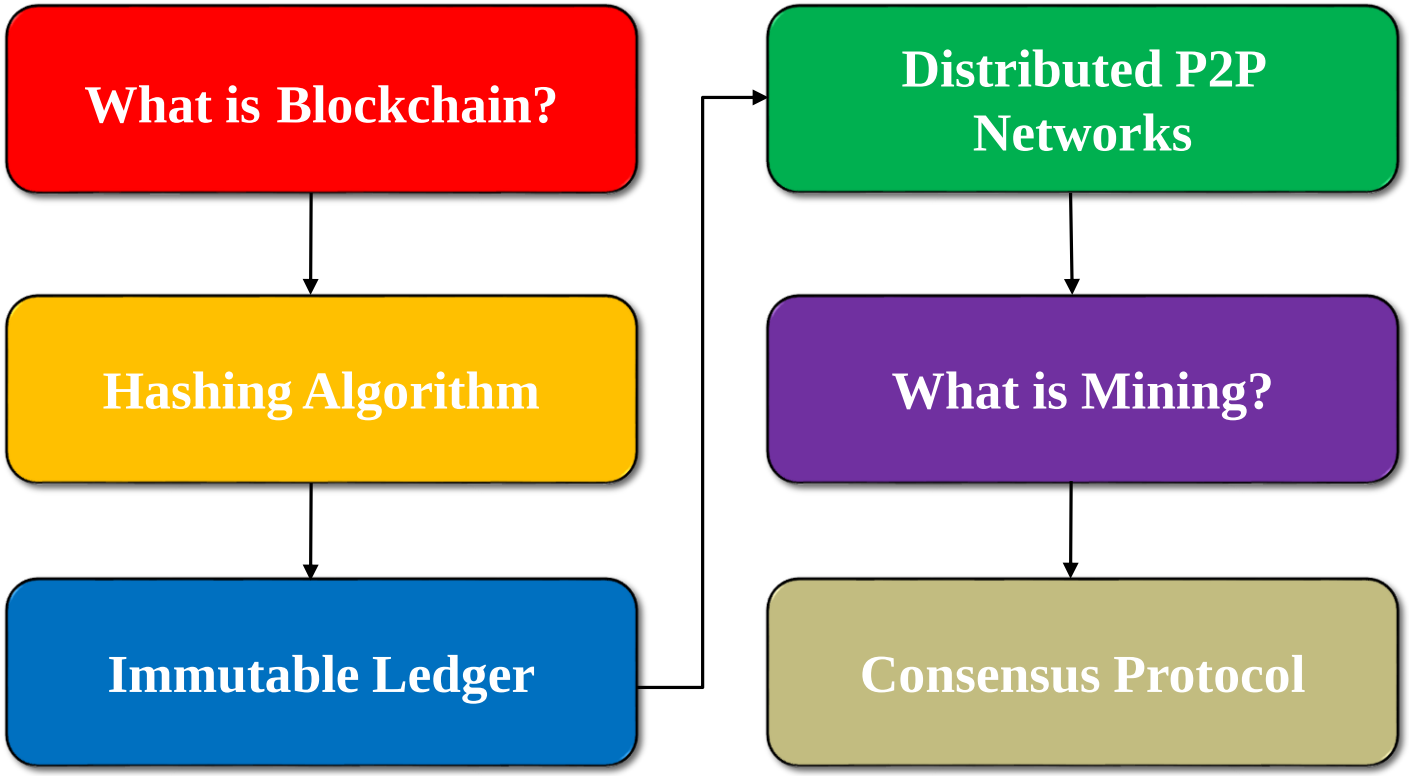
# Blockchain

Dr. Bahar Ali
Assistant Professor (CS), National University Of Computer and Emerging Sciences, Peshawar.

# Contents – Module A



# Blockchain Mining

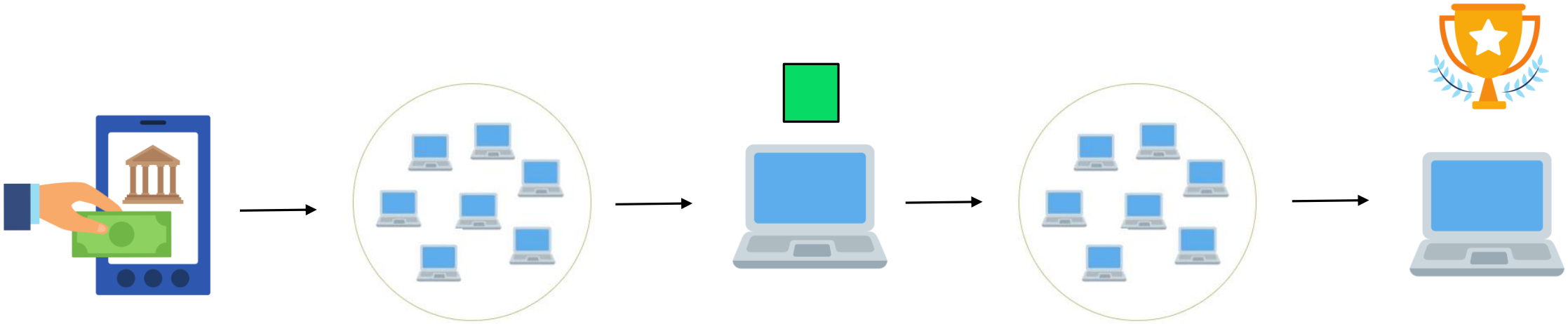
# Blockchain Mining

- When a transaction is done (Bitcoins are transferred)
- The transaction will be saved in a Mempool
- Miner or group of miners pick these transactions from a Mempool and add them to a block. Miners add as many transactions as possible
- Miners have to solve a mathematical problem called Proof of Work (PoW)
- A block is created for those miners, which solve the problem quickly

# Blockchain Mining

- Miners communicate across the network that the block is created
- Other will check if it is valid or not, so they will verify it
- If the block is valid then it will be added to a Blockchain
- The miners will be rewarded (will cover in details in the coming lectures)

# Blockchain Mining



Transaction

Solve Mathematical Problem

Miner Solved Problem First

Miners Verify the Validity

Block is added

# Blockchain Mining

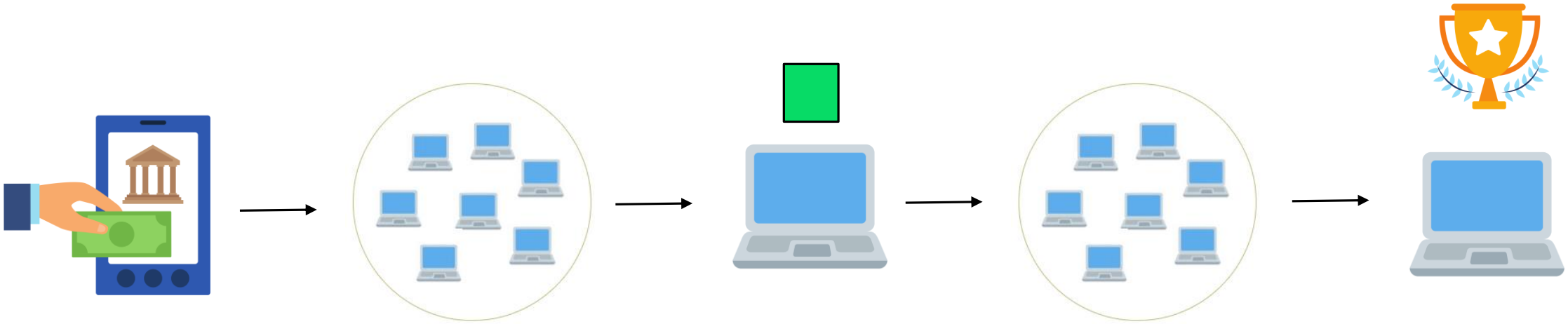
**Why Mining is important?**

- The main importance of mining is to secure the network
- There is not central authority, so this way transaction is verified
- Miners are rewarded for adding blocks to existing Blockchain

- So, through mining trust and security is created across the network
  - Trust
  - Security

# How Mining works: The Nonce

# Blockchain Mining



Transaction

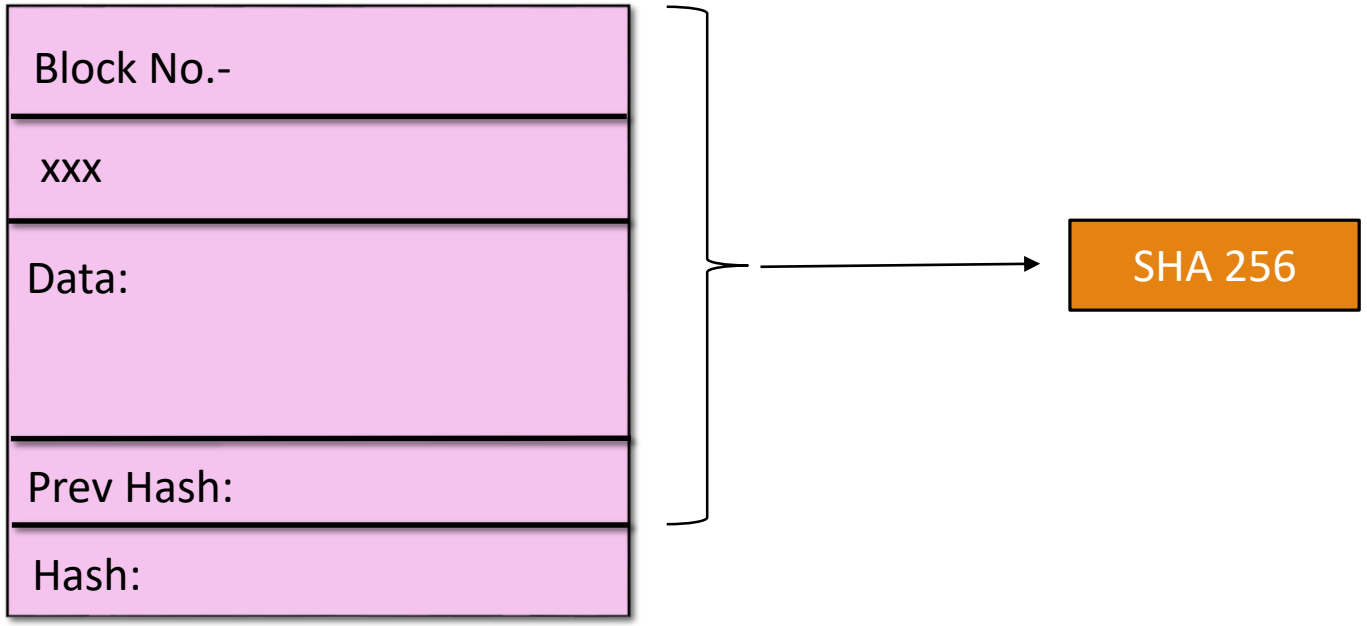
Solve Mathematical Problem

Miner Solved Problem First

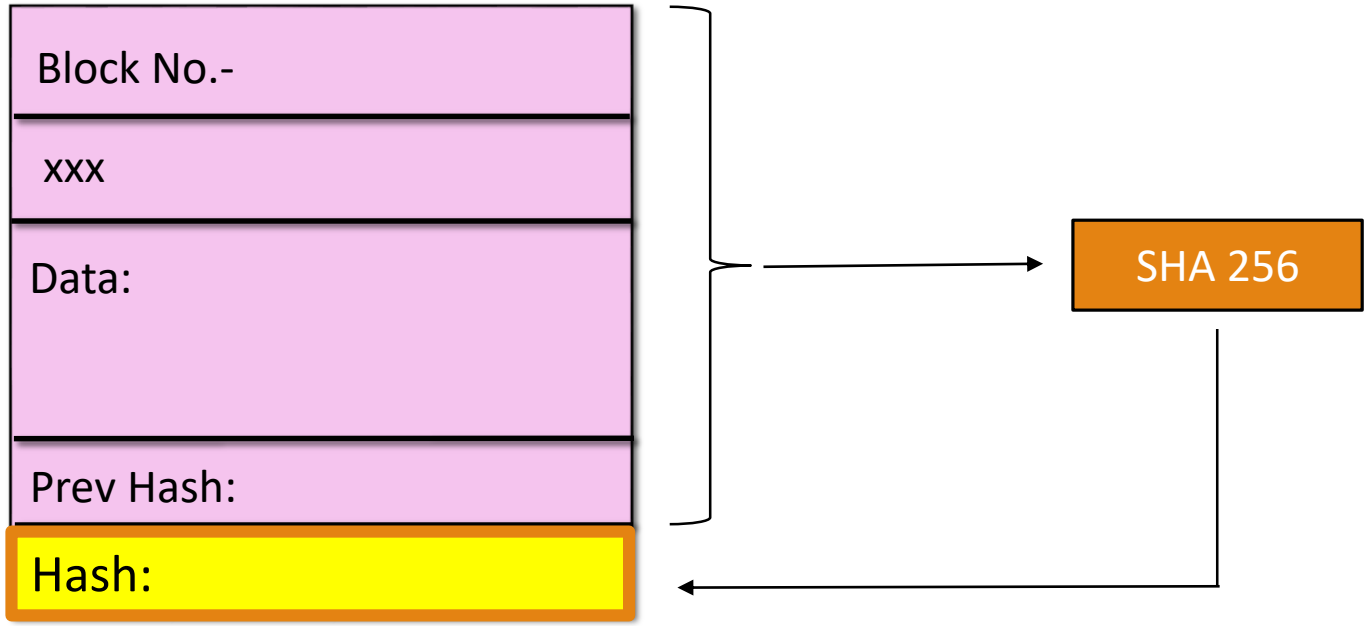
Miners Verify the Validity

Block is added

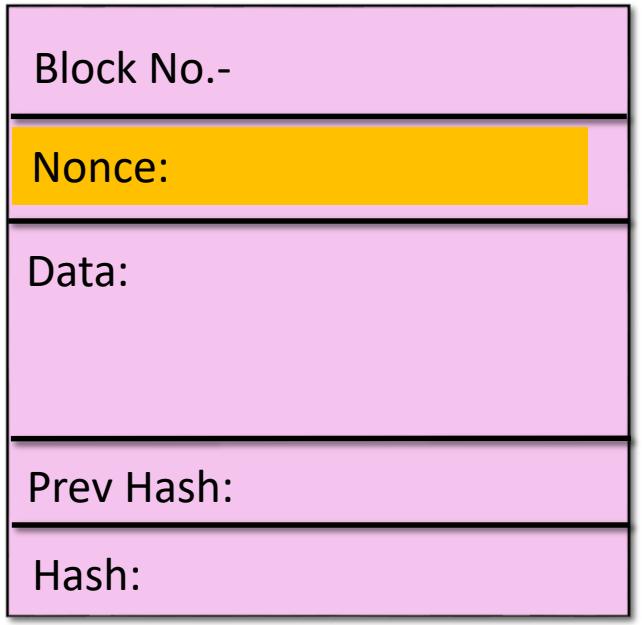
# The Nonce



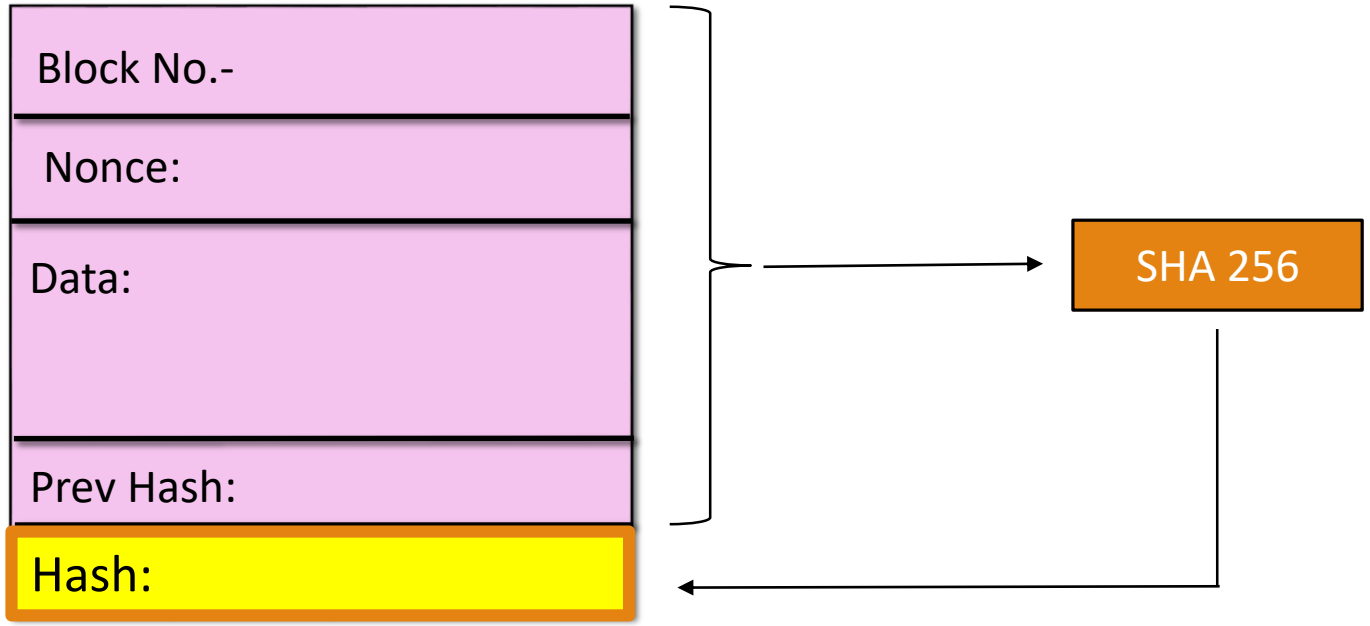
# The Nonce



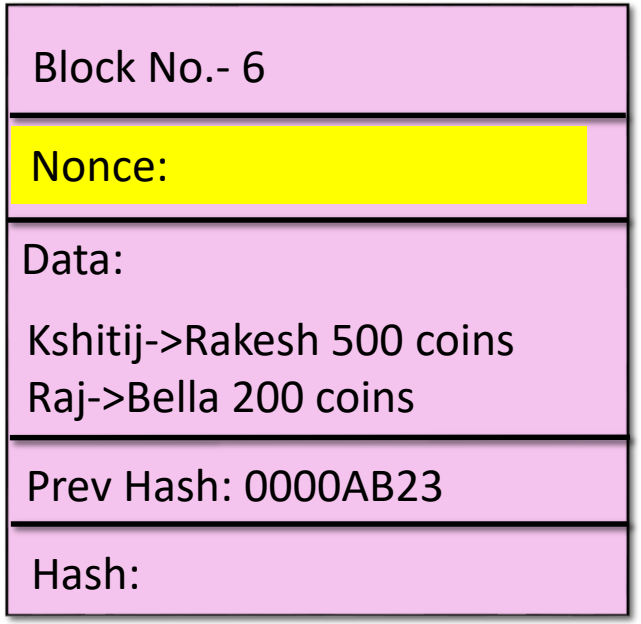
# The Nonce



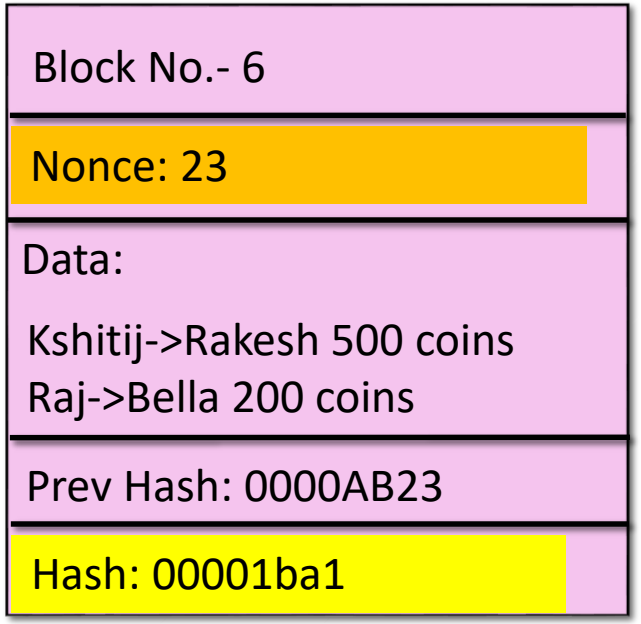
# The Nonce



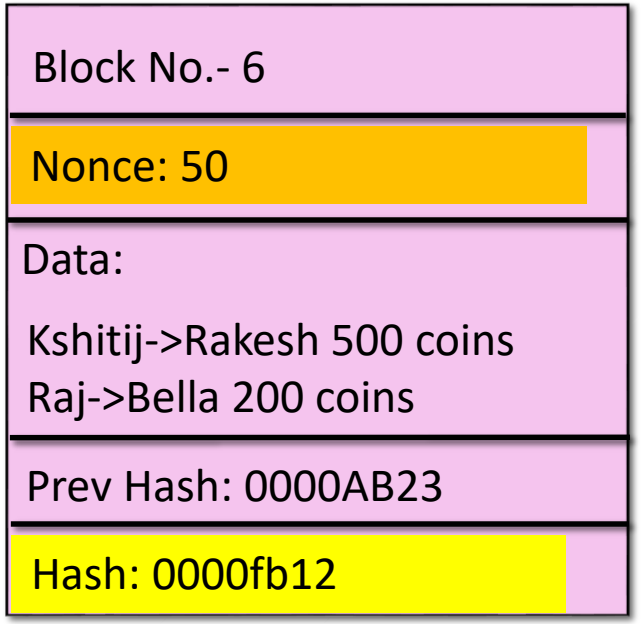
# The Nonce


Block No.- 6
Nonce:
Data:
Kshitij->Rakesh 500 coins
Raj->Bella 200 coins
Prev Hash: 0000AB23
Hash:

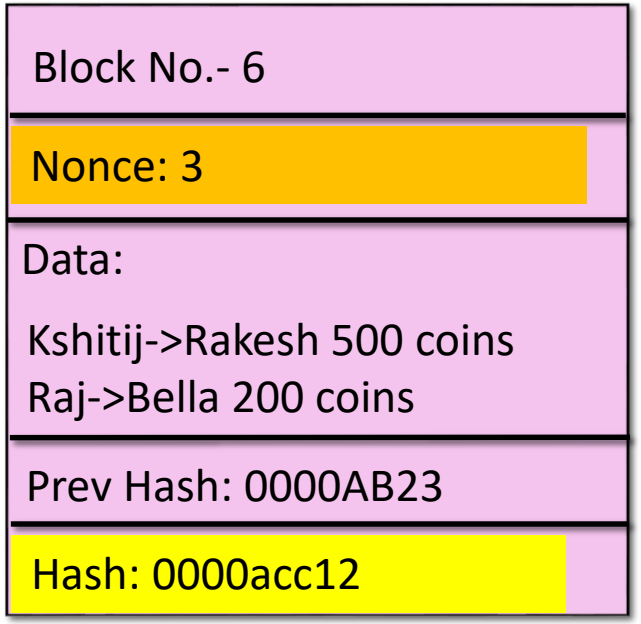
# The Nonce


Block No.- 6
Nonce: 23
Data:
Kshitij->Rakesh 500 coins
Raj->Bella 200 coins
Prev Hash: 0000AB23
Hash: 00001ba1

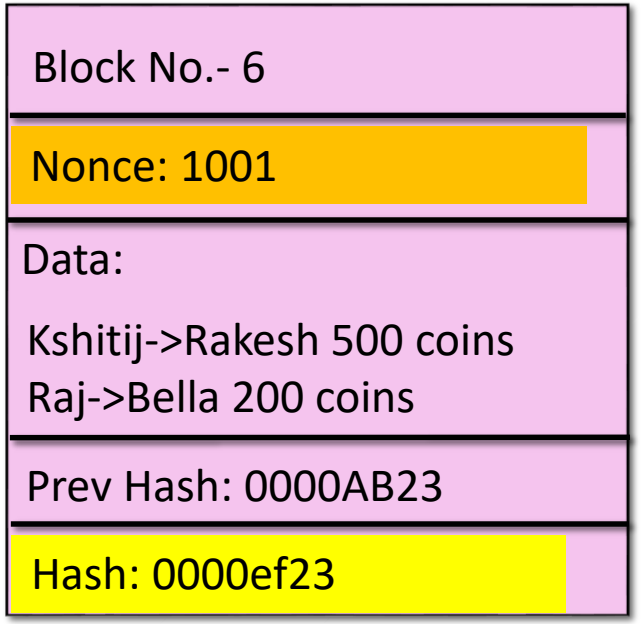
# The Nonce


Block No.- 6
Nonce: 50
Data:
Kshitij->Rakesh 500 coins
Raj->Bella 200 coins
Prev Hash: 0000AB23
Hash: 0000fb12

# The Nonce


Block No.- 6
Nonce: 3
Data:
Kshitij->Rakesh 500 coins
Raj->Bella 200 coins
Prev Hash: 0000AB23
Hash: 0000acc12

# The Nonce


Block No.- 6
Nonce: 1001
Data:
Kshitij->Rakesh 500 coins
Raj->Bella 200 coins
Prev Hash: 0000AB23
Hash: 0000ef23

# Hashing Algorithm Demo

**Online demonstration (Nonse)**

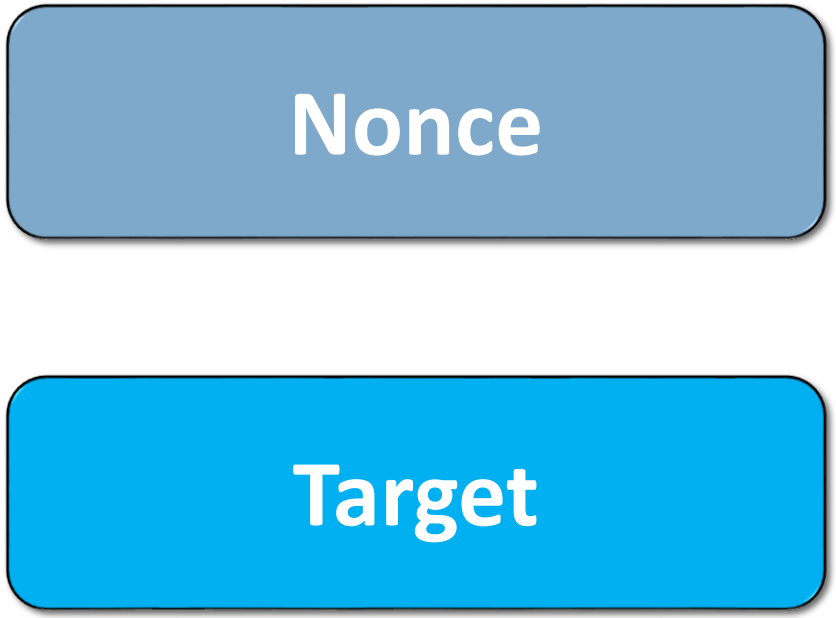
https://andersbrownworth.com/blockchain/

**Running your Node Server**

https://github.com/anders94/blockchain-demo/

# How Mining works: The Nonce

# How Mining Works ?



# How Mining Works ?

## Nonce:

- The nonce is the number that Blockchain miners are solving for.

# How Mining Works ?

## Target

- Target is a number used in mining.
- It is a number that a block hash must be below for the block to be added on to the Blockchain.
- The target adjusts every 2016 blocks (roughly two weeks) to try and ensure that blocks are mined **once every 10 minutes** on average.

# How Mining Works ?

Hexadecimal Numbers

| Decimal | Hexadecimal |
|---|---|
| 0 | 0 |
| 1 | 1 |
| 2 | 2 |
| 3 | 3 |
| 4 | 4 |
| 5 | 5 |
| 6 | 6 |
| 7 | 7 |
| 8 | 8 |
| 9 | 9 |
| 10 | A |

| Decimal | Hexadecimal |
|---|---|
| 11 | B |
| 12 | C |
| 13 | D |
| 14 | E |
| 15 | F |

# How Mining Works ?

- d2fd3930d274b202fe8e7cb431e38a8b64ec396e15f5717e60493234b0de210a
- 52d095795c1dc87ff2f6b4d9b005a1fe2cfed01103763c9443f6d4496df8e800
- 0000005432d9f64f6e05c019f9302162100163b6cdba06bd72eee35cd19aebf

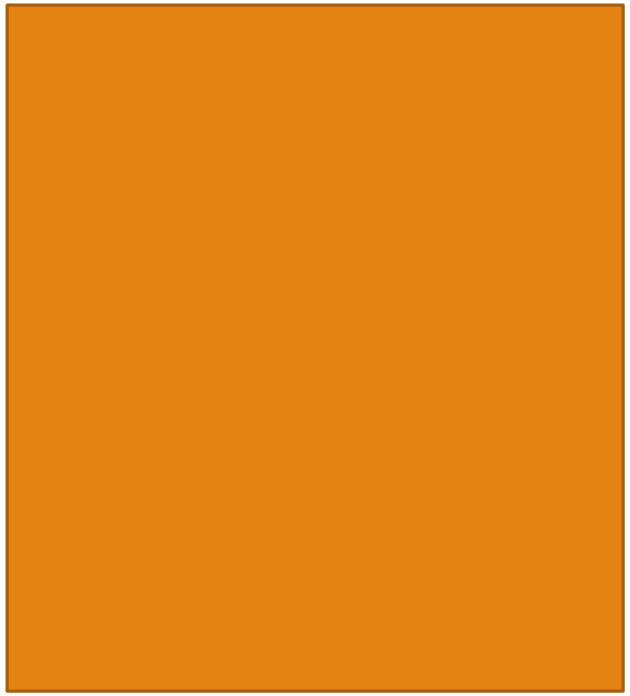
**Smallest**- 0000000.....0

**Largest**- fffffffffffff.....f

# How Mining Works ?

| Block No.-6 |
| --- |
| Nonce: |
| Data:<br>Kshitij->Rakesh 500 coins<br>Raj->Bella 200 coins |
| Prev Hash: 0000AB23 |
| Hash: |

All Possible Hashes



# How Mining Works ?

Block No.-6

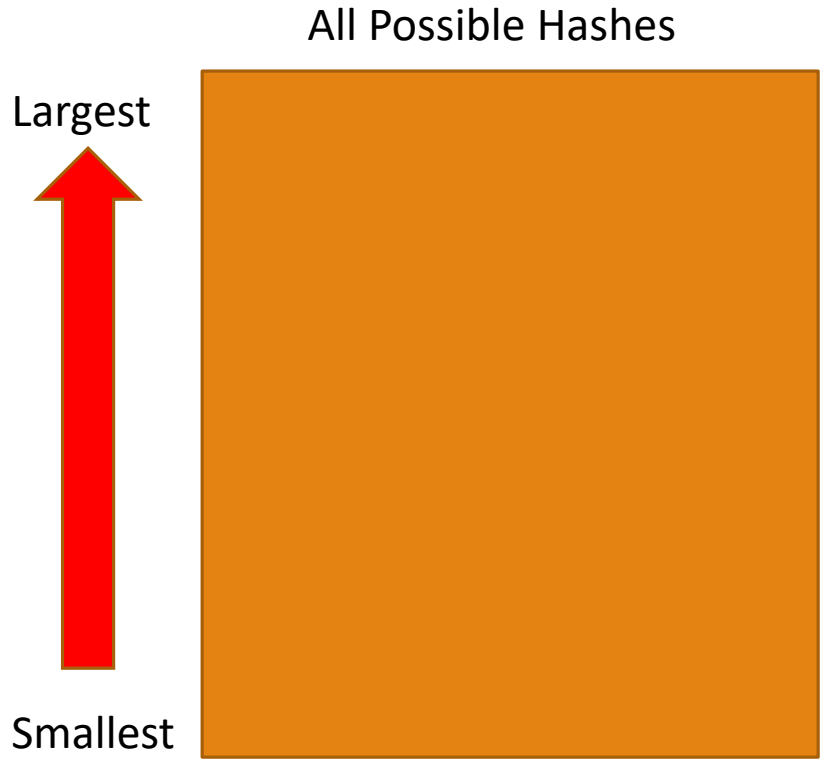
Nonce:

Data:

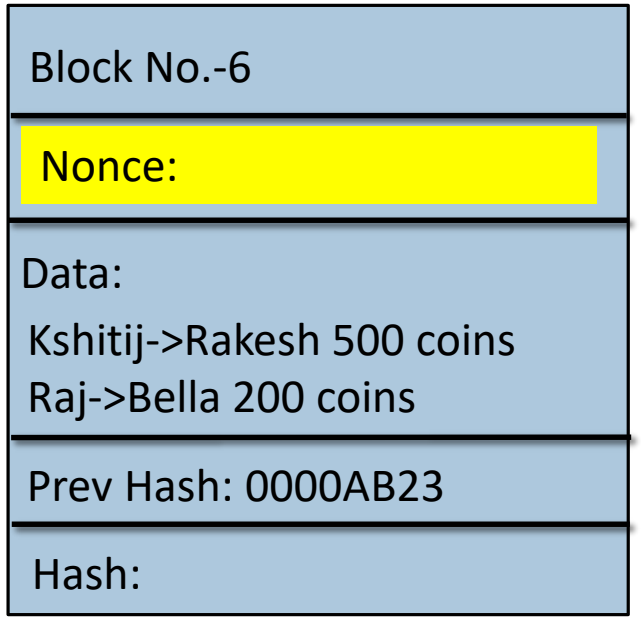
Kshitij->Rakesh 500 coins
Raj->Bella 200 coins

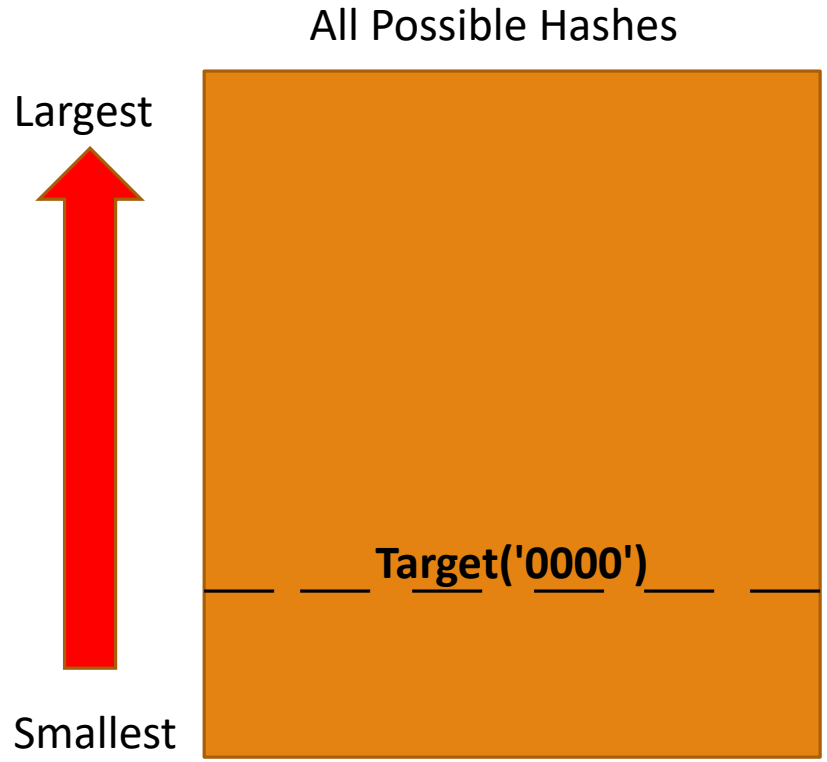
Prev Hash: 0000AB23

Hash:

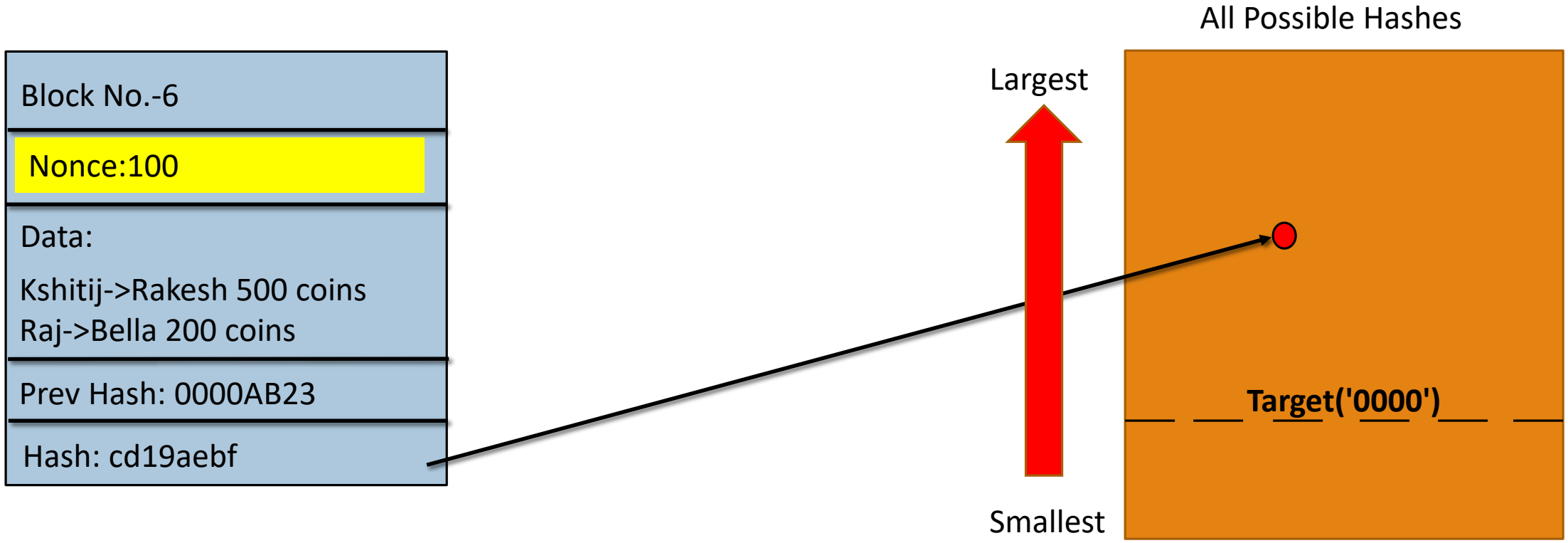


# How Mining Works ?

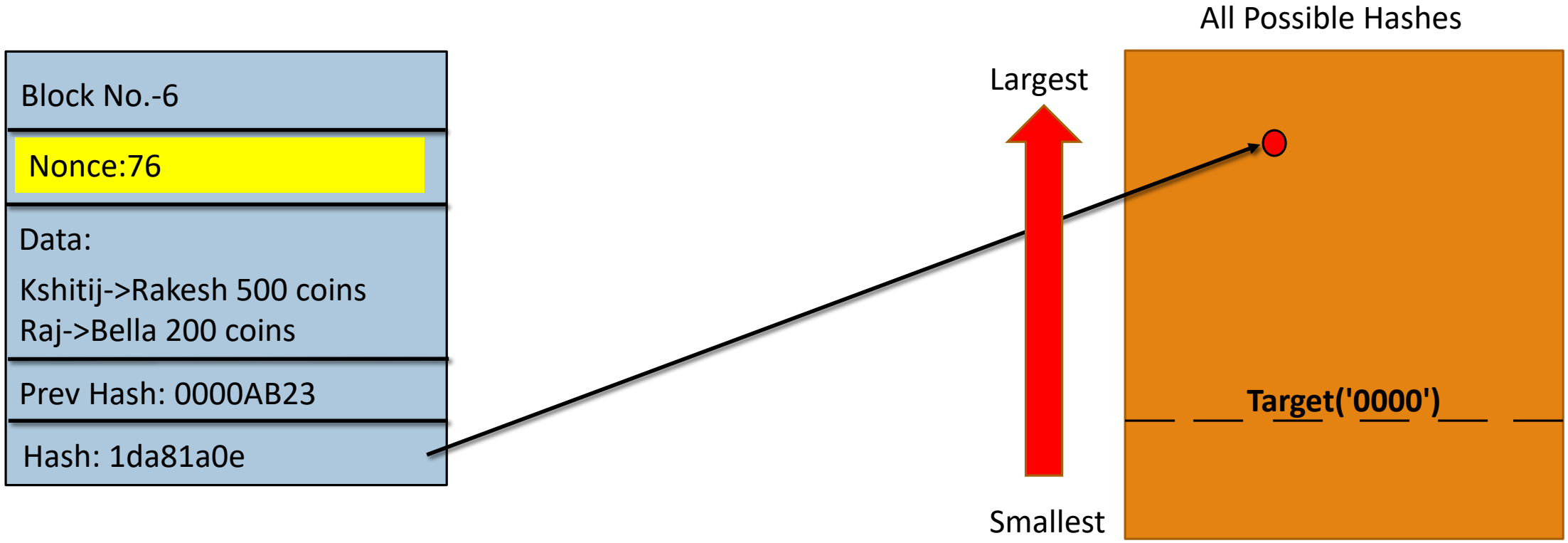


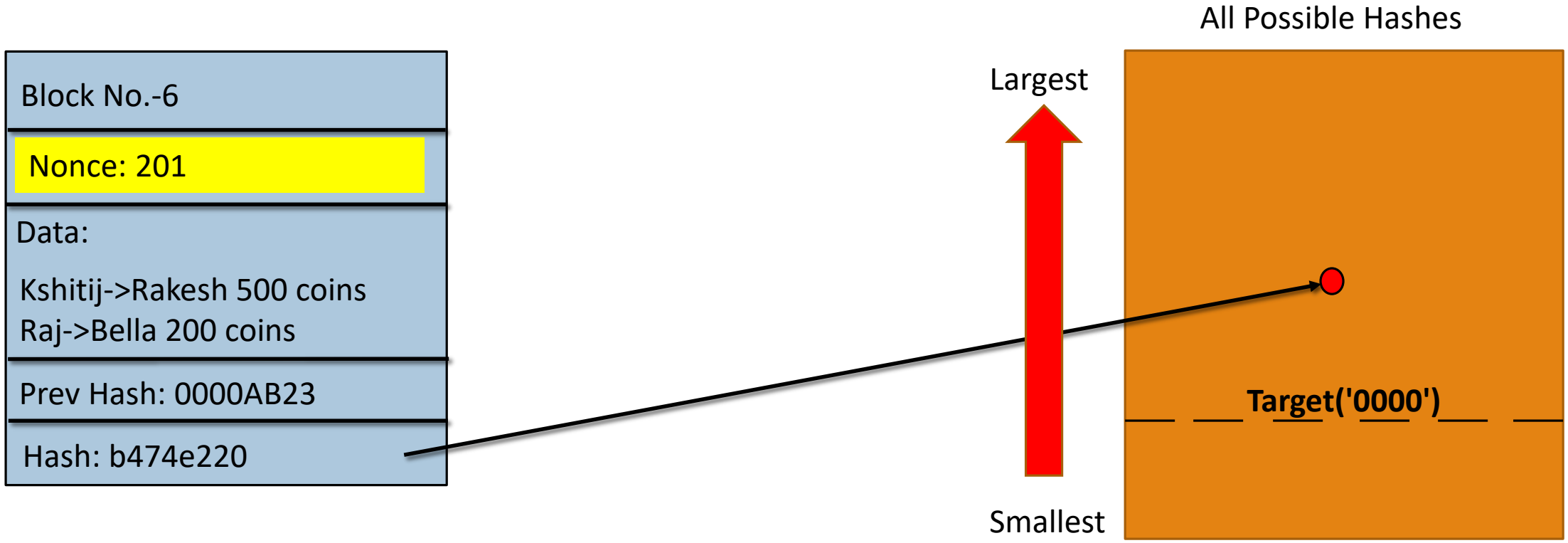
# How Mining Works ?



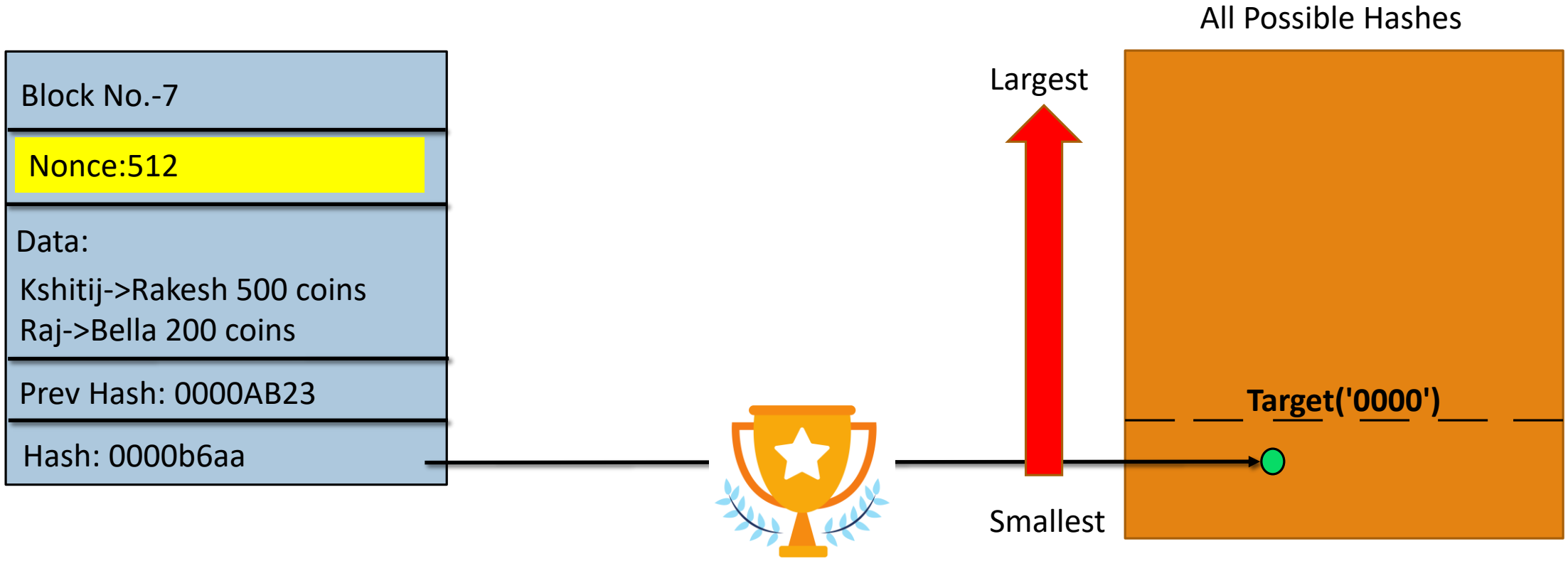
# How Mining Works ?



# How Mining Works ?



# How Mining Works ?



# Is Mining that easy?

# Challenges faced by Miners

Time Taking

Electricity Bills

Mathematical problem solving skill

Start All Over Again Attitude

Fast Computers