SWINBURNE UNIVERSITY OF TECHNOLOGY

Theory of Blockchain

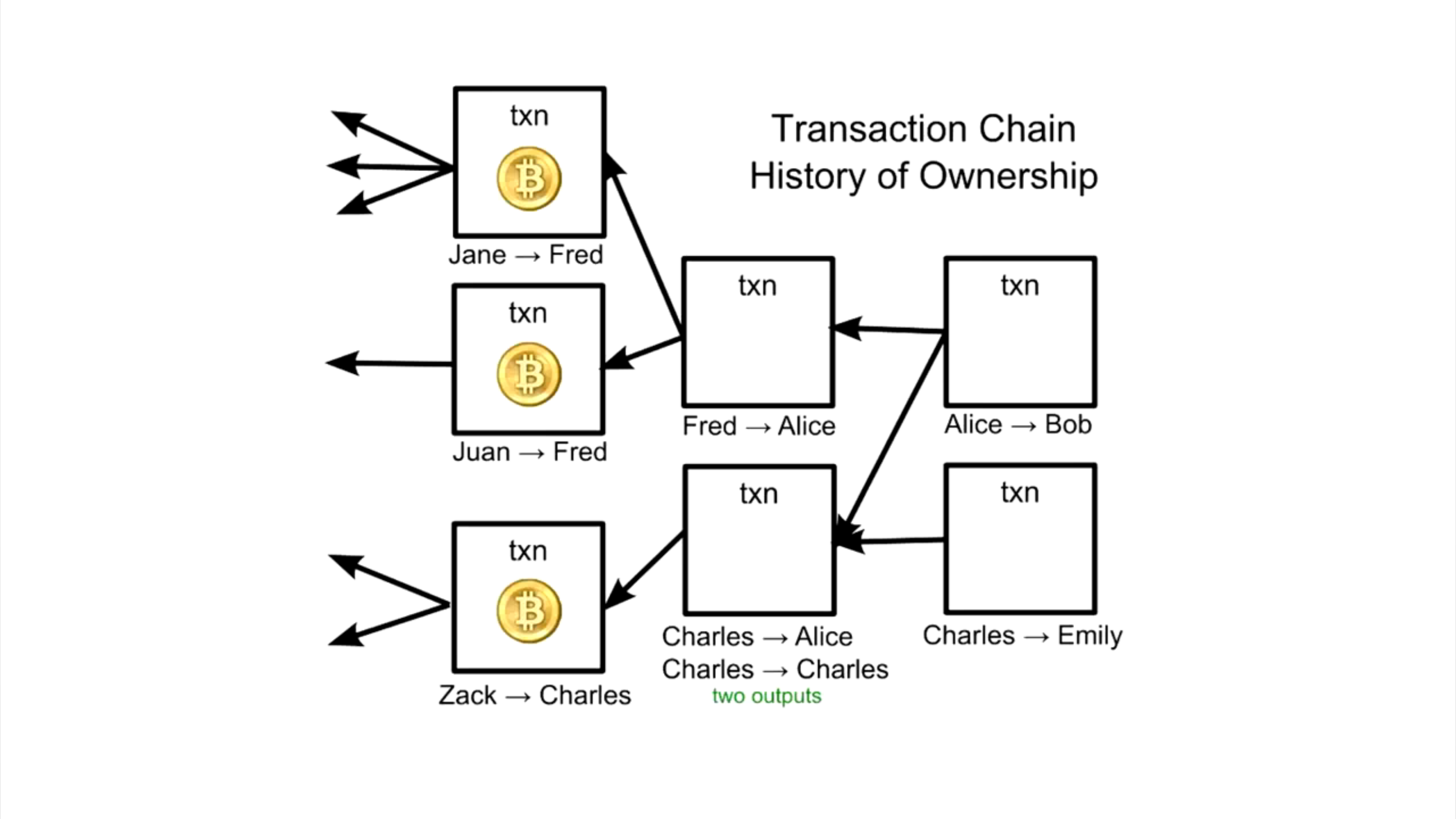
Session 6:

Bitcoin – Part 1

Module 1 - Block Generation, Mining, and Difficulty Adjustment

Sayad Haghighi

A Reminder ….

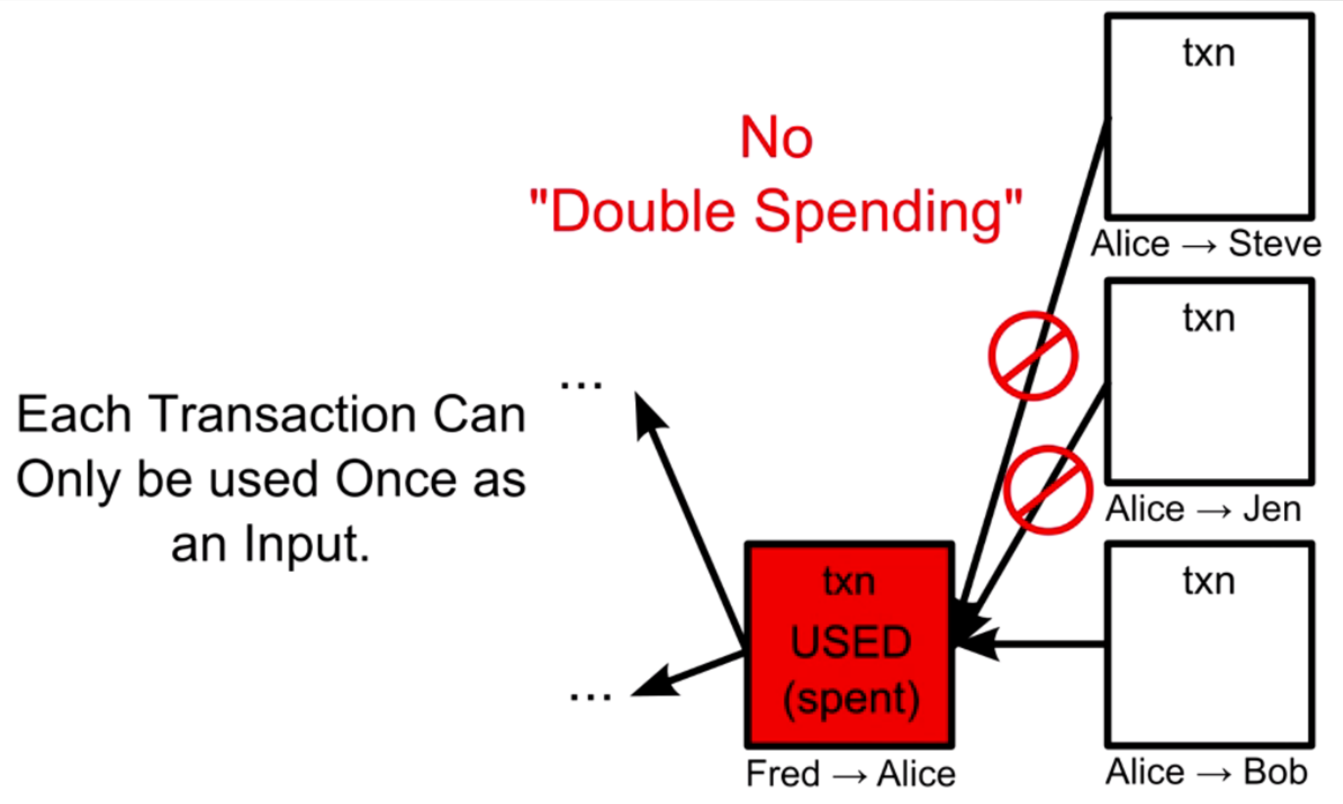


(How Bitcoin Works Under the Hood, Youtube)

Money Flow

When you first install the bitcoin client, it downloads all the previous transactions (from other nodes) and then verifies each along the tree, one by one up to the first transaction (which was from Satoshi to Hal Finney).

But how to prevent double spending?

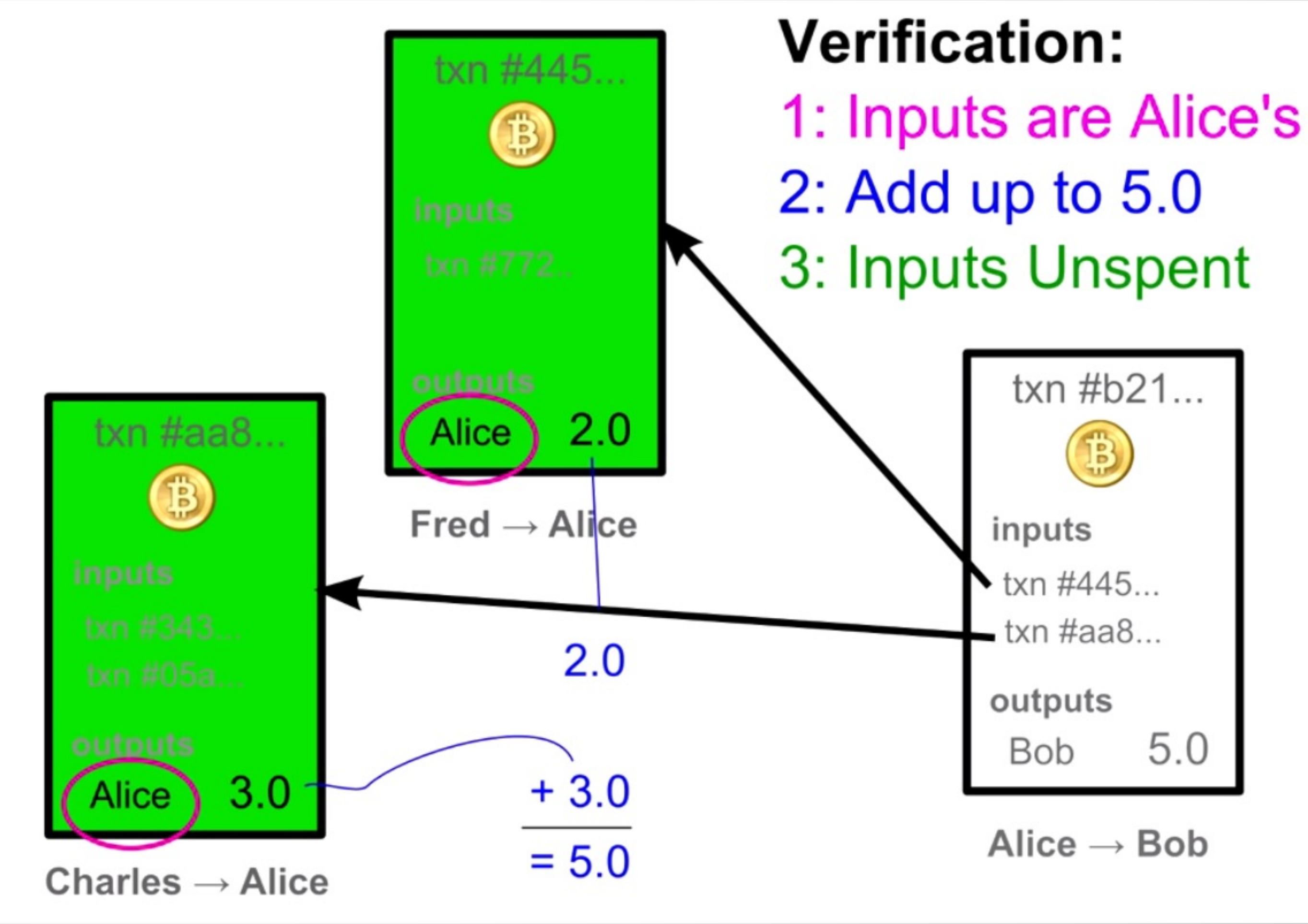


(How Bitcoin Works Under the Hood, Youtube)

Checking for double spending

You have to go through every previous transaction to make sure the inputs have not been spent somewhere else.

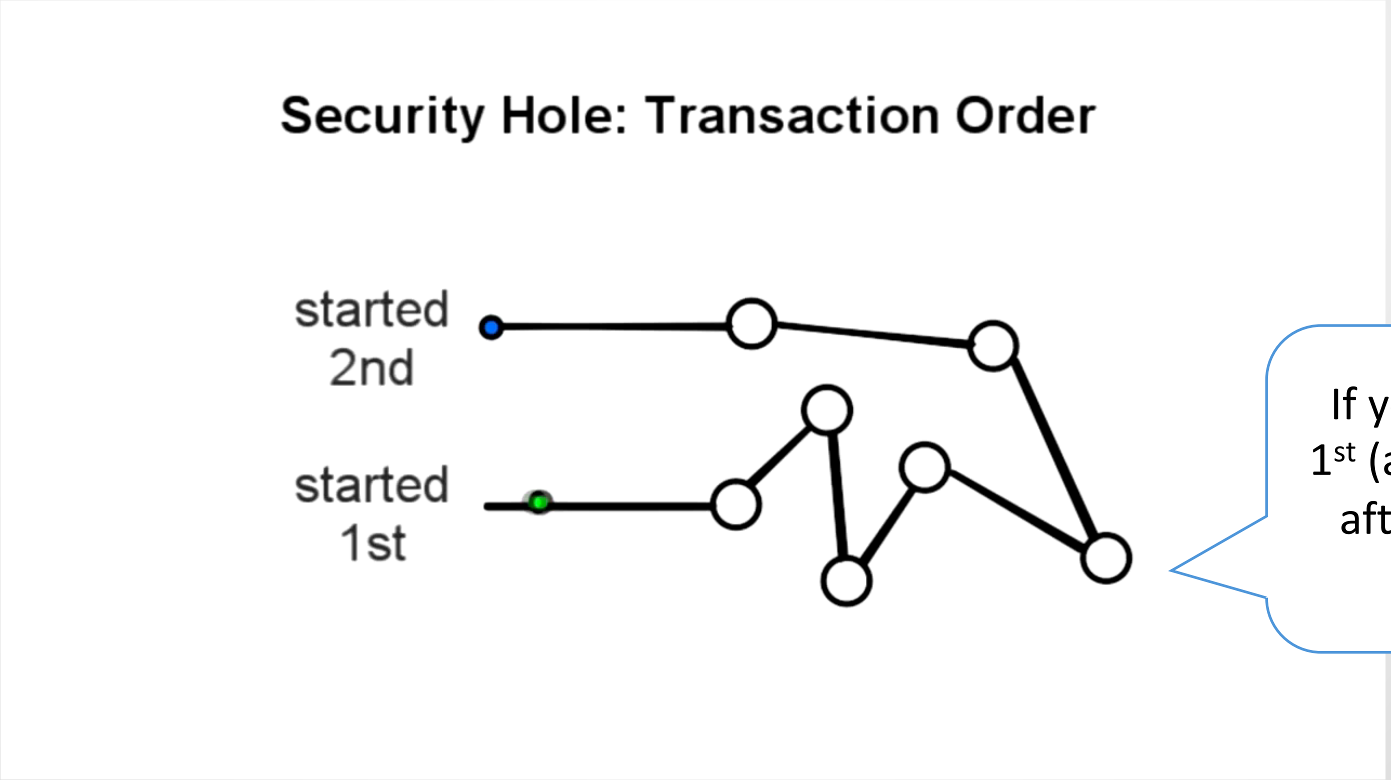
- It can be speeded up by indexing



(How Bitcoin Works Under the Hood, Youtube)

A Security Hole

Due to the network topology, a money can be spent twice and the second transaction is accepted first! Therefore, the 1st transaction (which was the real one) is deemed fraudulent and double spending.

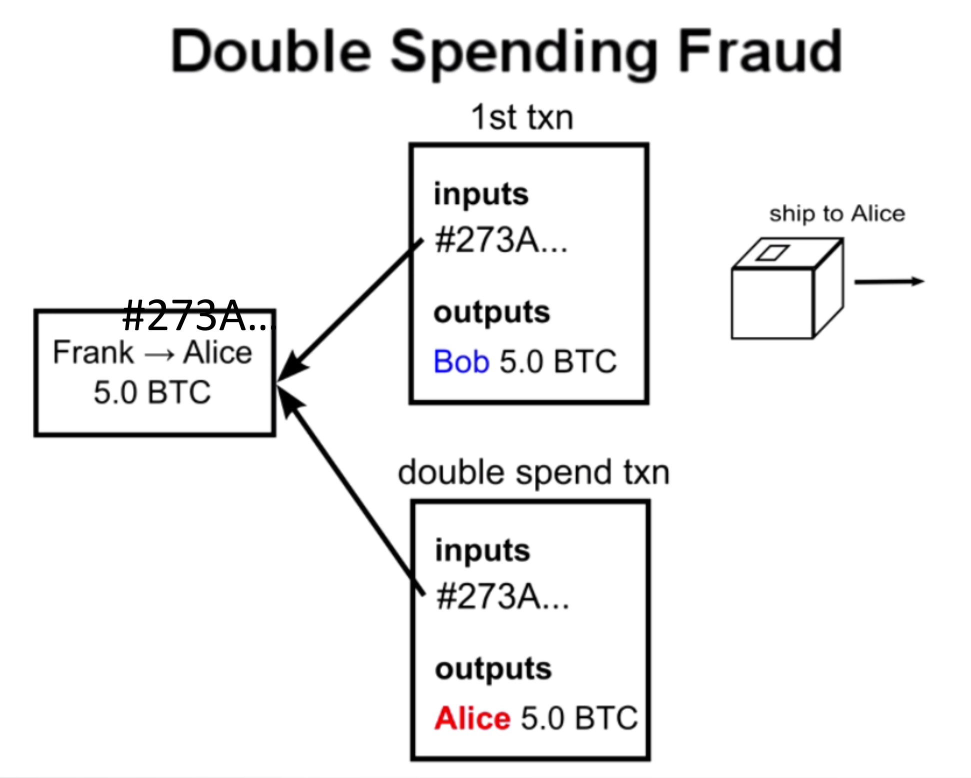


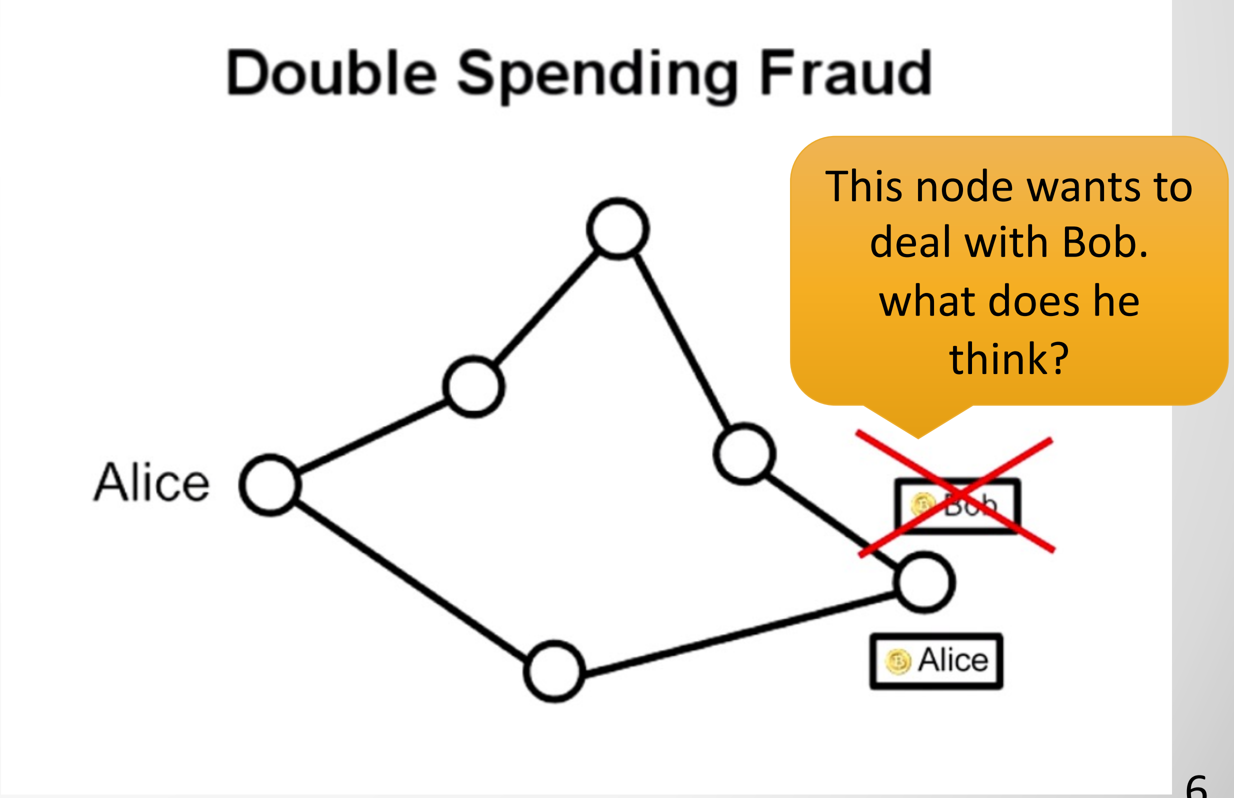
If you're here, you receive the 1st (actual) spending transaction after the second (fraudulent) one.

(How Bitcoin Works Under the Hood, Youtube)

Example of Double Spending Fraud Scenario

- Alice buys a product from Bob. Right after he ships the item, Alice makes another transaction and gives herself the money.





This node wants to deal with Bob. what does he think?

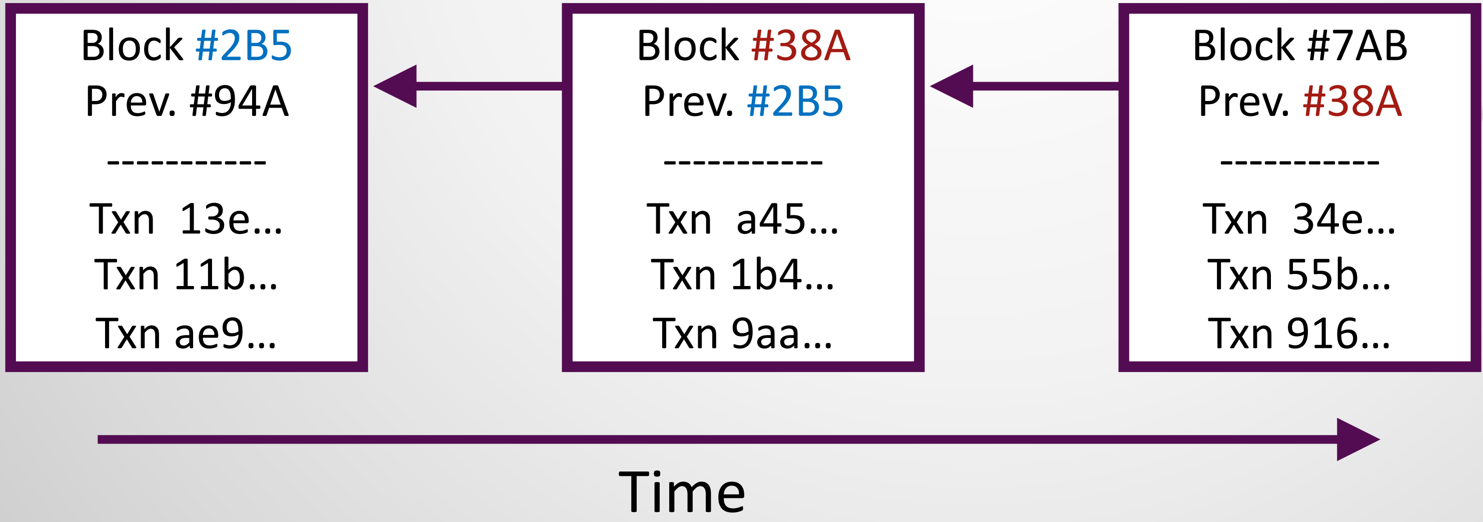
(How Bitcoin Works Under the Hood, Youtube)

Block Chain: a way to find the right transaction order

Overall, there will be disagreements over the network whether Alice or Bob owns the money and there’s no way to prove it.

➔ We should find a way to figure out the correct transaction order.

That was how **block chain** was invented.



Block #2B5
Prev. #94A

Txn 13e…
Txn 11b…
Txn ae9…

Block #38A
Prev. #2B5

Txn a45…
Txn 1b4…
Txn 9aa…

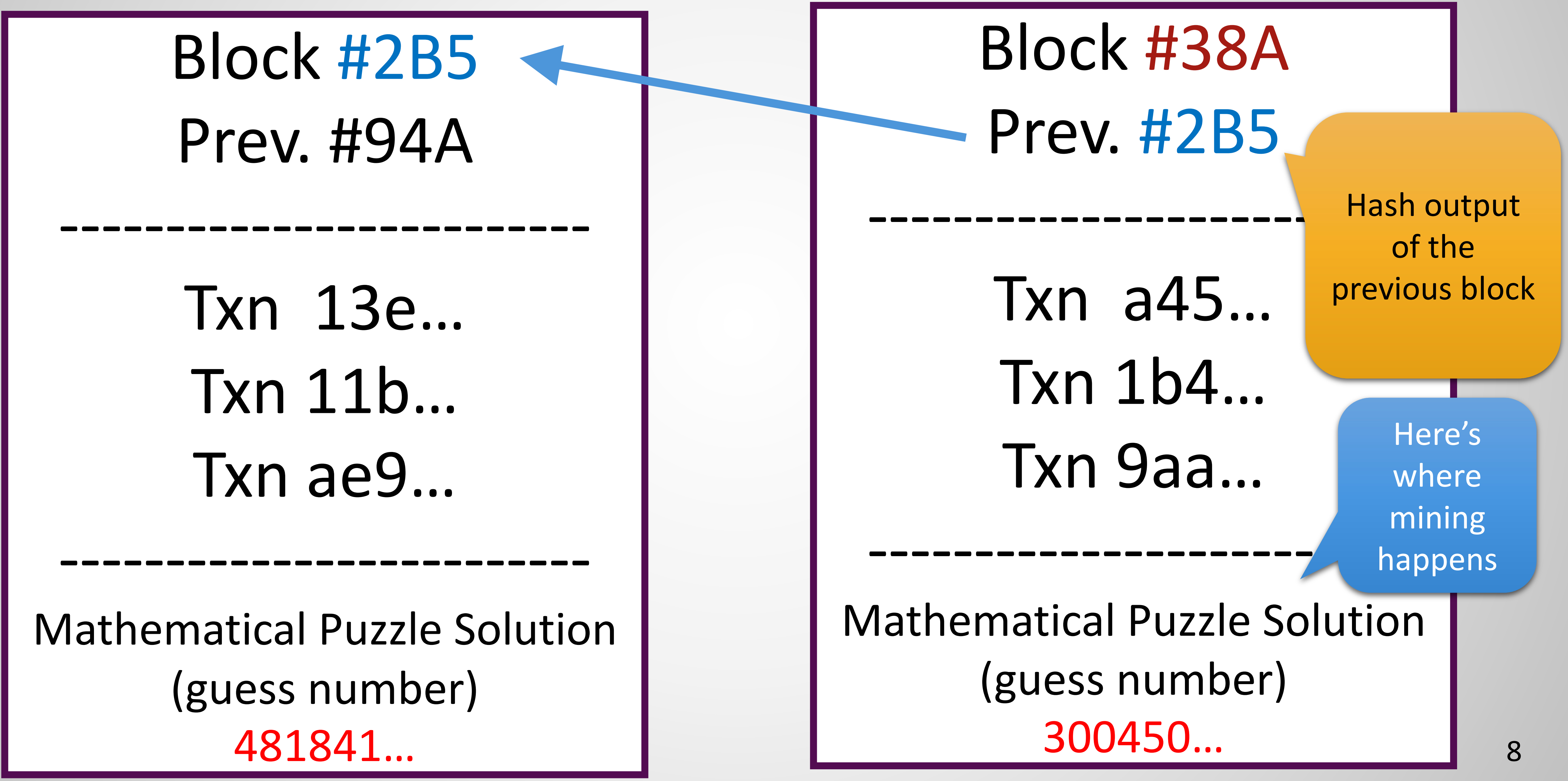
Block #7AB
Prev. #38A

Txn 34e…
Txn 55b…
Txn 916…

Time

Each block is a set of transactions plus a reference to chain it to the previous block.

Hash outputs are the Block IDs



Block #2B5

Prev. #94A

Txn 13e…

Txn 11b…

Txn ae9…

Mathematical Puzzle Solution (guess number)

481841…

Block #38A

Prev. #2B5

Txn a45…

Txn 1b4…

Txn 9aa…

Mathematical Puzzle Solution (guess number)

300450…

Hash output of the previous block

Here's where mining happens

How to make a block?

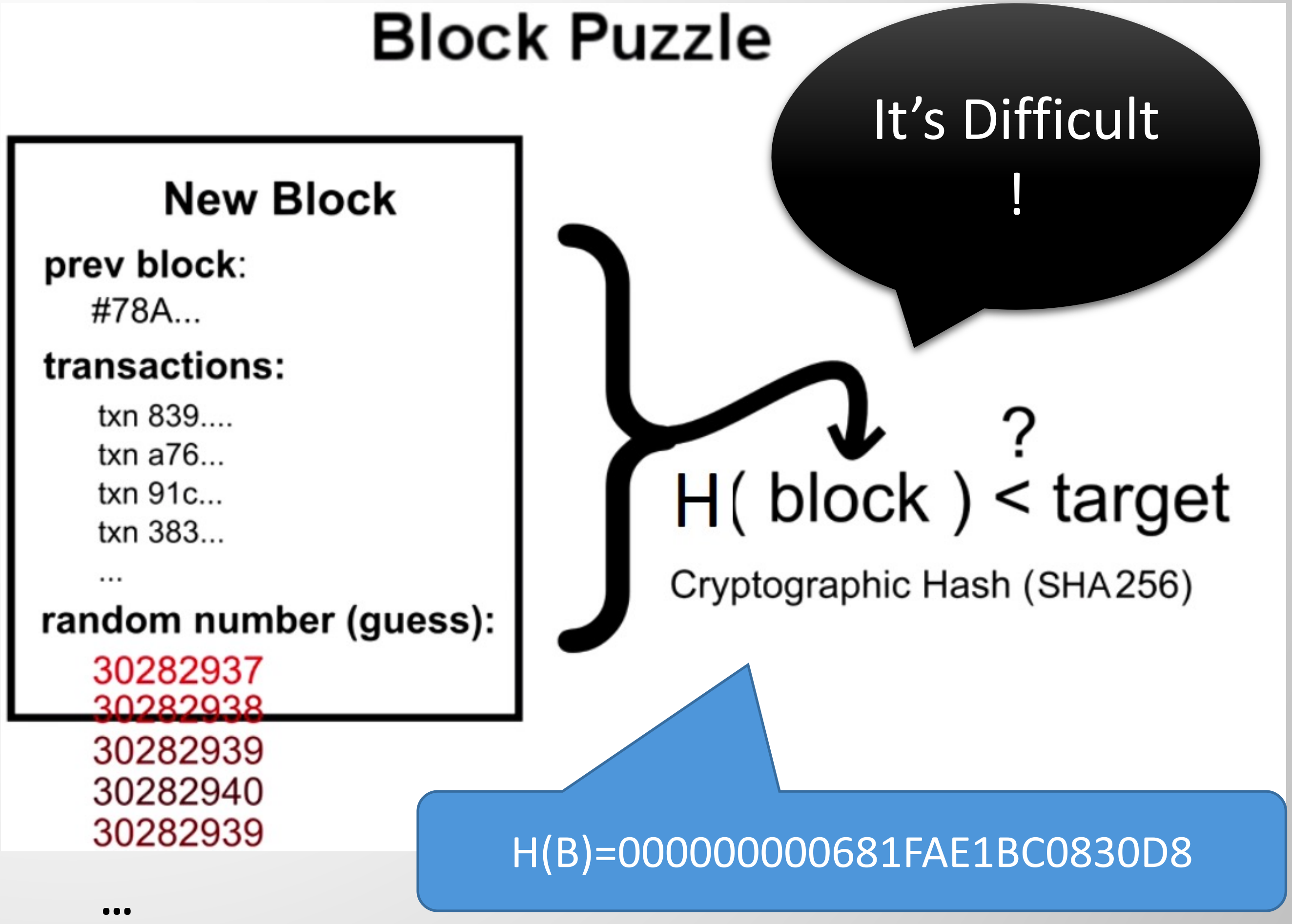
A block is made of a set of transactions happened in the same time slot (around 10 mins).

- Any node can pick a few unconfirmed transactions and create a block. By creating the block, it makes the transactions permanent (along his branch).
- To make a block, the node must solve a mathematical problem.

(How Bitcoin Works Under the Hood, Youtube)

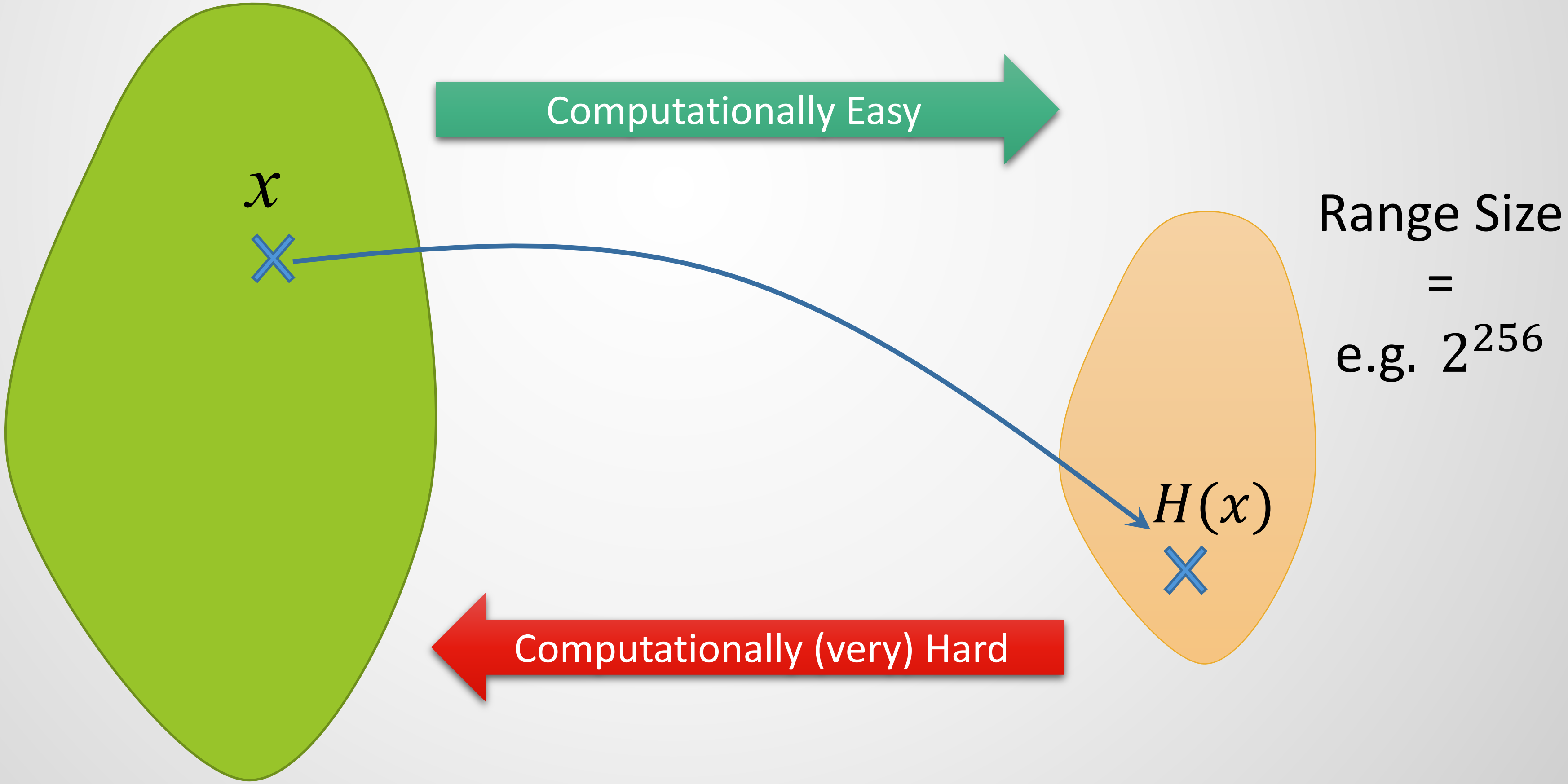
How to make a block?

To make a block, in addition to the transactions and a link to the previous block, one has to add a nonce in a way that the hash of the block has a specified number of 0's at the beginning. This means being smaller than the difficulty threshold.



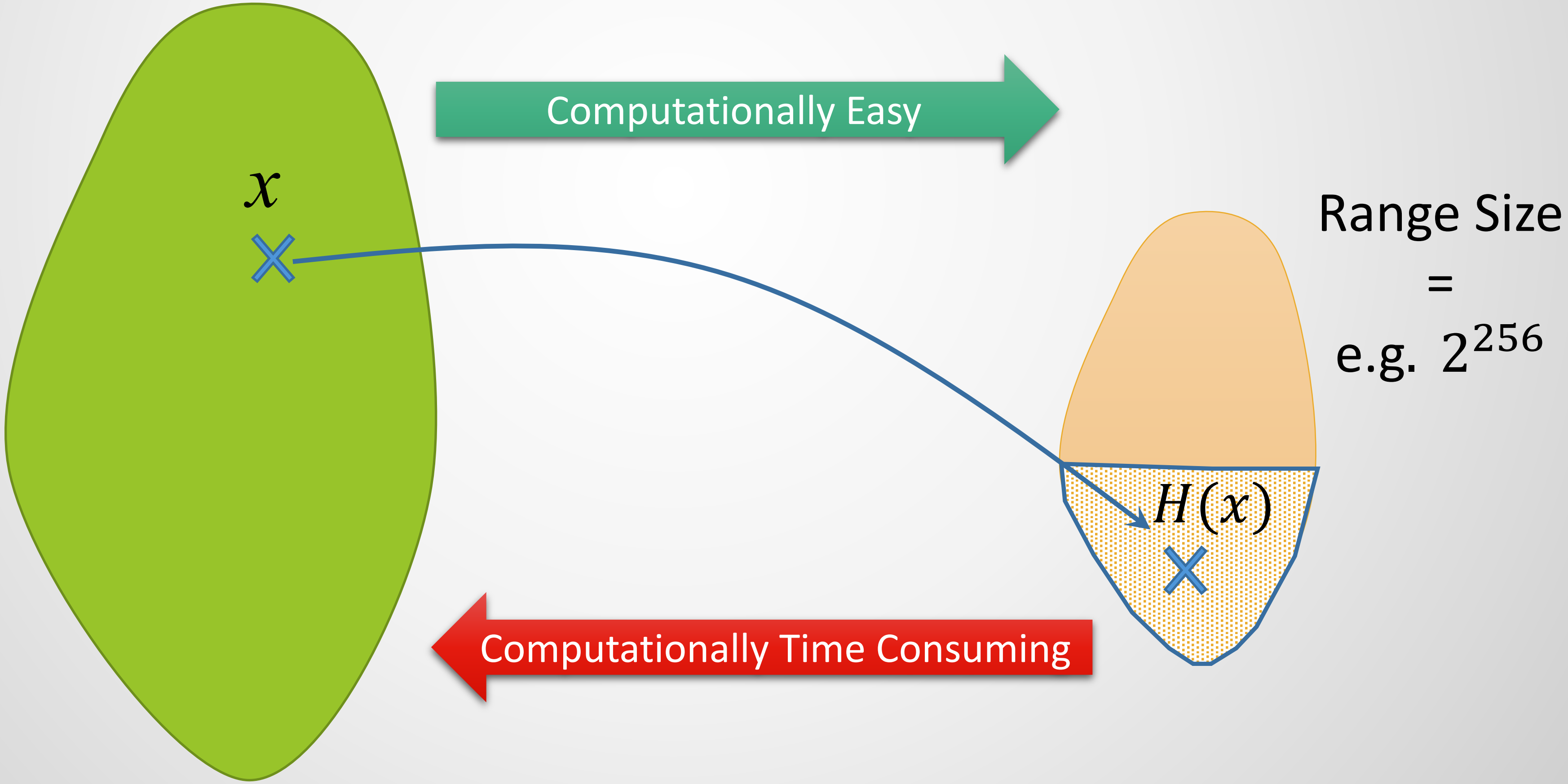
Why is it Difficult?

Do you remember the one-wayness property of hash functions? (property #4)



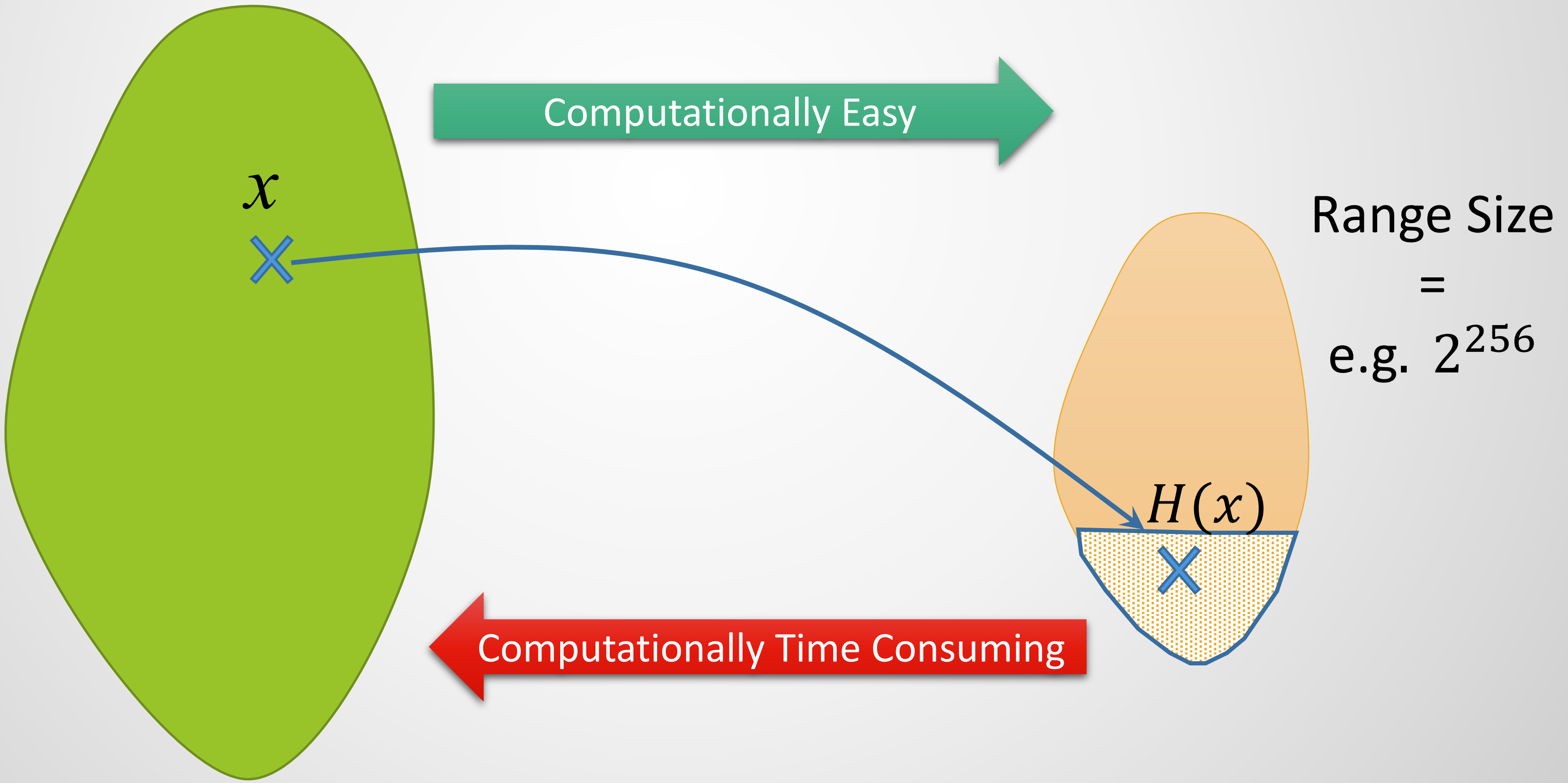
Why is it Difficult?

Now, imagine we want to solve the one-wayness problem, but not exactly. Instead of finding a point like x that exactly maps to H(x), we want to find a point like x that maps to any point inside a region in the range.



Why is it Difficult?

The size of the region determines the difficulty of solving this problem.



Difficulty Adjustment

The difficulty is set by the algorithm. It is adjusted every 2016 blocks based on average execution time for prior 2016 blocks to ensure future average execution time remains ~10 minutes. Of course a miner could ignore/break this algorithm but then they wouldn't be mining valid bitcoin blocks (they would be mining a fork).

- The bitcoin network rules define which difficulty each block has. This is done through a simple formula that only depends on the blockchain itself. This means that if you give me a blockchain with blocks 1 through N, I can tell you with 100% accuracy what the difficulty of block N+1 will need to be, and I ignore any blocks which have the wrong puzzle difficulties.

Difficulty Adjustment

- The actual formula is this: at every block N which is a multiple of 2016, look at the time stamps of the past 2016 blocks, and change the difficulty for what follows to:

$$new\ difficulty = \frac{(old\ difficulty) * (2\ weeks)}{time\ the\ past\ 2016\ blocks\ took}$$

14*24*60*60=1209600 seconds, and we aim that during this period, 2016 blocks are created, in average. We do this so that 1209600/2016=600secs=10 mins remains almost constant during bitcoin lifetime.

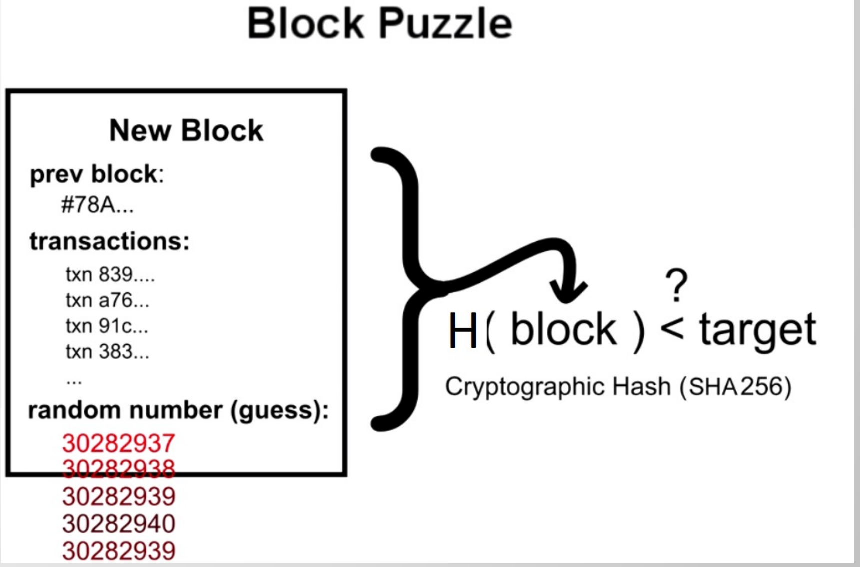
How to make a block?

Then, whoever receives the block, by taking the hash value can check if the issuer of the block has solved the hash puzzle.

- Hash puzzle is hard to solve since it’s a one way function

With all the nodes working on random numbers, it takes around 10 minutes to find a block.

- **So why should people do this?!**
  - There’s an incentive! **That’s how bitcoins are created!**



Block Puzzle

New Block

prev block:
#78A...

transactions:
txn 839....
txn a76...
txn 91c...
txn 383...
...

random number (guess):
30282937
30282938
30282939
30282940
30282939

$H(\text{ block }) \overset{?}{<} \text{target}$

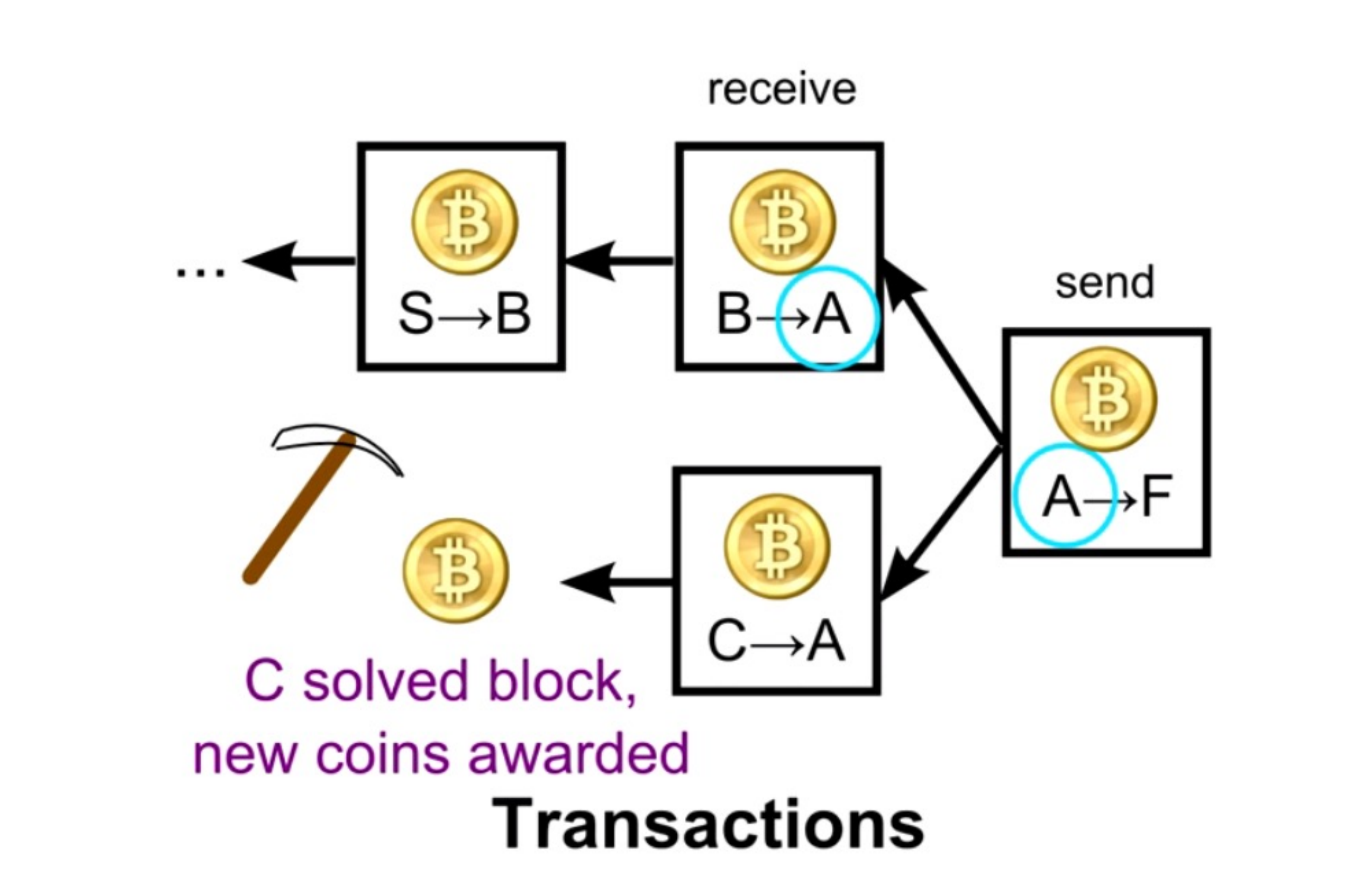
Cryptographic Hash (SHA256)

How to make a block?

- If you can find such a random nonce that gives such a hash value, you have not only added your block to the chain of blocks, but also will be rewarded X bitcoins.
  - This is called **Bitcoin Mining.**

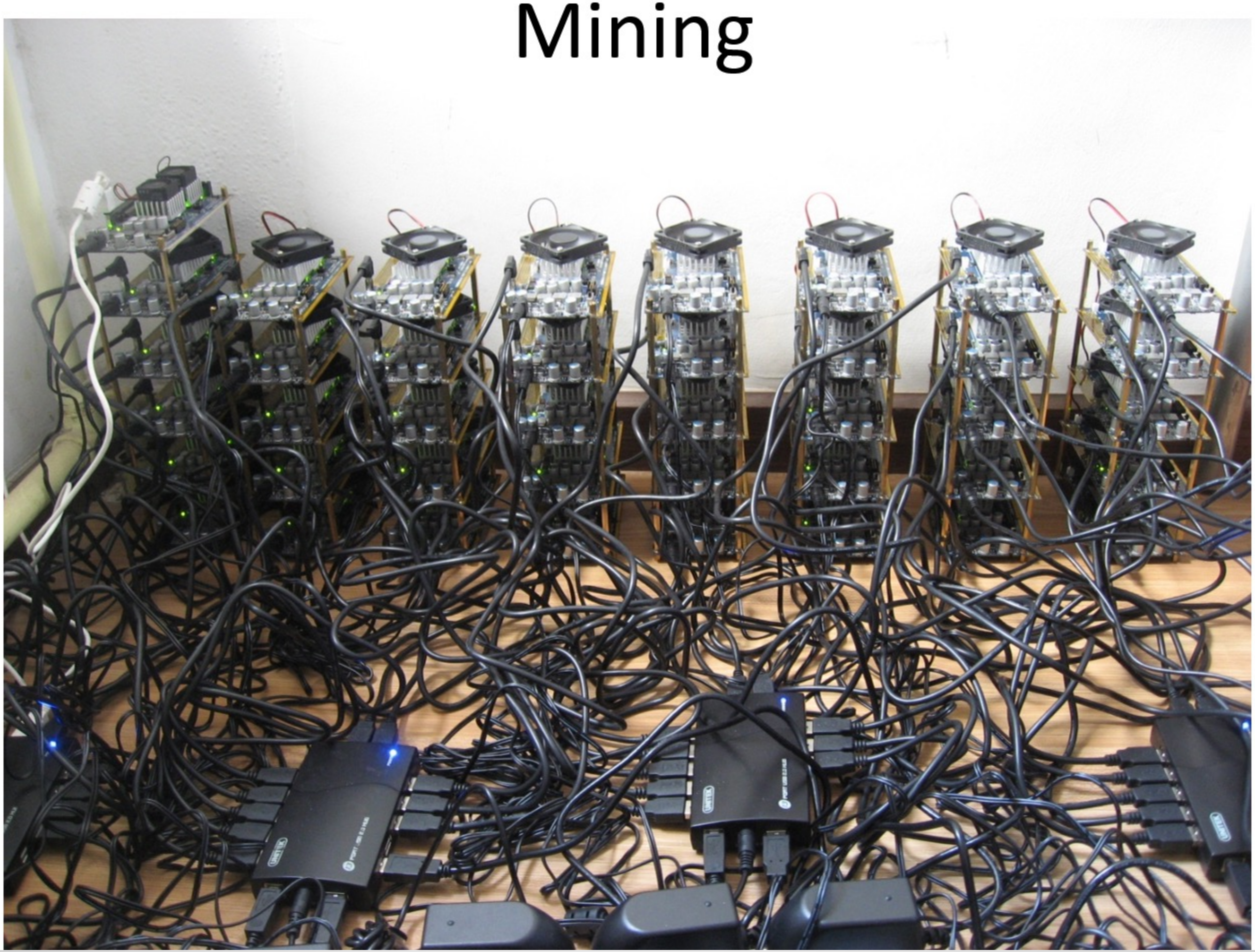
- Initially, X was 50. Every 4 years, the reward is divided by 2. Now (2020-2024) if you solve one block, you get 6.25 bitcoins.
  - **➔ # of Bitcoins is limited.**
  - This reward is a way to make nodes participate in storing/confirming the transactions. Otherwise, the history of transactions (showing the order of them, which is vital to prevent double spending) will be lost.

Two Valid Input Types – Bitcoin Generation



(How Bitcoin Works Under the Hood, Youtube)

Mining



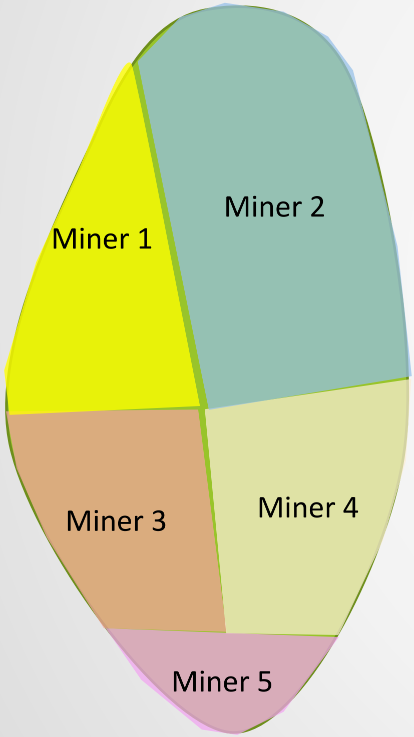
(Coman)

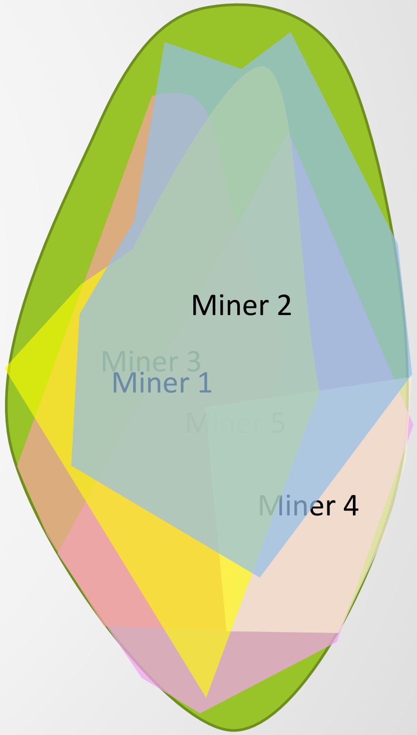
Mining Farm

(btcnn)

Individual Mining vs Pool Mining

Imagine we have a space to search for the solution of the Mining mathematical puzzle.

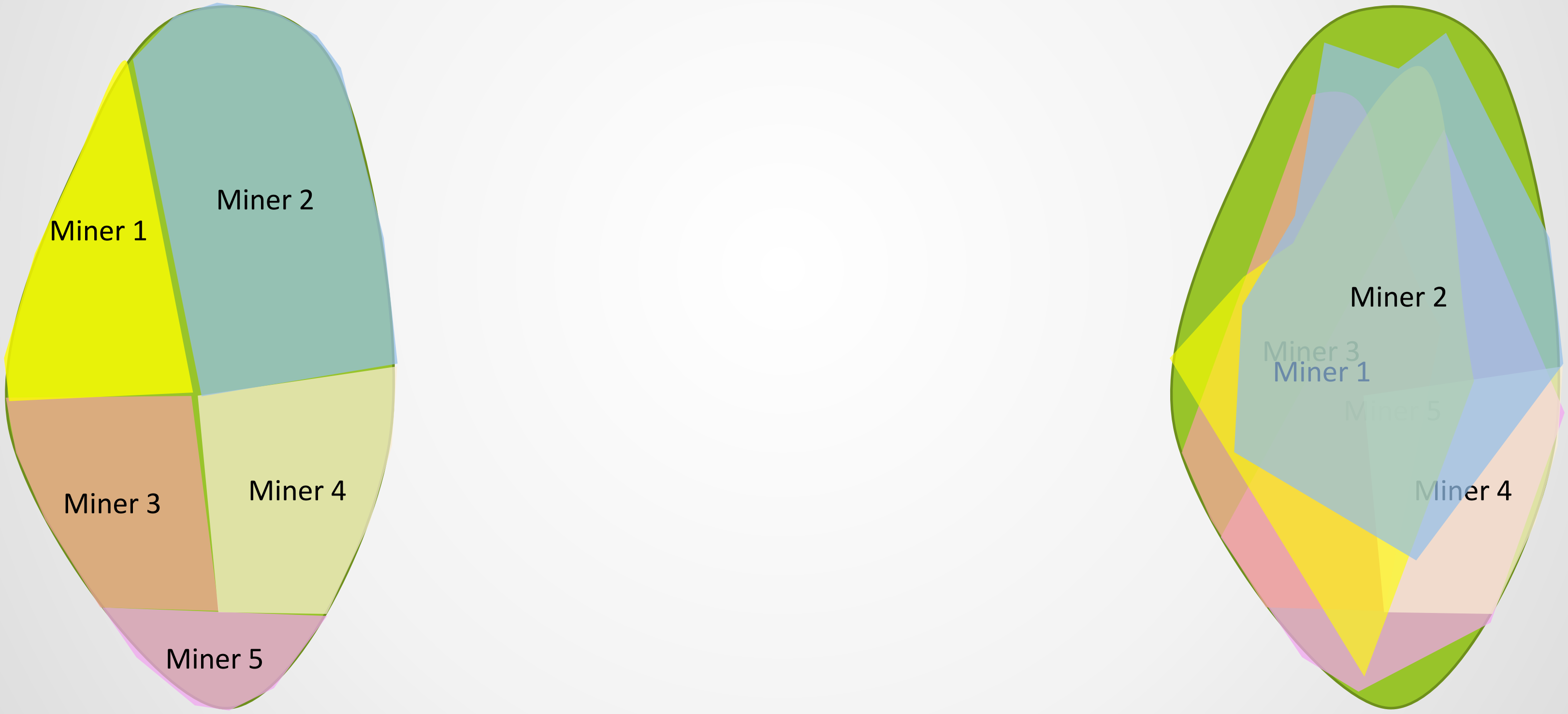




Which one is more effective?

Individual Mining vs Pool Mining

Pools are coordinators under which miners gather to orchestrate their area of search in order to find mining puzzle solution(s) more efficiently.



They agree to share the mining reward if one of them finds the solution. The solutions are usually submitted to the pool master and it distributes the rewards.

What Comes Next …

- We learned about distributed ledgers and transactions.
- We also learned how transactions are authenticated by asymmetric cryptography.
- In the next video, we explain Bitcoin details by starting from the problem of consensus and the problems not having it creates.

See you in the next video …