Mechanics of Bitcoin (4)

Mining & Consensus

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

- Introduction to Mining and Consensus
- Overview of Mining

Introduction to Mining and Consensus (2/5)

- **What is Mining?**
  - The process by which a new block and Bitcoins are added on the Blockchain network
  - Provide computing power, mine a block and receive Bitcoins as a reward
  - Solve difficult math problems based on cryptographic hash algorithms using computing power
  - Proof-of-Work: The process of finding answers of math problems
  - Prevent double spending which are transactions that consume the same Bitcoin more than once

Introduction to Mining and Consensus (3/5)

- **What is Mining?**
  - The miners will validate new transactions and then record those transactions on the ledgers of the nodes of the world ➔ “Approved” transactions
  - A node that has received an approved transaction can own the Bitcoin contained in the transaction
  - Incentives
    - Bitcoins generated with new block
    - Transaction fees

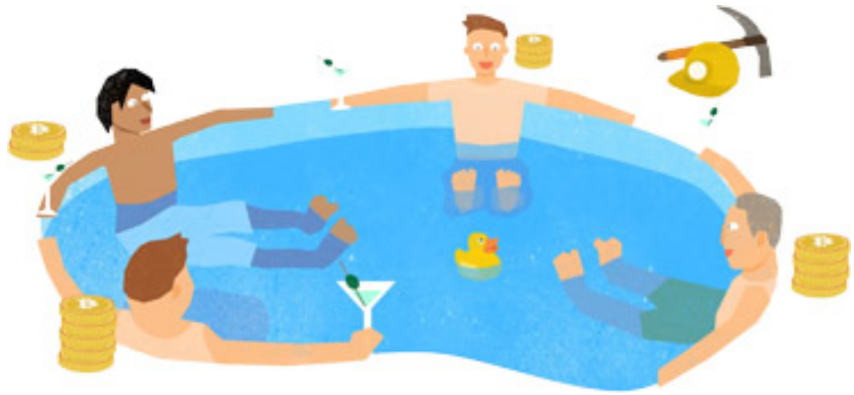
Introduction to Mining and Consensus (4/5)

- **Meaning of a new block generated from mining**
  - Indicates that competition among the miners is finished
  - Means that someone else in the competition has already won and that you have been defeated
  - Start of new competition

- **Mining node**
  - Specialized nodes
  - Receive unvalidated transactions on bitcoins and propagate them to other nodes
  - Add unconfirmed transactions to new blocks

Introduction to Mining and Consensus (5/5)

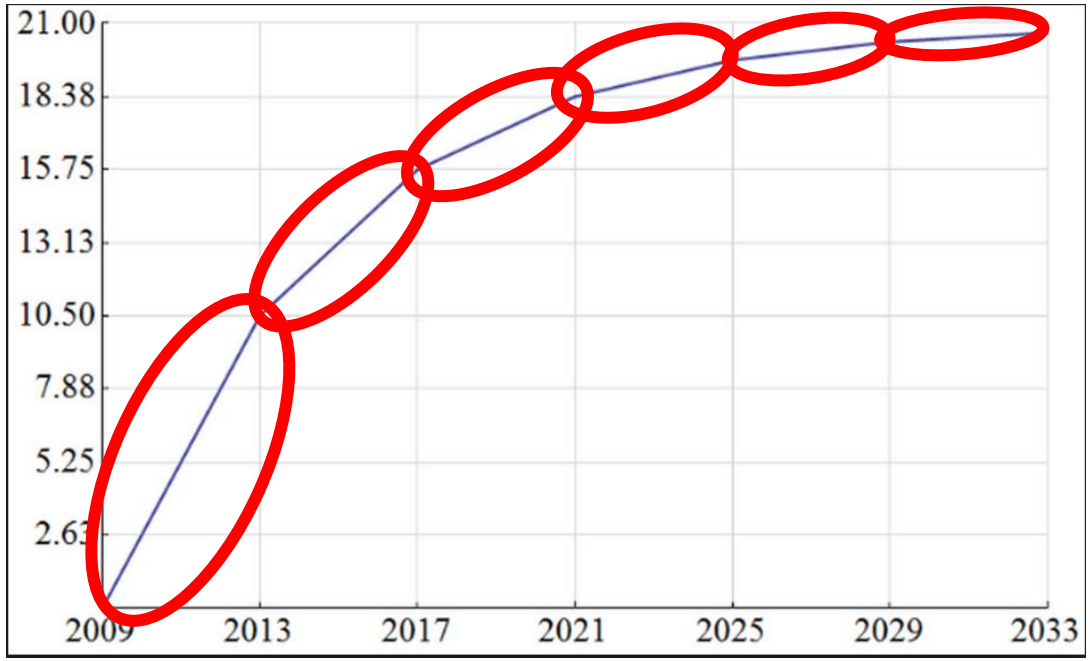
- **Mining Pool**
  - Allow miners to form a group to mine with others by sharing the load of mining to increase their chances of winning the competition
  - Share the incentives
  - Solo mining: miner can have all the rewards, but the success rate is very low
  - The amount of incentives is determined by how much the miners contribute to the pool through the PoW system
- **How to join a Mining Pool?**
  - Choose a Mining pool
  - Connect to the website, create an account and begin mining



http://bitcoindaily.com/media/bitcoin-pool-mining.jpg

Introduction to Mining and Consensus (1/5)

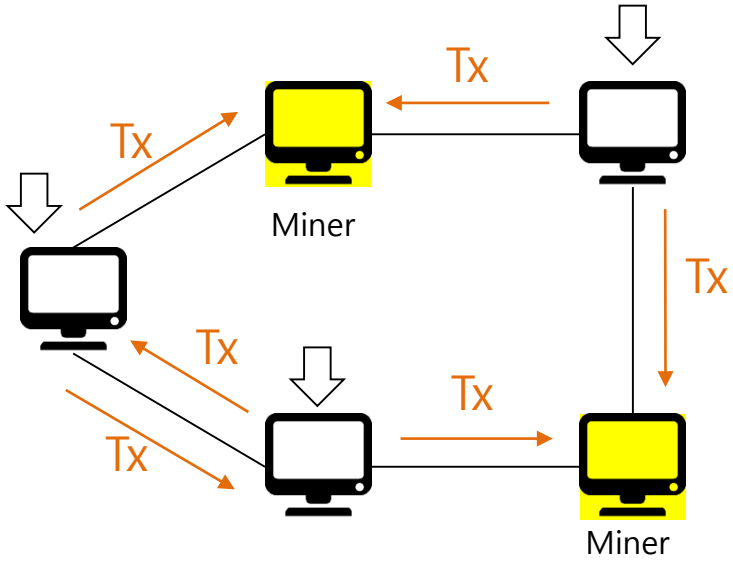
- **Bitcoin Economics and Currency Creation**
  - The amount of Bitcoin issuance is fixed
  - Each block is generated on average every 10 minutes
  - The amount of newly generated Bitcoins is reduced by 50% for every 210,000 blocks (approx. at every 4 years)



Overview of Mining Process (1/6)

1. Transaction Creation

- Node creates the transaction
- The node broadcasts the transaction to peer nodes connected to it

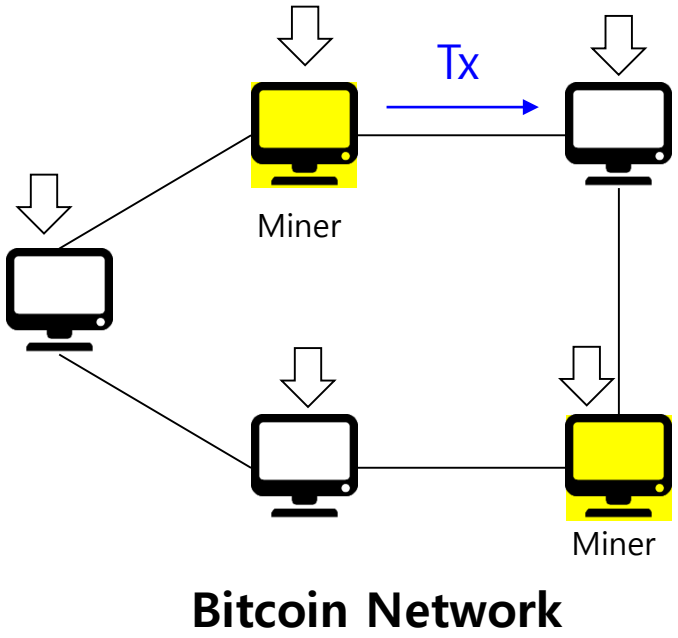


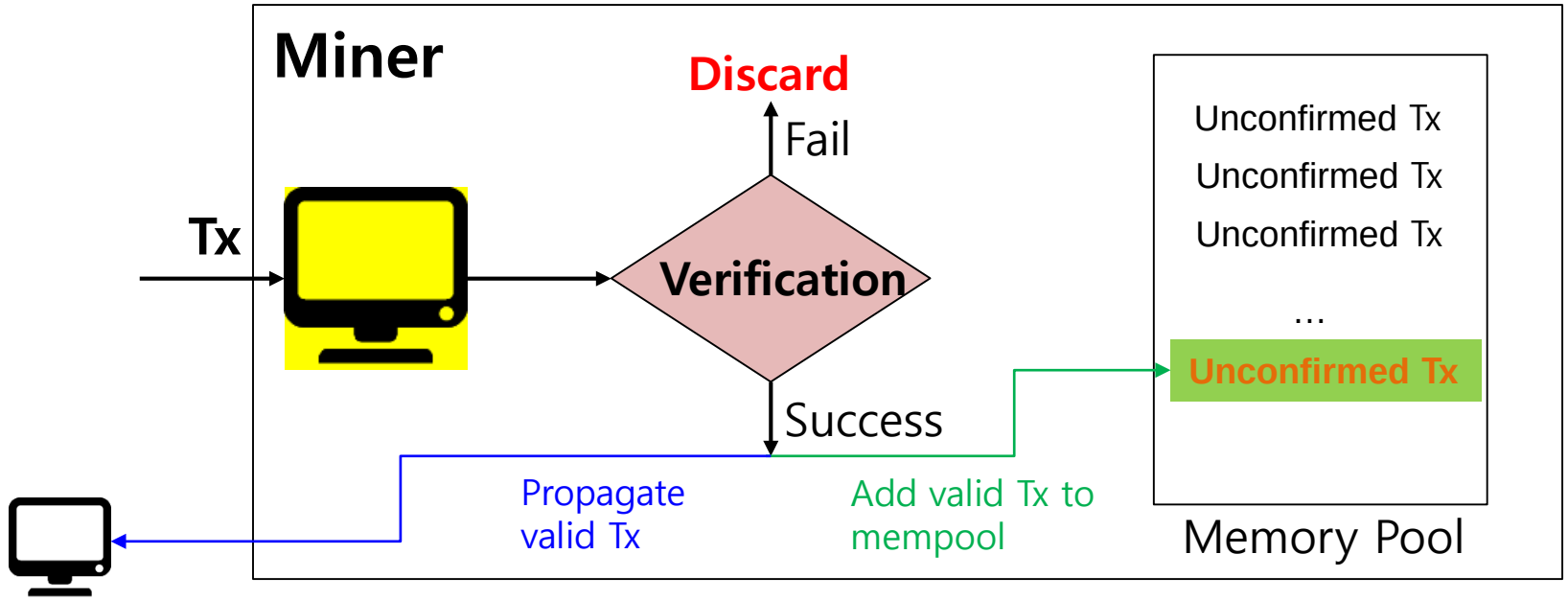
Bitcoin Network

Overview of Mining Process (2/6)

2. Verification of the transaction

- Check if the received transaction is valid or not
  - **Success:** Add this transaction to memory pool and propagate it to peer nodes
  - **Fail:** Discard this transaction (Invalid)

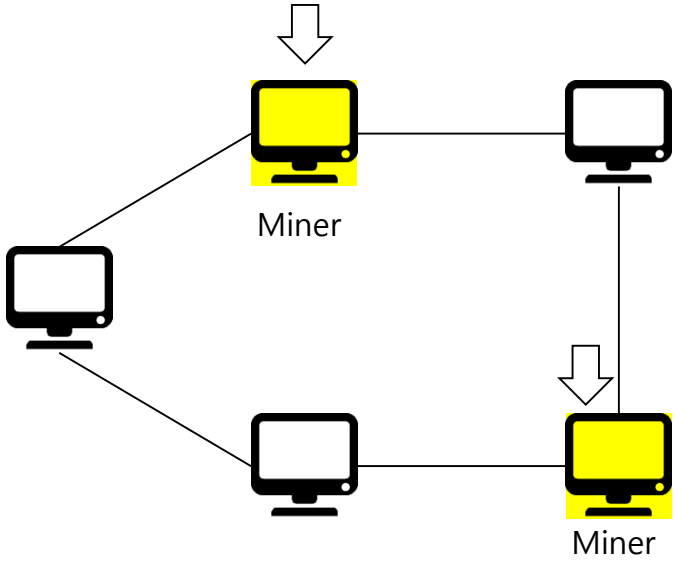


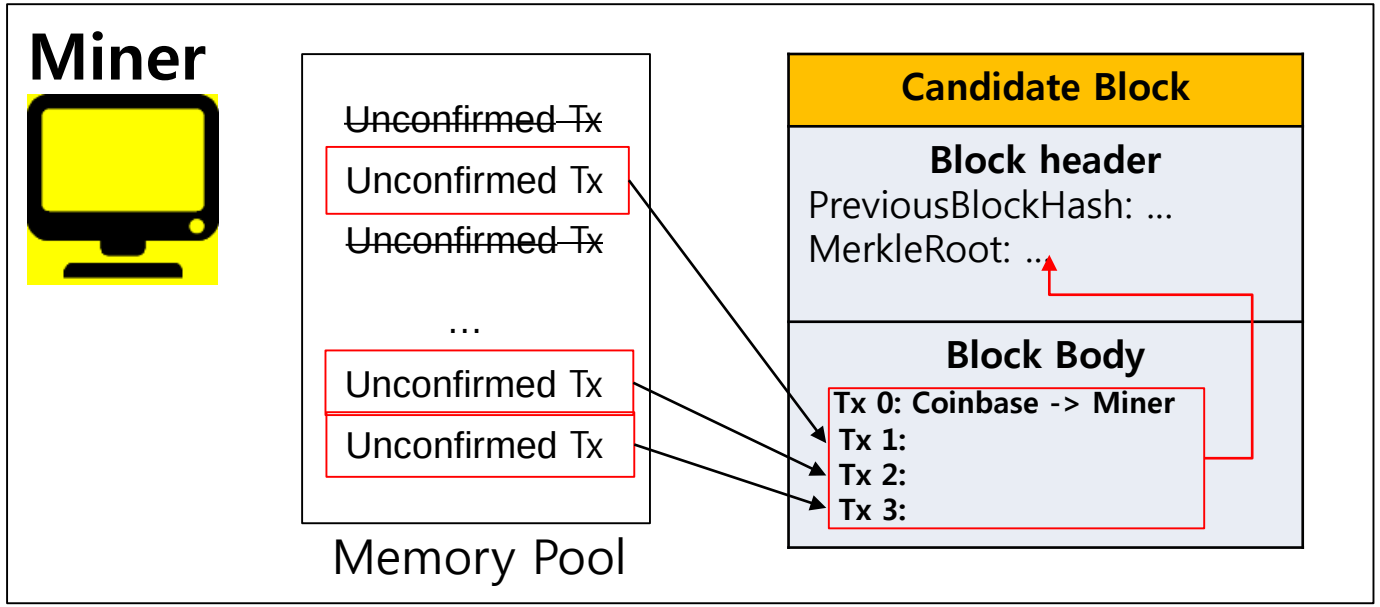


Overview of Mining Process (3/6)

3. PoW: Prepare for mining new block

- Remove the transactions included in previous block among transactions in memory pool
- Build a new block to be mined
  - Add a coinbase transaction to the block body
  - Add transactions in memory pool to the block body on a priority basis

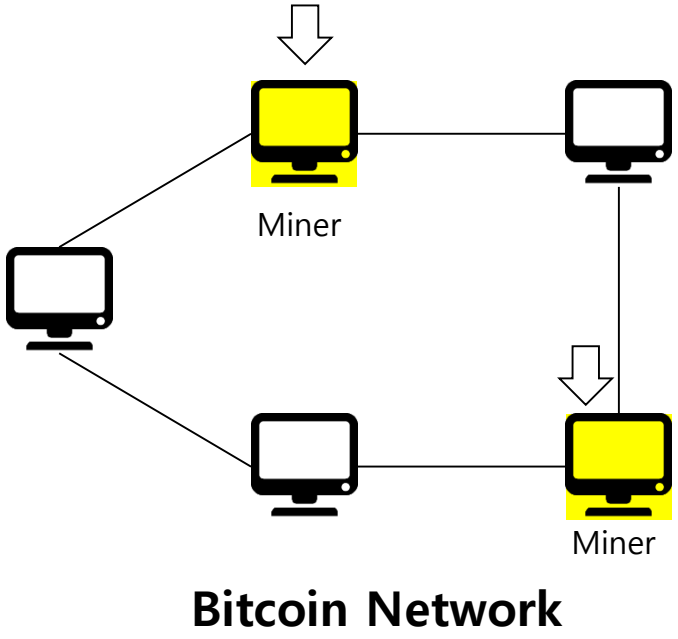


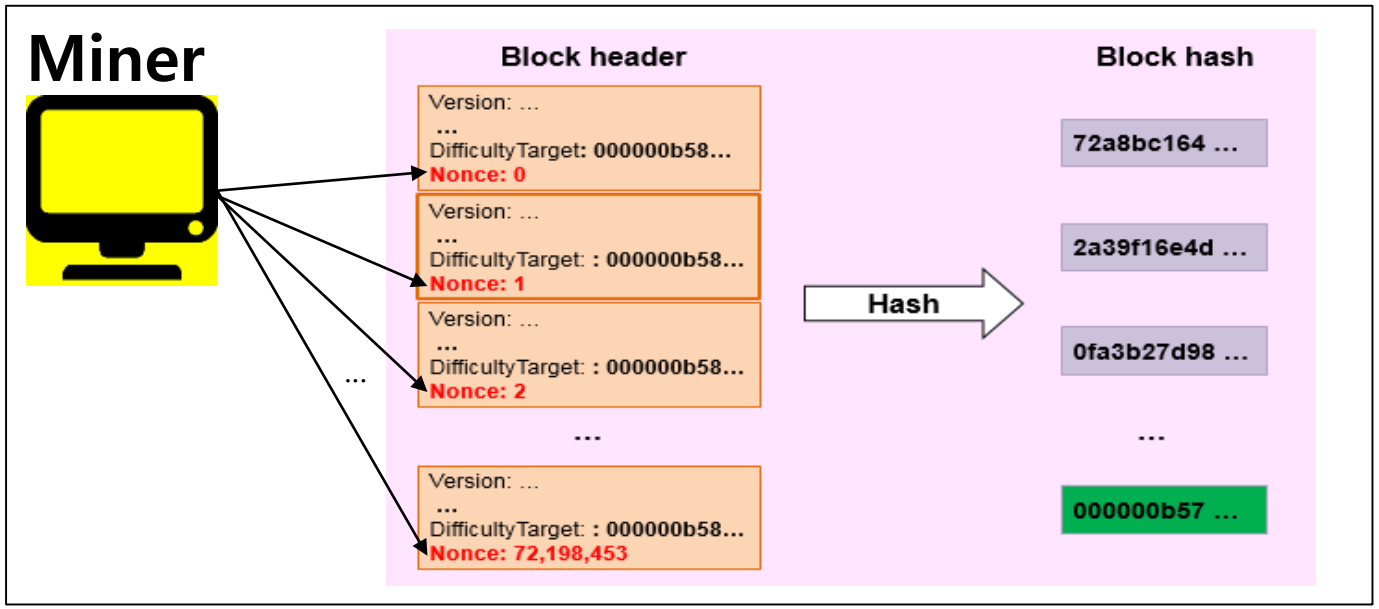


Overview of Mining Process (4/6)

4. PoW: Mine new block

- The Key is to **find the correct nonce**
  - Start nonce at zero and increase by one
  - Calculate hash value of the candidate block's header
  - Compare the hash value with DifficultyTarget

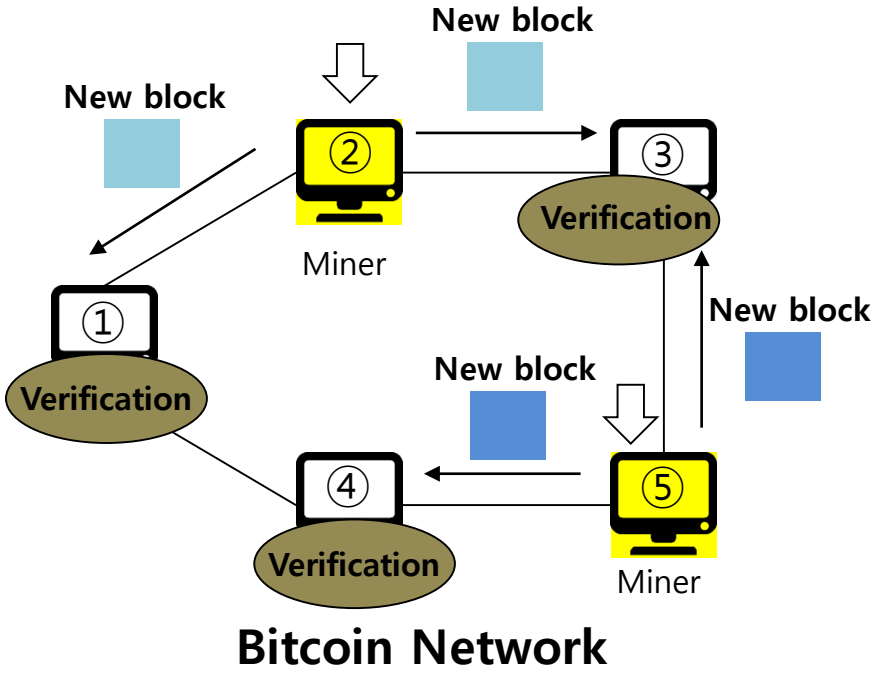


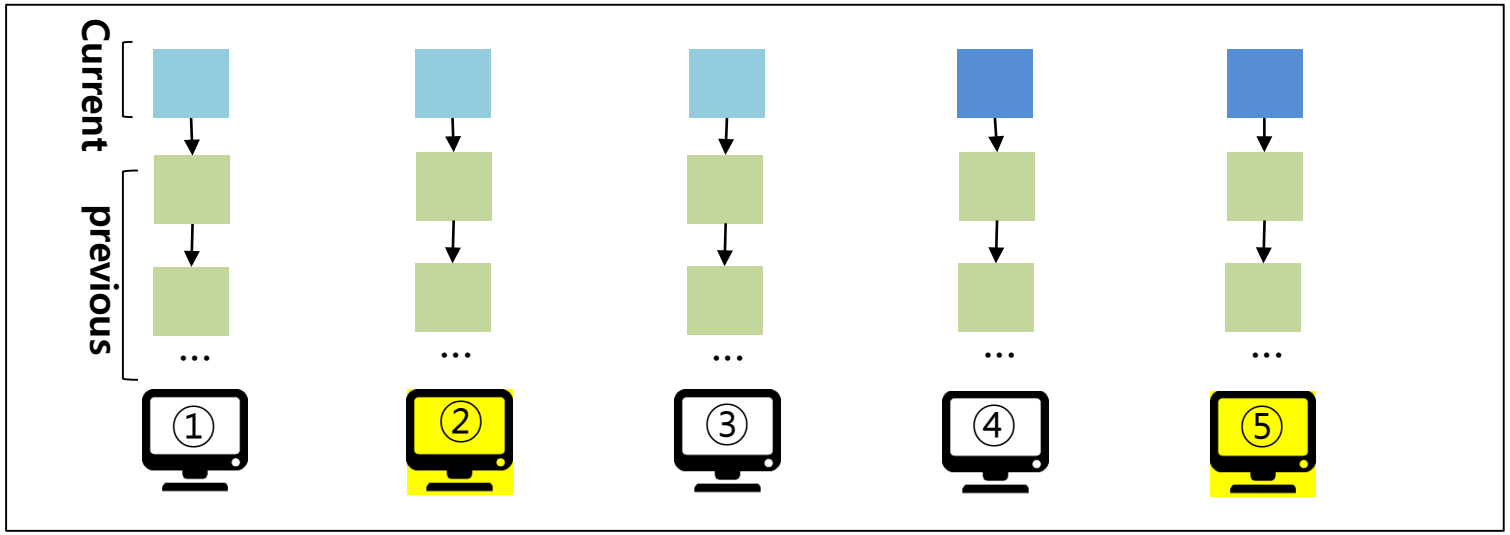


Overview of Mining Process (5/6)

5. PoW: Broadcast successfully mined block

- Broadcast new block to peer nodes
- New block is verified by every node receiving the block
- The result of broadcasting
  - This is the case that the two miners succeed in mining at the same time

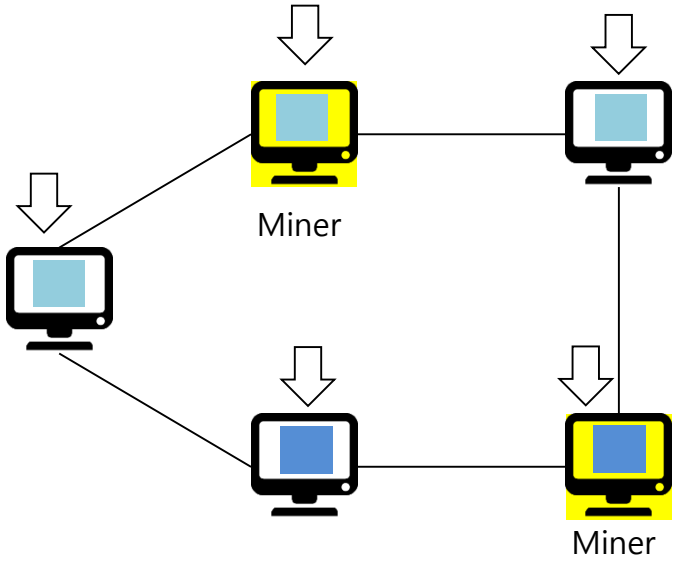




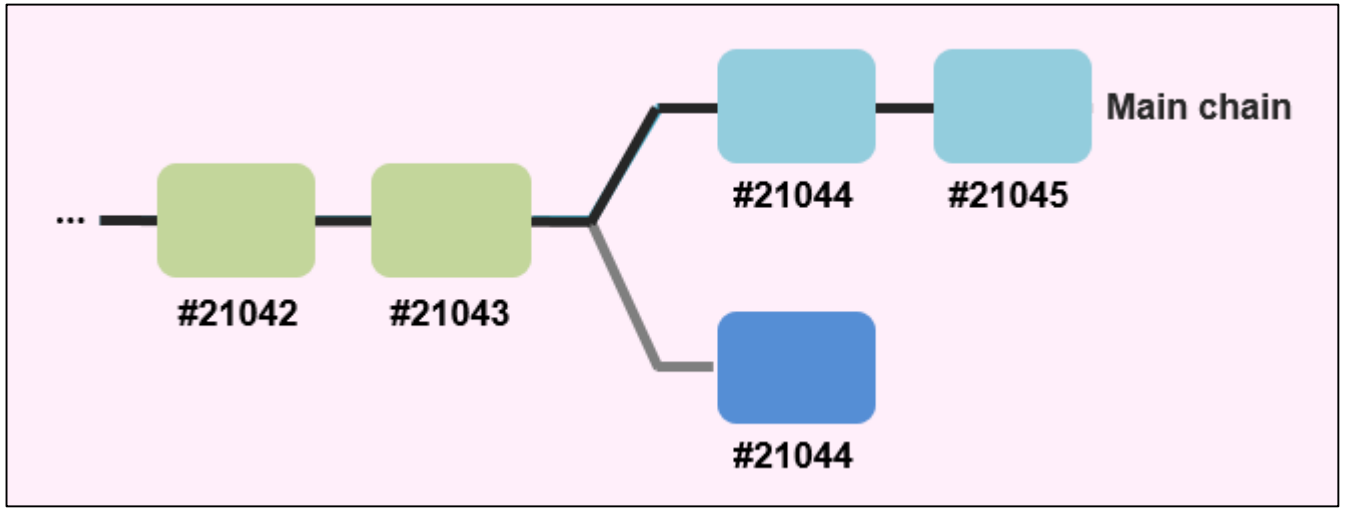
Overview of Mining Process (6/6)

6. Other Considerations

- Fork: Separates two chains
- Adjust DifficultyTarget
  - To maintain block generation time of 10 minutes



Bitcoin Network



Summary

- **Introduction to Mining & Consensus**
  - What is Mining?
  - Mining node & Mining pool
- **Overview of Mining Process**
  - Transaction Creation
  - Verification of the transaction
  - Prepare for mining new block
  - Mine new block
  - Broadcast successfully mined block

Reference

- Andreas M. Antonopoulos, **Mastering Bitcoin,** O'Reilly, 2014
- https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-transaction-block-chains
- https://en.wikipedia.org/wiki/Proof-of-work_system
- https://www.coursera.org/lecture/cryptocurrency/distributed-consensus-At1IC
- https://en.wikipedia.org/wiki/Mining_pool
- https://www.bitcoinmining.com/