Understanding Bitcoin

Vector Li

Learn from Peers

Building Combat Support in the Brigade Engineer Battalion:

...ting the Capabilities of ...gence and Signal Companies

...aptain Alan Adame

...BCT), 82d Airborne ...n Brigade Engineer ...loyment of multiple ...port brigade priori- ...tegration methods ...sion drives organic ...ance unique capa- ... initiatives are the ... the military intel- ...merged during the ...quipment fieldings

Colocating Command Posts

During joint forcible-entry operations, the MI and signal paratroopers deploy in small elements to embed with maneuver units or with the BCT headquarters to support multiple warfighting functions. Previously, the companies ran separate command posts (CPs). During the 1 BCT field training exercise in July 2015, the MI and signal companies merged CPs, resulting in several positive outcomes. The combined CP eased the constraint of the limited number of personnel available to execute battle-tracking operations. Also, colocating similar communication capabilities (joint capabilities release and frequency modulation

Learn from Peers Presents

Pretty Fly for a Brown Guy

Arjun's Plane and Simple Guide to Getting a Private Pilot's License

Bitcoin


BITCOIN·DIGITAL·DECENTRALIZED·PEER TO PEER
1 TROY OZ 999 FINE COPPER .MJB MONETARY METALS

Bitcoin


Bitcoin Price
Bitcoin.com
$18000.00
$16000.00
$14961.05
$14000.00
$12000.00
$10000.00
$8000.00
$6000.00
$4000.00
$2000.00
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
2018

Bitcoin

2008 paper

Bitcoin: A Peer-to-Peer Electronic Cash System

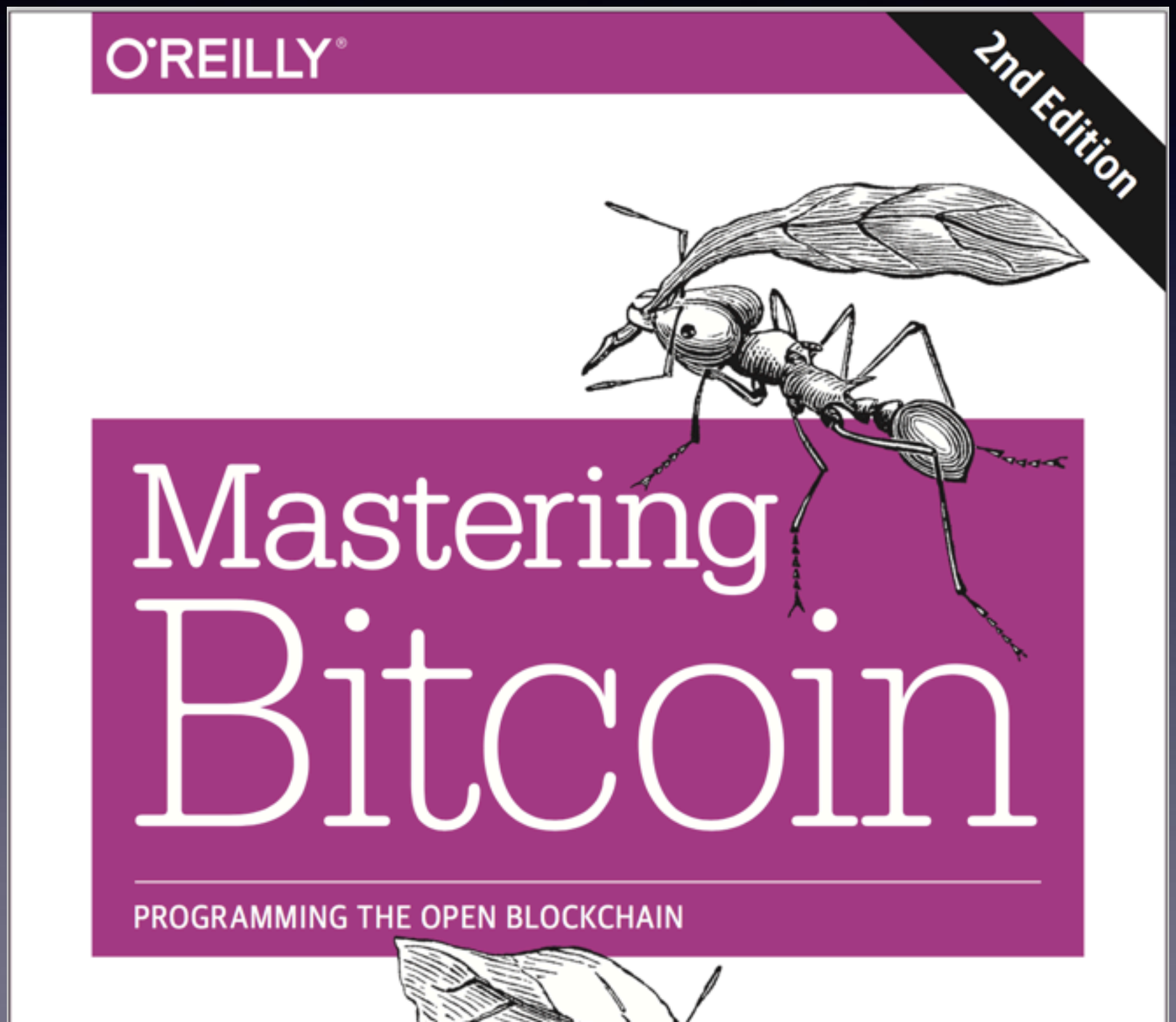
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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

Bitcoin


O'REILLY
2nd Edition
Mastering
Bitcoin
PROGRAMMING THE OPEN BLOCKCHAIN

Pre-Knowledge

- Public-Private key scheme
- Digital signature
- Hash function

Bitcoin System

Client	**Miner**
Transaction	**Blockchain**

Bitcoin Syster

Very Important:

Miner is a very miss leading term.

It is just like bank in financial world.

This is where money is stored, this is where transaction is recorded.

Keep that in mind, this is the first take away.

User	**Bank**
Transaction	**Ledger**

In This Talk

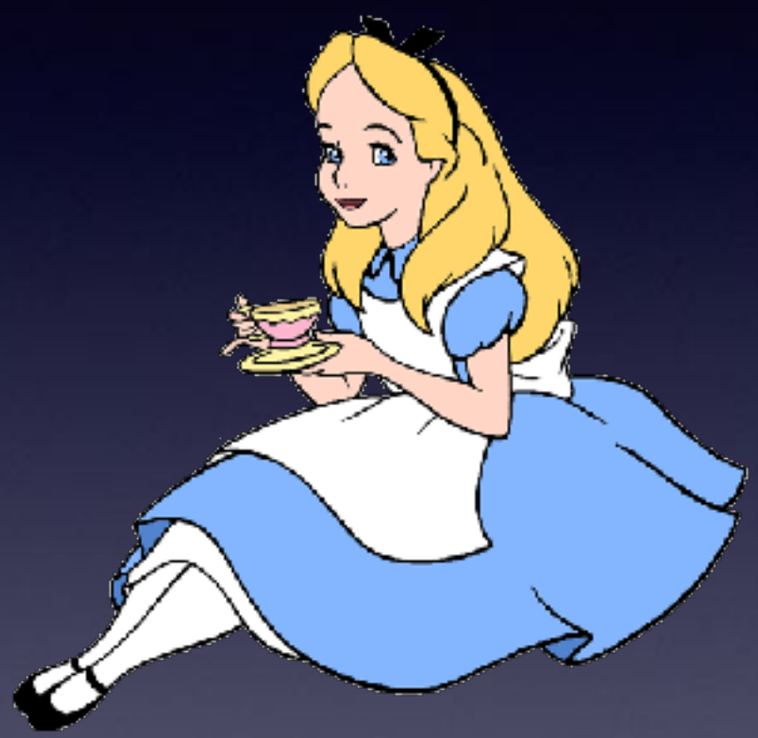
- Transaction

  How money is transferred

- Blockchain

  How transaction is recorded and how money is generated

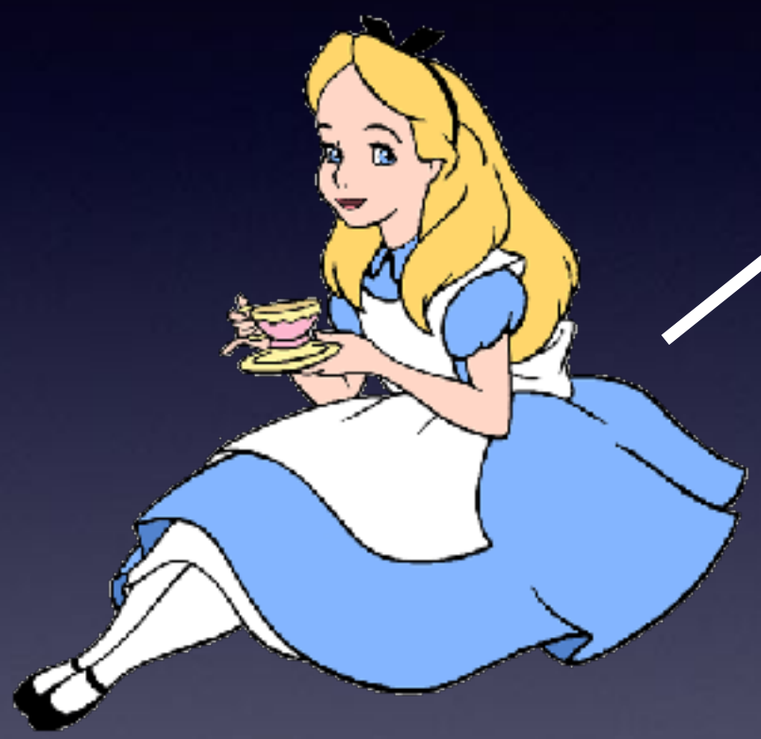
Transaction



5 BTC

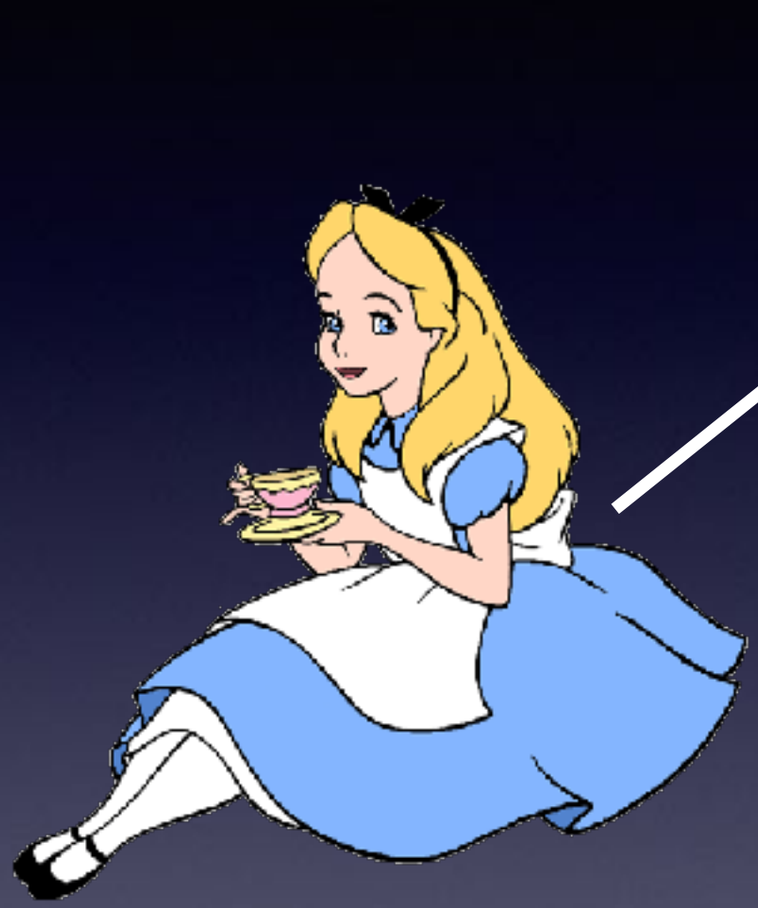
What if Alice doesn’t have 5 BTC ?
What if Alice cheats ?
What if Bob cheats ?

Transaction



Trusted Authority

Transaction

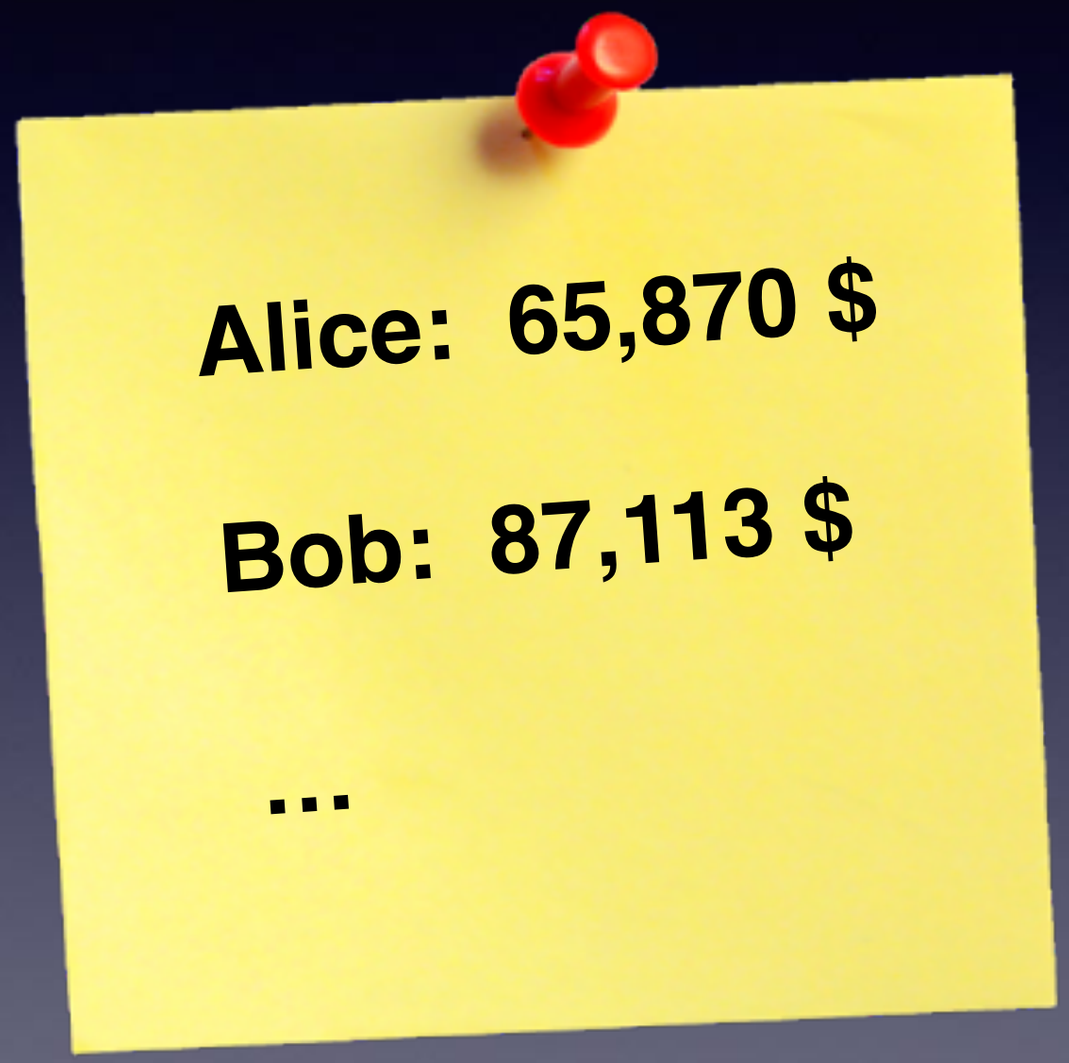


As long as majority of them are good nodes

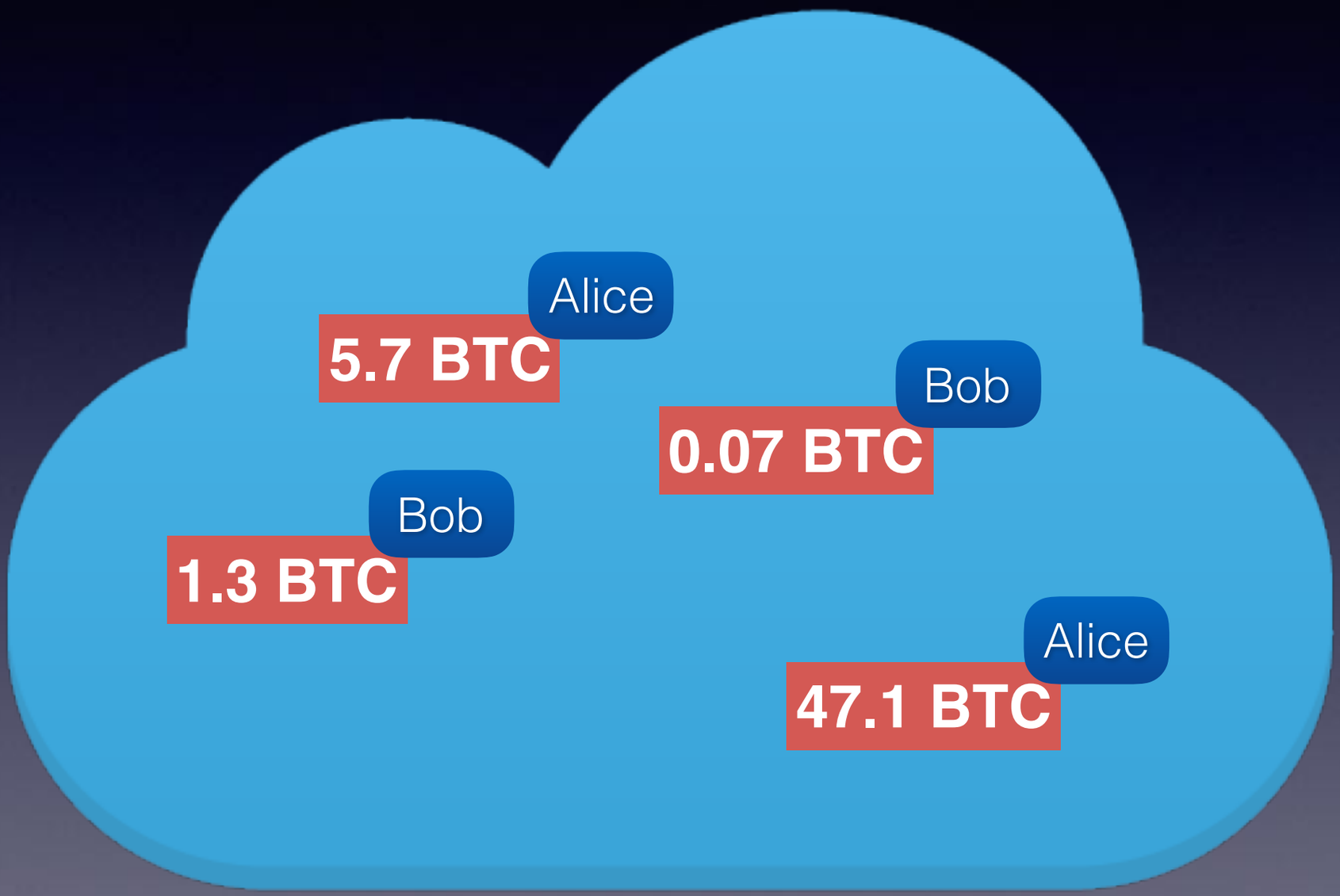
Transaction

- How a person’s balance is recorded.
- How a transaction is conducted.

How Banks Record Balance



How Bitcoin Records Balance



How Bitcoin Records Balance

- Unspent Transaction Output

UTXO

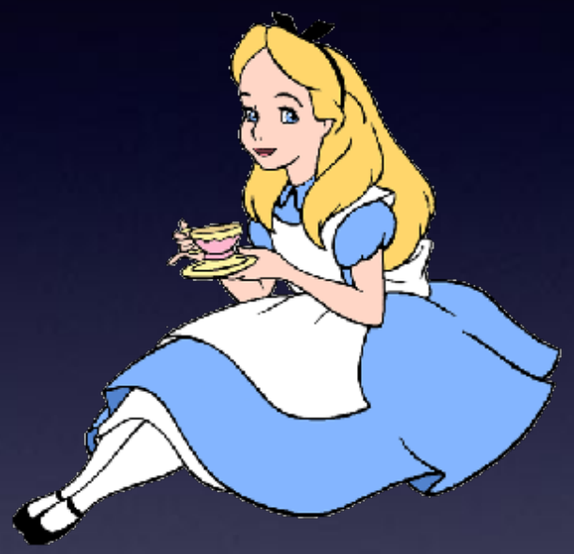
Just like a 5 dollar cash

- **discrete** and **indivisible**

Transaction Input will then disappear.

Since it has been consumed.

Transaction



5 BTC

Transaction Input

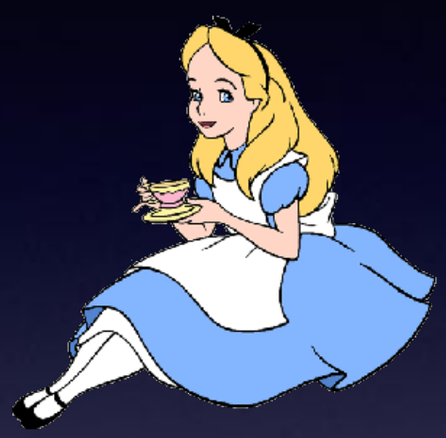
Transaction Output

Transaction

- How to make sure Alice indeed authorized this transaction.

- **Integrity** and **Authenticity**

Transaction



```
public key:   0x4587930FB…
private key: 0x17FA9C0F0…
```

Bitcoin Address is the hash of the public key

Alice will use her private key to sign this transaction

Bank(miner) will verify the signature and grant the transaction

UTXO

How do we indicate this 5.7 BTC belongs to Alice

A simple script program that
takes input and return true or false

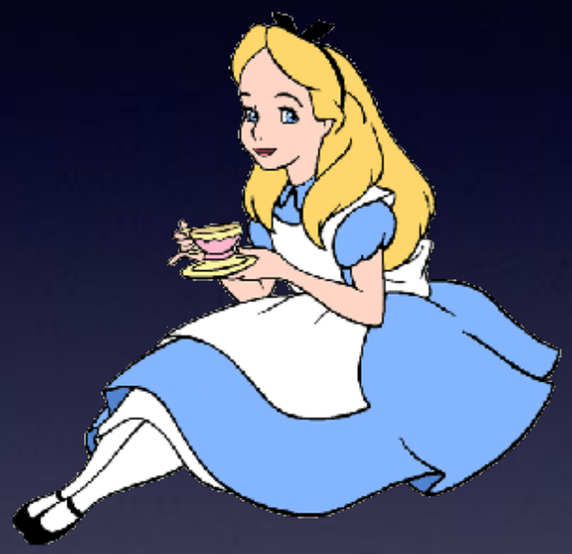
You can spend this money only if you provide inputs
that make the program return true

UTXO

- An example of locking script (high level):

```
fun verify(pubKey, Sig) {
   condition1 =  (Hash(pubKey) == ADDRESS)
   condition2 =  CheckSig(pubKey, Sig, MESSAGE)
   return condition1 && condition2
}
```

Transaction



5 BTC

5.7 BTC

Locking Script 1

Inputs

Transaction Input

5.0 BTC

Locking Script 2

0.7 BTC

Locking Script 3

Transaction Output

You can use any protocol you want, doesn't have to be the one we mentioned.

This is one is the most common one.

The bank don't know the money belong to who.

UTXO

- Bitcoin system is protocol independent.

  We can design our own protocol

- Banks(Miner) only record all the transactions

  Don't need to manage identities

Bitcoin System

Client	**Miner**
Transaction	**Blockchain**

Bitcoin System

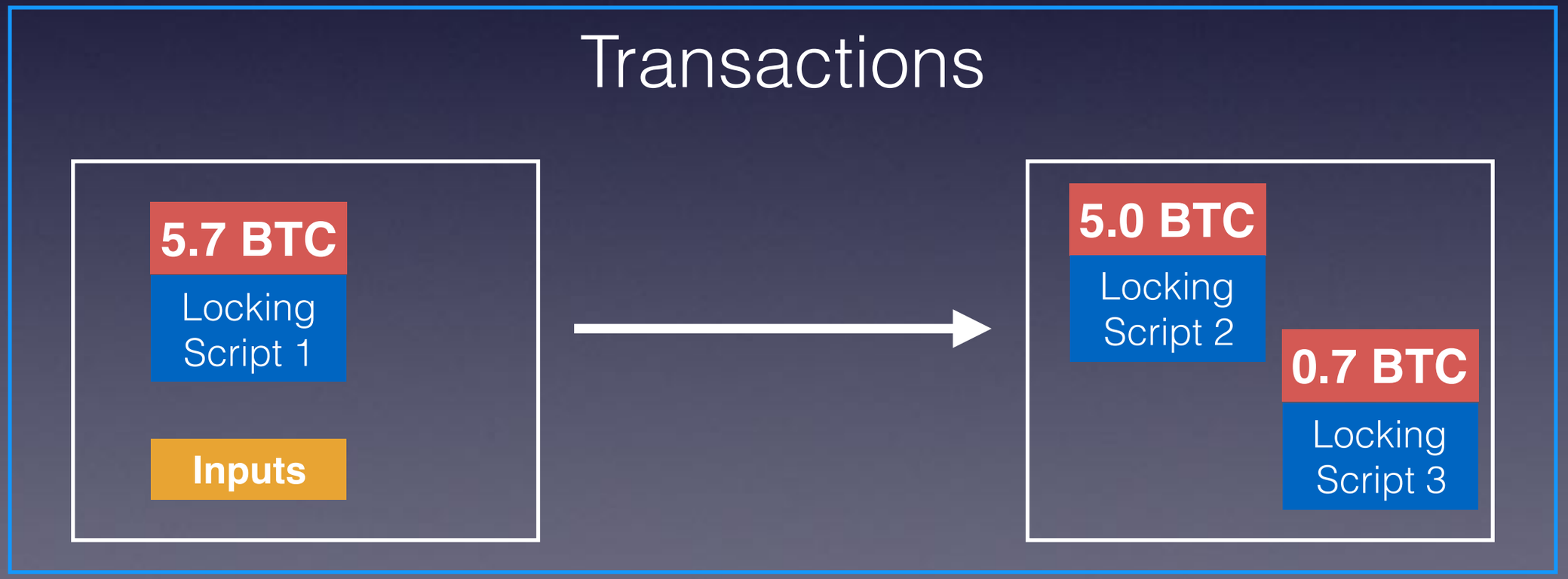
- Miners are servers.
  - Users are *clients* who use the system
  - Miners are *servers* who support the system

- Miners are interconnected and form a P2P network.

- Each Miner has a copy of a complete **blockchain**.
  - Bitcoin system guarantees all the miners achieve a global consensus.

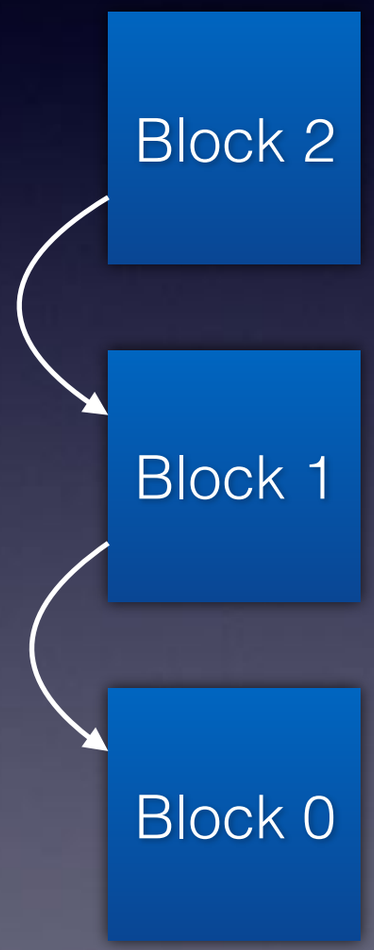
Blockchain

- Blockchain is where we record all the transactions.



Blockchain

- It is a chain of blocks
- It links backwards
- Each block records some amount of transactions



Blockchain

- Different transactions can have different sizes.

- Blockchain enforces the maximum size of one block: **1 MB**

  Different blocks can have different number of transactions

Structure of a Block

Size	Field	Description
4 bytes	Block Size	The size of the block, in bytes, following this field
80 bytes	Block Header	Several fields form the block header
1–9 bytes (VarInt)	Transaction Counter	How many transactions follow
Variable	Transactions	The transactions recorded in this block

Block Header

Size	Field	Description
4 bytes	Version	A version number to track software/protocol upgrades
32 bytes	Previous Block Hash	A reference to the hash of the previous (parent) block in the chain
32 bytes	Merkle Root	A hash of the root of the merkle tree of this block's transactions
4 bytes	Timestamp	The approximate creation time of this block (seconds from Unix Epoch)
4 bytes	Difficulty Target	The Proof-of-Work algorithm difficulty target for this block
4 bytes	Nonce	A counter used for the Proof-of-Work algorithm

Block Header

- Previous Block Hash

Size	Field
4 bytes	Version
32 bytes	Previous Block Hash
32 bytes	Merkle Root
4 bytes	Timestamp
4 bytes	Difficulty Target
4 bytes	Nonce

- The hash of the previous **block header**

- This is the “pointer” to the previous block.

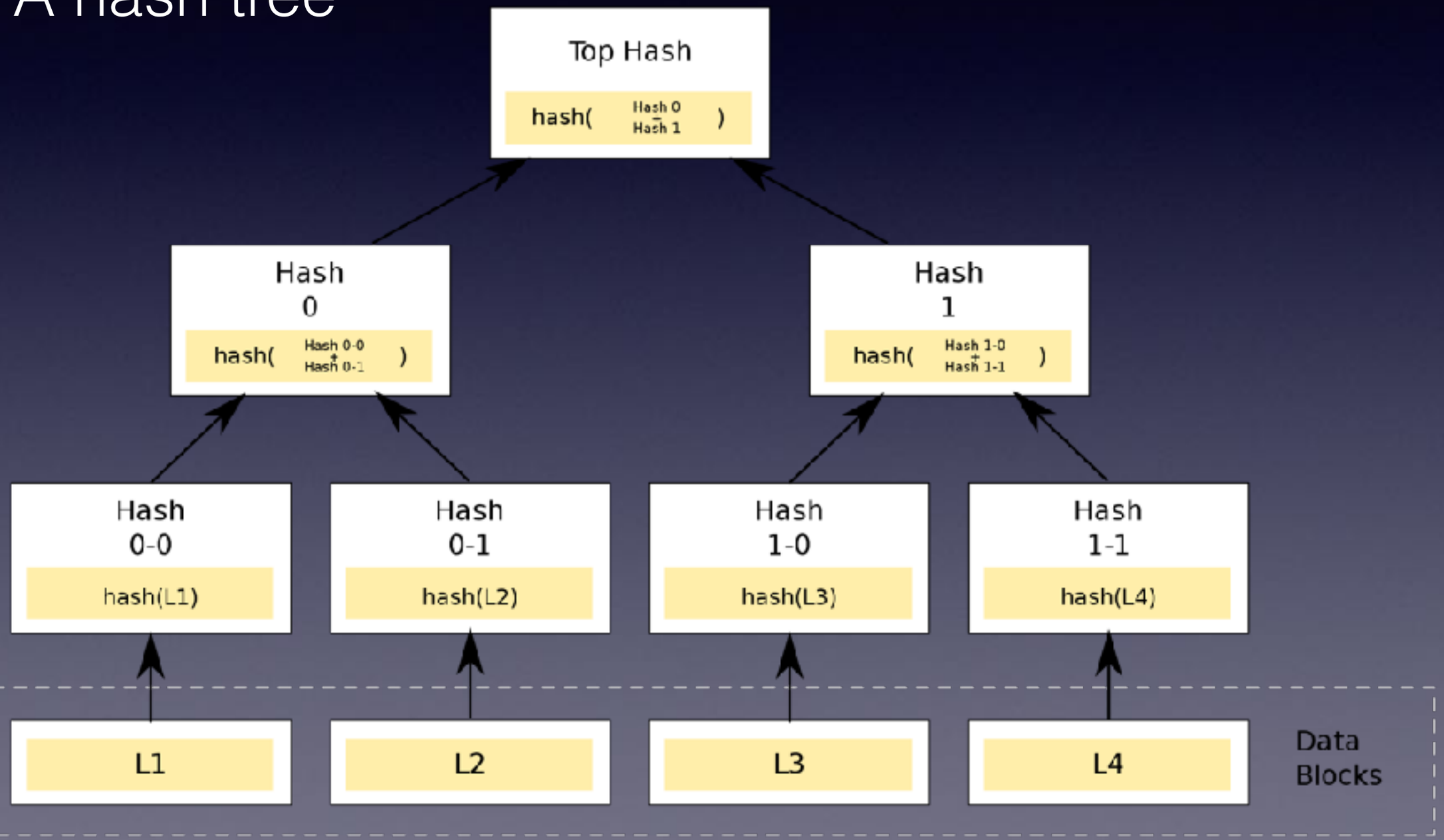
Block Header

Size	Field
4 bytes	Version
32 bytes	Previous Block Hash
32 bytes	Merkle Root
4 bytes	Timestamp
4 bytes	Difficulty Target
4 bytes	Nonce

- Merkle Root
- The hash of all the transactions in this block.

Merkle Tree

- A hash tree



Block Header

- Each block record some transactions and build a merkle tree for them.

- To verify that a transaction exists in one block, we only need to check the hashes on **one path**.

Target = coefficient*2^(8*(exponent–3))

Block Header

Size	Field
4 bytes	Version
32 bytes	Previous Block Hash
32 bytes	Merkle Root
4 bytes	Timestamp
4 bytes	Difficulty Target
4 bytes	Nonce

- To make a block valid, a Miner must construct the block so that:

```
Hash(Block_Header) < Difficulty_Target
```

Proof of Work

Bitcoin System

- Every transaction initiated by a **user** will be transmitted to all the **miners**

- Each miner will verify if a transaction is valid,

- Once verified, it will put the transaction into a local **pool**. Otherwise drop the transaction.

Bitcoin System

- Each miner will constantly select a bunch of transactions, together with one **coinbase** transaction, and try to construct a valid block.

  Tuning the `Nonce`, `timestamp` and `Merkle Root` to make the hash of the header smaller than the difficulty target

- Once a miner successfully constructs a valid block, it will broadcast the block to all the other miners.

  It is a competition

Bitcoin System

- Once a miner receive a valid block from another miner, it means he lost the competition.

- It will remove all the transaction in that new block from his **pool**, add the new block into the blockchain and start to compute the next block.

Bitcoin System

Once a transaction is recorded into the blockchain, it means this transaction is confirmed.

Bitcoin System

- Speed of blockchain growth.
- Miners’ incentive.
- Resolve conflict.

Speed of Growth

- The difficulty of constructing a valid block is controlled by the **`difficulty target`**

- Assume the possible results of a Hash function evenly distribute over the 32 bytes space.

- Finding an input whose hash is within **a small range** is more difficult.

Speed of Growth

- Bitcoin network try to control the growth speed to one new block every 10 minutes.

New Target = Old Target * (Actual Time of Last 2016 Blocks / 20160 minutes)

- Bitcoin system adjust the difficulty target every 2016 blocks.

Miners' Incentive

- In every block, there is a **coinbase** transaction.
- This is a special type of transaction which has no input, only output.
- In this transaction, a miner give himself a certain amount of bitcoins.

Miners' Incentive

- A miner has to maintain the blockchain to be able to join the competition.

  This is why miner is the bank in this scenario.

- A miner has to win the competition to get the reward.

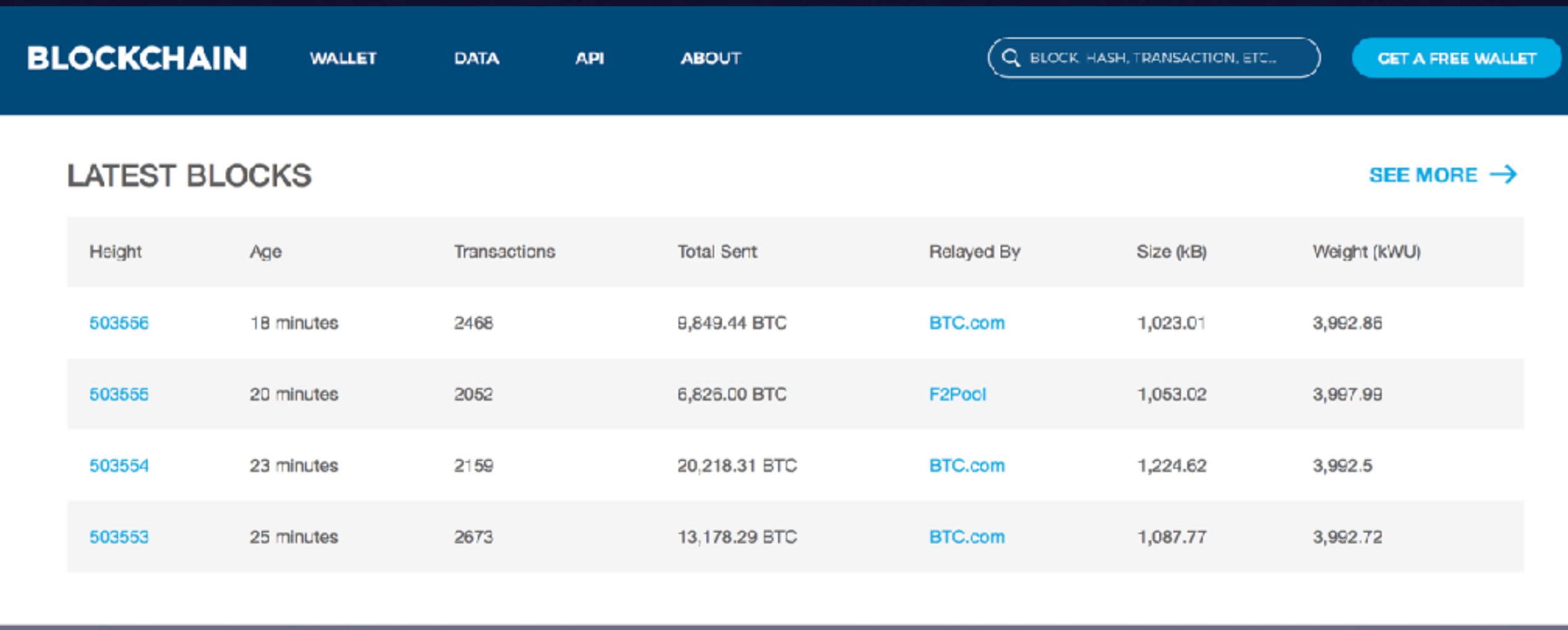
  It is a competition of computing power.

Miners' Incentive

- The new bitcoin in the coinbase transaction starts at 50 bitcoin per block.
- Every 210,000 blocks, this number reduce by half.

Blockchain Explorer

https://blockchain.info

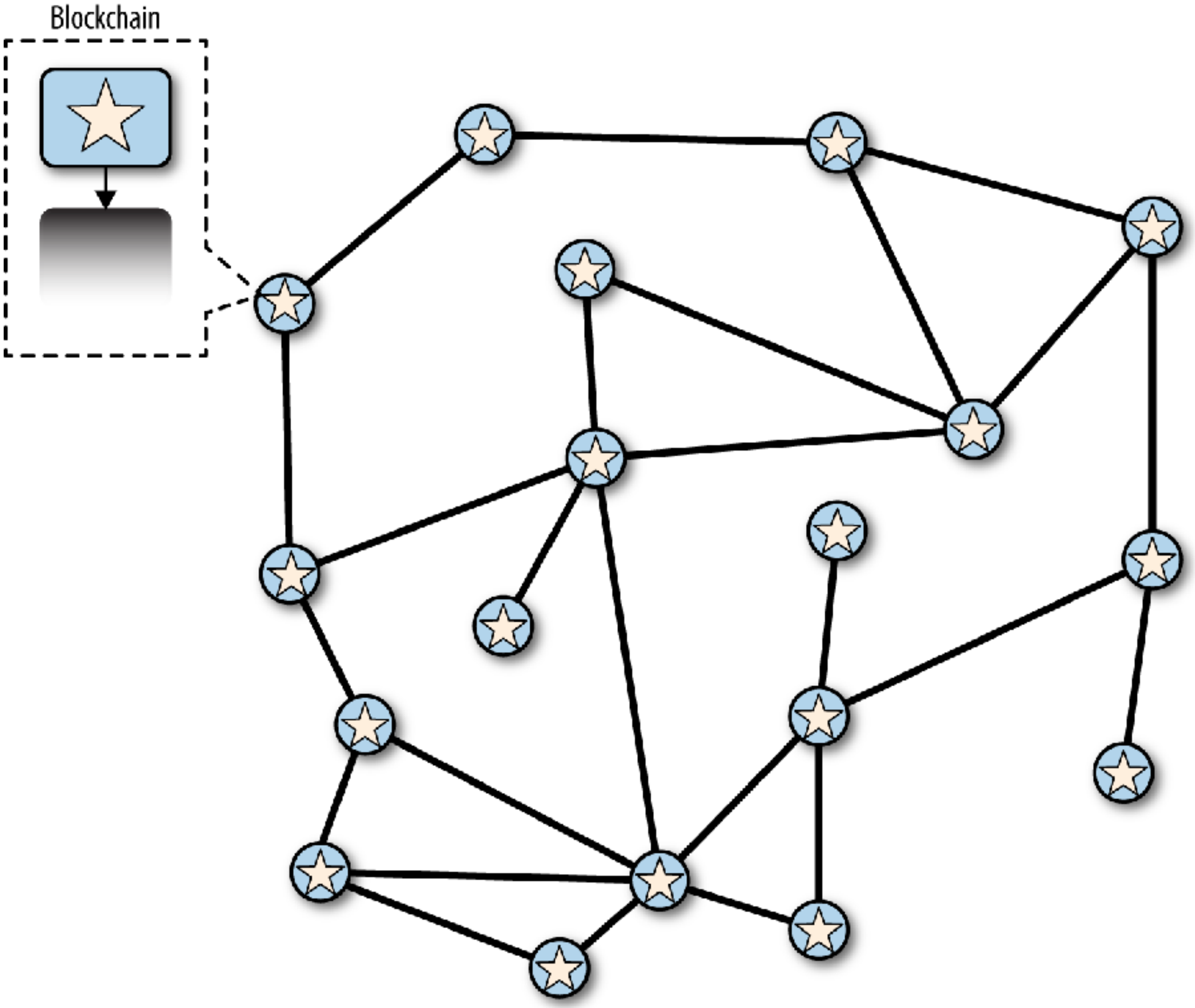


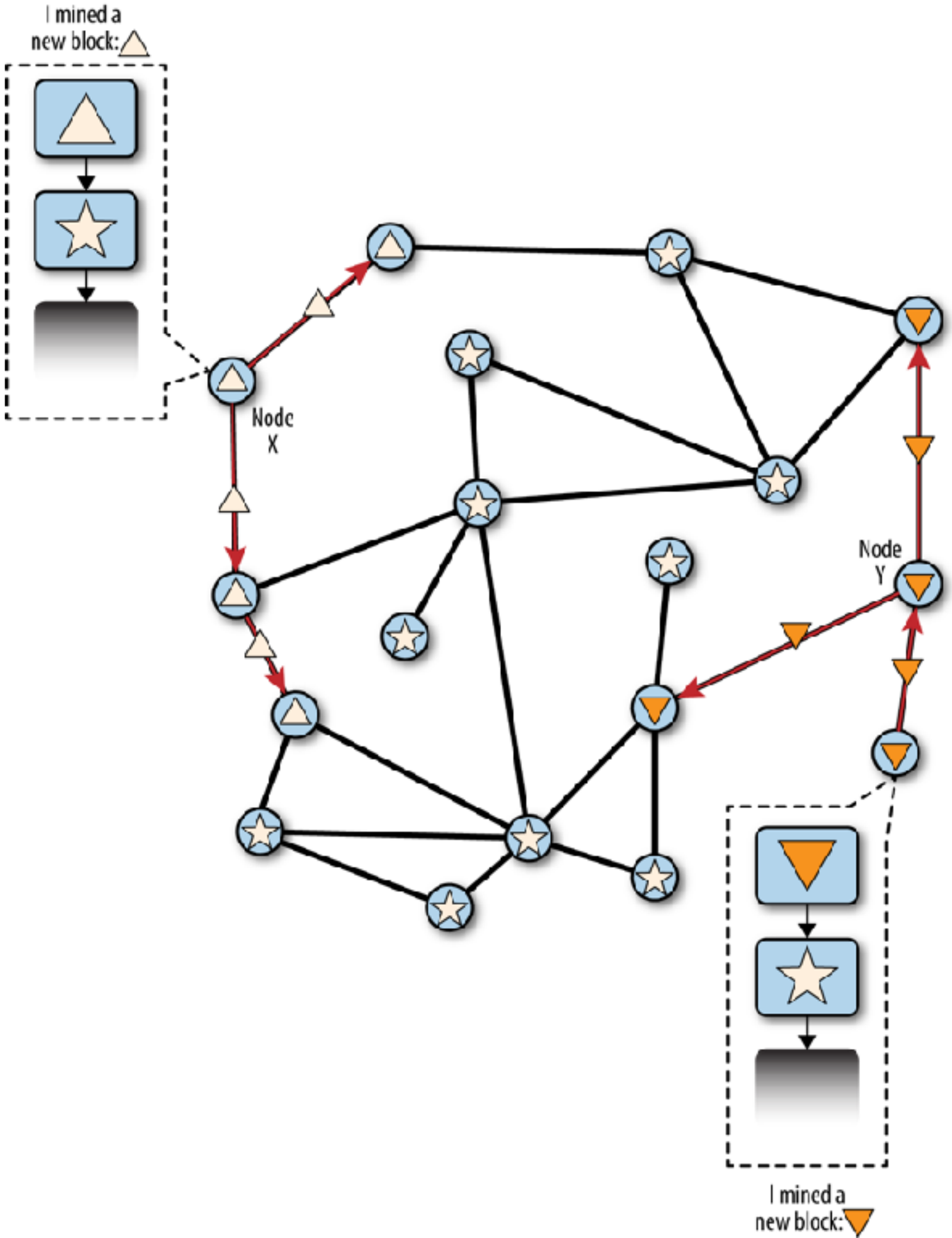
Economic Thoughts

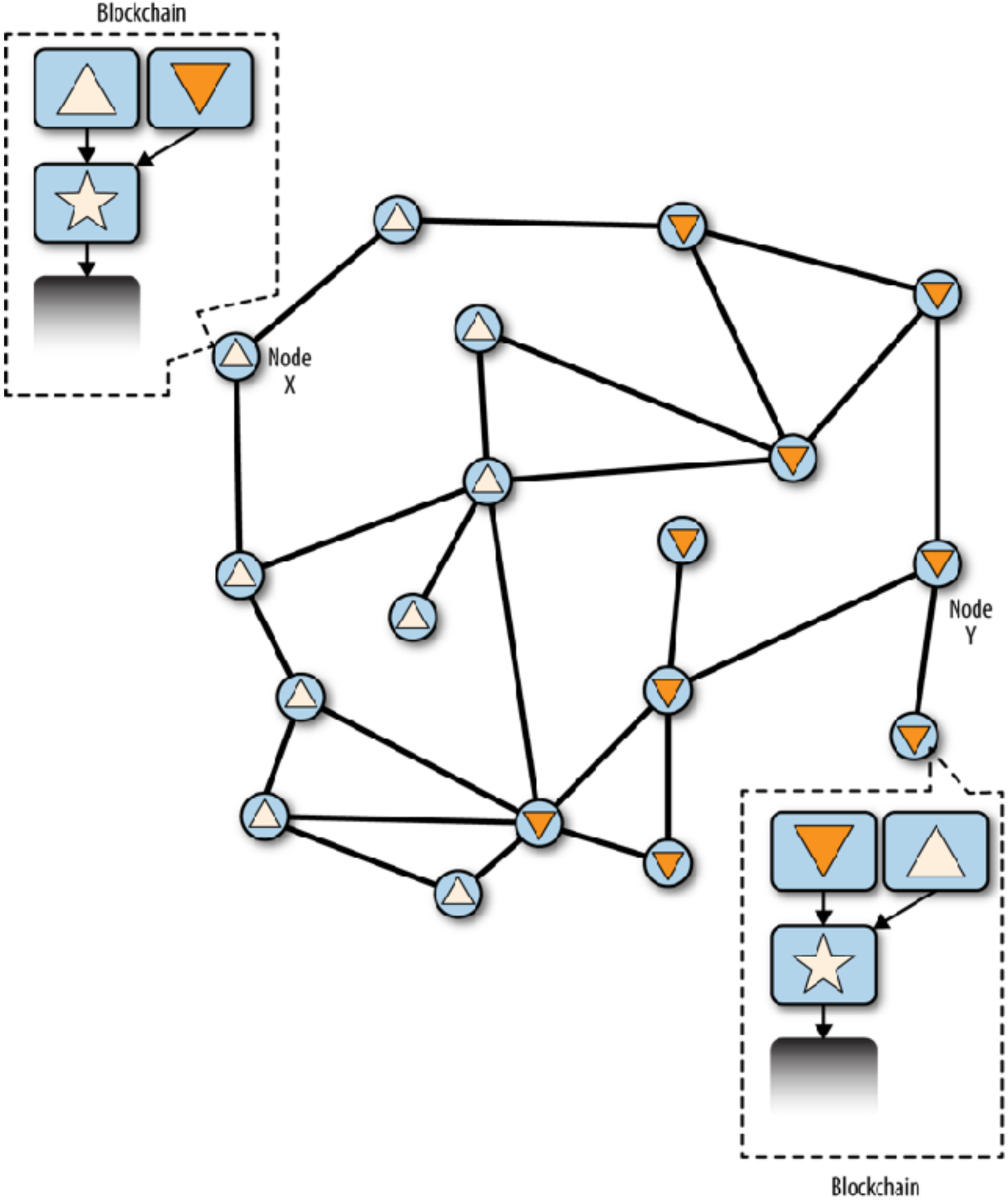
- Currency issuance without centralized authorities.
- Deflationary money.

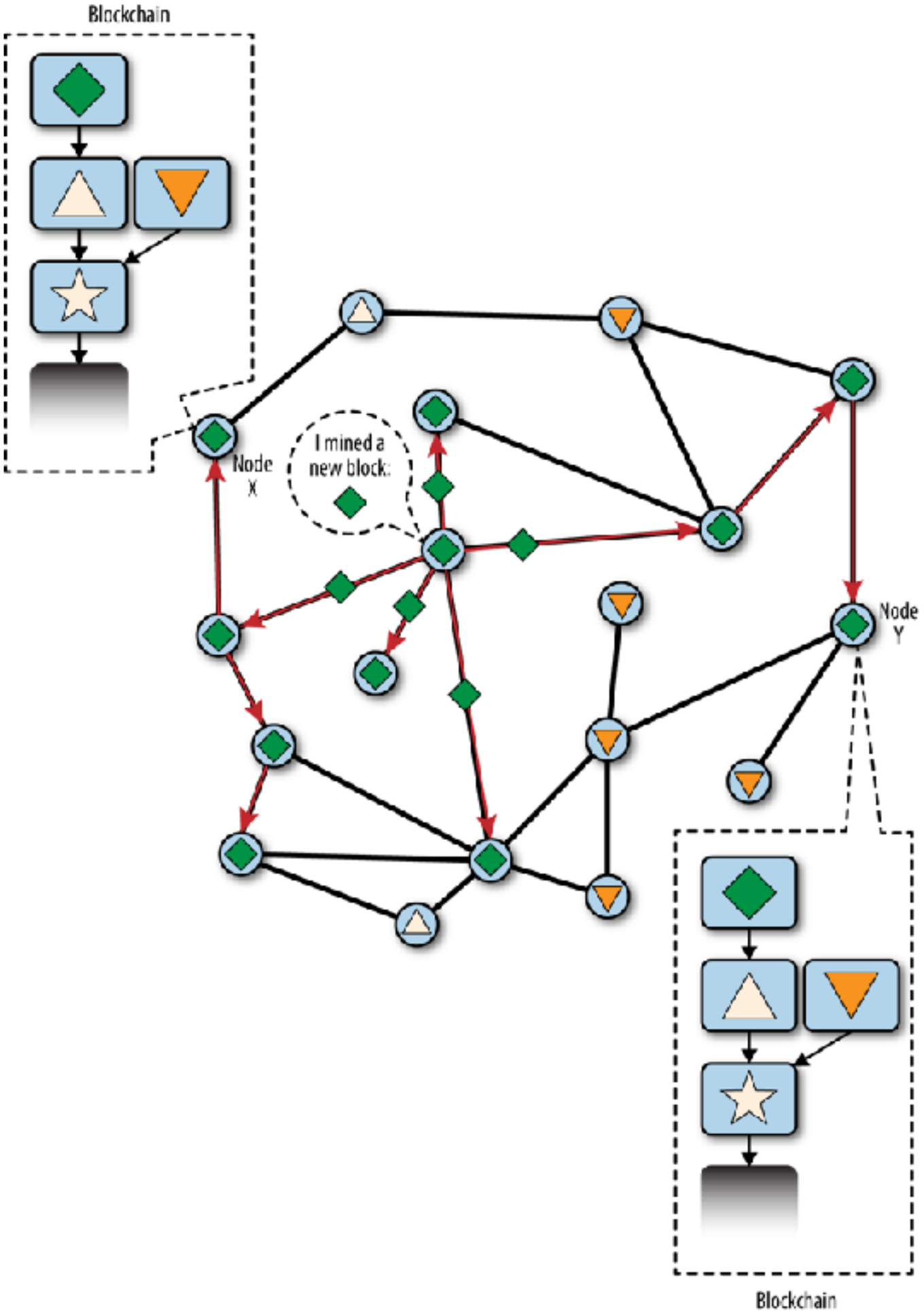
Resolve Conflict

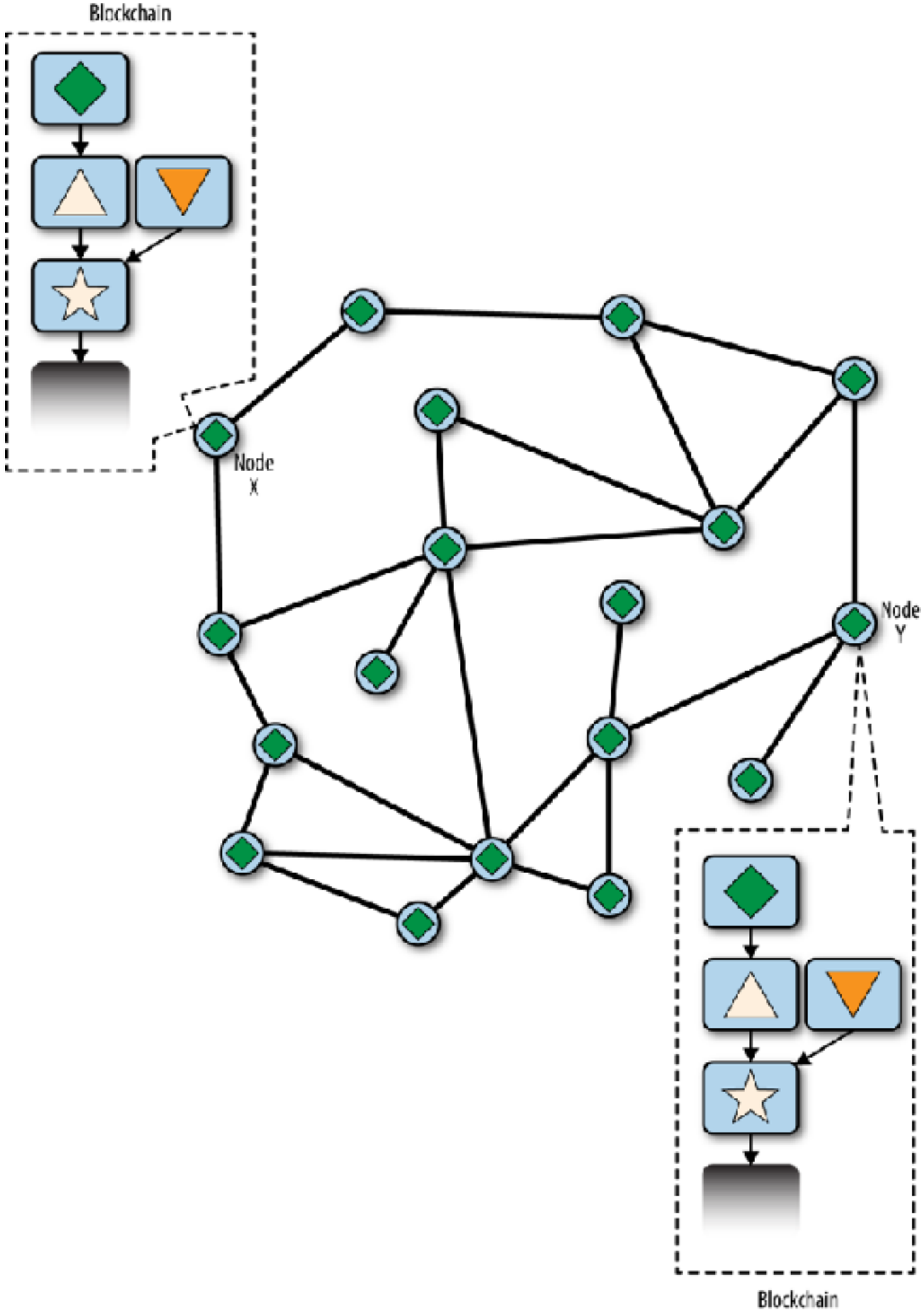
- What if two miners construct a new block at the same time?


Blockchain


I mined a
new block:
Node
X
Node
Y
I mined a
new block:


Blockchain
Node
X
Node
Y
Blockchain


Blockchain
Node X
I mined a new block.
Node Y
Blockchain


Blockchain
Node
X
Node
Y
Blockchain