Week 1 - Orientation Class [2 Aug 2024]

> **Timing** - Every Friday 7:30pm to 9:30pm IST
> Class Slides - DailyCode (100xdevs.com)
> Class Video - Take your development skills from 0 to 100 and join the 100xdevs community
> Assignment - Web3-Cohort---Orientation-6 Assignement Slide

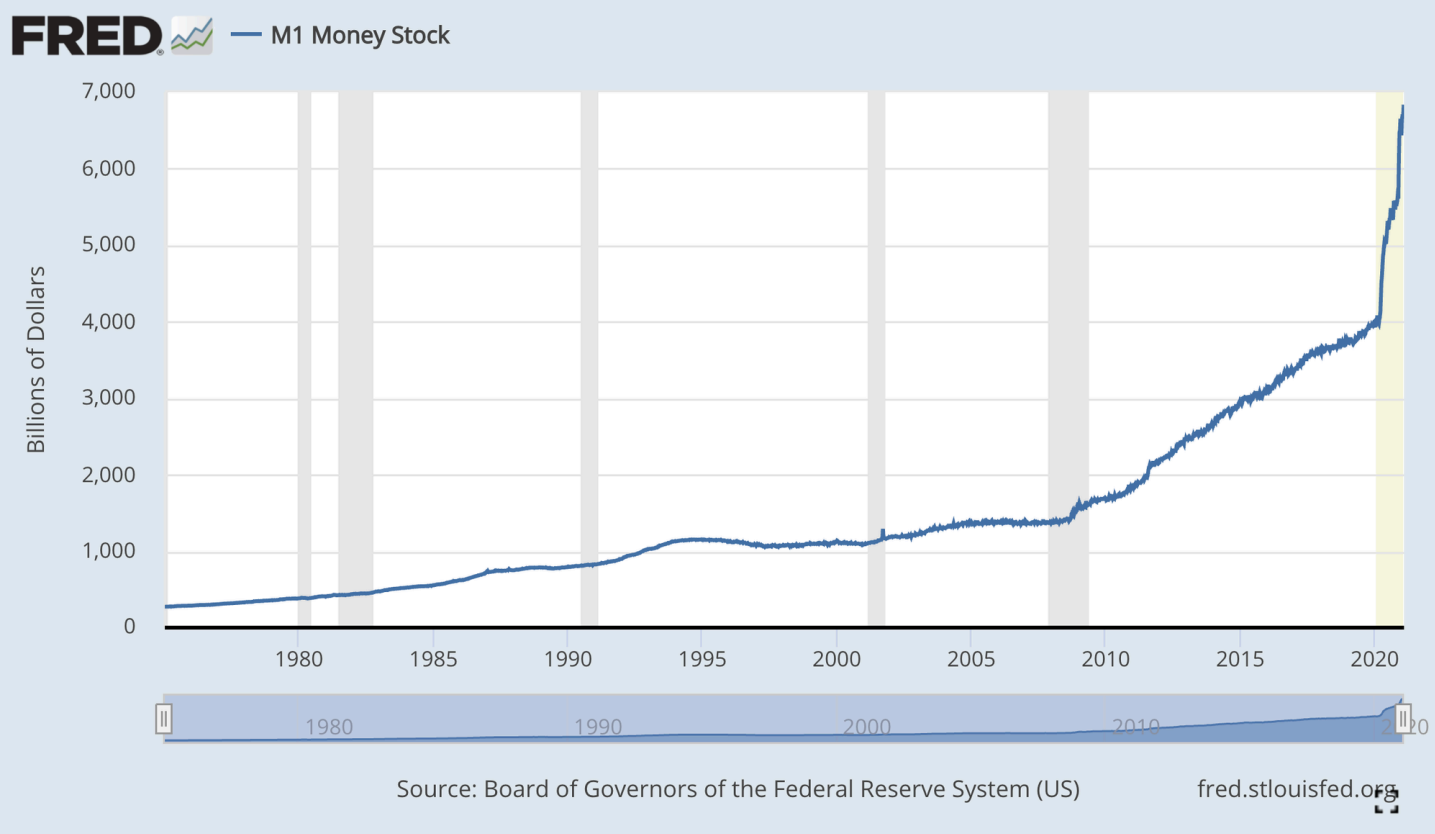
> **Syllabus** - Notion – The all-in-one workspace for your notes, tasks, wikis, and databases. (100xdevs.com)
> Harkirat Background - https://www.youtube.com/watch?v=gYK8azCYjnU

▼ Repositories to keep an Eye on during Cohort

1. https://github.com/code100x/stake - By **Harkirat Singh**
    1. Gambling website
2. https://github.com/code100x/tiplink - Led by **@cb7chaitanya**, mentored by Harkirat

▼ Solana Hackathon [Ends on 31st August 2024] details and project ideas

DailyCode (100xdevs.com)



Why Blockchains?

- **Inflating Currencies**: Central banks can print more money, leading to inflation.

- **Inflation Issues**: Printing money and distributing it to everyone causes inflation, reducing the value of money.
- **Random Bailouts**: Governments bail out failing institutions, creating unfair economic conditions.
- **Need for Better Currency**: A currency that is open, transparent, and immune to arbitrary printing is essential.
- **Fractional Reserve Banking**: Banks only keep a fraction of depositors' money on hand, which can lead to financial instability.
- **Currency Depreciation**: Traditional currencies lose value over time due to inflation.
- **Lack of Backing**: Modern currencies are not backed by tangible assets like gold or silver.
- **Recommended Watching**: *The Big Short* (film) provides insight into financial crises and the need for better financial systems.

What is Blockchain?

Blockchain is a decentralized and distributed digital ledger that records transactions across many computers, ensuring data security and transparency. It operates without a central authority, using cryptographic techniques to verify and add new transactions.

Main Characteristics of Blockchain:

1. **Decentralization**: Blockchain is managed across multiple nodes (machines), ensuring no single entity controls the data. Each node stores the entire blockchain, providing access to all data on the blockchain.
2. **Immutability**: Once data is recorded on a blockchain, it cannot be easily altered or deleted, ensuring the integrity of the records.
3. **Transparency**: All transactions recorded on a blockchain are visible to all participants, promoting openness and trust.
4. **Consensus Mechanisms**: Nodes in the network follow consensus mechanisms (e.g., Proof of Work, Proof of Stake) to validate transactions and add them to the blockchain.

Purpose of Blockchain:

The purpose of blockchain is to create a **network of computers that agree upon a common state of data**. This ensures that:

- Any person or organization can participate in the process.
- No single person or organization can control the process.

Blockchain enables secure, transparent, and tamper-proof transactions without the need for a central authority.

How to Create a New Currency with Blockchain

There is a need for **trustless**, **anonymized**, and **decentralized** form of money, blockchain solves it for us.

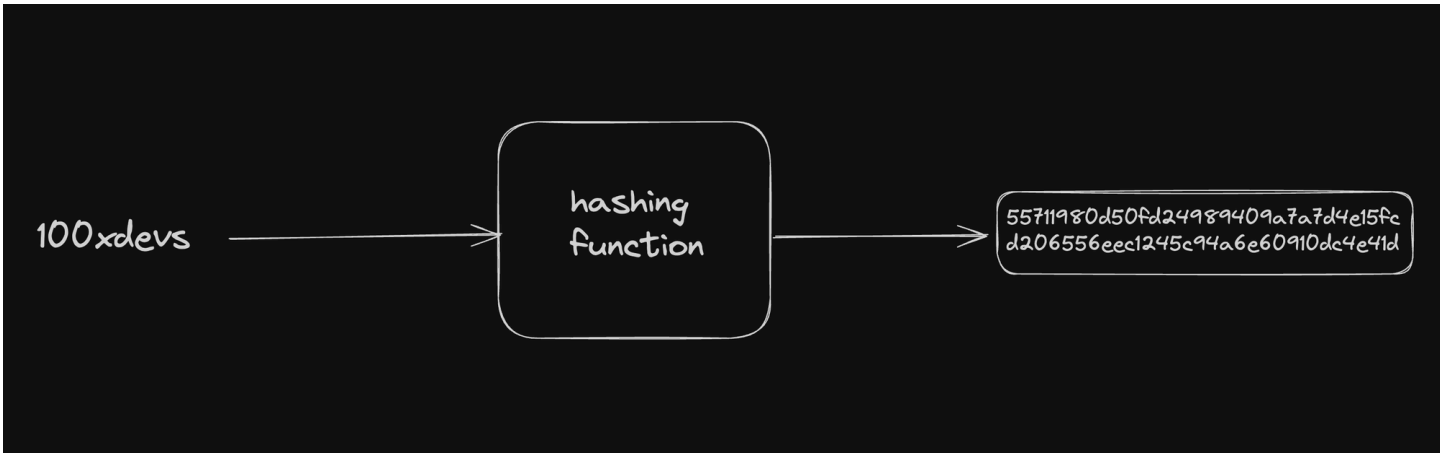
Key points:

1. **Avoiding Central Ownership**:
    1. Centralized control over currency can lead to misuse of power and lack of transparency.
    2. Blockchain technology eliminates the need for a central authority, distributing control among multiple nodes.
2. **Trustless System**:
    1. Blockchain enables the creation of currency without needing to trust a central authority.
    2. Transactions are verified by consensus mechanisms, ensuring security and integrity.
3. **Anonymization**:
    1. Blockchain technology supports anonymized transactions, protecting the privacy of users while maintaining transparency of the overall system.
4. **Decentralization**:
    1. Decentralized money operates on a network of nodes, preventing any single entity from

having control and reducing the risk of manipulation or failure.

By leveraging these principles, blockchain technology allows for the creation of new currencies that are secure, transparent, and free from centralized control.

> 💡 Bitcoin - But how does bitcoin actually work? (youtube.com)
> Bitcoin whitepaper - Bitcoin: A Peer-to-Peer Electronic Cash System



Hashing

Transforms input data of any size into a fixed-size string of characters.

- **Properties**:
  - **Deterministic**: Same input always produces the same output.
  - **Fast Computation**: Hash value can be quickly verified for any data.
  - **Pre-image Resistance**: Difficult to reverse the hash function to find the original input.
  - **Small Changes in Input Produce Large Changes in Output**: Tiny input changes drastically alter the hash output.
  - **Collision Resistance**: Difficult to find two different inputs that produce the same hash output.
- **Example - SHA-256**:
  - **Secure Hash Algorithm 256-bit**: Produces a 256-bit (32-byte) hash value from any input.

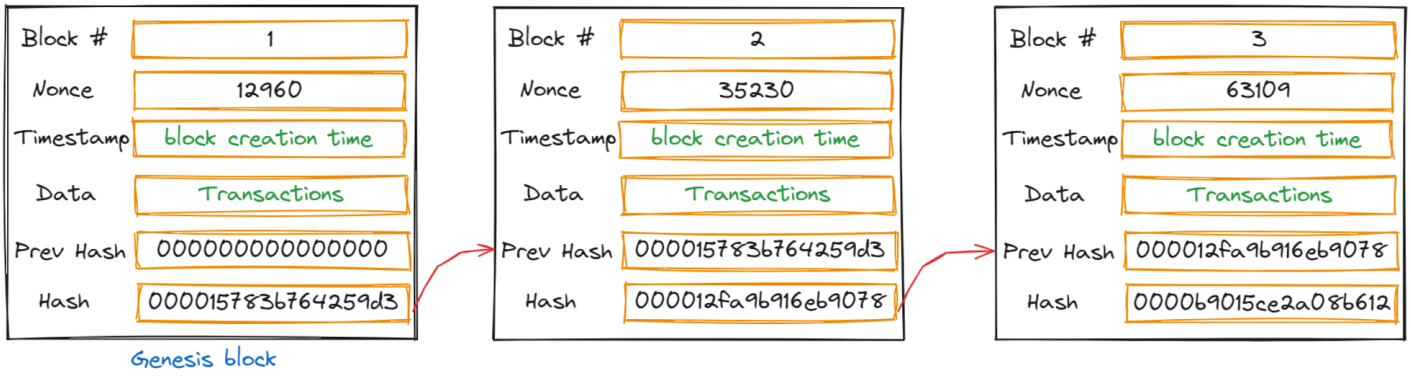
    ▼ **Code Example**:

```
const crypto = require('crypto');

const input = "100xdevs";
const hash = crypto.createHash('sha256').update(input).digest('hex');

console.log(hash)
```

💡 SHA256 - Online Tools (emn178.github.io)

Hashing vs. Encryption

- **Hashing**:
  - Converts data into a fixed-size string.
  - Irreversible (one-way function).
  - Used for data integrity verification (e.g., password storage, file verification).
- **Encryption**:
  - Converts data into a different format.
  - Reversible (two-way function) using a key.
  - Used for data confidentiality (e.g., securing communication, data storage).



How Does Blockchain Work?

- **Blocks**:
  - Data is stored in "blocks."
  - Each block contains:
    - A list of transactions.
    - A timestamp.
    - A cryptographic hash of the previous block.
- **Chain**:
  - Blocks are linked together in a chronological order.

- This creates a "chain" of blocks, hence the name "blockchain."

> 💡 Infographic - How Crypto-currency Works - Animagraffs
> Blochain Demo - Blockchain Demo (andersbrownworth.com)

Important Terms

- **Nonce**
  - A **unique number** that miners must find to produce a valid hash.
  - Used only once, it ensures the resulting hash satisfies the blockchain's difficulty conditions.
- Finding Nonce
  - **Miners and Compute Power**
    - Miners produce blocks in the blockchain.
    - The probability of producing the next block and earning the reward increases with more compute power.
    - Compute power is needed to calculate the correct nonce.
  - **Nonce and Proof of Work (PoW)**
    - The nonce is a number that, when added to the block data and hashed, produces a hash meeting the network's difficulty criteria.
    - The process of finding this nonce is known as **Proof of Work (PoW)**.
- **Consensus Mechanism**
  - A method ensuring all participants agree on the blockchain's state and the validity of transactions.
  - Acts as a rulebook for validating transactions and blocks.
- **Proof of Work (PoW)**
  - A **consensus mechanism** used in blockchain networks.
  - Requires solving complex mathematical problems to find the correct nonce.
  - Ensures the security and integrity of the blockchain by validating transactions and adding new blocks.