Mechanics of Bitcoin (5)

Mining & Fork

Prof. James Won-Ki Hong

Distributed Processing & Network Management Lab.
Dept. of Computer Science and Engineering
POSTECH

http://dpnm.postech.ac.kr
jwkhong@postech.ac.kr

Table of Contents

Detailed Mining Process (1/11)

- **Distributed Consensus**
  1) Every full node performs independent verification for each transaction
  2) Miners add the verified transactions to the new block through a Proof-of-Work algorithm
  3) After all nodes have verified the new block, it is connected to the Blockchain
  4) Every node selects the longest chain on the Bitcoin network

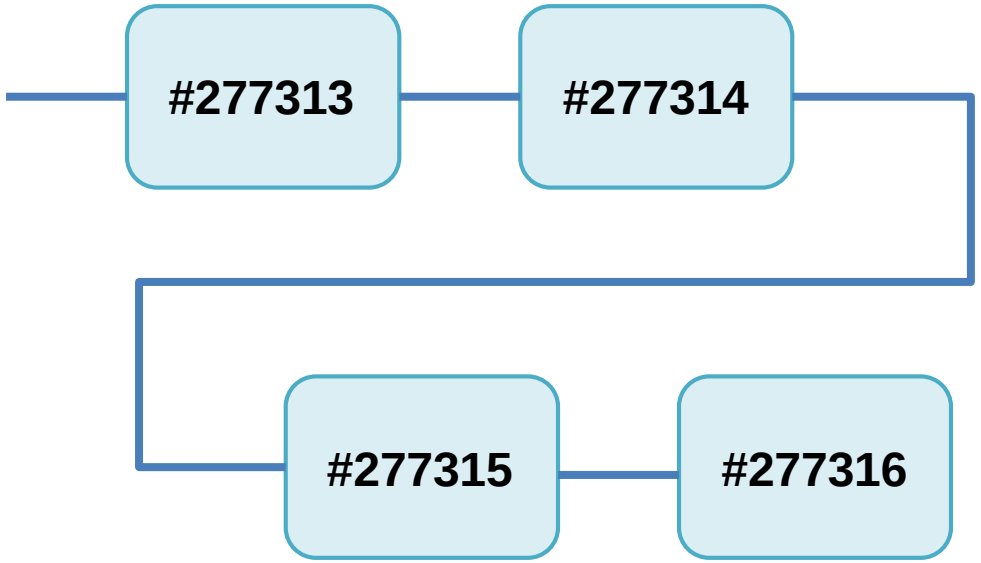
Detailed Mining Process (2/11)

- **Verification of Transactions**
  - The transaction's syntax and data structure must be correct
  - Coinbase transactions should not be relayed
  - For each input, if the referenced output exists in any other transaction in the pool, reject this transaction
  - Add to the orphan transactions pool, if a matching transaction is not already in the pool
  - For each input, the referenced output must exist and cannot already be spent
  - Reject if the sum of input values < sum of output values
  - Reject if transaction fee would be too low to get into an empty block

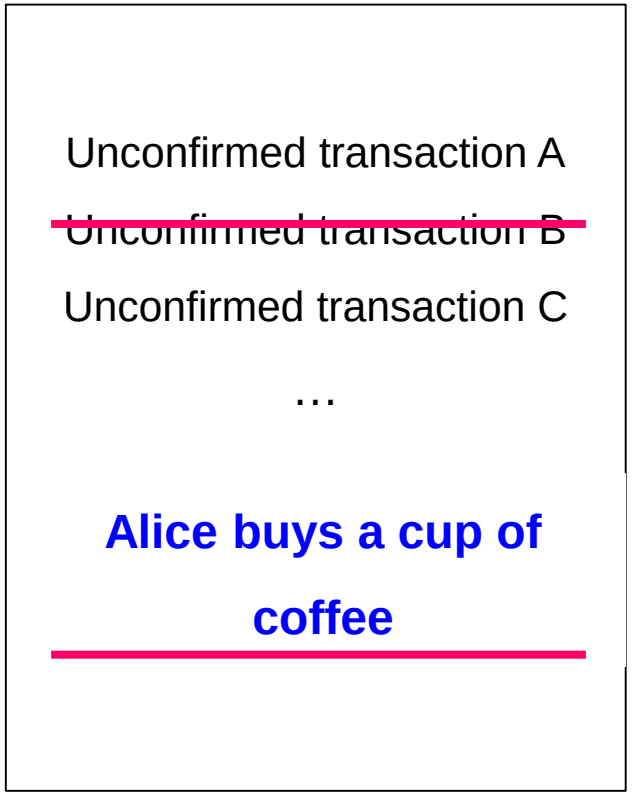
➢ **For a complete rules, checkout the Bitcoin protocol rules wiki**
https://en.bitcoin.it/wiki/Protocol_rules

Detailed Mining Process (3/11)

- **Adding a transaction to a block**



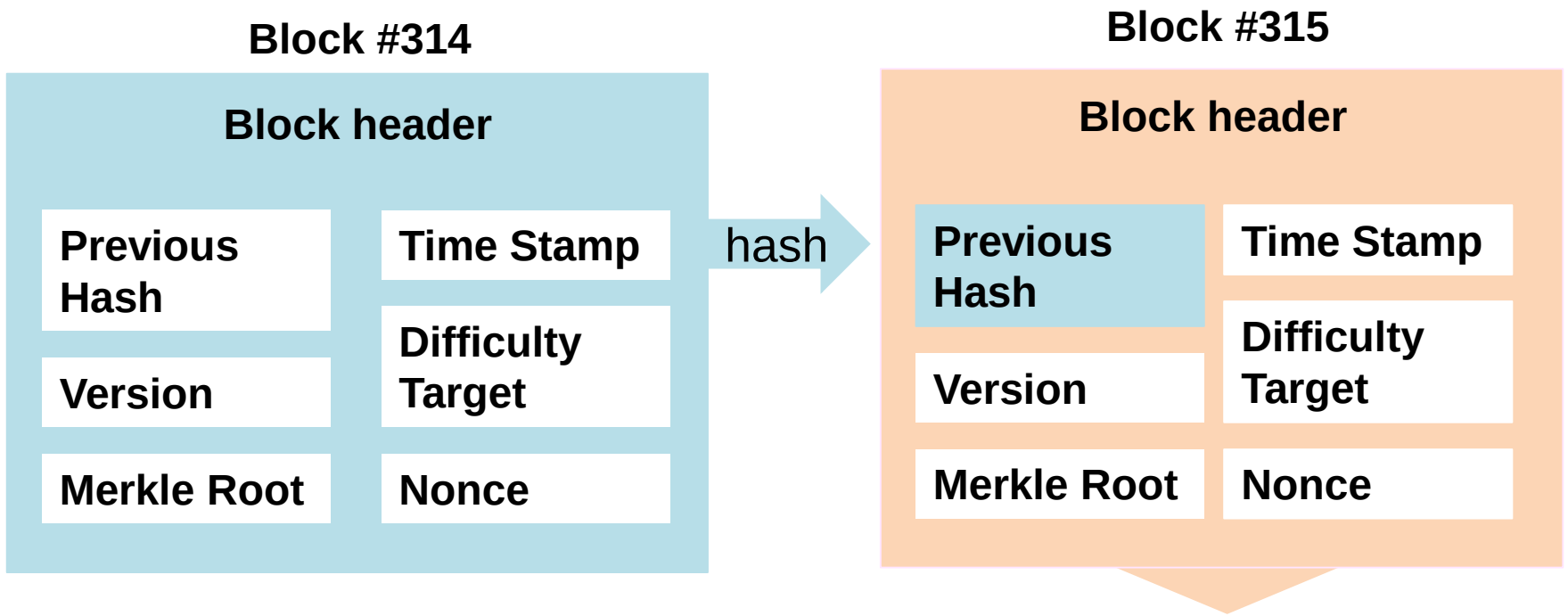
#277316
Candidate block



Memory pool
(transaction pool)

Detailed Mining Process (4/11)

- **Mining the Block(1)**
  - **Consensus in Bitcoin: Proof of Work**

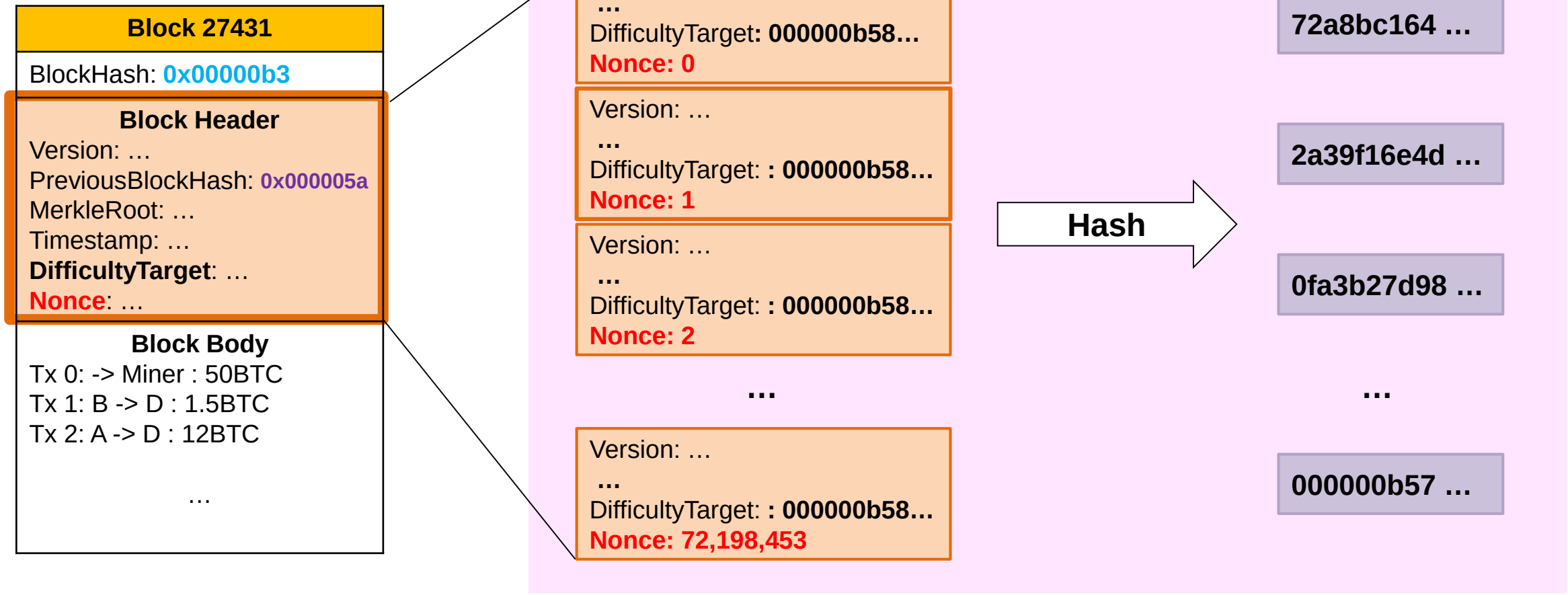


Hash(nonce + @) < Target Value

Find nonce to make hash value be under the target value

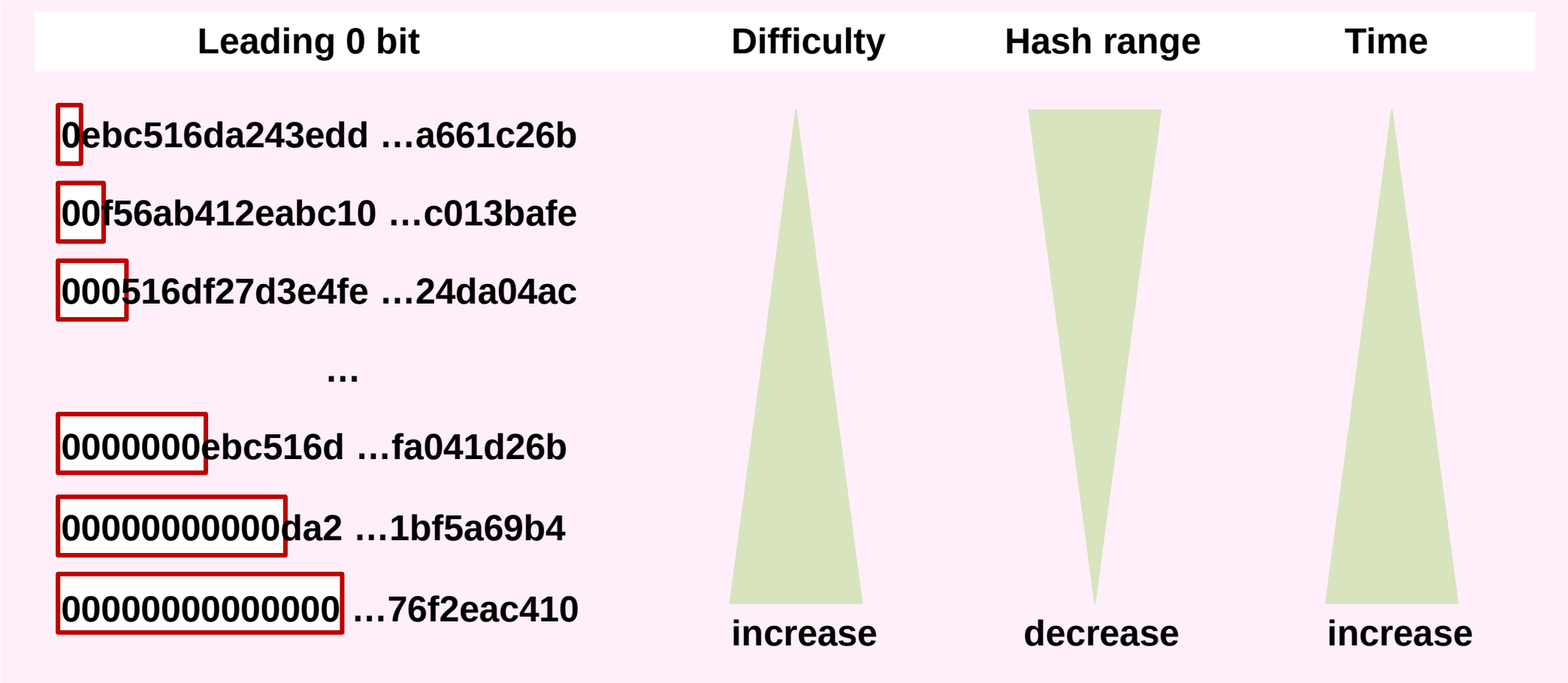
Detailed Mining Process (5/11)

- **Mining the Block(2)**
  - **Consensus in Bitcoin: Proof of Work**



Detailed Mining Process (6/11)

- **Mining the Block(2)**
  - **Difficulty: Difficulty bit**



Detailed Mining Process (7/11)

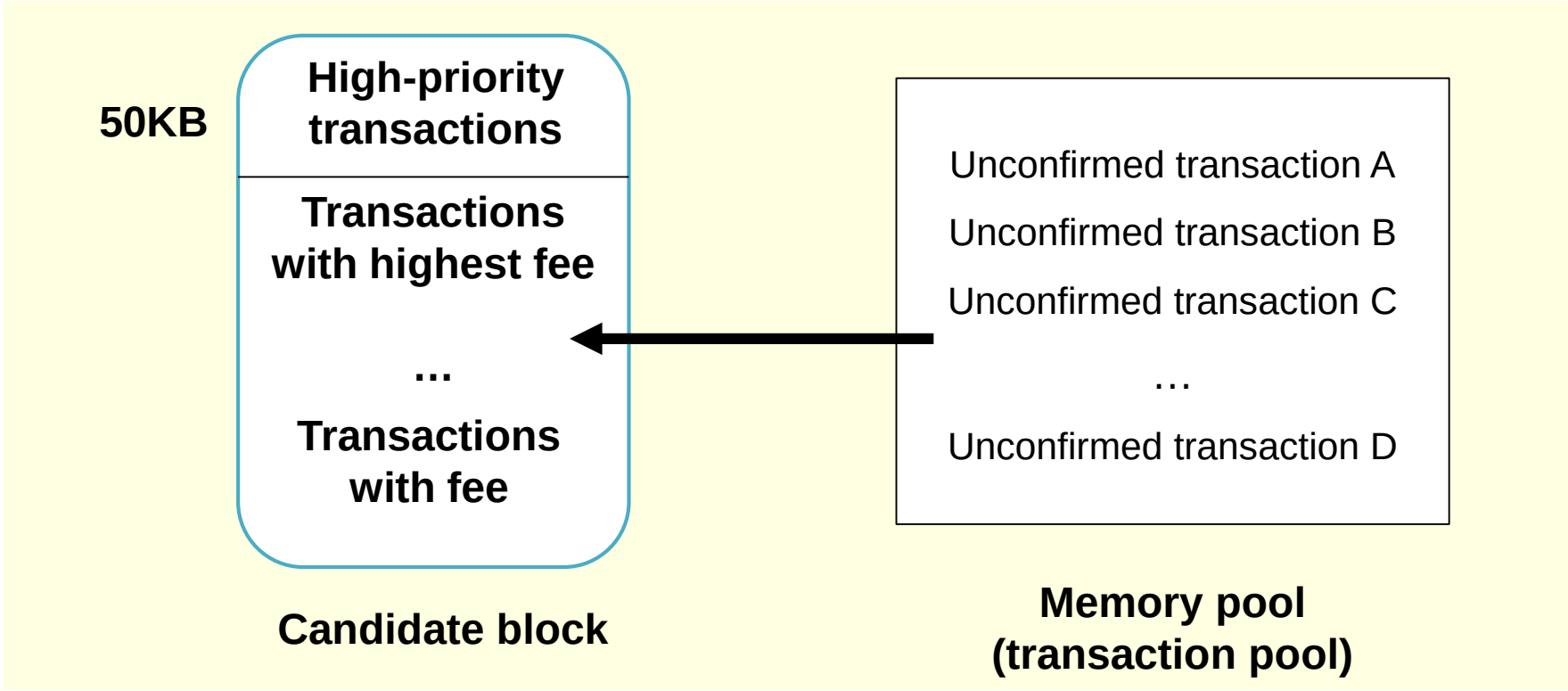
- **Difficulty**
  - 10 minute cycle
  - Be adjusted according to the rate of computer capacity increase and the number of computers participating in mining
  - Whenever 2016 blocks are added on the network, the nodes reset the difficulty target value

New difficulty = old difficulty * (Actual Time of Last 2016 Blocks / 20160 min)

- Time taken > 20160 min → decrease difficulty of mining
- Time taken < 20160 min → Increase difficulty of mining

Detailed Mining Process (8/11)

- **Incentives and Strategies: Transaction Ages, Fees and Priority**
  - **Priority is based on the age of UTXO to be consumed**
    - **UTXO with order and larger input values has higher priority**
  - **Priority = sum (Value of input * Input Age) / Transaction Size**



Detailed Mining Process (9/11)

- **Incentives and Strategies: Coinbase Reward and Fees**
  - **Generation transaction (= Coinbase transaction)**
    - The first transaction added to the block
  - **Coinbase**
    - newly generated coin while generating a new block
  - **Coinbase Reward**
    - Determined by the number of half-cycles of the Bitcoin Network
    - The number of half-cycles = Current block height / half-life interval(210000)
  - **Total Fees**
    - sum(inputs) - sum(outputs)

Detailed Mining Process (10/11)

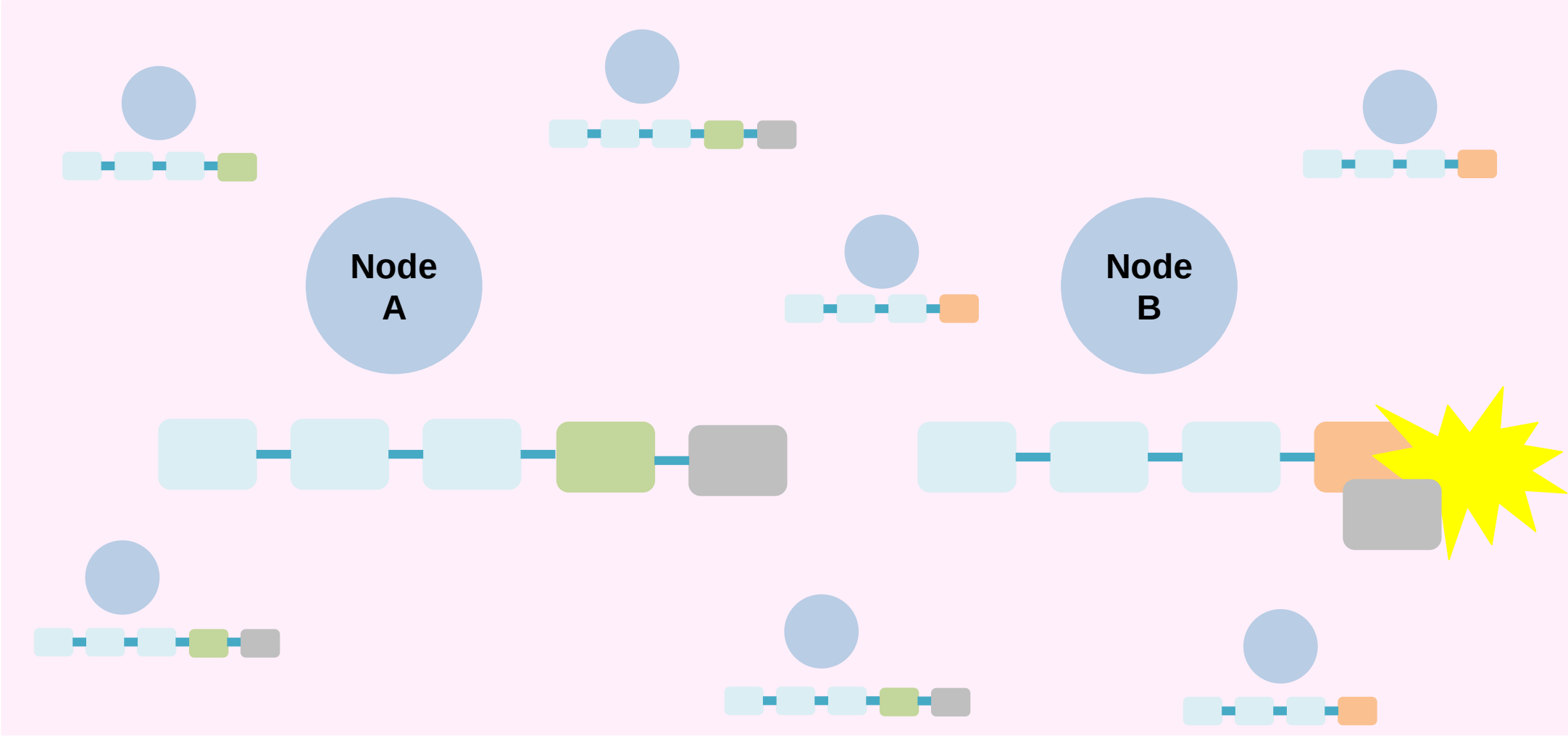
- **Incentives and Strategies: Coinbase Reward and Fees**
  - **277316 height**
  - **Coinbase Reward**
    - **277316 / 210000 = 1**
    - **50/2*1 = 25 Bitcoin**
  - **Total Fees:**
    - **sum(inputs) - sum(outputs)**
  - **Coinbase Reward + Total Fees**
    - **25 bitcoins + 0.09094928 bitcoin**


```
{
    "hex" : "01000000010000000000000000000000000000000000000000000000000000000000000000ffffffff\
0f03443b0403858402062f503253482fffffffff0110c08d9500000000232102aa970c592640d19de03ff6f329d\
6fd2eecb023263b9ba5d1b81c29b523da8b21ac00000000",
    "txid" : "d5ada064c6417ca25c4308bd158c34b77e1c0eca2a73cda16c737e7424afba2f",
    "version" : 1,
    "locktime" : 0,
    "vin" : [
        {
            "coinbase" : "03443b0403858402062f503253482f",
            "sequence" : 4294967295
        }
    ],
    "vout" : [
        {
            "value" : 25.09094928,
            "n" : 0,
            "scriptPubKey" : {
                "asm" : "02aa970c592640d19de03ff6f329d6fd2eecb023263b9ba5d1b81c29b523da8b21\
 OP_CHECKSIG",
                "hex" : "2102aa970c592640d19de03ff6f329d6fd2eecb023263b9ba5d1b81c29b523da8b21ac",
                "reqSigs" : 1,
                "type" : "pubkey",
                "addresses" : [
                    "1MxTkeEP2PmHSMze5tUZ1hAV3YTKu2Gh1N"
                ]
            }
        }
    ],
    "blockhash" : "0000000000000001b6b9a13b095e96db41c4a928b97ef2d944a9b31b2cc7bdc4",
    "confirmations" : 35566,
    "time" : 1388185914,
    "blocktime" : 1388185914
}
```

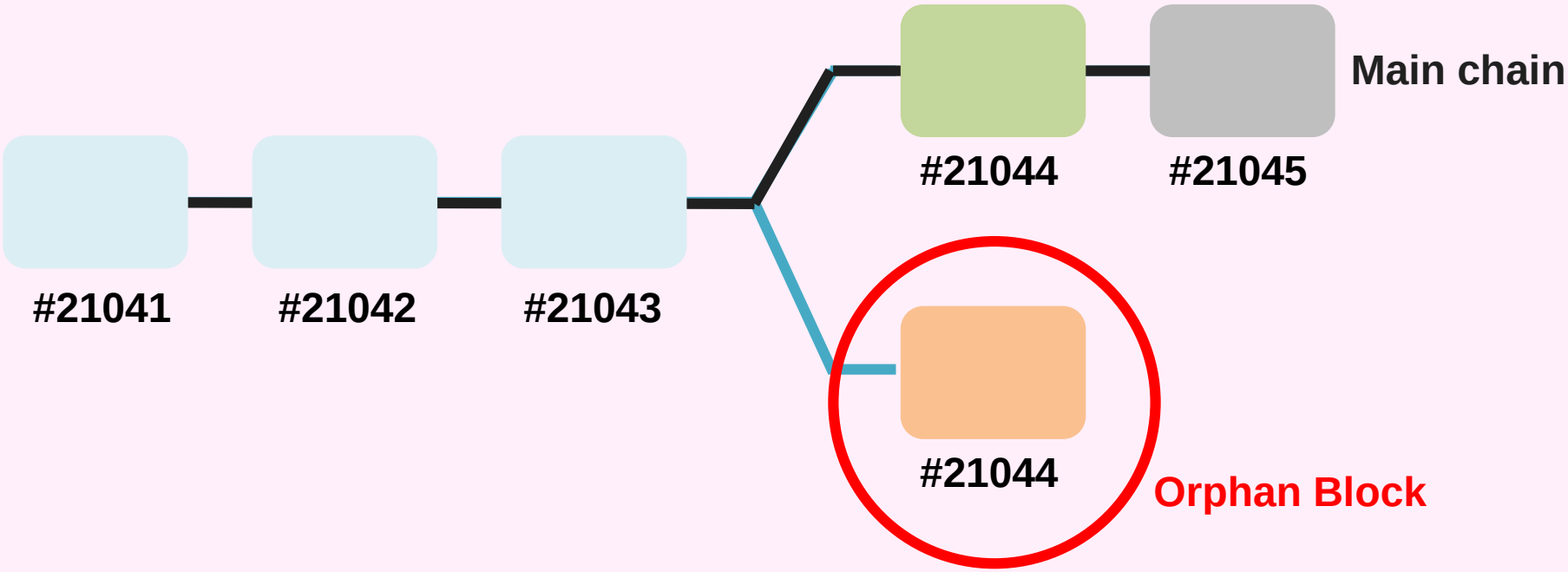
Detailed Mining Process (11/11)

- **Verifying new blocks**
  - **The block data structure is syntactically valid**
  - **The block header hash is less than the target difficulty (enforces the Proof-of-Work)**
  - **The block timestamp is less than two hours in the future (allowing for time errors)**
  - **The block size is within acceptable limits**
  - **The first transaction (and only the first) is a coinbase generation transaction**

Blockchain fork (1/3)



Blockchain fork (2/3)



Blockchain fork (3/3)

- **Confirmation**
  - **how many additional blocks are added after a particular transaction is included in a block**
  - **A sufficiently large confirmation**
    - **transaction has been kept in the block for a sufficiently long time and is therefore less likely to be canceled**
  - **1 confirmation**
  - **6 confirmation**

Summary

- **Detailed Mining Process**
  - Verifying transactions
  - Adding a transaction to a block
  - Consensus algorithm: PoW
  - Mining Incentives
  - Verifying a new block

- **Blockchain fork**

Reference

- Andreas M. Antonopoulos, **Mastering Bitcoin,** O'Reilly, 2014
- https://www.bitcoin.com/bitcoin-mining
- https://en.bitcoin.it/wiki/Proof_of_work
- https://www.coursera.org/lecture/cryptocurrency/mining-incentives-and-strategies-hvRiW
- https://www.youtube.com/watch?v=XCo6yyutYAM