

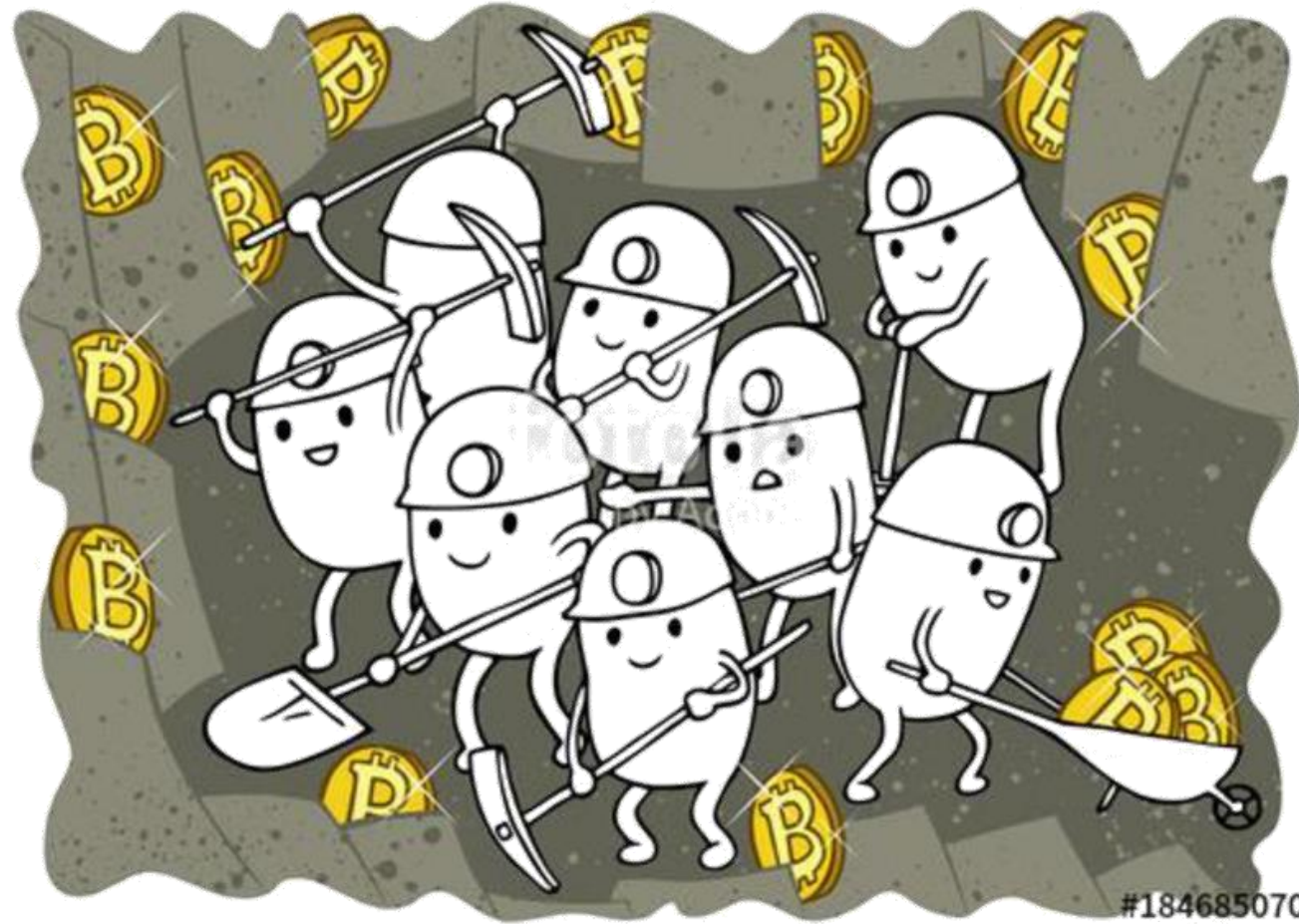
Virtuoso Infotech Pvt. Ltd.



# About Virtuoso Infotech

- Fastest growing IT firm; Offers the flexibility of a small firm and robustness of over 30 years experience collectively within the leadership team
- Technology expertise & passionate team
- Successful client engagements across India, USA, UK, Australia and Argentina
- Handle enterprise solutions that involve **30,000 active users**, more than 20 servers, **data volume as big as 5 million entries per day**

# Crypto Mining



- Prajyot Patle

# Agenda

- What does a miner do?
- Why Mining?
- How does a block look like?
- Proof of work
- Mining Difficulty
- How to mine?
- Demo

# How does a block look like?

- Index
- Timestamp
- Hash of previous block
- Data (Transactions)
- Nonce
- Hash

# What does a Miner do?

- Verify if broadcasted transactions are valid.
- Bundle transactions in a block.
- Select the hash of the most recent block, and insert into the new block.
- Solve the Proof-of-Work problem.
- When the solution is found, the new block is added to the local blockchain of the miner and broadcasted to the network of miners.
- Other miners accept the block only if:
  - . All the transactions in it are valid and not already spent.
  - . The proof of work is valid

# Why Mining?

- To allow bitcoin nodes to reach a secure, temper resistant consensus.
- To introduce bitcoin into the system.
- Miners are paid in block rewards and transaction fees.
- This both serves the purpose of introducing new coins in a decentralized manner as well as motivating people to provide security for the bitcoin system through mining.

# Proof-of-Work

- The proof-of-work involves scanning for a value that when hashed, the hash begins with a number of zeros.
- We find the proof-of-work by incrementing the a nonce in the block until a value is found that gives the block's hash the required zero bits.
- Once CPU work has been expended to make it satisfy the proof-of-work, the block can not be canged without redoing the work.
- As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.
- To modify a past block, an attacker would hae to redo the proof-of-work of the block and all the blocks after it and then compete with the current network.



# Mining difficulty

- The mining difficulty is the measure of how difficult it is to find a new block.
- It is recalculated every 2016 blocks to depending upon the current network mining power.
- As more miners join, the rate of block creation will go up. As rate goes up, the difficulty rises to compensate which will push the rate of block creation back down.
- It is adjusted so that a new block is generated every 10 minutes approximately.

# How to mine ?

- You need mining hardware.
  - CPU
  - GPU
  - ASIC Cards
- You need mining software.
- You need a wallet.
- Mining pools

**Demo**

# Thank You!

Virtuoso InfoTech Pvt. Ltd.  
4th Floor, Victory Landmark, Opp.  
D-Mart,  
Behind Dominos Pizza, Baner, Pune.

+91 8087081318  
support@virtuosoitech.com



[www.virtuosoitech.com](http://www.virtuosoitech.com)

