SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A++' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF INFORMATION TECHNOLOGY

BLOCK CHAIN AND CRYPTOCURRENCY

IV YEAR - VII SEM

UNIT 2 – Block chain Technologies

Intro - Block chain Technologies

BlockChain Technologies

BlockChain Technologies

Altcoins waiting to see what Bitcoin will do next

Brief Introduction

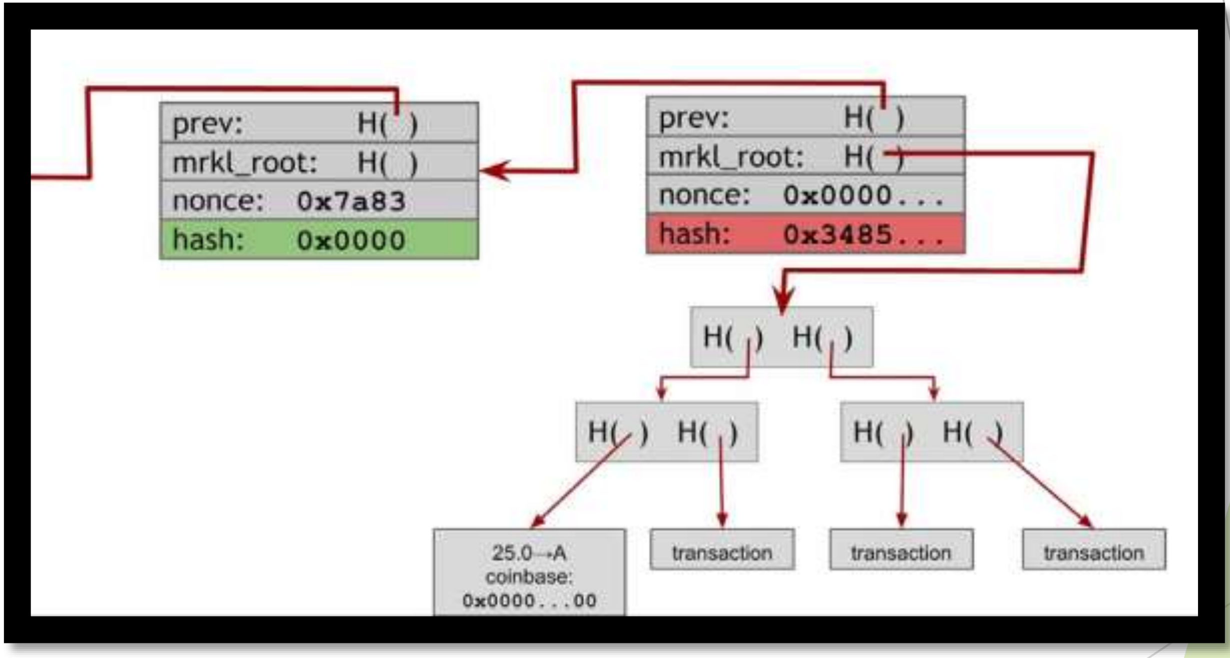
- Name: Radoslaw Krzeski
- Occupation: Digital Project Manager
- Interested in Blockchains as a tool for economic efficiency in the media industry

Bitcoin mining

- The authors warn of a goldrush race
- To join, we connect to other nodes and perform six tasks:
  - Listen for transactions
  - Maintain block chains and listen for new blocks (valid nonce)
  - Assemble a candidate block
  - Find a nonce that makes your block valid (hitting target)
  - Hope your block is accepted

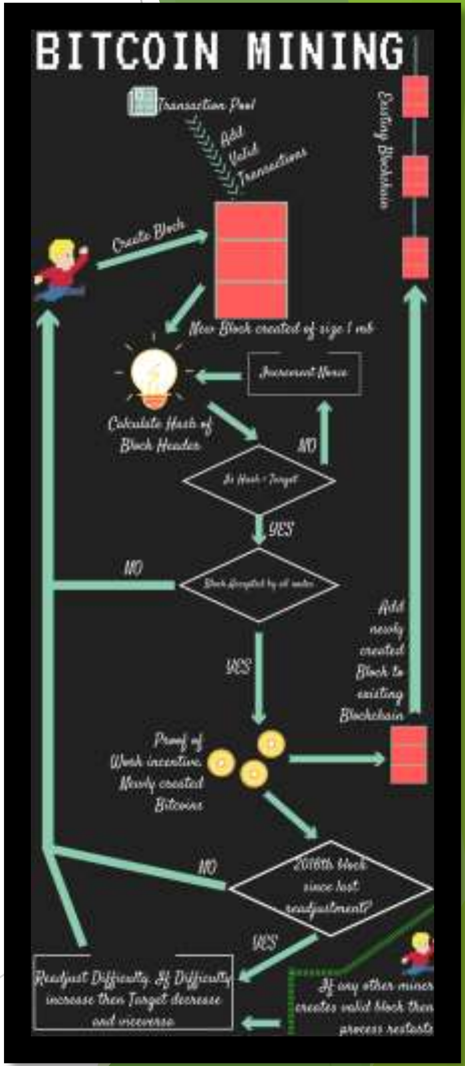
= Profit

Finding the Valid Block

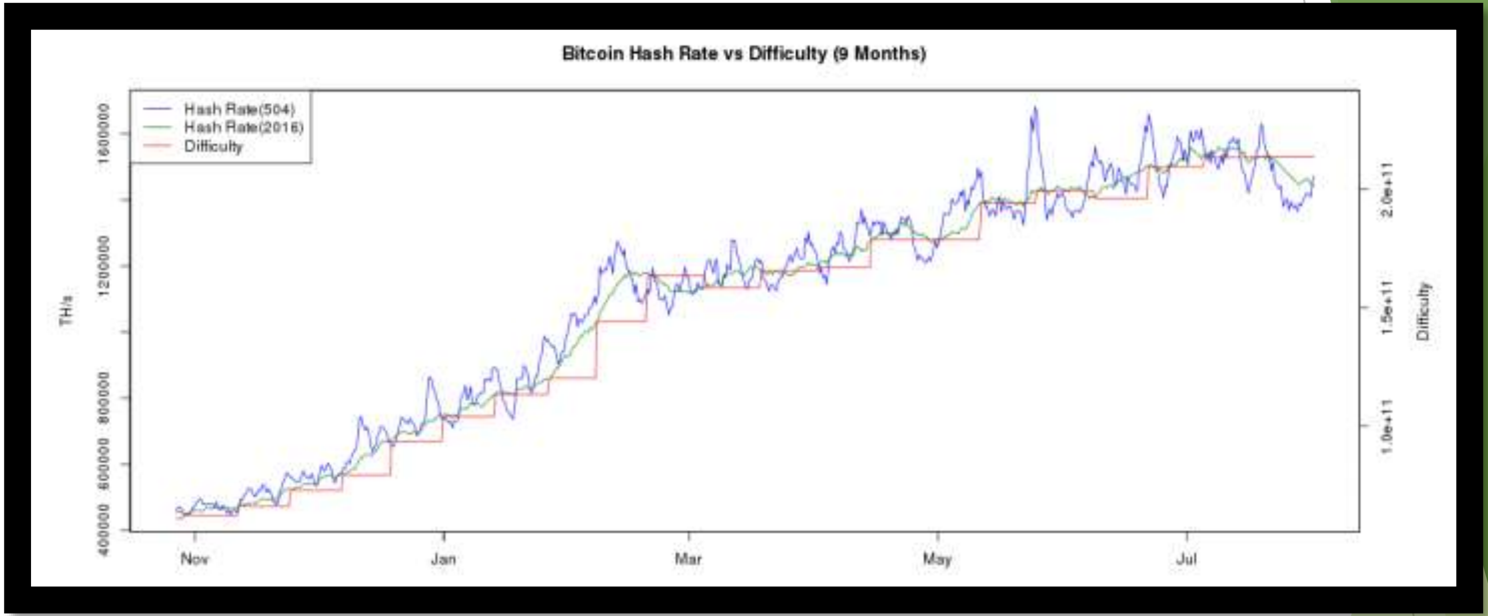


Determining Difficulty

- Changes roughly every two weeks
- Changes at every 2016 blocks
- Difficulty fluctuates based on given time to mine
- Miners on the same block have the same difficulty
- Allows consesus

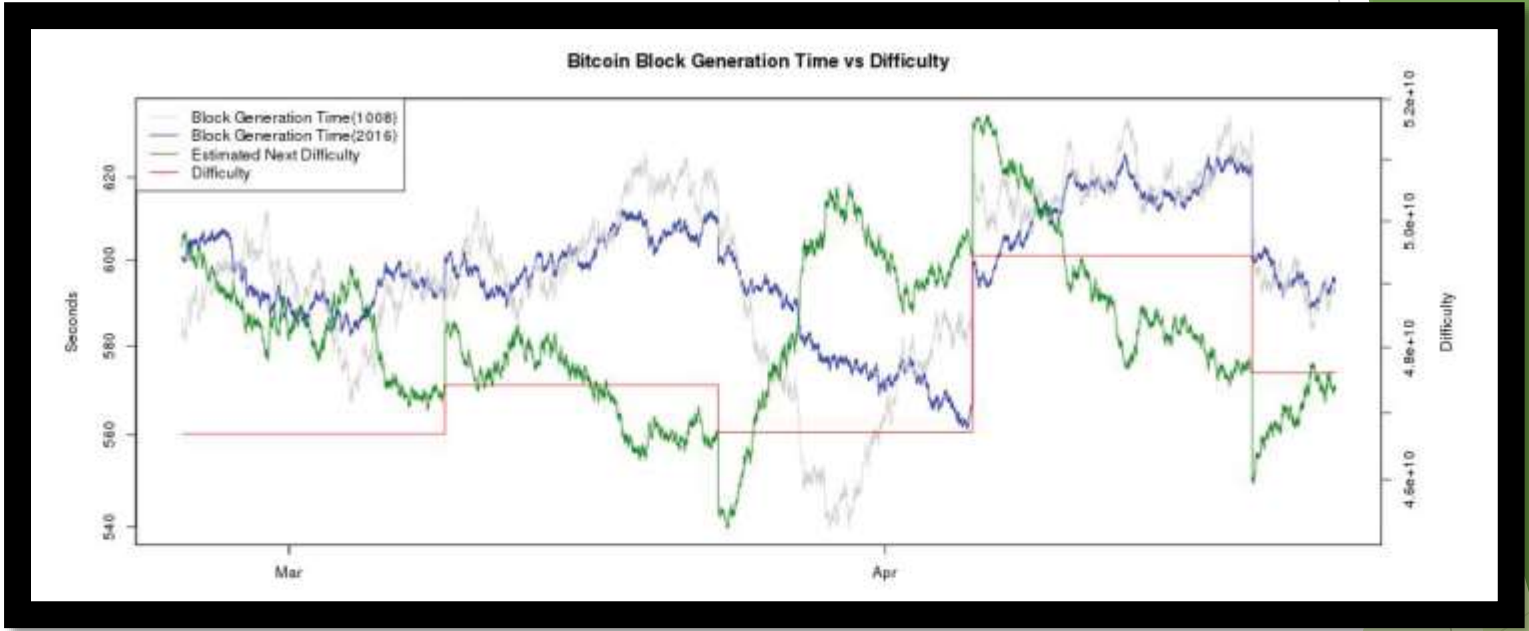

BITCOIN MINING
Transaction Pool
Add Valid Transactions
Existing Blockchain
Create Block
New Block created of size 1 mb
Increment Nonce
Calculate Hash of Block Header
NO
Is Hash < Target
YES
NO
Block Accepted by all nodes
YES
Add newly created Block to existing Blockchain
Proof of Work incentive. Newly created Bitcoins
NO
2016th block since last readjustment?
YES
Readjust Difficulty. If Difficulty increase then Target decrease and viceversa
If any other miner creates valid block then process restarts

BlockChain Technologies



Side Question; What is a death spiral?

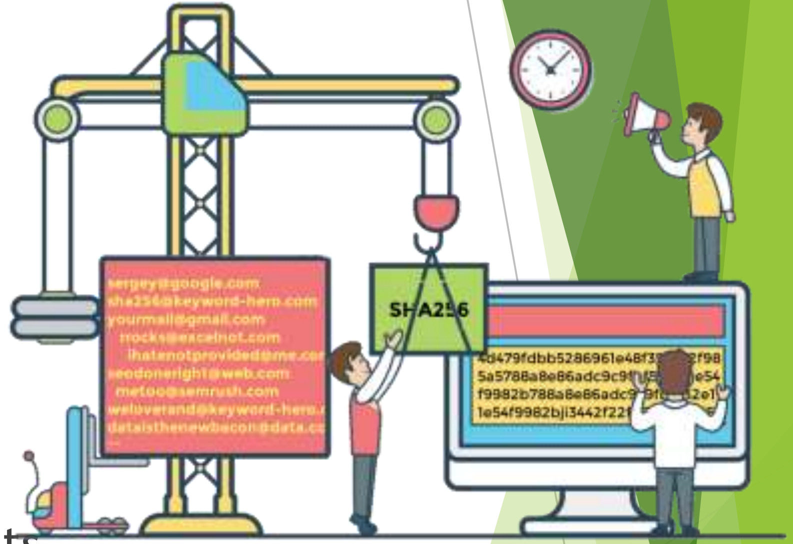
BlockChain Technologies



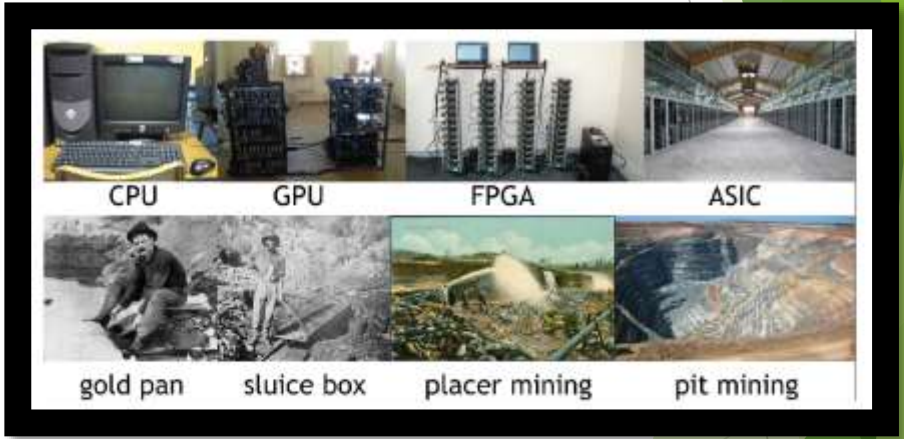
Mining Hardware

- SHA-256 Hash function
- Applied twice to a bitcoin block
- Impossible for normal computers
- CPU/GPU mining (2010 OpenCL)
- Arithmetic Logic Units (ALUs)
- Field Programmable Gate Arrays
- Application –Specific Integrated Circuits

Why are hashes non-reversible?

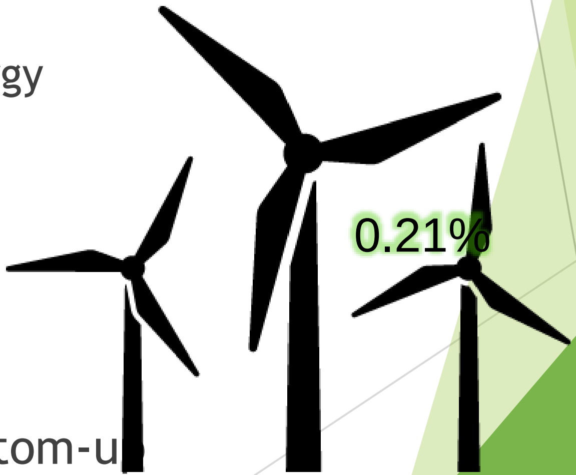


Professional mining



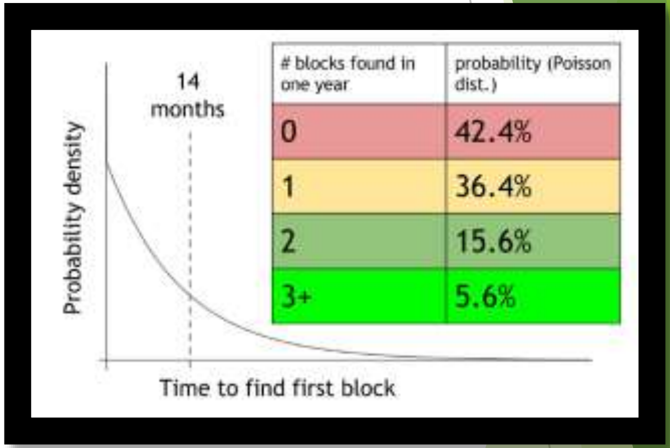
Energy consumption

- Laundauer`s Principle
  - (every time you flip a bit there is a minimum amount of energy required
  - Three steps to bitcoin`s usage of energy
    - Embodied energy
    - Pure Electrity
    - Cooling
- Two ways to calculate: Top-down/Bottom-up



Mining Pools

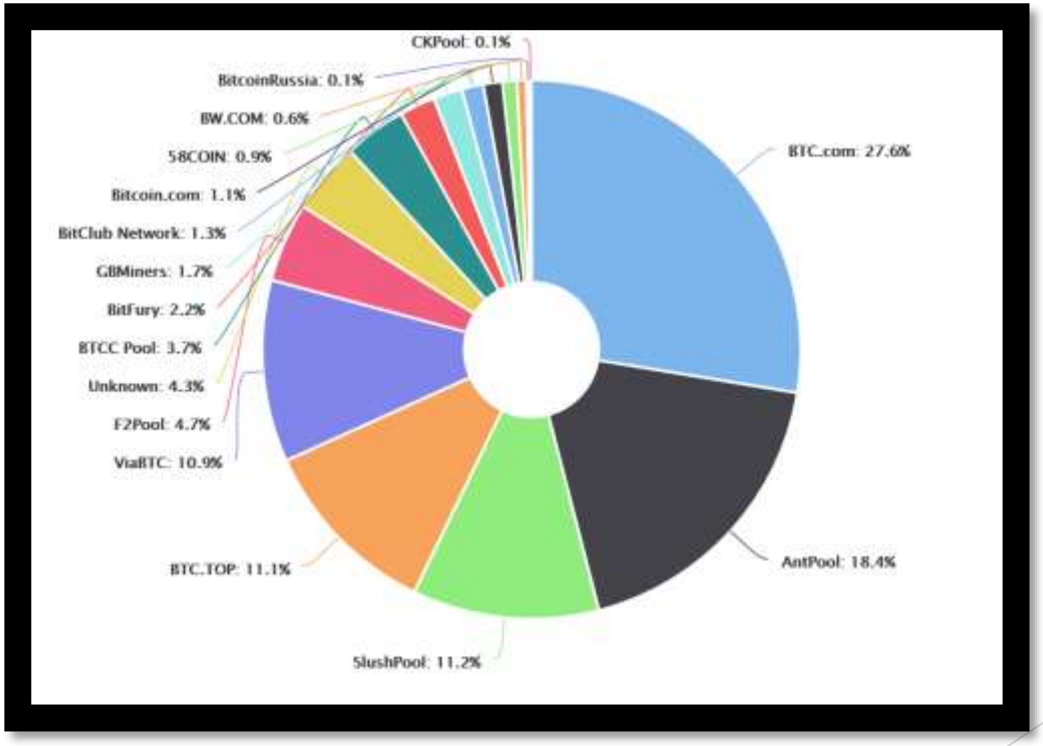
- Small chance of finding blocks
- Many miners, one pool manager
- Calculating mining shares by reporting near valid hashes and actual valid blocks
  - Pay-per share
  - Propotional
  - Pool hopping
  - Communication API`s



# blocks found in one year	probability (Poisson dist.)
0	42.4%
1	36.4%
2	15.6%
3+	5.6%

Mining Pools cont.

- 51%?



Mining Risks

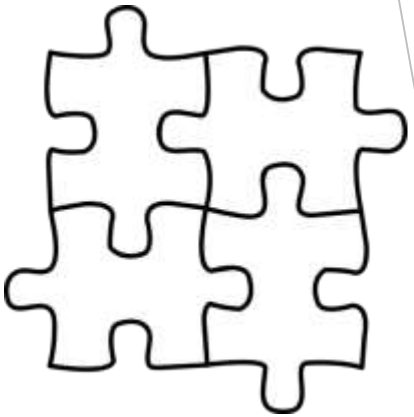
- Forking attack
- Goldfinger attack
- Forking via bribery
- Temporary block-withholding attacks
- Blacklisting / Punitive Forking

Alternative Mining puzzles

- Why do we have mining puzzles?
- A few basic requirements:
  - Quick to verify
  - Adjustable difficulty
  - Progress-freenes
  - Memoryless process
- What is a different word for «Bitcoin Puzzle»?

ASIC-resistant?

- «One-CPU-one-vote»
- Memory-hard puzzles
- Memory-bound puzzles
- Scrypt – although resitant, what happened?
- DASH(x11)
- Changing/Moving puzzles



Last Notes

- Proof-of-Useful-Work
- Nonoutsourceable Puzzles
- Virtual Mining

Discussion

- What constitutes the luck element, what is involved in the block creation to be accepted by the consensus chain?
- Is there a chance that two miners are mining the same block/puzzle?
- At one point the book mentions : «If the period were much higher, the network’s hash power might get too far out of balance with the difficulty.» - What happens then?
- What happens when we go from derived value from the mining to the transaction fees? How will miners change their behaviour?
- ASIC mining and the development of professional mining centers violate the original vision of Bitcoin which was to have a completely decentralized system in which every individual in the network mined on his or her own computer. Is it a violation of Satoshi Nakamoto’s original vision in terms of the mining or did he foresee it?

BlockChain Technologies

- What happens when we go from derived value from the mining to the transaction fees? How will miners change their behaviour?