White Paper

”Bitcoin: A Peer-to-Peer Electronic Cash System” by Satoshi Nakamoto

Table of contents

Introduction

trusted third party based model

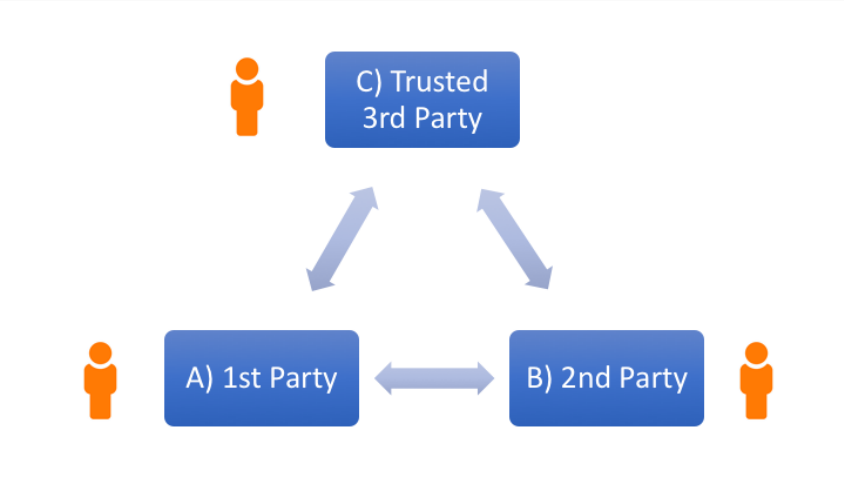

Figure 1: Trusted-third-party

- financial institutions as trusted third parties
- cost of mediation $\rightarrow$ transaction costs
- possibility of reversal $\rightarrow$ more information

peer-to-peer electronic payment system

What is needed?

- based on cryptographic proof instead of trust $\rightarrow$ transact directly with each other
- computationally impractical to reverse $\rightarrow$ protect sellers
- routine escrow mechanisms $\rightarrow$ protect buyers

Transactions

hash function

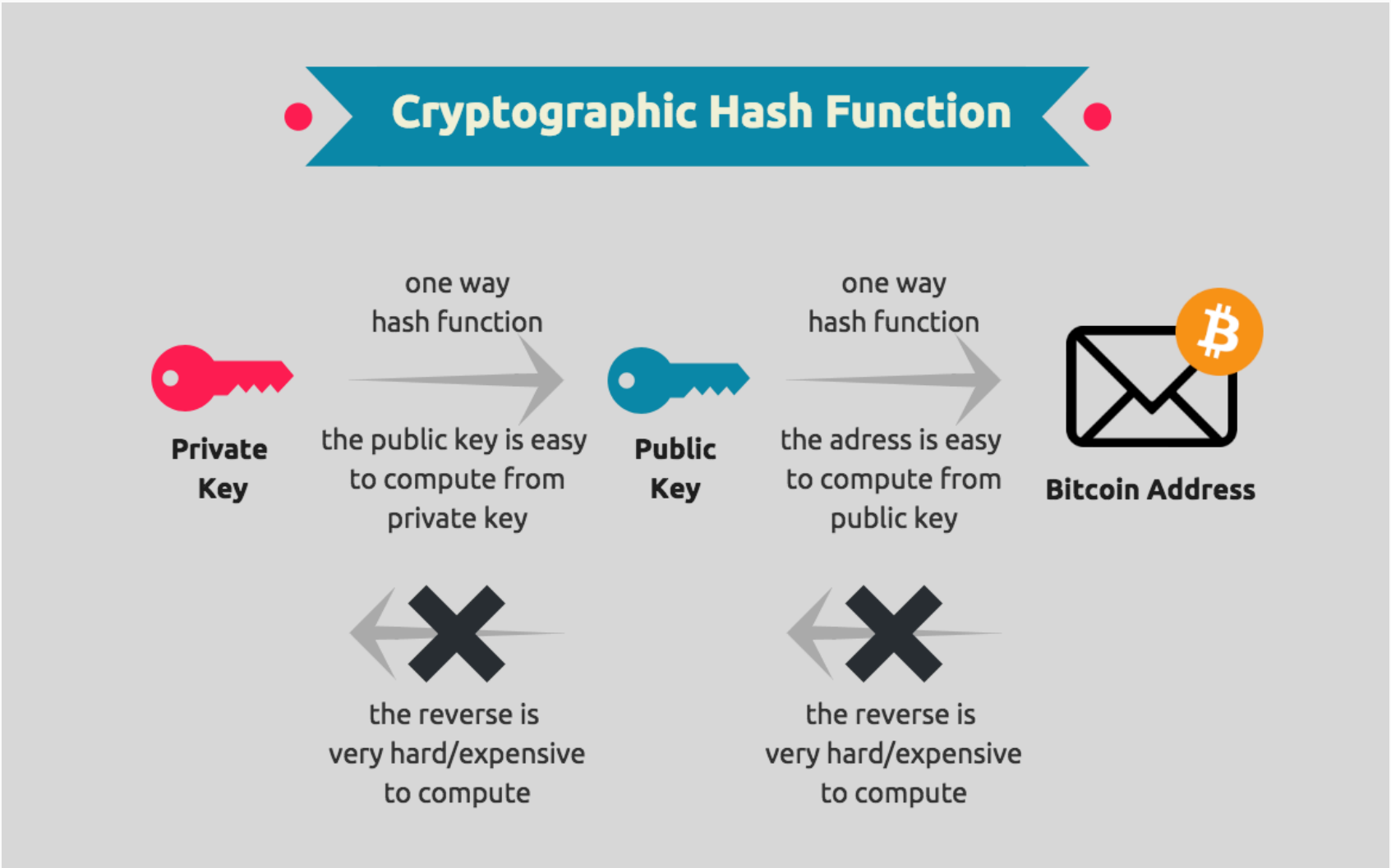

Figure 2: Hash function

digital signatures

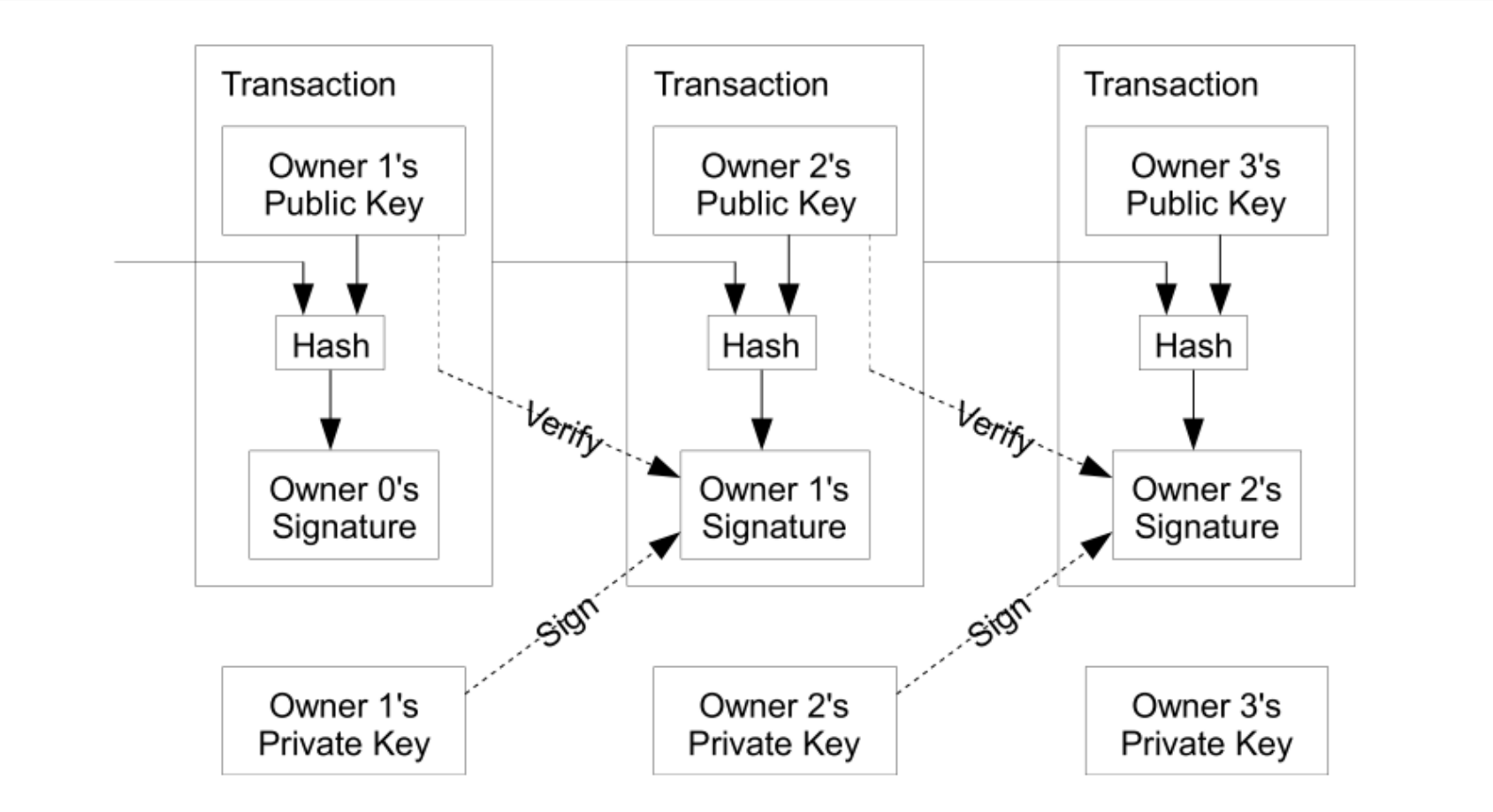

Figure 3: Transactions

verification

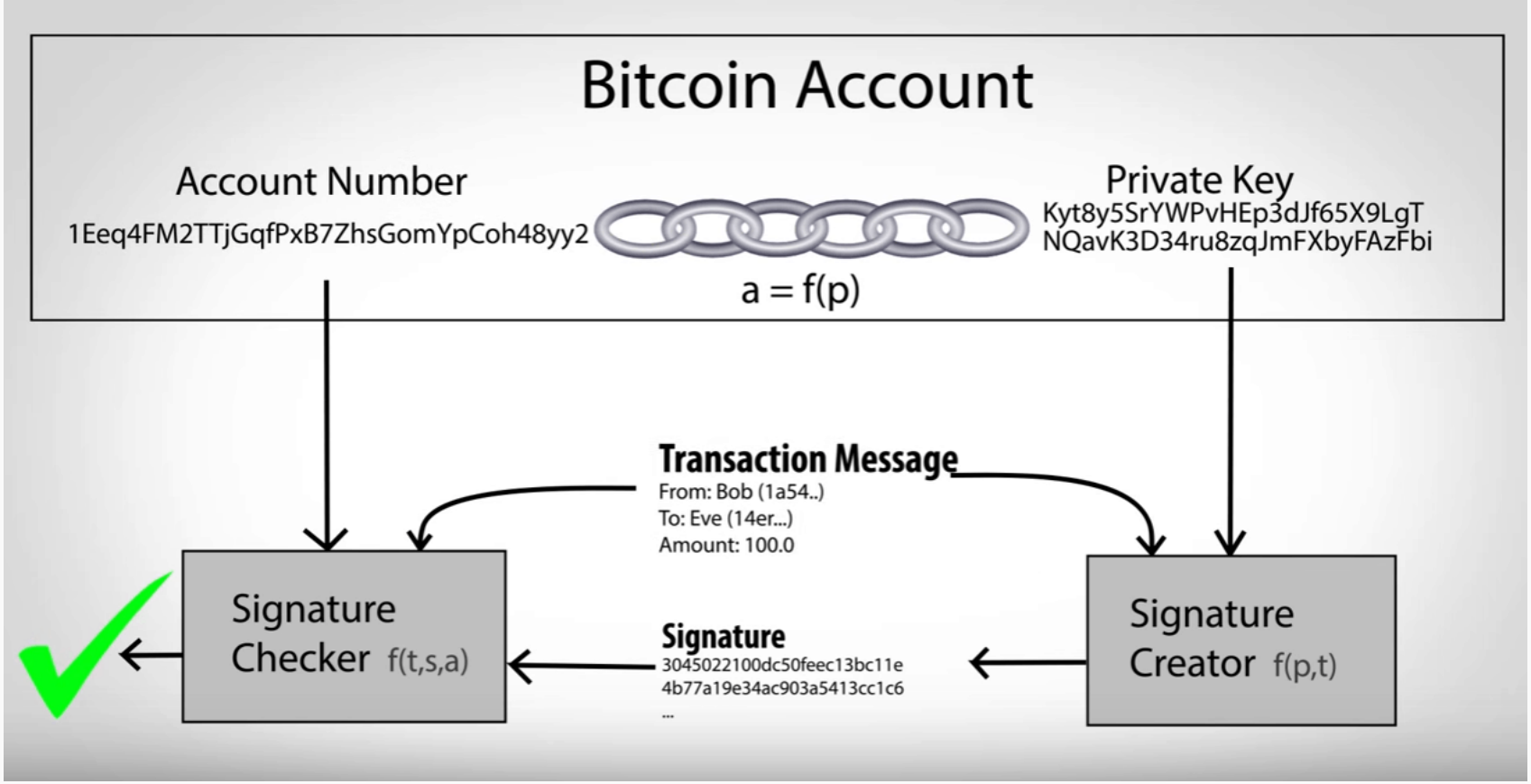

Figure 4: Transactions

double-spending

mint based model

- check every transaction
- return to the mint to issue a new coin
- depend on the mint

without a trusted party

- care about the earlist transaction
- be aware of all transactions
- publicly announced

Timestamp server

timestamp

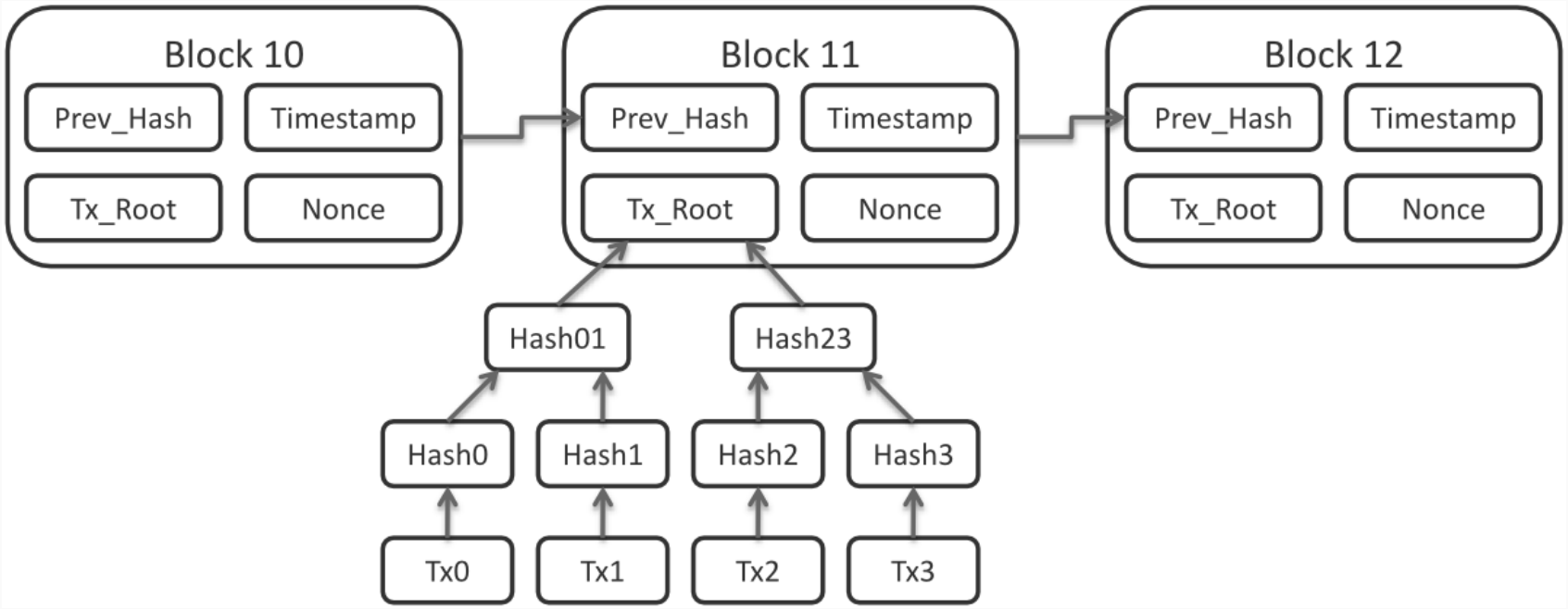

Figure 5: Timestamp

Timestamp proves that data must have existed at the time.

Proof-of-Work

proof-of-work

- a nonce (random number) in the block
- find the required number
- one-CPU-one-vote
- majority decision is represented by the longest chain

51% attack

- more than 50% of computing power
- prevent new transactions from comfirmations
- halt payments
- reverse transactions

Network

network

Distributed ledger

- New transactions are broadcast to all nodes
- Each node collects new transactions into a block.
- Each node works on finding a difficult proof-of-work for its block.
- When a node finds a proof-of-work, it broadcasts the block to all nodes.
- Nodes accept the block only if all transactions in it are valid and not already spent.
- Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

nodes

- the longest chain is considered to be the correct
- work on the first one received
- save other branch
- one branch becomes longer
- switch to the longer one

Hard folk

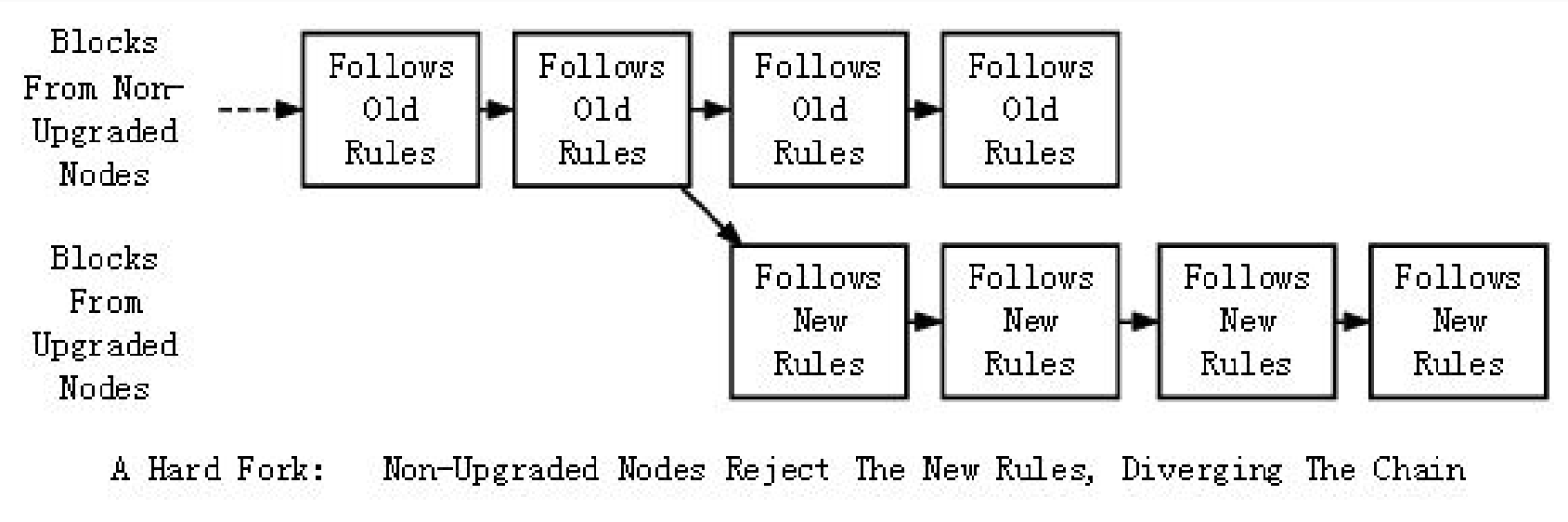

Figure 6: Hardfolk

Soft folk

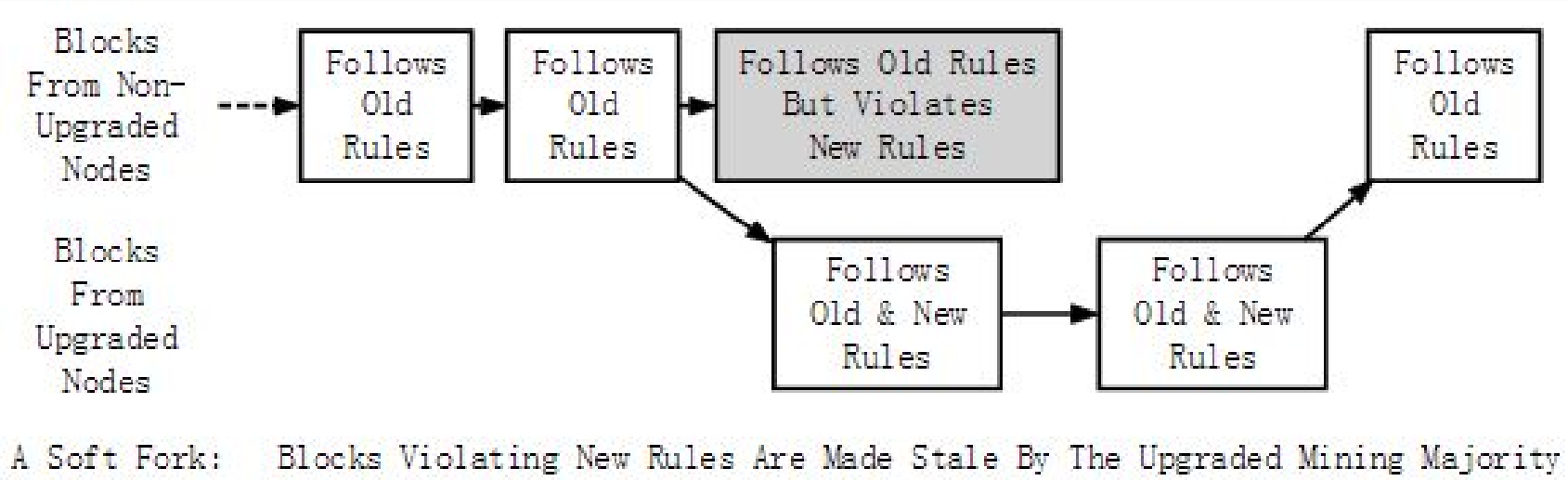

Figure 7: Softfolk

Incentive

incentive

1. a new coin (coinbase)
2. transaction fee (difference between inputs and outputs)

Extension

extensive knowledge

- total number is 21,000,000
- 1 BTC = 10,000,000 Satoshi
- mining reward halving every 4 years
- coin reward will decrease from 12.5 to 6.25 in 2020