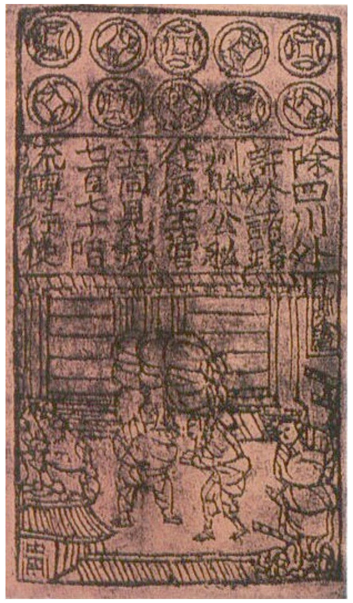
What is Bitcoin?

How Value Can Be Sent through the Internet
without a Third Party

Outline

- What is money?
- Cryptography primer
- Peer-to-Peer (P2P) networks
- What is Bitcoin?
- Future applications

What is money?

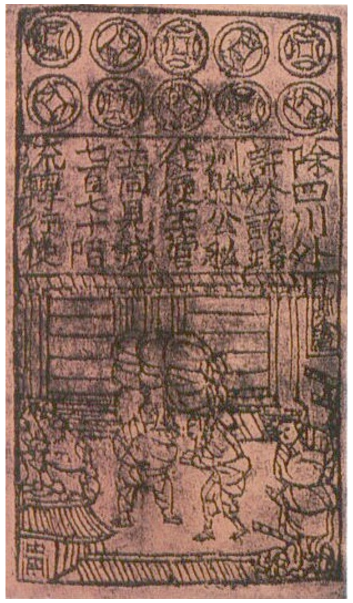


FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
B 03542754 F
WASHINGTON, D.C.
ONE DOLLAR

What is money?

Greek Coins

Chinese Banknote



Wampum

US Dollar

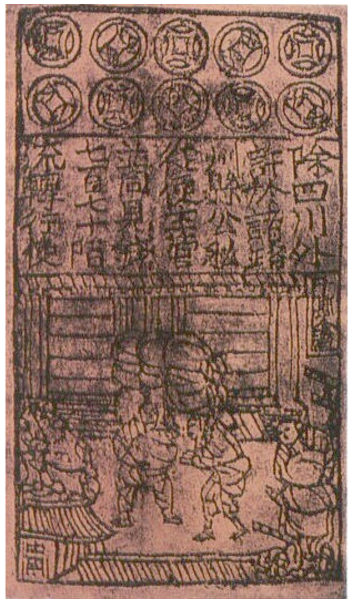
FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
B 03542754 F
WASHINGTON, D.C.
ONE DOLLAR

Shells from South Africa (75,000 BP)

What is money?

v1.0

v2.0



v3.0

v3.0

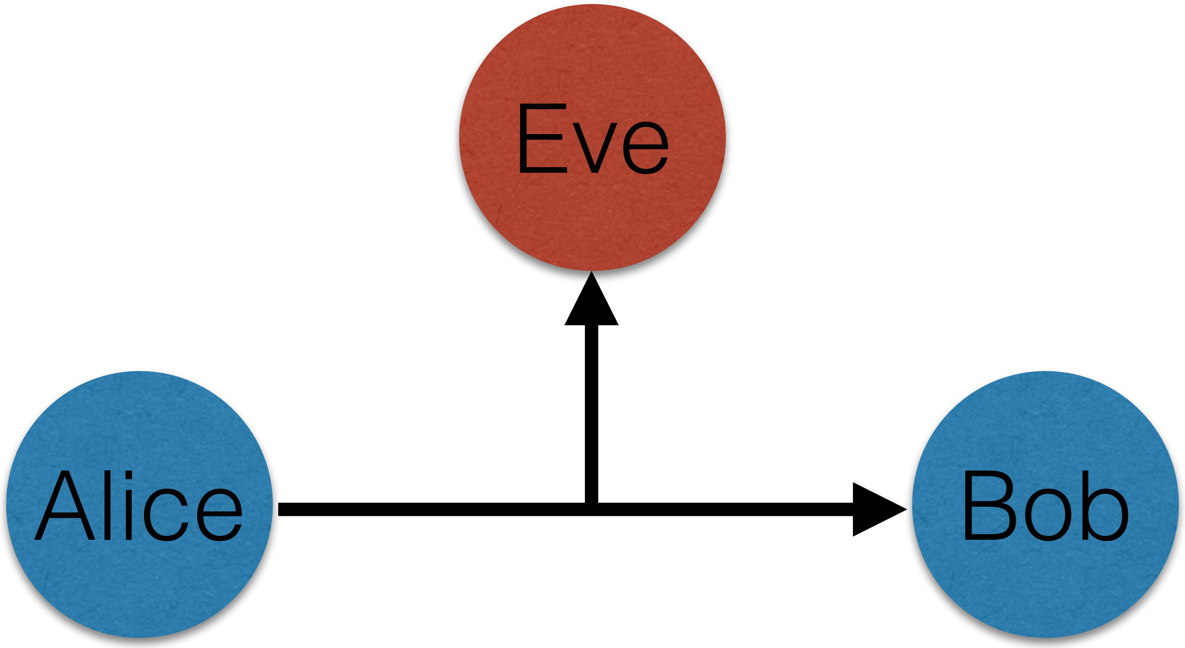
FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
B 03542754 F
WASHINGTON, D.C.
ONE DOLLAR

v4.0, v5.0

Dutch governor of New Amsterdam took out a large loan from a British bank in Wampum

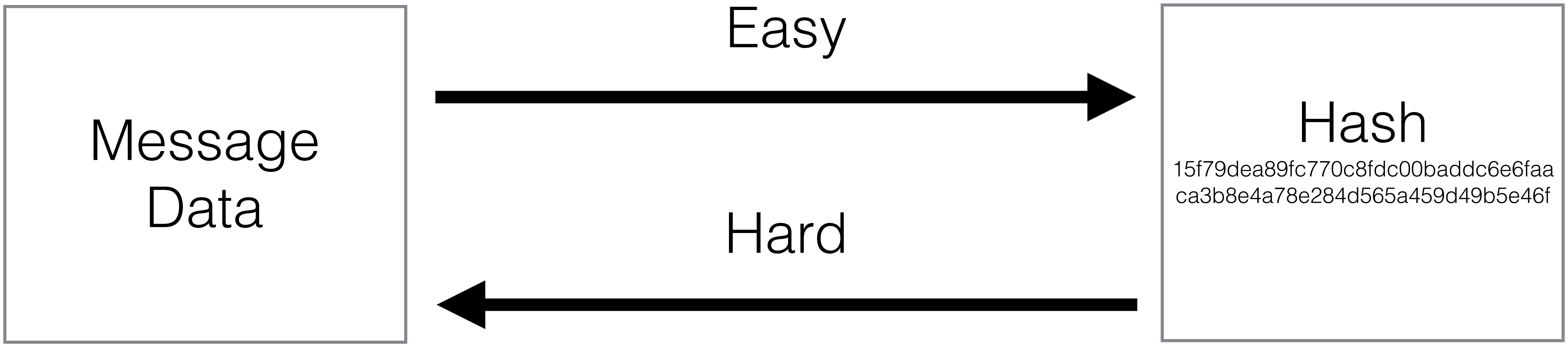
Cryptography

- Cryptographic Hash Function
- Public Key Encryption
- Digital Signatures



Cryptographic Hash Function

“One way function”



Message Data

Easy

Hard

Hash

15f79dea89fc770c8fdc00baddc6e6faa
ca3b8e4a78e284d565a459d49b5e46f

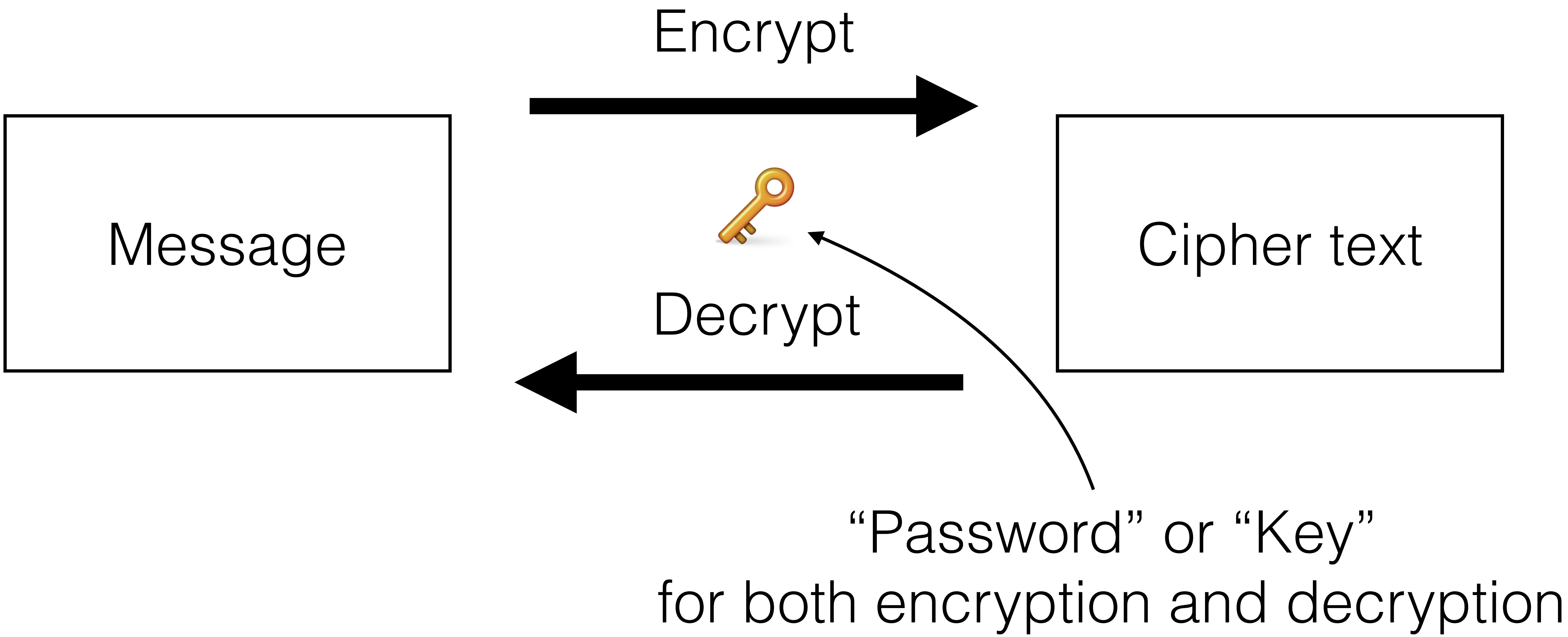
sha256(“Message Data”) = 15f79dea89fc770c8fdc00baddc6e6faaca3b8e4a78e284d565a459d49b5e46f

Cryptographic Hash Function

sha256(“Message Data”) = 15f79dea89fc770c8fdc00baddc6e6faaca3b8e4a78e284d565a459d49b5e46f

- Message authentication
- Password verification
- Unique identifier

Symmetric Cryptography



Encrypt

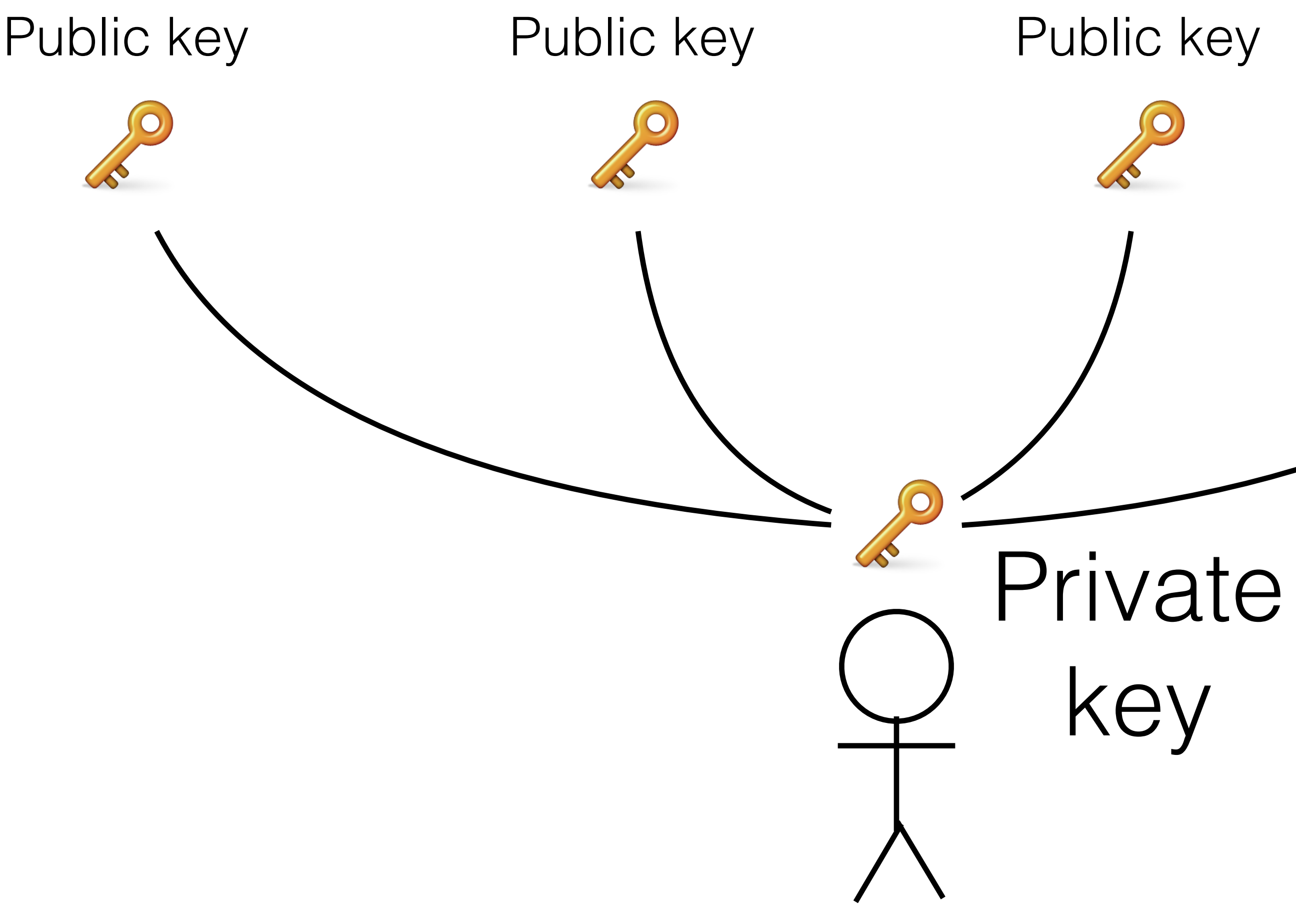
Message

Cipher text

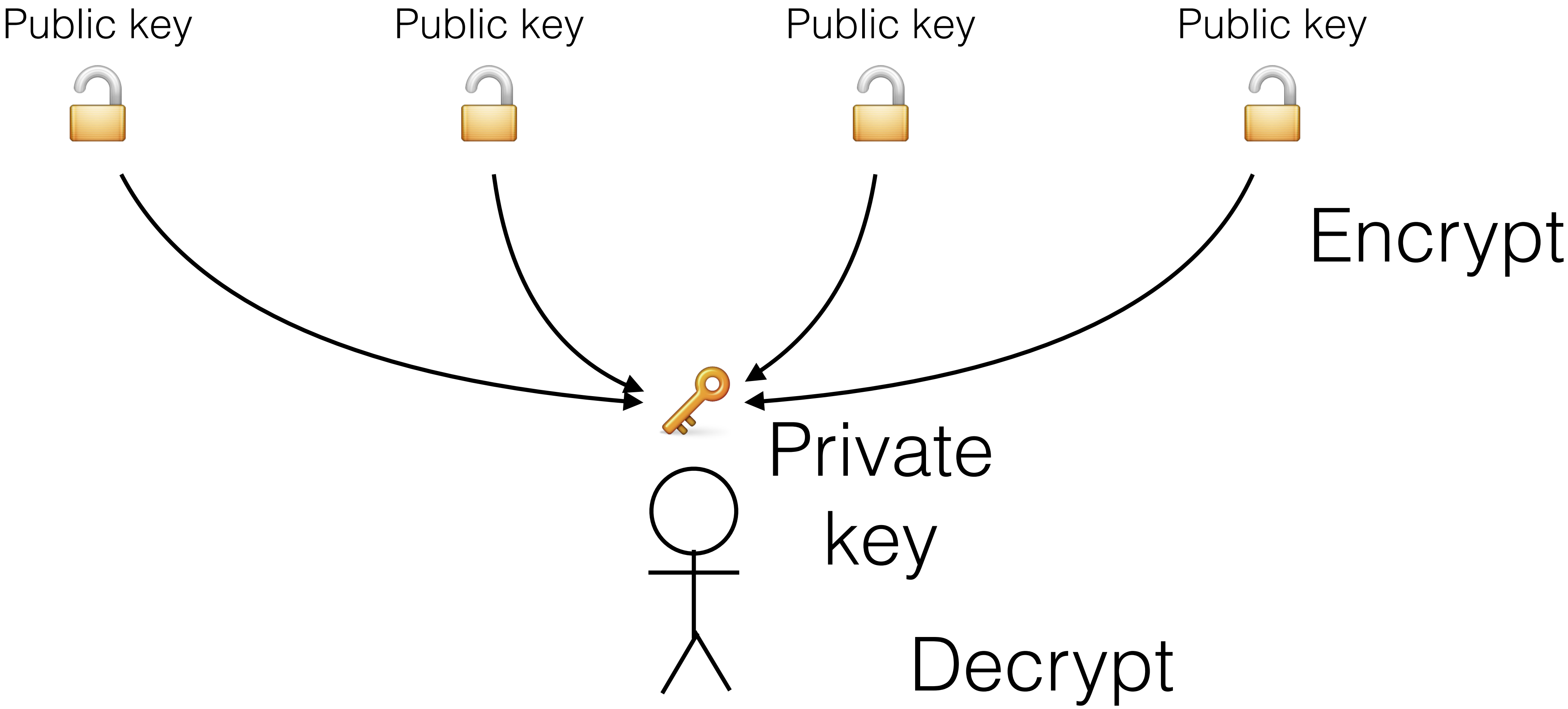
Decrypt

“Password” or “Key”
for both encryption and decryption

Asymmetric Keys



Public Key Encryption



Public key

Public key

Public key

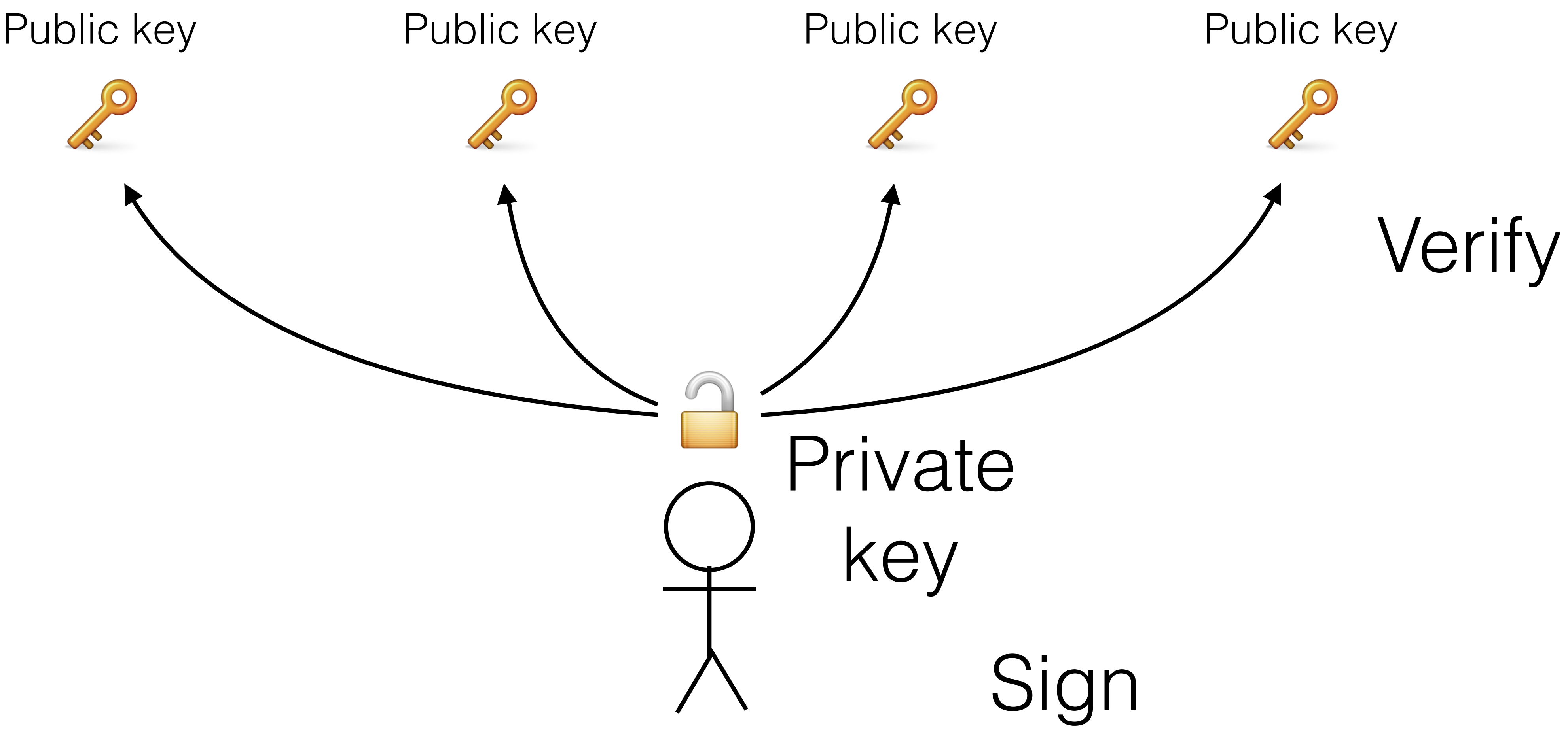
Public key

Encrypt

Private key

Decrypt

Digital Signature



Public key

Public key

Public key

Public key

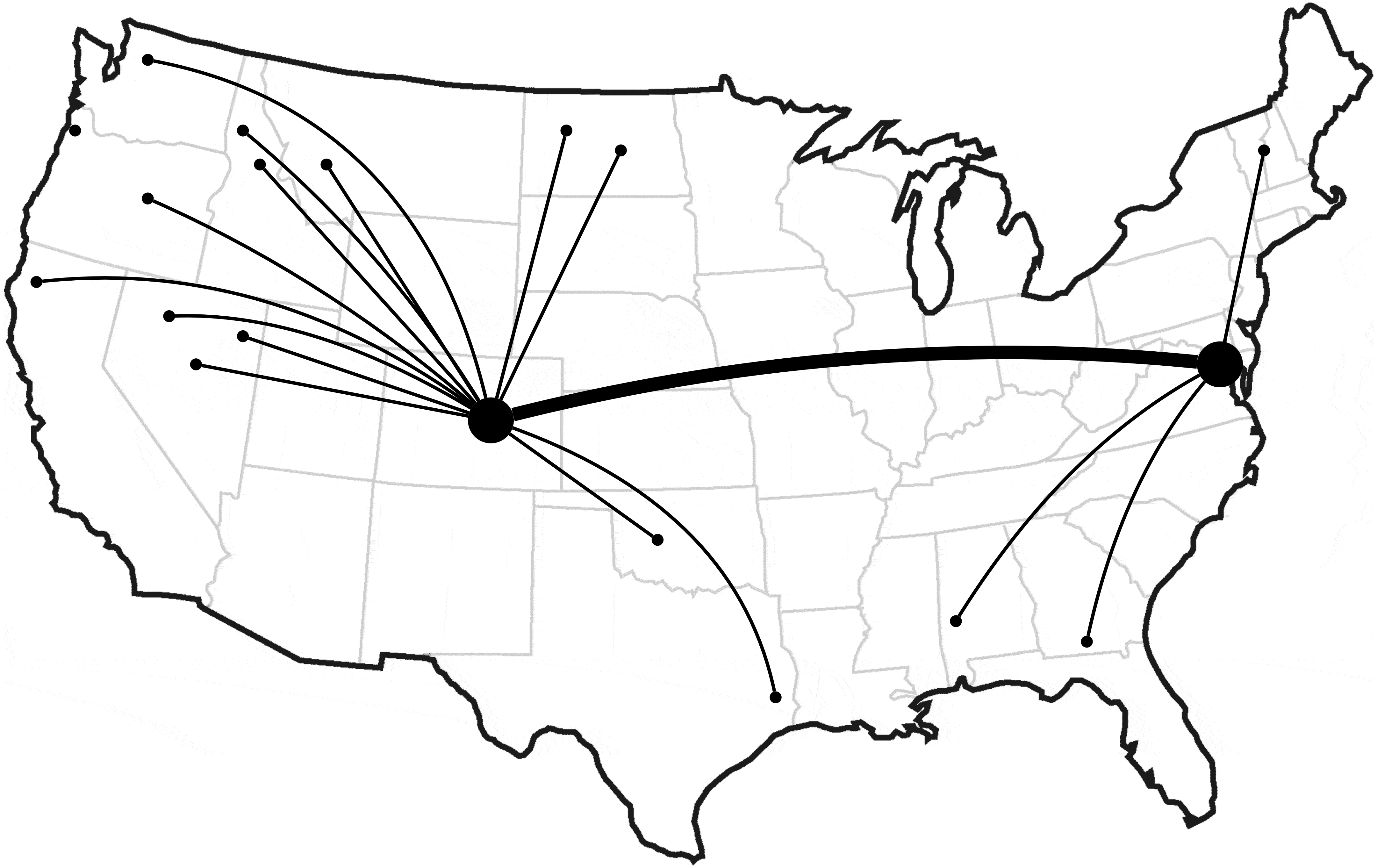
Verify

Private key

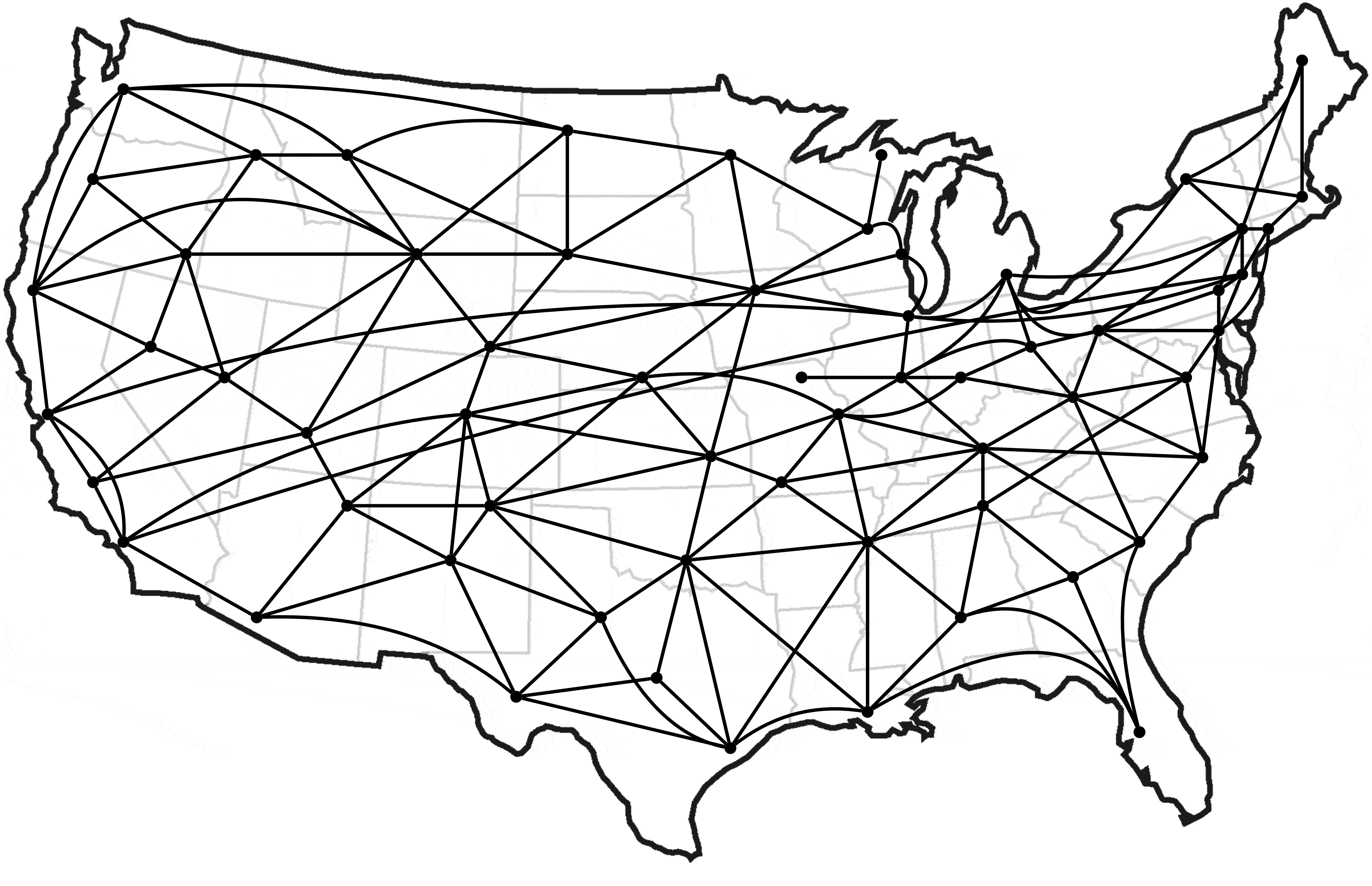
Sign

Why the Internet?

Why the Internet?



Why the Internet?



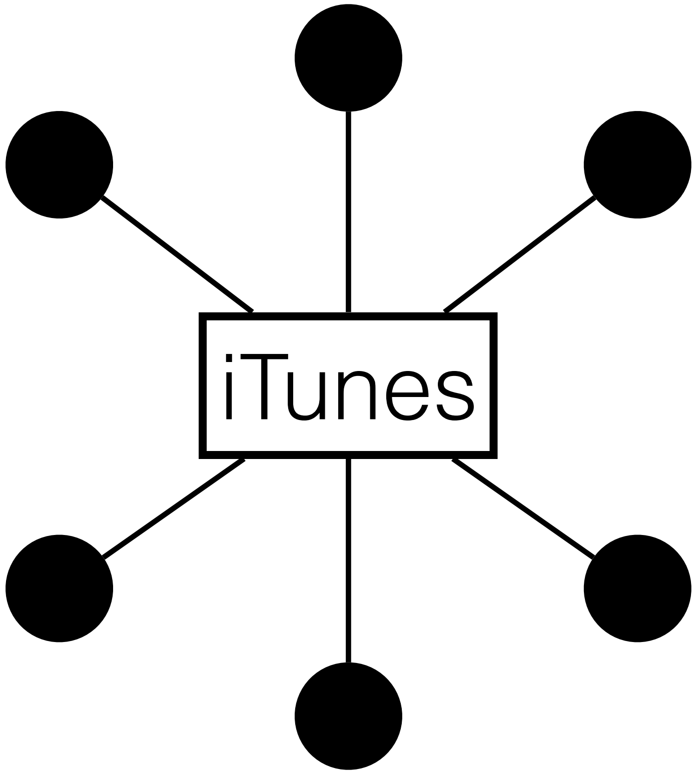
Why the Internet?

Nuclear attack resistant

P2P Networks

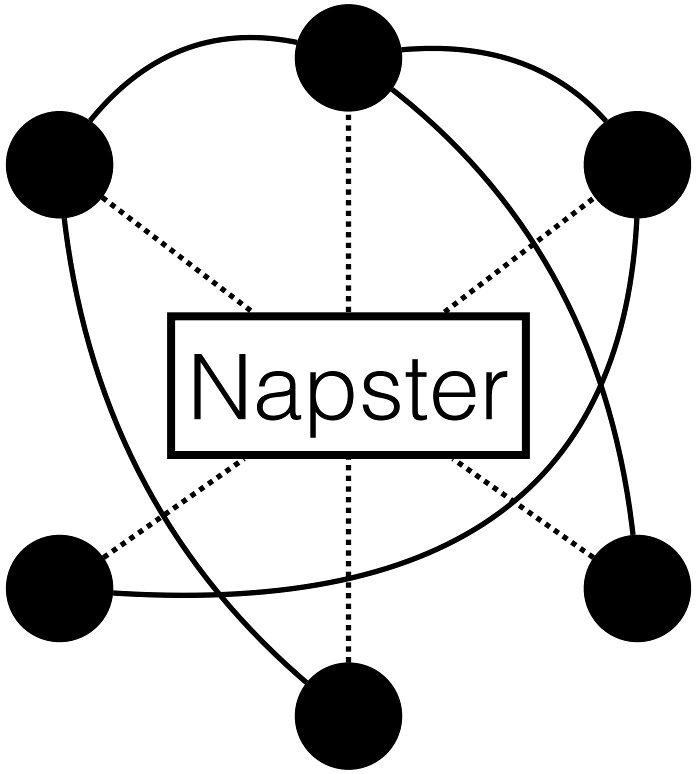
— Download

┄ Get Information



iTunes

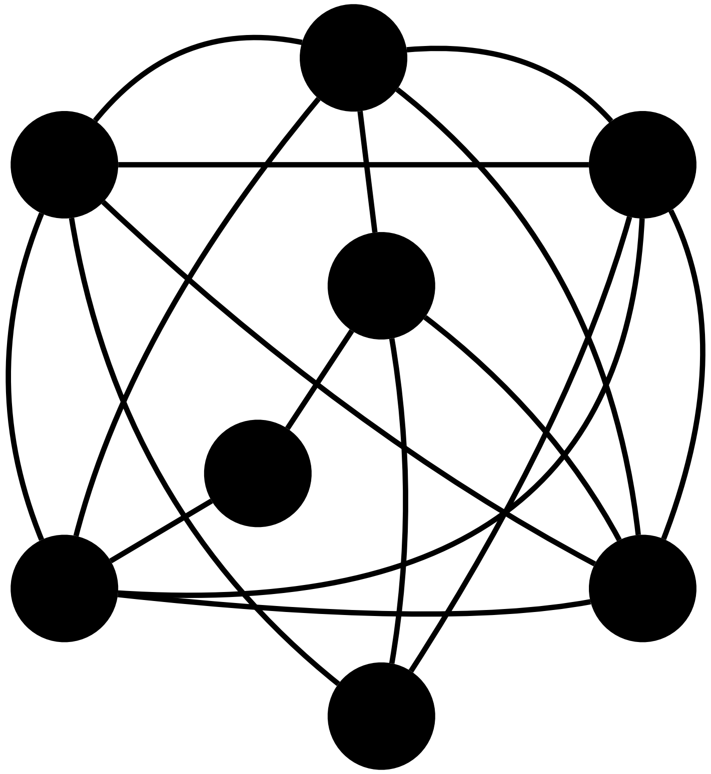
Centralized



Napster

Distributed

Bittorrent

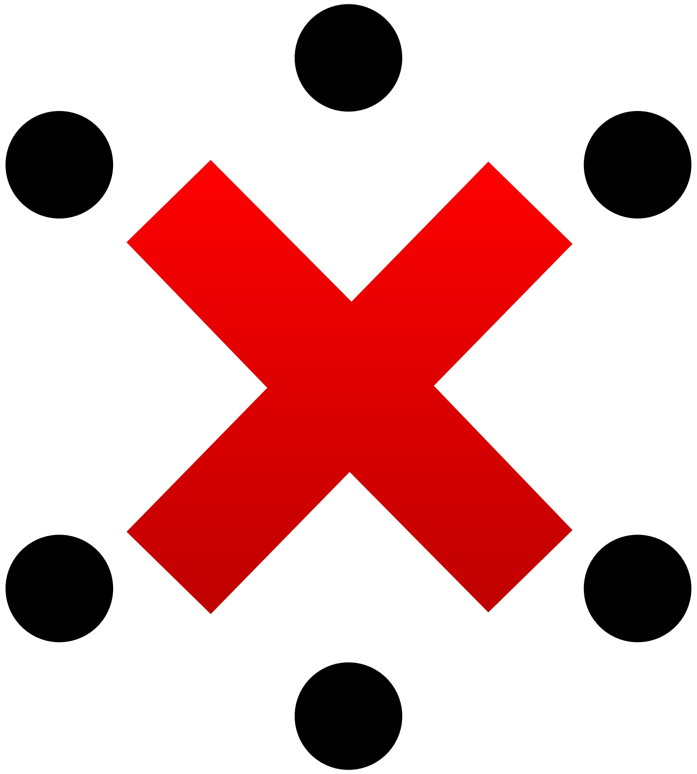


Decentralized

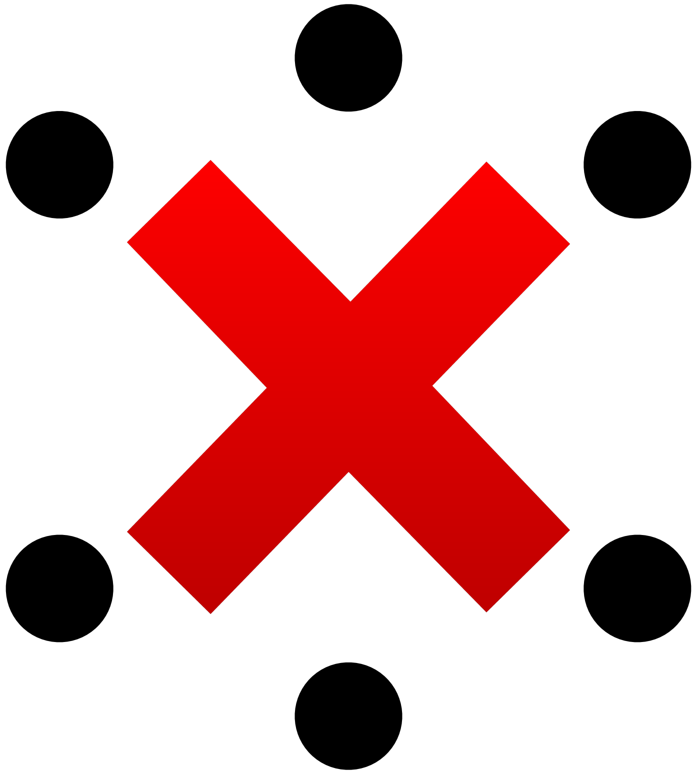
P2P Networks

—— Download

········ Get Information

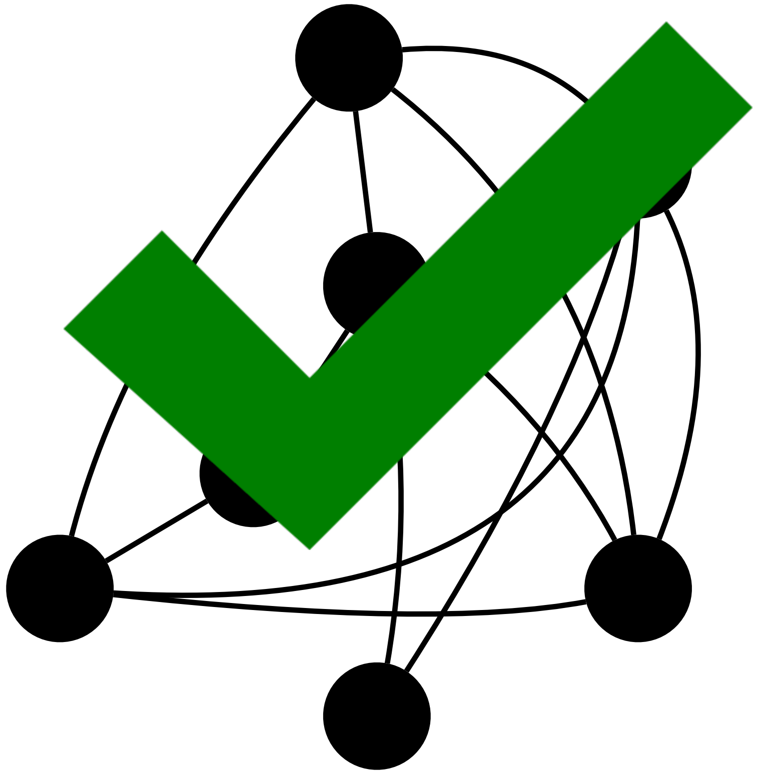


Centralized

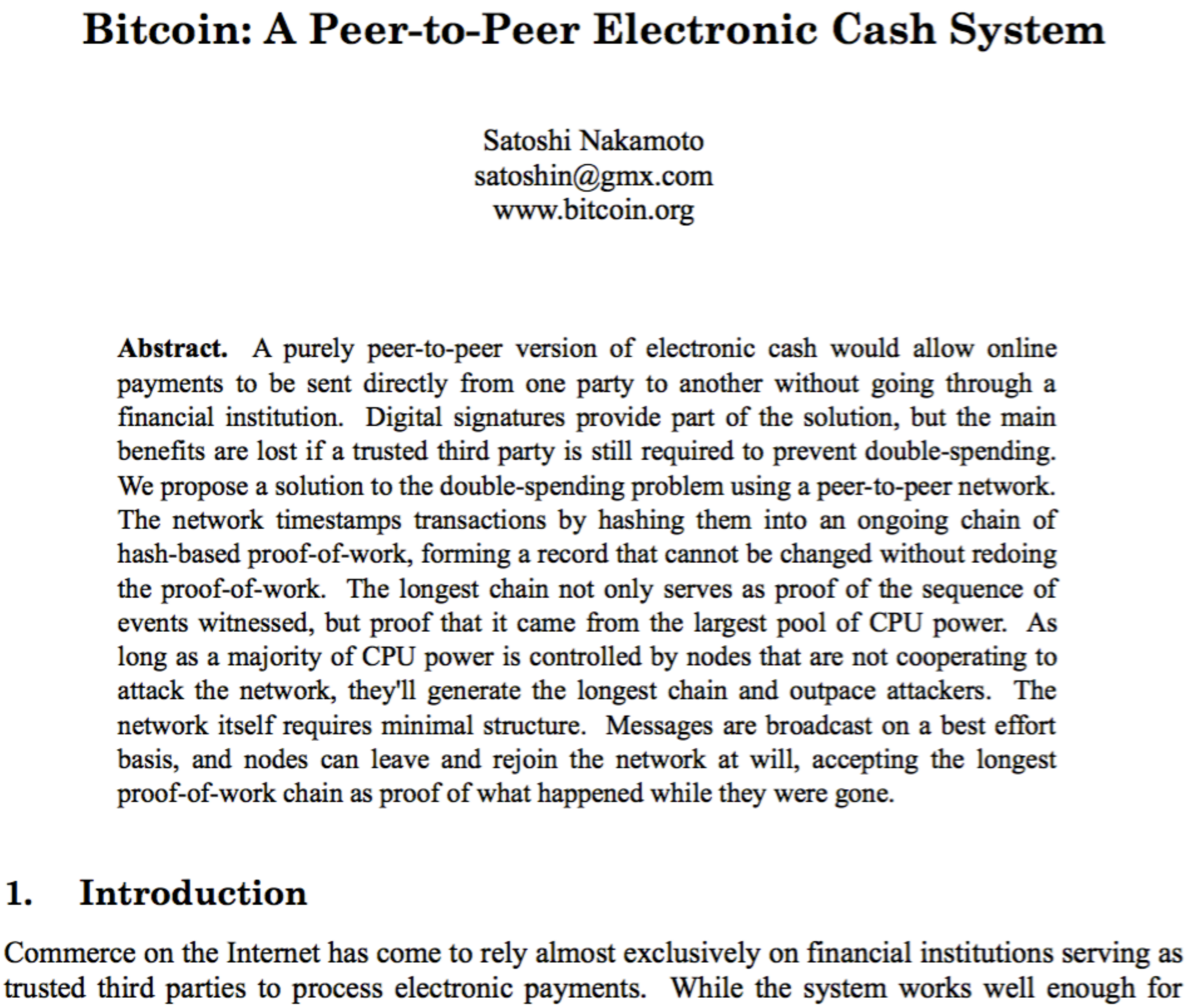


Distributed

Bittorrent



Decentralized



Bitcoin: A Peer-to-Peer Electronic Cash System

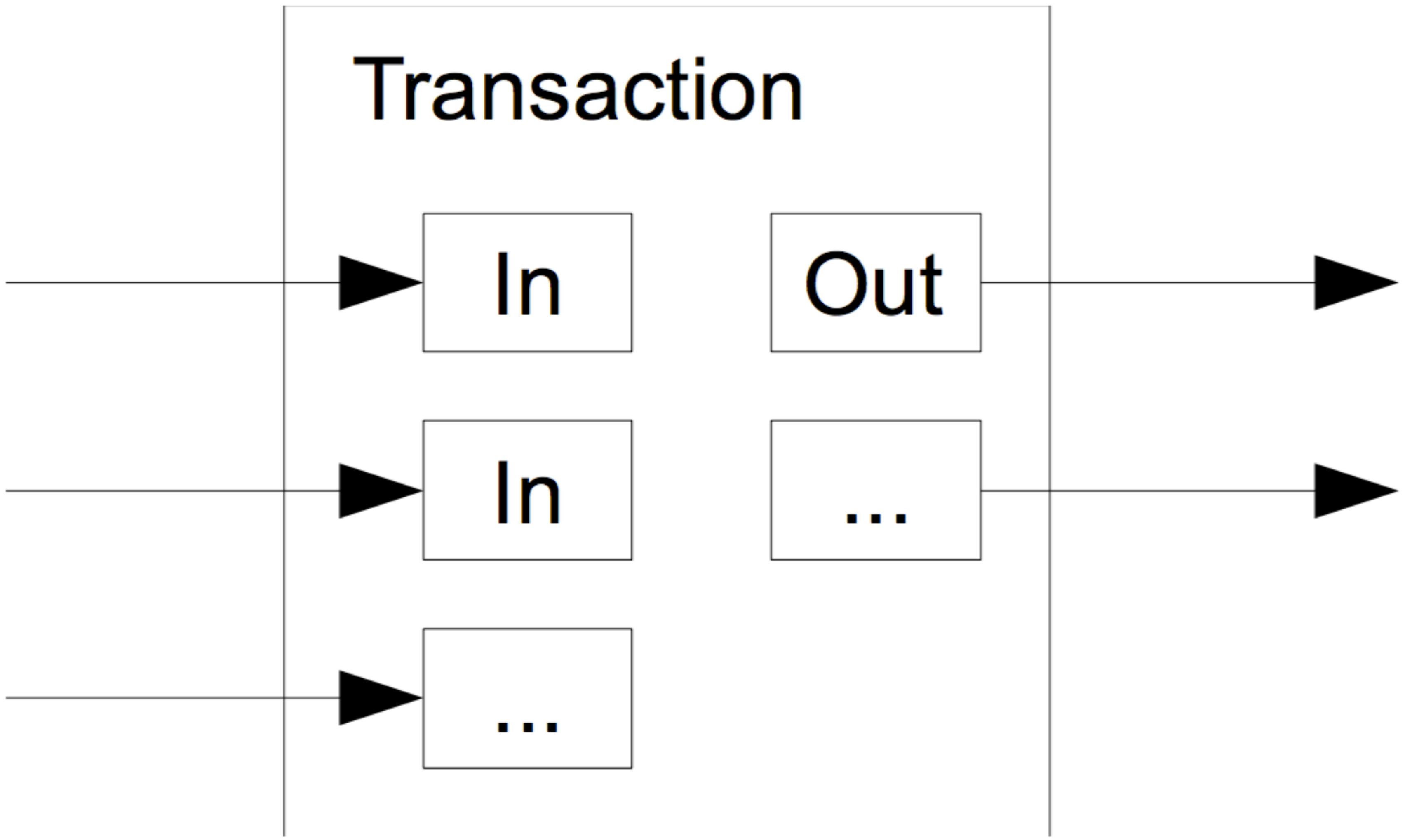
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

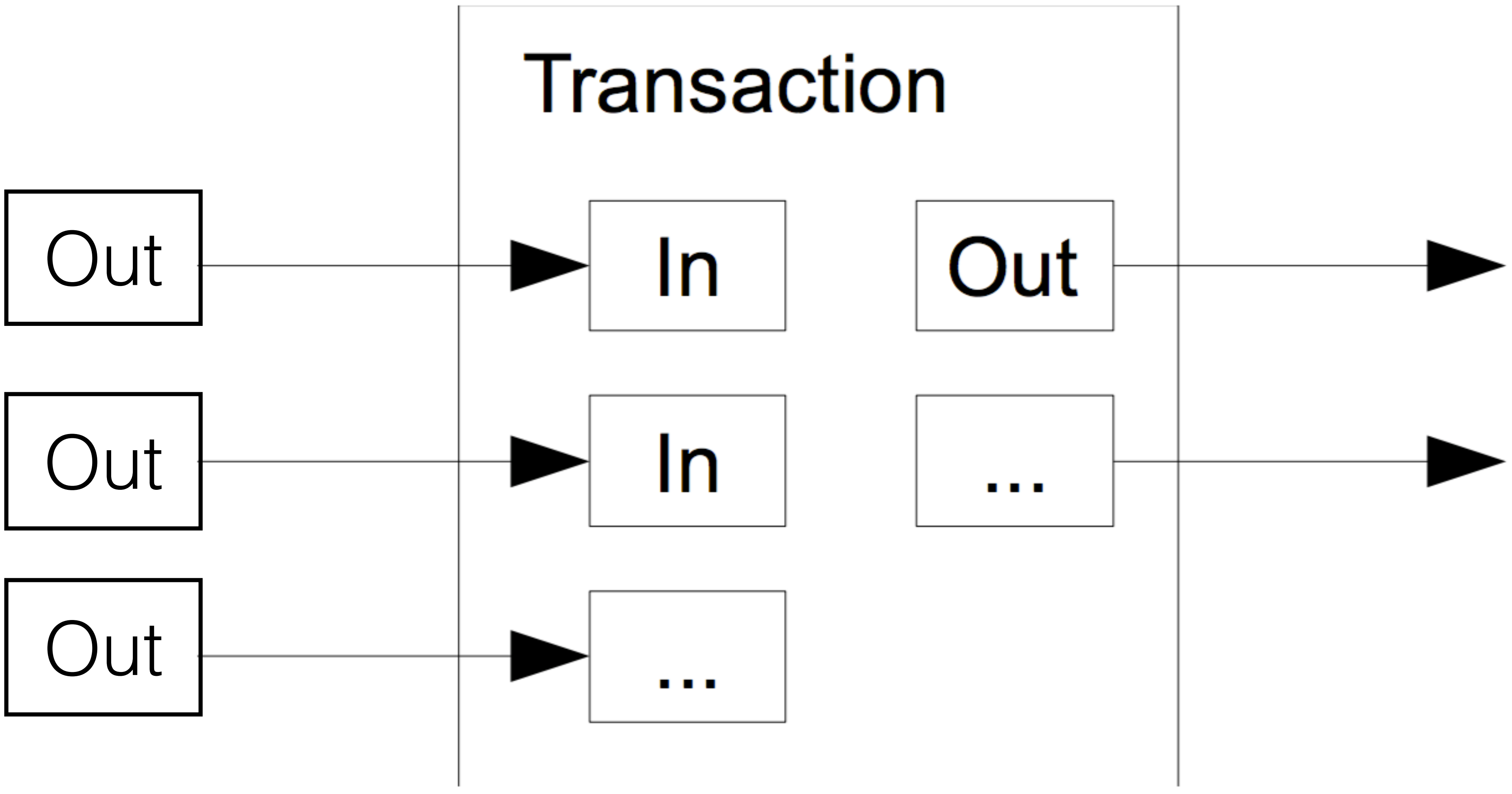
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for

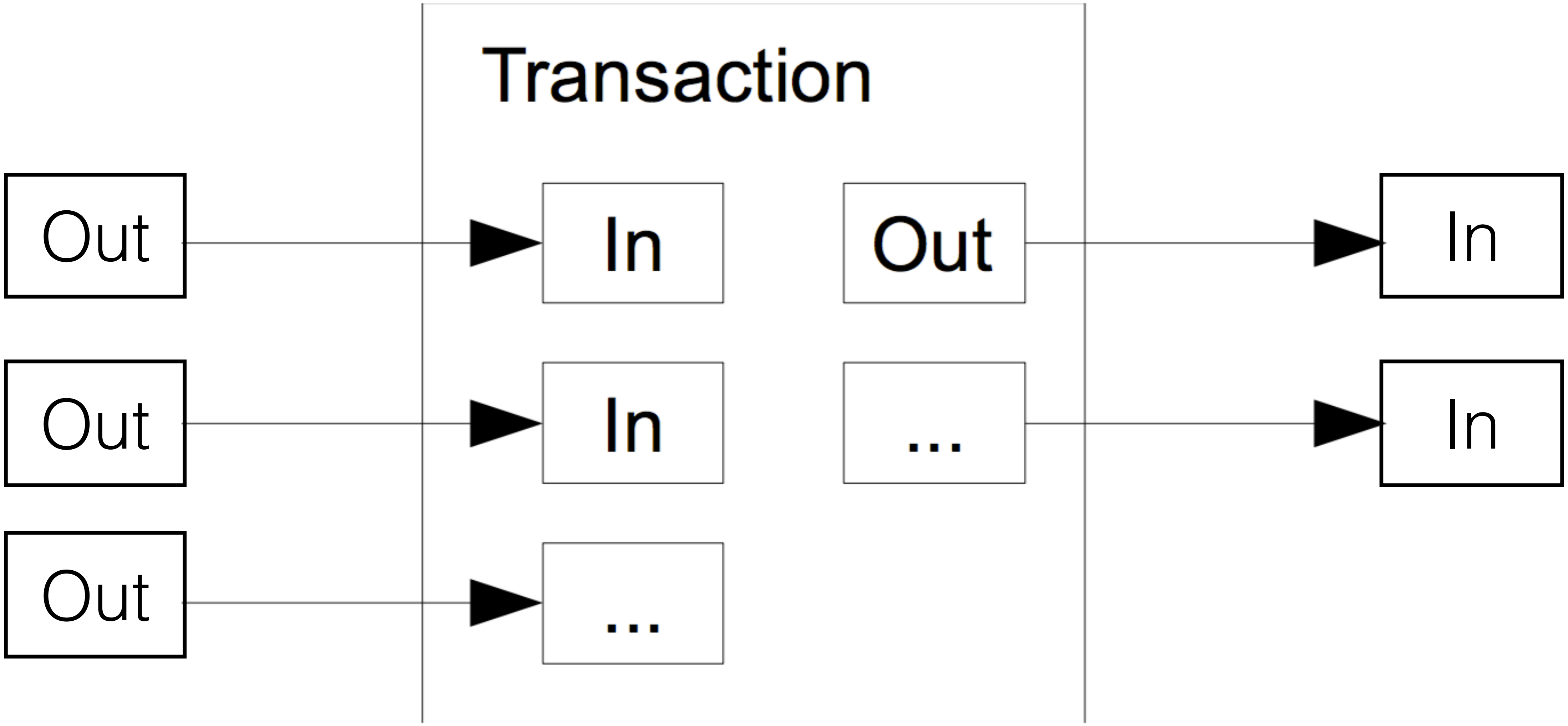
Transactions



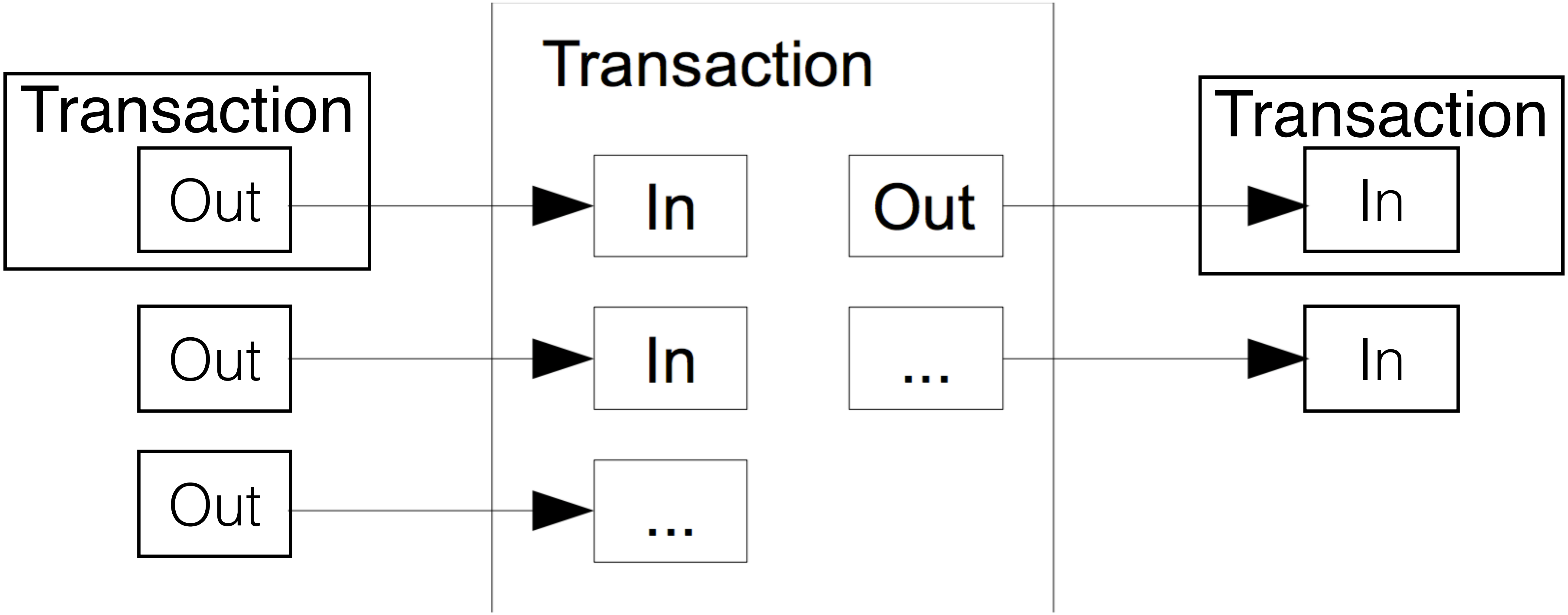
Transactions



Transactions



Transactions



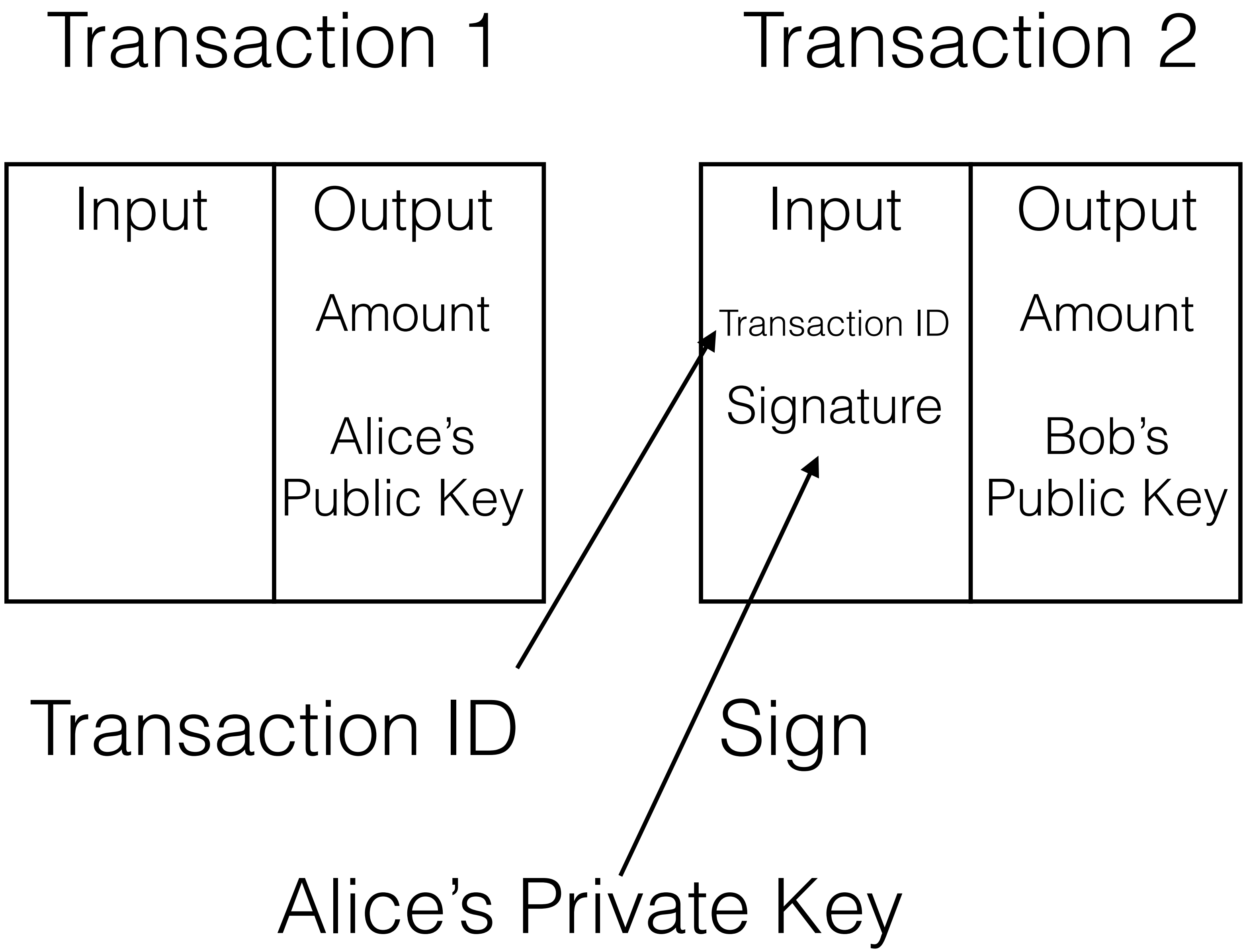
Transactions

Transaction 1

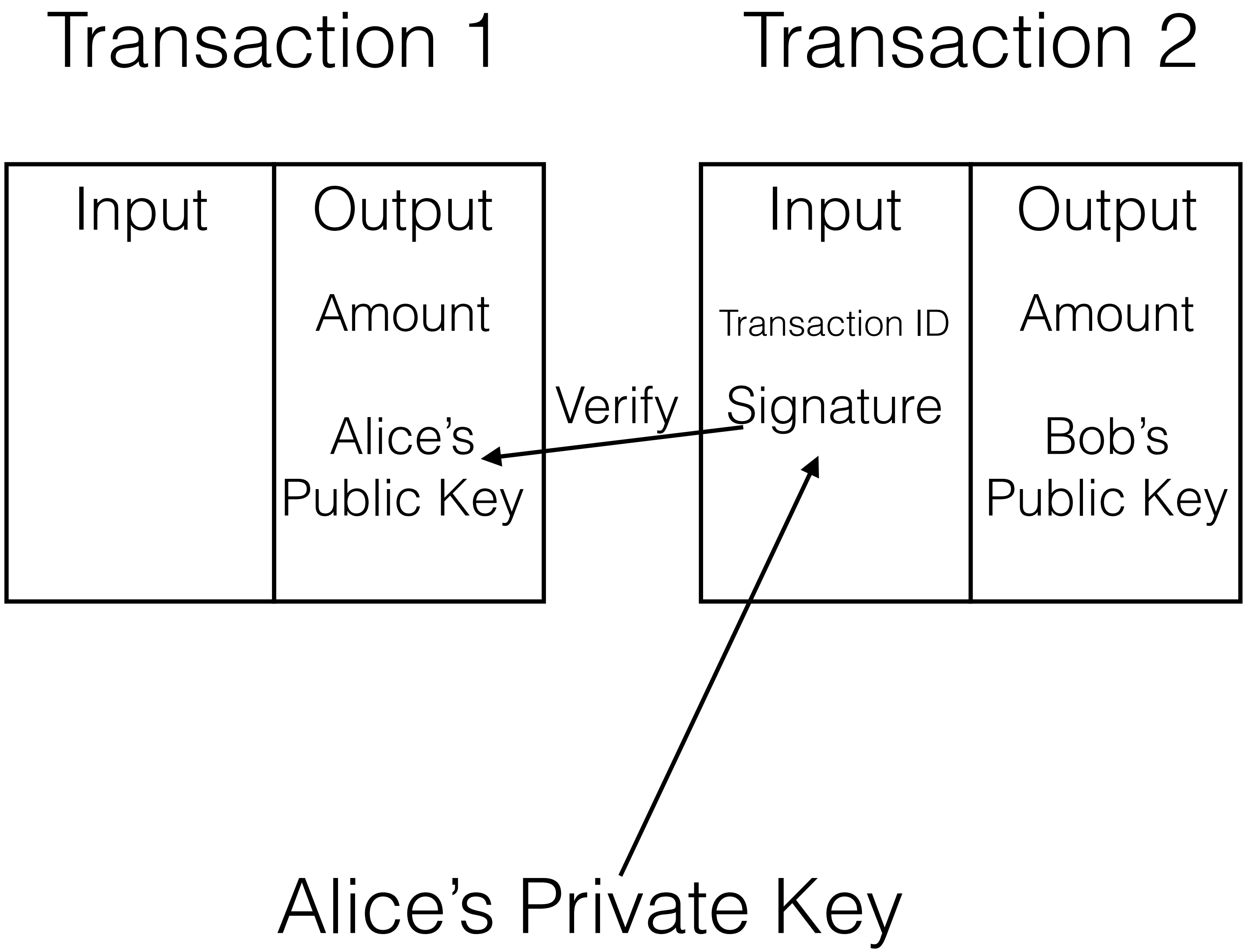
Input	Output
	Amount
	Alice’s Public Key

Transaction ID

Transactions



Transactions



Transaction 1

Transaction 2

Input

Output

Amount

Alice's Public Key

Verify

Input

Transaction ID

Signature

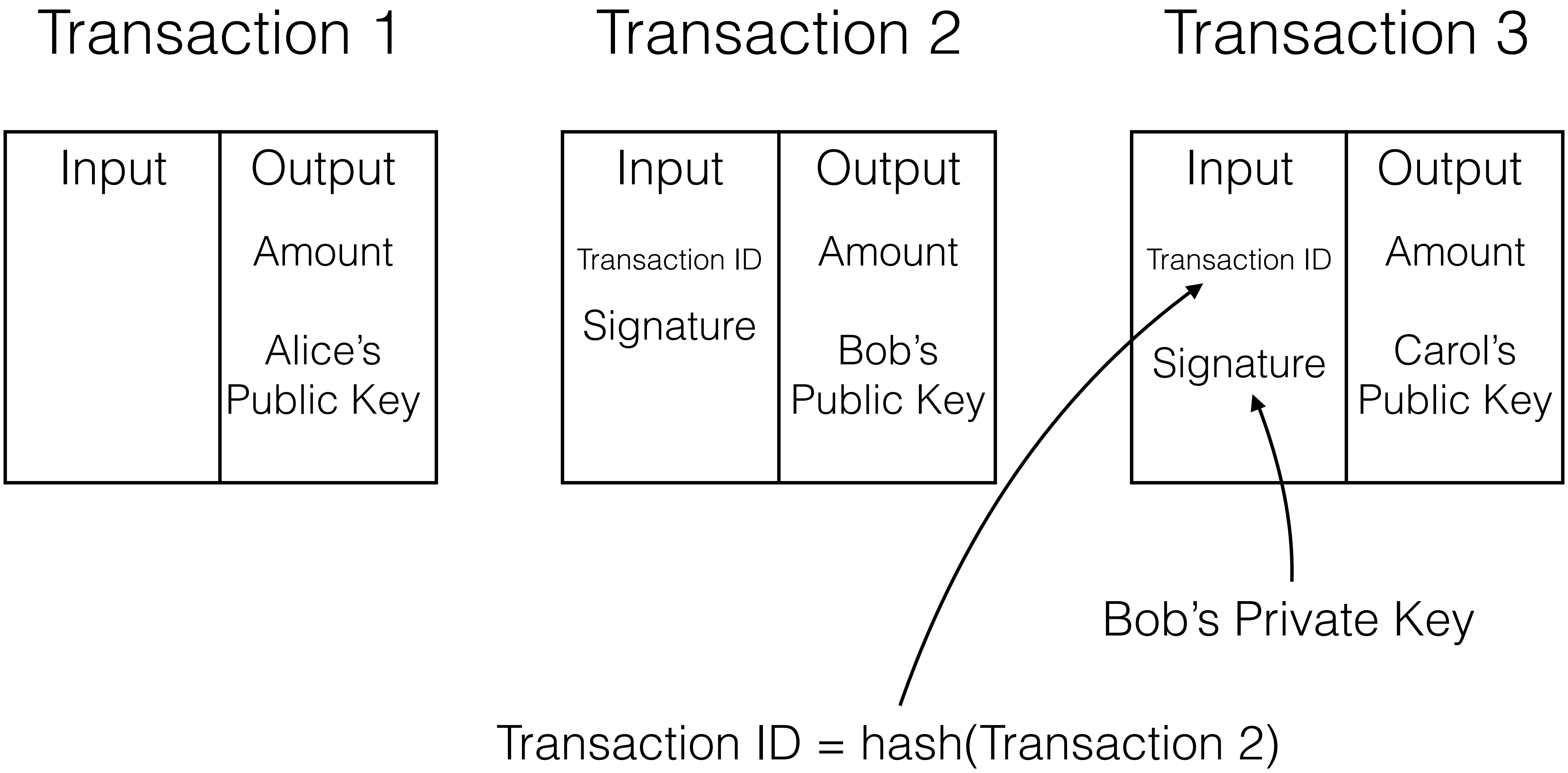
Output

Amount

Bob's Public Key

Alice's Private Key

Transactions



Transaction 1

Input

Output

Amount

Alice's Public Key

Transaction 2

Input

Transaction ID

Signature

Output

Amount

Bob's Public Key

Transaction 3

Input

Transaction ID

Signature

Output

Amount

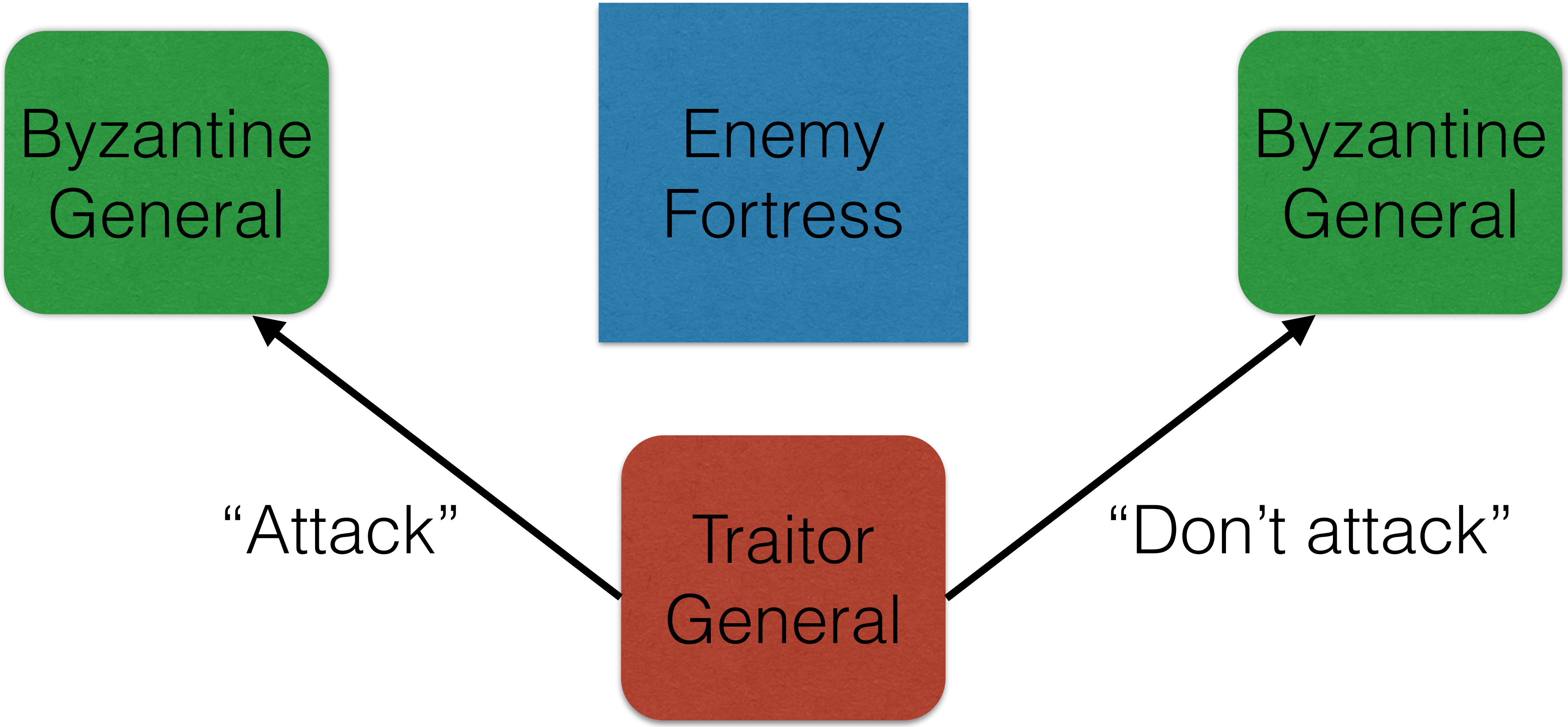
Carol's Public Key

Bob's Private Key

Transaction ID = hash(Transaction 2)

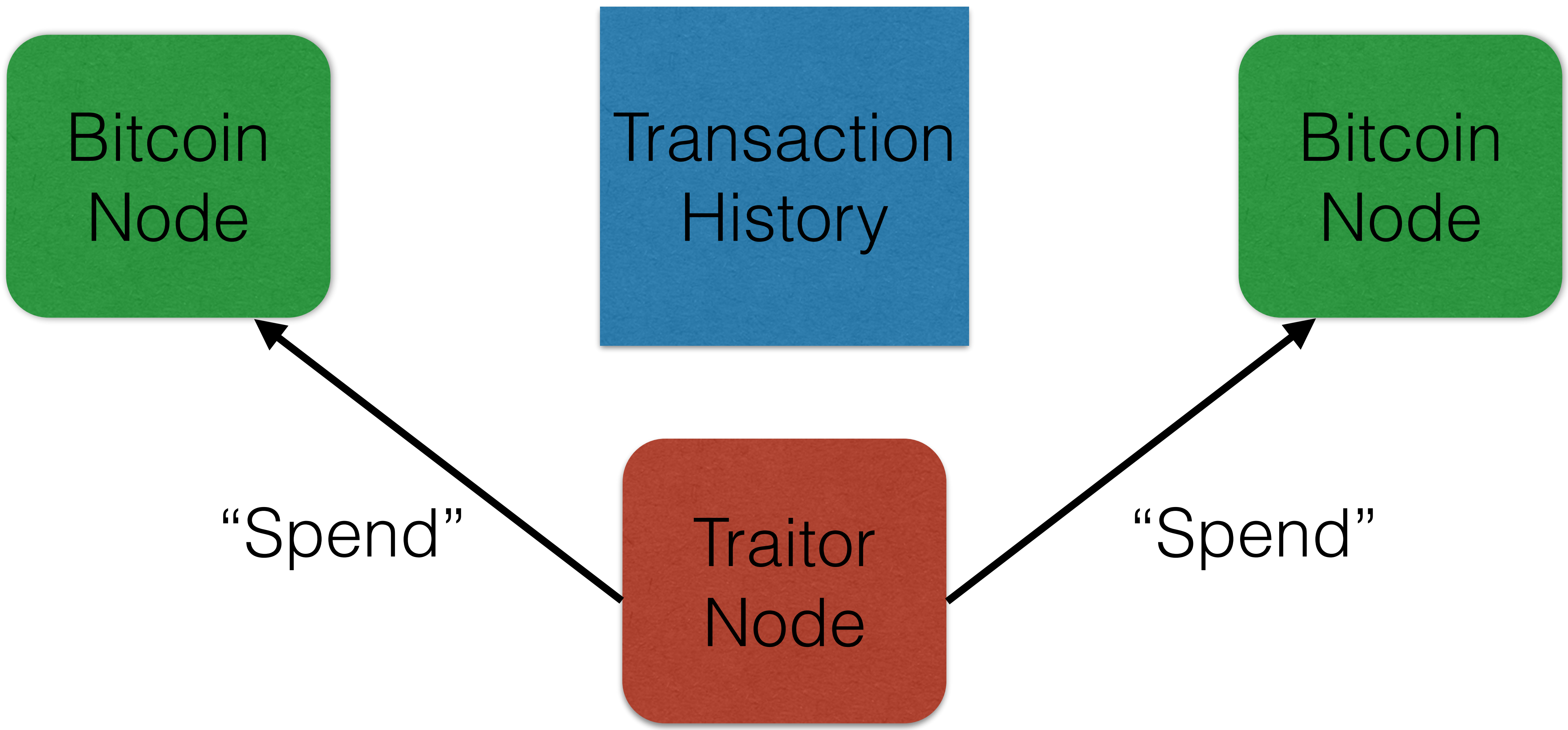
Byzantine Generals Problem

Distributed coordination problem

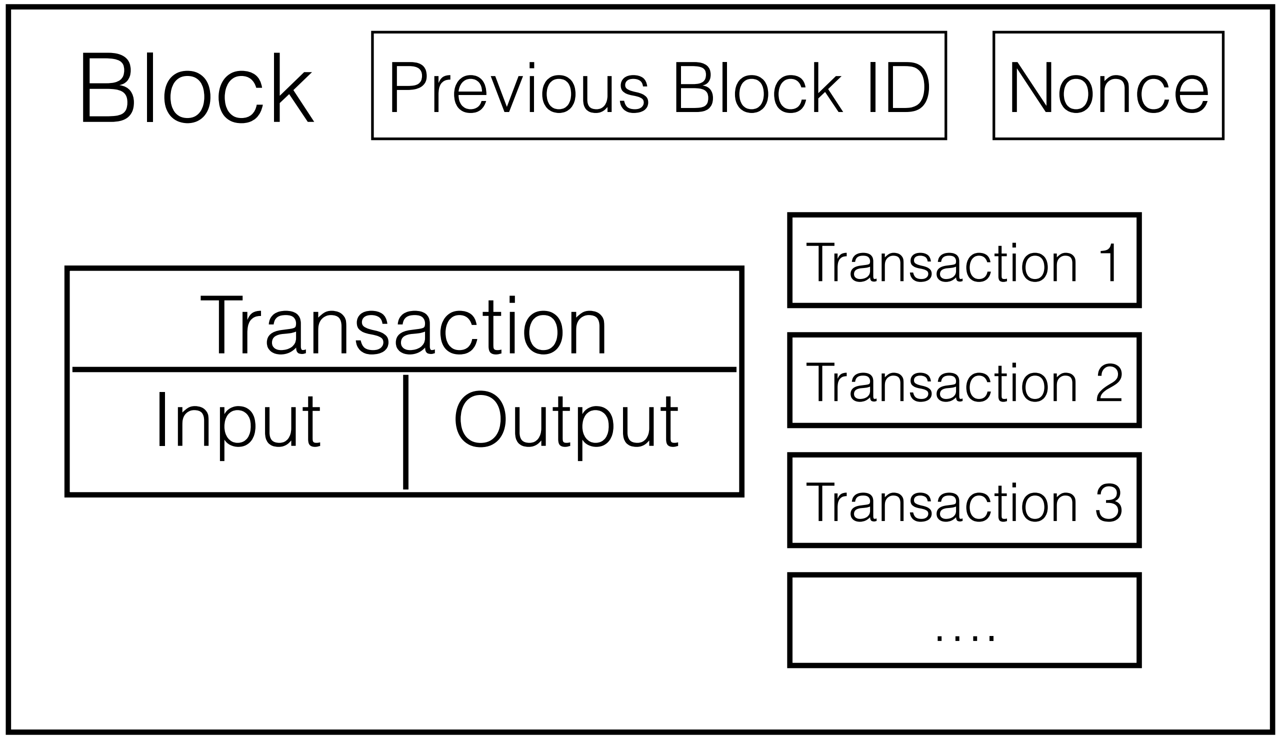


Byzantine Generals Problem

Distributed coordination problem



Blocks



Block

Previous Block ID

Nonce

Transaction

Input

Output

Transaction 1

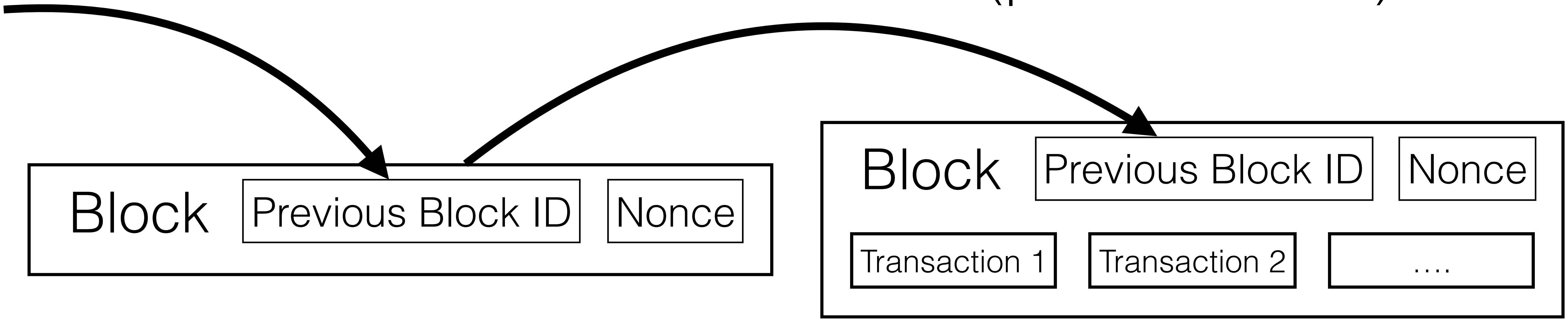
Transaction 2

Transaction 3

….

Blockchain

Previous Block ID = hash(previous block)

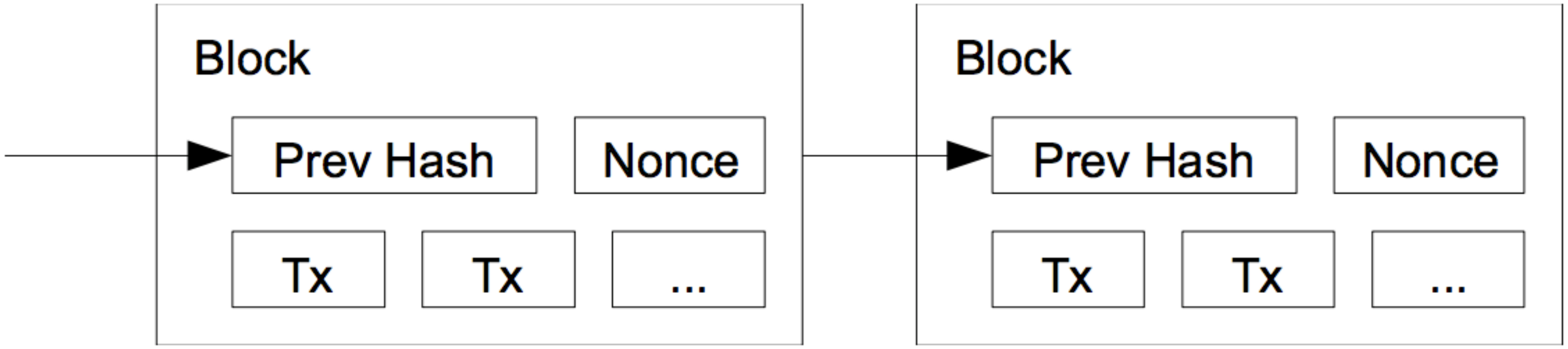


Block Previous Block ID Nonce

Block Previous Block ID Nonce

Transaction 1 Transaction 2 ….

Consensus

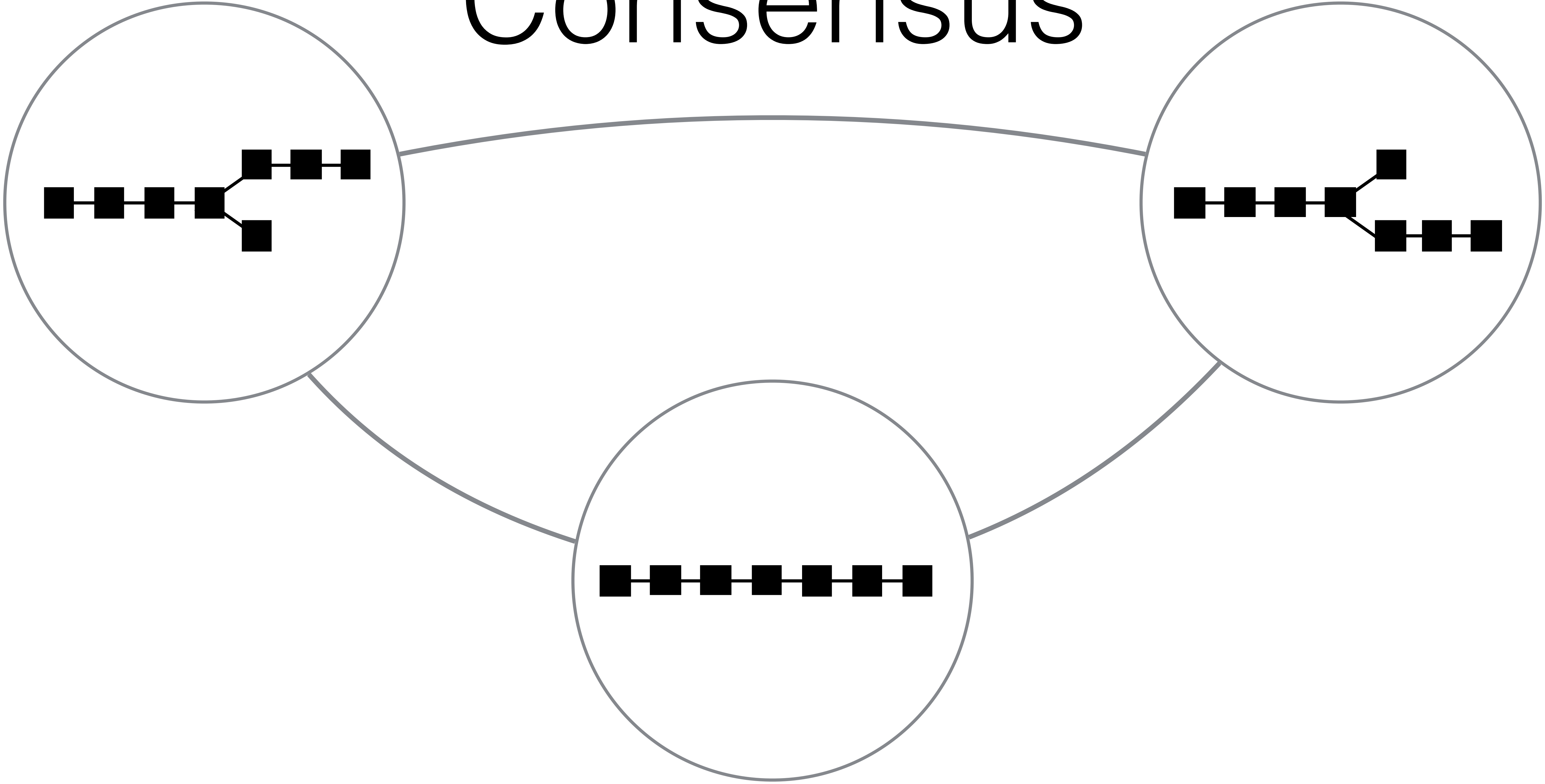


Block Hash < Target

Block Hash = hash(previous hash + nonce + transactions)

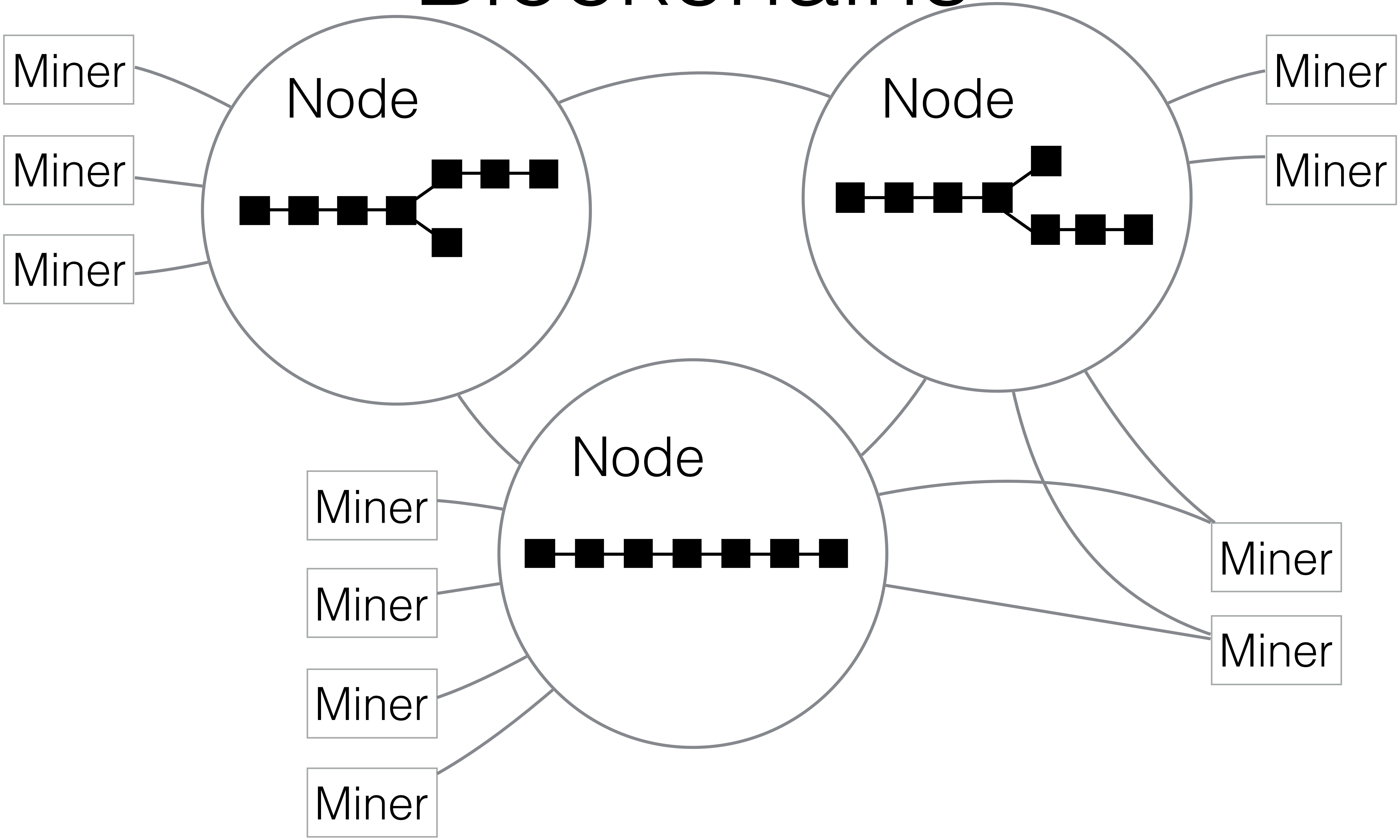
Trial and Error

Consensus

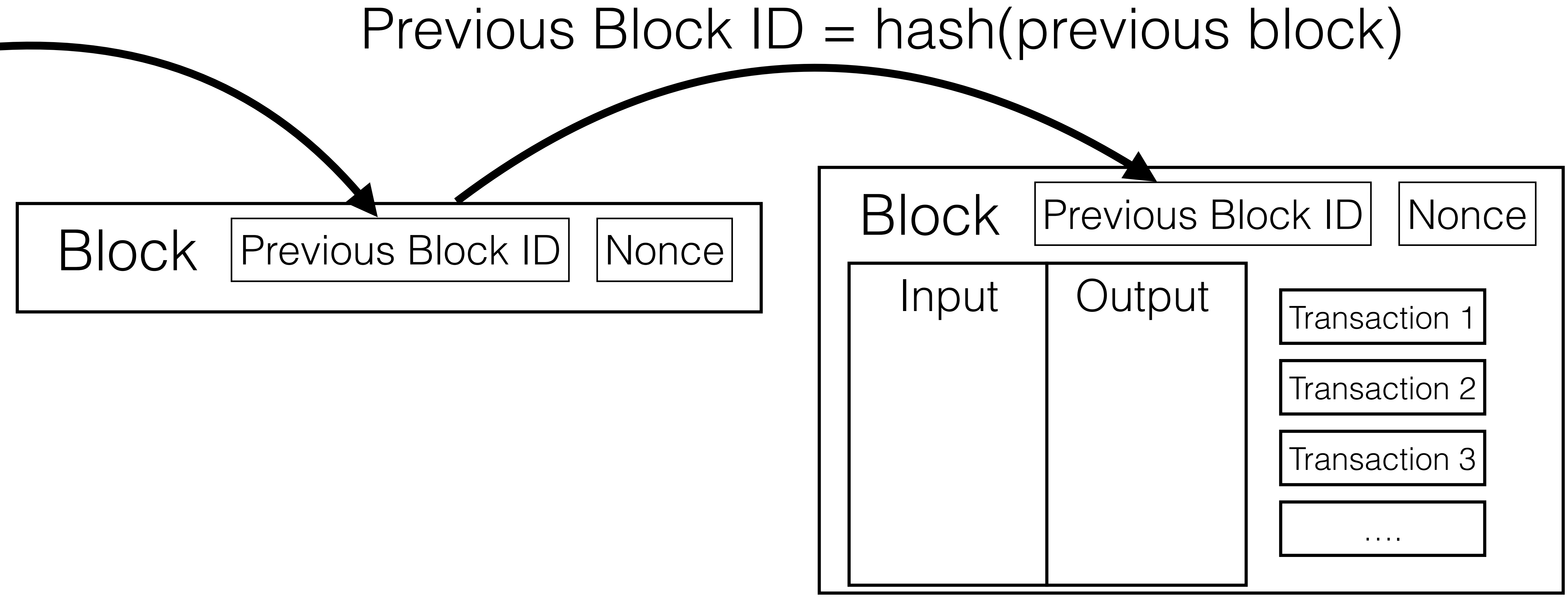


The fastest growing chain wins
Eventual consistency

Decentralized Network of Blockchains

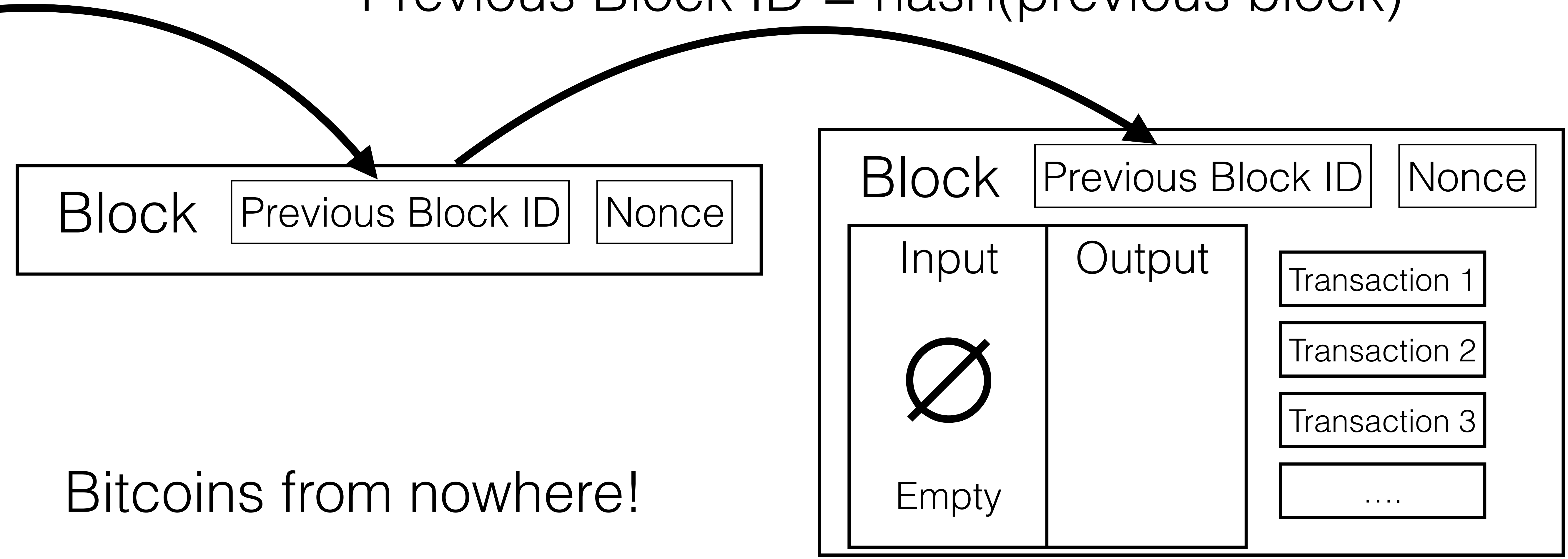


Mining Reward



Mining Reward

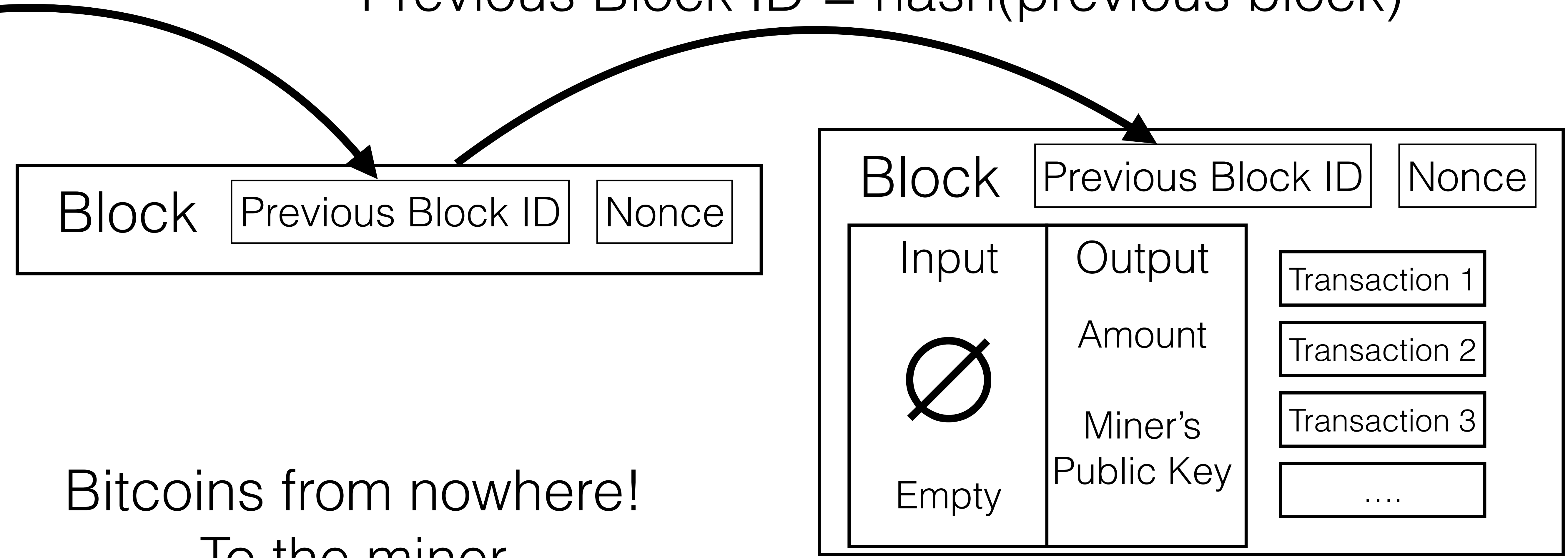
Previous Block ID = hash(previous block)



Bitcoins from nowhere!

Mining Reward

Previous Block ID = hash(previous block)



Bitcoins from nowhere!
To the miner

Bitcoin is 3 Things

1. Protocol

2. Decentralized P2P Network (of miners and nodes)

3. Unit of Value (1 Satoshi = 10^{-8} BTC)

What Do You Get?

- Global
- Trustless
- Open source
- Virtually instantaneous
- Cheap

Money

What Do You Get?

- Global
- Trustless
- Open source
- Virtually instantaneous
- Cheap

Bitcoin Script

- Programming language defining how outputs can be spent
- Multi-signature escrow
- Payment channels
- Trusts
- Two-man rule security
- Corporate approval process / Internal politics
- Title transfer
- Proof of Existence

Matthew Wraith
@wraith_m
Bitnomial

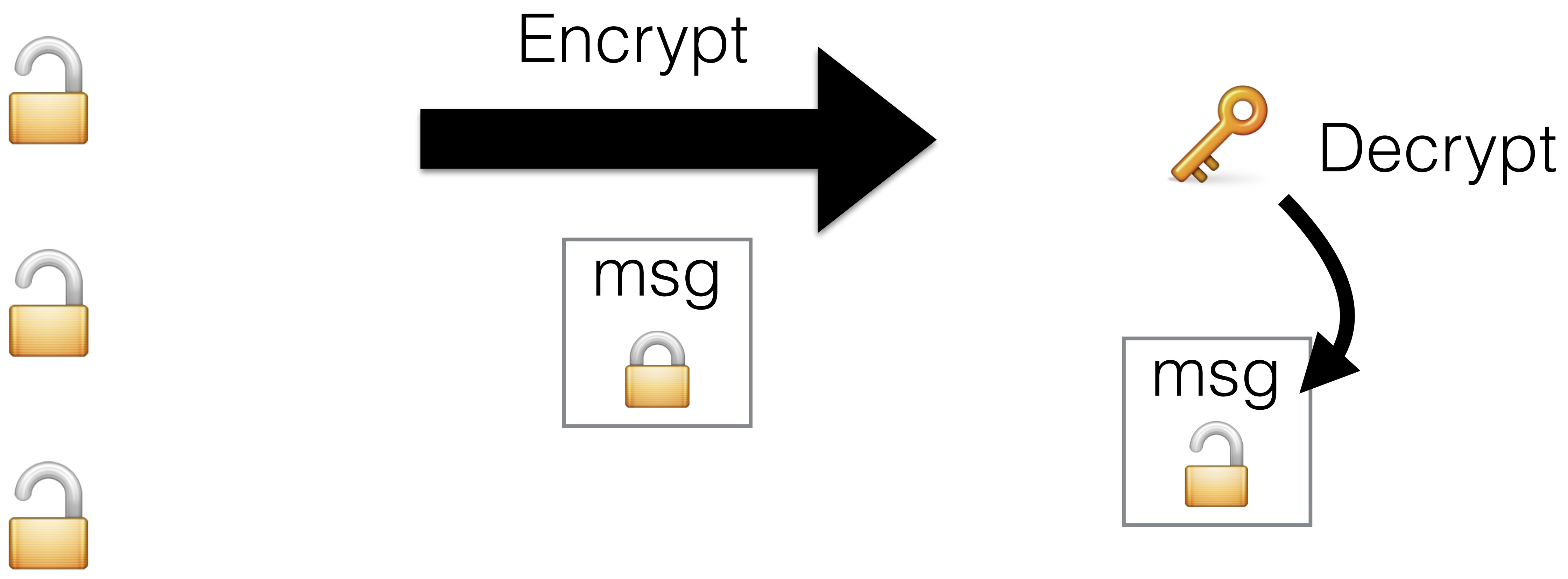
What Doesn’t Solve Byzantine Generals Problem?

- Venmo
- Credit cards

Public Key Encryption

Public Key

Private Key

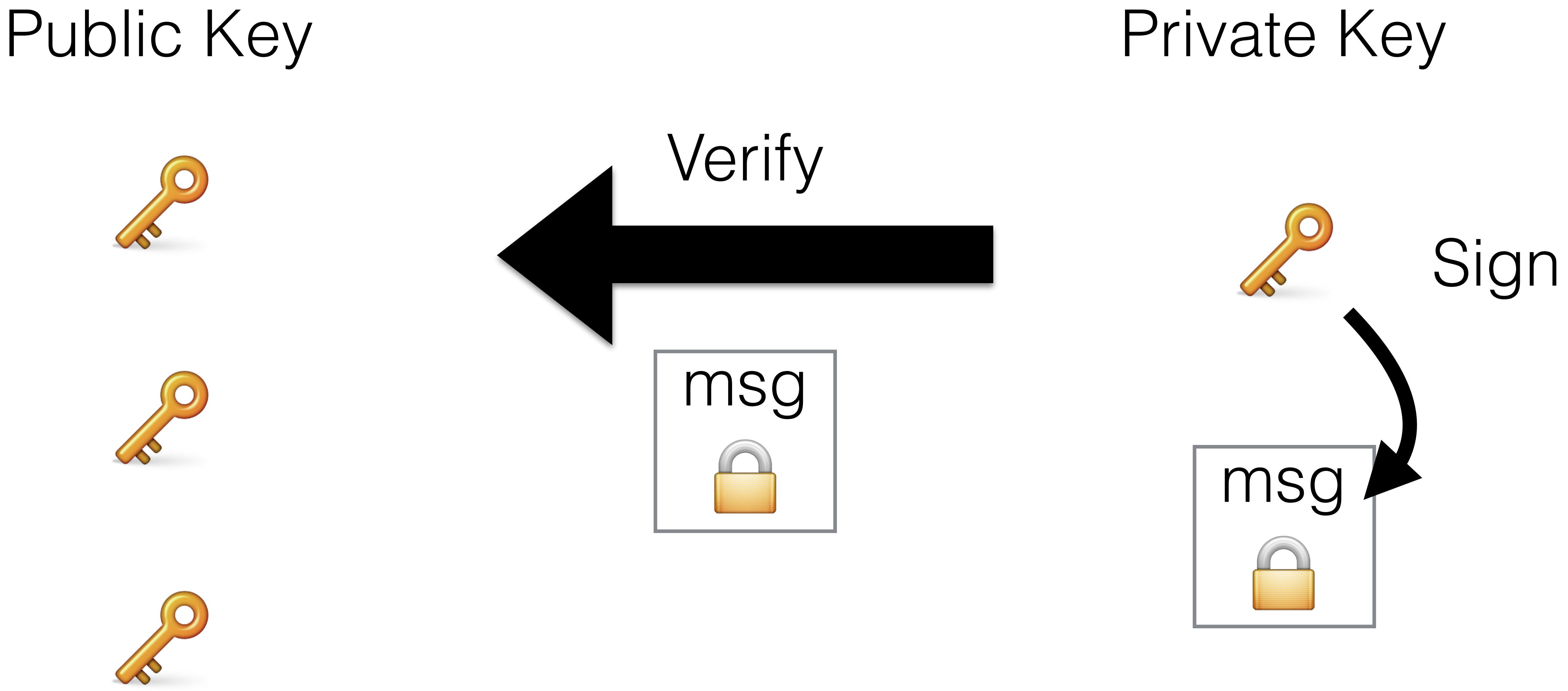


Just a number

cipherttext = E_pub(msg)
msg = D_priv(ciphertext)

Just a number

Digital Signatures



Public Key

Private Key

Verify

Sign

msg

msg

Just a number

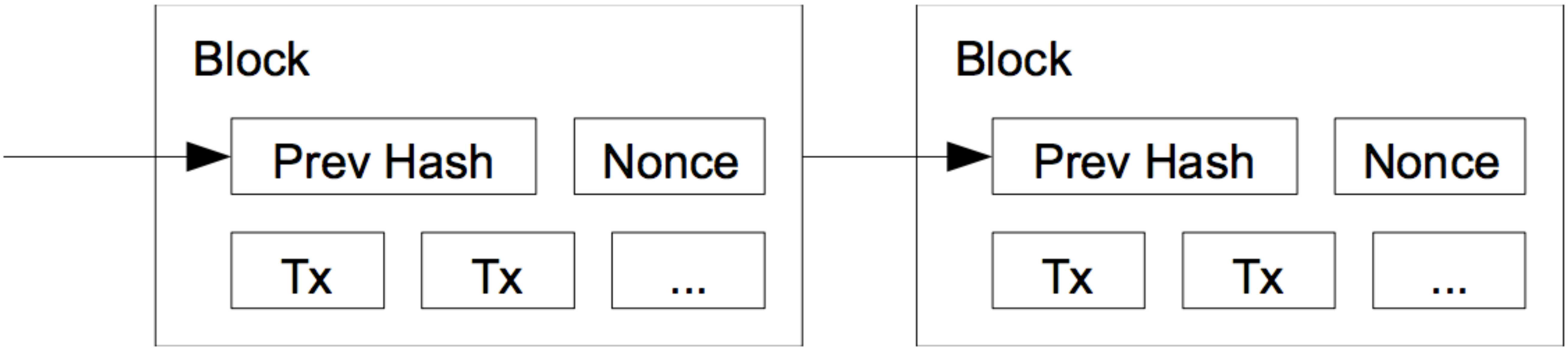
$$sig = E\_priv(msg)$$
$$msg = D\_pub(sig)$$

Just a number

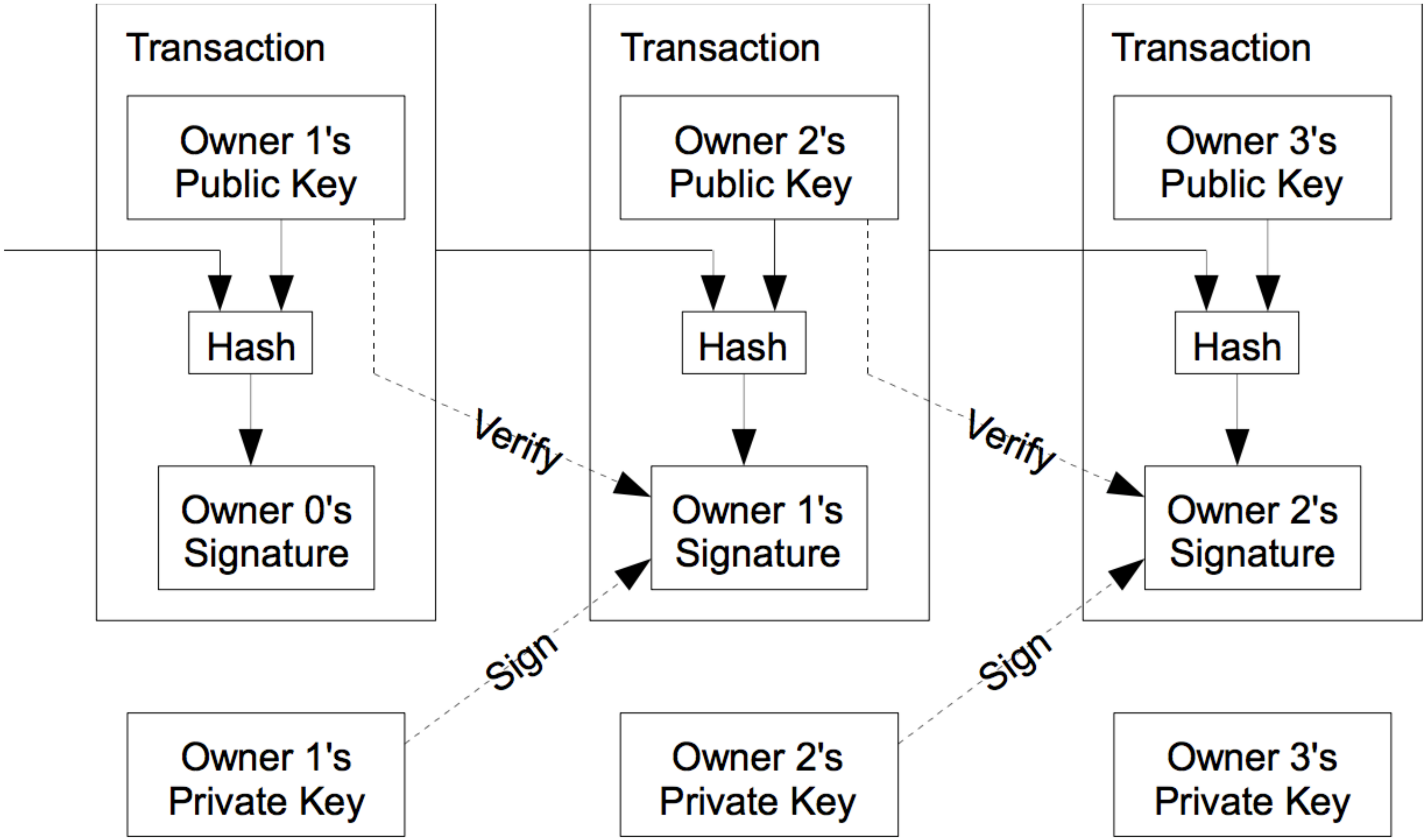
Multi-signature Script

Script = 2 pbk1 pbk2 pbk3 3 CHECKMULTISIGVERIFY

Blockchain



Transactions


Transaction
Owner 1's Public Key
Hash
Owner 0's Signature
Owner 1's Private Key
Verify
Sign
Transaction
Owner 2's Public Key
Hash
Owner 1's Signature
Owner 2's Private Key
Verify
Sign
Transaction
Owner 3's Public Key
Hash
Owner 2's Signature
Owner 3's Private Key