Consensus & Blockchain

S P Suresh

Chennai Mathematical Institute

Formal Methods Update Meeting

IIT Mandi

July 17, 2017

The Bitcoin revolution is upon us

What is Bitcoin?

- Bitcoin: an exciting new currency system
  - digital
  - decentralized
- Invented by Satoshi Nakamoto in 2008
  - Elegant solution to the Byzantine Generals problem

Benefits for the user

- International currency
  - Instant transfer with very low transaction fees
- Shop online while maintaining privacy
- No risk of inflation
- Fundamentally impossible to counterfeit

How Bitcoin works – overview

- No central authority
- Everyone maintains a ledger of all transactions
- Continuously updated by everyone
- Some of the updaters get rewarded with new bitcoins – **created out of thin air** (this is the process of **mining**)
- But there is a cap – **21 million bitcoins**, all mined by **2140**

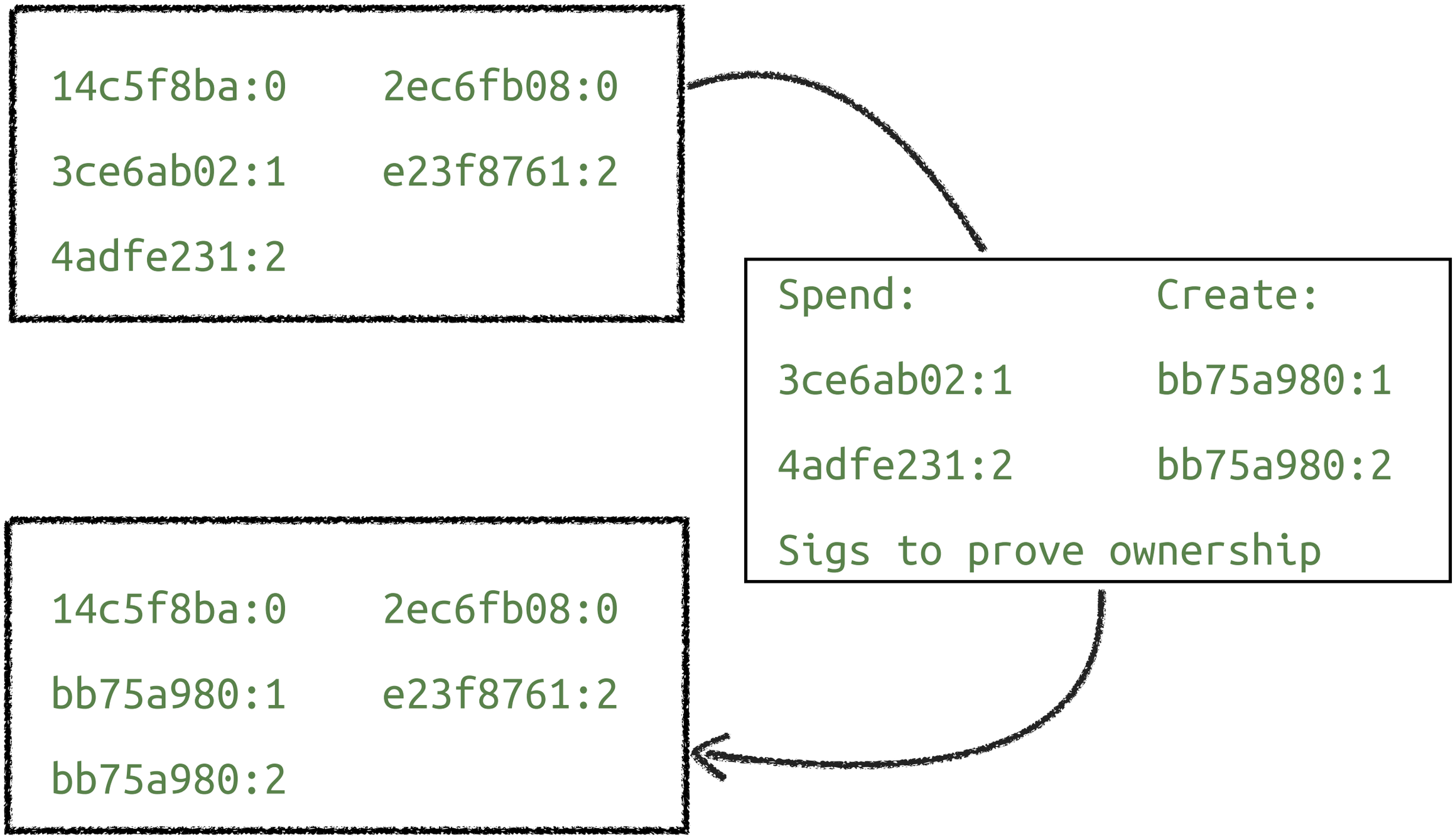
Fundamental challenges

- How to generate money without a central authority
- How to ensure money is not counterfeit
- How to prevent double spending
- How to validate transactions

Transactions

- Some input transactions
- Some output transactions
- Unspent amount — Comes back to sender
- Transaction fees — a small percentage
- Locking and unlocking scripts

State transition system



State transition system

```
Apply(S1, TX) -> S2:
```

1. For each input in TX:
    - If the referenced UTXO not in S1, return error
    - If the signature does not match the owner of UTXO, return error
2. Sum of inputs less than sum of outputs, return error
3. Return S2 with all input UTXO removed and all output UTXO added

Blocks

- Can store up to **1024** transactions
- Subject to revision
- Hash of all the transactions stored in the header

The blockchain

- The Bitcoin ledger
- Replicated across all users
- Every transaction is broadcast to everyone
- New chunks of transactions get added to the ledger in blocks (by **miners**), and broadcast to everyone
- Bitcoin wallets update their copy of the ledger

The blockchain

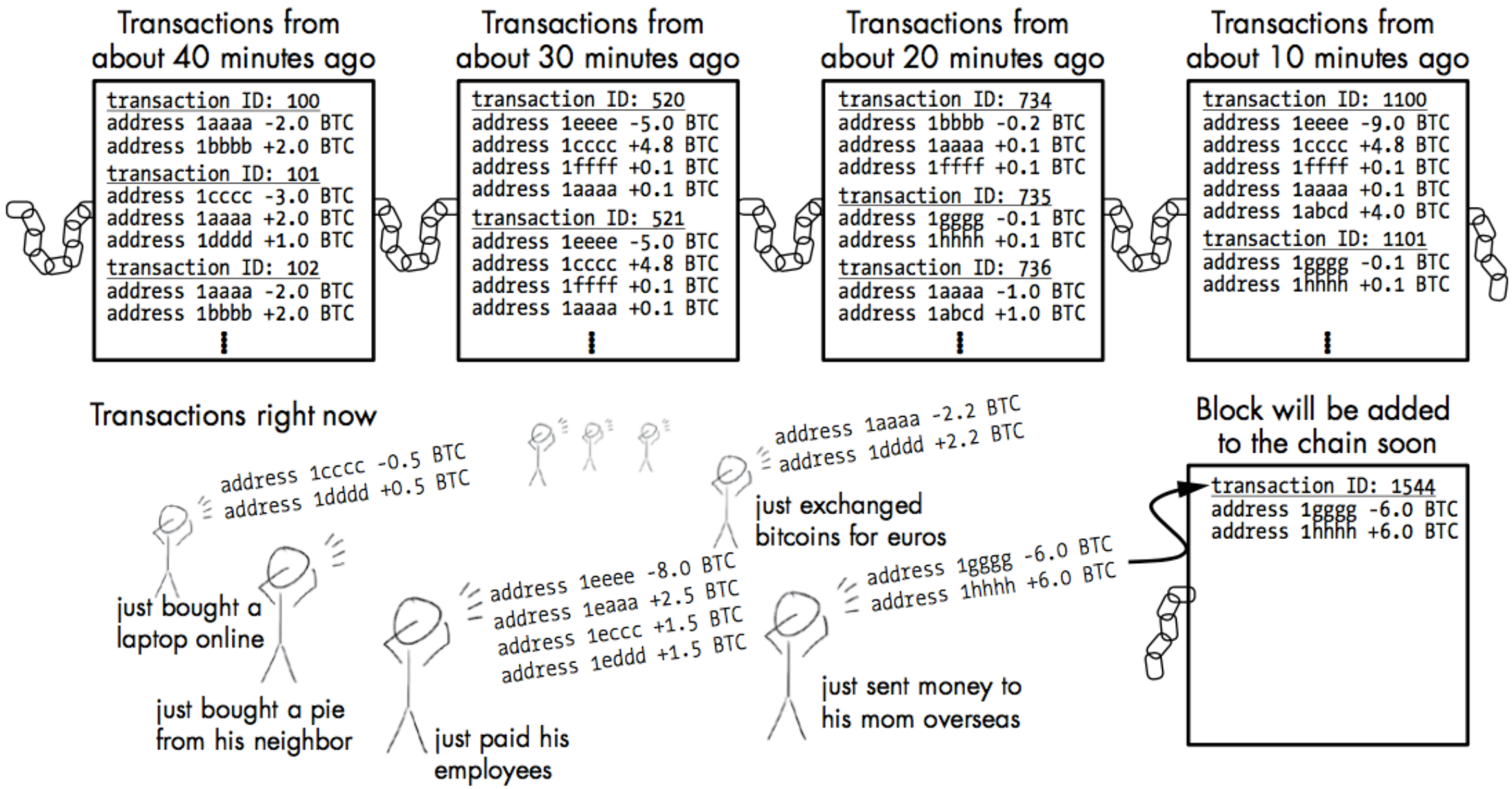


Figure 2-9: Bitcoin transactions are grouped into blocks that are added to the blockchain every 10 minutes.

Is a block valid?

---

1. Check if previous block referenced exists
2. Check timestamp
   - greater than timestamp of previous block
   - less than 2 hours into the future
3. Check proof of work
4. Let S[0] be state at the end of previous block
5. If the block has n transactions, do S[i+1] = Apply(S[i], TX[i])
6. Return S[n]

Concurrent chain management

- Maintain an ever growing chain
- Only operation provided is append a new entry to the chain
- Many users concurrently accessing the chain

- **Centralized** — Shared memory
- Users should agree on the last node added to the chain
- **Universal data structure** — Chain is a log of operations

Consensus objects

- Each node has details of the operation and a **consensus object**
- Users compete for the next node to add to the chain
  - The winner's node is added
- The consensus object regulates this competition
- Implemented using `compare-and-set`
  - Initialize `winner` to `-1`
  - `compare-and-set(winner, -1, processname)`

Distributed consensus

- There is no central controlling node in bitcoin
- How to achieve consensus?
  - Agents may lie!
- **Byzantine generals problem**
  - Heavily studied in distributed computing
  - Achieve consensus by a **maximal information protocol**
  - Works only when at most a third of the users are malicious
  - But … **everyone** is potentially malicious in the blockchain

The blockchain lottery

- **Miners** - run an open-source Bitcoin mining program
- Miners add new blocks to the ledger after checking correctness of transactions
- One winner is chosen from all the miners
- Rewarded with newly minted bitcoins and transaction fees

More on the blockchain

- No central authority to pick a winner
- Adding a block requires work
- Winner is the one who finishes this task first
- Sends **proof of work** to the other miners
- Others give up trying to add a block and accept the winner — why??

Blockchain forking

- Sometime two miners can strike the **same gold** at the same time!
- The blockchain has **forked**
- There are two versions of the blockchain now
- The longer chain is chosen by everyone
- **Eventually consistent!**

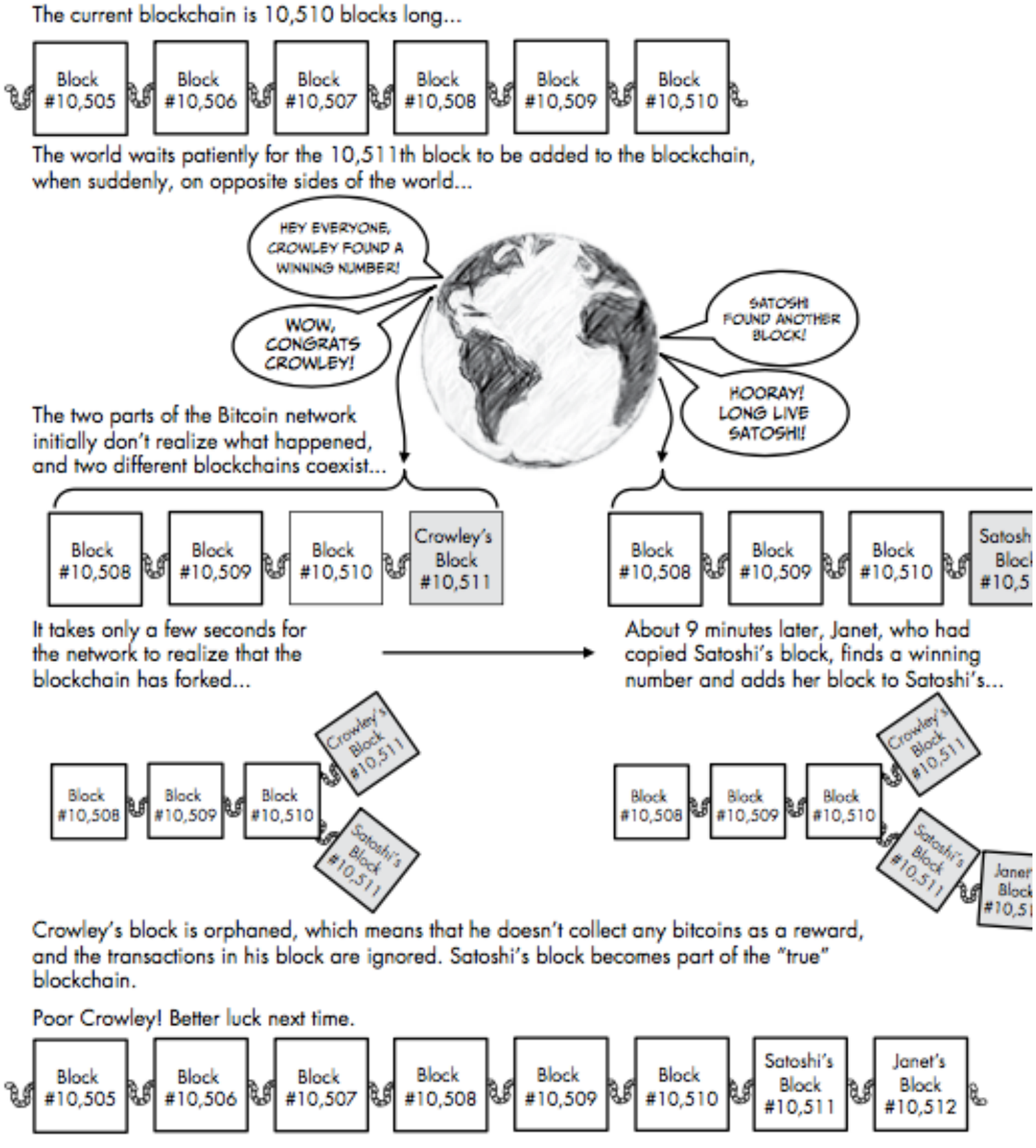


Figure 2-13: Bitcoin miners Crowley and Satoshi find a block at the same time, creating two copies of the blockchain. The resolution to the forked blockchain occurs when Satoshi's version of the blockchain adds another block before Crowley's, and Satoshi receives the reward.

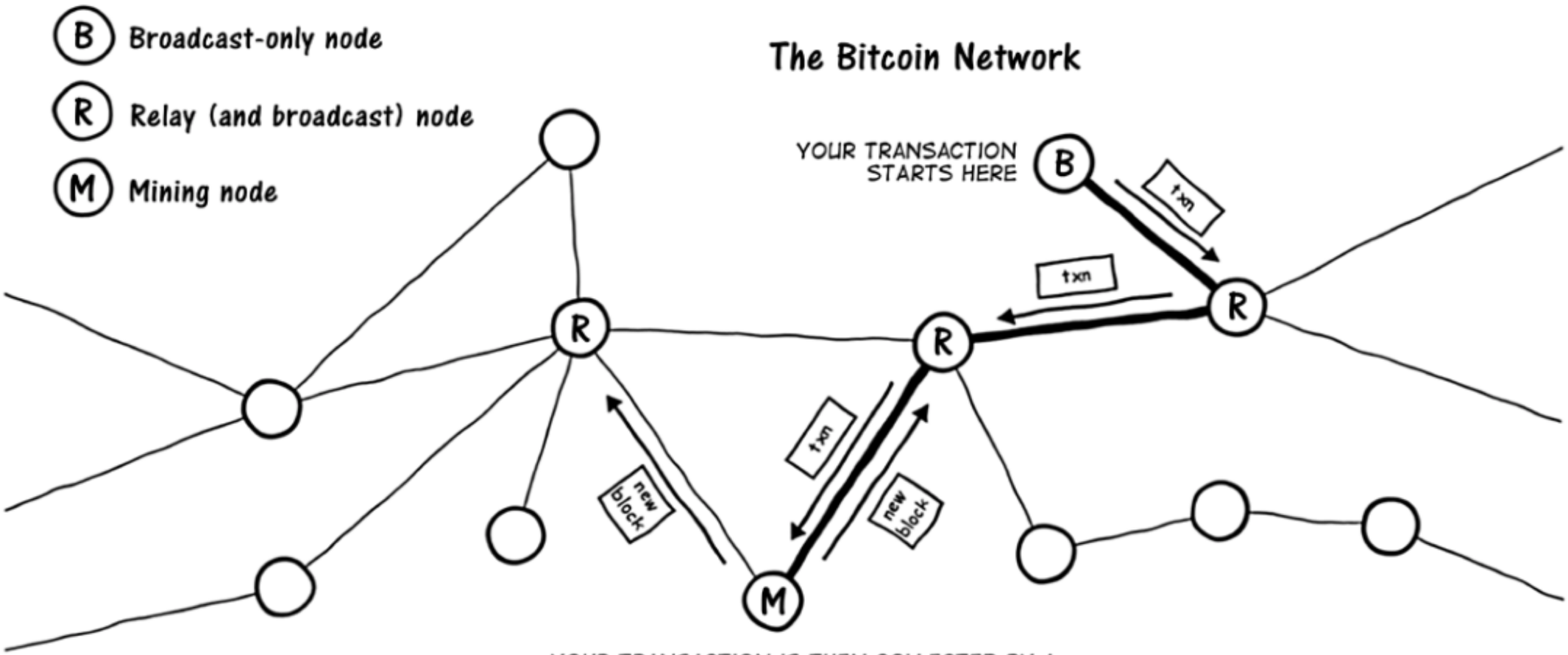
Mining

- Reward of the blockchain lottery
  - Winner gets both new bitcoins and transaction fees
- One new block is added to the ledger every 10 minutes
- Each miner adds one block once in 8 months
- Difficulty of task is calibrated (dynamically) to account for increase in computing power

Mining

- For the first 210,000 blocks, reward was 50BTC
- The reward halves for each chunk of 210,000 blocks
- The reward is now 12.5BTC
- One block added per 10 minutes, so roughly four years for 210,000 blocks
- By about 2140, almost all mining would be done
- The only incentive is the transaction fees after that point

Bitcoin mining – the process



YOUR TRANSACTION IS THEN COLLECTED BY A MINING NODE, WHERE IT IS PUT INTO A BLOCK. THIS BLOCK IS BROADCAST TO NEIGHBORING NODES.

Bitcoin mining – the process

- Relay nodes check the validity of transactions
- Within seconds, a transaction arrives at **all** mining nodes
- Mining nodes collect a batch of transactions and add it to the ledger after **solving** the block
- Within ten minutes of a transaction, a block containing the transaction is added to the ledger by some miner (usually one lucky winner)
- New block is broadcast to all nodes within seconds

Mining – solving a block

- Solving a block is the central idea in bitcoin
- A block consists of a list of transactions and a block header
- One special transaction added by the miner, awarding herself 12.5 bitcoins

Mining – solving a block

- Block header has
  - Hash of previous block header (chaining)
  - Hash of all transactions in this block
  - A nonce
  - A difficulty target
- Solving – **Find a nonce such that the hash of the block header is less than the difficulty target**

Vulnerabilities?

- Majority is not enough — **selfish mining**
- **Routing attacks**
- Anything else???

References

- Bitcoin for the Befuddled
- Mastering Bitcoin
- Lecture on Blockchain
- EconTalk episode
- EconTalk episode 2
- More EconTalk: Venezuela and Bitcoin
- Ethereum white paper