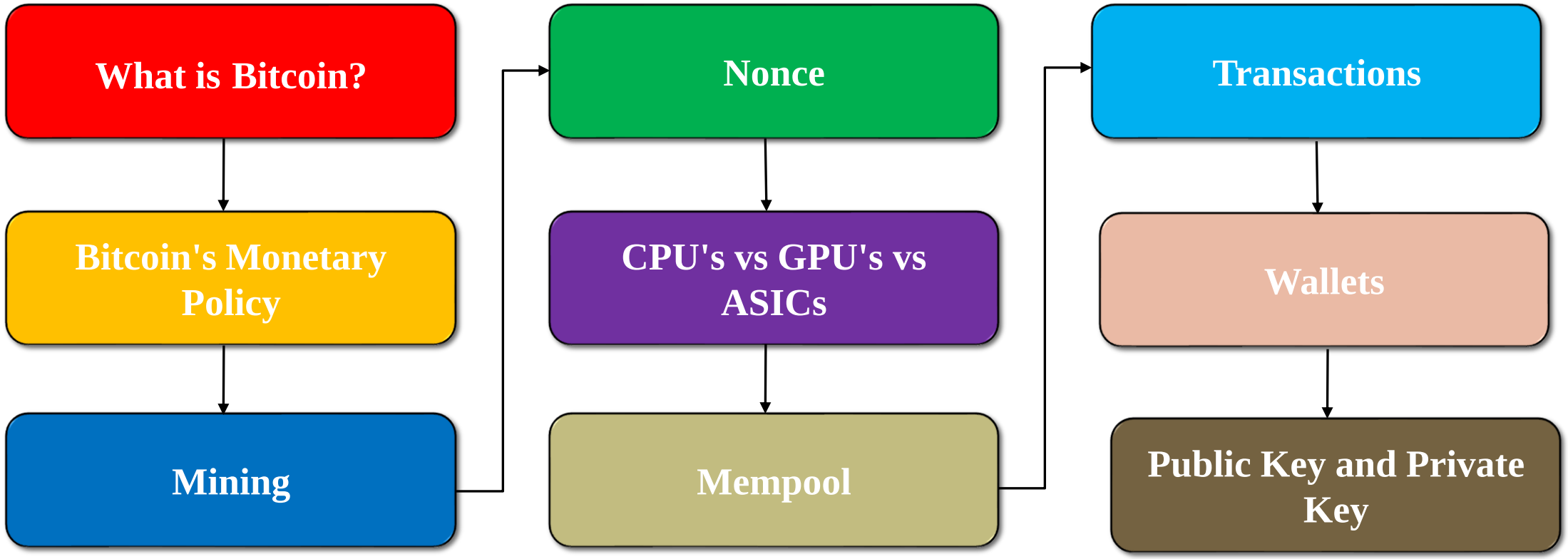
Blockchain

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

Cryptocurrency

Contents – Module B

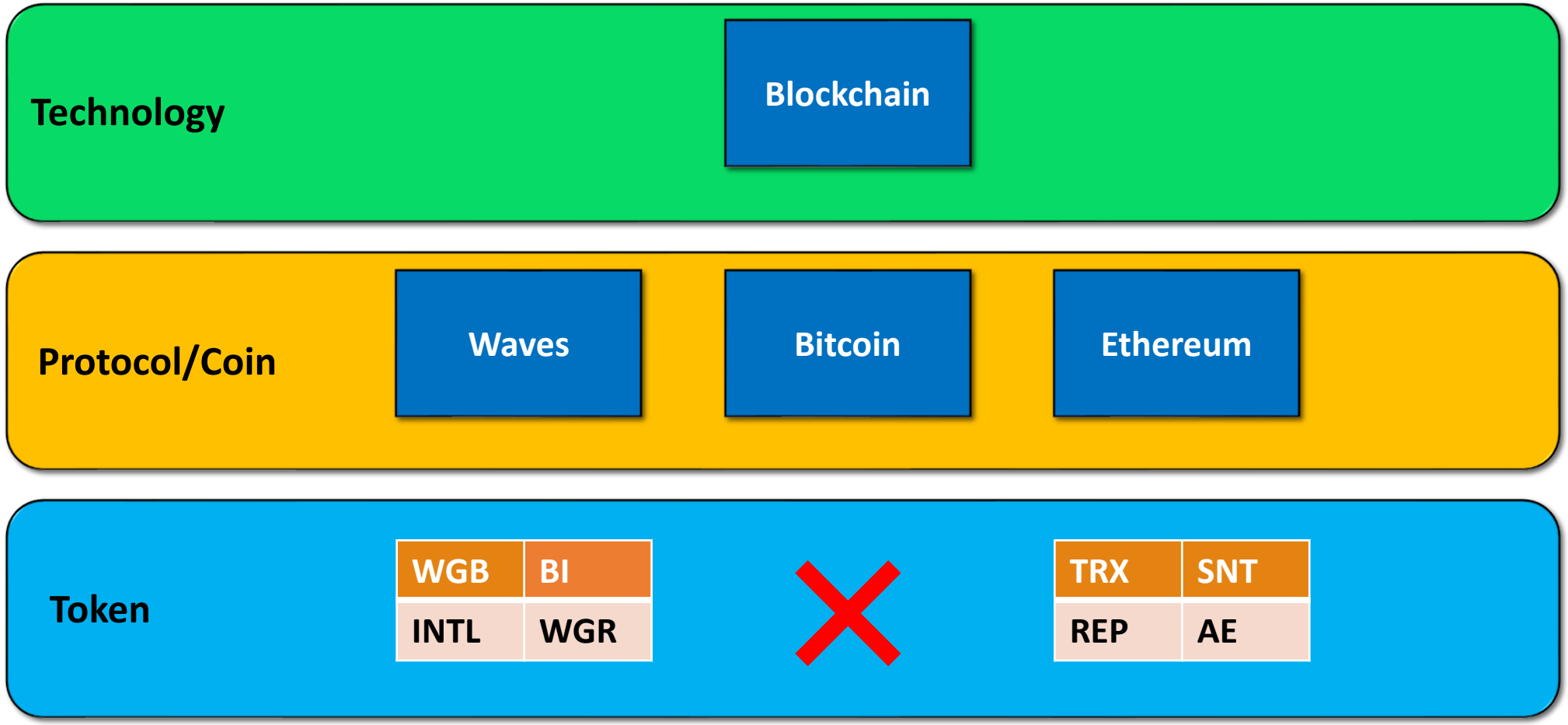


Founder of Bitcoin

Founder of Bitcoin

- **Satoshi Nakamoto**
- The first decentralized Blockchain was conceptualized by a person (or group of people) known as **Satoshi Nakamoto** in 2008.
- **Satoshi** published the Bitcoin white paper
- Created and deployed Bitcoin using Blockchain Technology
- As part of the implementation, he also devised the first Blockchain database

Coin vs Token



Blockchain vs. Bitcoin

- Blockchain is the Technology, whereas,
- Bitcoin is a protocol which uses Blockchain technology

Protocol: A set of rules for transmitting data between electronic devices, such as computers. For example, Bitcoin defines some set of rules i.e.

- How to work on Blockchain
- How mining will work
- How the rewards should be given to the miners etc.

Coin vs. Token

Coin:

- The coin is associated with the protocol
- The transaction take place and the fee is paid using these coins

Tokens:

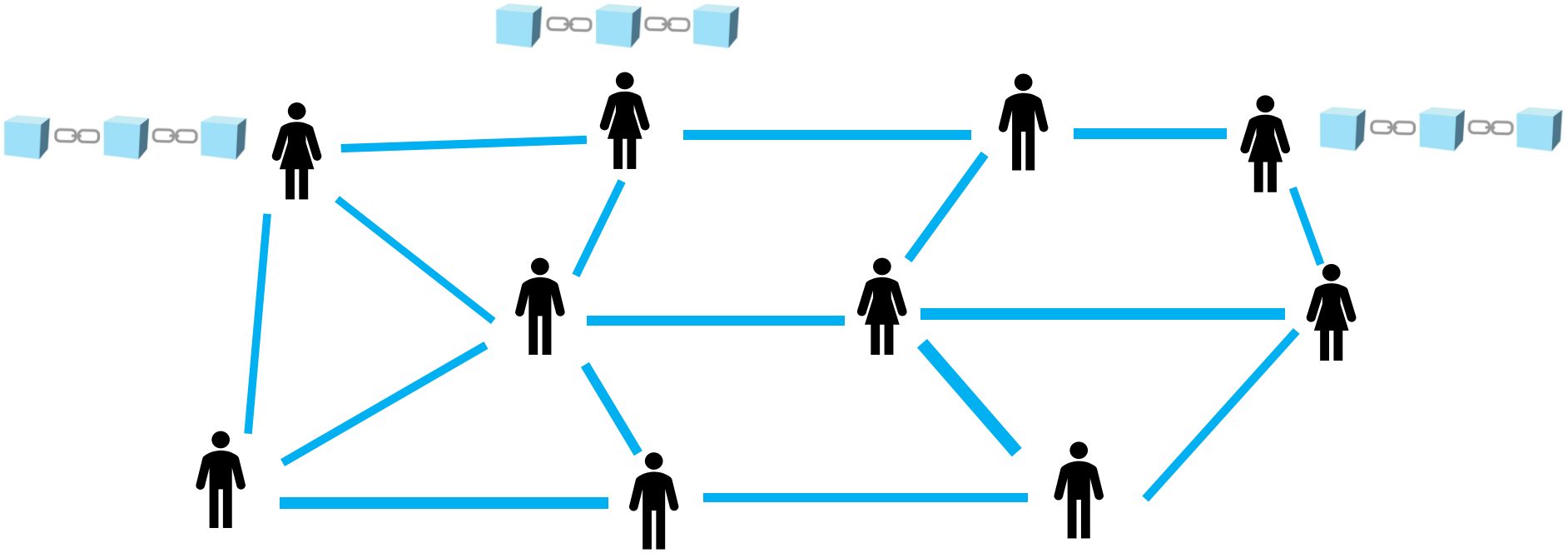
- Tokens are used/ based on these platforms (Bitcoin, Ethereum, Waves)

Coin Market demonstration
To see Coins vs. Tokens on different platforms
https://coinmarketcap.com/

Birth of Bitcoin

- The 2008 USA crisis destroyed people trust on central authorities like banks
- A new model and a class of asset was required, independent of central authorities
- In 2008, the Founder of the Bitcoin published a paper regarding Bitcoin based on Blockchain.
- As Blockchain removes the need of central authority, and people interact with each other directly.
- Bitcoin became popular and today it is the most popular Cryptocurrency

Bitcoin Network



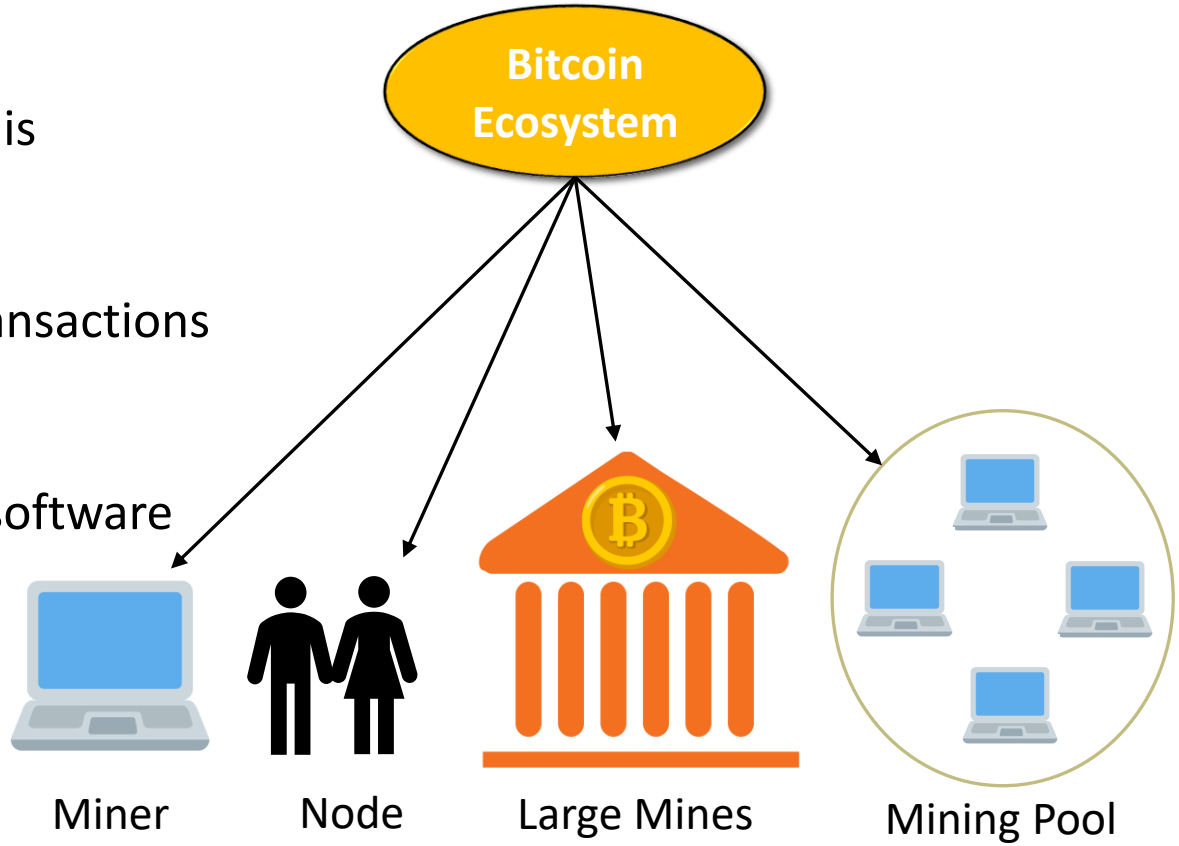
Bitcoin Ecosystem

Node:

- A computer that runs a Bitcoin software, and is connected to the Bitcoin network
- Validate, broadcast, process and store BTC transactions

Miner:

- A special type of node that runs a version of software that contains special rules for mining blocks



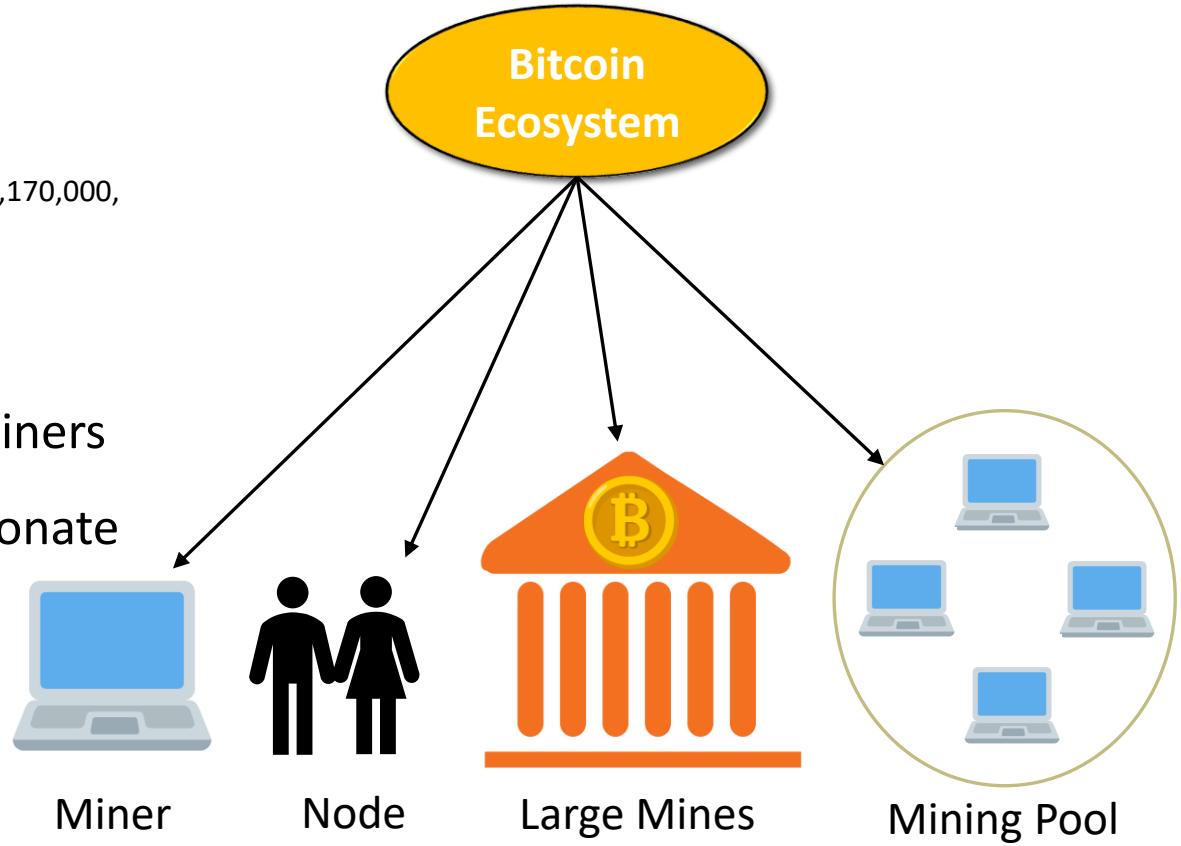
Bitcoin Ecosystem

Large mine:

- Has a huge setup
- **Dalian, China**: Hash rate is 360,000 TH, Monthly energy cost is $1,170,000, Mines 750 Bitcoin every month, and Mines 3% of all Bitcoins

Mining Pool:

- Coordinate mining activity from groups of miners
- The reward is distributed to miners proportionate to their number of resources
- Provide a steady stream of revenue for small scale miner



Bitcoin's Monetary Policy

Bitcoin Monetary Policy

- Every country has central authorities like banks etc. that control the control amount of money in a system
- Monetary Policy is used to maintain the supply of a currency (money)
- Bitcoin has its own monetary policy developed by Satoshi Nakamoto

Bitcoin's Monetary Policy

The Halving

Block Frequency

The Halving

Event	Date	Block number	Reward
Launch of Bitcoin	03 Jan. 2009	0	50 new XBT
1st halving	28 Nov. 2012	210’000	25 new XBT
2nd halving	09 Jul. 2016	420’000	12.5 new XBT
3rd halving	11 May 2020	630’000	6.25 new XBT
4th halving	Expected 2024	740’000	3.125 new XBT
5th halving	Expected 2028	850’000	1.5625 new XBT
Maximum supply reached	Expected 2140	6’930’000	0 new XBT

Note- Supply cap of Bitcoin is 21 million.

The Halving

- The bitcoins used in transaction fees halving every 210,000 blocks or four years
- That is why it is expected that these bitcoins will become 0 in 2140, therefore, no new bitcoins will be added to the system

The Halving

- You cannot create gold, but you can print currency as many as possible
- Therefore, the supply of any currency or bitcoins should be controlled
- When Zimbabwe's government prints many currencies, the banknote reached 100,000,000,000,000 (One hundred trillion dollars)
- However, what if the bitcoin used in transaction fees becomes 0?
- The fees will be directly deducted from the bitcoin account, as the bitcoins will be adopted by people at that time

The Halving

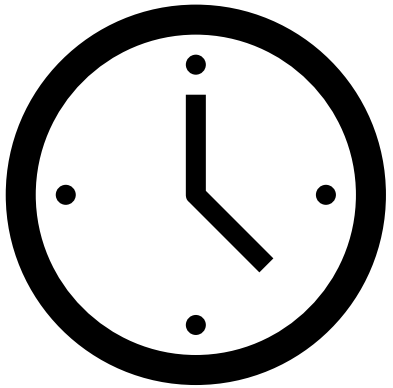

100000000000000 RESERVE BANK OF ZIMBABWE
100000
I promise to pay
the bearer on demand
AA0211549
ONE HUNDRED
TRILLION
DOLLARS
for the Reserve Bank of Zimbabwe
Dr. G. Gono
Governor
00 000 HARARE 2008
AA0

Block Frequency

- This states that on average it will take 10 minutes to create a new block

Q). How is the monetary policy working in the existing protocol?

A). This is done automatically by the bitcoin algorithm/ protocol



The Halving

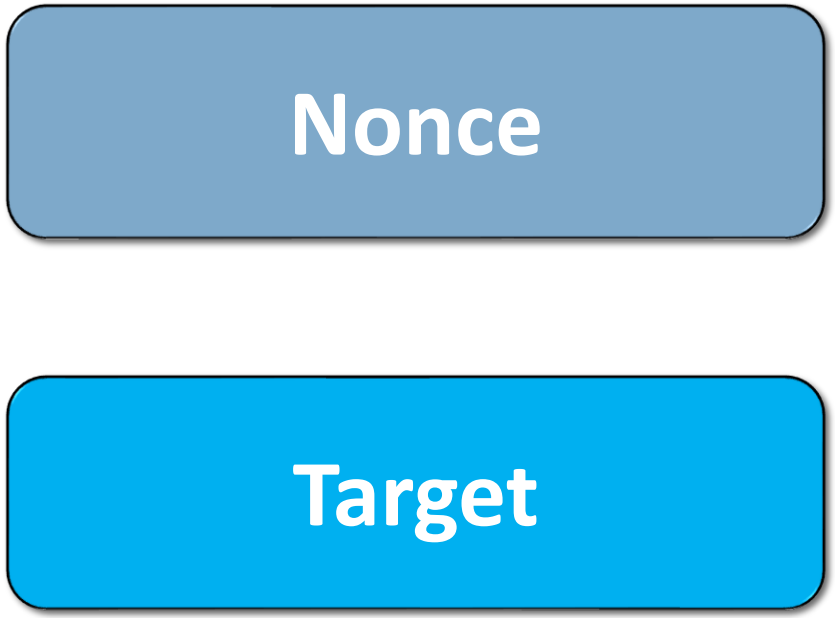
Demonstration: Checking the average time of mining a block

https://www.blockchain.com/explorer

https://www.blockchain.com/explorer/blocks/btc?page=1

- The Bitcoin Core protocol limits the block to 1 MB in size
- Each block contains at most some 4,000 transactions
- New blocks are added to the blockchain on average 10 minutes
- Therefore, the transaction rate is limited to some 7 transactions per second (TPS)

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 to the Blockchain.
- The target adjusts after every 2016 blocks (roughly two weeks) to try and ensure that blocks are mined **once every 10 minutes** on average.
- The target is adjusted by the algorithm or protocol automatically

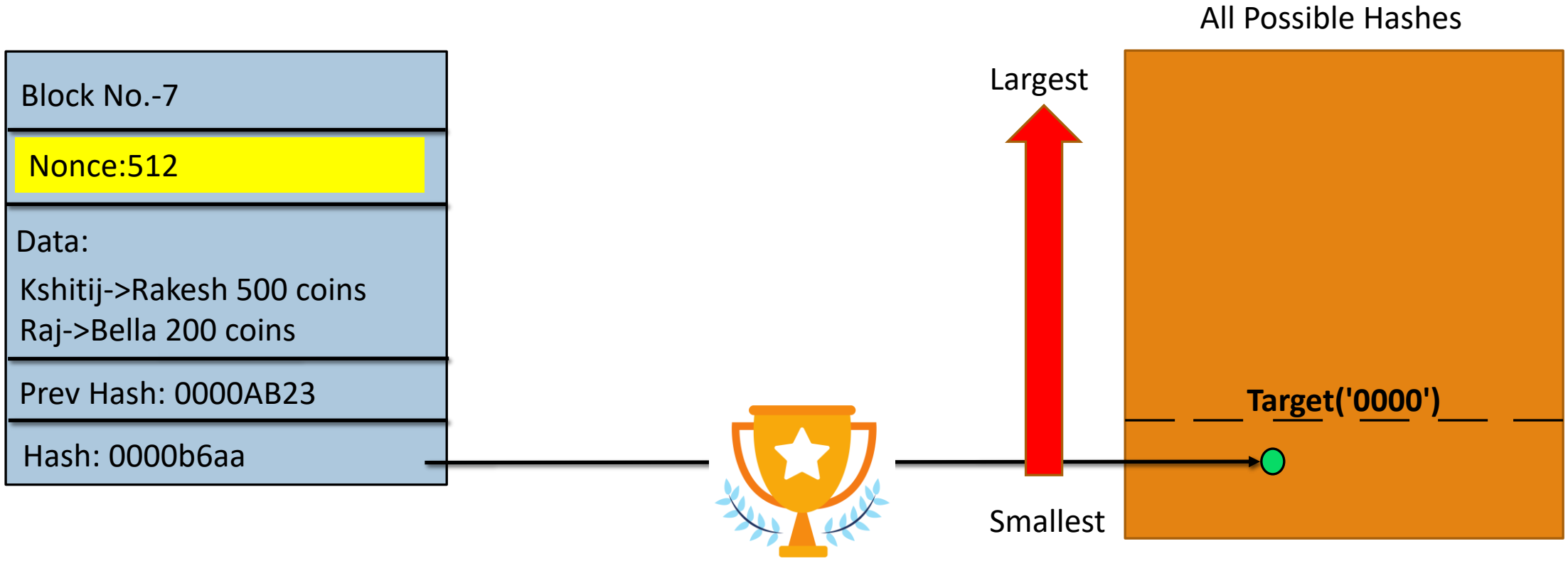
How Mining Works ?

- d2fd3930d274b202fe8e7cb431e38a8b64ec396e15f5717e60493234b0de210a
- 52d095795c1dc87ff2f6b4d9b005a1fe2cfed01103763c9443f6d4496df8e800
- 0000005432d9f64f6e05c019f9302162100163b6cdba06bd72eee35cd19aebf

Smallest- 0000000.....0

Largest- fffffffffffff.....f

How Mining Works ?



Bitcoin's Target History

Bitcoin's Target History

Bitcoin Genesis Block

Block# 0

Hash: 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

This is the Bitcoin genesis block it marks the birth of the Bitcoin network and was mined by the project's mysterious creator 'Satoshi Nakamoto'. Its 50 bitcoin coinbase reward is unspendable as it was omitted from the transaction database so any attempt to spend it would be rejected by the network. Whether this was intentional or not is unknown.
This block was mined on 1/03/2009, 23:15:05 by Satoshi.
A total of 0.00 BTC ($0.00) were sent in the block with the average transaction being 0.0000 BTC ($0.00). Satoshi earned a total reward of 50.00 BTC $0.00. The reward consisted of a base reward of 50.00 BTC $0.00 with an additional 0.0000 BTC ($0.00) reward paid as fees for the 1 transaction which were included in the block.

Bitcoin's Target History

Bitcoin Block

Block# 754,406

Hash: 000000000000000000074ba534a31b3bc67ccb0b4193fab88b88f0afd1b15d3d

This block was mined on 9/17/2022, 05:22:37 by Unknown. A total of 14,538.41 BTC ($289,334,787) were sent in the block with the average transaction being 8.7845 BTC ($174,823). Unknown earned a total reward of 6.25 BTC $124,383. The reward consisted of a base reward of 6.25 BTC for $124,383 with an additional 0.2087 BTC ($4,153.42) reward paid as fees for the 1,655 transactions which were included in the block.

Bitcoin's Target History

Block# 0

Mined on (1/03/2009, 23:15:05)

Hash: 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Target: 10 Zeros at the beginning

Block# 754,406

Mined on (9/17/2022, 05:22:37)

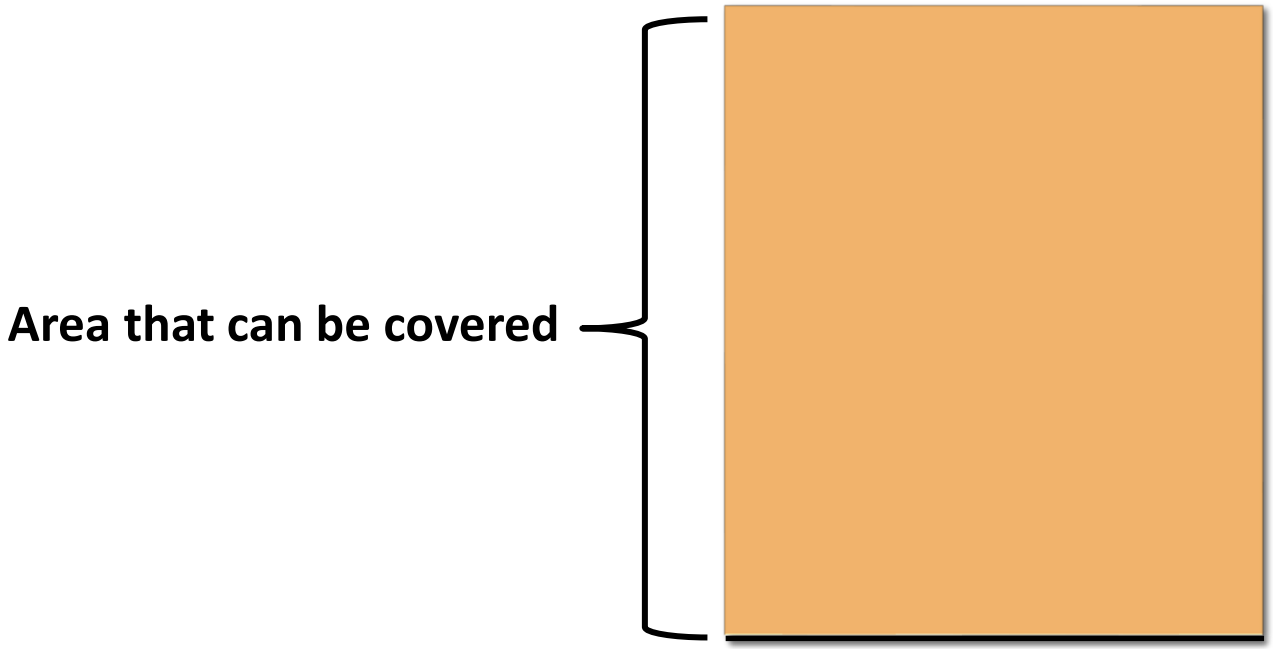
Hash: 000000000000000000074ba534a31b3bc67ccb0b4193fab88b88f0afd1b15d3d

Target: 19 Zeros at the beginning.

Bitcoin's Target Difficulty

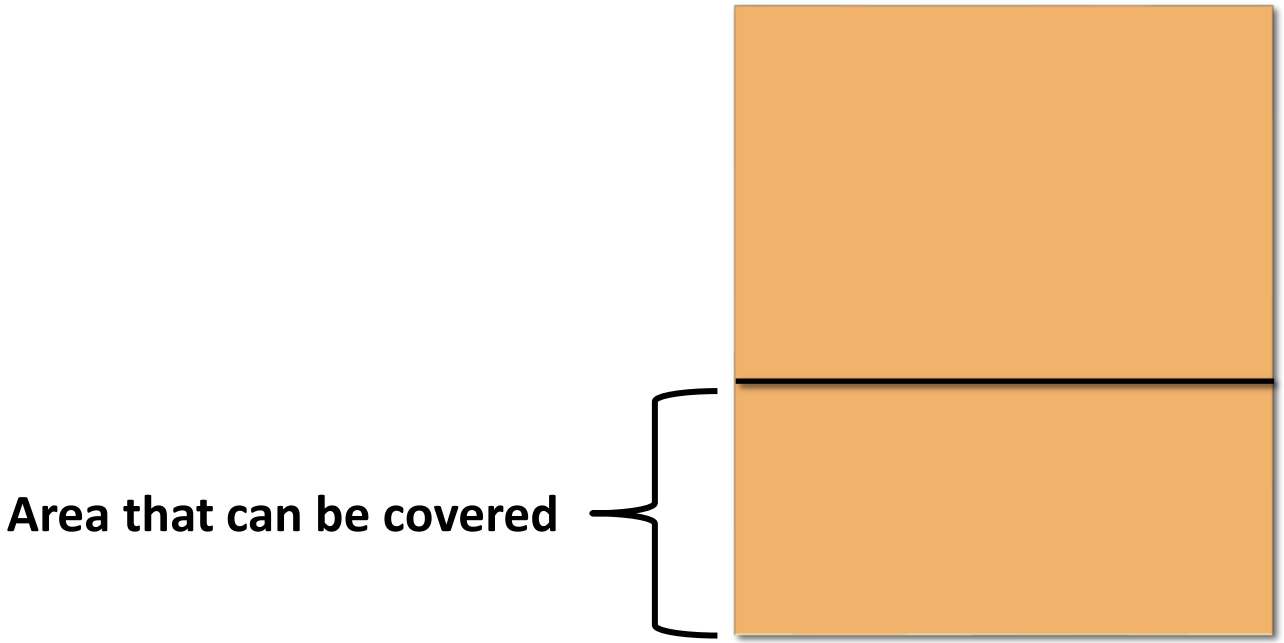
Understanding Mining Difficulty

Let's take a five-digit number= XXXXX



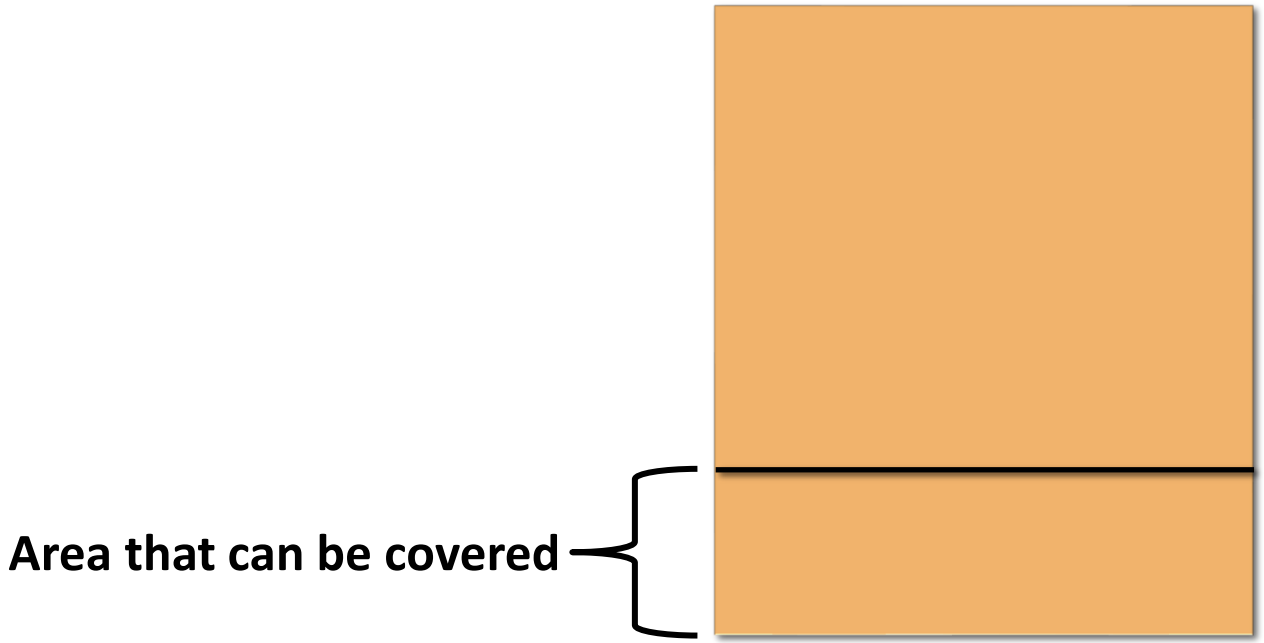
Understanding Mining Difficulty

Let's take a five-digit number= 0XXXX



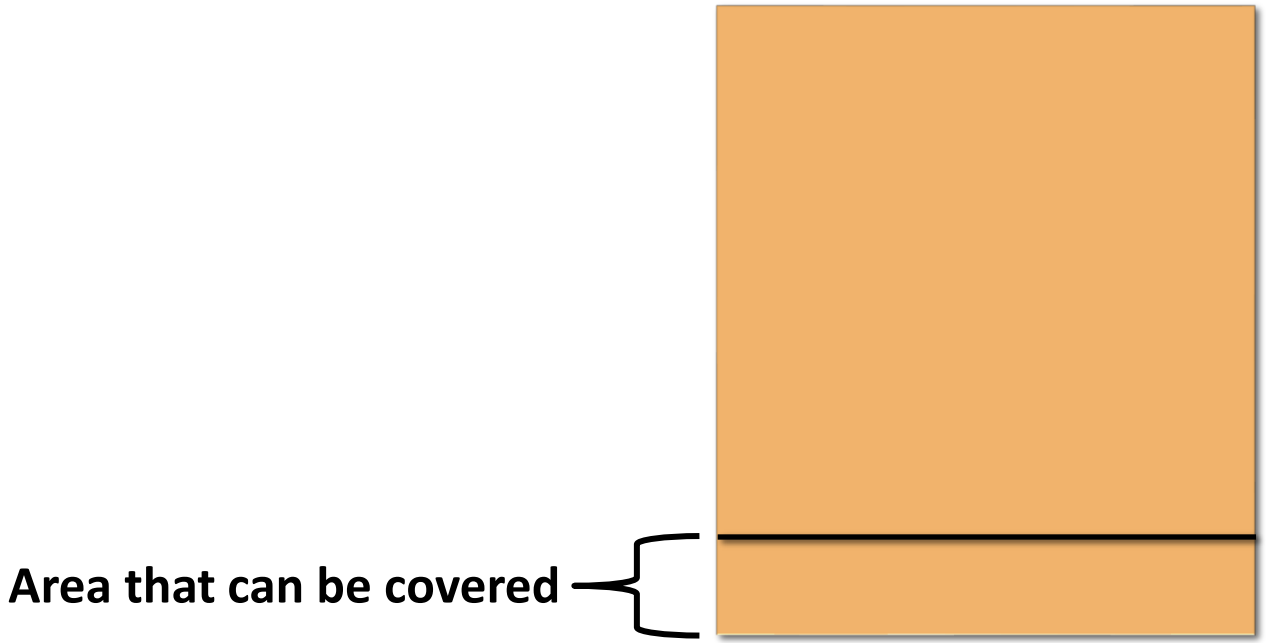
Understanding Mining Difficulty

Let's take a five-digit number= 00XXX



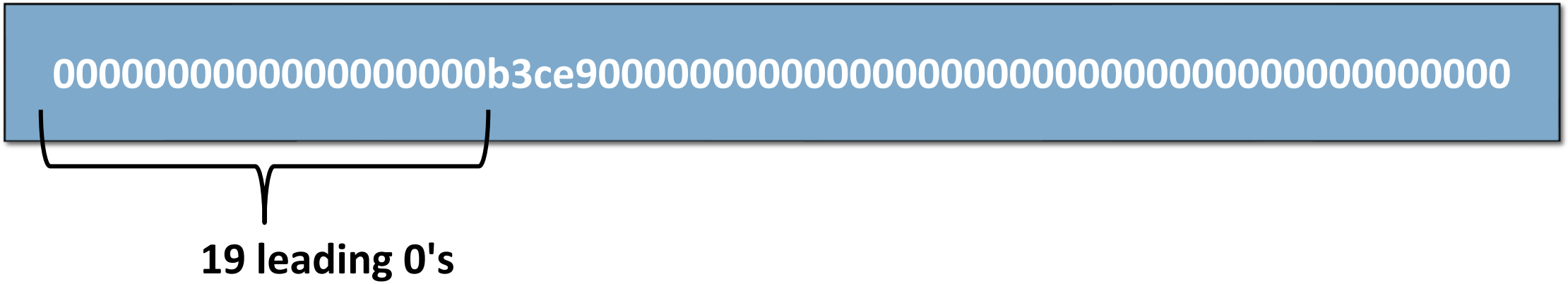
Understanding Mining Difficulty

Let's take a five-digit number= 000XX



Understanding Mining Difficulty

Current Target:



Understanding Mining Difficulty

Total Possible 64-digits hexadecimal numbers = 16^64 ≃ 10^77

Total valid hashed(with 19 leading 0's) = 16^(64-19) ≃ 10^54

The probability that a randomly picked hash is valid = (10^54/10^77) ≃ 10^-23

OR

The probability that a randomly picked hash is valid = (1/16)^19 ≃ 10^-23

Understanding Mining Difficulty

Q) Who adjusts the difficulty?

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

Satoshi Nakamoto