Lets Upgrade

#LETSUPGRADEADVANCEPROGRAM

BLOCKCHAIN PROGRAM

Batch 1

DAY 1

October 03rd 2020

1:00 PM

letsupgrade.in/advance/blockchain

Learning Path for Blockchain

1. Basics of Blockchain - Day 1
2. Cryptocurrency works - Day 2
3. Ethereum Theory - Day 3
4. Ethereum Practical - Day 4 & 5
5. Ethereum based 4 Projects - Day 6,7,8
6. Hyperledger Theory - Day 9
7. Practical Implementation of Hyperledger - Day 10,11,12,13, 14, 15
8. R3 Corda - Theory - Day 16
9. R3 Corda - 2 Projects - Day 17,18
10. Projects & Buffer days - (Remaining 6 Days)

Timings for the program

1. Weekends program (Sat & Sunday)
2. 12 Weeks program
3. Start from the scratch
4. 2-3 Hours each weekend
5. Community for Articles and Formal Questions & Discord group for doubts and other material
6. Help your peers to get LU Coins

Why we should learn Blockchain ?

- NO Hacking
- Huge Security Boost
- Verifiable
- Data Transparency
- Decentralized

What is Blockchain ?

- Internet is Hackable
- Authenticity of the data which is uploaded ?
- Tampering of the data once it is uploaded ?

To remove this all we need a system which stops the above mentioned points, so to do that we have created Blockchain

Assignment Number 1 -

Read the White Paper which Satoshi Nakamoto Had Published

https://bitcoin.org/bitcoin.pdf

What was the actual problem due to which Blockchain appeared ?

International banking crisis with the collapse of the investment in 2008

Assignment Number 2 -

https://en.wikipedia.org/wiki/Financial_crisis_of_2007%E2%80%932008

International banking crisis

Happened just because of only one particular bank giving away more loans

Satoshi Nakamoto

Satoshi Nakamoto is the author of the white paper "Bitcoin: A Peer to Peer Electronic Cash System".

As of today, no one knows who Satoshi Nakamoto is or even if he is one person or a group of people.

31th October 2008

Why Bitcoin: A Peer to Peer Electronic Cash System ?

1. We don't want any third party providing TRUST in the internet system
2. We wish to make our connected system so nice that we are fully able to trust the Internet system it self.
3. To make a Financial system which can run by the end consumers it self not by the bank people

What is the Problem with internet ?

1. Authenticity ?

2. Security ?

3. Need of Powerful third party for trust ?

Blockchain

Blockchain

A mix of Technology - Distributed Database & Cryptography where information is

- Verifiable
- Tamper-proof
- Immutable

- **Internet 2.0**

Blockchain

A mix of Technology - Distributed Database & Cryptography where information is

- Verifiable
  - You can check the data origin via Blockchain Network
- Tamper-proof
  - Even if you hack into the network and change few values, it will get back to normal state
- Immutable
  - It's unchangeable and non-modifiable (Once the data is written, it is there in forever)

- **Internet 2.0**

- Verifiable - Data which is there in the internet can be verified but even we can encounter the fake data

- You guys are owning one car of XYZ,
- the serial number of the car is in DB to verify it weather it is correct or wrong
- What are the database behind it, - SQL
-
- Car mechanic frnd + Me (Who has access to that DB, or I am hacker)
- Frnd will make one fake part of the car or fake car
- Sai can make the entry of the part my frnd made or sai can i actully go and modify some data in the SQL

- Unchangeable -

- I am having a university somewhere,
- You are a student of my university
- You passed out but your frnd got KT and failed
- You got a hacker/ he got access to the DB and
- Modified his entry as I AM Passed with 75%

CRUD - Create + Read + Update + Delete

- Tamper-proof

  - Iphone - Premium brand mobile phone
  - Jail break, a abroad phone where that is costed less is been jail breaked and the entry is modifed in the Companies DB with the help of some, XYZ people
  - Database is Tramperable

- Immutable

- I have Launched a Website,
- That is on a server
- My some important Data is also stored in that server,
- Somehow my server got deleted and i don't have any backup
- I need to prepare it back again
- Vanishing is known as Mutable
- Not Vanishing is know as Immutable

“A Blockchain is a constantly growing ledger that keeps a permanent record of all the transactions that have taken place, in a secure, chronological and immutable way in decentralized distributed network”

Why Internet is failing ?

1. Trust
    a. Data getting deleted easily
    b. Data getting modified easily

How normal DB Looks like, what are the challenges in them for internet and how to remove them

CRUD

Create Read Update Delete

Normal Database ...

Sr. No	Name	DOB	Marks
1	abc	1-1-98	78
2	ori	1-2-89	95
3	ghi	1-3-64	83
4	xyz	1-8-93	75
...	....	....	....

More about SHA -

https://www.movable-type.co.uk/scripts/sha256.htm

Create & Read

1. We need a DB which can store Records with Create and Read Options only

1. NON - Updatable & 2. Non - Deletable

1. Break all the rows in bundle of 10 each
2. Give Block Numbers
3. Now Generate SHA for the content in the block
4. Paste the sha inside the Previous Block signature in the upcoming block
5. We will create copy of the same database in 100 places
6. [Imaginary part] - all the changes in the main db will reflect in real time to all the other instance

Assignment - 3 (Self)

Home work -

https://andersbrownworth.com/blockchain/distributed

Step 1 -

- Instead of Having a full unlimited individual SQL DB
- Can we break the DB to 100 100 records only

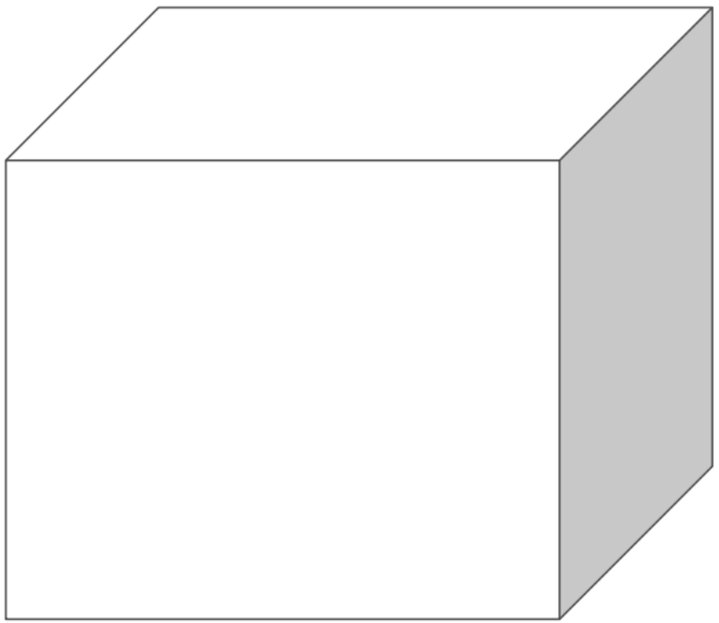
Step 2 -

Can we get a Unique Fingerprint of each Data Table of 100 ???

Yes we can get a Unique Fingerprint of the data using SHA 256

Now at least we are able to track if anything is getting changed in the data

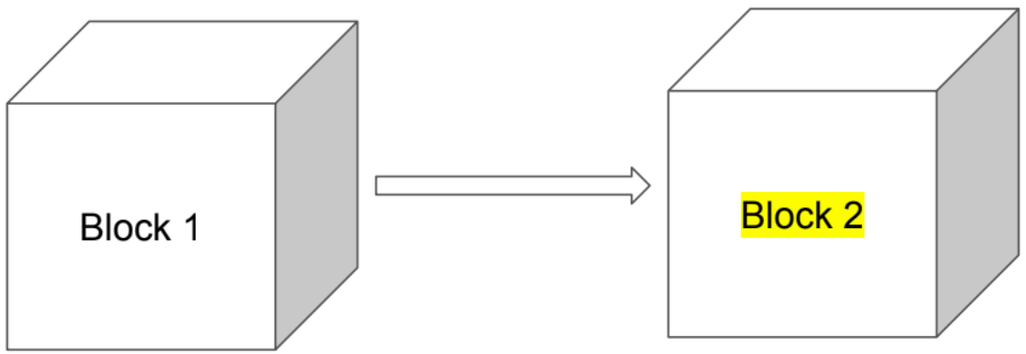
Block ?



A Block contain

- Block Number
- Transaction records
- Previous Block Signature

Blockchain ?



SHA-256 Signature of content in block - 0000acbdefxzancba

A Block contain

- Block Number - 2
- Trans Record
  Any Important Data you want to store
- Previous Block Key
  0000acbdefxzancba
- Mining Key

:. SHA = Secure Hash Algorithm

Block 1 => 0 + B = C

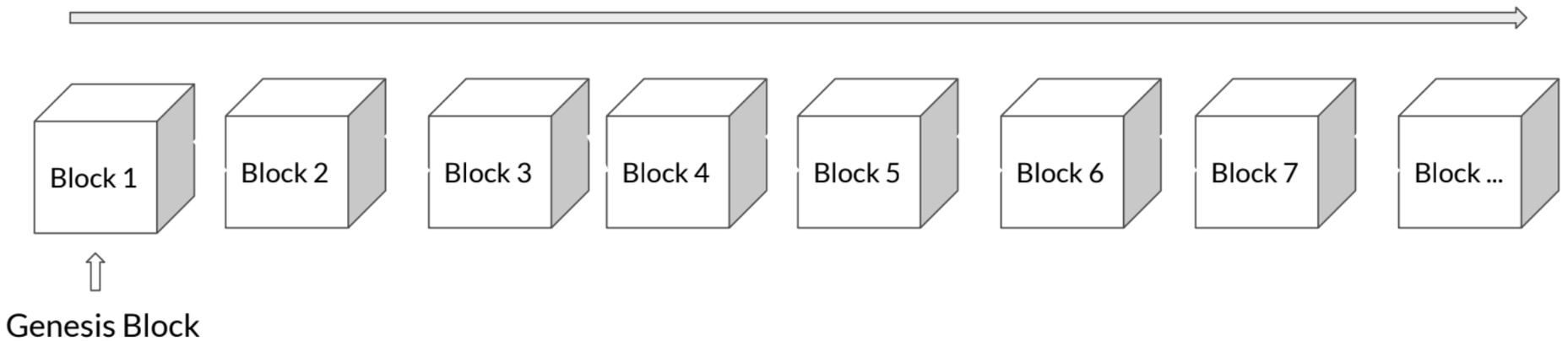
Block 2 => C + D = E

Block 3 => E + F = G

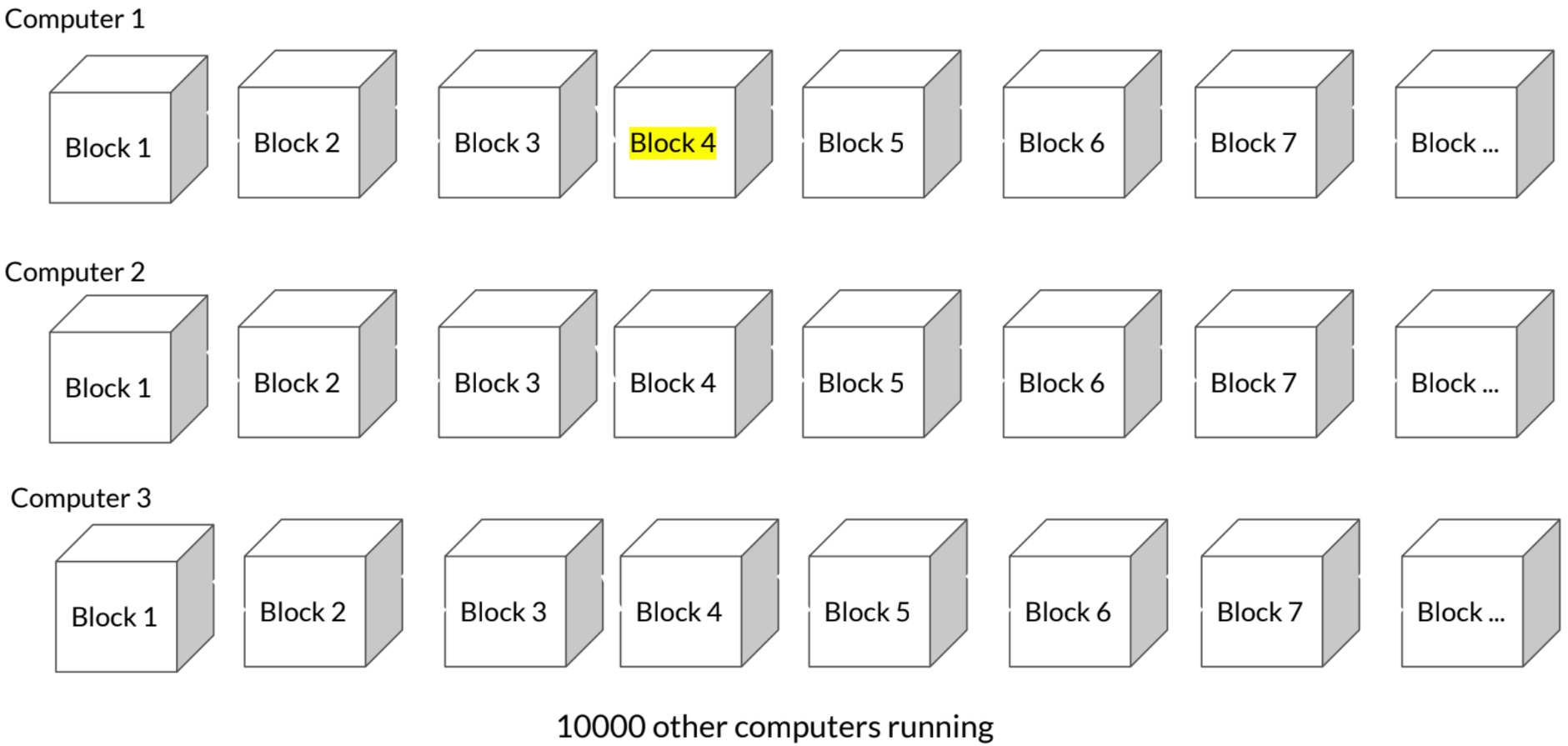
B, D & F are Data to be stored

C, E & G are the SHA(FP) keys

Blockchain ...


Block 1
Block 2
Block 3
Block 4
Block 5
Block 6
Block 7
Block ...
Genesis Block

Blockchain in action with peers



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