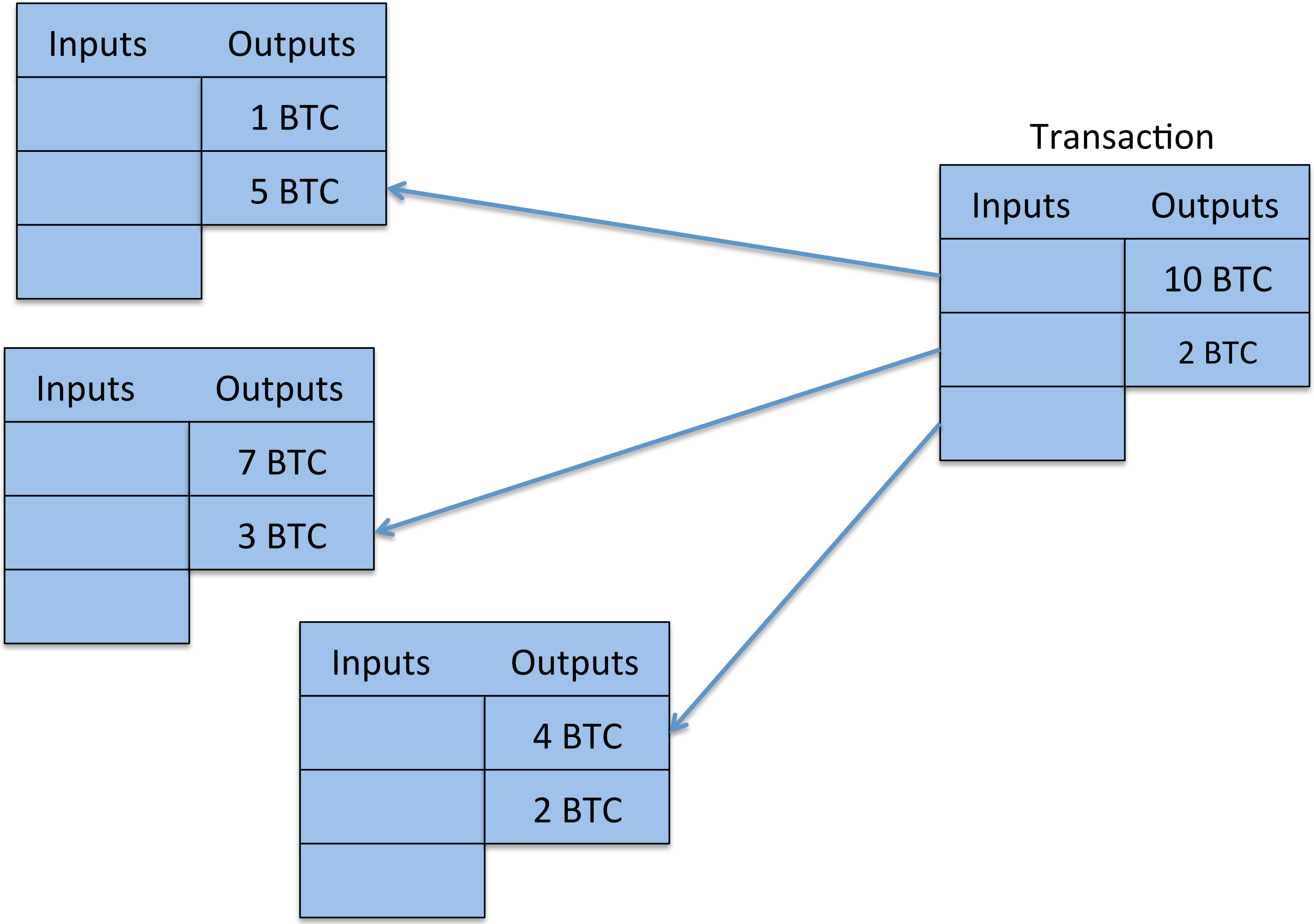
Outputs

10 BTC

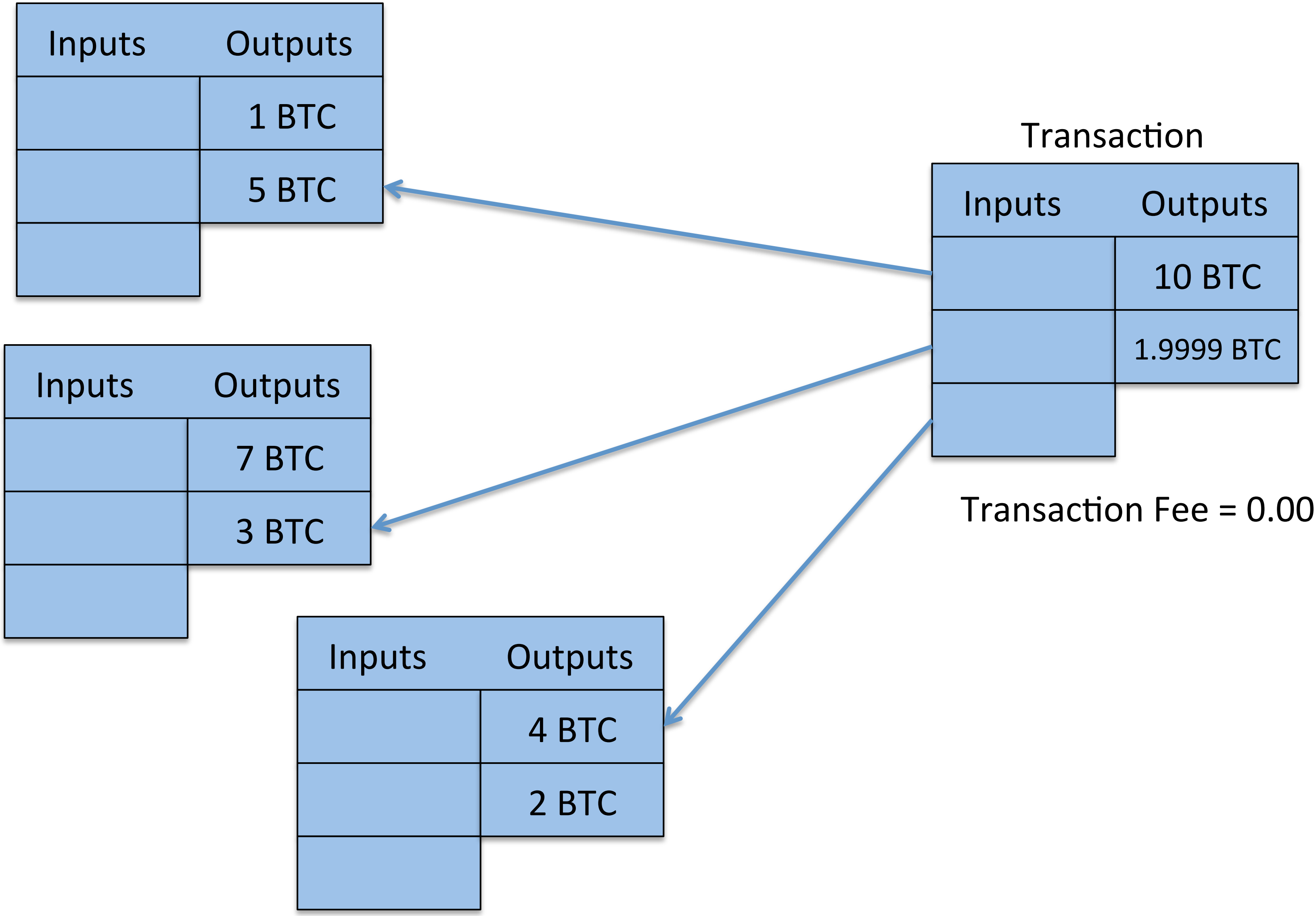
Creating a Transaction (2/7)



Creating a Transaction (4/7)



Creating a Transaction (4/7)



Inputs	Outputs
	1 BTC
	5 BTC

Inputs	Outputs
	7 BTC
	3 BTC

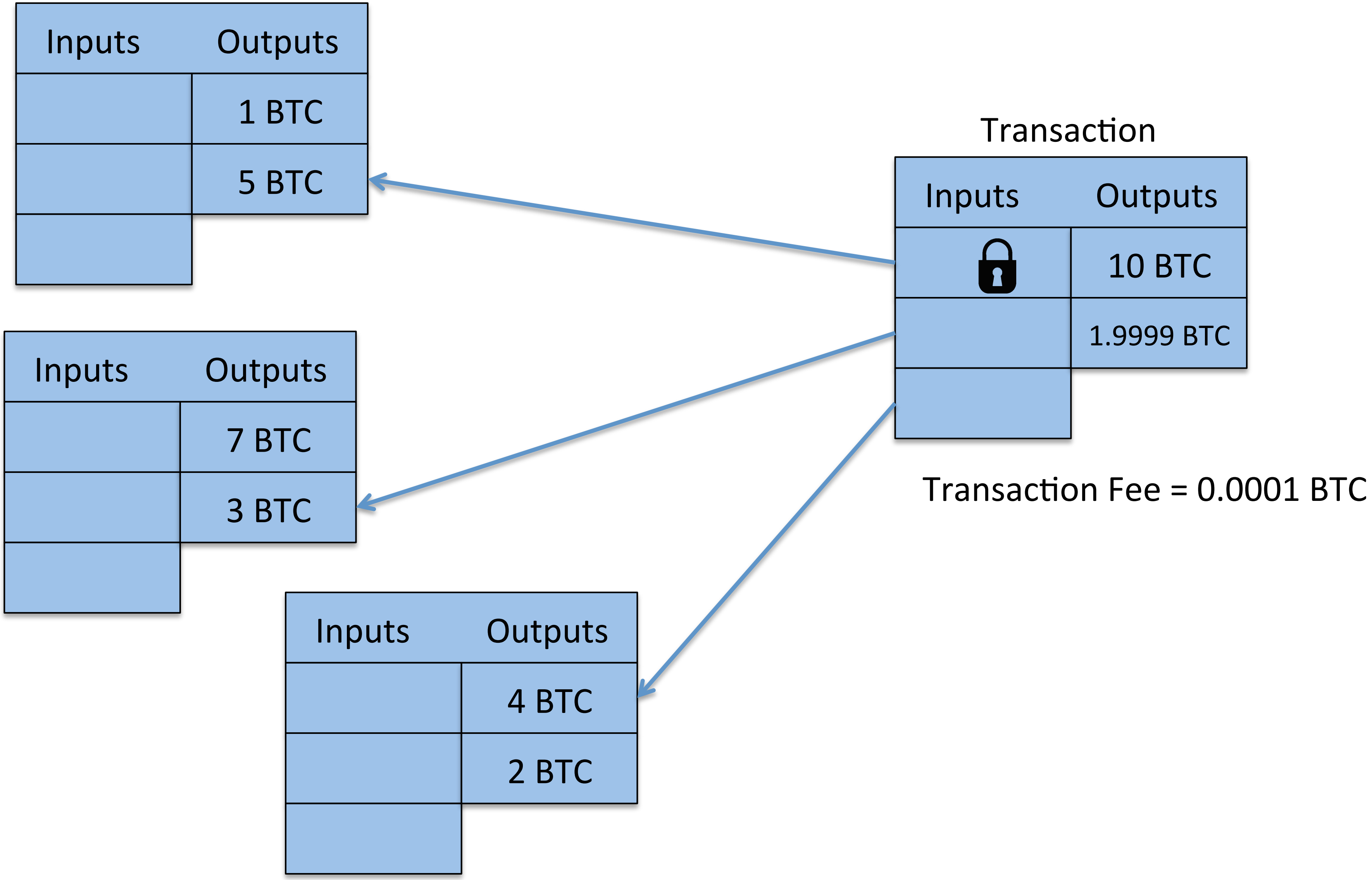
Inputs	Outputs
	4 BTC
	2 BTC

Transaction

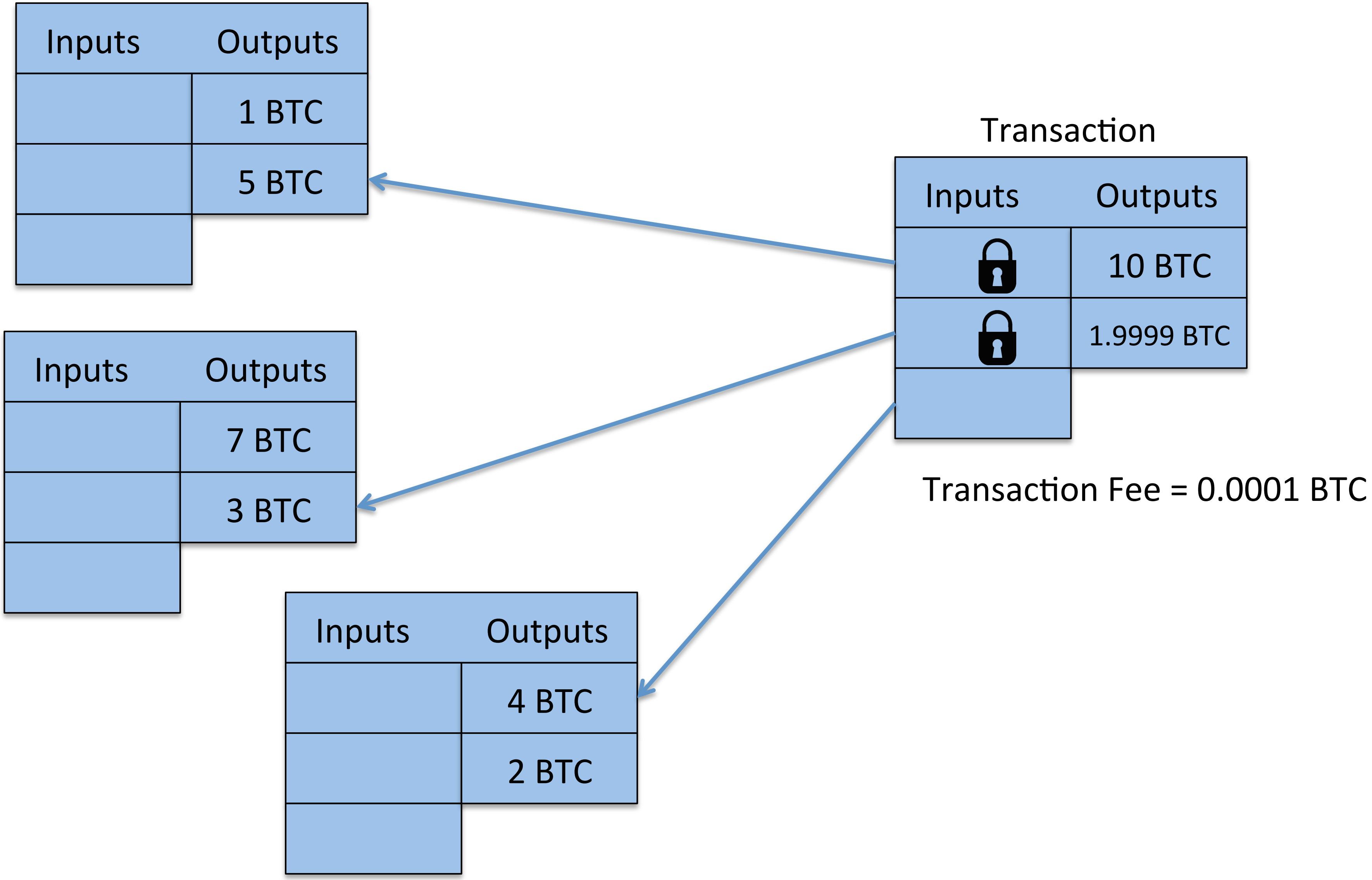
Inputs	Outputs
	10 BTC
	1.9999 BTC

Transaction Fee = 0.0001 BTC

Creating a Transaction (5/7)

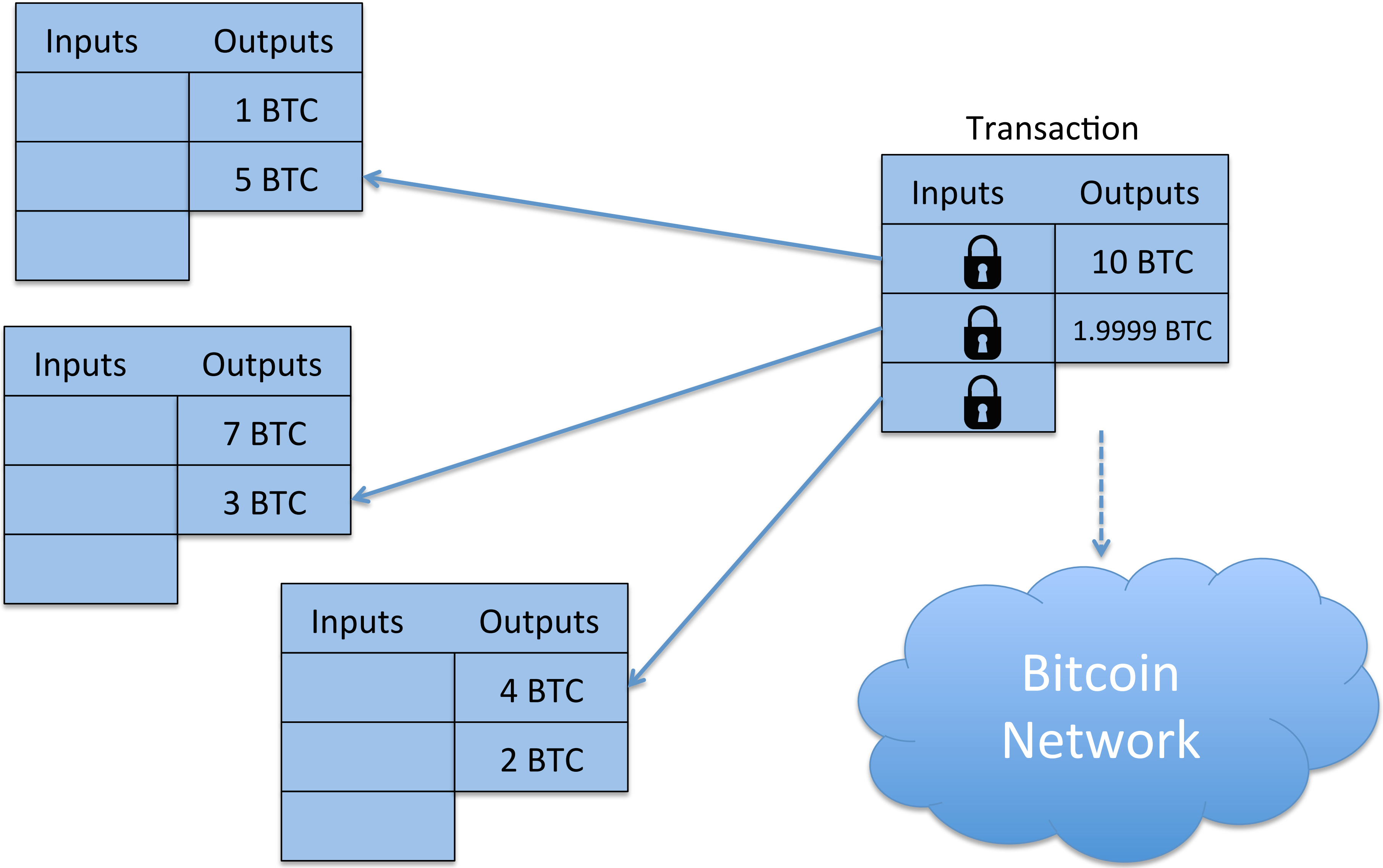


Creating a Transaction (6/7)



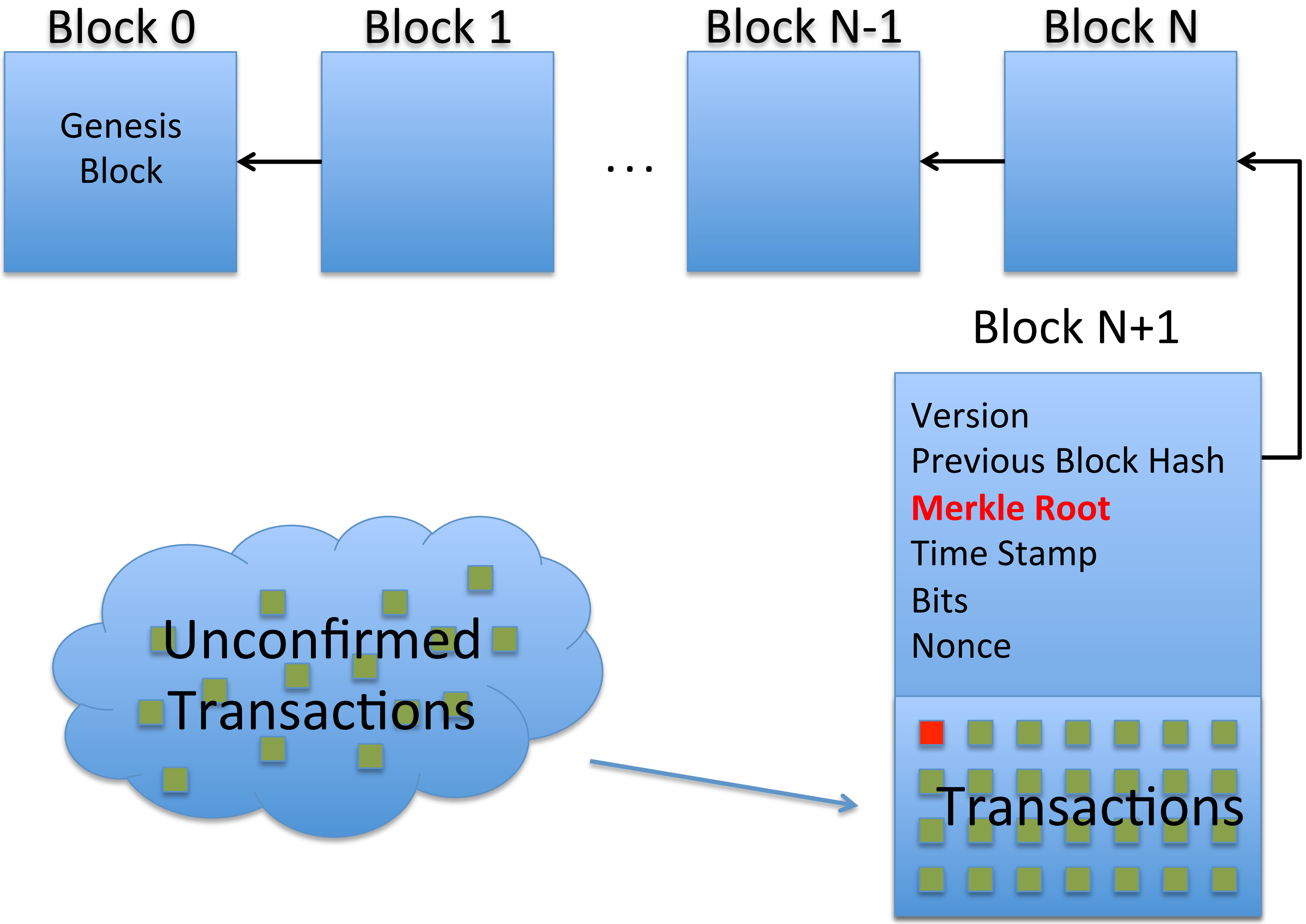
Transaction Fee = 0.0001 BTC

Creating a Transaction (7/7)

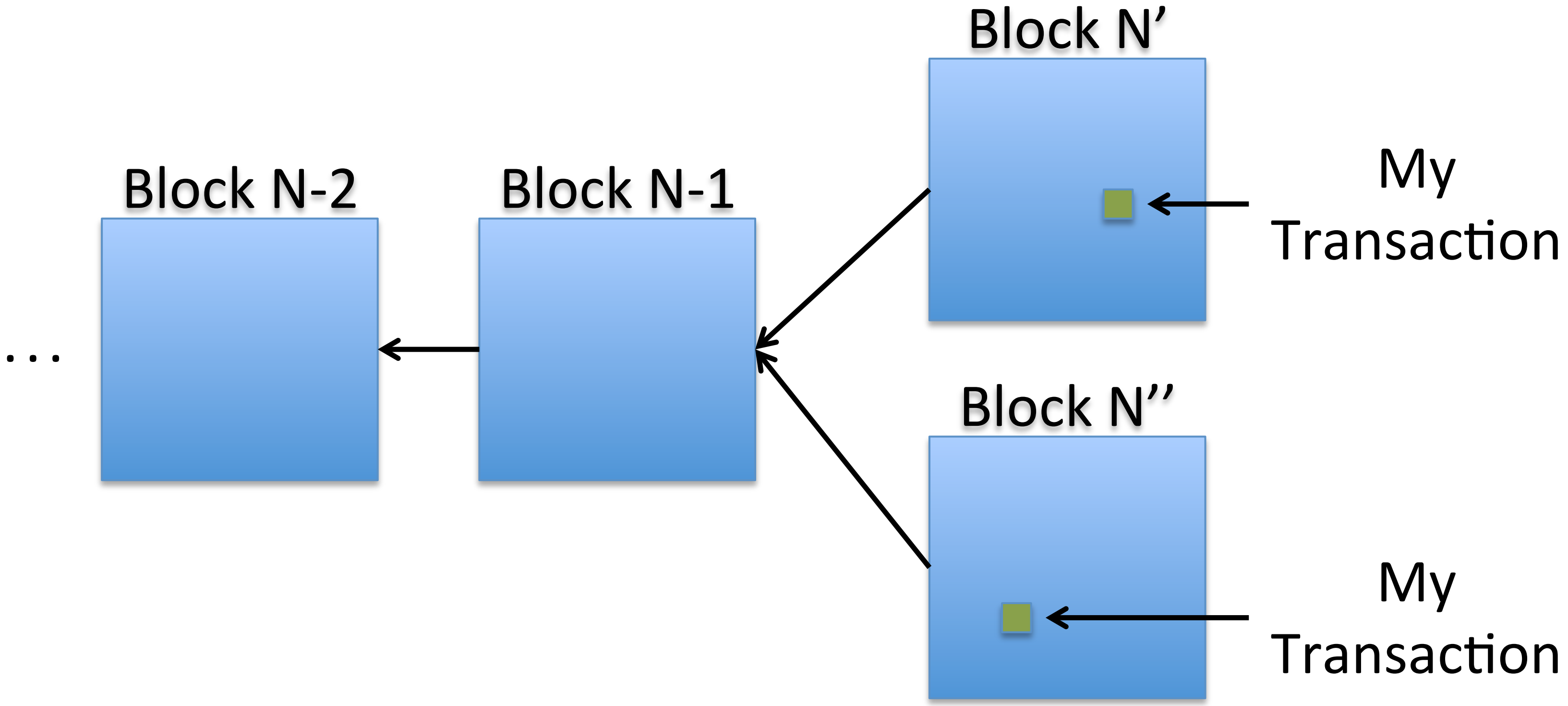


Transaction Relaying

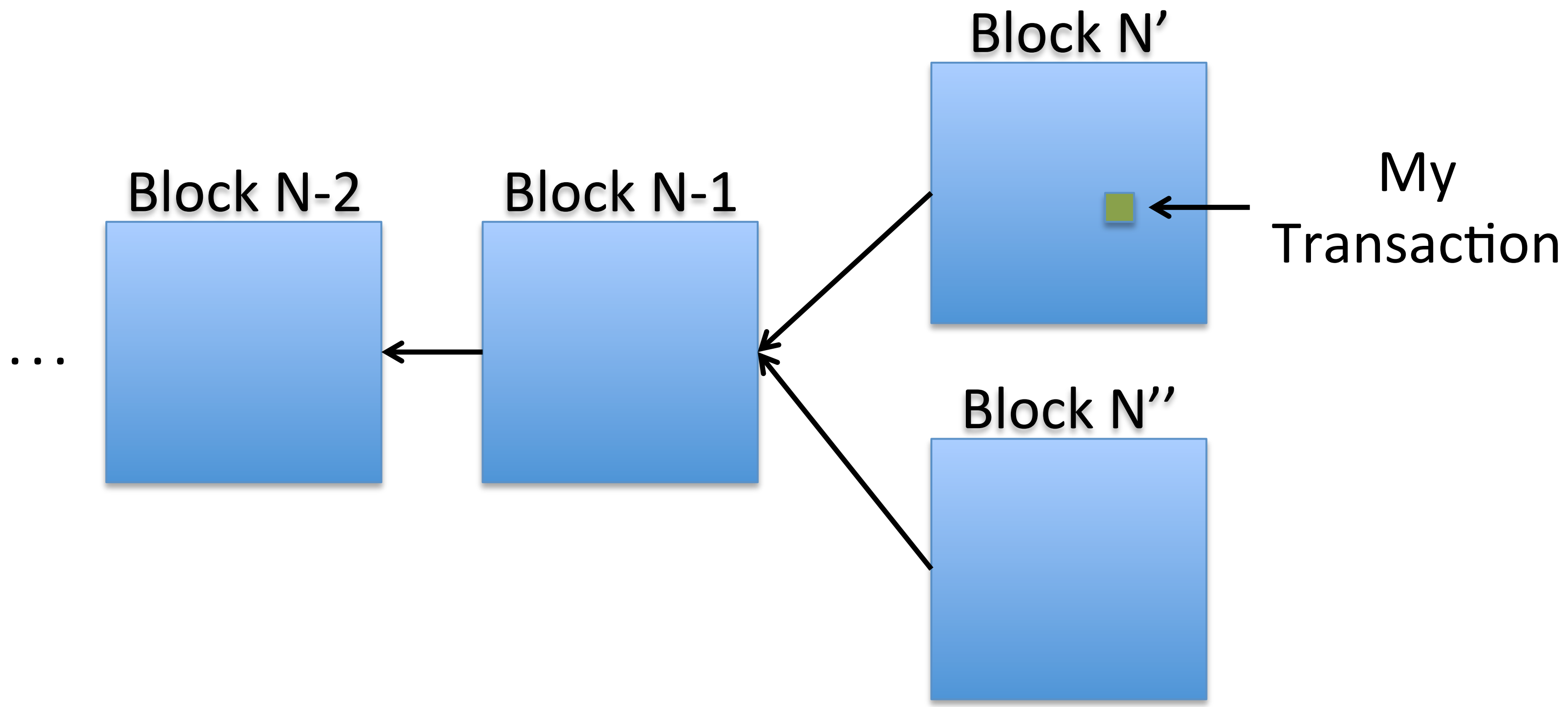
- Receive transaction from peer
- Verification (simplified):
  - Verify that the signatures are sound
  - Verify that the inputs are unspent
  - Verify that the sum of outputs <= sum of inputs
- Relay transaction to other peers


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

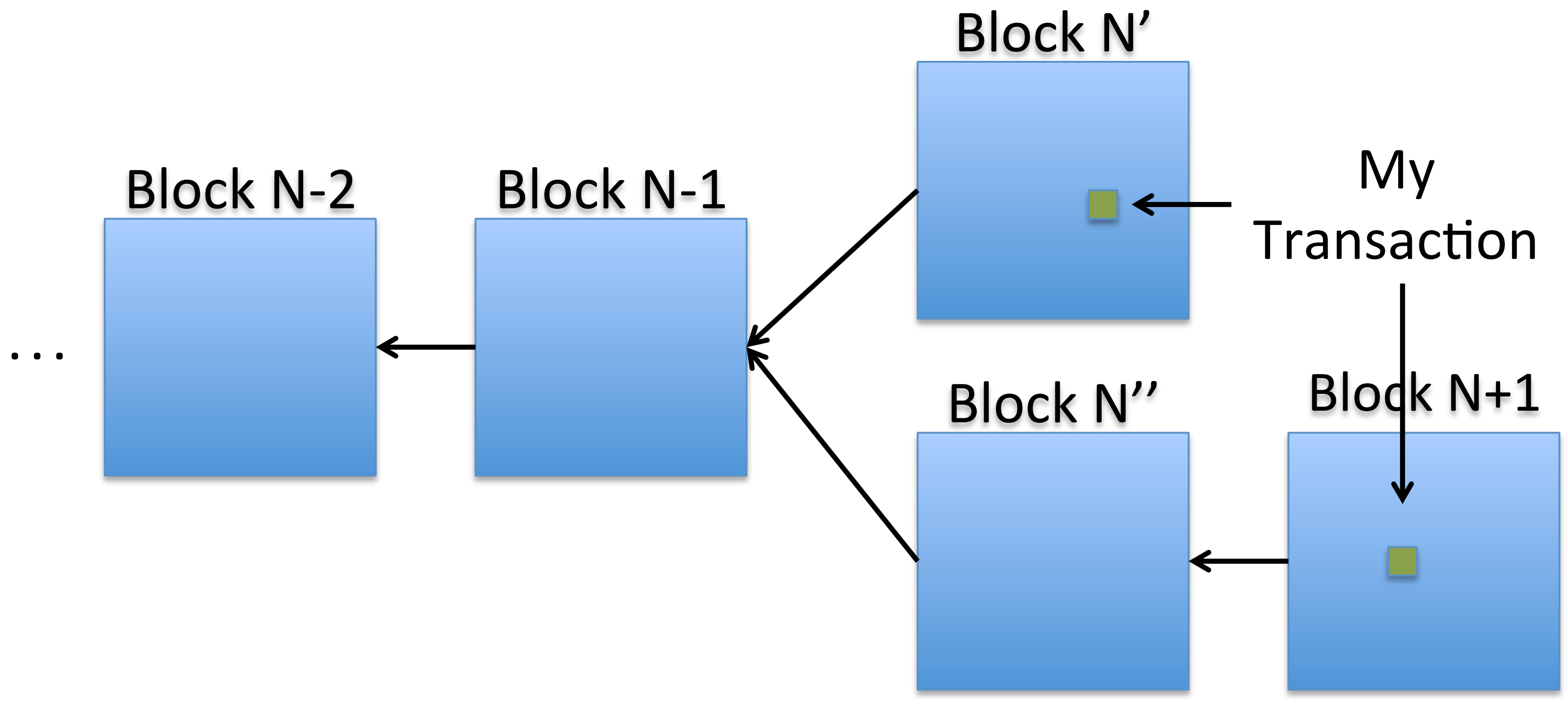
Transactions in Forks (1)



Transactions in Forks (2.1)



Transactions in Forks (2.2)

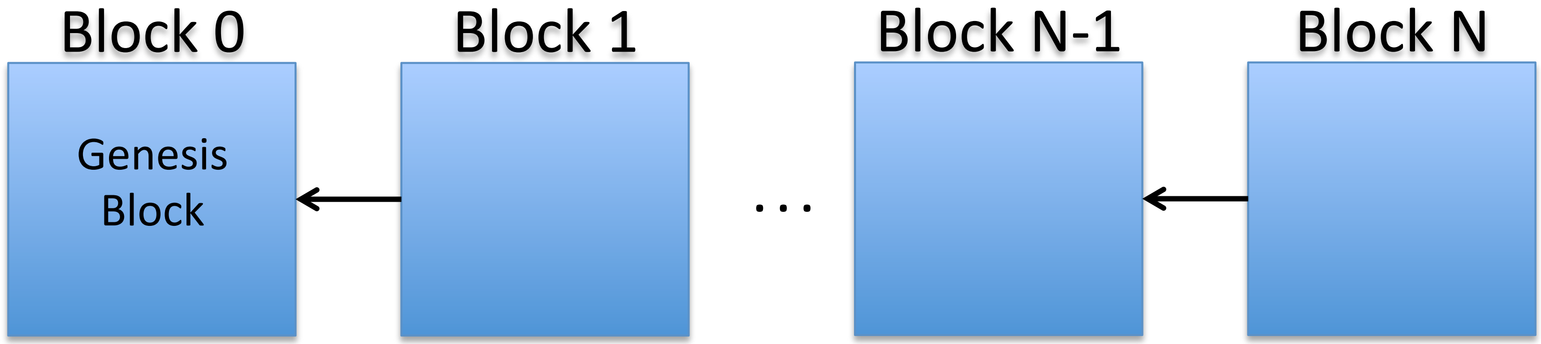


The longest chain wins!

Properties of Bitcoin (1/3)

No Counterfeiting

“NOBODY” can increase money supply at will



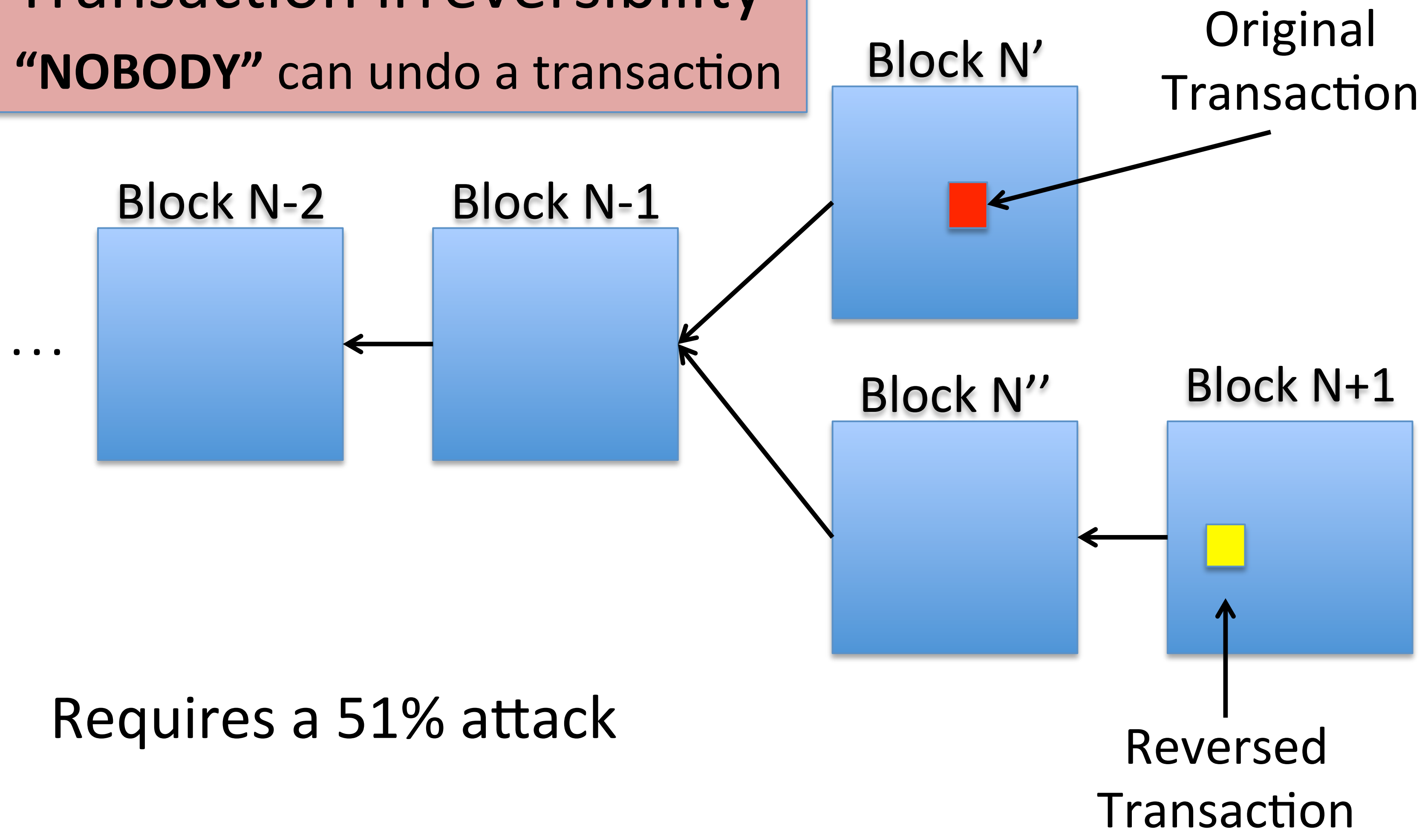
You are competing with the biggest distributed computer the world has seen.

If you can beat it, it just gets harder.

Properties of Bitcoin (2/3)

Transaction irreversibility

“NOBODY” can undo a transaction

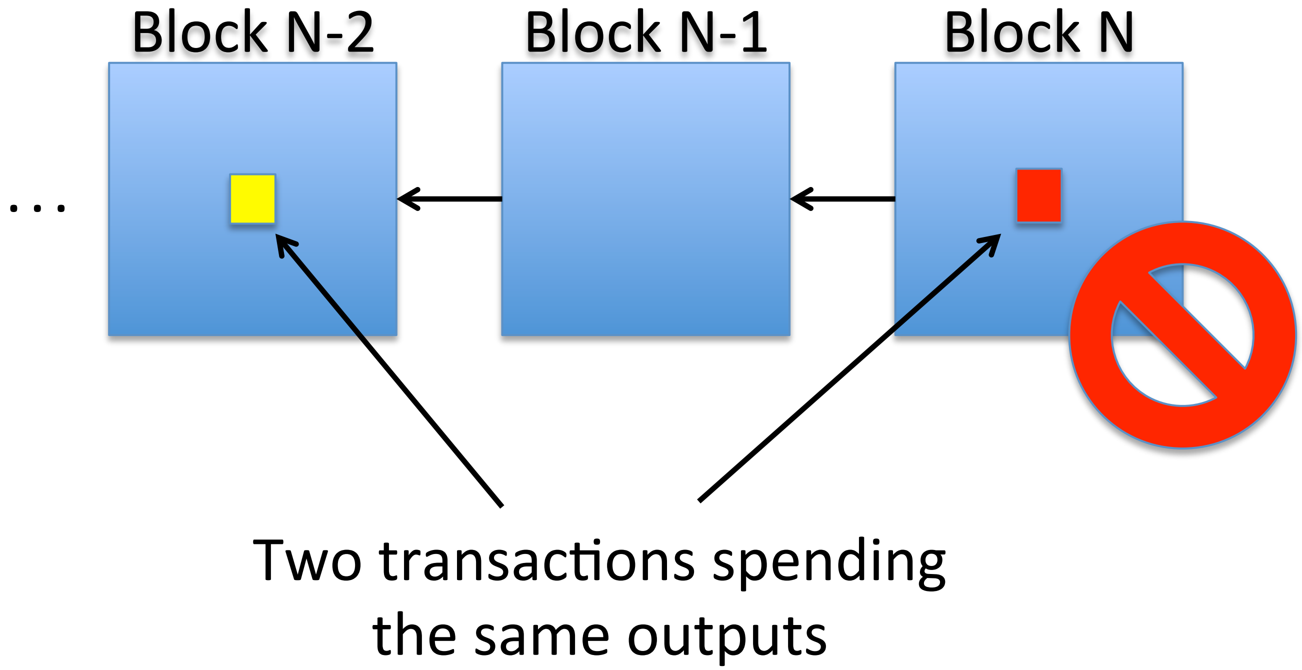


Requires a 51% attack

Properties of Bitcoin (3/3)

No Double Spending

NOBODY can spend the same value more than once



Two transactions spending
the same outputs

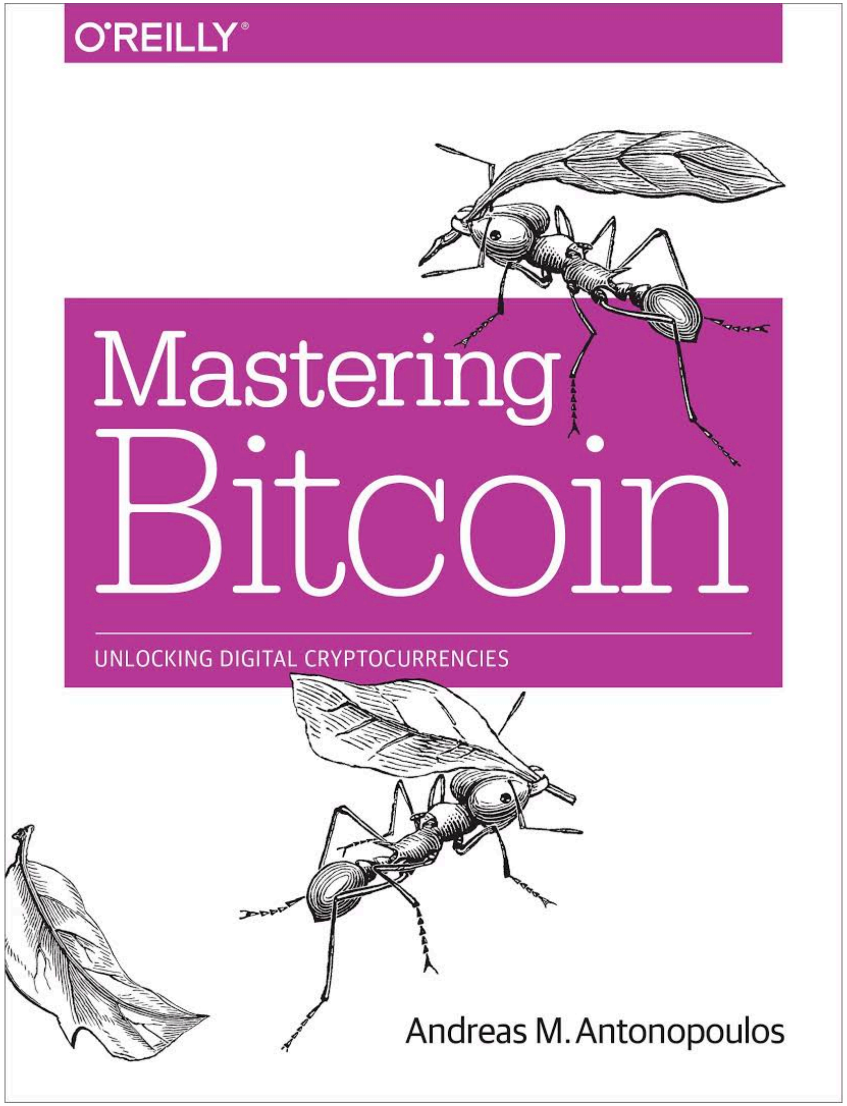
Blockchain Tech is New

Trustless decentralized ordering of events

- Decentralized DNS with **Namecoin**
  - A decentralized open source information registration and transfer system.
- Decentralized Stock Exchange
  - Coloredcoins.org is one of several solutions that allow you to issue and track digital assets on top of the Bitcoin blockchain.

We can do stuff that wasn’t possible before

Want to Know More?



Questions?

Jan Møller

Co-founder, CTO

Chainalysis