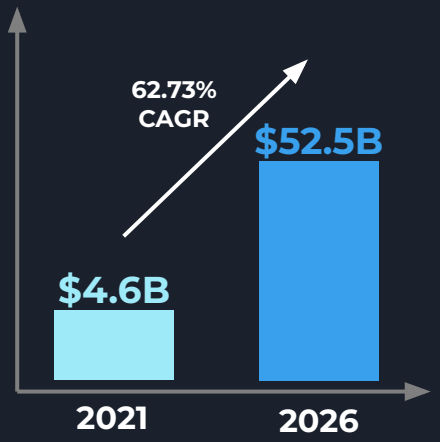
# Blockchain Basis and Machine Learning

Zhang Han
30/09/2022

# Why should you learn about Blockchain?

1




2


3

Source: Yahoo Finance

# Agenda

- Introduction To Blockchain
- Types of Blockchain Networks
- Bitcoin and PoW
- What Are Smart Contracts
- DApp on Ethereum
- How to Develop Smart Contracts?
- Blockchain and ML

# What Is Blockchain?

# A Blockchain Is

A type of decentralised database that stores information. These information is then linked to another block through cryptography.

# Blockchains VS Traditional Databases

Unlike traditional databases. **Blockchain's unique advantage** is that it collects information and data through blocks.

Hence, when these blocks are filled, they are then linked to a "fresh" block where the cycle continues. **This process is what forms a chain of blocks.** Hence the term Blockchain.

A new transaction is entered.

The transaction is then transmitted to a network of peer-to-peer computers scattered across the world.

This network of computers then solves equations to confirm the validity of the transaction.

Once confirmed to be legitimate transactions, they are clustered together into blocks.

These blocks are then chained together creating a long history of all transactions that are permanent.

The transaction is complete.

# Quiz:
# What are the following refers to in blockchain?

Computers that run the specific blockchain protocol

Contain transactions which are grouped together after each network consensus event emitted

Cryptographic mechanism that link blocks together, forming a chain of data with chronological orders and verified integrity

# Quiz:
# What are the following refers to in blockchain?

**Node -** Computers that run the specific blockchain protocol

**Block -** contain transactions which are grouped together after each network consensus event emitted

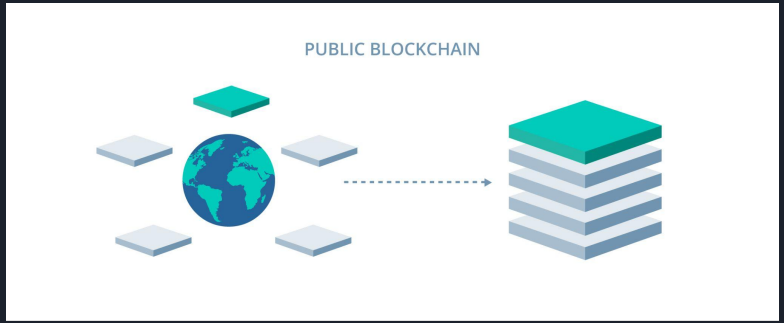
**Chain -** Cryptographic mechanism that link blocks together, forming a chain of data with chronological orders and verified integrity

# The Different Types Of Blockchain Networks

# Public Blockchains

## Permissionless

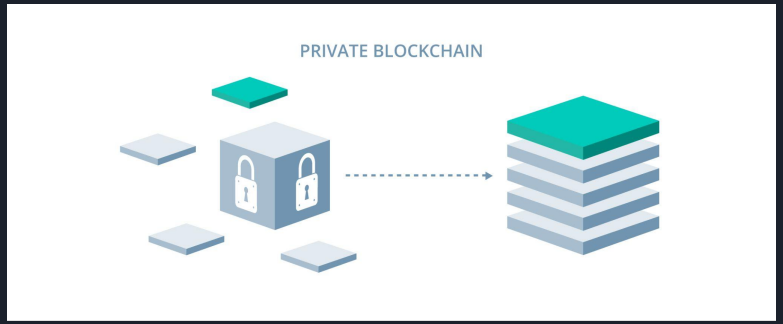
Anyone who is connected to the internet can join these public blockchain networks and become a part of it without the need to be granted authorization.



# Private Blockchains

## Centralised Network

Participants can join a private blockchain network only through an invitation where their identity or other required information is authentic and verified.



# Consortium Blockchains

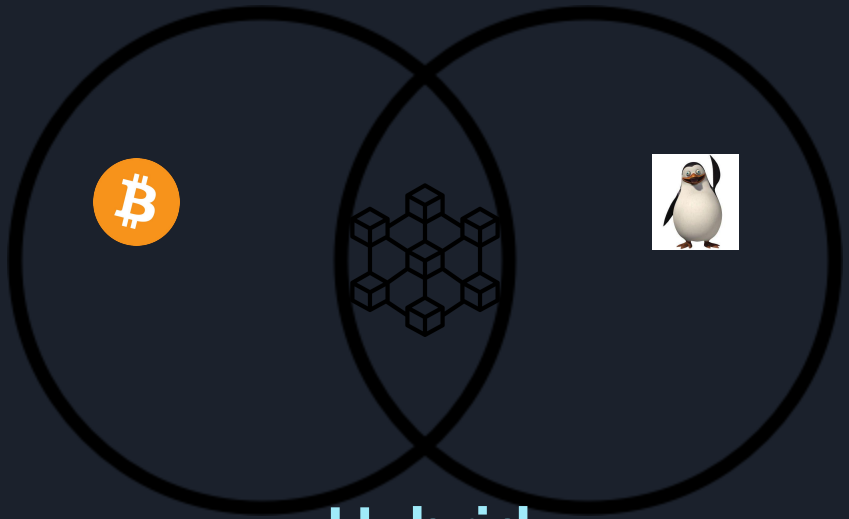
## Hybrid Distributed Ledger

With a consortium blockchain, companies are able to reap the benefits of increased security and privacy but at the cost of bad actors.

# Quick Snapshot

Permissionless

Permissioned



Hybrid

# Smart Contract VS Regular Contracts

**Speed, efficiency and accuracy**

Once the condition has been met, the contract is executed immediately. There is no for bottlenecks that come about from manual paperwork.

**Trust and Security**

Not only are blockchain transactions cryptographically secured, they are trustless as well. They is no need to question whether information has been altered for personal gains.

# Bitcoin and PoW

# The Birth Of Bitcoin

## 2009

Following the financial recession of 2008, on 23rd January of 2009, the world first saw Bitcoin’s ideologies laid out as a white paper, describing how the revolutionary cryptocurrency would work.

# The Founder(s) Of Bitcoin

## “Satoshi Nakamoto”

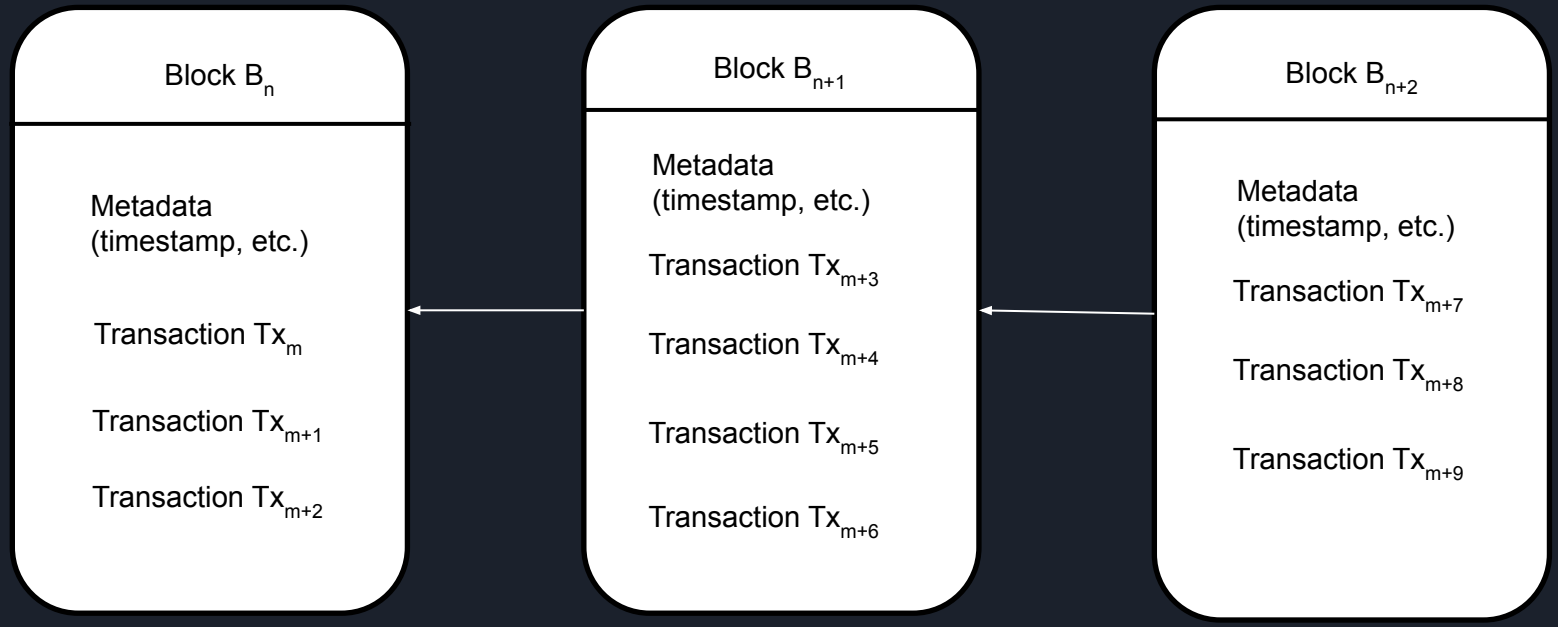
The white paper for Bitcoin was written by a person or a group of people calling themselves “Satoshi Nakamoto”. Till this day, no one knows who the real Satoshi Nakamoto is.

## Have You Ever Overpaid For Something?

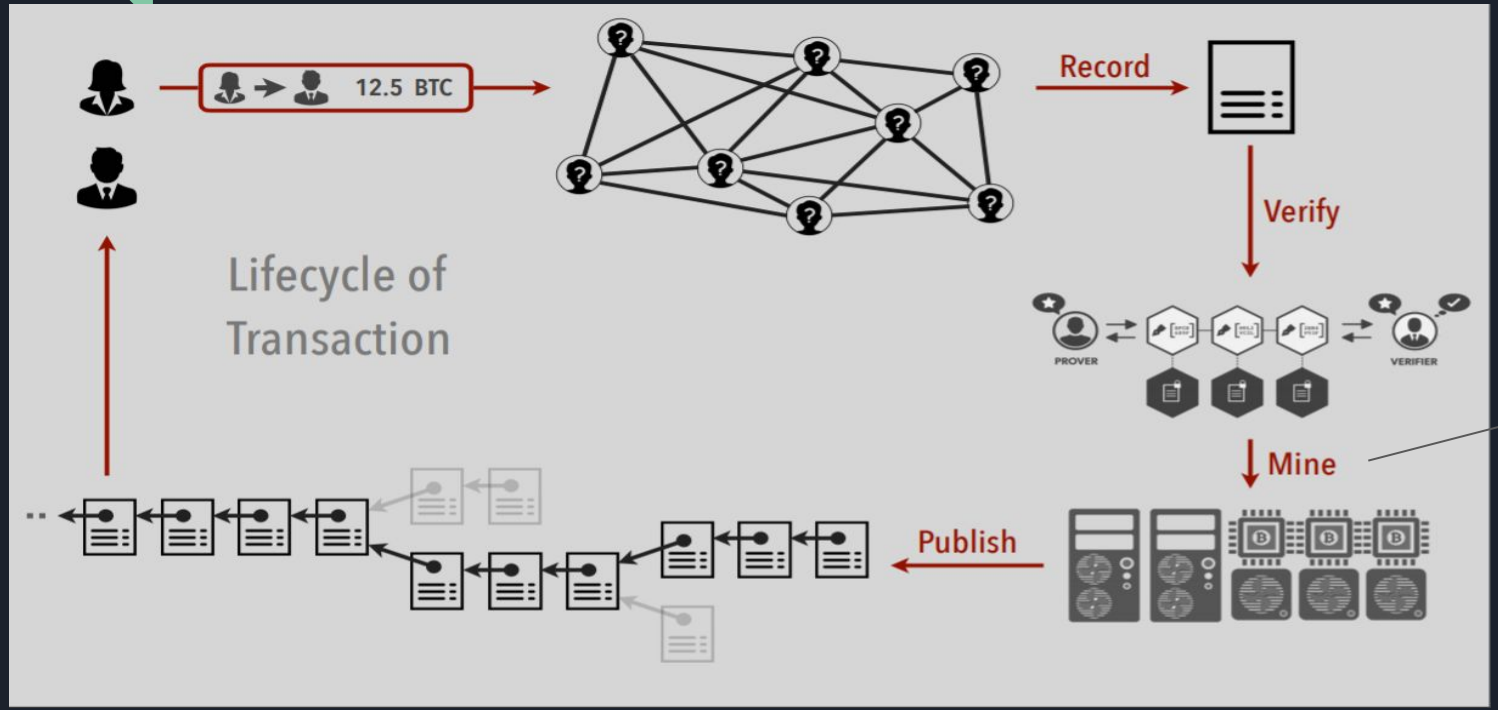
# Bitcoin Pizza Day

Laszlo Hanyecz famously paid a 10,000 bitcoins for two delivered Papa John’s pizzas.

# How Block-chained



# Lifecycle of a transaction




How does mining actually work??

# Hash function

A hash function is any function that can be used to map data of arbitrary size to fixed-size values

Link to witness the magic:
https://emn178.github.io/online-tools/sha256.html

# Mining Mechanism - Proof Of Work

The Lucrative Mining Puzzle

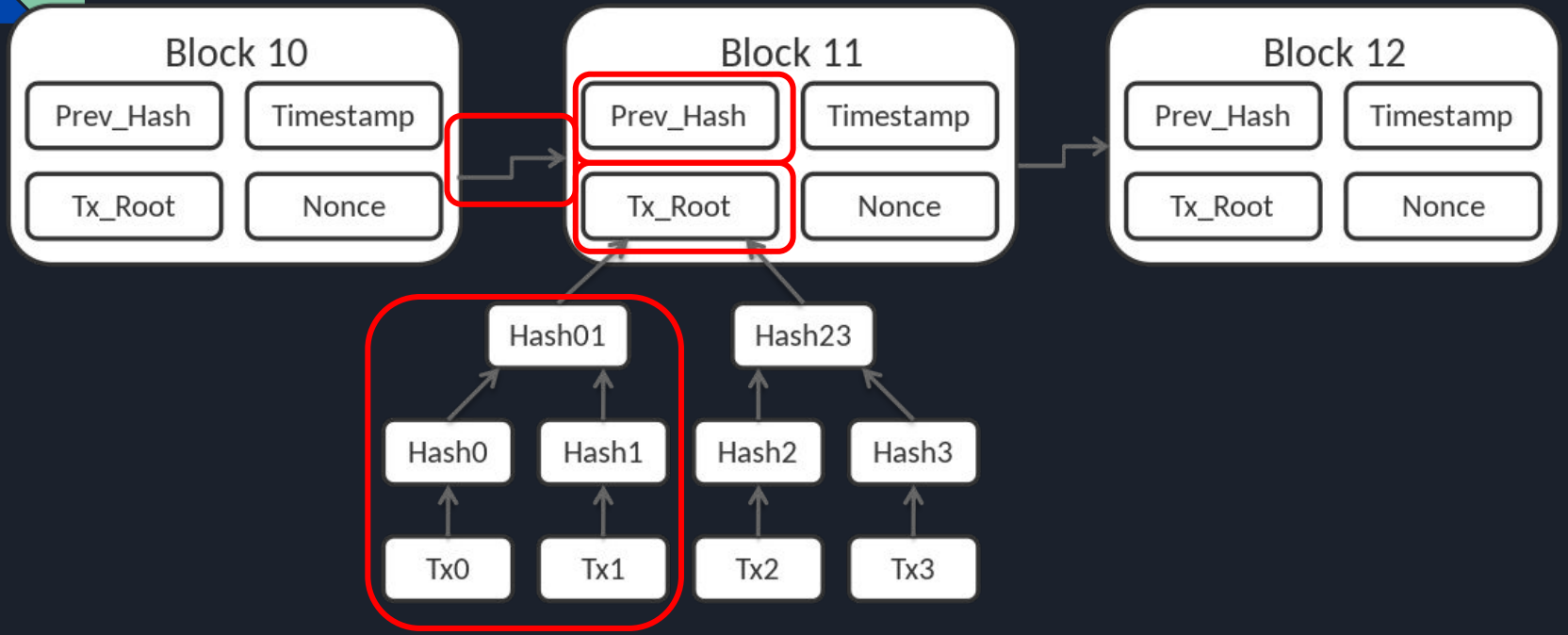
Dear miners, if you want to become the proposer of next block, please find a number N such that:

Hash ( N || content of the block) < target

There will be reward to the one who finds the solution first!

Hard to find (brute force), trivial to verify!!!

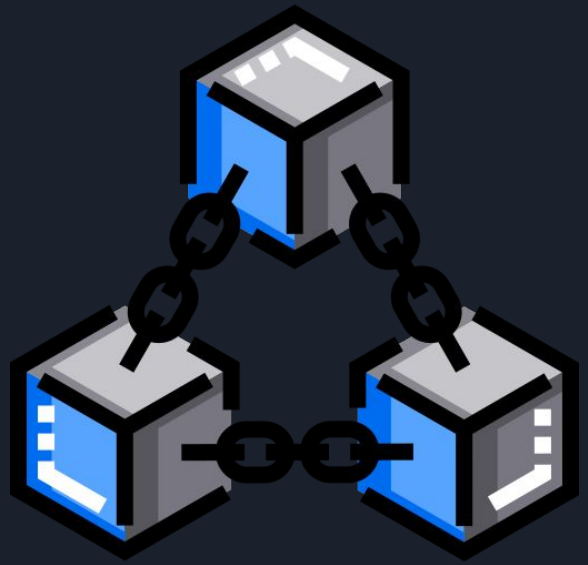
```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```


Block 10
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 11
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 12
Prev_Hash
Timestamp
Tx_Root
Nonce
Hash01
Hash23
Hash0
Hash1
Hash2
Hash3
Tx0
Tx1
Tx2
Tx3

# What Are Smart Contracts?

# Smart Contracts Are

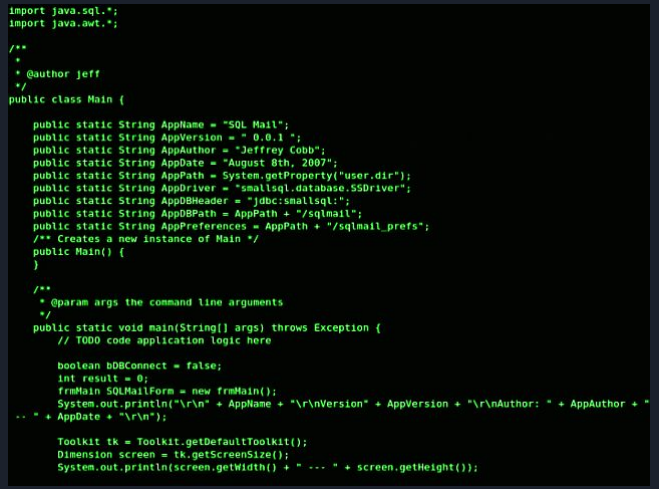
A simple program that's stored on a blockchain that runs when **predetermined conditions are met**. These smart contracts are used to **automate the execution of an agreement** so that all participants can be immediately certain of the outcome.



# How Do I Write A Smart Contract?

Here are the top few programming languages that you'll need to learn in order to write your very own smart contract.

1. Solidity
2. GoLang
3. Rust
4. JavaScript



```
import java.sql.*;
import java.awt.*;

/**
 *
 * @author jeff
 */
public class Main {

    public static String AppName = "SQL Mail";
    public static String AppVersion = " 0.0.1 ";
    public static String AppAuthor = "Jeffrey Cobb";
    public static String AppDate = "August 8th, 2007";
    public static String AppPath = System.getProperty("user.dir");
    public static String AppDriver = "smallsql.database.SSDriver";
    public static String AppDBHeader = "jdbc:smallsql:";
    public static String AppDBPath = AppPath + "/sqlmail";
    public static String AppPreferences = AppPath + "/sqlmail_prefs";
    /** Creates a new instance of Main */
    public Main() {
    }

    /**
     * @param args the command line arguments
     */
    public static void main(String[] args) throws Exception {
        // TODO code application logic here

        boolean bDBConnect = false;
        int result = 0;
        frmMain SQLMailForm = new frmMain();
        System.out.println("\r\n" + AppName + "\r\nVersion" + AppVersion + "\r\nAuthor: " + AppAuthor + "
-- " + AppDate + "\r\n");

        Toolkit tk = Toolkit.getDefaultToolkit();
        Dimension screen = tk.getScreenSize();
        System.out.println(screen.getWidth() + " --- " + screen.getHeight());
```

# Example: The Vending Machine Smart Contract


If you give me 1.20 SGD, and press this button, you will get a 100 Plus Bottle. I promise!!!!

# Example: The Vending Machine Smart Contract


If you give me 1.20 SGD, and press this button, you will get a 100 Plus Bottle. I promise!!!!

Behind the scene:

If money received == $2.50

&& the button on “100 Plus bottle” is pressed

then release 100 Plus

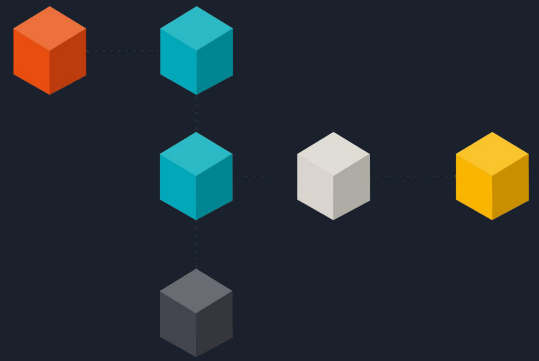
# How to Develop Smart Contracts?

# DApp on Ethereum

# What is Ethereum?

## Blockchain Protocol

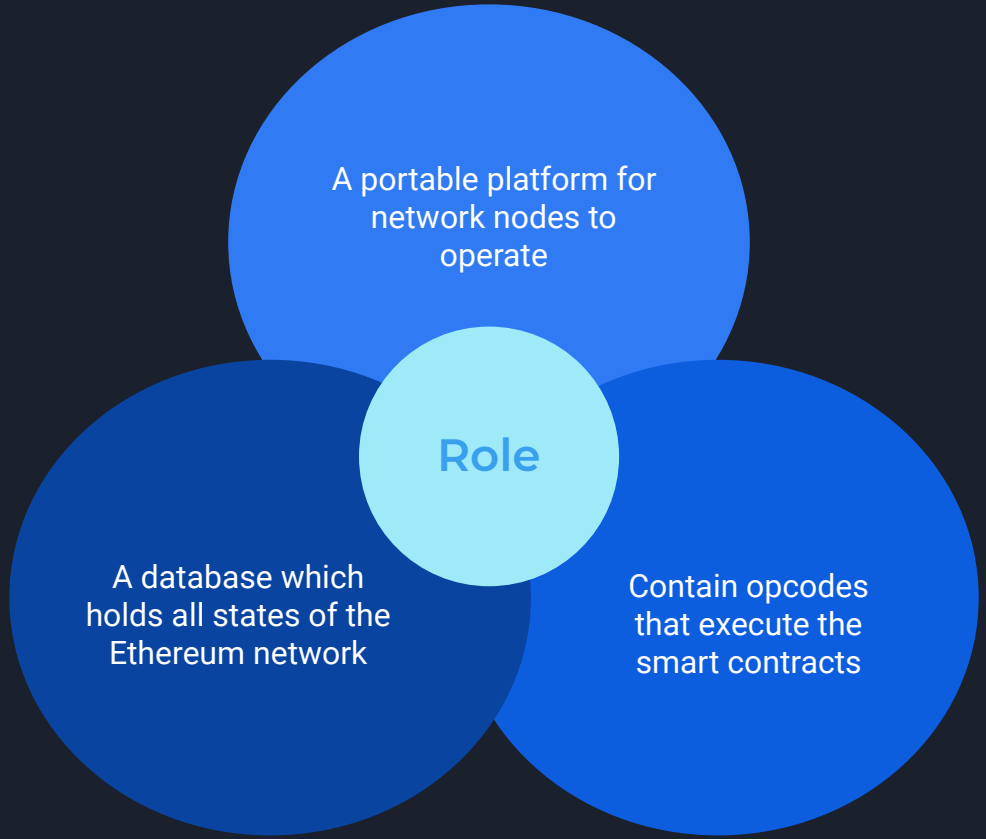
- Native currency (ETH)
- Consensus mechanism (PoW → PoS)
- Storage structure, protocol OpCode

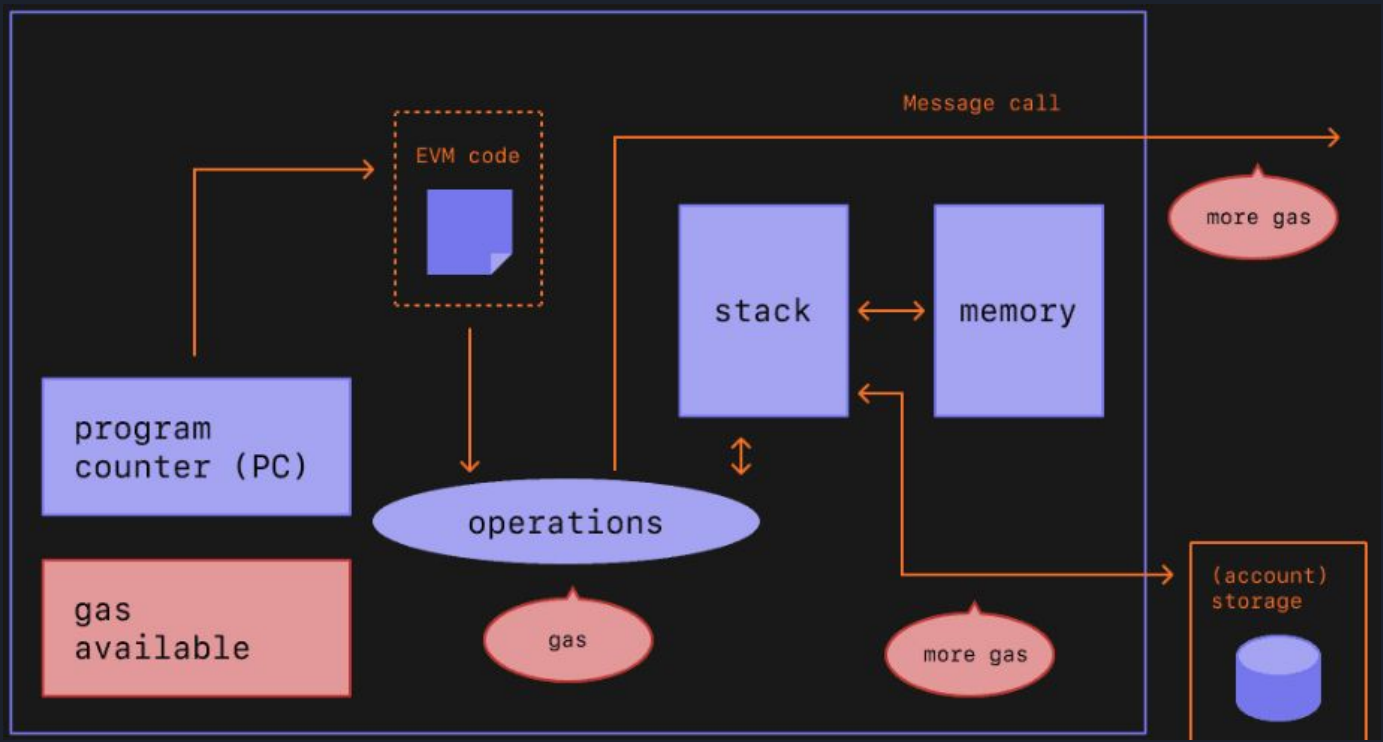


## Distributed State Machine

- Turing complete programs
- Gas to solve Halting problem
- Contract accounts (smart contracts)

# The Ethereum Virtual Machine (EVM)



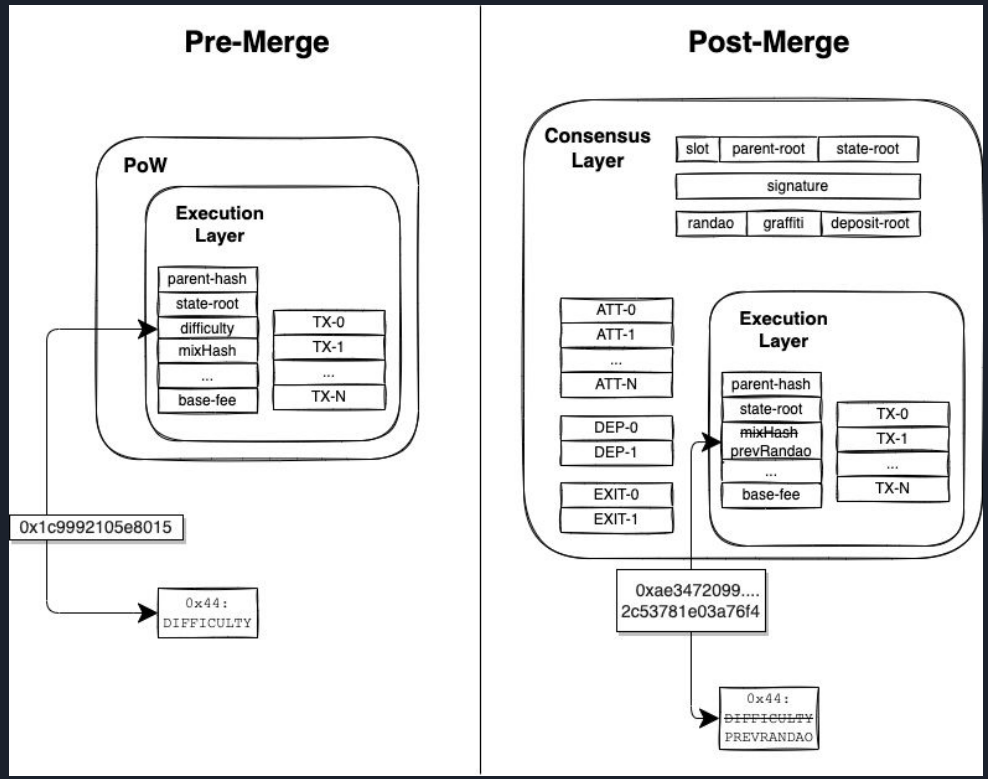



ethereum.org/en/developers/docs/evm [F.2]

# Upcoming Ethereum Merge

Impact on developers

- ❏ EIP 4399 - detect The Merge
- ❏ Blocktime exactly 12 seconds
- ❏ Block structure change
- ❏ OpCode change
- ❏ NO CHANGE on client side




https://blog.ethereum.org/2021/11/29/how-the-merge-impacts-app-layer

# Decentralized Application (DApp)

Decentralized Applications are applications that have multiple instance running on decentralized network instead of relying on a single authority, typically come with a sets of smart contracts and an user interface [4]

## Decentralized

Free from authority control and censorship

## Deterministic

Programs' logic function irrespective of execution environment

## Isolated

Failure or bugs can't be broadcasted to others applications

## Turing complete

Can execute arbitrary logic given the resources

# Benefits of Dapps

User Privacy


Zero Downtime


No Censorship

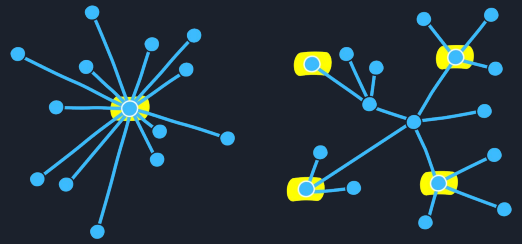
Absolute Data Integrity

Verifiable Behaviors

# Drawback of Dapps

Complex maintenance

Network congestion



Not fully decentralized

Performance Overhead

# How to Develop Smart Contracts?

# Set up

MetaMask

Remix IDE

# Create your Metamask account


https://www.one37pm.com/nft/how-to-set-up-metamask-wallet
(or quickly follow a written guide)

# Smart contracts prototype using Remix IDE

**Blazingly Fast Smart Contract Prototyping**

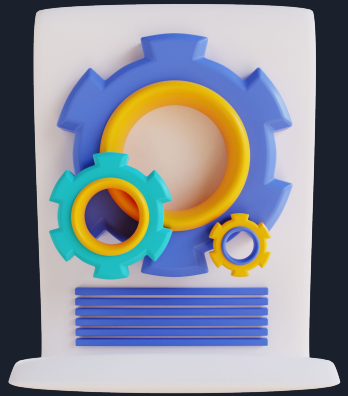
**Desktop/Browser compatibility**

remix.ethereum.org

**Official Ethereum Support**

# Learning with Scaffold-ETH

**Scaffold-ETH is a powerful boilerplate**
**https://github.com/scaffold-eth/scaffold-eth**



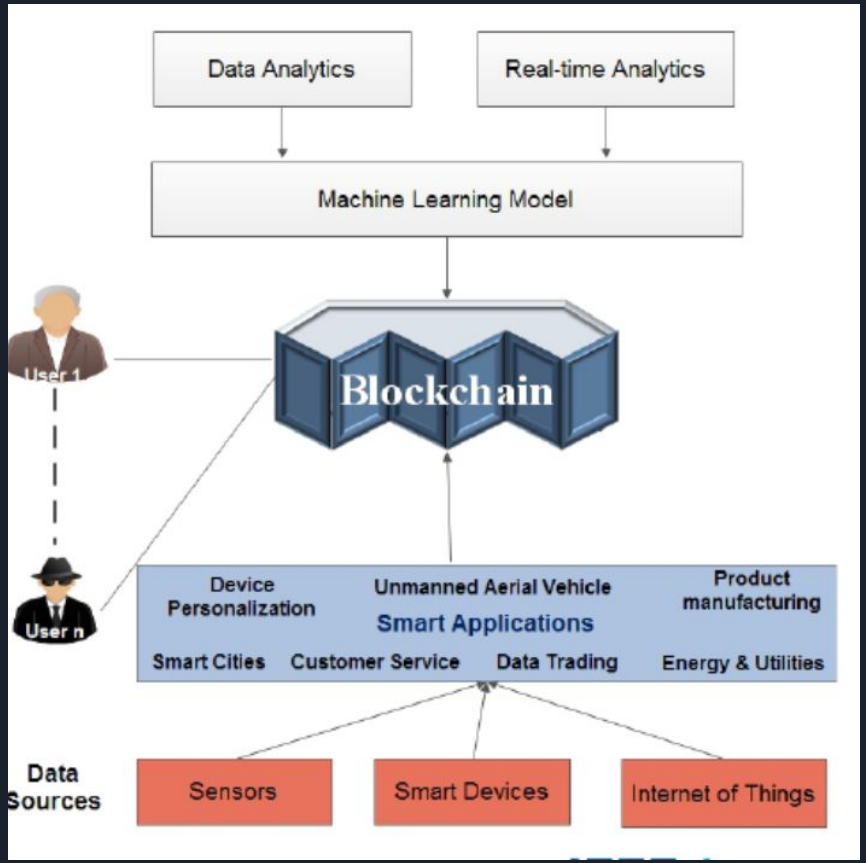
**Full stack with various fields & technology**

**Actively maintained, contain examples & quests**

# Blockchian and Machine Learning

# Two Possible directions

- ML to enchance the security of blockchain
- Use data in blockchian for ML




https://analyticsindiamag.com/how-machine-learning-can-be-used-with-blockchain-technology/

# Combined values of blockchain and AI

- Authenticity
- Augmentation
- Automation

https://www.ibm.com/topics/blockchain-ai

# Thank You!