NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Sandip Chakraborty
Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 11: Bitcoin Mining and Beyond

CONCEPTS COVERED

- Bitcoin Mining
- The Economic Model of Bitcoin
- Popularity of Cryptocurrencies

KEYWORDS

- Mining and Miners
- Mining reward
- Bitcoin Price
- Beyond Bitcoins

Bitcoin Mining: The Key to Consensus

- There are special nodes, called the Miners
- Miners propose new blocks – solve the puzzle (find the nonce corresponding to a target block hash), and add the solution as a **proof** of solving the challenge to be the leader
  - Solving the challenge needs some work to be done – ***Proof of Work (PoW)***

Bitcoin Mining: The Key to Consensus

- There are special nodes, called the Miners
- Miners propose new blocks – solve the puzzle (find the nonce corresponding to a target block hash), and add the solution as a **proof** of solving the challenge to be the leader
  - Solving the challenge needs some work to be done – ***Proof of Work (PoW)***

Why someone would want to be the leader?

Bitcoin Mining: The Key to Consensus

- There are special nodes, called the Miners
- Miners propose new blocks – solve the puzzle (find the nonce corresponding to a target block hash), and add the solution as a **proof** of solving the challenge to be the leader
  - Solving the challenge needs some work to be done – ***Proof of Work (PoW)***

Why someone would want to be the leader?

Earn money (bitcoin) by solving the puzzle!

Mining a Block: The Reward

Mining a Block: The Reward

The Economics behind Reward

Encourage the community to participate in the mining through incentivization

The Economics behind Reward

Encourage the community to participate in the mining through incentivization

Produces new Bitcoins in the System
(Similar to a Minting new Coins)

The Economics behind Reward

The Bitcoin network works like a Reserve Bank to regulate the flow of Money (Bitcoin) in the market, but without explicit governance

Blockchain 1.0: Distributed Ledger

- Use of the **Distributed Ledger Technology** (DLT) to design the "Money of the Internet" -- Bitcoin and other cryptocurrencies

Blockchain 1.0: Distributed Ledger

- Use of the **Distributed Ledger Technology** (DLT) to design the "Money of the Internet" -- Bitcoin and other cryptocurrencies
- 3rd January 2009: Nakamoto mined the first block of the Bitcoin network (called the genesis block)
  - 2013: Coinbase reported selling US$1 Million worth of Bitcoin
- Many other cryptocurrencies have been evolved after that
  - Ethereum
  - Litecoin
  - …

The Price of Bitcoins

- Bitcoin value increased drastically over time
  - May 2010: < $0.01
  - April 2014: $340 - $530
  - December 2017: ~$13800

  - Today (24 Sept, 2021 10:30 am): **$44,285.50**

Bitcoin Millionaires

Popularity of Cryptocurrencies

Popularity of Cryptocurrencies

Popularity of Cryptocurrencies

Growing interests in developing decentralized applications (Dapps)

What are these Dapps?

- DLTs can contain information beyond financial transactions
  - What about submitting an executable code as a transaction?

- Not a new idea, people already knows about **Remote Code Execution** or **Code Injection**

What are these Dapps?

- DLTs can contain information beyond financial transactions
  - What about submitting an executable code as a transaction?

- **Transaction gets executed ==** Your code is getting executed
  - And you have consensus on the code execution !

What are these Dapps?

- DLTs can contain information beyond fin
  - W
    tr
- Transa ecuted
  - A !

Smart Contacts

Will see them in the next lecture!

Thank you