Lets Upgrade

#LETSUPGRADEADVANCEPROGRAM

BLOCKCHAIN PROGRAM

Batch 1

DAY 2

October 04th 2020

1:00 PM

letsupgrade.in/advance/blockchain

Agenda Day 2 -

1. Demo with Anders.com
2. Knowing technical terms
3. BitCoin & Crypto
4. Types of Blockchain in detail

Block **Number -1**=>

B.No. +Previous Key + **Data +** **Nonce**

= **x** (C)

x is the Number of 0 required in the Beginning

Assignment 4 - Self based

Insert your own data in the Distributed Blockchain Example - https://andersbrownworth.com/blockchain/distributed

And mine it completely end to end all the levels and make a note of your mining time, change the data density to check if it takes more time to mine if the data is more.

And document your learnings from the experiment over - https://community.letsupgrade.in/group/blockchain-sept-2020

Why n Zeros are required in the start of Hash ?

- These n Number of zeros are required for Mining
- Mining is only a part of PUBLIC Blockchain
- So only for Public Blockchain we need that concept of n 0 in the beginning

Why mining is required in Public Blockchain

- Game theory is involved in Public Blockchain

- Keep on storing the data in your machine, I will give you an opportunity to win Rs. 5+ Lakhs every 10 min.

1. I am owning a Cycle Company
2. I manufacture 5 Cycles per day,
3. Due covid my cycles are not getting sold
4. So I decide, to still continue the production but store it in my parking lot or home
5. My parking lot is full, so i call u my frnd and I say that hey please park my cycles at ur home
6. Now as ur parking lot is also full, u will ask me to take away the cycle
7. But if I say, that Hey Frnd, please do something I will give Rs. 100 per day for each cycle u store.

Store the data in your computer every 10 min.

You will get a new Block/Data copy, which you need to store that in your PC

~~You will get some money for each block u store~~

Please store the data, every 10 min. You will get access to win INR 5 lakhs, based upon a math problem which you need to solve

Y 4 0's ??

We know the value of Block Number, Data to be store and Previous Key,

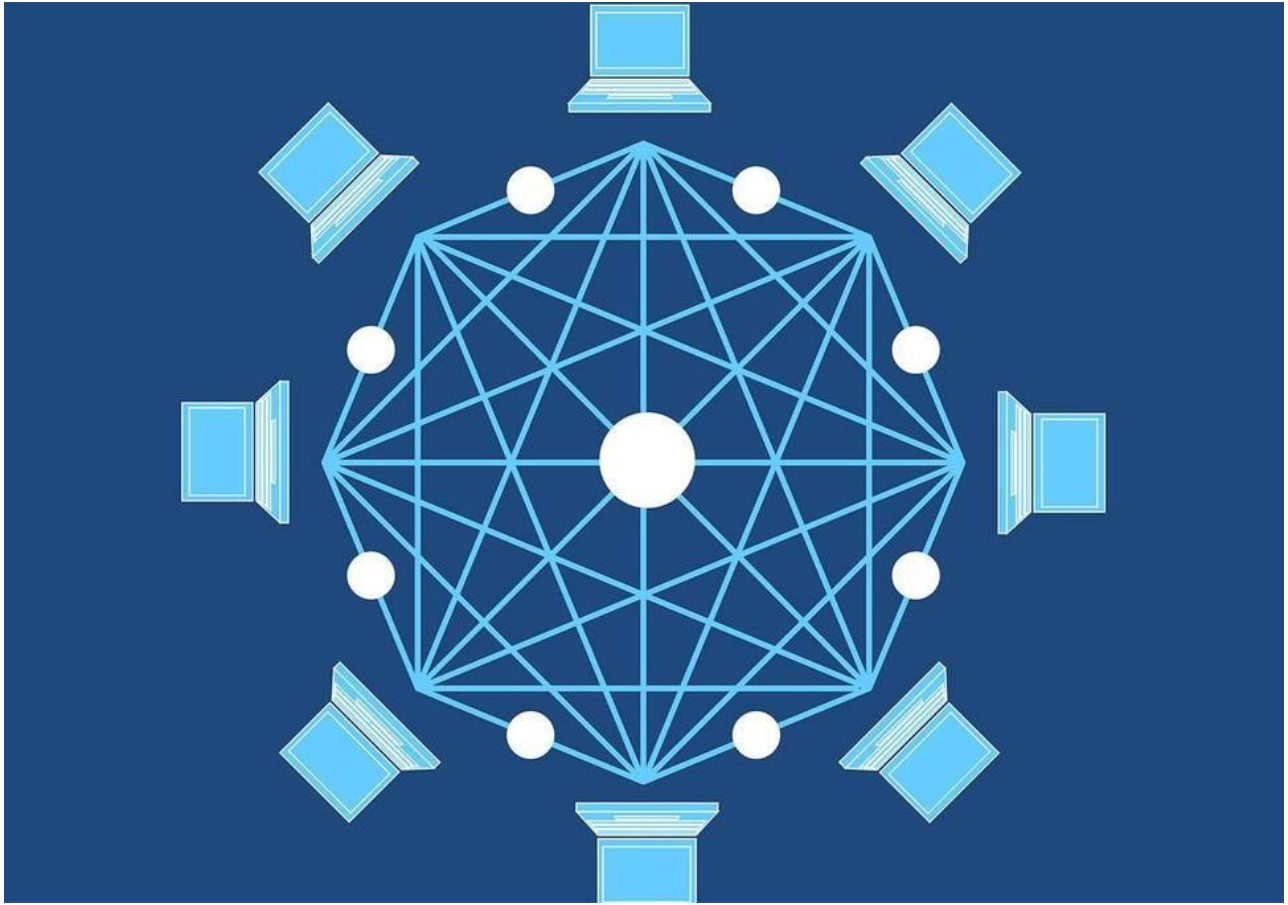
THis whole Numbers 0 are required for, the every 10 min. Mining game for storing the data

We can have any number of required 0's in the begin, but in case of BitCoin Network it is somewhere near 16 zero right now,

Consensus

It is related to 51% rule in Blockchain

It is simple voting for checking which data is correct and can be provided to the rest of the network



Distributed Network of computer where blocks are stored

“This mix of Technologies will create much wanted transparency and trust in system by eradicating middle man ”

Blockchain Council

Types of Blockchain ?

- Public Blockchain - Ethereum, Bitcoin - Mining
- Private Blockchain - R3 Corda
- Consortium Blockchain - Multi Chain, Hyperledger

Public Blockchain

1. Public blockchain is not governed by any industry or anyone it is been stored and maintained by Individuals

2. It has Mining involved in it

3. Ethereum and BitCoin

Private Blockchain

- This is a Blockchain type which been governed by a Private Company

- It costs more than Public Blockchain, but if the required resources are there, we can afford it.

- R3 Corda

Consortium/ Hybrid Blockchain

- It is governed by a Group of Private Stakeholders/ Orgs.
- It is kind of Shared resources which is hosted by all the stakeholders, and they all store the data in it
- Hyperledger and Multichain

Disadvantages of Blockchain

- High utility of the Electricity
- Mining is costly
- Resources used are more and more than required in traditional way.

Where can we use Blockchain ?

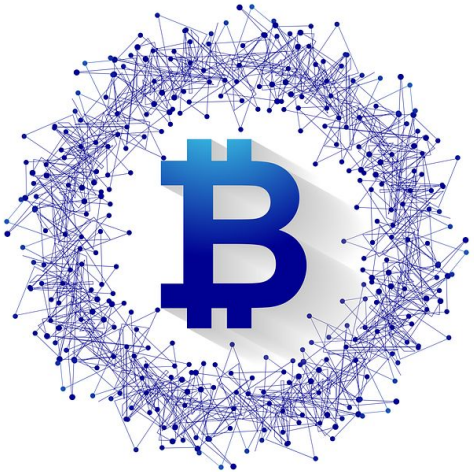
- Cryptocurrency (Bitcoin, ethereum, Altcoin, Litecoin, and 1540 currencies)
- Smart Contract -
    - Smart Contracts, also known as Smart Code or Smart Property, are computer protocols that can act as a contract. A Smart Contract can handle autonomously the enforcement and fulfillment of a contract without needing a third party to oversee that the contract is executed.
- Digital Voting
- Government Registration of land
- Supply chain management & Transportation (https://newsroom.ibm.com/2018-08-09-Maersk-and-IBM-Introduce-TradeLens-Blockchain-Shipping-Solution#:~:text=TradeLens%20is%20the%20result%20of,and%20spur%20industry%2Dwide%20innovation.)
- And Many

What makes Bitcoin so much Loveable?

- Works on Decentralized network
- Can send currency peer to peer
- No fiat currency needed
- No single point of failure
- More secure
- Less Prone to frauds & Tampering

Bitcoin - Cryptocurrency ?

- Bitcoin is a digital assets which can be bought, sold and Transferred over internet easily.
- It’s just like gold, silver, and diamonds
- It can be also used as Digital Currency.
- No Banks are needed anymore.



Bitcoin Mining ?

2123 + 678 + 675 +5732 + 5321 - 65753 - 467777563

=> 5 lakhs to Winner

How Does Public Blockchain Mining Works ?

1. Step 1 - How to generate a Hash
2. Step 2 - What all things a Block contain
    a. Block number
    b. Mining Key or Nouce
    c. Data
    d. Hash
3. Step 3 - We need N number of 0 in the Hash Key

4. Mining => A + **B** + C = D **(D should have N number of 0 in the Beginning)**
5. Y? N - 0's ?

How Mining Works?

- **Y 4 0’s ?** - these zeros can be varied based upon the network like ethereum, bitcoin and etc.
- We require these number of zeros for making the math problem complex day by day,
- And the person or node which gets the perfect nounce first will be awarded the bitcoins/ Cryptocurrency as per the rules.
- Once the node finds out the nocuce it is been circulated in the whole bitcoin network and others do validate it. (Just remember the Nishant example)

Bitcoin Mining

- To solve complex math problems and find solution for the cryptographic block.
- The first person to mine a blockchain is rewarded some amount of bitcoins
- New bitcoins are generated into the system by this method
- When Bitcoin Coin network gives away a new bitcoins to a Specific Node after every 10 Min. , this is a way to generate New Virgin BitCoins into the BitCoin Network
- Which these Miners can sell to common people later

Steps which are involved in mining ?

1. Trxns of BitCoin are happening in real-time between two peers
2. These Trxsn are grouped and sent in a Block
3. These Blocks are then sent to all the miniers for finding perfect nonce, which gets required number of 0 in the beginning
4. The person finding the perfect nonce first will get rewarded with X number of New Virgin BitCoins
5. Those Virgin BitCoins are then out in the market for rotation

6. This cycle continues and then we have our bitcoins running and new BitCoins are generated like this.

Lets see a real bitcoin Example

0.00000001 BTC

Satoshi - The smallest unit of Bitcoin possible.

Limited supply of bitcoins to increase demand

- The total number of bitcoins which will ever be available is 21 million bitcoins , last bitcoin will be mined sometime in the year 2140.
- But now we have 17 Million already mined till date

How this is possible ?

- The " **Halving** " effect
- 50 BitCoins - 3rd Jan 2009 - 3rd Jan 2012
- 25 Btc - 4th Jan 2012 - 3rd Jan 2016
- 12.5 Btc - 4th Jan 2016 - 3rd Jan 2020
- 6.25 BTC - 4th Jan 2020 - 3rd Jn 2024
- 3.125 BTC - 4th Jan 2024 - 3rd jan 2028

Smart Contract ?

- Contracts - a legal bond b/w two or more parties

- Smart Contract -
  - Certain piece of code(contract) which is stored inside the Blockchain network, when certain conditions are met they are executed on their own

Computer Programs which are run all the time at certain address inside the BLC Network, which can execute on it's own when some conditions are met wrt the contract